HAKIN9
ON DEMAND

Vol.2 No.10
Issue 01/2013(10) ISSN: 1733-7186

SPECIAL PUBLICATION
60+ PAGES

CYBERSECURITY
WILLIAM F. SLATER III PREPARES YOU FOR CYBERWAR AND CYBERATTACKS

HACK ME? NO, HACK YOU! THE PROS AND CONS OF ACTIVE CYBER DEFENSE

BASICS OF PACKET CRAFTING

THE RIGHT TO ANONYMITY

PLUS

INTERVIEW
WITH ASEEM JAKHAR, THE FOUNDER OF NULLCON SECURITY CONFERENCE

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch

Atola TECHNOLOGY

Visit atola.com for details

CRACK HACK FORUM

CHF is regarded as one of the best online hacking communinity with over 76k+ members.

CHF was created by a renowned hacker and web specialist named ProVirus.

-CHF-

- CHF has over 2k+ tutorials teaching you the very art of hacking from the very basic to the most advanced level.
- Has a special forum for cracked premium accounts worth thousands of dollars.
- The VIP section is filled with the tools and tutorials unseen elsewhere making the section unique.

Join CHF NOW!!!

www.CrackHackForum.com

Greetings to: Srinuboy, Terrorbyte, Rain112, Hacker4life, Rynaldo, Mschoudhry, fakhru

Hakin9 ON DEMAND team

Editor in Chief: Ewa Dudzic
ewa.dudzic@hakin9.org

Managing Editor: Ewa Duranc
ewa.duranc@hakin9.org

Jakub Walczak
jakub.walczak@hakin9.org

Editorial Advisory Board: Arsen Darakdjian, Scott Paddock, Matthew Holley, Derek Thomas, Kishore P.V.

Proofreaders: Ewa Duranc, Jakub Walczak, Derek Thomas, Kishore P.V.

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org

DTP: Ireneusz Pogroszewski

Marketing Director: *Pawel Plocki*
pawel.plocki@software.com.pl

Publisher: Hakin9 Media
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Dear Hakin9 Readers,

We have survived the end of the world and we are entering the new year with an issue devoted to Cybersecurity. We have done our best to bring you quality articles from our experts and we hope our January edition will provide you with valuable knowledge. This month, William F, Slater, III explains how to get your organization ready for cyberwar, Terrance Stachowski discusses active cyber defense, and Luciano Ferrari takes up industrial cybersecurity. Moreover, Pierluigi Paganini introduces you to anonymizing your network, Pankaj Patel explains how to keep web apps secure, and Mark Painter addresses the top three mobile application threats nowadays. In addition, our editor Ewa Duranc talks with Aseem Jakhar, the founder of nullcon Security Conference.

Hakin9's editorial team would like to give special thanks to the authors, betatesters, proofreaders and our editor in chief, Ewa Dudzic.

We hope that you will enjoy reading this issue!

Ewa Duranc, Jakub Walczak
& the Hakin9 Team

CONTENTS

"The journey of a thousand miles begins with a single step." Lao Tzu
One of your step is here…

Packet Manipulation

using hping2

In this fast growing digital world of internet billions of people are using internet. The base for this internet is bits then bytes and data which are called as packets. Now we are going to analyze these packets.

I love packets. Bcoz it is sweet. Do you want to taste it?

TCP is known as Transmission Control Protocol and it is the important protocol used in the internet today because it is connection oriented, reliable, provide no duplication and it uses Three-way Handshake mechanism (SYN, SYN-ACK, ACK) which ensures the connection between the client and the server system. It is a connection oriented protocol because it establishes a virtual connection before the data can be transferred between two systems. Reliable, it ensures that the data are delivered in the correct order in which order they were send. It works in Transport layer (Fourth layer) of OSI model. A TCP connection is identified by using the following parameters.

Ex: Source ip address, Source port, Destination ip address, Destination port (Table 1).

UDP

UDP is known as User Datagram Protocol it is a simple, connectionless protocol because the datagrams are not numbered even though sent by different users. It works in the Transport Layer (Fourth Layer) of the OSI model. It provides some error recovery services and it's primarily used for broadcasting messages over a network for maximum speed and bandwidth utilizing services such as video streaming, video conference and online games. A UDP connection is identified as like TCP connection.

Ex: Source IP address, Source port, Destination IP address, Destination port (Table 2).

The Figure 1 the TCP header format in which it uses 32 bit format, the source port uses 16 bits and it is used to uniquely identify the source port (Sender). The destination port also uses 16 bit and is used to identify the receiving port (Receiver). Each transmitting packet having the random initial sequence number which is used to keep track of how much data has sent and the acknowledgement number is increased by one with of sequence number to inform that the data was received successfully. Header Length is

Table 1. *Popular ports used by TCP*

S.No	Port	Protocol	Description
1	20 & 21	FTP	Data port & Control port
2	23	TELNET	Terminal Network
3	25	SMTP	Simple Mail Transfer Protocol
4	53	DNS	Domain Name Server
5	80	HTTP	Hyper Text Transfer Protocol
6	443	HTTPS	Hyper Text Transfer Protocol Secure

Table 2. *Popular ports used by UDP*

S.No	Port	Protocol	Description
1	13	Daytime	Returns the date and the time
2	53	Nameserver	Domain Name Service
3	69	TFTP	Trivial File Transfer Protocol
4	111	RPC	Remote Procedure Call
5	123	NTP	Network Time Protocol
6	161	SNMP	Simple Network Management Protocol

known as header length it used to indicate that were the data begins and always it uses multiples of 32 bits. Window size is used to mention the sender receiving capacity by default it uses bytes. Checksum is used to check the values of the header and the data to ensure that there is no modification in the information. Urgent pointer is used if the URG flag is set, then the sequence number indicating the last urgent data byte. We have some optional value to mention in this header such as optional data and its length (Table 3).

"As a young boy, I was taught in high school that hacking was cool." Kevin Mitinick.

The above UDP diagram uses the 32-bit format in which the source port uses 16 bits and it is used to uniquely identify the source port (Sender). The destination port also uses 16 bit and is used to

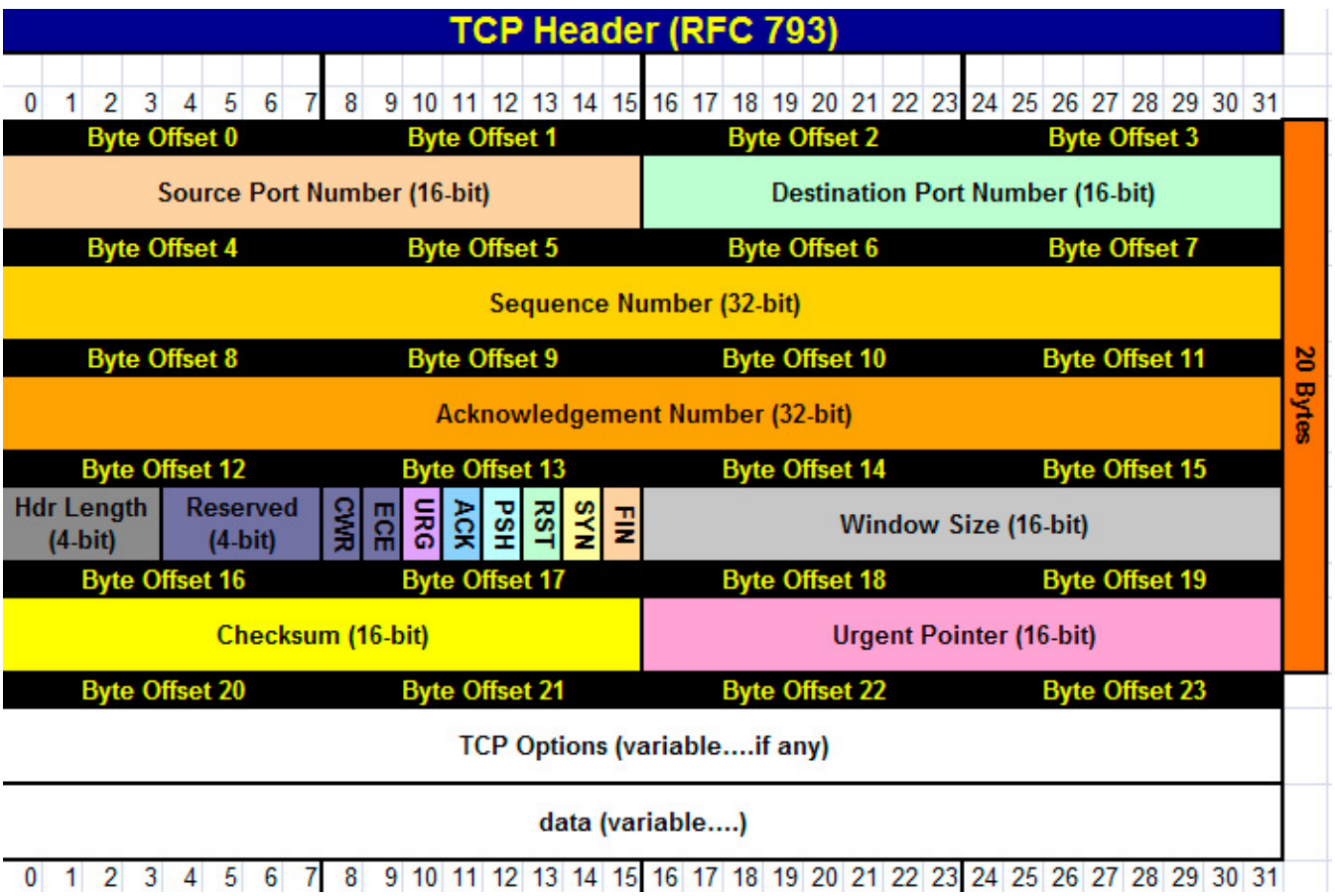


Figure 1. *TCP Header Information*

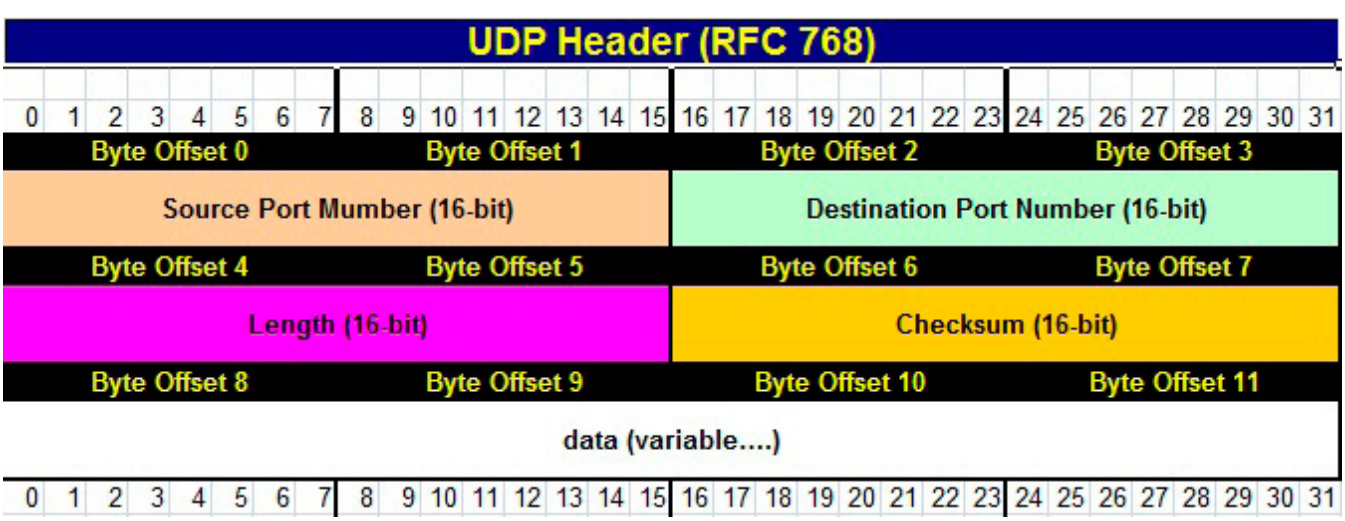


Figure 2. *UDP Header Information*

identify the receiving port (Receiver). These ports are used to assume that if it is a need to reply for request then these ports are used. If the source port as a client then it uses the ephemeral port numbers. If the source is a server then it uses the well-known port number. The length field is used to indicate the header and data length in bytes. The checksum field is used for error checking of the header and data.

"The world is a book and those who do not travel read only one page." Saint Augustine

Fragmentation

It is way of breaking the large IP packet in to smaller ip packets by fitting to a network MTU (*Maximum Transmission Unit*). If the transmitting packet is longer than the MTU, then the router fragments the packet. It may be done multiple times along route. The ip fragmentation process is done by the following:

- Extract the data field from the incoming packet.
- Divides the data field in to smaller fragments.
- Sends each fragment in its own ip packet.

For an example if the MTU having 600 octets and ip header hold 20 octets then the remaining 580 octets only available for data in each fragmented ip packet (Figure 3).

These fragmented packets are reassembled (defragmented) by the destination host.

Table 3. *TCP Flags*

Flags	Description
URG	Urgent Pointer is used for sending interrupts when set to 1
ACK	Acknowledgement used to acknowledge the connection
PSH	Push it will push the data to the stack
RST	Reset used to reset the connection
SYN	Synchronization used to setup the connection
FIN	Finish it will terminate the connection

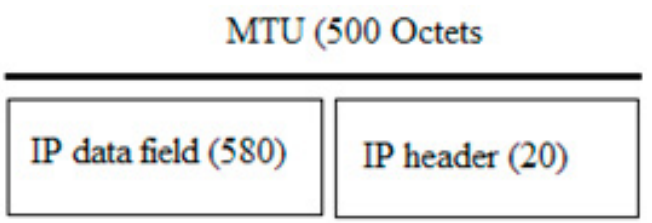


Figure 3. *Fragmentation example diagram*

Protocol Benders

Some of the applications are deviated from its normal behavior because they were designed differently. The following are the well-known protocol benders FTP, UNIX Trace route. I hope now you have more interest because you know very well about these both but you may don't know these are protocol benders.

FTP (File Transfer Protocol)

Let us see how FTP is a protocol bender. The expected behavior of FTP is it uses two ports one is used for client and another one is used for server during the three-way handshake mechanism. It uses one ephemeral port and one server port for the FTP connection while send/receive the data. FTP is slightly differ from the normal TCP communication model because it uses the two ports first port is used for controlling the FTP connection, the second one is used for exchange the data between the client and the server.

Unix Traceroute

It combines ICMP and UDP to navigate from source to the destination and it record all the paths it passing through the routers. It is similar to Windows Tracert it uses ICMP to discover but Unix Traceroute uses UDP to discover the host.

You should be aware that the both UNIX trace route and Windows Trace route only works if specific ICMP messages are allowed into the network. Both versions require that ICMP "time exceeded in-transmit" messages be allowed in to the network. The UNIX traceroute requires that ICMP "port unreachable" messages be allowed, and Windows tracert requires that ICMP echo requests be allowed.

"If you don't know where you're going, any road will take you there." George Harrison

Packet Crafting

Packet crafting is the heart of intrusion detection system and of understanding what is actually occurring in a network. As we know that these vulnerability assessment tools used by network engineers to test the security of their network, the same tool can also be used by hackers to find the vulnerabilities and to exploit them.

Steps:

- Packet Assembly.
- Packet Editing.
- Packet Playing.
- Packet Analyses.

Packet Assembly
This is the first step in packet crafting process, to decide that which network to be tested or hacked and tries to gather the vulnerability in the system.

Packet Editing
It is the second step in packet crafting process to add the values such as payload, checksum to gain as much information as possible.

Packet Playing
After creating the packet we have to send it to the target network and then collect the replaying packet to analyze the expected results. If the expected outcome is not achieved then you have to edit the scenario.

Packet analyzing
The collected packets are analyzed by using the tools like wireshark or any other network protocol analyzer (Table 4).

Packet crafting Techniques

As seen above, now we know the whole idea behind packet crafting to try to stimulate an attack, this will help you to learn about various networking device and their vulnerabilities. The most important thing is it can also be used to attack Web servers and other application gateways. The following are various packet crafting techniques.

- Ping fragmentation.
- Packet flag manipulation.
- Packet duplication.
- Protocol manipulation.
- Half open packets.

Ping fragmentation
The attacker try to send the maximum packet size which needs a reply, while replying the target also respond with larger packet size which consumes lot of bandwidth at the end denial of service. By sending ACK flag in the packet it confuses the destination service and closes the legitimate connection.

Table 4. *Various packet manipulation tools*

Method	Tools		
Packet Crafting	Hping2,	Colasoft packet builder	Scapy
Packet editing	Winsock Packet Editor	Netdude	Mergecap
Packet Replay	Netcat	Tcpreplay	Ostinato
Packet analyzer	Wireshark	Tcpdump	Capsa

Packet flag manipulation
As I mentioned above in TCP flags table, you know very about the flags. In three- way handshake mechanism, a SYN flag is set in the packet and sent to a destination to establish a valid TCP communication. This can be exploited by sending a RST or FIN packet, which reset or terminate the connection.

Packet duplication
The evil hackers capture the no of packets and resend it over the network. This will confuse the target system, which assumes that the previous connection was not properly answered or terminated. Real-time example of this attack is when a duplicate ACK or FIN packet is sent to the target without modifying any other data in the frame. This will cause the denial of service attack which makes the network resource unavailable.

Protocol manipulation
This method is used to test the vulnerability in the firewall. To confuse the firewall the flags like RST, FIN are set in the TCP and UDP protocol which reset the connection or terminate. The olden firewalls not able to handle this rule and shutting down but recent firewalls identify this behavior and drop the connection.

Half open packets
In TCP communication model we say half-open connection, when a host sends a SYN packet to destination and waiting for the SYN-ACK packet. Now the destination sends SYN-ACK packet however, the attackers does not reply to it, and instead they create a spoofed IP packet by changing the source IP and sending another SYN packet to the destination. This will cause the denial of service attack.

Introduction to Hping

Hping2 is a command-line oriented TCP/IP packet assembler and analyzer. It supports TCP, UDP, ICMP and RAW-IP protocols. It was main-

Table 5. *Different modes of hping*

S.No	Mode	Description
1	Tcp	Default mode
2	-0	Raw ip mode
3	-1	ICMP mode
4	-2	UDP mode
5	-8	Scan mode
6	-9	Listen mode

ly used as a security tool by network administrators. By default hping uses TCP mode, the following table shows the different modes (Table 5).

Features:

- Firewall testing.
- Port scanning.
- Network testing.
- Remote OS fingerprinting.
- It is also used by students to learn TCP/IP

For more detail and to download, visit *http://www.hping.org*. It is also available in Backtrack.

Craft TCP packets using hping2

Craft is a kind of art to make something; here we are going to create a TCP packet by specifying the TCP flags, destination port and a target address. Before sending the packets to the target you should be aware that, if you do not specify destinations port it will use default value as 0. If you do not specify the source port it will use random ephemeral port (Table 6 and Figure 4).

Use this help command to know some basics syntax and types `hping -h or hping -help`.

First we have to check that our target is alive or not, issue this command in your backtrack4.

Go to Menu > backtrack > Network Mapping > Identify Life Hosts > Hping2.

```
# "hping --icmp 192.168.1.6"
```

The above screen shot shows that the `icmp` command and the target is 192.168.1.6 marked in red box. It sends and receives the 7 packets and there is no packet loss in this time period marked as red.

Table 6. *Basic switches in hping*

S.No	Protocol	Switches	Description
1	usage	-c	Count packets
2	usage	-v	Ccurrent version
3	ip	-a	Spoof ip address
4	ip	-t	ttl default (64)
5	icmp	-C	default echo request
6	tcp/udp	-s	Source port
7	tcp/udp	-p	Destination port
8	tcp/udp	-q	Sequence number
9	tcp/udp	-M	Set TCP sequence number
10	tcp/udp	-L	Set TCP acknowledgement number

Table 7. *Notorious Hping commands*

S.No	Command	Description
1	hping -icmp TARGET IP	Check the target is alive
2	hping -d 500 TARGET IP	To send 500 bytes of data
3	hping -j TARGET IP	To produce the values in hex format
4	hping -S TARGET IP -p 445	To make SYN request to destination port
5	hping -2 TARGET IP	To add UDP packet with request
6	hping -1 TARGET IP	To make the ICMP request
7	hping -F TARGET IP -p 135	To send FIN packets to the destination ip and port
8	hping -R TARGET IP	To send the Reset packets to the destination
9	hping -a 122.122.122.122 -S TARGET IP	To send SYN packets using spoofed ip address
10	hping -SFPUA -c 4 TARGET IP	This will send one SYN, FIN, PUSH, URG, ACK flags set

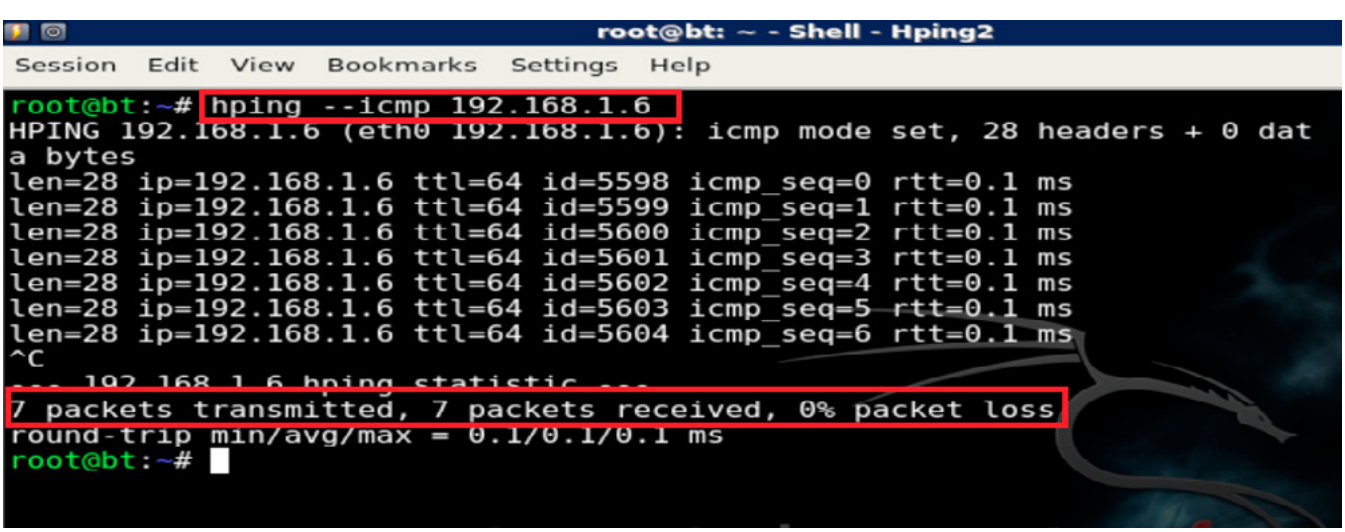


Figure 4. *hping2 interface*

Note
By default hping command continuously send packets to the target, to avoid this you can add "-c" to your command. This is to denote that the no of packets will send to the target.

Now you have the basic idea about the hping, flag and protocols so now we are going to do some evil thing which makes you more interesting and knowledgeable at the end (Table 7 and Figure 5).

Use of wireshark

Wireshark is a network protocol analyzer which capture the packet and display the packet as detailed as possible. It can use it to troubleshoot network problems, examine security problems and debug protocol implementation. Start this program after hping and before tcpreply.

Open the wireshark it will work in both UNIX and Windows operating system. Now select the interface using the capture button in the menu bar, a new window will open then select the interface you want to capture.

Replaying captured packets

TCP replay is a tool for replaying network traffic from files which saved by tcpdump. Tcpreply resend all packets from input files at the speed which they were recorded a specific data rate, or as fast as the hardware is capable. This is used to test the network devices such as routers, bridges and other gateway devices.

