Kang-Wei Chang
kwc305
N18515255
Lab1

1.
Nmap scan

(1) I use nmap -sV -O 10.10.111.0/24 in order to get the version of system -sV is for service Version dectection
(2)
host 10.10.111.120: tcp port 135,139,145,1025, 5000 are open. This host is running windows
localhost: port 111 is open
(3)

(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.

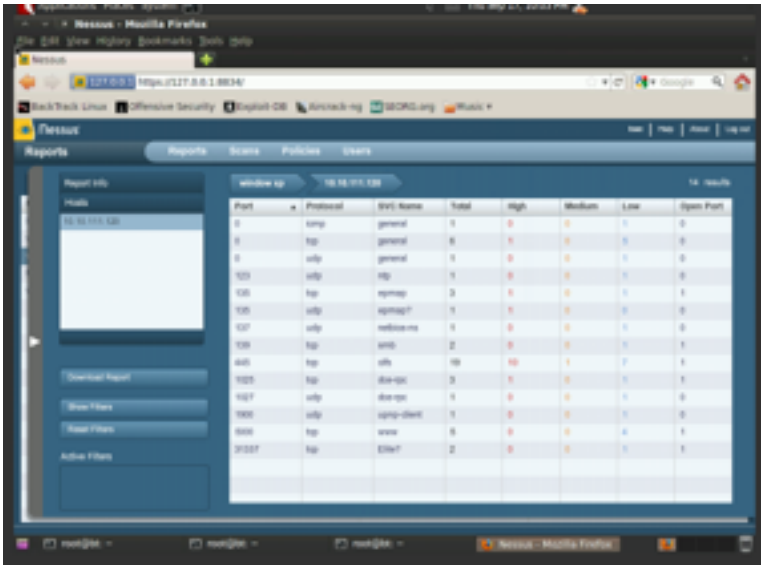
IP addresses and MAC addresses are reconnoitered, further information could be hijacked by MAC address spoofing or IP spoofing method.

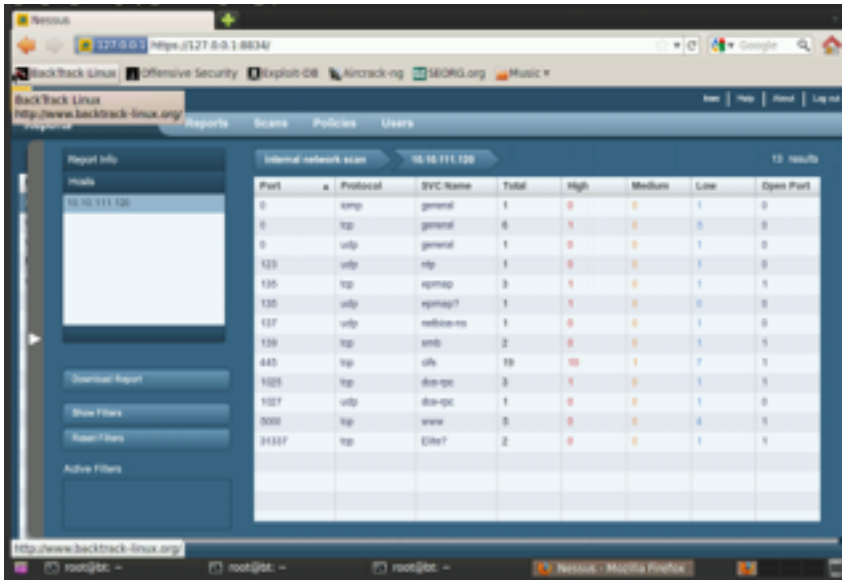
3.

