MODULE 03 FOOTPRINTIG AND RECONNAISSANCE LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/7172f790-9cdf-4d52-8e5b-9f70b624bba3?rc=10

2. https://labclient.labondemand.com/LabClient/c7ae60a5-feb4-47a5-8dc2-7a96eb51daaa?rc=10

3. https://labclient.labondemand.com/LabClient/430c9120-4145-4a3c-b369-fe2bc00c6eb3?rc=10

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01 - Task 01

For this task, I used a tool called Nmap to find active computers on a network. Nmap helps with network management and security checks.

Here's what I did:

1. Logged into the Parrot Security machine.

2. Opened the Terminal.

3. Ran commands with Nmap to find active computers:

    - First, I used a method called ARP ping scan.
    - Then, I tried a UDP ping scan.
    - After that, I used an ICMP ECHO ping scan.
    - Next, I did an ICMP ECHO ping sweep to check a range of IP addresses.
    - Lastly, I tried an ICMP timestamp ping scan.

Each time, Nmap showed if the target computer was active.

I also learned about other ways to find active computers using Nmap, like ICMP Address Mask Ping Scan, TCP SYN Ping Scan, TCP ACK Ping Scan, and IP Protocol Ping Scan.

Lab 01 -task2

In this task, I utilized Angry IP Scanner, a network scanner tool, to identify active hosts within the target network. Angry IP Scanner is an open-source tool capable of scanning IP addresses and ports to determine their availability.

Here's a breakdown of the steps I followed:

Accessing Angry IP Scanner:

Selected the Windows 11 machine.
Located Angry IP Scanner by searching for it on the Desktop using the Search icon.
Launched Angry IP Scanner.
Configuring Angry IP Scanner:

Clicked through the initial setup wizard and closed it.
Handled any security warnings to run the application.
Setting IP Range and Preferences:

Specified the IP range as 10.10.1.0 to 10.10.1.255.
Accessed Preferences and configured scanning options:
Selected Combined UDP+TCP as the Pinging method.
Chose to display only alive hosts responding to pings.
Initiating the Scan:

Started the scan using the specified IP range.
Monitored the progress through the scanning process.
Reviewing Scan Results:

Noted the total number of alive hosts found (in this case, 7).
Closed the Scan Statistics pop-up.
Observed the scan results displaying active IP addresses along with their hostnames.
Concluding the Task:

Completed the demonstration of discovering active hosts using Angry IP Scanner.
Noted other available ping sweep tools for future reference.
Through this process, I successfully identified active hosts within the specified IP range using Angry IP Scanner, contributing to network assessment and management efforts.

Lab 02 - Task 01: Perform Port and Service Discovery using MegaPing

In Task 01, I explored the functionality of MegaPing, a comprehensive toolkit designed for Information System specialists, system administrators, and IT solution providers. MegaPing offers a range of utilities for detecting live hosts, open ports, and active services within a network environment.

Here's what I learned from this task:

Understanding MegaPing's Capabilities:

MegaPing provides a suite of utilities including IP scanner, port scanner, DNS lookup, Finger, host monitor, NetBIOS scanner, ping, share scanner, traceroute, and Whois.
It enables users to detect live hosts, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, and more.
Installation and Setup:

I learned how to install MegaPing by navigating to the designated directory and executing the setup file.
The installation process involved following the InstallShield Wizard-driven steps and launching the program upon completion.
Navigating MegaPing GUI:

Upon launching MegaPing, I encountered the GUI displaying system information and proceeded to explore its functionalities.
Utilizing IP Scanner and Port Scanner:

With MegaPing's IP Scanner, I defined the IP range for scanning and initiated the scan to identify live hosts within the specified range.
I also utilized the Port Scanner feature to scan open ports and services on the target machine, obtaining detailed information about port numbers, service descriptions, and associated risks.
Understanding Security Implications:

The task highlighted the importance of understanding the security implications of open ports and services.
By identifying potential vulnerabilities, attackers can exploit them to compromise the target network and launch malicious attacks.
Through this task, I gained practical experience in using MegaPing to perform port and service discovery, enhancing my knowledge of network scanning techniques and security assessment practices.

Lab 02 - Task 02: Perform Port and Service Discovery using NetScanTools Pro

In Task 02, I got hands-on experience with NetScanTools Pro, a toolkit designed for network professionals to gather information and troubleshoot networks effectively. NetScanTools Pro offers various utilities to research IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs within a network.

