Study Guide

Scanning, Enumeration, and Vulnerabilities

Created By: Samia Oukemeni, Teaching Assistant

Module 1: Introduction

Lesson 1.1: Introduction to the course

- Some background in Kali Linux is necessary.
- Basic understanding of computer networking.
- Basic understanding of operating systems (windows server and windows 10).

Module 2: Check for live systems and ports

Lesson 2.1: Checking for Live Systems Lab Part 1

Skills Learned From This Lesson: *Nmap, ifconfig, Live systems*

- ifconfig command displays network interface configuration used in Unix-like operating systems.
- Nmap is a network scanner to discover hosts and services running on a network.
- The command nmap -h gives details about nmap and the option to use.
- Nmap -sn command is a ping scan used to send ping requests.
- Loopback address is an address that sends signals to the same computer for testing.

Lesson 2.2: Checking for Live Systems Lab Part 2

Skills Learned From This Lesson: *Nmap, Hping3, Live systems*

- nmap -sn 192.168.0.1/24 scans the whole range of IP addresses.
- nmap -Pn command is to skip host discovery and port scan all target hosts.
- hping3 is a free packet generator and analyzer for the TCP/IP protocol.
- *hping3 -h i*s used to see the help summary page.
- *hping3 -1* is used for ping scans.
- If studying for CEH from EC-Council, you need to know commands used like nmap and hping3 and understand the different flags used.
- If studying for CompTIA PenTest+, you need to understand the output and what commands are used.

Lesson 2.3: Checking for Open Ports Lab Part 1
Skills Learned From This Lesson: *Nmap, Port Discovery, scanning*

- Nmap is essential for CompTIA PenTest+ and CEH from EC-Council.
- Nmap 192.168.0.1 identifies all the ports that are open on the machine and it shows the services running in each particular port.

Lesson 2.4: Checking for Open Ports Lab Part 2
Skills Learned From This Lesson: *Nmap, Hping3, Port Discovery*

- hping3 -8 0-5000 -S command is used to:
  - **-8:** to enable the scan mode
  - **0-5000**: to set the range of ports
  - **-S** to set the SYN flag
- hping3 -8 0-5000 -S command shows the port responding with their respective services as well as the port not responding.

Module 3: Scanning

Lesson 3.1: Scanning Part 1
Skills Learned From This Lesson: ipconfig, Command prompt, cmd

- *ipconfig* command displays network interface configuration used in Windows operating systems.
- To launch the command on windows: either click on Command prompt(Admin, click on Run and type cmd.exe, or open File Explorer, and then navigate to the C:\Windows\System32 folder. Double-click the “cmd.exe”.

Lesson 3.2: Scanning Part 2
Skills Learned From This Lesson: *SYN scanning, Nmap, Half-connect scanning*

- *nmap -sS* is used for scanning TCP SYN port.
- nmap -sS is called as well half-open scan or half-connect scan.
- When nmap -sS is used without specifying any range of port, it performs a SYN scan on 1,000 well-known TCP ports on the target.
- nmap -sS shows all the open ports on the target and the services running on these ports.

Lesson 3.3: Scanning Part 3
Skills Learned From This Lesson: *Nmap, Full-connect scanning, TCP handshake*

- to run a full-connect scan, we use nmap -sT.
- -sT: to establish the full TCP handshake.
- The results from -sT are similar to results from -sS.
- It shows all the open ports and their corresponding services.

Lesson 3.4: Scanning Part 4
Skills Learned From This Lesson: *Nmap, Zenmap, Installation*

- Zenmap is the GUI version of nmap.

Lesson 3.5: Scanning Part 5
Skills Learned From This Lesson: *Nmap scanning, Zenmap, Xmas scan*

- An adversary uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header.
- Xmas scan (-sX) sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
- XMAS scans work against Linux-based machines, not Windows.
- sX –reason gives a reason to why a port is open or closed.

Lesson 3.6: Scanning Part 6
Skills Learned From This Lesson: *Nmap, ACK, scanning*

- TCP three-way handshake: Host A sends a TCP SYN packet to Host B, B sends a SYN-ACK and then A sends ACK.
- ACK scan is not used for determining the state of a port (open or closed).
- ACK scan is used to map out firewall rulesets, determining whether they are stateful or stateless.
- nmap -sA - p command:
    - **-sA:** to enable the ACK scan mode
    - **-p**: to set the port
- Port 80 is unfiltered.

Lesson 3.7: Scanning Part 7
Skills Learned From This Lesson: *Nmap, ACK scan, Windows Firewall*

- When blocking all incoming connections on windows firewall and run again **nmap -sA -p,** port 80 now is filtered.

Lesson 3.8: Scanning Part 8
Skills Learned From This Lesson: *Hping3, TCP SYN, Scanning*

- hping3 -8 0-5000 -S command is used to:
    - **-8:** to enable the scan mode
    - **0-5000**: to set the range of ports
    - **-S** to set the SYN flag

Lesson 3.9: Scanning Part 9
Skills Learned From This Lesson: *Hping3, ACK, Scanning*

- hping3 -c x -V -p xxxxx -s xxxx -A command is used to:
    - **-c:** packet count
    - **-V**: Verbose
    - **-p:** to specify the port number
    - **-s** to specify from where the packets are sent
    - **-A** to set the ACK flag
- 0% packet loss.

