**[Nmap scan]**

**Key Contributors:Abdulaziz**



**[02/7/23]**

This project and the preparation of this report were funded in part by ….through an agreement with the University of the Incarnate Word.

Cyber Security Systems and the University of the Incarnate Word

# EXECUTIVE SUMMARY

Start of executive summary ……

The use of Social-Engineer Tool Kit (SET), Nmap, and Metasploit by hackers can pose a significant threat to individuals and organizations that are using Wi-Fi WPA2 secured wireless networks. Social-Engineer Tool Kit (SET) is a powerful tool that can be used to create a range of social engineering attacks, including phishing emails, rogue access points, and fake websites. Nmap is a network mapping tool that can be used to scan for open ports and vulnerabilities in a Wi-Fi network, while Metasploit is a penetration testing framework that can be used to exploit these vulnerabilities and gain unauthorized access. Together, these tools can be used to launch sophisticated attacks on Wi-Fi networks, allowing an attacker to intercept sensitive information, such as usernames and passwords, and potentially gain access to sensitive data and systems. To protect against these types of attacks, it is essential to implement robust security measures, including strong passwords, two-factor authentication, and regular network vulnerability scans. Organizations should also provide regular security awareness training to their employees to help them identify and avoid social engineering attacks.

In project, there is performing an Nmap scanning to reveal exploitable open ports vulnerabilities. The scan will involve capturing open ports that are present in the target systems. An explanation of the exploited vulnerability will be made available and a comprehensive discussion of how hackers can take advantage of the vulnerability to compromise the vulnerable systems.

One is required to install Nmap in the project’s Kali Linux VM Ware. It’s normally important to confirm whether the IP address or hostname of the target system is reachable. You can do so by doing to the Kali Linux terminal and executing the command ***nmap scanme.nmap.org*** and scrolling to the table part that has the header ***PORT STATE SERVICE*** to see open ports as indicated in ***(Figure 1.1)***. For this project, there will be need to grep output to the “/home/kali/Desktop/Results” directory with greater effect ***(Figure 1.2)***.

You need to work with MSFvenom payload creator to actualize the attack by automating msfvenom and Metasploit processes. Use the command msfvenom and specify the IP address of payload listener (LHOST) as 10.0.2.15 and port number of reverse listener as 80 ***(Figure 2.1)***. Using the msfvenom and LHOST and LPORT, the payload and listener creation process will be successful and the specifying of connection back to listener establishing local host and local port.

Project Milestones

1. Install Nmap and confirm it can scan hosts to get open ports
2. Using Nmap scan localhost (127.0.0.1) and grep its output to “/home/kali/Desktop/Results”
3. Load Social-Engineering Toolkit and create a Payload and Listener
4. Specify the payload listener’s LHOST and reverse listener’s LPORT

Materials List:

1. 1 Virtual box
2. Kali Linux OS
3. Social-Engineer tool kit
4. Laptop
5. Nmap
6. Internet connection

Deliverables

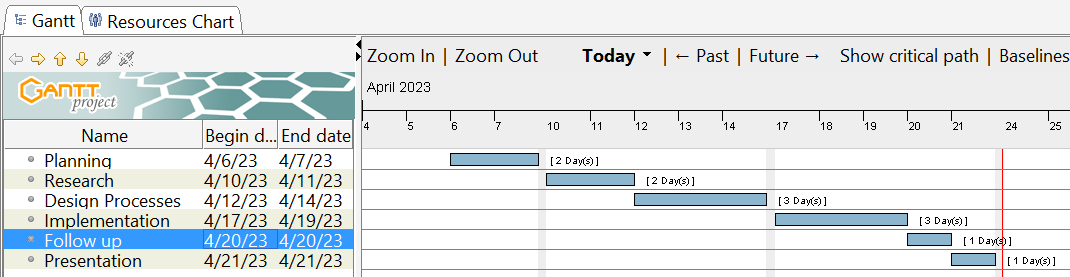
1. Ports open in the host identified by hostname scanme.nmap.org
2. Result for executing the command “Nmap -oG –vv” stored in “/home/kali/Desktop/Results”

Professional Accomplishments

1. Acquire knowledge on how to use Social-Engineering Toolkit to simulate attacks.
2. Knowledge and skills on how to use Wireshark to analyze
3. Knowledge on how to use Nmap for various host scanning activities

# PROJECT SCHEDULE MANAGEMENT

Create a Gantt chart with the application of your choice and replace it with the picture presented below.