Basic Usage

Now you have to specify the pcap file and the interface to send the traffic out interface `etho`:

```
# tcpreplay --intf1=eth0 sample.pcap
```

You can specify the different speeds

To replay traffic as soon as possible:

```
# tcpreplay --topspeed --intf1=eth0 sample.pcap
```

To replay traffic at a rate of 5 Mbps:

```
# tcpreplay --mbps=5.0 --intf1=eth0 sample.pcap
```

To replay traffic 5 times as fast as it was captured:

```
# tcpreplay --multiplier=7.3
--intf1=eth0 sample.pcap
```

To replay traffic at half-speed:

```
# tcpreplay --multiplier=0.5
--intf1=eth0 sample.pcap
```

To replay at 30 packets per second:

```
# tcpreplay --pps=30 --intf1=eth0 sample.pcap
```

To replay packets, one at a time while decoding it (useful for debugging purposes):

```
# tcpreplay --oneatatime --verbose
--intf1=eth0 sample.pcap
```

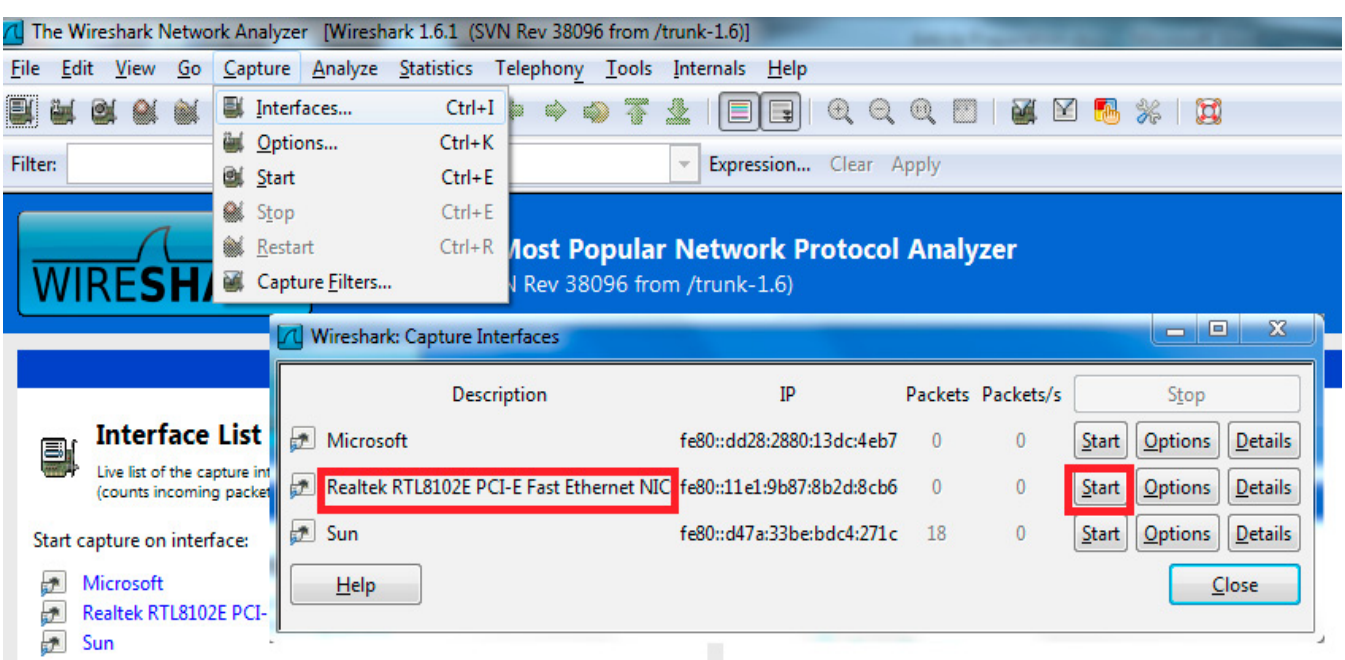


Figure 5. *Wireshark interface selection*

On the web

- *http://www.hping.org*
- *http://wireshark.org*
- *http://tcpreplay.synfin.net/*
- *http://www.linuxforu.com/2012/05/cyber-attacks-explained-packet-crafting/*

Replaying files multiple times

Using the loop flag you can specify that a pcap file will be sent two or more times:

To replay the sample.pcap file 20 times:

```
# tcpreplay --loop=20 --intf1=eth0 sample.pcap
```

To replay the sample.pcap forever or until CTRL-C is pressed:

```
# tcpreplay --loop=0 --intf1=eth0 sample.pcap
```

How to use tcpreplay tool

The above diagram shows that "tcpreplay" command and then the interface you going to use basically we are using etho (Ethernet interface) then the pcap file:

- Result 1: `tcpreply` command with the interface `-intf1=eth0` then the pcap file "`test.pcap`".
- Result 2: The no of packets send "26 packets" and with the speed of 0.12 Mbps.
- Result 3: It is same as result1 but using another file called `test2.pcap`.
- Result 4: The no of attempted packets and the successfully sent packet.

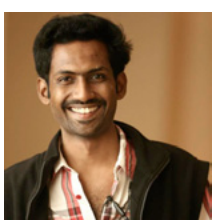
```
root@bt:~# tcpreplay --intf1=eth0 test.pcap    1
sending out eth0
processing file: test.pcap
Actual: 26 packets (5941 bytes) sent in 0.38 seconds
Rated: 15574.2 bps, 0.12 Mbps/sec, 68.16 pps    2

Statistics for network device: eth0
        Allempled packets:         26
        Successful packets:        26
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@bt:~# tcpreplay --intf1=eth0 test2.pcap    3
sending out eth0
processing file: test2.pcap
Actual: 42 packets (4612 bytes) sent in 0.67 seconds
Rated: 6821.7 bps, 0.05 Mbps/sec, 62.12 pps

Statistics for network device: eth0
        Attempted packets:         42    4
        Successful packets:        42
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@bt:~#
```

Figure 5. *TCP Replay*

Summary

As I mentioned above, the packet crafting attack is difficult to take on. First the company's network administrators and network engineer should understand their network, and they have to create their own security testing scenario to test their networking devices such as, firewall, IDS, IPS and routers. To protect your organization you should have the various level of defense security system for your network infrastructure.

VINOD SENTHIL



Vinod Senthil is the Director of infySEC, he is also a renowned Ethical Hacker and Cyber Crime Consultant who has worked with sensitive projects both in India and abroad. Having worked with 85 of the Fortune 500 companies, his work has gotten him recognition even from the likes of Mr. David Filo (Co-Founder, Yahoo!). He has written on various IT security topics ranging from wireless insecurities to website defacement. He has conducted numerous successful workshops nationally and internationally and has been covered by multiple prestigious English dailies and featured in many national Television Channels. He has helped both the Cybercrime department and banks to fix a major flaw in Credit Card industry. He is known moderating sessions for ASSOCHAM along with the Council of Europe, Strasbourg, France and the Ministry of Communications and Information Technology on "Cyber & Network Security" with the theme as "Safeguarding the Digital Economy".

Contact details:

vinod@infysec.com

https://www.facebook.com/vinodh.t

http://www.linkedin.com/in/vino007

NAGENDRAN

Nagendran is a B.Tech in computer science and engineering and he is passionate with network / cyber security and ethical hacking. He started his carrier as an associate security consultant at infySEC with prime focus on Networks and Hosts. He has been involved in Network Security research and packet crafting. He has been working extensively on DDOS and IRC based Botnet research. He is a part of Vinod Senthil's technology team.

Contact details:

nagendran@infysec.com

https://www.facebook.com/nagendran2012

http:// in.linkedin.com/pub/nagendran-r/28/a40/911

Technology is a double sided sword.
Internet makes you naked online!
Get Secured & Get Certified!

Welcome to the world of Certified Ethical Cracker with Hands-on practical sessions.

CERTIFIED ETHICAL CRACKER

An Advance **Information Security** Course

For more detais, visit:
http://www.infysec.com/training/courses/certified-ethical-cracker

infySEC UK :

145-157, St.John Street,
London, EC1V 4PW
England, UK

Phone: +44-7405190001

infySEC India :

#37/45, P.H Road,
Arumbakkam,
Chennai- 600106
TamilNadu, INDIA

Phone: +91-44-42611142,43

infySEC
Demystifying Innovations

www.infysec.com

enquiry@infysec.com

Applying a

Security Compliance Framework to Prepare Your Organization for Cyberwar and Cyberattacks

On Monday, CNN posted a web article with this headline, Nations Prepare for Cyberwar describing the inevitability of a cyberwar that is coming or possibly already here (Goldman, 2013).

One of the main disadvantages of the hyper-connected world of the 21st century is the very real danger that countries, organizations, and people who use networks computer resources connected to the Internet face because they are at risk of cyberattacks that could result in anything ranging from denial service, to espionage, theft of confidential data, destruction of data, and/or destruction of systems and services. As a recognition of these dangers, national leaders, business leaders and military of most modern countries are now acknowledging that the potential and likely eventuality of cyberwar is very real. This article will introduce come concepts about the realities and weapons of cyberwarfare and discuss how an organization can use a security compliance framework of controls to mitigate the risks of cyberattacks and cyberwarfare.

The Simple Truths of this Article

- Cyberwar is coming or could be already here. All the signs and news media coverage and publicly known actions of the U.S. Government confirm it
- If you use have an IT infrastructure that is important to your business operations, you need to protect your business from Cyberattacks and Cyberwarfare
- There are many things you can do, and things you cannot legally do if you are in the United States, to protect your business from Cyberattacks and Cyberwarfare. Restrictions inside the U.S. Code, Title 10, and other various cyber legislation strictly prohibit retaliation or going on the offensive. But you can prepare and protect yourself from cyberattacks.
- In any organization, Management Support is required to understand and allocate the resources to defend against cyberattacks.
- Understanding risk identification, threats, vulnerabilities, controls, performing risk assessment, and risk management are essential to becoming an effective protector of IT assets.
- Because of the complex nature of most IT infrastructures and assets and how they integrate with an organization's business operations, it is better to use some type of proven framework with which to assure that all the important aspects of compliance and infrastructure security have meet address and are being measured.

Cyberwar Concepts

Cyberattacks and cyberwarfare tactics, by some expert estimates, date back to the early 1980s when there was a set of suspicious explosions that were likely generated in control systems on some pipelines in Asia, though this has never been conclusively confirmed. However, the idea of using computers and software to attack another entity via networks dates back to the early 2000s and by some accounts, well before that. The diagram from Lewis University shows a brief graphic history between 2000 and 2009 (Figure 1).

Cyberweapons That We Know About

Cyberattacks and cyberwarfare tactics have typically been in the realm of Distributed Denial of Ser-

vice (DDoS) attacks with some more sophisticated attacks as shown in the Technolytics diagram in Figure 2.

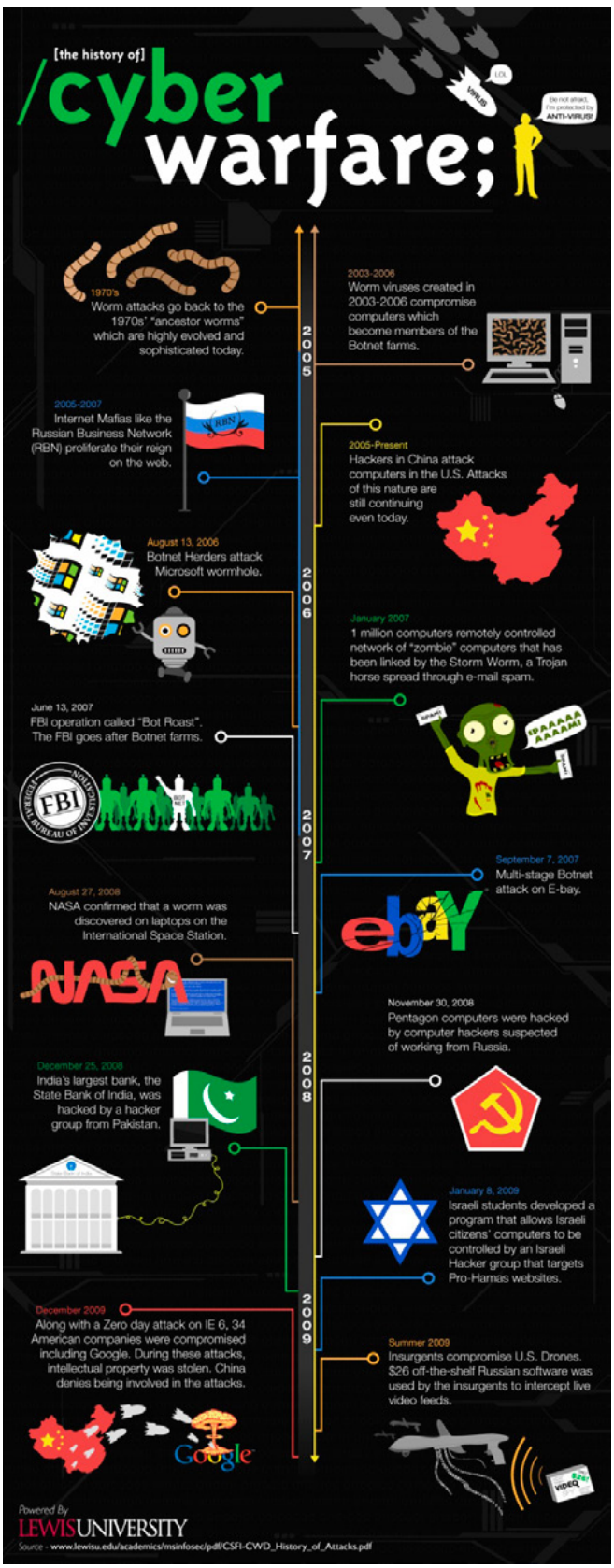


Figure 1. *A Brief History of Cyberwarfare by Lewis University, Romeoville, IL*

Since 2007, as the existence of well-orchestrated cyberwar attacks such as the DDoS attacks on Estonia (2007), Georgia (2008), and Kyrgyzstan (2009), as well as the Stuxnet (2010), Duqu (2011), and Flame (2012) have all become known to the world through security researchers, their victims, and the media. As a result, it has become apparent most who are watching this area that cyberspace has now become the new realm onto which the field of international conflict has been extended, and that cyberwarfare is now no longer a theoretical issue that could one day threaten those participants and systems that rely upon connections to the Internet and Internet-connected networks. Unfortunately however, despite the emergence of a new breed of intelligent cyberweapons (i.e. Stuxnet, Flame, Duqu, and Shamoon) with the ability to strike with precision and accuracy, the present findings and research on cyberwarfare related events shows that the U.S. is playing catch-up and doing so badly (Turanski and Husick, 2012).

The Figure 3 shows the rapid evolution of cyberweapons over time. It is obvious that according to this diagram, starting in about 2008, until what is predicted to be about 2020, the evolution of the sophistication of cyberweapons will be be quite significant. This rapid rise in sophistication and capabilities of cyberweapons, coupled with their relative ease of use, proliferation and economic benefit, will make these weapons very compelling for military and strategic use, and make the likelihood of cyberwar increasingly significant for the foreseeable future.

Who Is the "Enemy" or the "Adversary?"

In the world of cyberattacks and cyberwarfare, the issue of who your adversary usually depended on your perspective. From the perspective of the U.S. and its allies, the adversary usually falls into one of these five categories: Russia, China, North Korea, Iran, or non-state actors. Much is already known about our potential adversaries, such as Russia, China, North Korea and Iran, but what is perhaps less understood is the degree to which they have been successful in integrating cyberwarfare and cyberdeterrence capabilities into their own national war plans. Nevertheless, due to the previous extensive experience of China, Russia and the U.S. with strategic war planning, it is more likely that each of these countries stand the greatest chance of making integrating cyberwarfare and cyberdeterrence capabilities into their respective war plans. Yet, as far back as June 2009, it was clear that the U.S. and Russia were unable

to agree on a treaty that would create the terms under which cyberwarfare operations could and would be conducted (Markoff, J. and Kramer, A. E., 2009).

DDoS as a Service, as low as US$20 Per Hour

We now live in a world where the Internet and malware have made it possible to buy services such as DDoS attacks against an enemy or a competitor for prices as low as $20 hour. When you consider the implications of this idea, the economic will make the idea of tactical cyberattacks more appealing to organizations. I know some of the URLs where these

Figure 3. *Evolution of Cyberweapon Capabilities, 1994 – 2020, by Technolytics*

Cyber Weapons Class Capabilities Assessment

Threat Class	Threat Class Rating	Working Definition	2007 Threat Rating	2008 Threat Rating	2009 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Spoofing	3.4	As spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	3.5	3.8	3.9	3.0	3.0	3.6
Scanning	3.6	A sequential scan, potential attackers target or will randomly select an IP address in an effort to identify system vulnerabilities.	3.5	4.0	4.1	3.2	3.2	3.7
Dictionary Scanning	3.6	This type of attack exploits buffer overflow vulnerabilities in targeted client software through injection of malicious content.	3.4	4.0	4.0	3.2	3.5	3.6
Digital Snooping	4.5	The monitoring of digital networks or connections to uncover passwords or other data.	2.6	3.9	4.5	4.4	4.5	4.4
DoS & DDoS	2.9	The intentional overloading of a system with incoming traffic to cause system crashes.	2.9	3.9	3.9	1.0	3.8	3.0
Tunneling	4.3	Any digital attack that attempts to get "under" a security system by accessing very low level system functions.	3.4	3.9	4.4	4.5	4.2	3.9
Rootkits	5.0	A software tool that allows attackers to have "root level" access to the computer, which means it runs at the lowest level of the machine - below the OS.	NA	4.2	5.0	5.0	3.2	2.1
Counterfeit Hardware	3.4	The seizure of counterfeit IT equipment has raised concerns over cybersecurity. At this time, no practical method of verification exists and supply chain procurement safeguards are very limited at best.	1.5	2.8	4.2	4.8	2.5	2.0
Micro-processor Threats	2.5	The increasing complexity of modern microprocessor chips is almost certain to lead to undetected errors that can be exploited and the possibility of malicious micro code of circuitry.	1.3	1.6	2.2	4.8	2.1	1.0
Counterfeit Software	3.3	The explosion of counterfeit code has significant security risks. It is very likely that the software is substandard with hidden cybersecurity threats.	1.8	2.0	3.7	4.8	2.5	2.3
Cellular Attacks	2.5	Malware and becoming a node on a BotNet are now threats to cell phone users and services providers around the world. While this activity is relatively new, it is expected to grow rapidly.	NA	2.1	3.0	4.0	1.5	1.6
			1	2	3	4	5	

Figure 2. *Classes of Cyberweapon Capabilities, by Technolytics*

services are available, but rather than give them advertisement, I would just invite you to do an Internet search using your favorite search engine.

Understanding Risks and Threats and Vulnerabilities

To deal with the realities of cyberattacks and cyberwar, one must grasp a few simple concepts related to risk quantification, risk assessment, and risk management. Risk in the world of Information Technology is a calculation of the likelihood of an undesirable event based on the estimated severity of impact when the event occurs, the probability of the event's occurrence, and the ability to detect the event should it actually occur. Usually risk is usually explained and understood in terms of threats and vulnerabilities, and damages to assets. Risk is important to understand because risk reduction is usually accomplished by the application of one or more controls.

Examples of assets that could be impacted by risk in an organization include:

- Physical
- People
- Information (including documentation, strategy, business model, etc.
- Data and Databases
- Organization
- Websites
- Systems
- Servers, Computers, Network Infrastructure components, etc.
- Intangibles (brand, reputation, etc.)
- Services (Including power, cooling, backup power, and services provided to clients)

In addition, in the world of IT, you usually have four basic strategies to manage risk once it has been identified and assessed:

- Mitigate it
- Transfer it
- Avoid it
- Ignore it

I have included some diagrams to help readers understand the relationships between risk, vulnerabilities, threats, assets and controls that reduce risk (Figure 4 and Figure 5).

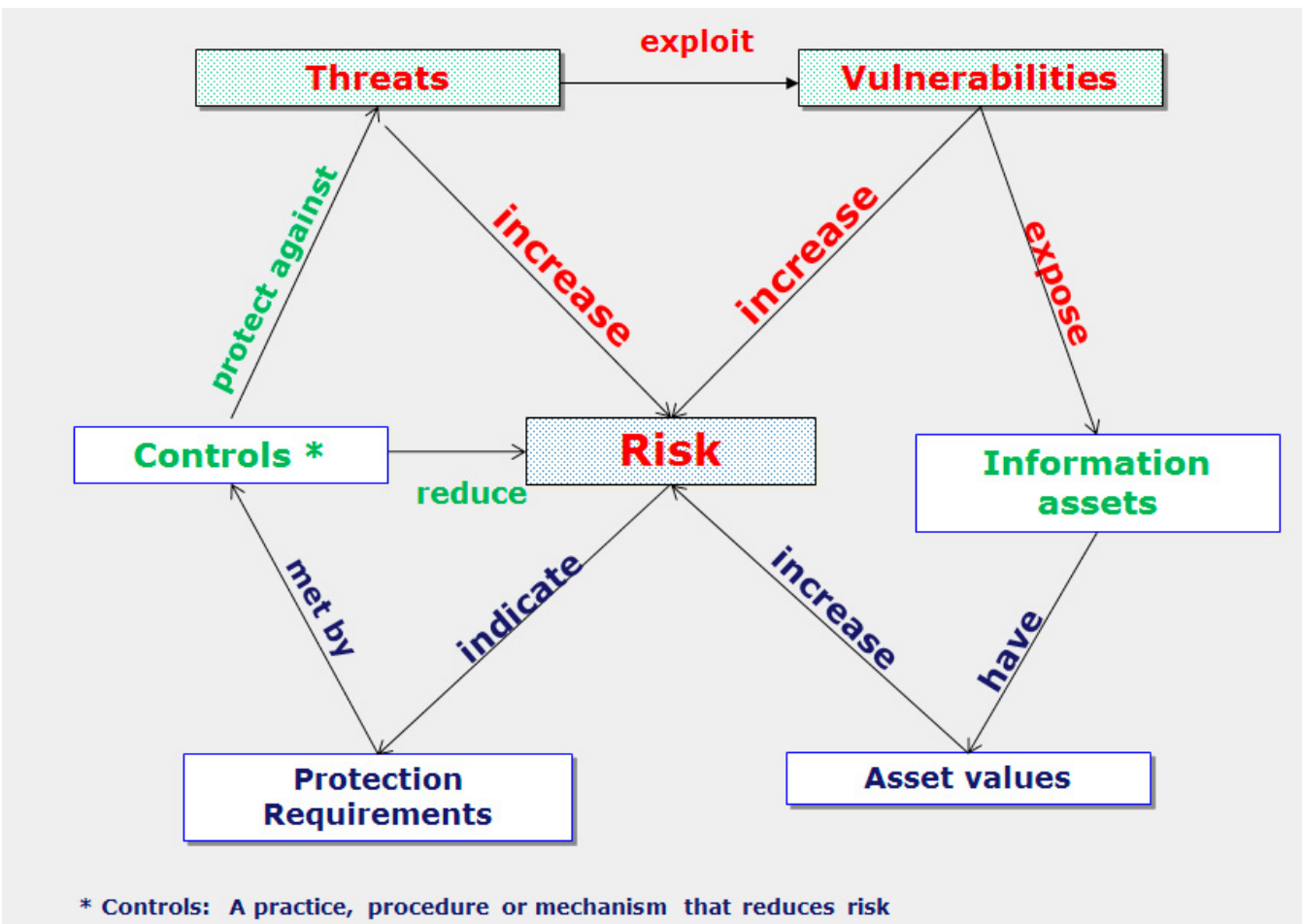


Figure 4. *Risk relationship diagram, from ISO27001.org*

What Is an ISMS?

The fast-paced, electronically-enabled business environment of the 21st century is characterized by the tactical and strategic uses of information as business enablers. In practically every organization, information is now seen as a primary asset and as such, it must be protected. Yet the proliferation and reliance on information in an organization also introduces responsibilities and risks which if not addressed, can subject the organization to extraordinary risks that could severely impact the viability of the business. The best strategy for an organization to manage these new business realities is to adopt a strong compliance management posture in the area of Information Security to ensure that its information assets are protected in the most comprehensive, standardized manner possible. Presently, the best tool to manage the challenges of Information Security is an enterprise Information Security Management System (ISMS). The ISMS is a centralized system of policies, procedures, and guidelines that when created and uniformly applied will provide the best practices to help ensure that an organization's Information Security is being managed in a standardized way using documented best practices. The introduction of an ISMS into am organization's business operations will serve to identify, document and classify information assets and risks and then document the mitigation of risks using established, documented controls. When an organization has chosen the standardized ISO 27001 Security Management Framework the key benefits to implementing an ISMS would be:

- The implementation of a standardized Information Security Management System into the organization
- Better management and fulfillment of the Information Security requirements from the organization's Clients
- Reduction of risks related to cyberattacks and cyberwarfare
- Reduction of risk of loss of existing customers
- Increased opportunities for new business
- Reduction of risk to regulatory penalties
- Reduction of risk reputational damage

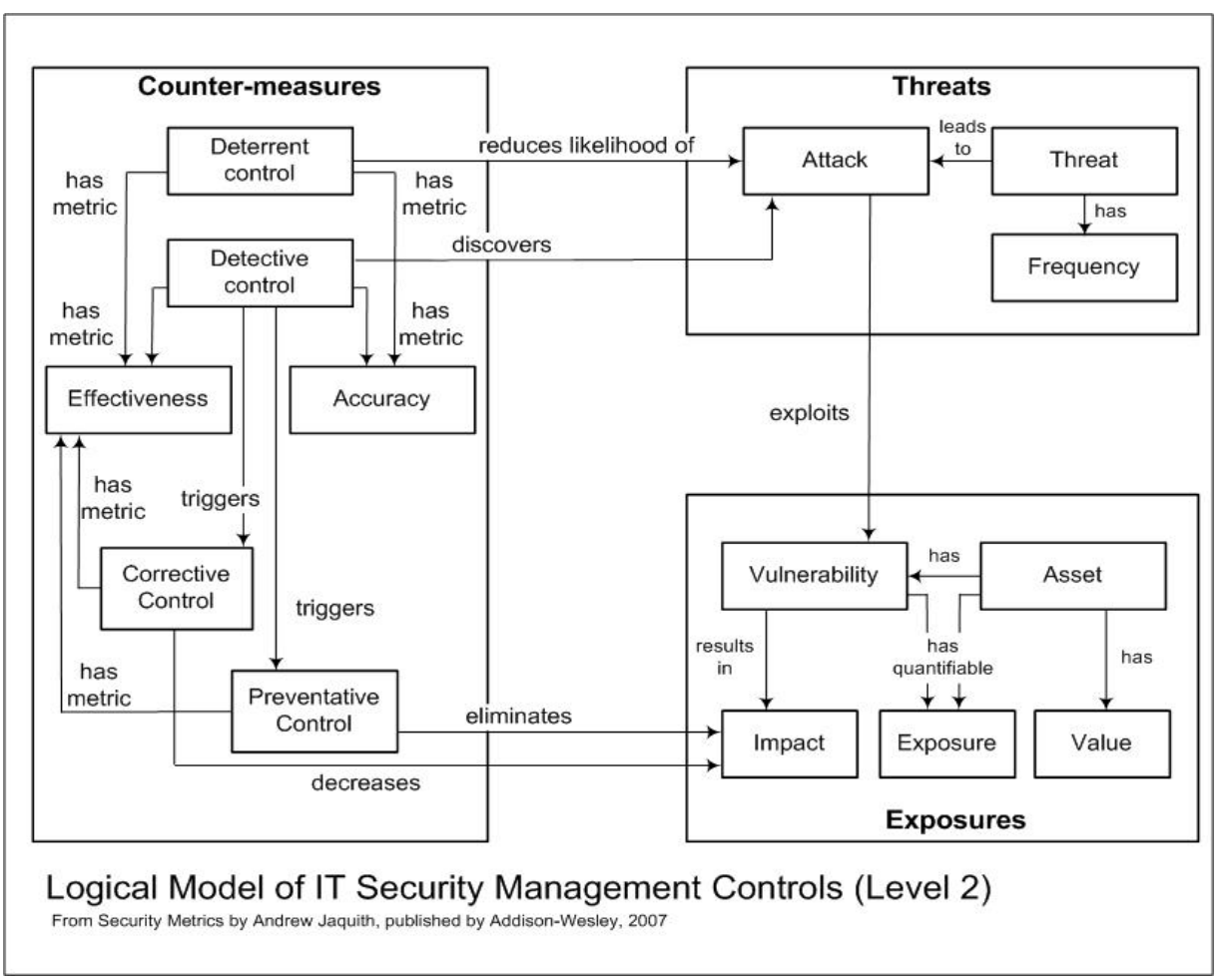


Figure 5. *Relationships between IT security management controls, Threats and Assets (Exposures), Jaquith, 2007*

- The creation of an Information Security-aware culture at the organization
- Enabling ISO27001-compliant offices to communicate and conduct business in areas affected by Information Security in a standard way
- Better management of IT assets and their associated risks
- The ability to have an Information Security Management System that is based on the Deming model of Plan – Do – Check – Act for continuous process improvement
- The adoption of the most widely recognized internal standard for implementing an ISMS

Note that the Information Security has rapidly risen to the forefront as a serious business issue. Because of its rapid rise to prominence and the dynamic and evolving nature of threats and the associated risk management efforts, the models to measure and quantify the value of such projects can often seem frustrating at best. So while this ISMS project may difficult to quantify using traditional methods such as return on investment, it is clear that the benefits of continued customer relationships as well as the ability to attract future customers through a demonstrated strong and continually improving posture of Information Security compliance management will far outweigh the costs associated with an ISO 27001project.