Here's what I learned from this task:

Installation and Setup:

I navigated to the directory and launched the setup file (nstp11demo.exe) for NetScanTools Pro.
Following the installation wizard, I ensured that the NetScanTools Pro Demo was launched after installation.
Exploring NetScanTools Pro Interface:

After launching NetScanTools Pro, I explored its main window interface, which provides access to different network troubleshooting tools.
Using Ping Scanner:

I used the Ping Scanner tool to scan within a specific IP address range (10.10.1.5 - 10.10.1.23) to find active machines in the network.
The Ping Scanner provided a list of active machines, which helped me understand the network better.
Performing Port Scanner:

With the Port Scanner tool, I entered the IP address of the target machine (10.10.1.22) to scan for open ports and services.
The Port Scanner gave detailed information about open ports and their associated services, which was useful for assessing network vulnerabilities.
Understanding Security Implications:

Through the scans conducted with NetScanTools Pro, I learned about potential vulnerabilities within the network.
Identifying open ports and services helped me make informed decisions about strengthening network security.
By using NetScanTools Pro, I gained practical skills in port and service discovery, which are essential for network troubleshooting and security assessment.

Lab 02 - Task 03: Perform Port Scanning using sx Tool

Task 03 introduced the sx tool, a command-line network scanner capable of conducting various types of scans such as ARP scans, ICMP scans, TCP SYN scans, UDP scans, and application scans like SOCS5 scans, Docker scans, and Elasticsearch scans.

Here's what I learned from this task:

Understanding sx Tool Functionality:

The sx tool offers a range of scanning options including ARP scans, TCP scans, and UDP scans to discover open ports and associated services on target machines.
It provides flexibility in conducting network reconnaissance and security assessments.
Performing ARP Scans:

I utilized sx to perform ARP scans on the target subnet (10.10.1.0/24) to identify IP addresses and MAC addresses associated with connected devices in the local network.
The ARP scan provided essential information for further network analysis and mapping.
Generating ARP Cache File:

With the sx tool, I created an ARP cache file using the --json option to convert the output to JSON format.
The arp.cache file served as input for subsequent scans, enhancing efficiency and reducing redundant scanning efforts.
Conducting TCP Scans:

Using the TCP scan feature of sx, I listed all open TCP ports on the target machine (10.10.1.11) within the specified port range (1-65535).
This scan helped in identifying potential entry points and vulnerabilities in the target system.
Exploring UDP Scans:

I performed UDP scans on the target machine to check the status of specific ports, such as port 53 and port 500.
The UDP scan results provided insights into port availability and potential security risks associated with open ports.
Through this task, I gained practical experience in using the sx tool for port scanning and network reconnaissance, which are crucial aspects of network security assessment and penetration testing.

This concludes Task 03 of Lab 01, where I demonstrated port scanning using the sx tool and documented the acquired information for further analysis and network security enhancement.

Lab 02 - Task 04: Explore Various Network Scanning Techniques using Nmap

Task 04 introduced Nmap, a powerful network scanning tool equipped with various inbuilt scripts and scanning mechanisms. Nmap facilitates the discovery of open ports and services running on target hosts by sending crafted packets and analyzing responses.

Here's what I learned from this task:

Nmap offers a plethora of scanning options including TCP, UDP, and advanced scanning techniques like OS detection, version detection, ping sweeps, etc.
It employs diverse scanning mechanisms to gather comprehensive information about target networks and hosts.
Performing TCP Connect Scan with Nmap:

I used Zenmap, the GUI frontend for Nmap, to conduct a TCP connect scan (-sT) on the target IP address (10.10.1.22).
The scan results provided details about all open TCP ports and associated services on the target machine.
Exploring Stealth Scan Techniques:

I explored stealth scan techniques including TCP half-open scan (-sS) and Xmas scan (-sX) to evade detection and gather information about open ports and firewall configurations.
These scans utilize specific flag combinations to elicit responses from target systems while minimizing the footprint of the scanning activity.
Investigating Advanced Scanning Techniques:

I conducted advanced scans such as TCP Maimon scan (-sM) and ACK flag probe scan (-sA) to detect filtered ports and infer firewall presence on the target machine.
These scans provided insights into the network's security posture and potential vulnerabilities.
Performing UDP Scan:

I performed a UDP scan (-sU) to identify open UDP ports and services running on the target machine.
The UDP scan revealed information about services that operate over UDP and potential attack vectors.
Creating Custom Scan Profiles with Zenmap:

I learned to create custom scan profiles using Zenmap's Profile Editor, enabling tailored scanning configurations for specific scenarios.
Custom profiles allow for efficient and targeted scanning operations based on the desired scanning parameters.
Utilizing Aggressive Scan Options:

I explored aggressive scan options (-A) to perform comprehensive scanning including OS detection, version scanning, script scanning, and traceroute.
Aggressive scans provide detailed insights into target hosts and networks, aiding in vulnerability assessment and penetration testing.

