Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 22/08/2023

Assignment Details

Assigned Date: 21-08-2023

Due Date: 22-08-2023

Topic: Port Scanning

Introduction

For this assignment, I conducted a port scanning exercise using the nmap command within Kali Linux. I targeted three distinct machines on the network to identify open ports and services. By executing the nmap command with appropriate flags and specifying the IP addresses of the target machines.

Content

METASPLOITABLE2

Metasploitable is a purposely vulnerable virtual machine (VM) that's used for training, practicing, and demonstrating various cybersecurity techniques and tools, particularly penetration testing and ethical hacking. It's designed to simulate a range of security vulnerabilities and weaknesses commonly found in real-world systems, making it an ideal environment for security professionals, students, and researchers to learn about and practice exploiting vulnerabilities in a controlled and safe setting.

Port scanning is a technique used to discover open ports on a target system. It involves sending network requests to a range of ports on a target system and analyzing the responses to determine which ports are open, closed, or filtered. Nmap (Network Mapper) is a popular open-source tool used for port scanning and network discovery.

IPv4 address: 10.0.2.5

Commands:

nmap 10.0.2.5	//Basic Scan
nmap -sV 10.0.2.5	//Version Detection
nmap -T4 -A 10.0.2.5	//will get version, OS, certificates and keys

Open Ports	Service Version	Operating System
21/tcp ftp	vsftpd 2.3.4	Metasploitable2
22/tcp ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)	(Linux)
23/tcp telnet	Linux telnetd	
25/tcp smtp	Postfix smtpd	
53/tcp domain	ISC BIND 9.4.2	
80/tcp http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	
111/tcp rpcbind	2 (RPC #100000)	
139/tcp netbios-ssn	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	
445/tcp microsoft-ds	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	
512/tcp exec	netkit-rsh rexecd	
513/tcp login		
514/tcp shell		
1099/tcp rmiregistry	GNU Classpath grmiregistry	
1524/tcp ingreslock	Metasploitable root shell	
2049/tcp nfs	2-4 (RPC #100003)	
2121/tcp ccproxy-ftp	ProFTPD 1.3.1	
3306/tcp mysql	MySQL 5.0.51a-3ubuntu5	
5432/tcp postgresql	PostgreSQL DB 8.3.0 - 8.3.7	
5900/tcp vnc	VNC (protocol 3.3)	
6000/tcp X11	(access denied)	
6667/tcp irc	UnrealIRCd	
8009/tcp ajp13	Apache Jserv (Protocol v1.3)	
8180/tcp unknown	Apache Tomcat/Coyote JSP engine 1.1	