Indeed, after implementing the ISMS under ISO 27001 standards, an organization will have better control of the Information that is the lifeblood of its business, and it will be able to demonstrate to its customers and its business partners that it too has adopted a strong posture of compliance in the area of Information Security.

What is ISO 27001?

ISO 27001 is an international standard with 133 controls in 11 domains which provide structured standard for the creation of an Information Security Management System based on strongly focused risk management and continuous process improvement under the Plan – Do – Check- Act model. The present version was developed in 2005 and an updated version is expected to be published by ISO sometime in 2013. This version is predicted to have several additions that will focus on Cloud Computing and also standardized IT services and service management as described under ITIL and ISO 20000. In fact, in October 2012, the ISO 27013 standard was published and it demonstrates how to integrate an ISO 2000 – based Service Management System with an ISO 27001-based Information Security Management System.

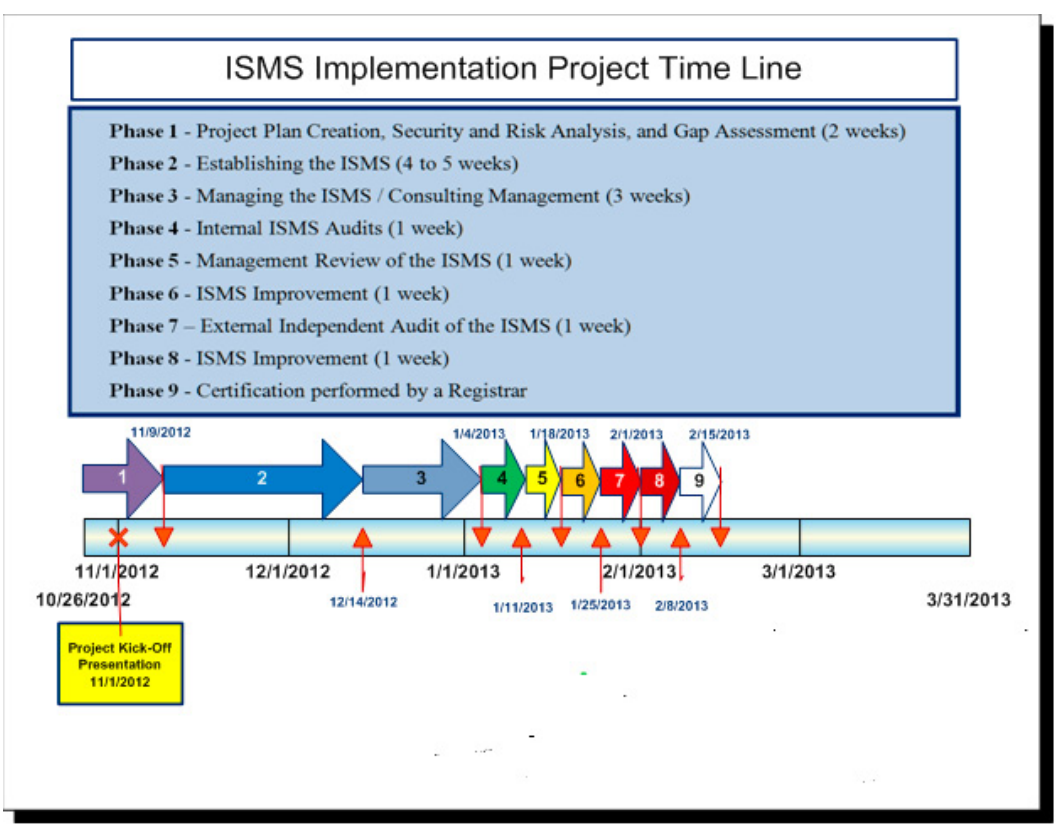


Figure 6. *A Fast-track ISMS Implementation Project Timeline, William Slater, 2012*

What Cyberattack / Cyberwarfare Risk Remediation Project Using ISO 27001 Might Look Like

It is possible to create and implement an ISMS using a fast-track method as shown in Figure 6. Note that management must support such a project in terms of resources (monetary, people, and assets) and politically in order for it to be successful. Nevertheless, it is possible to accomplish such a project if management and the project team have the will and resources to succeed.

Figure 7. *ISO 27001 ISMS Registrants by Continent as of 2011 (source unknown)*

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS *
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	SA-9, SC-8, SC-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
A.10.9.2 On-line transactions	SC-3, SC-7, SC-8, SC-9, SC-14
A.10.9.3 Publicly available information	SC-14
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12

Figure 8. *Mapping ISO 27001 Annex A controls to NIST 800-53 Controls (FISMA)*

Should You Get Your Organization Certified in ISO 27001?

Should you get your organization certified in ISO 27001 if you make the effort to remediate your cyberattack and cyberwarfare risks using an ISO 27001 ISMS control framework? The quick answer is, it depends. Currently, there are less than 9000 ISO 27001 ISMS certificate holders worldwide. Despite the apparent emphasis on security and risk reduction, quite often, organizations will pursue the ISO 27001 certification either to comply with regulatory requirements (as is required in India), or as a business enabler, because their business partners and/or customers expect it or have greater confidence in an organization that has an ISO 27001 certification. Though is is not easy or inexpensive in terms of resources to earn or maintain and ISO 27001 certification, the return on investment, particularly in areas like the North America and South America where the ISO 27001 certification is still relatively rare, can be quite significant.

Figure 7 shows the numbers of ISO 27001 ISMS Certificate Registrants by continent as of 2011. Note that according the PECB, a certification body that trains and certifies ISO 27001 implementers and auditors, the number of ISO 27001 ISMS Certificate Registrants is expected to double each year in North America for the foreseeable future.

Is Compliance with the ISO 27001 Standard or Some Other Security Compliance Framework Still Important Even If Your Organization Doesn't Get Certified?

Personally, I believe that the chief responsibility of the leadership of organization is to recognize risks and reduce them, as cost effectively as possible to manageable levels, and to comply with the laws and regulations that impact its operating environment. Even if an organization does not seek or achieve a certification under a security compliance standard such as ISO 27001, the organization can embrace and comply with the security controls of a security compliance standard, and thereby significantly reduce its business and security risks. The value in each of these security compliance frameworks (i.e. ISO 27001, PSC DSS. FISMA, HIPAA, etc.) is that each offers a set of well defined controls that are structured in a way to allow the organization that adopts then to visibly demonstrate its efforts to reduce risks to its assets and its operating environment.

Mapping to Achieve Compliance with Two or More Security Compliance Frameworks

When an organization is required to comply with two or more security compliance frameworks, a process known as "mapping" using a table showing the similarity of various controls is used to understand and communicate the specific controls of each standard, and usually on a one to one basis.

Typically, the standard that is already in place or the one that is the most familiar is represented on the left column, and the newer standard that is required for a new compliance initiative is located on the right column. An example is shown in Figure 8.

Using ISO 27001 Controls to Defend Against Cyberwarfare and Cyberattacks

Of the 133 controls defined in Annex A of the ISO 27001 standard, not all of these are required to reduce the risk of cyberattacks and cyberwarfare. However, using my knowledge of the ISO 27001 standard framework of 133 controls, and my knowledge of the various characteristics and aspects of cyberattacks and cyberwarfare, I created the table in Appendix A that can be used to understand how these various defined controls can be used to mitigate the risks associated with cyberattacks and cyberwarfare. The right-most column gives a simple yes or no to indicate the usefulness of the control in the mitigation of risks associated with cyberattacks and cyberwarfare.

Recommendations

He section has been divided into recommendations for four distinct groups of people that will probably comprise the population of this magazine's readers. I deliberately omitted government officials and military officials because they have their own elite teams of cyberwarfare experts to advise them on these issues.

In addition, they have a perspective of cyberattacks and cyberwarfare in which they must consider battle plans and strategies that include both offensive and defensive operations. To best understand the true nature of cyberdeterrence and cyberwarfare, everyone would be well advised to read many of the materials in the reference section of this article, and in particular, read Martin Libicki's book, Cyberdeterrence and Cyberwar, because I consider it to be the best unclassified reference on the market.

For IT Professionals

- Educate yourself, continually about Cyberwarfare.
- Stay abreast of the threats and vulnerabilities associated with your infrastructure and the information technologies that you work with.
- Stay abreast of the security controls required to mitigate the risks associated with the information technologies that you work with.
- Where possible, get professional training and certifications associated with IT security and your job positions.

For IT Managers

- Learn the security compliance standard or standards that will enable you to help your organization effectively lower risk to acceptable levels.
- Learn risk management in the IT world.
- Learn what your teams do and keep them motivated to be the best at what they do.

For Executives and Business Owners

- Remember your responsibilities to the Board of Directors, your shareholders and other stakeholders in your organization: Cyberattacks and cyberwarfare represent serious threats that can obliterate an organization's ability to function (see the 2007 cyberattacks in Estonia, or the 2008 attacks in Georgia if you require more proof). If you plan for your organization to be an ongoing concern for the foreseeable future, you have no alternative than to ensure it is protected from cyberattacks and the effects of cyberwarfare.
- Learn the security compliance standard or standards that will enable you to help your organization effectively lower risk to acceptable levels.
- Learn risk management in the IT world.
- Learn what your managers and your teams do and keep them motivated to be the best at what they do.

For Hackers

- Consider becoming legitimate because the need for experienced cybersecurity professionals to defend organizations and countries has never been greater and in the long run, the compensation will probably be much more lucrative.

Resources

- Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.
- Brewer, D. and Nash, M. (2010). Insights into the ISO/IEC 27001 Annex A. A paper written published by Dr. David Brewer and Dr. Michael Nash to explain ISO 27001 and Risk Reduction in Organizations. Retrieved from *http://www.gammassl.co.uk/research/27001annexAinsights.pdf* on March 10, 2011.
- Bush, G. W. (2008). Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House January 2008. Retrieved from *http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative* on January 5, 2012.
- Calder, A. and Watkins, S. (2012). IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 5th edition. London, U.K.: IT Governance Press.
- Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.
- Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HarperCollins Publishers.
- Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from *http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf* on October 10, 2012.
- Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.
- Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retrieved from *http://www.infracritical.com/papers/nstb-2481.pdf* on December 20, 2011.
- Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from *http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf* on September 30, 2012.
- Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillan.
- Gerwitz, D. (2011). The Obama Cyberdoctrine: tweet softly, but carry a big stick. An article published at Zdnet.com on May 17, 2011. Retrieved from *http://www.zdnet.com/blog/government/the-obama-cyberdoctrine-tweet-softly-but-carry-a-big-stick/10400* on September 25, 2012.
- Gjelten, T. (2010). Are ‚Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from *http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet* on December 20, 2011.
- Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from *http://www.npr.org/templates/story/story.php?storyId=130260413* on December 20, 2011.
- Gjelten, T. (2011). Security Expert: U.S. ‚Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from *http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet* on December 20, 2011.
- Gjelten, T. (2011). Stuxnet Raises ‚Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from *http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar* on December 20, 2011.
- Goldman, D. (2013). Nations prepare for cyber war. An article published at CNN on January 7, 2013. Retrieved from *http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html?hpt=hp_c3* on January 7, 2013.
- Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare. Cambridgeshire, U.K.: IT Governance.Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.
- ISO. (2005) "Information technology – Security techniques – Information security management systems requirements", ISO/IEC 27001:2005. Retrieved from *http://www.ansi.org* on February 1, 2011.
- Jaquith, A. (2007). Security Metrics. Boston, MA: Addison Wesley.
- Kaplan, F. (1983), The Wizards of Armageddon: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.
- Kerr, D. (2012). Senator urges Obama to issue ‚cybersecurity' executive order. An article published at Cnet.com on September 24, 2012. Retrieved from *http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/* on September 26, 2012.
- Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.
- Langer, R. (2010). A Detailed Analysis of the Stuxnet Worm. Retrieved from *http://www.langner.com/en/blog/page/6/* on December 20, 2011.
- Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.
- Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from *http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all* on June 28, 2009.
- Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at Poltix. Topix.com. Retrieved from *http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war* on September 22, 2012.
- McBrie, J. M. (2007). THE BUSH DOCTRINE: SHIFTING POSITION AND CLOSING THE STANCE. A scholarly paper published by the USAWC STRATEGY RESEARCH PROJECT. Retrieved from *http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA423774* on September 30, 2012.
- Obama, B. H. (2012). Defense Strategic Guidance 2012 – Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from *http://www.defense.gov/news/Defense_Strategic_Guidance.pdf* on January 5, 2012.
- Obama, B.H. (2011). INTERNATIONAL STRATEGY for Cyberspace. Published by the White House on May 16, 2011. Retrieved from *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf* on May 16, 2011.
- Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.

- Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.
- Radcliff, D. (2012). Cyber cold war: Espionage and warfare. An article published in SC Magazine, September 4, 2012. Retrieved from *http://www.scmagazine.com/cyber--cold-war-espionage-and-warfare/article/254627/* on September 7, 2012.
- Saini, M. (2012). Preparing for Cyberwar – A National Perspective. An article published on July 26, 2012 at the Vivikanda International Foundation. Retrieved from *http://www.vifindia.org/article/2012/july/26/preparing-for-cyber-war-a-national-perspective* on October 14, 2012.
- Sanger, D. E. (2012). Confront and Coneal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.
- Schmidt, H. S. (2006). Patrolling Cyberspace: Lessons Learned from Lifetime in Data Security. N. Potomac, MD: Larstan Publishing, Inc.
- Schmitt, E. and Shanker, T. (2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. An article published in the New York Times on October 17, 2011. Retrieved from *http://www.nytimes.com/2011/10/18/world/africa/cyber--warfare-against-libya-was-debated-by-us.html* on October 17, 2011.
- Slater, W. F. (2013). ISO 27001 Resource Page. Retrieved from *http://billslater.com/iso27001* on January 12, 2013.
- Stiennon, R. (2010). Surviving Cyber War. Lanham, MA: Government Institutes.
- Strohm, C. and Engleman, E. (2012). Cyber Attacks on U.S. Banks Expose Vulnerabilities. An article published at BusinessWeek.com on September 28, 2012. Retrieved from *http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability* on September 30, 2012.
- Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.
- The ISO 27000 Directory. (2012). An Introduction to ISO 27001, ISO 27002....ISO 27008. Retreived from *http://www.27000.org/index.htm, http://idcontent.bellevue.edu/content/CIT/cyber/615/compliance* on December 7, 2012.
- Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from *http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html* on October 25, 2012.
- U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from *http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf* on November 3, 2012.
- U.S. Department of Defense, JCS. (2006). Joint Publication (JP) 5-0, Joint Operation Planning, updated on December 26, 2012. Retrieved from *http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf* on October 25, 2012.
- Waters, G. (2008). Australia and Cyber-Warfare. Canberra, Australia: ANU E Press.

- Make sure that if you do join a team that it is a winning team.

Conclusions

This article has covered some of the better known aspects of cyberattacks and cyberwarfare, and attempted to show that risks can be managed by applying security compliance frameworks such as ISO 27001. While this has only been an introduction, because scores of books have been written on these topics since 2005, it is important to understand these basic concepts and take them seriously. The future of your business, the satisfaction and confidence of your stakeholders, business partners, and your customers all depend on your ability to protect your business and its operations capabilities in the day and age of cyberattacks and cyberwarfare.

WILLIAM F. SLATER, III

William F. Slater, III is an IT Security consultant who lives and works in Chicago, IL, United States of America. He has worked in Information Technology since 1977. In March 2013, he will complete his third graduate degree, an M.S. in Cybersecurity. Though he has prior experience as a computer systems staff officer serving at Strategic Air Command Headquarters from 1977 to 1980, and as an civilian IT service management Project Manager working with the U.S. from 2009 to 2010, and he has had a top secret clearance (1977 – 1980) and a secret clearance (2009 – 2011), he did not access any classified documents from the U.S military or the U.S. government to research and write this paper. This paper is therefore, is an unclassified document that was researched and written using resources that are available to the general public. Other information reflected in this paper is the professional opinion of Mr. Slater, who is solely responsible for the content of this paper.

Finally, Mr. Slater is a very patriotic American who always hopes for the best for the Republic of the United States of America and her Allies. This includes trying to do what is in his power as an IT professional, an educator, and a writer to make the use of Cyberspace and the Internet safe for everyone.

Appendix A – ISO27001 Domains, Control Objectives and Controls

ISO 27001:2005 Controls		
Clause	Section	Control Objective/Control
Security Policy	5.1	Information Security Policy
	5.1.1	Information Security Policy Document
	5.1.2	Review of Information Security Policy
Organization of Information security	6.1	Internal Organization
	6.1.1	Management Commitment to information security
	6.1.2	Information security Co-ordination
	6.1.3	Allocation of information security Responsibilities
	6.1.4	Authorization process for Information Processing facilities
	6.1.5	Confidentiality agreements
	6.1.6	Contact with authorities
	6.1.7	Contact with special interest groups
	6.1.8	Independent review of information security
	6.2	External Parties
	6.2.1	Identification of risk related to external parties
	6.2.2	Addressing security when dealing with customers
	6.2.3	Addressing security in third party agreements
Asset Management	7.1	Responsibility for Assets
	7.1.1	Inventory of assets
	7.1.2	Ownership of Assets
	7.1.3	Acceptable use of assets
	7.2	Information classification
	7.2.1	Classification Guidelines
	7.2.2	Information Labeling and Handling
Human Resource Security	8.1	Prior to Employment
	8.1.1	Roles and Responsibilities
	8.1.2	Screening
	8.1.3	Terms and conditions of employment
	8.2	During Employment
	8.2.1	Management Responsibility
	8.2.2	Information security awareness, education and training
	8.2.3	Disciplinary process
	8.3	Termination or change of employment
	8.3.1	Termination responsibility
	8.3.2	Return of assets
	8.3.3	Removal of access rights
Physical and Environmental Security	9.1	Secure Areas
	9.1.1	Physical security Perimeter
	9.1.2	Physical entry controls
	9.1.3	Securing offices, rooms and facilities
	9.1.4	Protecting against external and environmental threats
	9.1.5	Working in secure areas
	9.1.6	Public access, delivery and loading areas
	9.2	Equipment security
	9.2.1	Equipment sitting and protection
	9.2.2	Support utilities
	9.2.3	Cabling security
	9.2.4	Equipment Maintenance
	9.2.5	Security of equipment off-premises
	9.2.6	Secure disposal or reuse of equipment
	9.2.7	Removal of Property
Communications and Operations Management	10.1	Operational Procedures and responsibilities
	10.1.1	Documented operating Procedures
	10.1.2	Change Management
	10.1.3	Segregation of Duties
	10.1.4	Separation of development and Operations facilities
	10.2	Third Party Service Delivery Management
	10.2.1	Service Delivery
	10.2.2	Monitoring and review of third party services
	10.2.3	Manage changes to the third party services
	10.3	System Planning and Acceptance
	10.3.1	Capacity management
	10.3.2	System acceptance
	10.4	Protection against Malicious and Mobile Code
	10.4.1	Controls against malicious code
	10.4.2	Controls against Mobile code
	10.5	Back-Up
	10.5.1	Information Backup
	10.6	Network Security Management
	10.6.1	Network controls
	10.6.2	Security of Network services
	10.7	Media Handling
	10.7.1	Management of removable media
	10.7.2	Disposal of Media
	10.7.3	Information handling procedures
	10.7.4	Security of system documentation
	10.8	Exchange of Information
	10.8.1	Information exchange policies and procedures
	10.8.2	Exchange agreements
	10.8.3	Physical media in transit
	10.8.4	Electronic Messaging
	10.8.5	Business Information systems

	10.9	Electronic Commerce Services
	10.9.1	Electronic Commerce
	10.9.2	On-Line transactions
	10.9.3	Publicly available information
	10.1	Monitoring
	10.10.1	Audit logging
	10.10.2	Monitoring system use
	10.10.3	Protection of log information
	10.10.4	Administrator and operator logs
	10.10.5	Fault logging
	10.10.6	Clock synchronization
Access control	11.1	Business Requirement for Access Control
	11.1.1	Access control Policy
	11.2	User Access Management
	11.2.1	User Registration
	11.2.2	Privilege Measurement
	11.2.3	User password management
	11.2.4	Review of user access rights
	11.3	User Responsibilities
	11.3.1	Password Use
	11.3.2	Unattended user equipment
	11.3.3	Clear Desk and Clear Screen Policy
	11.4	Network Access control
	11.4.1	Policy on use of network services
	11.4.2	User authentication for external connections
	11.4.3	Equipment identification in networks
	11.4.4	Remote diagnostic and configuration port protection
	11.4.5	Segregation in networks
	11.4.6	Network connection control
	11.4.7	Network Routing control
	11.5	Operating System Access Control
	11.5.1	Secure Log-on procedures
	11.5.2	User identification and authentication
	11.5.3	Password Management system
	11.5.4	Use of system utilities
	11.5.5	Session Time-out
	11.5.6	Limitation of connection time
	11.6	Application access control
	11.6.1	Information access restriction
	11.6.2	Sensitive system isolation
	11.7	Mobile Computing and Teleworking
	11.7.1	Mobile computing and communication
	11.7.2	Teleworking
Information Systems Acquisition Development and Maintenance	12.1	Security Requirements of Information Systems
	12.1.1	Security requirement analysis and specifications
	12.2	Correct Processing in Applications
	12.2.1	Input data validation
	12.2.2	Control of internal processing
	12.2.3	Message integrity
	12.2.4	Output data validation
	12.3	Cryptographic controls
	12.3.1	Policy on the use of cryptographic controls
	12.3.2	Key Management
	12.4	Security of System Files
	12.4.1	Control of Operational software
	12.4.2	Protection of system test data
	12.4.3	Access control to program source library
	12.5	Security in Development & Support Processes
	12.5.1	Change Control Procedures
	12.5.2	Technical review of applications after Operating system changes
	12.5.3	Restrictions on changes to software packages
	12.5.4	Information Leakage
	12.5.5	Outsourced Software Development
	12.6	Technical Vulnerability Management
	12.6.1	Control of technical vulnerabilities
Information Security Incident Management	13.1	Reporting Information Security Events and Weaknesses
	13.1.1	Reporting Information security events
	13.1.2	Reporting security weaknesses
	13.2	Management of Information Security Incidents and Improvements
	13.2.1	Responsibilities and Procedures
	13.2.2	Learning for Information security incidents
	13.2.3	Collection of evidence
Business Continuity Management	14.1	Information Security Aspects of Business Continuity Management
	14.1.1	Including Information Security in Business continuity management process
	14.1.2	Business continuity and Risk Assessment
	14.1.3	developing and implementing continuity plans including information security
	14.1.4	Business continuity planning framework
	14.1.5	Testing, maintaining and re-assessing business continuity plans
Compliance	15.1	Compliance with Legal Requirements
	15.1.1	Identification of applicable legislations
	15.1.2	Intellectual Property Rights (IPR)
	15.1.3	Protection of organizational records
	15.1.4	Data Protection and privacy of personal information
	15.1.5	Prevention of misuse of information processing facilities
	15.1.6	Regulation of cryptographic controls
	15.2	Compliance with Security Policies and Standards and Technical compliance
	15.2.1	Compliance with security policy
	15.2.2	Technical compliance checking
	15.3	Information System Audit Considerations
	15.3.1	Information System Audit controls
	15.3.2	Protection of information system audit tools

Industrial Cybersecurity

There are lots of misunderstandings concerning Industrial Cybersecurity. The IT World is completely different from the Industrial World, but due to the necessity of communications between industrial facilities they were using the network and systems which where developed and deployed never worrying about security.

Engineers work to make control systems more usable, more reliable, efficient, inter operable, all those things that make them more vulnerable. You will be driven through some history, theory, and some practical exposure on hacking industrial environments and how to protect them.

Control System

A Control System is a set of instruments, controls, and controllers used to manage and control the behavior of process machinery and thus, the process (Figure 1).

Figure 1. *Controller System Room*

They can be divided as:

- instruments (Sensors include temperature, flow, pressure, etc.),
- controls (affect or modify operation of machinery or process. For example, code, alarms, buttons, switches, HMI's, indicators),
- controllers (SCADA – Supervisor Control and Data Acquisition, DCS – Distributed Control Systems, PLC – Programmable Logic Controllers),
- Process Machinary (pumps, valves, actuators).

