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:

ii) apt-get install armitage

Metasploit Framework

Exercise 1.

i) 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)?

ii) 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.

iii) 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?

Armitage

Exercise 2.

i) 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)

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

ii) What other subnet/s apart from 192.168.2.0/24 is/are reachable?
iii) How many live hosts are present in the other subnet/s? What are the operating systems of the live hosts?
iv) What are the open ports on the live hosts in the other subnet/s?
v) Use Proxychains, Port Forwarding and the following machines information to do the lateral movement:
   a. 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
   b. There is another machine with IP addresses of 192.168.10.30. There is a user called ' Administrator' with a password: Centurion2021Pretorian
   c. 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