# TABLE OF CONTENTS

[EXECUTIVE SUMMARY 3](file:///C:\Users\cayru\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\5\Attachments\Pro%20Template-1%5b61%5d.docx#_Toc133159515)

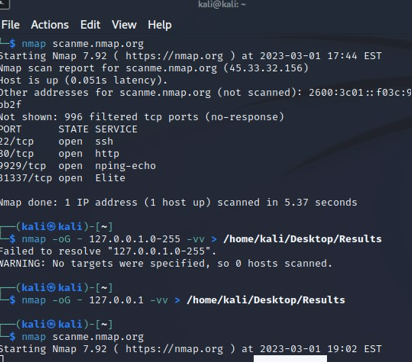
[Gantt chart 5](file:///C:\Users\cayru\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\5\Attachments\Pro%20Template-1%5b61%5d.docx#_Toc133159516)

[Phase 1: Host Discovery 7](file:///C:\Users\cayru\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\5\Attachments\Pro%20Template-1%5b61%5d.docx#_Toc133159517)

[Phase 2: Port Scanning & Exploiting Vulnerabilities 8](file:///C:\Users\cayru\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\5\Attachments\Pro%20Template-1%5b61%5d.docx#_Toc133159518)

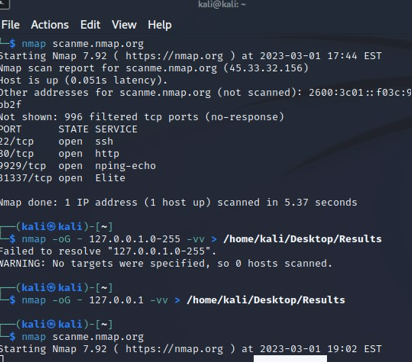
[Phase 3: Network Traffic Analysis 11](file:///C:\Users\cayru\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\5\Attachments\Pro%20Template-1%5b61%5d.docx#_Toc133159519)

# Phase 1: Host Discovery



**Figure 1.1 \ nmap scanme.nmap.org**

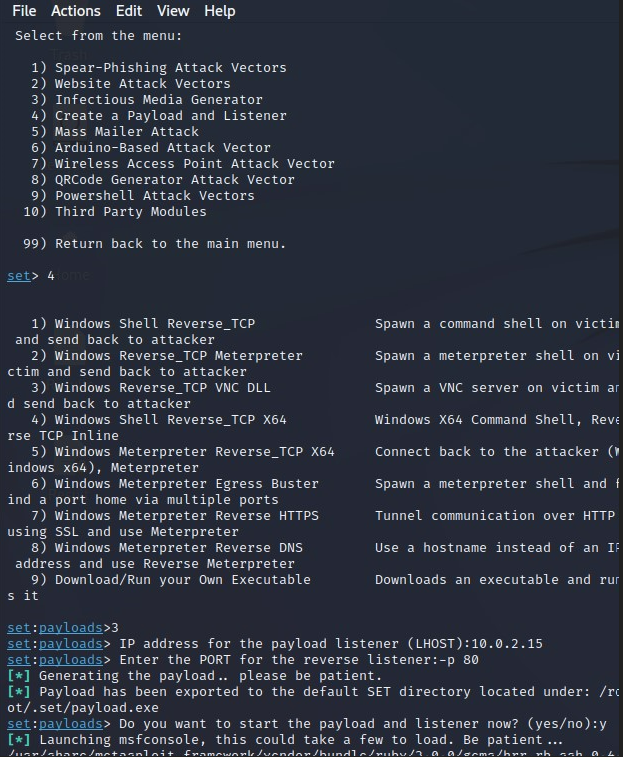
**Figure 1.1** shows execution of the command ***nmap scanme.nmap.org*** on Kali Linux terminal to get a table with header ***PORT STATE SERVICE*** that contain open ports for host identified by hostname scanme.nmap.org.