In order to operate, industrial facilities will require many PCs, Servers, PLCs, DCSs, HMIs, as well as many other network components.

Is Industrial Cybersecurity a real threat?

No major incident happened yet, but there are several small scale incidents that have already taken place:

- 1999: Petroleum pipe line exploded in Washington. This was considered the first Cybersecurity attack that resulted in 3 fatalities. A pipeline carrying gasoline failed due to damage caused by a third party during construction on adjacent facilities. The pipeline failure resulted in discharging 277,000 gallons of product into a creek bed (Figure 2).
- 2001: California Utility was compromised. It was undetected for 20 days. The attacker had full control for 20 days. It was due to unfirewalled connections and many unused ports opened. But luckily, this part of the plant was still under construction.
- 2003: Safety system failure in Ohio at Davis-Besse plant caused by the Slammer Worm. Luckily, this part of the plant was under construction as well. What could have happened if those plants were fully operated?
- 2006: Embedded software discovery. Suspected to be the work of a foreign government seeking to compromise the grid in a time of war.

2012: Nuclear threats using Stuxnet, the first and major threat against a nuclear facility of public

Figure 2. *Bellingham Pipe Line Explosion*

knowledge. It was stealthy only, but the attacker could be using it to compromise, getting control of a PLC mechanism, for example.

Existing facilities are not secure. Some of them are 60 years old, some are only a couple years old. But the main reason is the majority of those facilities were not designed for network and security. Newer facilities are implementing better practices and methods, but are still flawed.

Everything that have been done so far is too slow and not enough. There are regulations but they are not really enforced. Guidelines and recommendations exists also, but not much beyond that. Now, nuclear facilities are different. They are more regulated by the government. All the nuclear plants in the United States are now undergoing process and equipment changes in order to comply to the new Cybersecurity plans for nuclear reactors.

Many issues, like bad designs and also bad implementations, happen even before the plant exists by itself. Bringing new technologies to old facilities that are insecure also brings lots of vulnerabilities in the name of friendly use. Manufactures are adding features to their equipments, for example devices you can program using your iPhone, even through bluetooth connection, or PLC, which you can access over the Web with no passwords set. It's really good in terms of Maintenance and Operations point of view but not from a security perspective.

There are maybe 10 to 15 major vendors of basic infrastructure for industries worldwide. Half of them are in the United of States (GE, Rockwell, Emerson). The other half are internationals (Siemens, ABB, Schneider). All of them sell all over the world except that US companies are not supposed to sell to North Korea or Iran. If you think about Stuxnet others can. At a first look it may be all industrial matter but can be military as well when you thing about how a ship is constructed for example. Ventilation, air conditioner and how a pump works on ships are the same as industrial. This is why DOD – Department of Defense is so concerned nowadays.

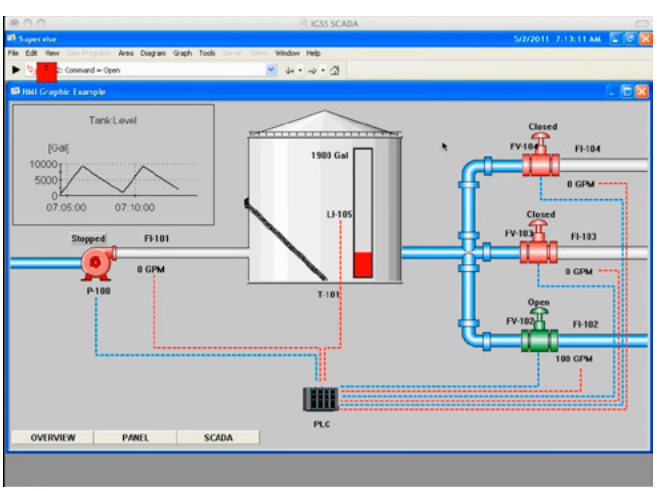


Figure 3. *IGSS SCADA System*

Compliance and standards

There are rules and regulations you can follow to protect your plant:

- NERC – National Energy Regulatory Commission. Fines up to $1milion per violation per day,
- NIST – National Institute of Standards and Technology. Voluntary standards. Covers items from cell phones to domain implementation,
- NRC – Nuclear Regulatory Commission. Mandatory for nuclear facilities. Compliance is needed to maintain license to operate,
- many others.

To protect your plant is simple: truly protect the cybersystems effectively and responsibly and the nuances of compliance standards become somewhat irrelevant. You shouldn't have to tailor plant processes to compliance standards, you should be interpreting compliance standards based on effective existing processes. Just do it right.

Security flaws and mitigation of a PLC

One of the main issues is the ability to remotely operate a PLC and be able to make writhes on the PLC and most users are not aware of this functionality. Many times the manual indicates it's not capable.

Authentication is the another main problem as password protection is disabled by default. Engineers normally don't change the default password provided by vendors.

Commands to write to the PLC passed by URL to CGI script is the another common issue.

There are many methods and dangerous tools that could be used today to attack a control system. Metasploit is highly available for free on the Internet today and it can be used against control systems. With only 4 lines of code you can take control of many controllers that are being used in the industry today and and there is no patch for it, because it's inherited from the design of the system.

Compromising a Control System

In this session, we're going to focus on vulnerabilities found on *Interactive Graphical SCADA System* (IGSS) developed by 7 Technologies from

Denmark, and how the published "Proof of Concept (PoC)" code/data packets can be leveraged to building and executing your own malicious code. The end result is a complete compromise or "pwning" of the control system.

This vulnerability allow me to run remote commands with low effort and high impact.

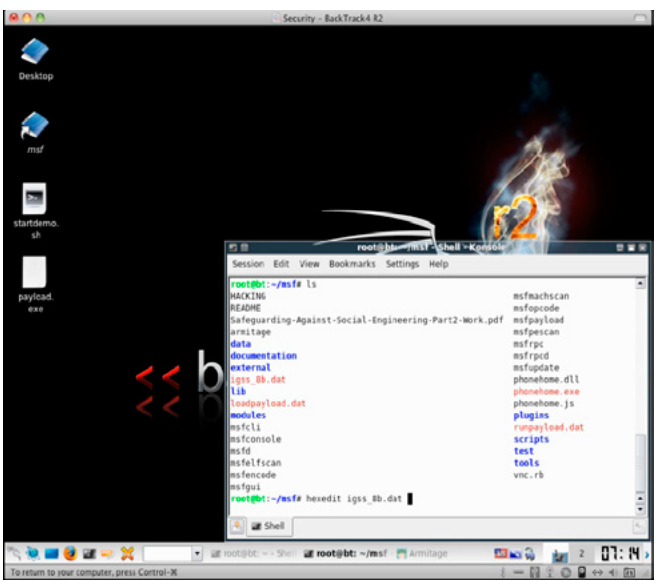


Figure 4. *Using Hexedit on BackTrack to analyse the igss_8b.dat file*

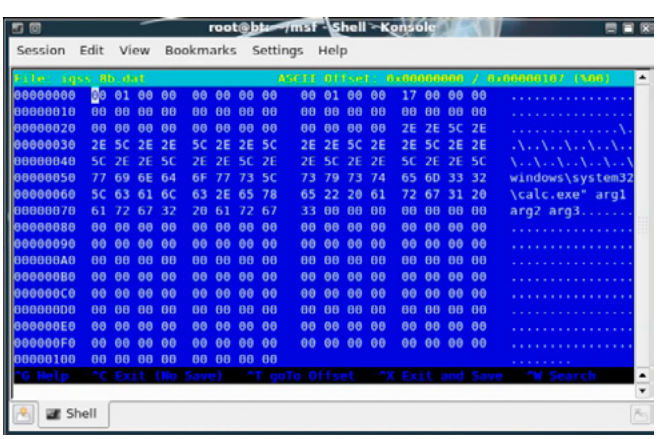


Figure 5. *Content of igss_8b.dat file*

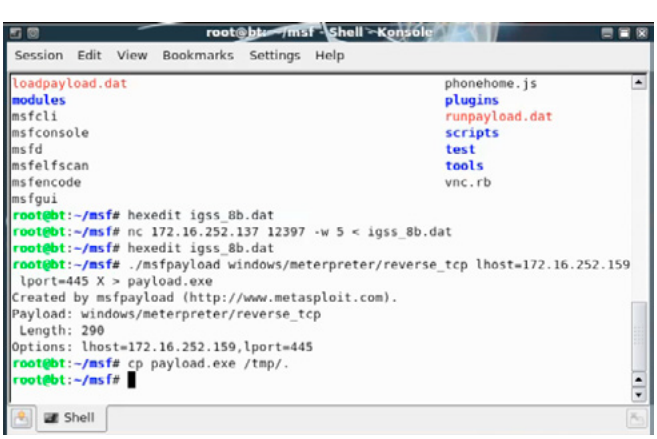


Figure 6. *Sequence of Commands*

In Figure 3, you can see a simple process with a feed pump on the left supplying a product to storage tank. From that storage tank, you have three outlet valves that you can open or close at any given time.

This can represent a general water distribution system or it can also be used in an oil refinery.

Using BackTrack Operation System, and Metasploit you can change and add the payload of the file and allow it to request commands from an attacker system (Figure 4-6).

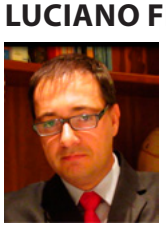
In result, the attacker may have full control of the system, having the same image from Figure 3 and be able to open the pump or the valves!

For this particular threat, patches were already available, but not all systems administrators are doing a great job applying them.

Summary

Industrial Cybersecurity is getting more and more attention with passing of time and there is an enormous gap between Industrial world and IT world, as well as between the usability and interoperability of that systems and their security, that need to be covered. If you are an IT Security Professional and are working in Industry, are you taking care of the industrial environment IT Security as well? If not, what are you waiting for?

LUCIANO FERRARI



Luciano Ferrari has more than 15 years of experience in IT. He is a Brazilian living in the US and has bachelor's degree in Microelectronics, post-graduate education in Computer Networks and an Executive Master of Business Administration (MBA). He specializes in Green IT, Computer Networks, IT Security, Risk Management, Cryptography, Project Management, and IT Management.

Contact: lferrari@lufsec.com

Blog: www.lufsec.com

twitter: @lucianoferrari

Hack Me? No, Hack You!

The Pros and Cons of Active Cyber Defense

Active cyber defense, or the act of striking back at cyber attackers, is a growing practice being advocated by various governments, corporations, and security experts around the world. Some victims of cyber attacks are increasingly implementing active cyber attack measures, firing back at their attackers with equal levels of aggression.

Active cyber defense is a hotly debated topic, with many complex issues, technical hurdles, legal concerns and ethical dilemmas – as with most things of this nature, there are ardent supporters on both sides of the debate – those who advocate for utilizing active cyber defense, and those who oppose it. This article will weigh the pros and cons of active cyber defense, and question if it is in fact the best way forward in securing our networks.

Introduction

Computers and technology are the cornerstone of modern-day life. Advances in Information Technology and the Internet have created a digital-bridge which spans the globe, allowing people to stay connected, keep informed, conduct business, and enjoy new avenues of entertainment. These advances have significantly reshaped the way business is conducted; organizations can rapidly share intellectual property and products, new avenues for interacting with customers are constantly being developed, and the face of the global economy has been forever changed. These advances have also enabled governments around the world to better work together and protect their nation's interests. That being said, these advances do not mark a flawless leap towards a utopian society, while much good has come from the advances in technology, those same advances which allow zeros and ones to travel around the globe in the blink of an eye, have provided criminals a new avenue to commit crimes, cyber activists an avenue which they can forcefully promote their agenda, and governments the ability to weaponizing their cyber arsenal to gain an edge over rival nations, by complimenting their kinetic weapons with digital equivalents.

Image: Terrance Stachowski, 2012

There are plenty of cyber buzzwords floating around these days; cybercrime, cyber warfare, cyber attacks, and cyber terrorism have all but become household terms. In October of 2012, Defense Secretary Leon E. Panetta cautioned that the United States is facing the possibility of a "cyber-Pearl Harbor" and is increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks, and the government [1].There are conflicting opinions on how serious cyber threats are, and how to best address them. Some experts warn that we are racing towards a cyber-Armageddon, while others dismiss these opinions as little more than exaggerated fear-mongering.

Regardless of the what the future Internet landscape may shape up to be, there is little doubt that we are currently living in an age where cyber attacks are on the rise. According to the 2012 Cost of Cyber Crime Study, which was conducted by the Ponemon Institute and sponsored by HP, the occurrence of cyber attacks has more than doubled over a three-year period, and the financial impact has increased by nearly 40 percent [2]. Cyber crimes will likely continue to gain momentum in the foreseeable future, but from a defensive perspective we must question if a traditional, layered – yet passive – defensive strategy is enough moving forward, or if an active cyber defense is required.

What is a Cyber Attack?

There are various types of cyber attacks. In a broad sense a cyber attack can be defined as an attack on a computer system or network. The offending attacker may be an individual, a group, or even a nation-state. Attackers range in abilities, from script kiddies who are novice hackers with limited skills – to highly-skilled cyber criminals. Motivating factors vary, but the goals of a cyber attack are typically to commit fraud, theft or alteration of data, disruption of services, abuse of IT resources, or violation/theft of personal privacy information. Some example categories of cyber attacks:

- Zero-Day exploits/attacks: This type of attack is when an attacker utilizes an exploit or vulnerability for which no patch currently exists.
- Denial of Service (DoS) attacks: Disrupt services of targeted system or network by consuming bandwidth or taxing a machine's resources.
- Distributed Denial of Service (DDoS) attacks: Similar to a DoS attack, but attacks are conducted from multiple attacking machines.
- Defacement of websites: This type of attack aims to modify the content of a website, or redirect guests to a counterfeit site.
- Spam campaigns: This type of attack sends massive quantities of unwanted, unsolicited 'spam' messages or e-mails to the target; typically used for advertising products.
- Malicious Software / Malware Attack: This type of attack includes Trojans, viruses, and worms, which can be used to disrupt operations, steal information, or create backdoors into systems.

These attacks are often stacked and deployed in tandem, i.e. a Zero-Day exploit may be utilized to exploit a vulnerability which allows the attacker to inject the system with a backdoor such as a *remote access Trojan* (RAT) which gives the attacker administrative control of a machine, or to inject viruses or other malicious software into the network.

According to the Department of Defense Strategy for Operating in Cyberspace (2011): "Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners. Moreover, this threat continues to evolve as evidence grows of adversaries focusing on the development of increasingly sophisticated and potentially dangerous capabilities [3]."

Challenges Organizations Face

Some major challenges that organizations are currently facing:

- The number of vulnerabilities are constantly growing in number.
- Attackers are becoming more sophisticated in their attack methods.
- Traditional security practices are largely reactionary, i.e. patching vulnerabilities as patches become available, blocking offending IP addresses only after they are identified as a threat.
- Many companies may not have the right blend of security professionals, manpower, or resources to adequately monitor, identify, patch and secure their networks from attacks in a timely fashion.
- Attribution is arguably the single-most frustrating challenge that organizations face in regards to cyber attacks. Pinning down where an attack is truly originating from, and discov-

ering who is ultimately responsible, is an extremely complex technical undertaking. Identifying the attack source is much more complicated than simply tracing an IP address back to the offending machine; the problem is that most accomplished attackers are skilled in the ways of obscuring their footsteps by utilizing covert channels, proxies, services such as *The Onion Router* (TOR), and make use of botnets, etc.

Stefan Ortloff, a Kaspersky Lab expert, has demonstrated how peer-to-peer botnets have evolved past the traditional botnet architecture. In a traditional botnet, there is a single *command and control-center* (C&C) managing the bots, thus there is a single point-of-failure, as seen in Figure 1. The Hlux/Kelihos (peer-to-peer) botnet as seen in Figure 2, doesn't use a centralized C&C, so it makes taking down this type of botnet much harder [4].

Ortloff states that by design, the size of a peer-to-peer botnet can only be estimated; the old Hlux botnet which was taken down in September 2010 is estimated to have had 40,000 different IP addresses involved, whereas the new botnet is estimated to have had 110,000 IP addresses involved.

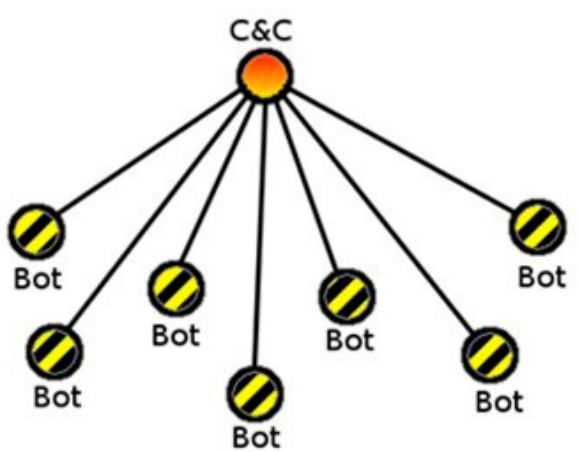


Figure 2. *Stefan Ortloff, 2012 [5]*

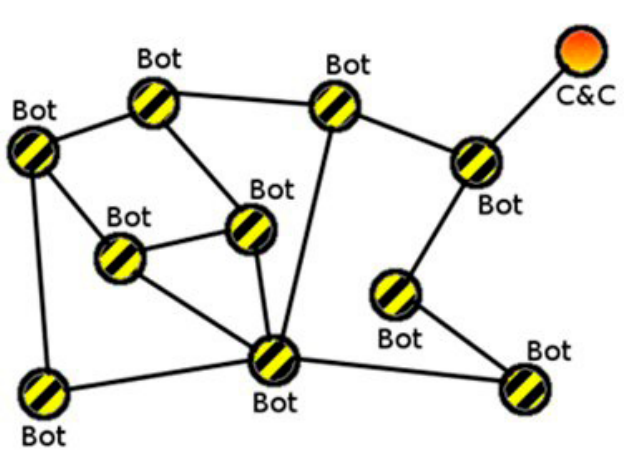


Figure 3. *Stefan Ortloff, 2012 [6]*

Arguments Favoring Active Cyber Defense

According to Hayes and Kesan (2011): "Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks." [7]

Many advocates of active cyber defense agree on the above points, primarily that parties have the right to defend themselves through deterrence, and by making the cost too great for attackers to continue their efforts, that passive defense does little to dissuade attackers.

Jeff Bardin (2012) argues: "The legal issues notwithstanding, offensive cyber actions are the only way we are going to get our adversaries to pay attention. Whether they are cyber criminals, foreign intelligence services, cyber proxies, hackers, hacktivists, or some other such adversary, we need to do more than just stand and take a beating... When we attack the attackers (and this is not active defense), they cannot attack us. Most cyber criminals have absolutely no defensive posture whatsoever. When hit with an offensive attack, they quickly shift their targets since it is not cost effective and their whole intent is economic in nature... There is positive outcome when attacking your cyber adversaries. It disrupts their command and control. If forces them off their mission. It forces the adversary to invest in measures they have never invested in. It forces a ripple in their activities that can then be tracked through primary, secondary and tertiary actions." [8]

Many developed nations are currently developing and employing active cyber defense capabilities to thwart intrusions, limit loss or damage, and disrupt adversary activities on their systems and networks. The United States Department of Defense is expanding its formal and informal cyber cooperation to a wider circle of allies and partner militaries to increase collective self-defense and boost collective deterrence. The DoD will create new opportunities for like-minded states to work

cooperatively based on shared principles; expanded and strengthened relationships with allies and international partners can maximize scarce cyber capabilities, mitigate risk, and create coalitions to deter malicious activities in cyberspace [9].

Common arguments for utilizing an active cyber defense often deliver some of the following points:

- Law enforcement isn't working, or the legal system is too slow or unable to provide solutions – particularly when the attacks originate from a different country.
- There are not enough qualified law enforcement agents to perform investigations, and too few with the skills required to go toe-to-toe with cyber criminals.
- Organizations have the right to self-defense.
- Stolen data actually belongs to the victim, so it's within their right to go and retrieve their data from the attackers.
- The cost of not hacking back is too great. Organizations cannot sit idle while their information is being stolen or their services are being disrupted.
- Another popular argument/mindset is what I call "The Sign Reads Beware of Dog" approach, basically it's the notion that if organizations make it known that they are willing to utilize active cyber defense techniques, they will scare off potential hackers.

Examples of Active Cyber Defense in Practice

There have been several notable botnet takeover/takedown operations. David Dittrich has done some excellent work on compiling and examining a list of botnet takeover and takedown activities. In his paper *So You Want to Take Over a Botnet...* (2012), he notes that all takedowns coordinating civil and/or criminal legal process with technical methods (Waledac, Rustock, Coreflood, and Kelihos) succeeded on first try, while those only using civil legal process (the first attempt at taking down Ozdok) or using only technical means (Torpig, Ozdok, and Pushdo) did not [10].

Arguments Opposing Active Cyber Defense

The arguments against utilizing active cyber defense are abundant and are just as compelling as the arguments put forth by advocates.

Jody Westby argues: "The perceived value of active defense has to be weighed against the risk and cost. On the risk side, there is the clear possibility that playing cat and mouse with sophisticated cybercriminals may cause them to up the stakes and launch more destructive attacks… even after lying low for a considerable period of time." [12]

According to Jarno Limnell: "We cannot solely focus on increasing offensive activities in cyberspace. Fighting fire with fire will lead us to a dan-

Botnet	Peak Size (est)	First Seen	Take Down	Time Elapsed	Success on 1st try	Used Legal Process
Torpig	180,000	Feb 2006	Jan 2009	3 years	No	No
Ozdok	264,784 [1]	Early 2008	Nov 2009	2 years	No	No
Mariposa	12 million [2]	May 2009	Dec 2009	7 months	No	No [3]
Waledac	6,600+ [4]	Apr 2008	Feb 2010	3 years	Yes	Yes
Pushdo	1.5-2 Million	Jan 2007	Aug 2010	3.5 years	No	No
Bredolab	30 million [5]	Mid-2009	Oct 2010	1.5 years	No	Yes [6]
Coreflood	378,758 [7]	2001	Apr 2011	10 years	Yes	Yes
Rustock	1.6 million [8]	2006	Mar 2011	5 years	Yes	Yes
Kelihos	41,000	Dec 2010	Sep 2011	8 months	Yes	Yes

Table 1: Botnets subject to highly publicized takedown efforts (by takedown date)

[1] *Unique IPs connecting to FireEye's sinkhole in 24 hrs. The 2008 estimate of 35,000 by Marshal Software [35, 36] provided no time frame or counting methodology.*
[2] *Unique IP addresses over an unspecified time period [10]. Other estimates show no more than 1.5M per day.*
[3] *The Mariposa Working Group did not use legal process in their botnet takedown attempts, but information they obtained was provided to law enforcement who eventually made arrests.*
[4] *Count of actively spamming nodes in 24 hr period.*
[5] *Count of total infections, not to be considered a single monolithic botnet of 30M computers. Also, counting method and time period used to establish count was not specified.*
[6] *Criminal procedures were used to seize control of C&C servers.*
[7] *Unique IP addresses seen over a six month period.*

Figure 4. *David Dittrich, 2012 [11]*

gerous future. As has been the case many times in the history of the physical world, offensive actions can quickly lead to greater problems. The danger of escalation is always present. In today's digitally interconnected world there is also a huge potential for unpredictable side effects and collateral damage from aggressive actions." [13]

Arguments against utilizing active cyber defense often present the following points:

- Ther is an attribution problem. Nailing down exactly where the attacks are originating is much easier said than done.
- Instead of taking out the command and control machines, there is a chance to cause collateral damage to those machines which are unknowingly acting as bots.
- Some feel that active cyber defense is tantamount to taking the law into your own hands.
- Organizations may not be adequately equipped or knowledgeable enough to perform these actions. Being a security professional does not necessarily qualify someone to make the right judgment calls, especially if guided by emotions (frustrated, having a desire to punish, seek revenge or retribution, etc), nor does it mean that they are qualified or skilled enough to go toe-to-toe with cyber criminals. An *Information Security Officer* (ISO) is not synonymous with being a skilled hacker or counter-attack specialist; counter-attacking script kiddies may work, but counter-attacking a highly-skilled cyber criminal who makes their living by performing cyber attacks could be comparable to bringing a knife to a gun fight.
- Who performs oversight and scrutinizes those engaging in active cyber defense and holds them accountable for their actions? Where are the defined rules of engagement, or are they developed on the fly? Who is accountable when the tit-for-tat escalates and gets out of hand and there is no oversight mechanism in place?
- A lot of hypothesizing and arguments are being brought forward by non-technical individuals in leadership roles, it may be dangerous for these individuals to weigh in on extremely complicated and technical issues of attack and defense if they are not knowledgeable on such things.
- Counter-attacks have the potential to spiral into kinetic warfare.
- There is an idea that damaging the attackers machine will disrupt their ability to conduct attacks, but this may not be totally true if the attacker is utilizing a virtual machine which can be reloaded in the matter of seconds. In this case, it may not be much of a deterrent, and depending on the attacker, attacking them may catch their full attention and cause them to ramp up their efforts, it could be seen as a game of sorts or a challenge to the attacker.
- An organizations network is an immobile, stationary target, whereas attackers are mobile, and have time on their side to regroup. They have the ability to disappear and reappear at a later time, location, to work on masking or obfuscating their attack channels, and can assemble additional attack bots or seek out additional help to attack the organization.
- Just as customer confidence in an organization may suffer if breaches are made public, so too may the organization's reputation be damaged if their active cyber defense activities were exposed to the public.
- How much of your network does the attacker already have control of? Could they be monitoring internal organization discussions related to the counter attacks? Could they watch the methods being deployed and adjust fire accordingly? Does the enemy have an insider in the company who is able to provide them with details of counter attack plans?
- Many who disagree with active cyber defense argue that it is unethical for organizations to take it upon themselves to strike back.
- Attackers don't care about laws, ethics, collateral damage, reputations, shareholders, etc. They have the luxury of using anything and everything at their disposal to attack an organization. Without having the same disregard for rules, laws, ethics, etc. how can an organization reasonably perform counter-attacks and guarantee 100% that no collateral damage will occur?