WINDOWS7

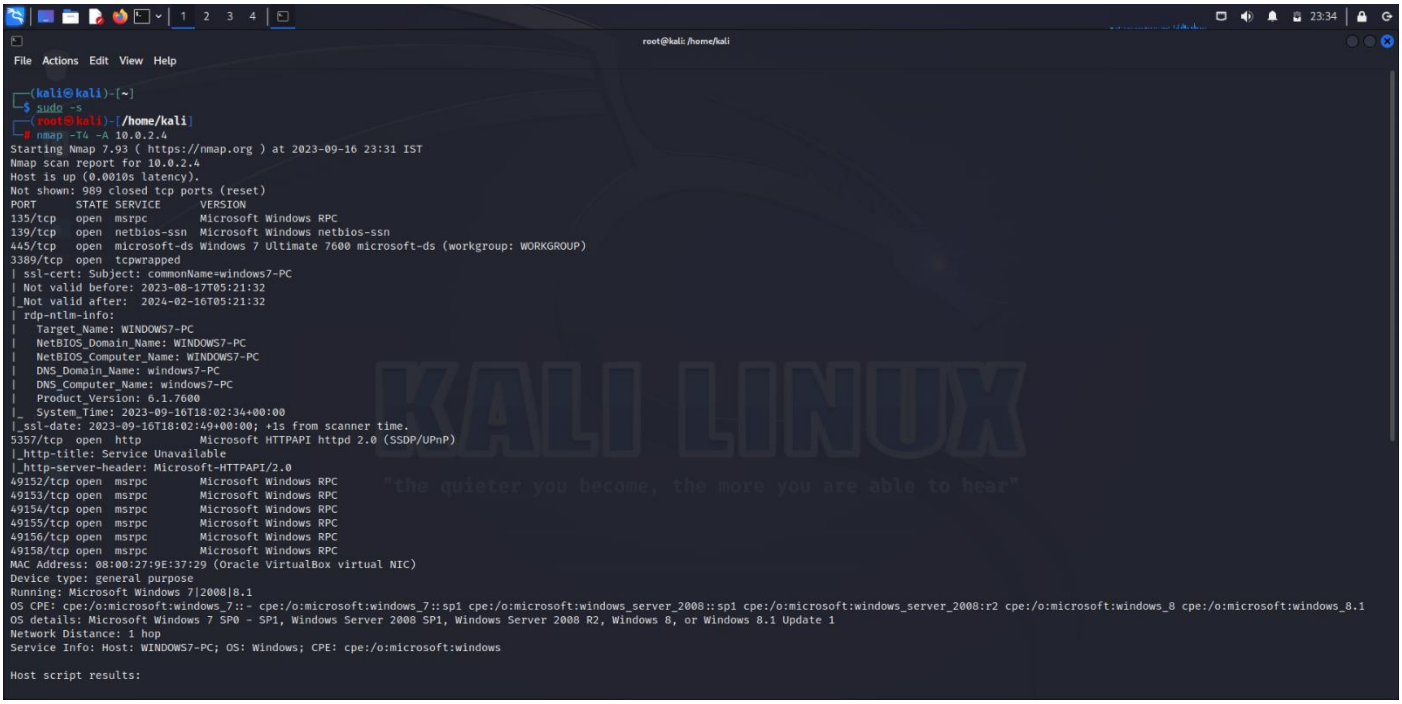
IPv4 address: 10.0.2.4

Commands:

nmap 10.0.2.4 //Basic Scan

nmap -sV 10.0.2.4 //Version Detection

nmap -T4 -A 10.0.2.4 //will get version, OS, certificates and keys



Open Ports	Service Version	Operating System
135/tcp msrpc	Microsoft Windows RPC	Windows7
139/tcp netbios-ssn	Microsoft Windows netbios-ssn	
445/tcp microsoft-ds	Microsoft Windows 7-10 microsoft-ds(WORKGROUP)	
554/tcp rtsp		
2869/tcp icslap	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
3389/tcp ms-wbt-server		
5357/tcp wsdapi	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
10243/tcp unknown	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
49152/tcp unknown	Microsoft Windows RPC	
49153/tcp unknown	Microsoft Windows RPC	
49154/tcp unknown	Microsoft Windows RPC	
49155/tcp unknown	Microsoft Windows RPC	
49156/tcp unknown	Microsoft Windows RPC	
49158/tcp unknown	Microsoft Windows RPC	

scanme.nmap.org (Website)