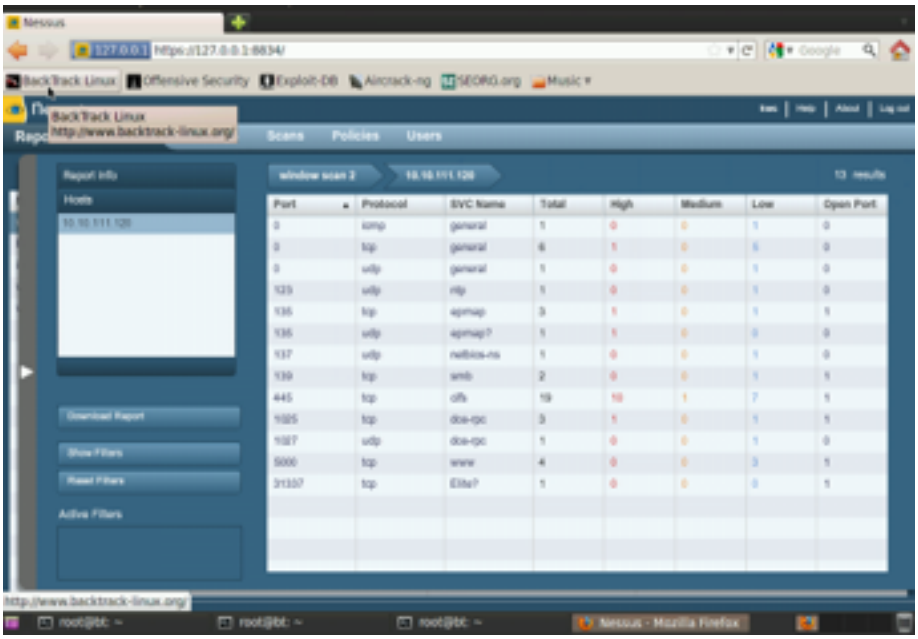
Since

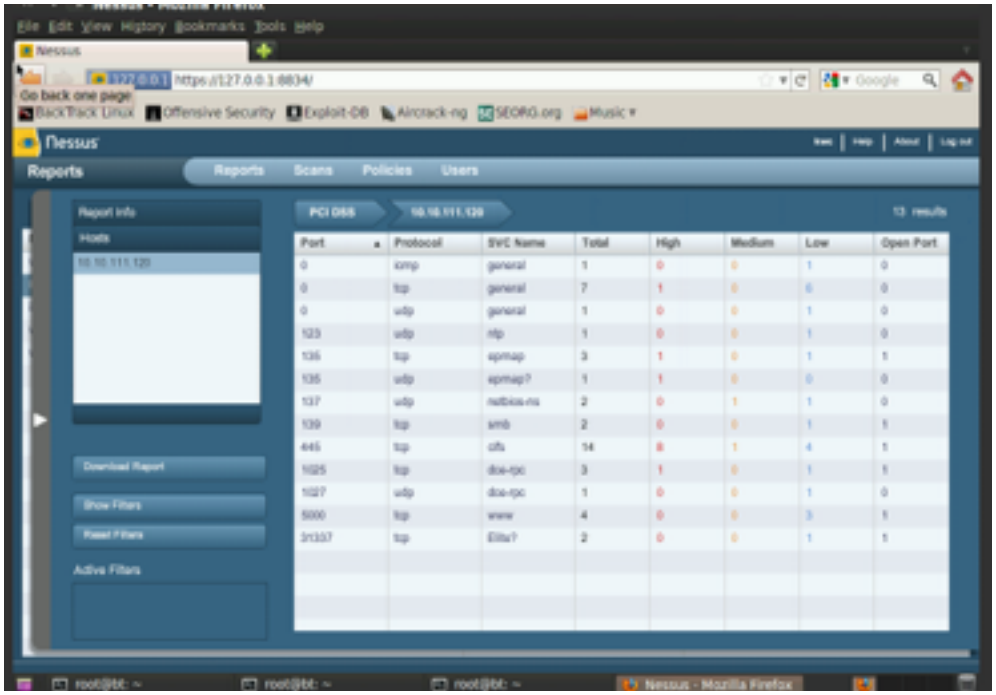
OS versions are detected, attacker could exploit the target with known vulnerabilities to focus on the loop hole

2.