Legalities of Active Cyber Defense

Active cyber defense techniques fall into something of a legal gray area, but one could assume that both the organization and individuals engaging in these actions run the risk of facing civil liabilities and criminal penalties.

The Computer Fraud and Abuse Act (CFAA) though originally intended to fight fraud, has been amended with verbiage pertaining to worms, viruses, and other malicious code. The CFAA makes it a crime to "intentionally access a computer without authorization" and "intentionally causes damage without authorization." [14] The key words being: 'intentionally access, and damage.'

David Willson, a retired Army JAG officer and an attorney focuses on understanding the restrictions of what IT security professionals can do under the limits of current laws, he says: "You want to go after them and block them." He says that there is no consensus among lawyers focusing on this topic, but he emphasizes that organizations being attacked "should look beyond your network and figure out what's coming after you," and that there is a case to be made that organizations should "strike back defensively... Can you do it technically? Yes. Legally? I'd argue, yes." [15]

Is Active Cyber Defense the Best Way Forward?

Both sides of the argument deliver stubborn points to support their position. Though not wholly against the idea of active cyber defense, particularly in regards to government and military controlled programs which I support, I personally lean more towards those who oppose active cyber defense being used by private organizations who feel they can handle the situation on their own.

I feel that many organizations rank security low on their priority list, and look to budget for a simple, easy kill, vendor-provided solution. Ma-

References

1. Bumiller, E., Shanker, T. (2012). *Panetta warns of dire threat of cyberattack on the U.S.* Retrieved from: *http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0*
2. HP (2012). *HP research: Cybercrime costs rise nearly 40 percent, attack frequency doubles.* Retrieved from: http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html
3. Department of Defense (2011). *Department of Defense strategy for operating in cyberspace.* Retrieved from: http://www.defense.gov/news/d20110714cyber.pdf
4. Ortloff, S. (2012). *FAQ: Disabling the new Hlux/Kelihos botnet.* Retrieved from: *http://www.securelist.com/en/blog/208193438/FAQ_Disabling_the_new_Hlux_Kelihos_Botnet*
5. Figure 1. See 4.
6. Figure 2. See 4.
7. Hayes, C. M., Kesan, J. P. (2011). *Mitigative counterstriking: Self-defense and deterrence in cyberspace.* 25 Harvard Journal of Law and Technology 429 (2012); Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Illinois Public Law Research Paper No. 10-35. Retrieved from: http://ssrn.com/abstract=1805163
8. Bardin, J. (2012). *Caution: Not executing offensive actions against our adversaries is high risk.* Retrieved from: *http://blogs.csoonline.com/security-leadership/2469/caution-not-executing-offensive-actions-against-our-adversaries-high-risk*
9. See 3.
10. Dittrich, D. (2012). *So you want to take over a botnet...* Retrived from: *https://www.usenix.org/conference/leet12/so-you-want-take-over-botnet*
11. Figure: 3, see 10.
12. Westby, J. (2012). *Caution: Active response to cyber attacks has high risk.* Retrieved from: *http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#*
13. Limnell, J. (2012). *Controversial active cyber defense.* Retrieved from: *http://www.infosecisland.com/blogview/22757-Controversial-Active-Cyber-Defense.html*
14. Computer Fraud & Abuse Act (18 USC 1030) (2001). Retrieved from: *http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf*
15. Messmer, E. (2012). *Hitting back at cyberattackers: Experts discuss pros and cons.* Retrieved from: *http://www.networkworld.com/news/2012/110112-cyberattackers-263885.html*
16. See 4.

ny organizations look to cut costs by reducing the number of security professionals required to adequately defend a network, and continue to lower wages which doesn't attract highly-skilled security experts. For many organizations which have never suffered from a major security incident, security is simply seen as a painful, expensive requirement to merely remain compliant with laws and regulations.

I think the idea of an active cyber defense initiative would be a hard sell to many companies because of the consumption of time, money and resources, as well as the cost of finding and hiring the right mix of professionals who have the skills required to perform counterattack actions; additionally, performing counterattacks do not produce long-term benefits, it may stop or disrupt the current attack, but it doesn't fix the larger problem of an inadequately administered network. I would argue that money would better be spent on training the organization's staff on best security practices, hiring additional security staff with the skills to cover the gaps in the current team, and bringing in outside auditors and penetration testers who could identify and patch vulnerabilities. Organizations would do better to focus on areas such as stronger security policies and procedures, better security controls, more training, and sharper security practices such as improved logging, data collection, event auditing, immediate vulnerability patching, etc.

Though it may be embarrassing, or damage share holders confidence, organizations who come under attack should work to collect and preserve evidence, perform forensics actions, and then report the findings to law enforcement so that attacker trends, methods, and actions can be learned from.

That being said, I believe there is an argument to be made that organizations who specialize in striking back, or take down operations (i.e. Kaspersky Lab partnered with research teams at CrowdStrike, the HoneyNet Project and Dell SecureWorks in the March, 2012 takedown of Hlux/Kelihos [16]) should work with law enforcement, governments, and the legal system, to develop a controlled and methodical way forward. Basically I'm not arguing that organizations should take counterattack options off the table, but what I am arguing is that the actual process should be left to professionals who specialize in this sort of work, rather than be undertaken by an ISO who may dabble in hacking on the weekends. Working with specialists who do this sort of a thing for a living, and can successfully shut down the attacks, preserve evidence along the way, and work with the legal process is the way forward on this, if it must be done.

Conclusion

There is no question that cyber attacks are on the rise, and many frustrated organizations are in search of a new way to deal with the persistent threats, but do the risks, ethics, laws, and the probability to cause collateral damage outweigh their need to utilize active cyber defense strategies, or is there simply no other way forward but to turn the internet into a wild west shootout?

In a perfect world there would be well defined national and international laws and policies guiding who has the authority to take down attackers, there would be a cyber police division who specialized in taking down threats in a quick and efficient manner, there would be official oversight to the take down operations, and there would be international government and legal cooperation to handle these attacks, but we are a long way off from this ideal existence. There has to be further intelligent discussions among law enforcement, tech savvy security professionals, and policy makers moving forward. Organizations who have suffered attacks should feel compelled to transparently share reports detailing attacks on their networks so that the security community as a whole can grow and move forward intelligently, making decisions based on fact rather than rhetoric, best guesses, or just flat-out wrong information. Until a stronger set of laws and policies are developed, until better cooperation occurs, we may be looking at a future where organizations are compelled to simply say: "Hack me? No, hack you!"

TERRANCE STACHOWSKI

ARE YOU GAME?

GSM EXPLOITATION SOFTWARE EXPLOITATION MALWARE DESIGN ANALYSIS

THE NEXT SECURITY THING

DATE AND VENUE TRAINING : 27TH AND 28TH FEB 2013 CONFERENCE : 1ST AND 2ND MARCH 2013 BOGMALLO BEACH RESORT, BOGMALLO

n|ucon

FOR BOOKING AND SPONSPORSHIP - SPONSOR@NULLCON.NET OR CONTACT ANTRIKSH SHAH - +91 922 900 657

VISIT -WWW.NULLCON.NET

SILVER SPONSORS: Microsoft Praxeva ASSOCIATE SPONSORS: Adobe innobuzz iSIGHTPARTNERS SANS

MANAGED AND MARKETED BY PAYATU TECHNOLOGIES PVT. LTD WWW.PAYATU.COM

Introduction

to Anonymizing Networks – Tor vs I2P

The Right to Anonymity

Every operation made in cyber space, every visited web site, and every web service accessed, leave traces of the user's experience on the Internet. This information is considered very precious for commercial and intelligence purposes.

Private companies and governments are constantly monitoring the world wide web to collect and correlate the information to use in analysis on the user's behavior, but who manages these data, how does he do it, and which are the real finalities of monitoring activities?

Data acquired during the monitoring of the Internet often are personal information, even socially harmful, that may be available, intentionally or not, to anyone beyond the time limits dictated by the principle of finality of the data. Even if such data were deleted, they may still be accessible through storage mechanisms such as "cached".

Surveillance and monitoring are activities of primary interest for many governments that in many cases trace political opponents with dramatic consequences that flow in fierce persecution.

Recently the demand of anonymity has increased, mainly to respond to the large diffusion of surveillance platforms deployed all over the world, but the concept of anonymity induces fear in our imaginations due to the direct link that is usually made to illicit activities. It must considered that anonymity of user's experiences on the web could also be motivated by noble argumentations, such as the fight for the human right to liberty of expression, avoidance of censorship, liberal promotion and the circulation of thought.

Anonymous communications have an important role in our political and social discourse. Individuals desire to hide their identities because they may be concerned about political or economic retribution, harassment, or even threats to their lives.

How to anonymize the user's experience?

In the Internet, every machine is identified by its IP address that could be hidden by using anonymizing services and networks such as I2P and Tor network. Usually the anonymizing process is based on the concept of distribution of routing information. During the transmission of data between two entities in a network it is impossible to not know prior the path between source and destination, and every node of the network manages minimal information to route the packets to the next hop without conserving history on the path. To avoid interception, large use is made of encryption algorithms that make impossible the wiretapping of the information and the recomposition of the original messages.

The Tor Network

The Deep Web is the set of information resources on the World Wide Web, not reported by normal search engines. It is a network of interconnected systems not indexed having a size hundreds of times higher than the current visible web.

A parallel web that has a much wider number of information represents an invaluable resource for private companies, governments, and especially cybercrime. In the imagination of many persons, the Deep Web term is associated with the concept of anonymity that goes with criminal intents that cannot be pursued because they are submerged in an inaccessible world. It's fundamental to remark that this interpretation of the Deep Web is deeply wrong.

Tor is the acronym of "The Onion Router", a system implemented to enable online anonymity

thanks to the routing of Internet traffic through a worldwide volunteer network of servers hiding user's information.

As usually happens, the project was born in the military sector, sponsored the US Naval Research Laboratory, and from 2004 to 2005 it was supported by the Electronic Frontier Foundation.

Access to the network is possible using a Tor client, a software that allows user to reach network resources otherwise inaccessible. Today the software is under development and maintenance of Tor Project. Using a Tor Network a user could avoid his tracing, his privacy is guaranteed by the unpredictable route of the information inside the net and due to the large adoption of encrypting mechanisms.

Connecting to the Tor network

Imagine a typical scenario where Alice desire to be connected with Bob using the Tor network. Let's see step by step how it is possible.

She makes an *unencrypted* connection to a centralized directory server containing the addresses of the Tor nodes. After receiving the address list from the directory server the Tor client software will connect to a random node (the entry node) through an *encrypted* connection. The entry node would make an encrypted connection to a random second node which would in turn do the same to connect to a random third Tor node. The process goes on until it involves a node (exit node) connected to the destination.

Consider that during Tor routing, in each connection, the Tor nodes are randomly chosen and the same node cannot be used twice in the same path.

To ensure anonymity the connections have a fixed duration. Every ten minutes, to avoid statistical analysis that could compromise the user's privacy, the client software changes the entry node.

Up to now we have considered an ideal situation in which a user accesses the network only to connect to another. To further complicate the discussion, in a real scenario, the node Alice used could in turn be used as a node for routing purposes with other established connections between other users.

A malevolent third party would not be able to know which connection is initiated as a user and which as a node, making the monitoring of the communications impossible (Figure 1).

The Tor client distributed from the official web site of the project could be executed on all the existing platforms and many add-ons are freely avail-

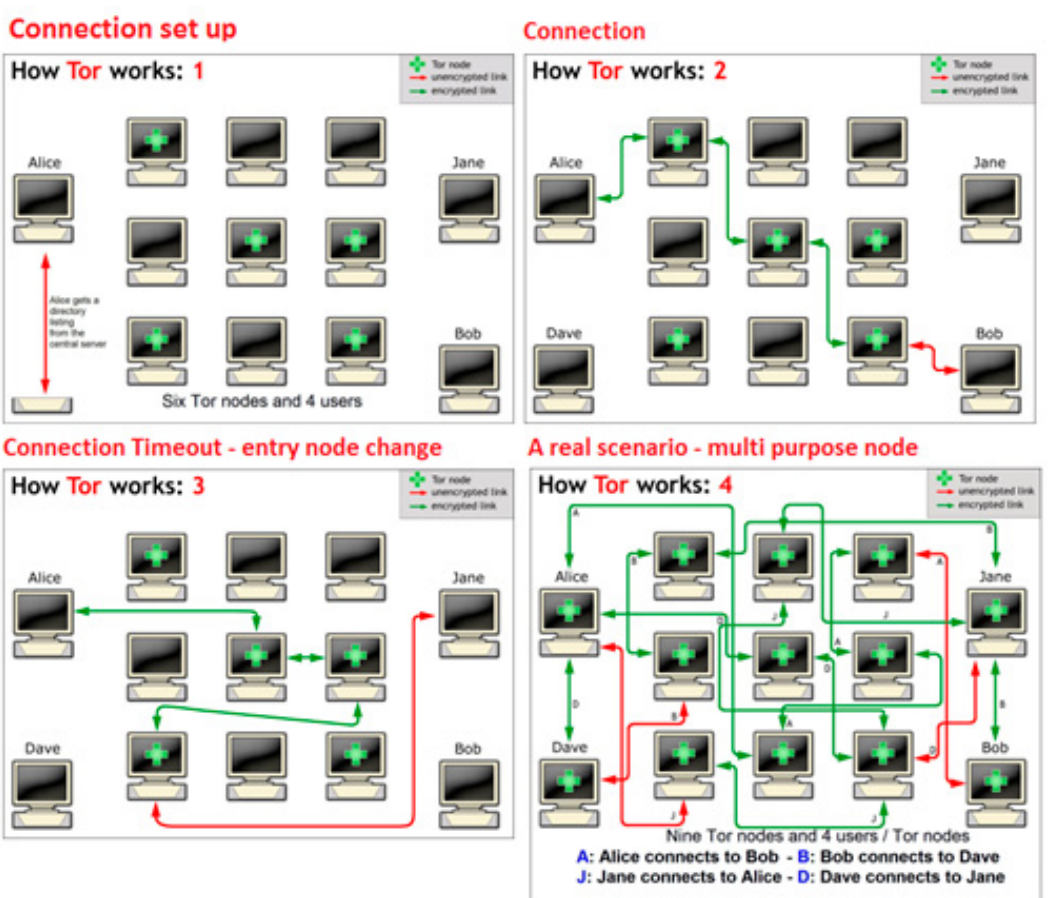


Figure 1. *Tor Routing*

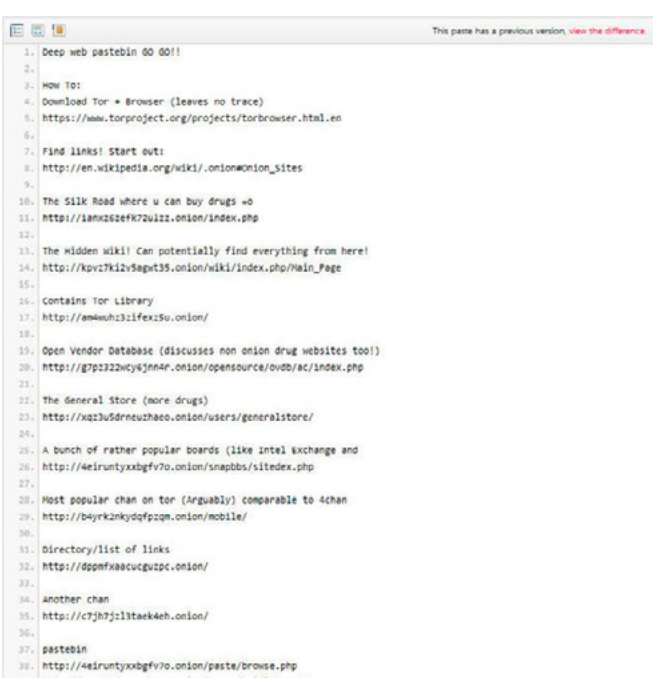
able that allow the integration of navigation software in existing web browsers. Despite that the network has been projected to protect user's privacy, to be really anonymous it's suggested to go though a VPN.

A better mode to navigate inside the Deep Web is to use the Tails OS distribution which is bootable from any machine without leaving a trace on the host. Once the Tor Bundle is installed, it comes with its own portable Firefox version, ideal for anonymous navigation due to an appropriate control of installed plugins.

The user must be aware of the presence of many plugins in his browsers that expose his privacy to serious risks. Many of these plugins could be used to reveal a user's information during the navigation.

As said, the resources inside the Tor network are not indexed and is very hard to find them if we are accustomed to classic search engines. The way to search the information is profoundly different due to the absence of indexing of the content. A practical suggestion to new users is to refer to Wikis and BBS-like sites that aggregate links, categorizing them in more suitable groups of consulting. Another difference that the user has to take in mind is that instead of classic extensions (e.g. .com, .gov), the domains in the Deep Web generally end with the .onion suffix. The following is a short list of links that have made famous the Deep Web published on Pastebin: Figure 2.

Cleaned Hidden Wiki should be a also a good starting point for the first navigations: *http://3suaolltfj2xjksb.onion/hiddenwiki/index.php/Main_Page*.



```
Deep web pastebin GO GO!!

HOW TO:
Download Tor + Browser (leaves no trace)
https://www.torproject.org/projects/torbrowser.html.en

Find links! Start out:
http://en.wikipedia.org/wiki/.onion#onion_sites

The Silk Road where u can buy drugs =o
http://ianxz62ef k72ulzz.onion/index.php

The Hidden Wiki! Can potentially find everything from here!
http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page

Contains Tor Library
http://am4wuhz3zifexz5u.onion/

Open Vendor Database (discusses non onion drug websites too!)
http://g7p3322wcy6jnn4r.onion/opensource/ovdb/ac/index.php

The General Store (more drugs)
http://xqz3u5drneuzhaeo.onion/users/generalstore/

A bunch of rather popular boards (like intel exchange and
http://4eiruntyxxbgfv7o.onion/snapbbs/sitedex.php

Most popular chan on tor (Arguably) comparable to 4chan
http://b4yrk2nkydqfpzqm.onion/mobile/

Directory/list of links
http://dppmfxaacucguzpc.onion/

Another chan
http://c7jh7jz13taek4eh.onion/

pastebin
http://4eiruntyxxbgfv7o.onion/paste/browse.php
http://xqz3u5drneuzhaeo.onion/users/boi/?show=65
```

Figure 2. *Tor Links*

Be careful, some contents are labeled with commonly used tags such as CP= child porn. PD is pedophile, stay far from them.

The Deep Web is considered the place where everything is possible, you can find every kind of material and services for sale, most of them illegal. The hidden web offers to cybercrime great business opportunity, hacking services, malware, stolen credit cards, and weapons.

We all know the potentiality of the e-commerce in the ordinary web and its impressive growth in last couple of years, well now imagine the Deep Web market that is more than 500 times bigger and where there is no legal limits on the goods to sell. We are faced with amazing businesses controlled by cyber criminal organizations.

I2P

According to the official definition, "I2P is a scalable, self organizing, resilient packet switched anonymous network layer, upon which any number of different anonymity or security conscious applications can operate".

I2P is an open source project developed in early 2003 by a group of full time developers with a group of part time contributors from all over the world.

It is fundamental to understand that inside an I2P network the "hidden" component is represented by an application in execution on the node doing, and of course the path followed by the information to reach the destination. Another important concept for I2P is the "tunnel", a directed path which extends through an explicitly selected list of routers. The first router that belongs to a tunnel is named "gateway".

The communication within a tunnel in unidirectional, this means that it is impossible to send back data without using another separated tunnel.

Also for I2P a layered encryption model is implemented, known as "garlic routing" and "garlic encryption", the information transits on network routers that are able to decrypt only the respective layer.

The information managed by each single node is composed by:

- IP address of the next router
- encrypted data to transfer.

The original architecture provides two further definitions:

- "outbound" tunnels are those tunnels used to send messages away from the tunnel creator
- "inbound" tunnels are those tunnels used to bring messages to the tunnel creator.

Another element of critical importance for the I2P model is the network database (known as "netDb"), a pair of algorithms used to share the following metadata with the network:

- "routerInfo" – a data structure to provide routers the information necessary for contacting a specific router (their public keys, transport addresses, etc). Each router send its routerInfo to the netDb directly, that will collect info on the entire network.
- "leaseSets" – a data structure to give routers the information necessary for contacting a particular destination. A leaseSet is a collection of "leases". Each of them specifies a tunnel gateway to reach a specific destination. It is sent through outbound tunnels anonymously, to avoid correlating a router with its leaseSets. A lease contains the following info:
  - Inbound gateway for a tunnel that allows reaching a specific destination.
  - Time when a tunnel expires.
  - Pair of public keys to be able to encrypt messages (to send through the tunnel and reach the destination).

I2P Routing

When Alice wants to send a message to Bob, she does a lookup in the netDb to find Bob's leaseSet, giving her his current inbound tunnel gateways.

Alice's router aggregates multiple messages into a single "garlic message", encrypting it using a particular public key, in this way only the public key owner can open the message.

For typical end to end communication between Alice and Bob, the garlic will be encrypted using the public key published in Bob's leaseSet, allowing the message to be encrypted without giving out the public key to Bob's router.

She selects one of her outbound tunnels and sends the data include of necessary instructions message and with instructions for the outbound tunnel's endpoint to forward the message on to one of Bob's inbound tunnel gateways. When the outbound tunnel endpoint receives those instructions, it forwards the message according the instructions provided, and when Bob's inbound tunnel gateway receives it, it is forwarded down the tunnel to Bob's router.

Be aware, we have said that transmission is unidirectional, this means that if Alice wants Bob to be

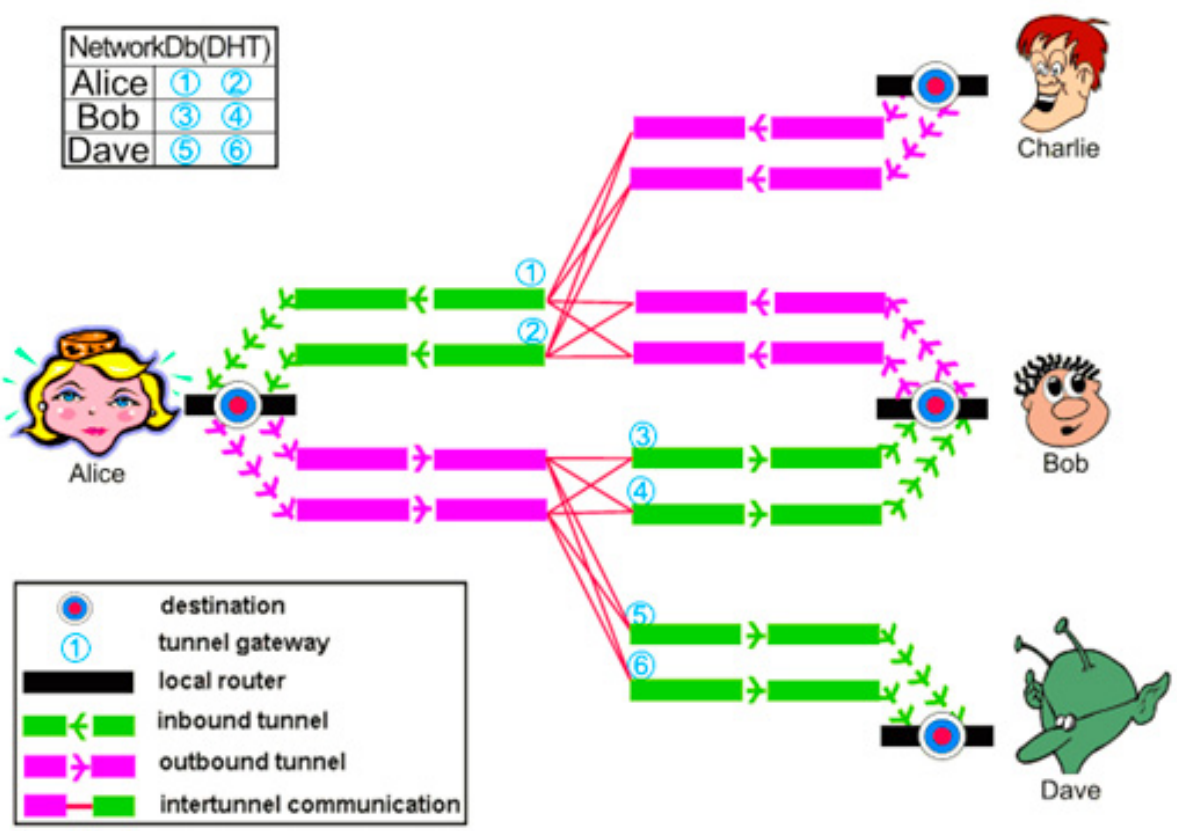


Figure 3. *I2P Routing*

able to reply to the message, she needs to transmit her own destination explicitly as part of the message itself.

I2P is end-to-end encryption. No information is sent in clear or decrypted during its path including the sender and recipient. To each node is assigned an internal network address different from the network IP address that isn't used (Figure 3).

Layered Encryption

The term layered encryption refers to the encryption process used during the transfer from a source to the destination through a series of peers that composes the tunnel.

Both Tor and I2P use layered cryptography. Intermediate entities have only to know how to forward the connection on to the next hop in the chain but cannot decipher the contents of the connections.

I2P is end to end encryption. No information is sent in clear or decrypted along its path, including the sender and recipient. To each node is assigned an internal network address different from the network IP address that isn't used.

I2P uses cryptographic ID to identify both routers and end point services, for naming identifiers is used the "Base 32 Names" techniques that attributes a SHA256 digest to the base64 representation of the destination. The hash is base 32 encoded and ".b32.i2p" is concatenated onto the end of the hash (Figure 4).