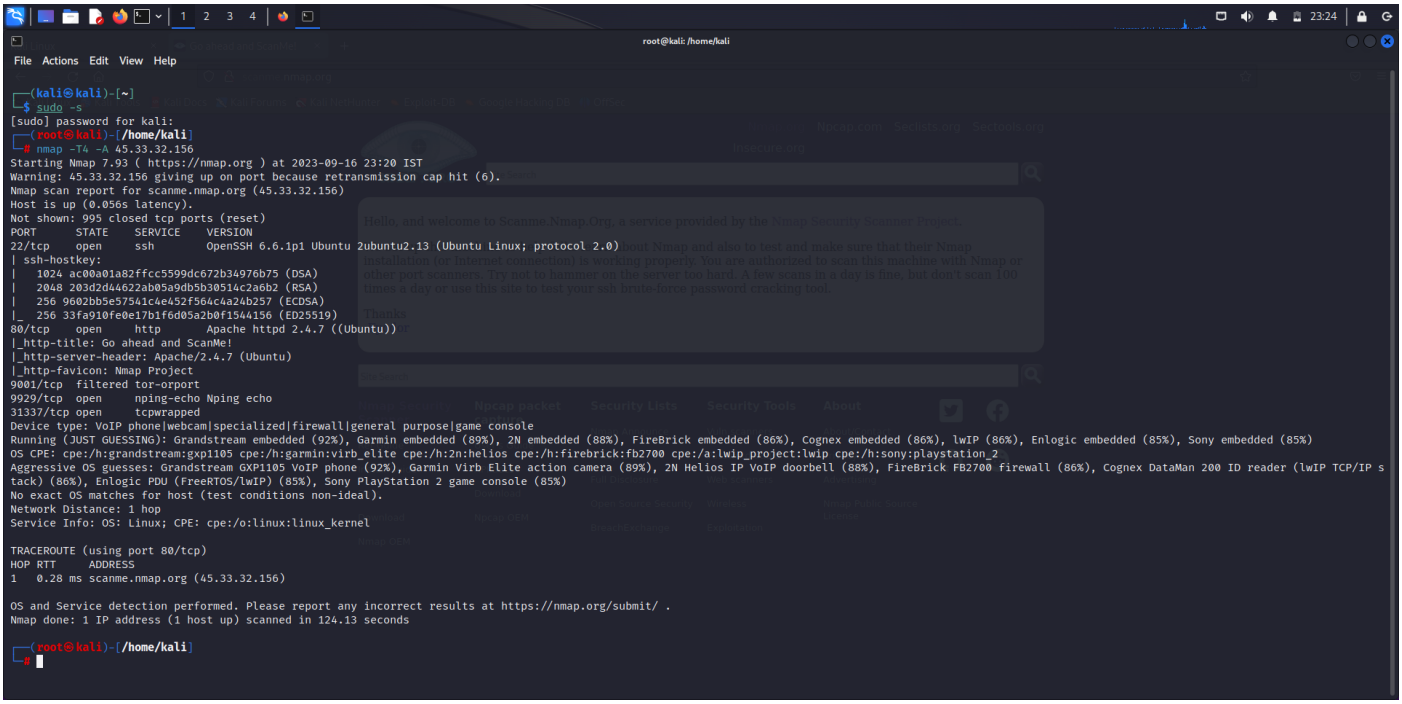
IPv4 address: 45.33.32.156

Commands:

nmap 10.0.2.4 //Basic Scan

nmap -sV 10.0.2.4 //Version Detection

nmap -T4 -A 10.0.2.4 //will get version, OS, certificates and keys



Open Ports	Service Versions	Operating System
22/tcp ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	Ubuntu (Linux)
80/tcp http	Apache httpd 2.4.7	
9001/tcp		
9929/tcp		
31337/tcp Elite tcpwrapped		

Analysis

The Nmap scan of the target website revealed a range of open ports and associated services. The scan indicated a diverse set of services including FTP, SSH, HTTP, SMTP, and more. Additionally, the presence of outdated or potentially misconfigured services like Telnet and anonymous FTP access raised concerns about potential security vulnerabilities. The scan underscores the importance of maintaining updated and secure service configurations to mitigate possible exploitation risks.

Conclusion

In conclusion, the Nmap port scan of the target website provided valuable insights into the network's exposed services and potential security vulnerabilities. The wide range of open ports revealed a diverse set of services, highlighting the need for robust security measures to protect against potential attacks. The presence of outdated or insecure services, such as Telnet and anonymous FTP access, underscores the importance of regular security assessments and updates. However, it is crucial to stress that ethical considerations and proper authorization are paramount when conducting any form of scanning. By adhering to ethical guidelines and maintaining vigilant security practices, organizations can better safeguard their digital assets and maintain a strong security posture.

References

[An InfoSec Blog for anyone interested to learn security and Hacking (wordpress.com)]

[Nmap: the Network Mapper - Free Security Scanner]