Through this task, I gained practical experience in utilizing Nmap for network reconnaissance and security assessment purposes. I learned to leverage a variety of scanning techniques and interpret scan results to identify potential security risks and weaknesses in target environments.

This concludes Task 04 , where I explored various network scanning techniques using Nmap and documented acquired information for further analysis and network security enhancement.

Lab 02 - Task 05: Explore Various Network Scanning Techniques using Hping3

Task 05 introduced Hping3, a command-line network scanning and packet crafting tool for the TCP/IP protocol. Hping3 enables users to study target behavior, identify services, and explore open ports using TCP, UDP, ICMP, and raw-IP protocols.

Here's what I learned from this task:

Understanding Hping3 Functionality:

Hping3 is a versatile tool for network scanning and packet manipulation, offering capabilities to send ICMP echo requests and support for TCP, UDP, and other protocols.
It enables users to gather information about target hosts, including the services they offer, open ports, and even the target's operating system.
Executing TCP ACK Scan with Hping3:

I used Hping3 to perform an ACK scan (-A) on port 80 of the target machine (Windows Server 2022, 10.10.1.22).
The scan revealed that the port is open based on an equal number of packets sent and received, indicating a lack of response and hence an open port.
Conducting SYN Scan with Hping3:

I executed a SYN scan (-8) on ports 0-100 of the target machine, revealing open ports and associated services.
The SYN scan efficiently interacts with target hosts, utilizing SYN, ACK, and RST flags to gather information about open ports and services.
Performing FIN, PUSH, and URG Scans:

I utilized Hping3 to conduct FIN, PUSH, and URG scans on port 80 of the target machine, identifying open ports based on response patterns.
These scans exploit specific flag combinations to elicit responses from target hosts, aiding in the detection of open ports and potential vulnerabilities.
Executing TCP Stealth Scan with Hping3:

I performed a TCP stealth scan (--scan 0-100 -S) to identify open ports and services running on the target IP address.
The stealth scan discreetly interacts with target hosts, leveraging SYN packets to probe for open ports without triggering intrusion detection systems.
Conducting ICMP Ping Scan:

I executed an ICMP ping scan (-1) on port 80 of the target machine to determine its availability and responsiveness.
The ICMP scan confirmed the target's presence by sending echo requests and receiving ICMP replies, indicating an active host.
Exploring Additional Scanning Techniques with Hping3:

I learned about additional scanning techniques such as subnet scans for live hosts and UDP scans, extending the scope of network reconnaissance and service discovery.
Through this task, I gained hands-on experience in using Hping3 for network scanning and exploration. I learned to leverage its capabilities to uncover open ports, identify services, and assess target network security.

From Task 1 of Lab 3, i learned:

Purpose of OS Discovery:

i understood the significance of performing OS discovery as part of ethical hacking and penetration testing processes.
OS discovery helps in identifying potential vulnerabilities and selecting appropriate exploits for target systems.
Banner Grabbing Techniques:

i learned about banner grabbing techniques, which involve actively or passively gathering information about the target system's operating system and services.
Active Banner Grabbing with Wireshark:

You gained hands-on experience in actively identifying the target system's OS using Wireshark, a network protocol analyzer.
This involved capturing network packets between the target system and another machine and analyzing key packet fields.
Understanding TTL and TCP Window Size:

You learned about the significance of Time-to-Live (TTL) and TCP Window Size fields in IPv4 packets.
TTL values provide insights into the operating system of the target system, with different OSes having distinct default TTL values.

You understood that TTL values decay as packets traverse network hops, enabling inference about the distance and type of the target system.
Interpreting Packet Capture Results:

You practiced interpreting packet capture results in Wireshark, focusing on ICMP reply packets from the target system.
By analyzing TTL values, you made informed guesses about the target system's OS, such as Windows or Linux.
Documenting Findings:

i learned the importance of accurately documenting findings during network analysis and OS discovery. This involved recording TTL values, OS assumptions, and other relevant information for future reference and reporting.

Lab 3 - Task 2: OS Discovery with Nmap Script Engine (NSE)

Nmap, with its NSE, becomes a powerful tool for extracting valuable information from target systems. NSE offers scripts that unveil various details like OS, computer name, domain, and more. Leveraging NSE, you can gather extensive insights into the target system.