The sender repeatedly encrypts the data to transmit and at each hop is applied the proper decryption process. During the building phase, only the routing instructions for the next hop are exposed to each peer, meanwhile during the transferring, messages are passed through the tunnel, and the message and its routing instructions are only exposed to the endpoint of the tunnel.

Note that it is necessary to introduce an additional end to end layer of encryption to hide the data from the outbound tunnel endpoint and the inbound tunnel gateway, meanwhile each tunnel has a layered encryption to avoid unauthorized disclosure to peers inside the network.

At each hop the peer decrypts the message, extracting data and routing instructions, and sends them to the successive peer, encrypting all using the recipient's public key. The process is repeated until it has one layer of encryption per hop along the path. The algorithm used for encryption of the packets are ElGamal and AES encryption.

Garlic Routing

Garlic Routing is very similar to onion routing with several differences. Let's consider first of all that in garlic routing, it is possible to aggregate multiple

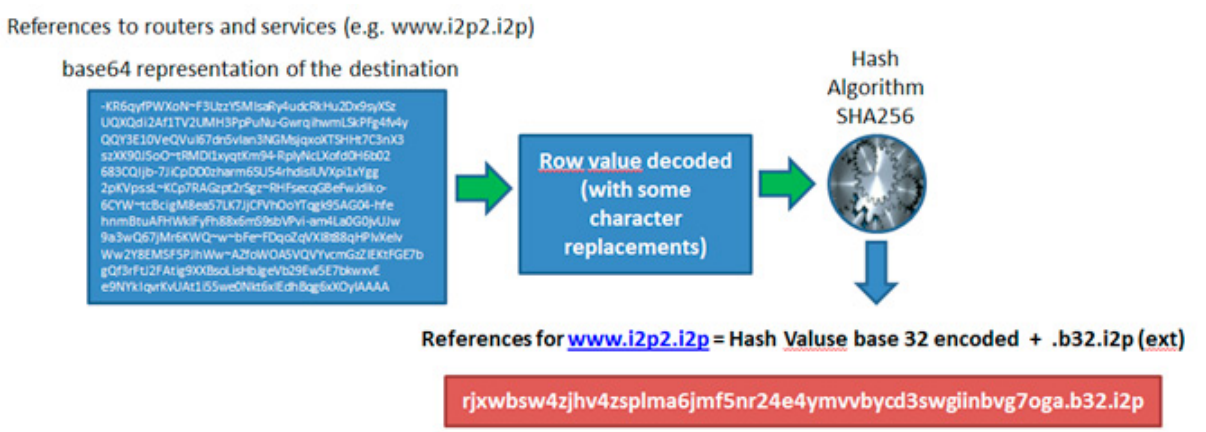


Figure 4. *Base 32 Names*

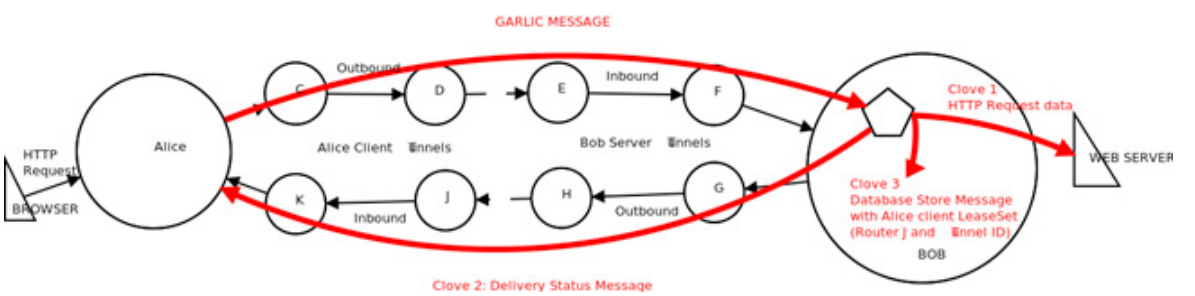


Figure 5. *Garlic Message*

messages. Another difference from Tor is that the tunnels are unidirectional.

Garlic routing in I2P is adopted mainly in three distinguished phases:

- For building and routing through tunnels (layered encryption). In I2P communication tunnels are unidirectional; this means that each interlocutor has to create a couple of tunnels, one for outbound and one for inbound traffic. There is also the possibility of a reply from the recipient, therefore another couple of tunnels must be created for a total of four tunnels.
- For bundling, determining the success or failure of end to end message delivery.
- For publishing some network database entries (Figure 5).

Comparison

The core design goal for I2P network is to allow the anonymous hosting of services, like Tor Hidden Services, rather than focusing on anonymous access to the public Internet such as Tor network. I2P does provide direct access to the public Internet via "out proxies". The functionality is offered by various internal services to proxy out onto other anonymizing systems such as Tor.

I2P APIs are designed specifically for anonymity and security, while SOCKS is designed for functionality. In the I2P total security is ensured against detecting client activity.

Without doubt Tor network has a greater visibility in the landscape of anonymizing networks. It is largely used by governments, hackers and also common people that in many countries try to elude censorship. The documentation related to the Tor network is more detailed and complete with respect to I2P and it is available in different languages.

From a technical point of view, Tor appears more efficient due to a better memory management and low bandwidth overhead for its clients. Despite these considerations, I2P services are faster than hidden service in Tor. A mechanism of performance ranking is implemented in I2P allowing the analysis of real performance of the nodes.

Every node in I2P architecture is also generally a router, so there is not a rigid distinction between a server and a pure client like there is in the Tor architecture. I2P implements a Packet switched routing instead of circuit switched that allows a better balancing of data across the network and major reliability. Let's remember that tunnels are unidirectional, meanwhile circuits are bidirectional.

Unlike Tor, I2P doesn't use centralized directory servers, but it utilizes a Distributed Hash Table (DHT). A distributed architecture system eliminates the risks of a single point of failure.

While Tor is developed using C language, I2P is based on Java.

References

- *http://www.i2p2.de/index.html*
- *https://www.torproject.org/*
- *http://www.i2p2.de/_static/pdf/i2p_philosophy.pdf*
- *http://www.i2p2.de/how_intro*

Conclusion

The article has the main purpose to introduce basics of the two most diffused softwares to anonymize a user's experiences on the web, Tor and I2P. Their importance in very high; thanks these networks it is possible to avoid censorship and monitoring. At the moment I have a meaningful experience with Tor networks, its community as said provides a great support for those users that desire or need to be anonymous on Internet.

I believe that despite the fact that I2P has existed about a decade, it is very under-utilized, the presence of a limited community represents in my opinion a brake on its growth.

I have used both and I found both efficiency effective. I tried also to sniff a package using specific software with the intent to disclose navigation data or any reference to the user's identity, of course without success.

The success of anonymizing a network is related to their diffusion, and without doubt Tor is a step forward, and the more users have access to sharing resources, the faster will be the navigation.

PIERLUIGI PAGANIN

Pierluigi Paganini is a security researcher for InfoSec Institute. InfoSec Institute is a security certification company that has trained over 15,000 people including popular CEH and CCNA certification courses.

Web Application Security Nowadays

Web Applications have become most crucial nowadays because we are now moving towards the new era of technology, where the web will play an important role and become a sensitive area of concern.

First we will talk about the web and its future scope. Few years ago, the web was a prominent place to showcase brands, share information, and media through it. Moreover, mails were the demanding features of the web.

Also, its popularity was limited to some people who are aware of technology and computers. Then there were some bottlenecks like cost, bandwidth etc.

But now it is the web and the Internet everywhere. On Desktop systems, mobiles tablets etc. all support the web. And the Internet is for every device. All the bottlenecks are trivial these days.

The web has evolved and changed the way people interact with eachother.

Now the Internet is used to share info, shop, work, entertainment etc. Even some businesses are only 'on' and 'for' the web.

This has increased the complexities with a lot of technologies and protocols working together in the background. Nowadays, we are also talking and working with cloud computing, mobile/tablet computing etc., which makes the web a very sensitive area of concern from the security point of view.

Cybersecurity is now the concerning topic because nowadays, the conditions in the fiction movies like 'The Net' 1 and 2 can be plotted in the real world.

Here we will see some ways in which web application may become vulnerable and ways by which these vulnerabilities can be avoided.

- Form Data Manipulation,
- Request Forgery,
- Sessions,
- Cookies,
- XSS,
- Injections,
- SQL Injections.

Form Data Manipulation

Forms are the unavoidable part of the web. As it's the way by which we can take inputs and information from users, its security is also important. What a hacker can do is change the possible inputs and make it a large form to handle or can malform to make false and fake information in the web app.

For example, if we take the following form under consideration: Listing 1.

Now, we can modify the form by the simplest available tool – *Google Chrome Developer Tools* and add a file input (LIsting 2).

We can see that now we can upload the file to the target server. Though, the file input won't make any big deal but it will occupy storage and port of the server for the time till which the page is active. And if the uploaded file is large in size, that will cause the server to listen to the browser until the browser doesn't finish. Now assume a scenario in which there is an extension to the browser which injects malicious input field in firms and large files can be uploaded by a large number of users. That would take the face of DDoS and may paralyze the server for some time, causing the web app to stop working.

In another case, the application has the file input to accept images and have some JavaScript validation on it. The user can modify the form, turn the script off, or upload a large file to the server and surely the web application will process it. How bulky it would become for server to handle it.

Preventions and Security

These types of attacks can be avoided by restricting users to use custom forms like forms created by the help of JavaScript and when the form has to be submitted by JavaScript; two step form submissions can be applied. Along with the two step verifications apply the server side validations and security checks because a client's system cannot be completely trusted for the safe input.

Request Forgery

Request Forgery is a very possible type of attack which a web app can face. Request Forgery, which is very well known as CSRF (*Cross Site Request Forgery*), stands for sending the requests to the web app from an unknown source and pretend to be sent from a known and authorized source.

To act this attack, an attacker may use the cURL. cURL or Canonical URL is the way to transfer data between servers in form of URL Syntax. In other words, it is a way to access the URL resources through various protocols. The cURL is available to be accessed from UNIX/Linux CLI. Library for various programming languages is also available. So an attacker with basic understanding of cURL can make CSRF attack happen.

For example I can send a request to the URL *www.google.com* with the following PHP code: Listing 3.

Listing 1. *Establishing a form*

```
<form name="" method="" action="">
<label>Email</label><input type='text' name='email' > <br/>
<label>Password</label><input type='password' name='pass' > <br/>
<input type='submit' name='login' value='Login' />
</form>
```

Listing 2. *Modifying the form*

```
<form name="" method="" action="">
<label>Email</label><input type='text' name='email' > <br/>
<label>Password</label><input type='password' name='pass' > <br/>
<input type='file' name='file' > <br/>
<input type='submit' name='login' value='Login' />
</form>
```

Listing 3. *Sending a request to a URL*

```
<?php
   $url = "http://www.google.com/";
   $ch = curl_init($url);
   curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
   echo $curl_scraped_page = curl_exec($ch);
   curl_close($ch);
?>
```

Listing 4. *Making a request appear as if sent from a mobile phone*

```
<?php
   $url = "http://www.google.com/";
   $ch = curl_init($url);
   $user_agent = 'Mozilla/5.0 (Linux; U; Android 2.2.1; de-de; HTC_Wildfire_A3333 Build/FRG83D)
                  AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1';
   curl_setopt($ch, CURLOPT_USERAGENT, $user_agent);
   curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
   echo $curl_scraped_page = curl_exec($ch);
   curl_close($ch);
?>
```

There are many curl options with which a request can be made to appear cleaner and harder for receiving server. Let's try to send a request to *www.example.com* and make it appear as it is coming from an Android Phone. The site will respond according to mobile phone if it handles mobile OS differently (Listing 4).

cURL can also be used to send a POST request to the servers as the form submits. This may lead to a severe possibility of phishing attacks.

For example, if we can make a phishing page just by copying the source of any site and changing the action attribute of main login form. Now on my action page we will collect the POST data and extract the data in which we are interested.

Now as we have got the data, we can forward that POST data to the original action page and show the complete output to the user. A regular user would not doubt the page and we have got our thing.

Preventions and Security

The request source is still the attackers' source so detecting and identifying the source can help you prevent these attacks. Moreover, you can use the session IDs to validate the requests, so that CSRF can be prevented. Attaching the validation tokens to URLs will also help. The form actions should be attached with a validation token. The access validation token should be generated based upon signatures of accessing system and IP address.

You can use prebuilt hashing functions to generate the access tokens or you can create your own also by using the existing ones.

For example here I am using MD5 and SHA to generate a hash of 40 characters (Listing 5).

This way, you can create your own hashing techniques and it will be unknown to the attacker.

Listing 5. *Generating a hash with MD5 and SHA*

```
<?php
   function generateToken(){
      $time = date( 'U' );
      $str1 = str_split( md5( $time ) );
      $str2 = str_split( sha1( $time ) );
      $hash = '';
      for( $I = 0; $I<20; $I++){
         $hash .= $str1[$I];
         $hash .= $str2[$I];
      }
      return $hash;
   }
?>
```

Sessions

Sessions are commonly used to keep the application safe and track the user's activities on application. As everybody knows sessions are stored on the server for every user. Session Hijacking attack is the famous attack for defacing sessions.

An attacker tries to copy the session from another system to his/her own system to gain the credentials of the user of another system. These attacks may benefit the attacker in any way or it may be done just for fun. Whatever the reason, your users and their data are at stake.

The simplest available tool and script is a Firefox extension. This extension hijacks the user's sessions in the same wireless network.

Preventions and Security

Session hijacking attack is simply not avoidable and curable. The security is completely dependent on authentication and authorization system employed in the web app. And yes, keep track of each and every session created and manage them effectively.

Reduce the session timeout time, validate the browsers and the OS of the session logged on, because it would happen for very rare cases that the user and the attacker will have the same OS browser and other measurable identities and entities, for example, OS, Browser, OS & Browser version etc.

Cookies

Cookies – the regular user and an attacker will think about different objects but both will have the same joy. For the web, cookies are the data stored by websites in the user's browsers. These cookies are used to store some amount of information which will help other components of web applications function properly, saving the user ID or user email in a cookie will save a SELECT query from the database.

Cookies have an expiration date, data value, and the domain restrictions. Many web app developers use cookies to store some data in the browser, such as "remember me" logins, session IDs, same user identification, etc. Cookies are not used commonly nowadays because of their vulnerabilities. It's like a treat to hackers and attackers.

Though, the use of cookies is deprecated in web applications and websites, it is still used frequently.

Now for example, let's look at a "remember me" login system. Here is the php code to handle data on the server (Listing 6).

As you can see in the code above, stealing the cookie from the user's browser can easily allow the attackers to take a partial control of the user's account.

Preventions and Security

It's OK to use cookies but due to the vulnerabilities, they can be compromised anytime, so I suggest to minimize the use of cookies and use sessions instead.

Moreover, if bound to use cookies, you can employ some authentication and authorization schemes to prevent the penetration, for example: assign session IDs with cookies,

- record IP, user agent string and match them on every new access,
- try to determine and store the location of the IP address to verify if possibly the same computer system is accessing and using web app through those cookies,
- only keep those values in cookies which are least sensitive and can help you gain the required application state,
- keep the cookie expiration time as low as possible.

Nowadays, many sites are warning the users that they are storing cookies on their browsers so that the user has an idea of possible security attacks.

XSS

XSS, that is Cross Site Scripting, is a special type of injection attack in which an attacker can inject a client side script, include or run any script on your website from any other source website to gain certain amount of access and privileges in web applications. This is done in order to bypass the browser's same origin policy applied on scripts. Those accesses and privileges are not going to completely paralyze the web app, but it will surely have some effects and might be just the beginning of the attack, and then it will surely go severe.

Let's have an example of an attack. Here in the example, we are having a text area to accept the lengthy messages.

Now the attacker can put a script code in that text area. Whoever is the receiver of that message, when the message is being read by user, he/she will not see the script code but will have that code on the page.

If that code contains some malicious code able to bomb the messages to its fellow friends, then it will surely harm your web app.

Or, the attacker's script can post the pornographic content to the fellow friends of the user and spread it to your web application.

Listing 6. *PHP code to handle data on server*

```
if(isset($_POST['submit_login']))
{
   $username =  trim($_POST['email']);
   $pwd=md5($_POST['pass']);

   $sql="select * from users where `email`='".$username."' and `password`='$pwd'";
   $res=mysql_query($sql);
   $row = mysql_fetch_assoc($res);
   if(mysql_num_rows($res)>0)
   {
   if(isset($_POST['stay']) && $_POST['stay']=="on") {
      setcookie("email", $username, time()+60*60*24*10,"/");
      setcookie("session", session_id(), time()+60*60*24*10,"/");
      $_SESSION['email']=$username;
      $_SESSION['id'] = $row['id'];
   }
   else {
      $_SESSION['email']=$username;
      $_SESSION['id'] = $row['id'];
   }

   $sql = "insert into `users_online`(`user_id`,`ip_addr`,`session_id`) values('".
               get_userID($_SESSION['email'])."', INET_ATON('".$_SERVER['REMOTE_
               ADDR']."'),'".session_id()."')";
   $res = mysql_query($sql);
}
```

This attack happened on Orkut Social Networking site in which attacker's script post *Bom Sabado* which linked to a Brazilian Community, and when the user clicked on the link, the user got subscribed to that community.

Preventions and Security

The Cross Site Scripting attack can be filtered and checked by taking care of the inputs received from the web application. These inputs must be checked for the HTML tags and other unwanted inputs like *script* tag, *onclick*, *onhover,* or event handler attributes. Many web applications use JavaScript to make the application interactive, make it tough to intercept, and make the use of Object Oriented approach in the JavaScript application.

SQL Injections

SQL injection is the use of especially crafted inputs in the input fields to escalate the login or any authentication and authorization schemes of the web application, and gain the access and permissions to use it like a fully innocent and normal user.

For example, you have seen Listing 1 and Listing 6. Now if we provide the following input in the input fields of emails and passwords, then we can have the escalated login to the web application (Listing 7 and Listing 8).

The SQL query should be built like

```
SELECT * FROM users WHERE email = 'example'
and pass='example_pass'
```

But now due to SQL injected input, it becomes similar to the following query

```
SELECT * FROM users WHERE email = 'a' or 1=1
or 'b' and pass='a' or 1=1 or 'b'
```

This query will result in the first available record in the database and provide full access to the attacker with the first user account.

Listing 7. *Making escalated login to web application*

```
email: a' or 1=1 or 'b
pass: a' or 1=1 or 'b
```

Listing 8. *Making escalated login to web application*

```
$email = $_POST['email'];
$pass = $_POST['pass'];
$sql = "SELECT * FROM users WHERE email
= '$email' and pass = '$pass';
$res = mysql_quer($sql);
```

The above explained SQL injection is the basic example; there are many more and yes, there are scripts and applications developed to exploit the vulnerability of SQL injection in the web application.

A SQL injection also needs to be taken care of because it affects both the front end and the back end of the web application.

Preventions and Security

The SQL injections can be prevented by escaping the user input for the SQL character set. The escaping process involves adding a backslash ('\') just before every SQL special character. They are called injections because the attacker injects some part of the string. Iin the combination of our strings, it makes a malicious one which, while executed, produces results desired by the attacker.

Some More Prevention

Some attacks may not be interfaced from your web application but are similarly severe. The attacks can exploit the currently present vulnerability of the system to deface it and gain what they want. Here I am listing some of the best practices of Server Environment:

- turn off the Directory Listing. It will prevent from showing the attacker what you have on your web server,
- turn on the URL rewriting feature of the server and try to hide the file extensions from the URL, so that it will confuse the attackers about the technology used by your server. Instead of that, use the error logs and reports for debugging purpose,
- turn off the error reporting which will prevent exposure of the error and related details to normal users and the attackers,
- keep the webpage execution time low because it will prevent such attacks as buffer overflow, DoS, DDoS, etc.
- the production environment should not have any server side output commented or hidden by the Client Side Markup because the attacker will surely analyze the webpage to obtain info about your web application. And of course, many regular users have the tendency to see the source code of the webpage,
- the JavaScript code used while in production should be minified, because it will prevent script kiddies to try any hack and trick on your web application,
- reduce the maximum File Upload size,
- escape every input received from the User

On the Web

- *http://www.useragentstring.com/pages/Mobile%20Browserlist/* Collection of User Agent Strings of Mobile Phones.
- *https://www.owasp.org/index.php/Main_Page* OWASP (Open Web Application Security Project) project for Web Application security awareness

Glossary

Minified JavaScript: *http://jscompress.com/* when JavaScript Code is processed to remove all the unnecessary character from the source code without changing the functionality. It's called Minified JavaScript.

Side because it may contain any type of script or injection code. So, to prevent those cases, escape the inputs received,

- web applications must have the robots.txt file, which contains the code to deny the listing of sensitive files and directories in search engines,
- whatever programming environment you deploy, keep track of the new versions of programming environment objects because new version were needed to be released to nullify vulnerabilities or add new features to the environment object. If it's about new features only then you don't need to worry. But if it is a vulnerability fix version, then you need to think whether you are using any part of code that can be exploited by that vulnerability.

Summary

Web applications should be treated and worked for their security because whatever the present Internet represents you, it's the web application. There are many who will want to put your application or site down due to many reasons like Market Competition, Script Kidding, Fun, Tests etc. Whatever would be the reason of the attack, you would not like your application to go down and loose its consumer's interest.

Cyber security is not the objective to attain but a process that must be followed to keep applications safe and up in all cases.

PANKAJ PATEL

The author has been working as a web developer for a company and also as a freelancer. He is a blogger by nature and blogs on 'Time to Hack' http://time2hack.com. He works on Linux (Fedora) and holds the Diploma of Computer Applications (DCA) and Bachelor's Degree (BE) in Computer Science Engineering. During his education and career he has gained some certifications like EMC ISA, CISE, MTA DBA, MTA WDF, IBM Certified Application Developer RAD, and IBM Certified Solution Developer WID.

Mobile Applications:

are you prepared to carry the risk?

Addressing today's top three mobile application threats

There is no question that mobile computing is growing at an exponential rate. This rapid transformation has caused security concerns to be outpaced by the ease of use, flexibility and productivity of mobile devices. When vulnerabilities are exploited, the security of mission-critical data becomes a serious threat.

Gain insight into the top three mobile application security threats facing organizations today and receive recommendations for mitigating associated risk.

According to Morgan Stanley research, the smart phone will become the dominant computing platform by the end of 2012, with more units being sold than desktops and laptops combined ("Ten Questions Internet Execs Should Ask & Answer"; Morgan Stanley Technology Research Presentation by Analyst Mary Meeker; Web 2.0 Summit, San Francisco, CA; Nov. 16, 2010.). It's been a remarkable and rapid transformation that much like the advent of the web has left security concerns outpaced by the ease of use and flexibility of a new tool.

The HP Fortify on Demand Manual Testing Team analyzed security threats associated with a number of mobile applications to identify the most common vulnerabilities.

The HP team found that applications on mobile devices are just as prone to security vulnerabilities as their web counterparts. There were numerous instances of insecure use of mobile API's, data exposure in transit and at rest, and other serious threats. Both iOS applications and Android applications were represented in the analysis. The analysis outlines the top three security concerns discovered in the survey sample set, along with recommendations as to how organizations can mitigate the associated risk.

You'll learn

- Mobile applications are just as prone to security vulnerabilities as their web counterparts.
- Insecure use of mobile API's, data exposure in transit and at rest and other serious threats make this shift to mobile computing a top concern for businesses today.
- The top three mobile application security threats observed in a sample set.
- Recommendations on how to mitigate the risk of security vulnerabilities in mobile computing.

Sensitive data leakage over insecure channels

The HP Team analysis discovered that more than half of applications (51%) are susceptible to information leakage vulnerabilities. A user's personal data was often sent over unencrypted network protocols such as HTTP. Much of this information was basic, such as names, addresses and phone numbers; however, it also included the current location of the user and the specific device identifier (aka the UDID).

A device identifier can be leveraged for incredibly targeted attacks against specific users. If the geo-location, unique device identifier and personal details of the device owner could all be intercepted via a vulnerable application, then an attacker would be able to actually locate a 'target' in the real world. The potential implications of this can be staggering.

Less dramatic, but equally concerning would be a situation involving application exploitation: if the application has been sending the UDID, full name, address, etc., to a vulnerable web service, and that web service was susceptible to SQL Injection, then every bit of data on that mobile device could be accessed.

Data transmitted over insecure channels is not limited to personal data – application data is also susceptible. The team found that log in information, user credentials, session ID's, tokens and sensitive company data were all being sent over unencrypted network protocols like HTTP. The consequences for a vulnerable banking application could be devastating. If credentials, session identifiers, personably identifiable information or other sensitive data was being transmitted to a backend server, the transmission must be secure. Otherwise, data could be intercepted by an attacker, using common network packet capturing tools or applications (i.e. DroidSheep).

The analysis also revealed that as much as 75% of the applications tested were capable of sending tracking data to third party advertising and analytics providers. While not technically a vulnerability, this does offer more attack vectors for a potential attacker if those providers are themselves not secure, or are sending the data over an insecure connection. Mobile application developers should consider the security of everything their applications can communicate with, not just their own applications. This extends to every third party service or library they used to build applications.

Lost / stolen devices

Devices get lost. Devices are stolen. This is not new and will certainly continue, but with the proliferation of mobile computing, the effort that organizations put into securing vulnerabilities introduced by lost or stolen devices has become more front and center.

Encryption on corporate computers is now standard protocol for most Fortune 500 companies. Ten years ago the news was filled with stories of data stolen from lost PC's. This has definitely reduced, in part because of legislative requirements, but also because corporations have learned their lessons the hard way. However, these same standards are not applied to mobile devices, and in the age of *Bring Your Own Device* (BYOD) to work, this is a still a critical problem that needs attention.

Mobile applications present unique areas of risk when a device they are running on is lost or stolen. 68% of the applications tested in this analysis did not secure the data stored on the device. As a result, attackers were able to obtain elevated privileges on a stolen device to access sensitive application data.

