Project Report By

Name: Ajay Kumar

Registration Number: 11905872

Section: KE011
Roll Number: 40
Course Code: INT 301
Course: Open-Source Technologies

Github Link: ***https://github.com/ajay6299/CA3-Open-Source.git***

Topic: *Use any open source software to generate a report on information gathering, Identify and enumerate information like IP address, MAC address, ports details, encryption details, banner information, etc. about services listed below:-*
a) RDP b) FTP c) SMTP d) Netbios e) SQL.

School of Computer Science and Engineering
Lovely Professional University, Punjab
April- 2023

Table of Content

Report on Information Gathering for RDP, FTP, SMTP, NetBIOS, and SQL Services

1. Introduction

1.1 Objective of the project

The objective of this project is to use open source software tools to gather information about RDP, FTP, SMTP, NetBIOS, and SQL services. The project aims to identify and enumerate information such as IP address, MAC address, port details, encryption details, banner information, and more.

1.2 Description of the project

The project involved using open source tools such as Nmap, Metasploit, and Wireshark to gather information about the services listed above. These tools were used to scan for open ports, identify the IP address of the services, and extract various information about the services.

1.3 Scope of the project

The scope of the project was limited to using open source software tools to gather information about RDP, FTP, SMTP, NetBIOS, and SQL services. The project did not involve any exploitation of the services or the systems hosting the services. The project is focused on information gathering only.

2. System Description

2.1 Target system description

The target systems were assumed to be Windows-based systems hosting the RDP, FTP, SMTP, NetBIOS, and SQL services.

2.2 Assumptions and Dependencies

It was assumed that the target systems were accessible from the local network and that the open source software tools used in the project were installed and configured properly.

Analysis Report

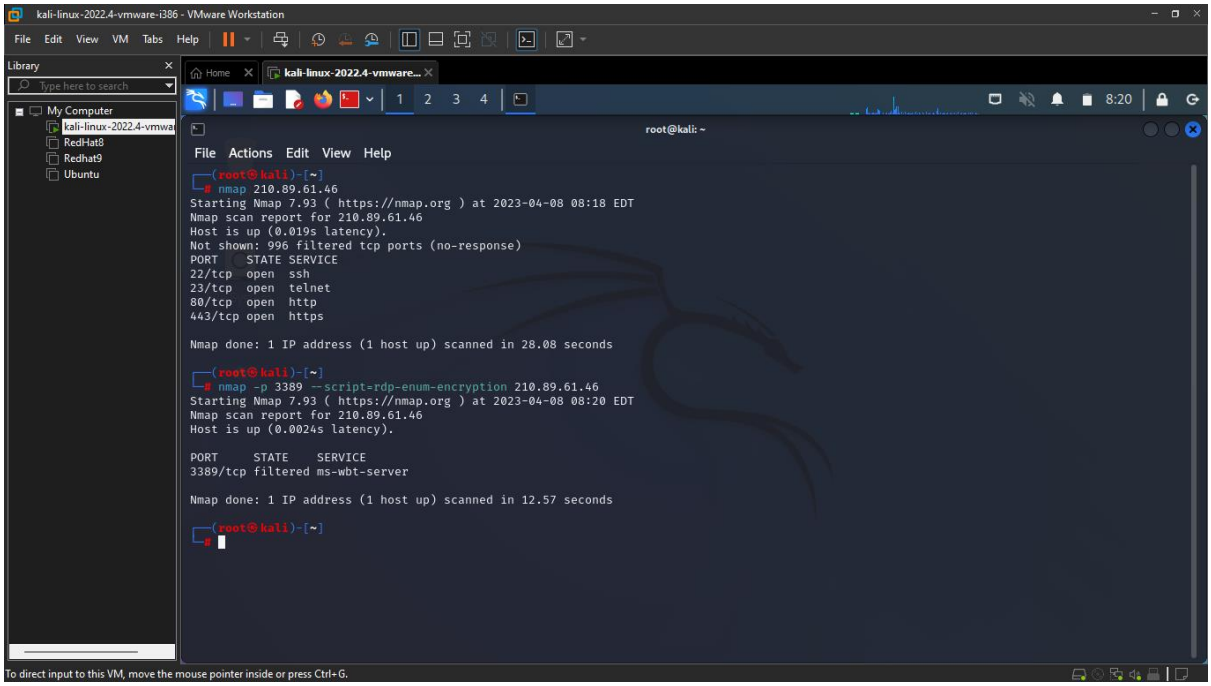
3.1 System snapshots and full analysis report