Let's walk through the process of OS discovery using Nmap and NSE:

Accessing Parrot Security Machine:

Access the Parrot Security machine by selecting it.
Logging In:

Log in using the default attacker username and password "toor".
Opening Terminal:

Launch the Terminal window by clicking the MATE Terminal icon.
Switching to Root:

Gain root access by typing "sudo su" and entering the password "toor".
Performing Aggressive Scan:

Execute the command "nmap -A [Target IP Address]" to conduct an aggressive scan.
The aggressive scan provides comprehensive details about open ports, services, and target system characteristics.
It might take around 10 minutes to complete.
Reviewing Scan Results:

Examine the scan results showcasing open ports, running services, and OS-related details under the Host script results section.
Performing OS Discovery:

Initiate OS discovery with the command "nmap -O [Target IP Address]".
This scan reveals the OS running on the target system along with other pertinent information.
Executing Customized Script:

Run the command "nmap --script smb-os-discovery.nse [Target IP Address]" to execute a customized script.
The script attempts to ascertain OS, computer name, domain, workgroup, and current time over the SMB protocol.
Analyzing Scan Results:

Analyze the scan results to uncover details like the target OS, computer name, NetBIOS computer name, etc., presented under the Host script results section.

Lab 3- Task 3: OS Discovery with Unicornscan

Unicornscan, a Linux-based tool, aids in network reconnaissance by scanning TCP and UDP ports. It reveals open ports, services, and TTL values, which hint at the target's operating system.

Steps:

Access Parrot Security.
Gain root access in Terminal.
Navigate to the root directory.
Scan Windows Server 2022
Review TTL value (128) indicating a Windows OS.
Scan Ubuntu
Review TTL value (64) suggesting a Linux-based OS.
Conclude the OS discovery session.
Document findings for analysis.

Lab4 - Task 1: Scan Beyond IDS/Firewall with Nmap

Access Windows 11 and enable Windows Defender Firewall.
Launch Wireshark to capture packets.
Switch to Parrot Security and open Terminal.
Gain root access and navigate to the root directory.
Observe captured packets in Wireshark.

Analyze results to evade IDS/firewall effectively.
Nmap offers robust features to scan beyond IDS/firewall using evasion techniques. Document findings for further analysis.

Lab4 - Task 2: Create Custom Packets using Colasoft Packet Builder to Scan Beyond IDS/Firewall

Use Colasoft Packet Builder to craft custom TCP packets for scanning beyond IDS/firewall.
Procedure:
Access the Windows Server 2019 machine.
Log in with the Administrator user profile and password.
Allow PC discoverability on the network.
Launch Wireshark from the Desktop.
Start packet capture on the Ethernet interface.
Open Colasoft Packet Builder 2.0 from the Desktop.
Select the appropriate network adapter.
Add an ARP packet with a Delta Time of 0.1 seconds.
Edit packet decoding information using Decode Editor and Hex Editor.
Send the packet in Burst Mode with no delay.
Analyze captured ARP packets in Wireshark.
Export the created packet for future use.
Colasoft Packet Builder enables the creation of custom packets to bypass IDS/firewall and assess network security. Document findings and be mindful of potential security implications.

Lab4 – Task3:

The lab delves into the intricacies of bypassing network security measures like firewalls and IDS (Intrusion Detection Systems) through a series of evasion techniques and packet crafting tools. Ethical hackers and penetration testers must navigate these security perimeters to evaluate the robustness of target networks.

Understanding network security limitations is crucial for professionals in the field.
Techniques such as packet fragmentation, source routing, and IP address spoofing are explored to bypass firewalls and IDS.
Various tools like Nmap, Colasoft Packet Builder, and Hping3 are employed to execute evasion strategies and craft custom packets.
Demonstrations include creating TCP/UDP packets, manipulating source ports, and executing TCP SYN flooding attacks.
The lab emphasizes documentation of findings and comprehension of the impact of security bypassing techniques.

Lab 5: Network Scanning with Various Tools

The lab focuses on extracting comprehensive information from target networks using network scanning tools. Ethical hackers and penetration testers utilize these tools to identify potential vulnerabilities and assess network security measures effectively.
First, Network scanning tools provide insights into live hosts, open ports, and running services within target networks.
Metasploit Framework offers a modular approach for discovering security vulnerabilities, aiding in penetration testing and IDS signature development.
Demonstrations include initiating scans, importing results, and analyzing data using Metasploit commands.
Techniques such as SYN scanning, TCP scanning, and SMB version identification are explored to gather detailed information about target systems.
The lab emphasizes the importance of documentation and analysis to identify potential security risks and vulnerabilities effectively.
the lab underscores the significance of network scanning in understanding the security posture of target networks and highlights the critical role of ethical hacking practices in ensuring robust network defenses.