It is imperative that all credentials stored on a mobile device be either encrypted on Android or stored to the Keychain on iOS. Application sand-

boxing (limiting the resources the application can access) and code signing (putting restrictions in place to guarantee the code has not been altered) can help mitigate this in most scenarios. However, these can be bypassed by common device rooting (gaining privileged control) and jail-breaking techniques, giving the attacker total access to the entire file system of the device.

Malicious applications

In addition to protecting mobile applications from outside agents, these mobile applications must also now be protected from other applications stored on the same device. Nearly a quarter (24%) of the applications the team tested logged or stored sensitive data on the device that was readable by other non-privileged applications on the device.

10% of the applications tested allowed attacks via inter-application communication or via weak permissions (Android Intents/Permissions or iOS custom handlers). Malicious applications can typically only access another application's data if the data was stored world-readable (i.e. SD card) or if the application logged any sensitive data (Android Log method or iOS NSLog method). If a malicious application is able to load code that can elevate privileges, it may be able to completely compromise another application's data.

Inter-application communication can occur in both Android and iOS. While working with developers, we've observed developer confusion around how to properly implement Android permissions as well as inter-app communication due to its more granular, complex model.

For Android, developers should use the principle of least privilege and only define necessary permissions in AndroidManifest.xml for the application to function properly. Caution should be exercised when sending implicit Intents and exporting components. Explicit Intents should be used when possible. Exporting components should be avoided unless absolutely necessary.

For iOS, developers should validate the source bundle identifier to the open URL method when implementing custom protocol handlers. All sensitive logging calls should be disabled for applications in production. For Android, sensitive data should never be allowed to be written to world-readable/writable files or stored to the SDCard.

Recommendations

There are certain actions that organizations can take to mitigate the risk of mobile application security vulnerabilities. First, applications need to be manually audited and assessed before products are launched. This allows organizations to determine if any input injection vulnerabilities or information leakage vulnerabilities are present. The code should be analyzed via static analysis when being developed to find code-based vulnerabilities. As with any application, it's much more cost effective to address security vulnerabilities during development rather than after it has been released.

Secure data transmission standards should be included as part of any application's requirements, especially if an application is being developed by a third-party. The same goes for secure data storage and application logging. Reasonable inter-application communication exposure and permissions in application requirements should be stringently defined. These concerns should all be addressed in the requirements phase and tested during development.

Lastly, when performing security testing and analysis on mobile applications, the server-side web services and APIs that the mobile clients talk to should be taken in context and analyzed for vulnerabilities. High-risk vulnerabilities may be missed if the two are tested out of context with each other.

MARK PAINTER

Mark Painter has been in the security industry since 2002, when he joined SPI Dynamics. During his tenure, he's focused on vulnerability research, product management and social media. Painter is currently the Product Marketing Manager for the HP Fortify WebInspect product suite as well as HP Fortify on Demand professional services.

IMF
INTERNATIONAL MANAGEMENT FORUM

IT Security Courses and Trainings

IMF Academy is specialised in providing business information by means of distance learning courses and trainings. Below you find an overview of our IT security courses and trainings.

Certified ISO27005 Risk Manager
Learn the Best Practices in Information Security Risk Management with ISO 27005 and become Certified ISO 27005 Risk Manager with this 3-day training!

CompTIA Cloud Essentials Professional
This 2-day Cloud Computing in-company training will qualify you for the vendor-neutral international CompTIA Cloud Essentials Professional (CEP) certificate.

Cloud Security (CCSK)
2-day training preparing you for the Certificate of Cloud Security Knowledge (CCSK), the industry's first vendor-independent cloud security certification from the Cloud Security Alliance (CSA).

e-Security
Learn in 9 lessons how to create and implement a best-practice e-security policy!

Information Security Management
Improve every aspect of your information security!

SABSA Foundation
The 5-day SABSA Foundation training provides a thorough coverage of the knowlegde required for the SABSA Foundation level certificate.

SABSA Advanced
The SABSA Advanced trainings will qualify you for the SABSA Practitioner certificate in Risk Assurance & Governance, Service Excellence and/or Architectural Design. You will be awarded with the title SABSA Chartered Practitioner (SCP).

TOGAF 9 and ArchiMate Foundation
After completing this absolutely unique distance learning course and passing the necessary exams, you will receive the TOGAF 9 Foundation (Level 1) and ArchiMate Foundation certificate.

TOGAF

cloud CSA security alliance

CCSK

CompTIA CLOUD ESSENTIALS

ArchiMate®

SABSA

For more information or to request the brochure please visit our website:
http://www.imfacademy.com/partner/hakin9

IMF Academy
info@imfacademy.com
Tel: +31 (0)40 246 02 20
Fax: +31 (0)40 246 00 17

Wireshark

How to Dig Out the Sniffing Potential from It?

Wireshark is the perfect tool for capturing and analyzing traffic on a wired ethernet network, IEEE 802.3, virtual networks, or nowadays, also wireless network, IEEE 802.11.

Wireshark has multiple capabilities: filtering protocols, IP addresses' sources or/and destinations, or aggregating all the packets from a designated communication and showing the file content transmitted in just one command .

If the communication is not ciphered, it is possible to see in clear text the identification of the user and the respected password transmitted.

It is also known as the trouble solve when the problem reaches the layer 2 or 3 from the OSI model, including QoS problems and overcharged communications.

This article gives an overview to understand the reason of Wireshark's existence and the potential it delivers for the IT community.

Introduction

Wireshark exists since 2006, when Gerald Combs was working for an Internet Service Provider, ISP. During that time, it was named Ethereal. Combs developped the application to help identify problems in the complex network. Just four years later, in August 2010, the name was changed to Wireshark when Riverbed Technology Company purchased CACE Technologies Company.

Riverbed Technology is also known for a wide variety of solutions and products that I had the pleasure to integrate in projects and implement.

What are the real application features?

It can:

- read live data from IEEE 802.3, IEEE 802.11, PPP/HDLC, ATM and Bluetooth,
- provide deep inspection of hundreds of protocols like: IP, HTTP, SMTP, DNS, FTP, SMB, DHCP and also P2P applications like Bit Torrent,
- provide live capture packets, exhibited in the application screen and written simultaneously in a file that can be analyzed offline and shared with manufactures and internal support teams,
- apply multiple filters, distinguishing the packets information through different colors based on protocols and highlight the corresponding communication selected from the first packet to the last,
- identify VoIP traffic,
- decrypt many protocols,
- supported in Windows environment, Linux, UNIX, OS X, Solaris, and most of Linux and UNIX flavors,
- be exported to other formats like plain text, CVS, or XML,
- new protocols support is added in each new update or release.

Advisory note

Before starting to capture all the traffic in any network, I should advice all readers that all the actions described in this article should be carried out with the proper approval documentation from the IT infrastructure Owner and Security Managers, except in case of laboratories and virtual environments specific for those tests. Keep in mind that doing such a capture without the right approval is illegal and also can contain private and confidential data.

For the sake of this article, a virtual environment was created to simulate the traffic between two S.O. machines. One plays as the client and the other as the Server.

In this concrete scenario, the client will also use the Wireshark application.

Usually, I prefer to use BackTrack distribution in my laboratories, the last version 5 releases 3 are perfect because comes already with the Wireshark application installed (version 1.8.1).

In this scenario for the server, I have defined a Windows 7 from Microsoft with the FileZilla server installed. Also for the purpose of this test I will create a new user and password.

As most of the readers have probably already detected I will demonstrate a communication based on FTP protocol.

I would like to say that there is nothing like a memorized image to understand what we are talking about. A simple vision of the created environment is always important to have references over the test that we are preparing to execute. I have developed an illustration, Figure 1, to establish this baseline.

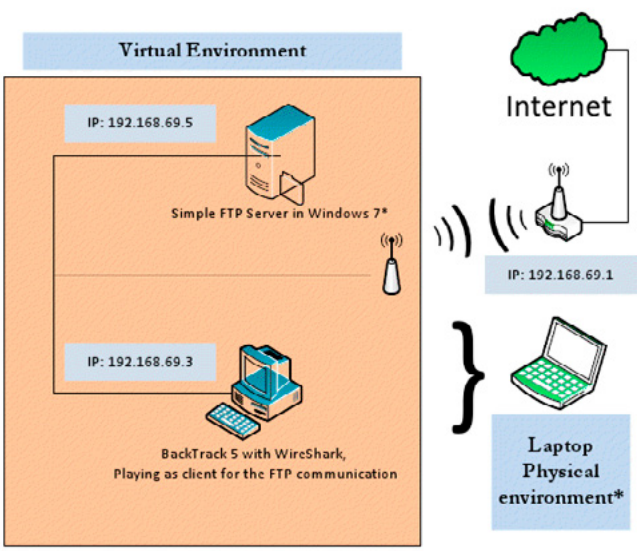


Figure 1. *Network Topology*

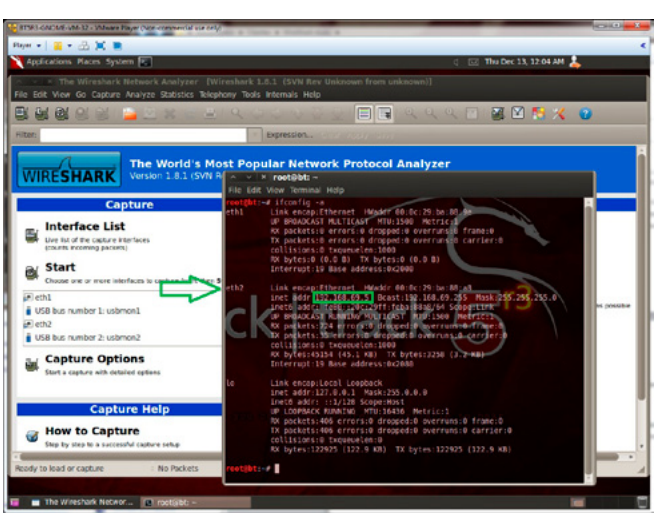


Figure 2. *Client network*

At the first instance, let's look at the illustration provided above.

The Laptop has a virtual network that is linked to the Wireless physical network; the virtual environment is based on VMWare Player.

What is the real difference between the regular virtual network environment and the one I provide to the readers?

The complexity is increased because, even in the scope of virtual environment, normally the IP addresses are defined or obtained from the DHCP service associated with the virtual network.

In this case, we are at the virtual level but the IP addresses provided are from the Wireless Internet Router. The real difference is at the level of Internet access; both can access the internet without dependencies. Each one can be up and running independently and access the internet. At the same time, they can communicate between themselves in a semi-public network. This method is called bridge mode but normally is used for only one machine with two interfaces.

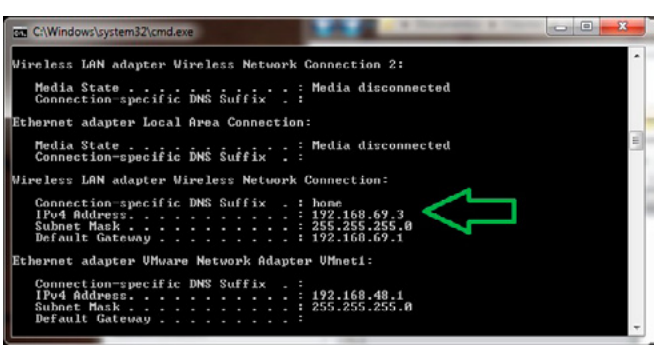


Figure 3. *Server network*

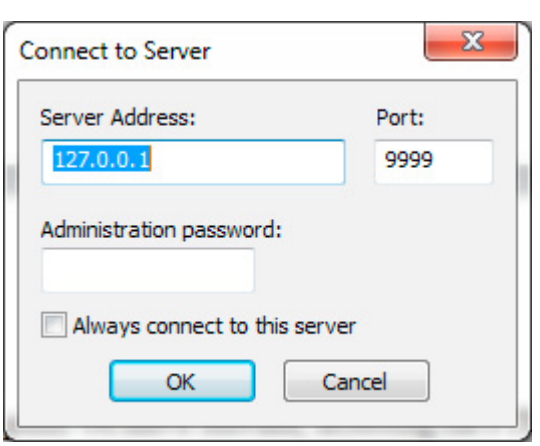


Figure 4. *Connecting to the interface of FileZilla, in this case I am running on port 9999, but the readers can define the port above 1024 and associate a password for administration*

At this point, I will provide also the illustration of each environment machine: Figure 2 and Figure 3.

At this point we move forward, access the FTP Server application, FileZilla, and create the user. Before that, in order to start we must run the FileZilla service or choose it to run automatically during the installation (Figure 4).

At this level, the readers should see the following interface: Figure 5.

The next step is to create the user to test the service and define the password as the following illustration.

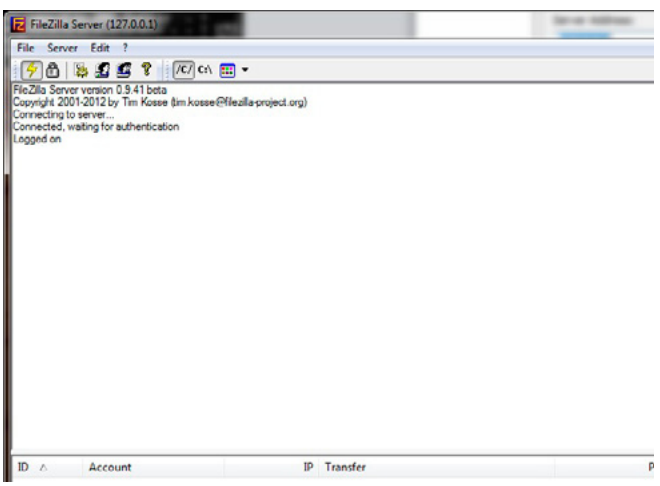


Figure 5. *FileZilla Server*

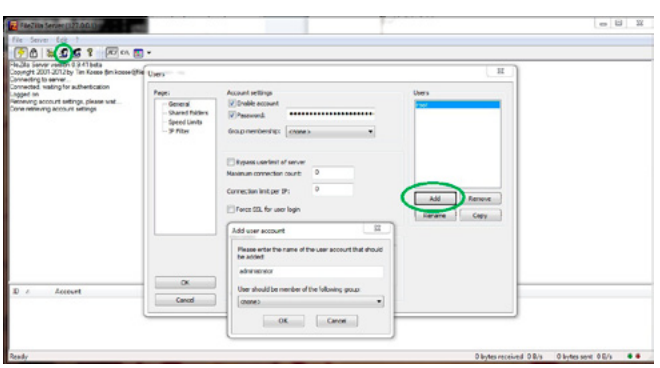


Figure 6. *FileZilla Server credentials*

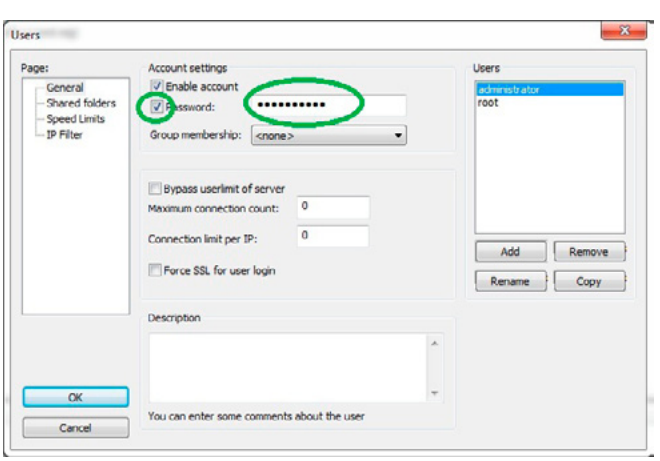


Figure 7. *FileZilla Server password*

First go to the face image, in the upper left corner, then select “Add” to open a new window identified as “Add user account.” Define the name of the user (Figure 6).

The second step is to select the box associated to and define the password (Figure 7).

After clicking “OK,” the reader will receive an alert due to the directory associated with the user (called “Shared Folders”). At this level, I advise that the readers create a new directory and

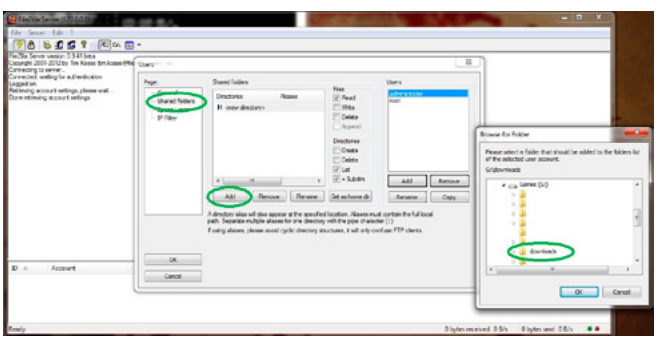


Figure 8. *Shared Folders*

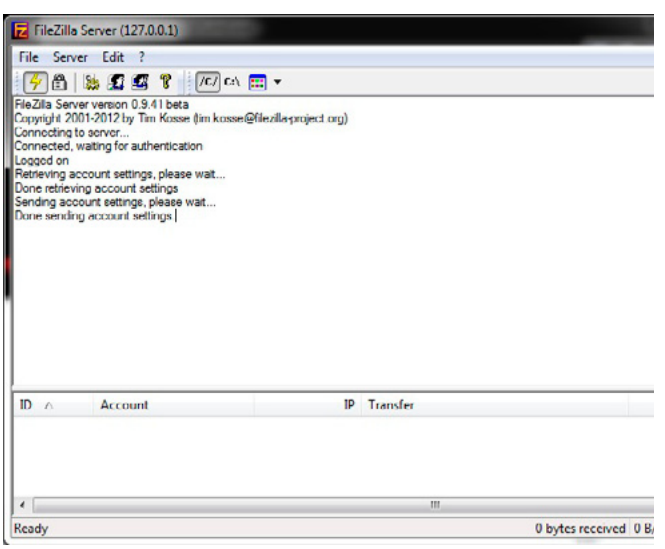


Figure 9. *Filezilla concluded*

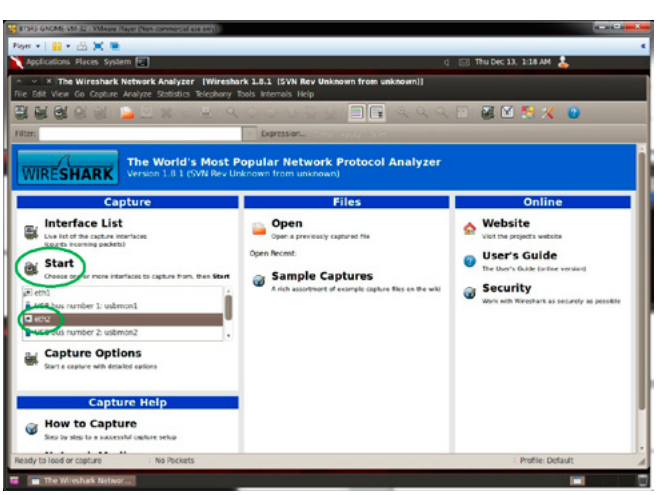


Figure 10. *Wireshark starting*

not simply select an already used one. This directory should be empty, and only after that the files should be transferred. Next, the transfer stops the service or immediately remove the files from the directory to another not shared directory.

After creating this directory, associate it to the user through this step:

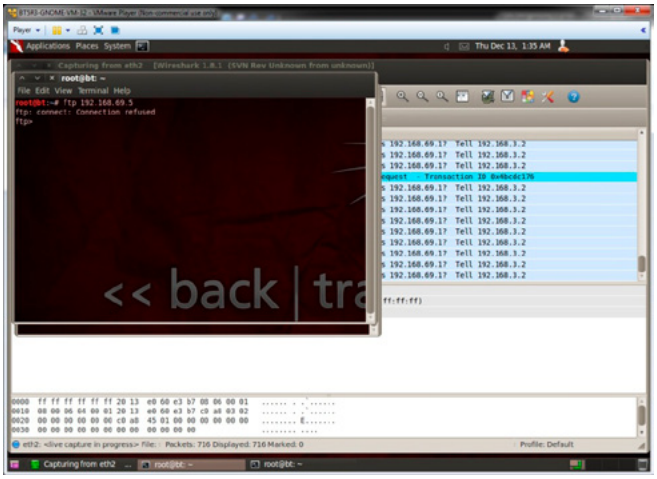


Figure 11. *FTP Client*

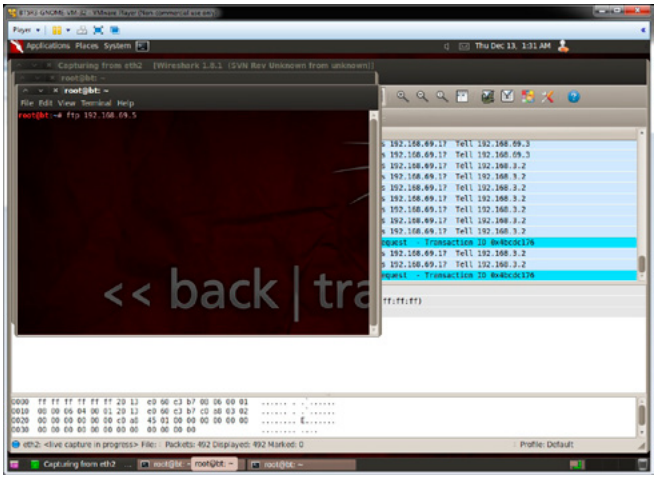


Figure 12. *FTP Client fail*

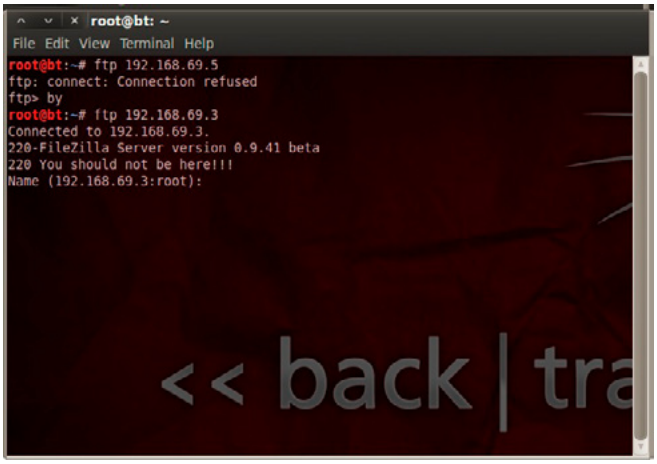


Figure 13. *FTP Client success*

In “Page,” (left hand side), select “Shared folders,” “Add,” select the correct directory, and process with the “OK” button (Figure 8).

The option associated with the “Files” should be read only with the option for the client to be able to “List.” In real environments, it is not a good practice to leave the “List” function active, because the remote user could list the files available and obtain a part or all the files.

In such cases, it is always good to provide the name of the file, so the remote user could only obtain those provided.

For that matter, at this point I will leave the “List” option active to prove that the file is available.

This stage is concluded; the message in the end of this process should indicate that the account settings are done (Figure 9).

After the first phase, it is time to move on to the second phase.

The second phase consists in activating the Wireshark service and capturing the traffic.

For that, let's jump to the virtual machine with BackTrack 5, and start the identification of the interface.

If we compare it with the first illustration (Figure 10), the application Wireshark should be visible and the interface(s) available should be listed above in the “Start” option.

The interface that should have the same IP address as the network, in this case (based on Figure 2 provided before) corresponds to `eth2`. Let's check again.

Based on the verification, the interface `Eth2` should be selected in the “Start” section.

At this phase, the Wireshark is ready to start capturing traffic, the readers are seeing some traffic, some packets are broadcast, and the other could be some DHCP requests or Arp requests.

At this point, we should move fast, because the traffic that we really want to analyze is not captured.

Open a terminal in the client machine and execute a FTP command to the FTP server.

The command should be similar to the following, differing according to the IP address and network that the readers have chosen.

If they are the same, just execute “ftp 192.168.69.5.” (Figure 11)

The result from the executed command could be one of the following:

Fail, informing that the connection was denied or refused (Figure 12).

If this is your case, don’t panic – the reader should verify the permission from the external to access your machine.

This verification is done at the firewall level of this machine, virtual or physical. The reader should open the port 21 to permit the client to access the application, in this case FileZilla ftp server.

After this change is done, retry the last step again, executing ftp 192.168.69.3

Success, following by the request of the username and password (Figure 13).

On the Server side, the information in the FileZilla interface should be the following: Figure 14.

At this point, the reader should insert the User and Password that we have defined before.

The output of the process of authentication and transference of one file should be similar to the illustration below.

If the reader is not so well familiar with the FTP commands, please refer to the end of the article for links to this topic (Figure 15).

At this stage to finish the capture of traffic, the readers should close the terminals or switch to the

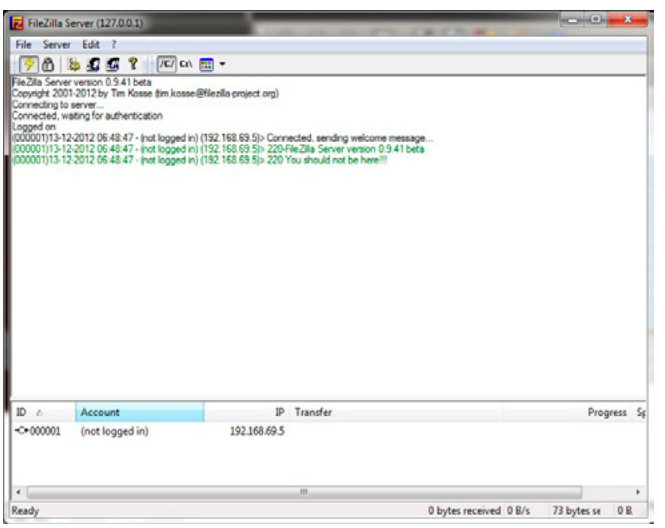


Figure 14. *FTP Client success – part 2*

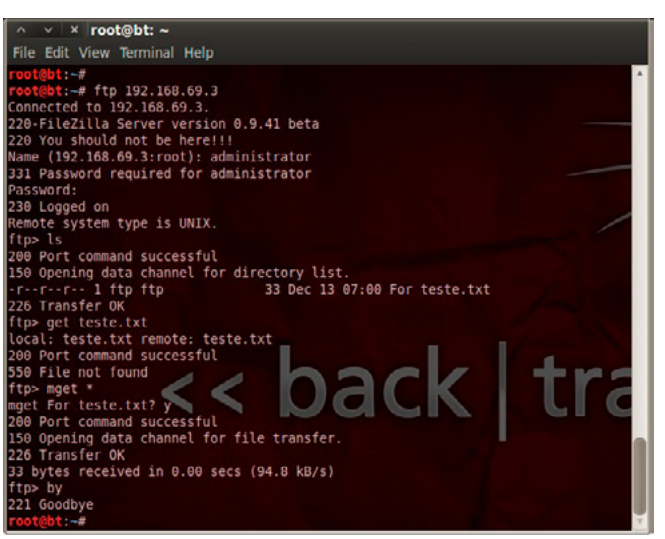


Figure 15. *FTP Client success – part 3*

Wireshark application and stop the process of capture with the stop button as illustrated (Figure 16).