**Figure 1.2 \ nmap –oG 127.0.0.1 –vv > /home/kali/Desktop/Results**

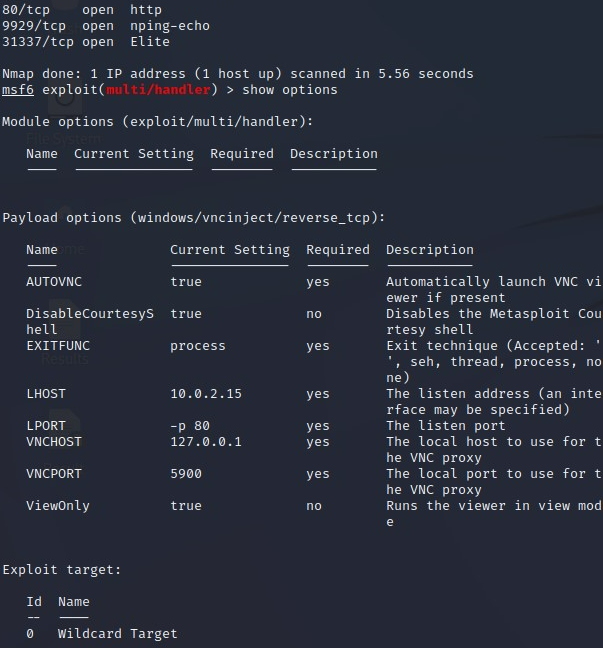
In ***Figure 1.2*** there is executing the command *nmap –oG 127.0.0.1 –vv > /home/kali/Desktop/Results* which is need to scan host identified by ip address 127.0.0.1 and grep its output to the ***“/home/kali/Desktop/Results”*** directory with greater effect.

# Phase 2: Port Scanning & Exploiting Vulnerabilities



**Figure 2.1 \ settoolkit**

Figure 2.1 shows loading of the Social-Engineering Toolkit by executing the command settoolkit in the Kali Linux VM and selecting option 4, which is “create a Payload and Listener” before specifying the IP address of payload listener (LHOST) as 10.0.2.15 and port number of reverse listener as 80.



**Figure 2.2 \ scanning for vulnerabilities using Metasploit**

**Figure 2.2** above shows how one can scan vulnerabilities of a given host using metasploit.

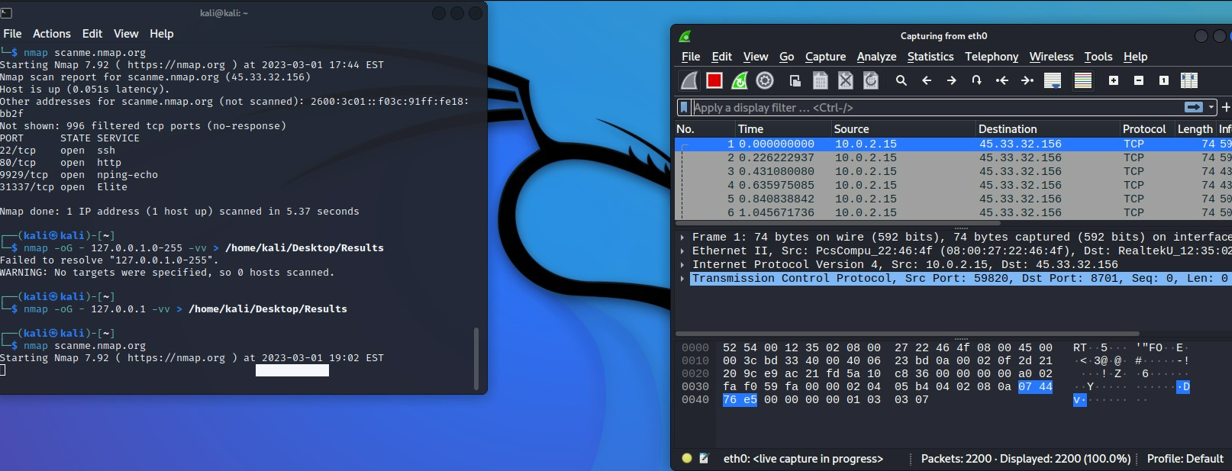
Text

Description automatically generated

**Figure 2.3 \ Exploiting Vulnerabilities using metasploit**

**Figure 2.3** show how one can exploit RFI vulnerabilities using Metasploit module.

# Phase 3: Network Traffic Analysis



**Figure 3.1 \ Analyzing Network Traffic using Wireshark**

Figure 3.1 shows scanning of host using a Nmap and analyzing the resulting network traffic using wireshark. Wireshark uses Nmap for scanning.

* <https://github.com/AlenaziAbdulaziz/-cyberknowledge.git>

<https://www.tecmint.com/nmap-network-security-scanner-in-kali-linux/>

* <https://nmap.org/>