Nessus
BackTrack Linux
http://www.backtrack-linux.org/
Reports
Scans
Policies
Users
Report Info
Hosts
Download Report
Show Filters
Reset Filters
Active Filters
Port
Protocol
SVC Name
Total
High
Medium
Low
Open Port
http://www.backtrack-linux.org/
root@bt: ~
root@bt: ~
root@bt: ~
Nessus - Mozilla Firefox


Nessus
BackTrack Linux
http://www.backtrack-linux.org/
Scans
Policies
Users
Report Info
Hosts
Download Report
Show Filters
Reset Filters
Active Filters
Port
Protocol
SVC Name
Total
High
Medium
Low
Open Port
http://www.backtrack-linux.org/
root@bt: ~
root@bt: ~
root@bt: ~
Nessus - Mozilla Firefox

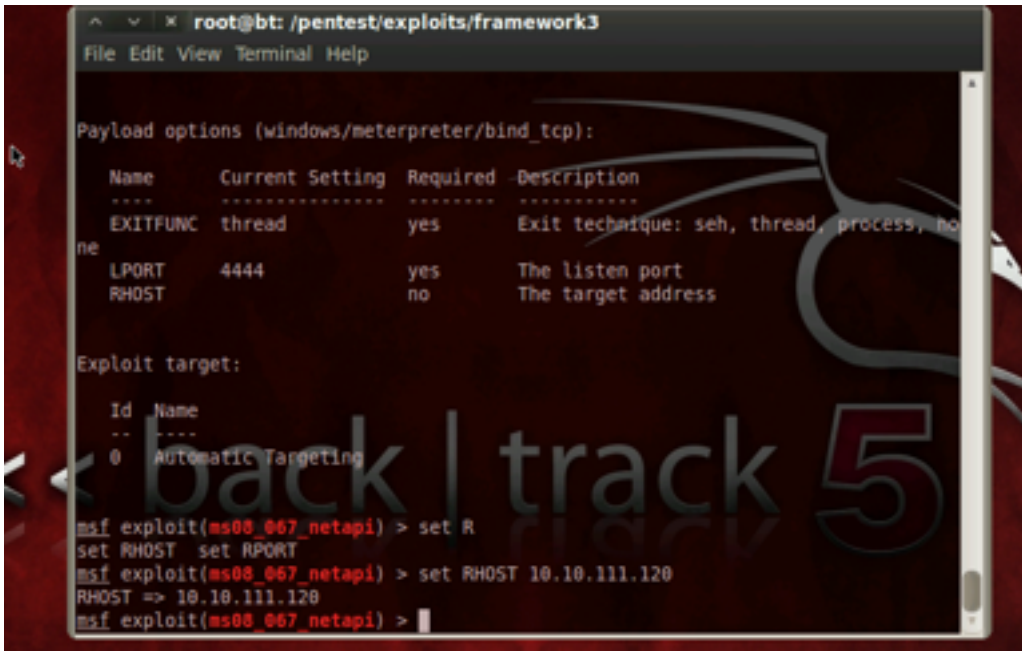

Nessus
Reports
Scans
Policies
Users
PCI DSS
10.10.111.120
13 results
Port
Protocol
SVC Name
Total
High
Medium
Low
Open Port


window xp
10.10.111.120
135 / tcp
List
Detail
2 results
Plugin ID
Name
Port
Severity
10736
DCE Services Enumeration
epmap (135/tcp)
Low
21655
MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncred
epmap (135/tcp)
High