Now the phase 3 begins, analyzing the captured traffuc and applying filters.

Concerning the filtering function, what is done is applying expression to decrease the amount of traffic and specify the communication that we want to identify and analyze.

The comparison functions available are:

eq, == Equal
ne, !=Not Equal
gt, > Greater Than
lt, < Less Than
ge, >= Greater than or Equal to
le, <=Less than or Equal to

The junction of the expression is accomplishing through Boolean expression:

and, && Logical AND
or, || Logical OR
not, ! Logical NOT

Refer to the list of possible filters through the link provided at the end of the article.

I suggest to begin with a list of what we want to apply before starting to apply expressions or defining Filter expressions.

So at this level, we want to filter by IP address and protocols.

Let's create the list:

```
IP address "Source" = 192.168.69.3 and
                192.168.69.5
IP address "Destination" = 192.168.69.3 and
                192.168.69.5
Protocol = FTP
```

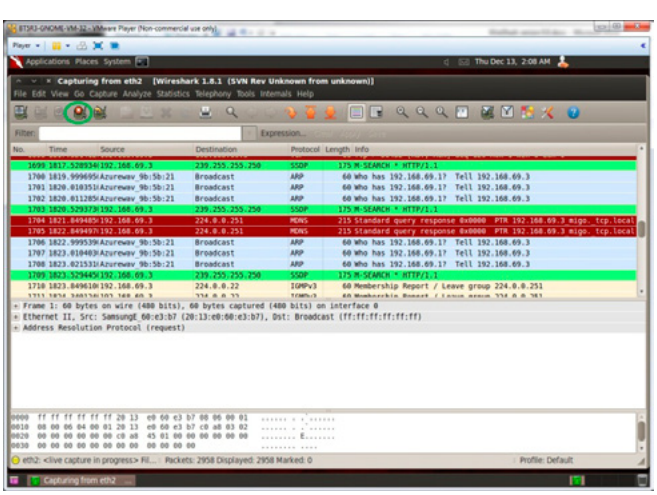


Figure 16. *Wireshark stop*

Let's convert the list to the language that in fact Wireshark can interpret, defined as a "Filter."

```
ip.addr == 192.168.69.0/24 and ftp
```

This expression is a macro of the list. If the reader wants to perfect match the list, they should use the following filter:

```
ip.addr == 192.168.69.3 and ip.addr
== 192.168.69.5 and ftp
```

Either way, the result should be similar, showing only the bilateral communication between the two machines, which the IP address are 192.168.69.3 and 192.168.69.5, filtered by the FTP protocol.

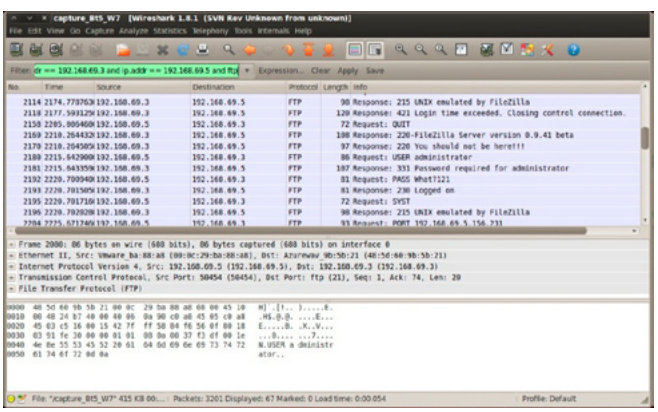


Figure 17. *IP addresses and FTP protocol*

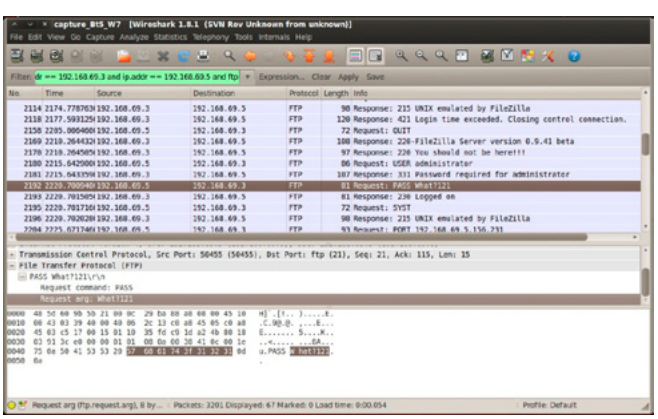


Figure 18. *Filtering by password*

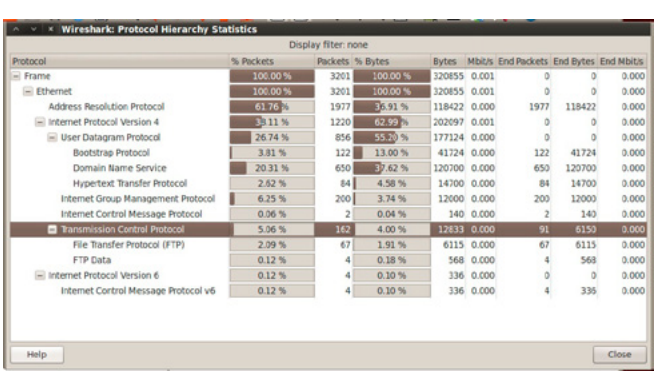


Figure 19. *Statistics*

Notes

Software and information available to support the tests:

- Wireshark, software, *http://www.wireshark.org/download.html*
- Wireshark, User's Guide, *http://www.wireshark.org/docs/wsug_html_chunked*
- Wireshark, filters list *http://www.wireshark.org/docs/man-pages/wireshark-filter.html*
- Backtrack 5 r3, *http://www.backtrack-linux.org/downloads*
- FTP Filezilla server & client *http://filezilla-project.org*
- IEEE 802.11, *http://en.wikipedia.org/wiki/IEEE_802.11*
- IEEE 802.3, *http://en.wikipedia.org/wiki/IEEE_802.3*
- OSI model, *http://en.wikipedia.org/wiki/Osi_model*
- QoS, Quality of Service, *http://en.wikipedia.org/wiki/Quality_of_service*
- FTP Commands, *http://www.cs.colostate.edu/helpdocs/ftp.html*

Based on this list, let's generate the expressions, as illustrated Figure 17.

As the readers can see, the FTP protocol uses the transference of data and credentials in clear text mode, so it's easy to identify the User that was authenticated "administrator."

In this line of thought, identified two lines bellow, is the password transmitted, as the illustration demonstrates (Figure 18).

As demonstrated, the applicability of the Wireshark application is enormous, and the access to the statistics indicators' leverages the global application to one of our favorite "must have" for the technical support or traffic investigation.

For the record, the total amount of packets transmitted in this global communication were 3201, the FTP service analysis represents only 5% of the packets or 4% of the data transmitted.

That opens the door to investigate what are the remaining 95% of the packets doing in our lab network, as illustrated Figure 19.

Try to see the full statistics functions, with special attention to the Flow Graph that provides the first handshake between the machines and further communication of the FTP protocol. It is also very interesting to check if there are any delays in the communication because each packet is displayed with the referential time (Figure 20).

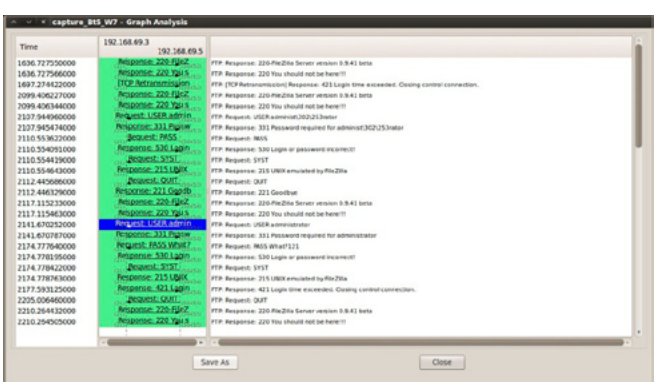


Figure 20. *Flow Graph*

Things to remember

Define and apply the filter before starting the capture. Tthis will decrease the amount of traffic written in the output file.

Check the port mirror function – this is important in real environments.

If your internal or DMZ networks don't have IDS/IPS equipment, it's a good practice to capture traffic during one full day to have a notion of the type and level of saturation of the traffic. For the external network, it's a good measure to verify the QoS traffic and the possible identification of retransmissions and packet delays.

Conclusion

As a resume of all actions taken through this article the reader is able to use Wireshark and its configurations needs at a basic level, capture and analyze traffic, apply filters and some good methods when working with this tool.

The traffic statistics are essential to map and mitigate possible problems, increase the service over the business of the company and have the right controls for the global communications.

Wireshark is a very useful tool for problem solving and is available in most of the operation systems.

MANFRED FERREIRA

Manfred Ferreira is currently an IT Strategy Advisor, who has been working for 16 years in the information security marke, developing projects for the European committee in the early years. He is business-oriented and provides Business Continuity Management and Information Security advisories. He specializes in security solutions assessment and penetration testing in the context of risk identification and mitigation.

Part of information is disclosed in the professional network.

LinkedIn: pt.linkedin.com/pub/manfred-ferreira/15/536/698

E-mail: manfredf@zonmail.pt

EBCG
WE BRING INTELLIGENCE TOGETHER

3rd Annual

CYBER SECURITY SUMMIT

"Coping with Cyber Risk in Practice"

11th & 12th April 2013, PRAGUE

Special Offer
in cooperation with:
Haking
IT SECURITY MAGAZINE
20% off!
(Discount code: HknIT)

Does you organization implement Cyber Security Solutions? Would you like to learn from industry peers on how they do this? Do you have a solution that you would like to present in front of the biggest industry minds?
The CSS will bring together key corporate security decision makers to discuss the strategic priorities, potential risk factors and threats. Together, they will provide you with inspirational guidance on how industry experts respond to these denunciatory challenges.

Why should you attend?

- Gain an insight into the IT incidents
- Understandt how nations premier companies are improving their cyber security
- Address your questions to the best experts
- Find out how secure you are and what level and form of attack could come in to you
- Review your level of security and readiness for penetration
- Align your security strategy with critical business and corporate goals
- Obtain the latest update on state of art in digital treats in cyber underground
- Utilize the full potential of cyber security
- Learn how to information awareness can minimize your risk
- **HOT TOPIC:** Banking Malware and Threats

What distinguishes this event?

CSS is not a typical summit focused on government agencies. The light is shed on coping with cyber risk in the enterprise world. Building on the success of our previous events, the distinguishing features of this unique format are:

- One of the best experts in the world answers your question and provide their in-depth know-how
- Unique mix of 15 presentations, practical sessions, key studies
- Exclusive senior-level attendance
- Practical and up-to-date studies and solutions
- Customized itineraries
- EBCG ThinkTank sessions - who knows your business better than your peers

4 Ways to contact us:

Tel.: +421 2 3220 2200
Fax: +421 2 3220 2222
e-mail: event@ebcg.biz
web: www.ebcg.biz

Interview with

Aseem Jakhar

Ewa Duranc, Hakin9 Magazine Editor speaks with Aseem Jakhar the Founder of nullcon Security Conference.

Ewa Duranc: Can you introduce yourself to our readers?

Aseem Jakhar: I am currently the Director, Research at Payatu Technologies, a security services organization with expertise in product/application security assessment. I have 9 years of experience in system programming, security research, consulting and managing security software development projects. Have worked on various security software including IBM ISS Proventia UTM appliance, messaging/security appliance, anti-spam engine, anti-virus software, Transparent HTTPS proxy to name a few. An active speaker at various security and open source conferences including Defcon, Hack.lu, Blackhat, Xcon, Cyber security summit, Cocon, OSI Days, Clubhack, Gnunify. I am the author of open source Linux thread injection kit – Jugaad and Indroid which demonstrate a stealthy malware infection technique and desktops OS and Android. I'm also known in the security community as the founder of null -The open security community, registered not-for-profit organization *http://null.co.in*, the largest security community in India.

ED: Ok, Let's talk about nullcon Security Conference. What was the idea of creating it?

AJ: nullcon was founded in 2010 with the idea of providing an integrated platform for exchanging information on the latest attack vectors, zero day vulnerabilities and unknown threats. Our motto – "The next security thing" drives the objective of the conference i.e. to discuss and showcase the future of information security and the next-generation of offensive and defensive security technology. The idea started as a gathering for researchers and organizations to brain storm and demonstrate why the current technology is not sufficient and what should be the focus for the coming years pertaining to information security. In addition to security, one of the section of the conference called Desi Jugaad (Hindi for "Local Hack") is dedicated to hacking where we invite researchers who come up with innovative security/tech/non-tech solutions for solving real life challenges or taking up new initiatives.

ED: What are the type of events that happen at nullcon?

AJ: nullcon is a 4 day summit. The first two days are dedicated to security training given by renowned security experts, followed by a two day conference which comprises of talks, workshops, hacking competitions, villages and after parties.

Hacking Competitions

We conduct three different types of hacking challenges:

- HackIM – The pre-con online competition (*http://ctf.nullcon.net*). The first three winners get free VIP passes for the conference.
- Battle Underground – It runs during the conference over the cloud, so people who cannot participate in nullcon also get to take part in the challenge.
- JailBreak – We started Jailbreak in 2012. It happens two days before the conference and

is a 36 hrs continuous in-house competition. The participating teams are kept under house arrest. They are given a main objective which can be either writing exploits, tools or finding vulnerabilities in software products. During the challenge the teams are given small puzzles to solve after every few hours and the team that cracks the puzzle first is allowed 15 mins to move out of their room and use the toilets, cook food and eat. The team that finishes the challenge is allowed to break free from the Jail. All teams are given 20 mins speaking slot during the conference to talk about their solution and the methodology used and the winners are selected by a panel of judges. The winning team takes away $$$. The last Jailbreak was amazing and we also shot the videos of the competition. Folks who are interested can take a look at:

- JailBreak Teaser – *http://www.youtube.com/watch?v=xciUR9fUarU*
- JailBreak Episode 1 – *http://www.youtube.com/watch?v=2Ehrv0_6wB0*
- JailBreak Episode 2 – *http://www.youtube.com/watch?v=78GLbFVOb3g*

Workshops

We are introducing workshops in the upcoming conference. The workshops will be free for the attendees and run parallel to the talks. We have some amazing workshops lined up for nullcon Goa 2013.

Villages

These are informal learning sessions on tech/non-tech subjects where participants get direct hands-on on different subjects such as hardware, robotics, smartphone OS.

Networking parties

We make sure that delegates get a good feel of Goa and can network with peers and speakers in an informal setting.

ED: What projects are you working on? Can you tell me about them?

AJ: Nullcon keeps us busy for a good amount of time during the year. Other than the conference, we specialize in security assessment for *applications/products/telecom/mobile*. We also do customized security training and consult on Secure SDLC process. Our clients include financial institutions, security appliance, online product companies, healthcare, telecom operators to name a few in Asia and Europe.

ED: Nullcon Events date from 2010. What topics do you cover during your conferences? Who attends them?

AJ: We focus on upcoming and next generation offensive and defensive security technology. The topics range from APT, Cyber operations, to exploitation of different technology and systems, cloud, telecom, hardware, web etc. We welcome anything new, interesting and that has a significant impact on security.

The attendees are a mix of researchers, executives, students and Govt. officials. We get a very good participation in terms of footfall from the Govt. sector in India. It is good to see that things are changing in the Govt. sector and officials are releasing the impact nullcon has in the overall development of information security awareness in the country. The awareness level in the corporate sector is also increase every year.

ED: Let's move on to the upcoming conference? How many speakers do you have?

AJ: Nullcon is not just a conference, it's an experience by itself where we celebrate the achievements of the security community with a lot of cutting edge learning.

There are a few new events in the pipeline such as pre-con night hack talks, hardware villages. Various events during the conference include

Talks

We have more than 20 speakers with some really amazing content.

Reboot Film

We are honoured to have Joe Kawasaki, Director of reboot film at the conference where we will be showing the movie along with a Q&A session with Joe.

Hacking Competitions

- HackIM starts in mid Jan 2013 *http://ctf.nullcon.net*
- Jailbreak will be held on 27-28th Feb 2013
- Battle Underground will be held during the conference 1-2nd March

P-A-R-T-Y

A break from the high tech learning in the day to give you a good dose of Goa.

- Speakers after dinner party – An informal welcoming of all the speakers.

- Nullcon nertworking party – An invitation only party for speakers, volunteers and the Corporate delegates on 1st March 2013.
- A visit to Saturday night bazaar – An open air flee market, bars, DJs, Live bands on 2nd March 2013.

Exhibition
Yes, we have a full-fledged exhibition for security companies to come and showcase their products and services.

Job Fair
As part of the Exhibition we also organize a Job fair booth and assist organizations look for skilled professionals. Attendees drop their resumes and we share it with the organizations participating in the conference. It is a very economical and easy way to find the best resources in security.

Workshops (1-2nd Mar 2013)

- GSM Exploitation by Aaron deMello
- Understanding Smart Malware by Shesh Sarangdhar
- Introduction to Peach fuzzing framework by Adam Cecchetti, Deja Vu Security
- Memory Forensic by Prince Boonlia

Training (27-28th Feb 2013)

- Penetration Testing SmartGrid & SCADA by Justin Searle
- The Art of Exploiting Injection Flaws by Sumit Siddharth
- Xtreme Android Hacking by Aseem Jakhar
- Reverse Engineering and Malware Analysis by Abhishek Datta
- Xtreme Exploitation by Omair
- Mobile Application Hacking – Attack & Defense by Hemil Shah
- Xtreme Web Hacking by Akash Mahajan & Riyaz Walikar
- Cyber Warfare Intelligence and Intrusion Operations by Atul Agarwal

If that's not all, the beach is right next to the venue so you can take a break anytime you feel like and stroll on the beach.

ED: Why did you choose Goa as the venue?

AJ: In India we have been to many conferences organized in IT hubs such as Bangalore, Delhi, Mumbai etc. The problem we see is that the delegates are not able to concentrate on the talks due to their office work and many delegates have to unwillingly depart to their office in the middle of the conference because of some or the other. We wanted a location where delegates will not bothered about going back to office and can also take time out from their busy schedule and concentrate on what they have come to nullcon for i.e. learn, network and relax. We found Goa as the ideal place to host nullcon. Goa is one of the famous International destinations which attracts a lot of tourists from all over the world and for international security professionals we add the conference twist to the place, so every year they can take vacation to Goa and enjoy both the place as well as the conference.

ED: How has the security scene in India changed over the years?

AJ: Drastically. I remember the time when there were no avenues to learn, meet and network with security professionals in India and the difficulties of finding good mentors, content etc. Year by year we see an increase the no. of paper submissions from local researchers with some really amazing research which is also admired world over, but was hard to find earlier. In the late 90s and early/mid 2000 there were closed groups and communities and the information exchange was limited to them. And then nullcon happened! It worked as a catalyst to the networking of the security community here. On a lighter note some people regard nullcon as the infosec hippie revolution (in a good way) because of the counter culture that it has brought in the information security and hacking scene.

ED: What is null – The open security community? Tell us something about it?

AJ: It all started back in 2008, we and a bunch of colleagues were discussing about active information sharing platforms in information security domain. India being the global hub of software development, it was a little surprising that there were no active and open infosec communities. This coupled with the problems we faced during our learning phase because of no one to talk to, mentor and guide us. We thought of starting a community with no boundaries i.e. anything security and hacking was welcome. The aim was to share knowledge and assist any organization with security related issues.

null was the primary inspiration to start the nullcon Security Conference.

We started the null mailing list in July-Aug 2008 and made our first public appearance at Bar-

Camp Pune in Nov 2008, where we announced that we are starting physical null community meet ups in Pune. There were a few hackers and security professionals whose needs were answered by null and they joined in as volunteers. There has been no looking back since then. It has not been easy but has been a very interesting journey. Null is now a registered non-profit society with over 2800+ members on the mailing list and more than 150 security professionals and hackers meet every month in different cities at the null meets.

We currently have six active null chapters throughout India in major cities – Pune, Bangalore, Mumbai, Delhi, Hyderabad and Chennai. Every chapter is run by 2-3 Moderators. The moderators decide the agenda of the monthly meets and make sure we have a suitable place for the meets. There are generally presentations by members and discussions on hot topics in security. The chapters run independently with all the information being collated on our community portal *http://null.co.in* It is amazing to see the kind of deep technical knowledge talks and information exchange happening at the null meets. The meets are free for everyone i.e. no registration and as we at say at null – just come with an open mind. People interested in opening local null chapters can directly contact us and we can assist them with the same.

ED: Do you work on any projects in null?

AJ: We have several projects running. All projects are run by null members who have volunteered and taken some time out of their busy schedule to manage those projects.

Software projects

There are various open source security software written and contributed by null members. The details can be found at – *http://null.co.in/section/atheneum/projects/.* Some of the noted projects include Game|Over – The web security learning platform, Jugaad – Linux remote thread injection kit, Wireplay – server communication fuzzing tool, Malware analyser and many more.

Project KeedAJ

A database of vulnerabilities found in the wild. Researchers who find it difficult to report and get the vulnerability fixed, report it to us and we take on the responsibility of reporting it to vendor and getting it fixed. There is no restriction on the type of vulnerability one can report i.e. even vulnerabilities in custom websites can be reported to Keeda. For more details you can visit *http://keeda.null.co.in.*

Null Jobs

A free portal for posting and applying for security jobs. We have been running the portal for more than a year now and have received hundreds of job postings and applications. Many people have found the right jobs through the portal. We have changed the way how security job openings were communicated in the past by way of having a centralized portal for most of the security jobs in India. We plan to take it international in sometime and assist the international community for the same. Details can be found at *http://jobs.nullcon.net*.

null HumlAJ

Humla literally means attack in hindi. An offensive hands-on informal workshop and gathering. This happens in most of the null chapters. It is a day long session on any offensive technology picked up by the volunteers. We have a Humla champion who runs the show. The session is totally free, however to maintain the quality we keep limited registrations.

ED: Any message for our readers?

AJ: I request you to come out of your office space and contribute to the community as much as you can. Believe me when I say that the best way to learn is to share and network with the community.

Take some time out of your busy schedule and come down for nullcon. We promise an experience never experienced :). We have special packages for international delegates.

And as they say for nullcon – Beware! Be There! Get ready to Goa!

ED: Thank you very much! Good luck!

GENEVA WORLD TRADE CENTER II T. +41 22 723 24 24 F. +41 22 788 35 71 info@htbridge.ch

SPTechCon
The SharePoint Technology Conference

March 3-6, 2013 → San Francisco

Get the scoop on SharePoint 2013!

Register Early and SAVE!

The Best SharePoint Training!

Choose from over 90 Classes & Workshops!

Check out these NEW! classes, taught by the industry's best experts!

- How to Install SharePoint 2013 Without Screwing It Up — Todd Klindt and Shane Young
- What IS SharePoint Development? — Mark Rackley
- SharePoint Performance: Best Practices from the Field — Jason Himmelstein
- Creating a Great User Experience in SharePoint — Marc Anderson
- Ten Best SharePoint Features You've Never Used — Christian Buckley
- Understanding and Implementing Governance for SharePoint 2010 — Bill English
- Building Apps for SharePoint 2013 — Andrew Connell
- SharePoint Solutions with SPServices — Marc Anderson
- Lists: Used, Abused and Underappreciated — Wes Preston
- Planning and Configuring Extranets in SharePoint 2010 — Geoff Varosky
- Creating Simple Dashboards Using Out-of-the-Box Web Parts — Jennifer Mason
- Integrating SharePoint 2010 and Visual Studio Lightswitch — Rob Windsor
- Solving Enterprise Search Challenges with SharePoint 2010 — Matthew McDermott
- Getting Stuff Done! Managing Tasks with SharePoint Designer Workflows — Chris Beckett
- SharePoint 2013 Upgrade Planning for the End User: What You Need to Know — Richard Harbridge
- Ten Non-SharePoint Technical Issues That Can Doom Your Implementation — Robert Bogue
- SharePoint MoneyBall: The Art of Winning the SharePoint Metrics Game — Susan Hanley
- Intro to Branding SharePoint 2010 in the Farm and Online — Randy Drisgill and John Ross
- How to Best Develop Requirements for SharePoint Projects — Dux Raymond Sy

Lots more online!

A BZ Media Event

Central Contractor Registration

Follow us: twitter.com/SPTechCon

www.sptechcon.com


[GEEKED AT BIRTH.]
[IT'S IN YOUR PULSE.]
LEARN:
Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering
Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies
University of Advancing Technology
UAT
Learn. Experience. Innovate.
You can talk the talk.
Can you walk the walk?
www.uat.edu > 877.UAT.GEEK
PLEASE SEE WWW.UAT.EDU/FASTFACTS FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.