Practical 4

Tuesday, 16 August 2022 5:28 PM

ISEC3002 Penetration Testing and Defence
Workshop 4
Metasploit Framework & Proxychains

The purpose of this workshop is to practice using Metasploit Framework, Armitage, and Proxychains.

Part 1: To complete this set of exercises you will need to have Armitage installed on your Kali VM. The installation process is simple – all it needs is to start the installation process:

apt-get install armitage

Metasploit Framework

Exercise 1.

Scan the machines in the cyber range with the command line version of Metasploit - msfconsole. Compare your results with those you obtained in previous workshops. Which machine in the cyber range has two network cards (specify the name and IP addresses)?

https://www.offensive-security.com/metasploit-unleashed/port-scanning/
First I got the hosts up in the 192.168.2.0/24 subnet using:
nmap -T5 -sP -oG - 192.168.2.0-255 | grep Up | awk -F " " '{print $2}' > hostsUp.txt
on msfconsole I used auxiliary(scanner/portscan/syn) with options RHOSTS as file:hostUp.txt and PORTS as 1-65535
To detect which host has two network cards, use auxiliary(scanner/smb/smb_version) with options RHOSTS as file:hostsUp.txt, then run the hosts to see which hosts have two entries in the database.

How many machines in the cyber range provide FTP services? Name at least four systems offering FTP and name at least two machine offering anonymous FTP access.

Used auxiliary(scanner/portscan/tcp) setting the port as 21 for FTP.
3 are, 192.168.2.4, .12 and .20 are running a service on port 21.
Used auxiliary(scanner/ftp/anonymous) and 192.168.2.4, .12 and .20 allow anonymous FTP read / access

How many machines are offering NFS file shares? Specify at least three systems offering NFS shares. Does the machine with network cards offer such a share? What auxiliary or tool did you use to find and list the NFS shares?

Using either auxiliary(scanner/portscan/tcp) (setting ports as 111) and auxiliary(scanner/nfs/nfsmount) there's 1 machine offering NFS file shares which is 192.168.2.20.

Armitage

Exercise 2.

Repeat the exercises from the previous section but this time use the Metasploit GUI – Armitage.

Part 2: To complete this set of exercises you will need to have Proxychains installed on your Kali VM.

Proxychains

Use the Proxychains tool to conduct basic reconnaissance of another subnet. The machine with two network cards has multiple accounts – one of them is quintus which is of particular interest as it has a very poor password: *password1*.

Exercise 3.

(Hint: nbtscan, netdiscover, Lateral Movement, SSH Pivoting, Port Forwarding, nmap) Proxychains and tor

Go to google and search for: "What is my IP"
https://www.whatismyip.com/
Check and write down your IP address?
Install Proxychains in Kali Linux if necessary
Modify the Proxychains configuration file to enable options by deleting the # in the front of them or adding lines if necessary
sudo gedit /etc/proxychains4.conf
enable *dynamic_chain*
comment *strict_chain*
add these lines at the end:
socks4 127.0.0.1 9050
socks5 127.0.0.1 9050
Install *tor* in Kali Linux
sudo service tor start
sudo service tor status
netstat -ano | grep LISTEN | grep 9050
proxychains4 firefox duckduckgo.com
Go to: https://www.dnsleaktest.com/
Check your IP address?
proxychains4 nmap -sT -PN -n -sV -p 80 scanme.nmap.org

What other subnet/s apart from 192.168.2.0/24 is/are reachable?
How many live hosts are present in the other subnet/s? What are the operating systems of the live hosts?
What are the open ports on the live hosts in the other subnet/s?
Use Proxychains, Port Forwarding and the following machines information to do the lateral movement:

There is a machine that has two NICs with IP addresses of 192.168.2.150 and 192.168.10.10. There is a user called 'quintus' with a password: password1
There is another machine with IP addresses of 192.168.10.30. There is a user called ' Administrator' with a password: Centurion2021Pretorian
There is another machine with IP addresses of 192.168.10.4. There is a user called ' Vinicius' with a password: password1

Reference

https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
https://www.offensive-security.com/metasploit-unleashed/
https://docs.rapid7.com/metasploit/credentials-tutorial
https://stationx-public-download.s3.us-west-2.amazonaws.com/Metasploit-cheat-sheet.pdf
https://www.youtube.com/watch?v=QynUOJanNqo
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt2666925c05bfae0c/5e34a63e07e2907e353a2f5b/metasploit-cheat-sheet-2.pdf