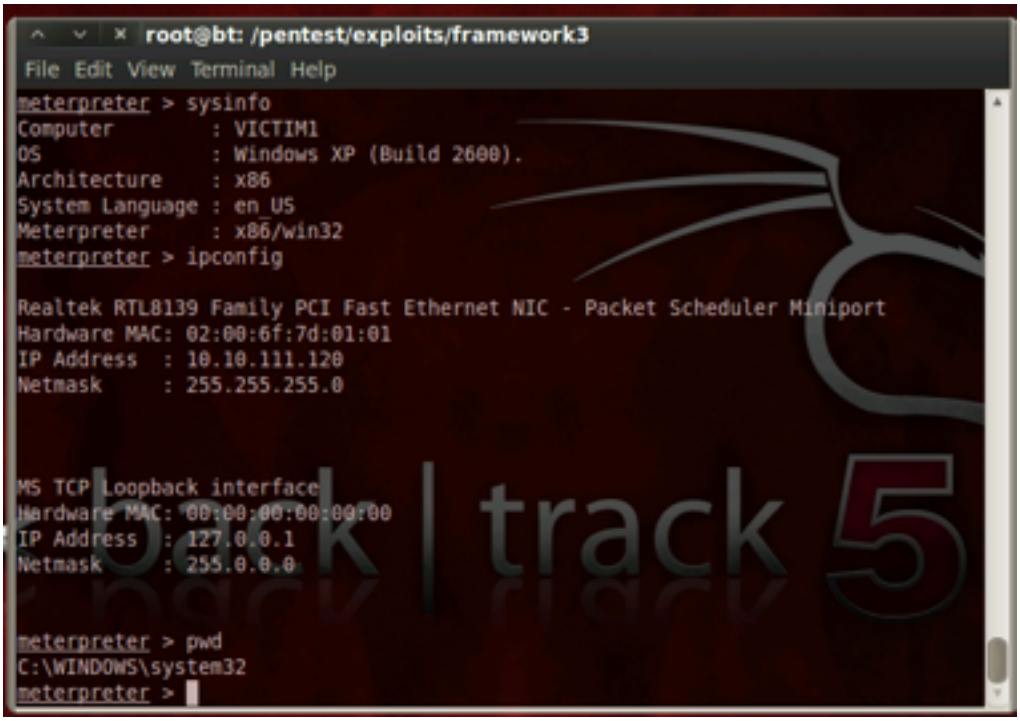
3. exploit with metasploit:

(1)
I use ms08_067_netapi and bind_tcp as payload

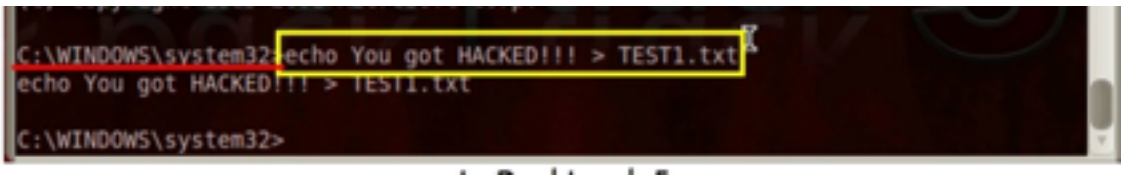
set remote host 10.10.111.120, which is windows machine