Lesson 3.10: Scanning Part 10
Skills Learned From This Lesson: *Hping3, Xmas, Scanning*

- hping3 -c x -V -p xxxx -s xxxx -M x -UPF command is used to:
    - **-c**: packet count
    - -**V:** Verbose
    - **-p** to specify the port number
    - **-s** to set TCP sequence number
    - **-UPC** to set the URG, Push, and FIN flags
- After running hping3 -8 80 -V -S 192.168.0, we got a response from port 80, it means that it is open.

Lesson 3.11: Scanning Part 11
Skills Learned From This Lesson: *Hping3, ACK scan, Windows Firewall*

- When changing the option of windows firewall to "Block all incoming connections" and running hping3 -c x -V -p xxxxx -s xxxx -A, all the packets sent are lost.

- This scan helps to know if there is a firewall is in the way.

Module 4: Fingerprinting and Banner Grabbing

Lesson 4.1: OS Fingerprinting Lab

Skills Learned From This Lesson: *Nmap scan, Operating System detection, Fingerprinting*

- nmap -sS -O command is used to:
  - **-sS**: for TCP SYN scanning
  - **-O**: to enable operating system detection

Lesson 4.2: Banner Grabbing Lab

Skills Learned From This Lesson: *Nmap scan, Operating System detection, banner grabbing*

- nmap -sS -p xxxx -A command is used to:
  - **-sS**: for TCP SYN scanning
  - **-p**: to set the port number
  - **-A**: aggressive mode
- To determine what OS is in use.
- It gives also the services that are running on open ports.

Module 5: Enumeration Tools

Lesson 5.1: Zenmap

Skills Learned From This Lesson: *Nmap scan, Zenmap, Enumeration*

- nmap -T4 -A -v
  - **-T4**: to speed scans up by by assuming that you are on a reasonably fast and reliable network.
  - **-A**: aggressive mode to detect OS and Services
  - **-v**: verbose to get as much information as possible
- Help to get the OS running on the target machine.
- Detect the open port and their corresponding services.

Lesson 5.2: Dig and Finger Commands

Skills Learned From This Lesson: *Enumeration, Dig command, Finger command*

- Dig is a tool/ command used for querying Domain Name System (DNS) name servers.
- dig axfr practise-labs.com:
  - **axfr:** to provide a complete listing of domain records**.**

- The lab wasn't successful because the server practise-labs.com is not vulnerable to DNS Zone Transfers.
- Dig stands for Domain Information Groper.
- Finger command is used to lookup users on a remote system.
- finger -s root:
    - displays information about all the users available on the system including beside root

Module 6: Vulnerabilities

Lesson 6.1: Vulnerability Scanner Setup and Configuration Lab 1 Part 1
Skills Learned From This Lesson: vulnerabilities scanning, penetration testing, CORE Impact

- CORE Impact Professional is a penetration testing tool.
- Network scan types:
    - Fast: gather just enough information about the hosts to be able to launch attacks
    - Detailed: gather additional detailed information about the host and use additional techniques to validate the information learned about the target hosts.
    - Custom: you may choose the options you want for the scan. It is recommended for advanced users.

Lesson 6.2: Vulnerability Scanner Setup and Configuration Lab 1 Part 2
Skills Learned From This Lesson: vulnerabilities scanning, penetration testing, CORE Impact

- Detailed scan gives more in-depth information about each items scanned.

Lesson 6.3: Vulnerability Scanner Setup and Configuration Lab 2 Part 1
Skills Learned From This Lesson: vulnerabilities scanning, penetration testing, OpenVAS

- nano Scanning_Target_List is used to create the file " Scanning_Target_List".
- the Ctrl button + press x is to exit the file created.
- sudo openvas-start is used to open OpenVas under the user student and not root.
- to make sure that OpenVas is functional, it directs to a firefox page: Greenbone Security Assistant login page.

Lesson 6.4: Vulnerability Scanner Setup and Configuration Lab 2 Part 2
Skills Learned From This Lesson: vulnerabilities scanning, penetration testing, OpenVAS

- The report lists
    - the vulnerabilities found on the target hosts.
    - Severity

    - Host IP address
    - Port
- By clicking on a vulnerability, the report provides more information:
    - Summary
    - Impact
    - CVE code (if any)
    - Solution
    - Affected OS/Software
    - Insights
- The report can be generated as PDF.

Module 7: Conclusion

Lesson 7.1: Vulnerability Scan

Skills Learned From This Lesson: vulnerability, scanning

- Assessment of the course: Vulnerability Scan on Cybrary.

Lesson 7.2: Conclusion

Skills Learned From This Lesson: vulnerability, scanning

- Different types of scans: Xmas scan, SYN scan, ACK scan.
- OS fingerprinting and detection.
- OpenVAS is free while Nessus is paid version.