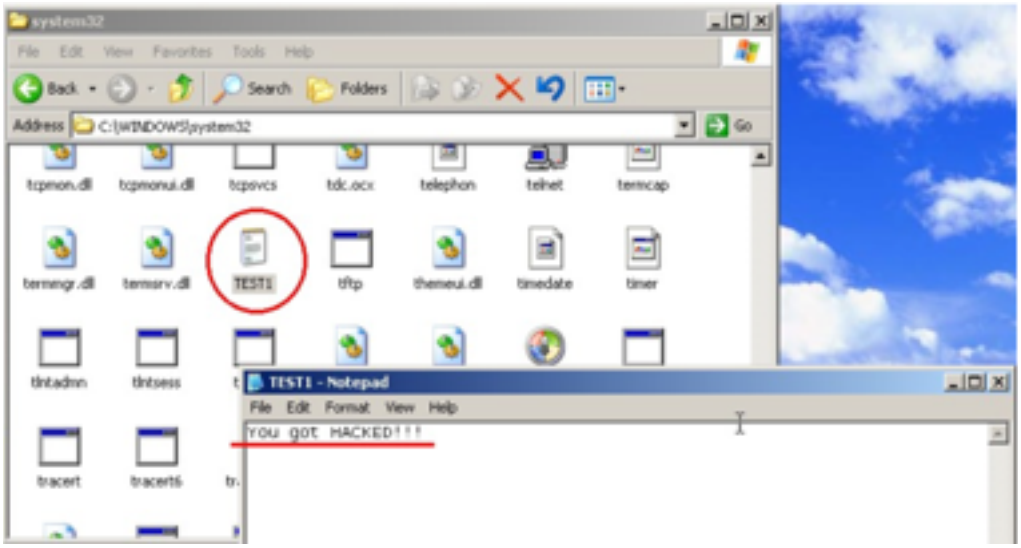


after enter the victim machine, I get the sys info and shell into window machine



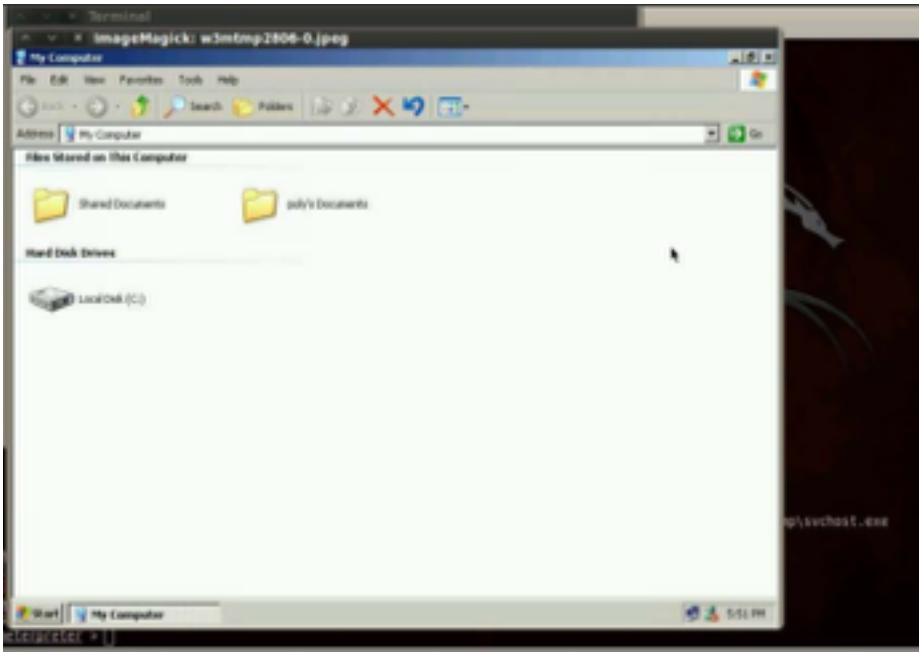
(2)




system32
File Edit View Favorites Tools Help
Back Search Folders
Address C:\WINDOWS\system32
Go
tcpmon.dll
tcpmonui.dll
tcpsvcs
tdc.ocx
telephon
telnet
termcap
termmgr.dll
termsrv.dll
TEST1
tftp
themeui.dll
timedate
tiner
tlntadmn
tlntsess
tracert
tracert6
TEST1 - Notepad
File Edit Format View Help
You got HACKED!!!

(3)


meterpreter > migrate 1660
[*] Migrating to 1660...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...success.
meterpreter > screengrab
Screenshot saved to: /root/hNVwHAZV.jpeg
meterpreter >


ImageMagick: w3mtmp2806-0.jpeg
My Computer
Shared Documents
Hard Disk Drives

(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.