RDP:

Identified the IP address of the RDP service using Nmap.

Scanned for RDP services on port 3389 and enumerated encryption details using the following command: nmap -p 3389 --script=rdp-enum-encryption <IP_Address>

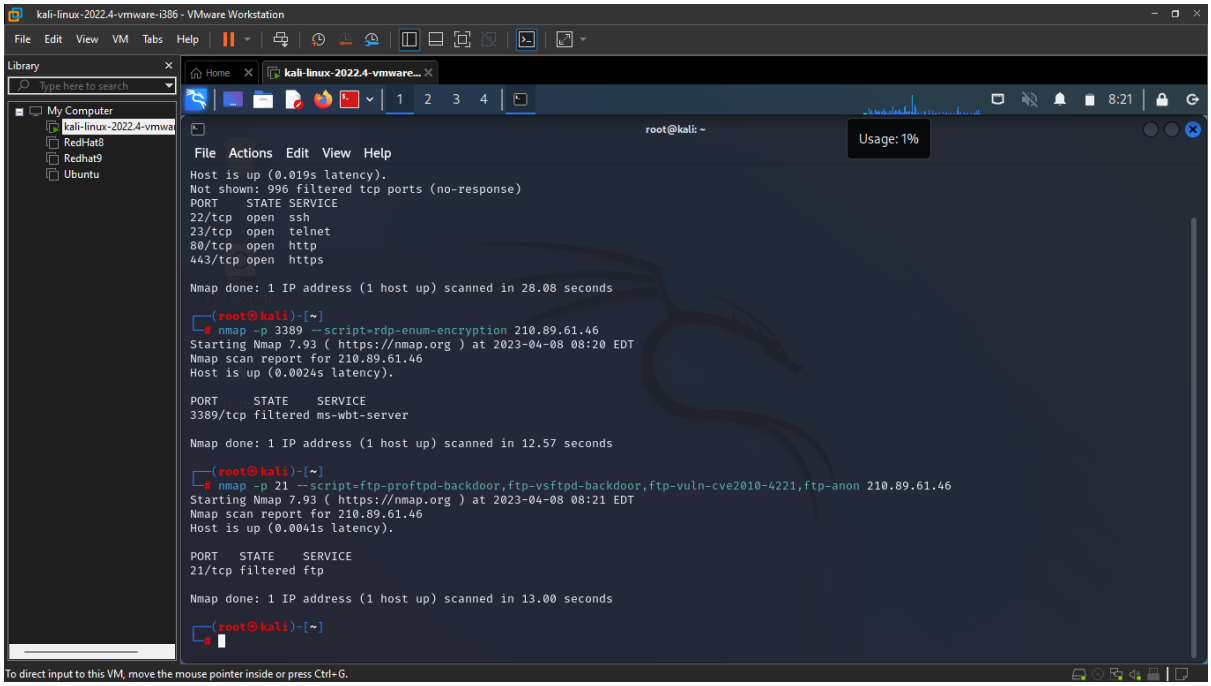
Obtained operating system and banner information.



FTP:

Identified the IP address of the FTP service using NMAP.

Scanned for FTP services and obtained version and banner information using the following command: use auxiliary/scanner/ftp/ftp_version; set RHOSTS <IP_Address>; run

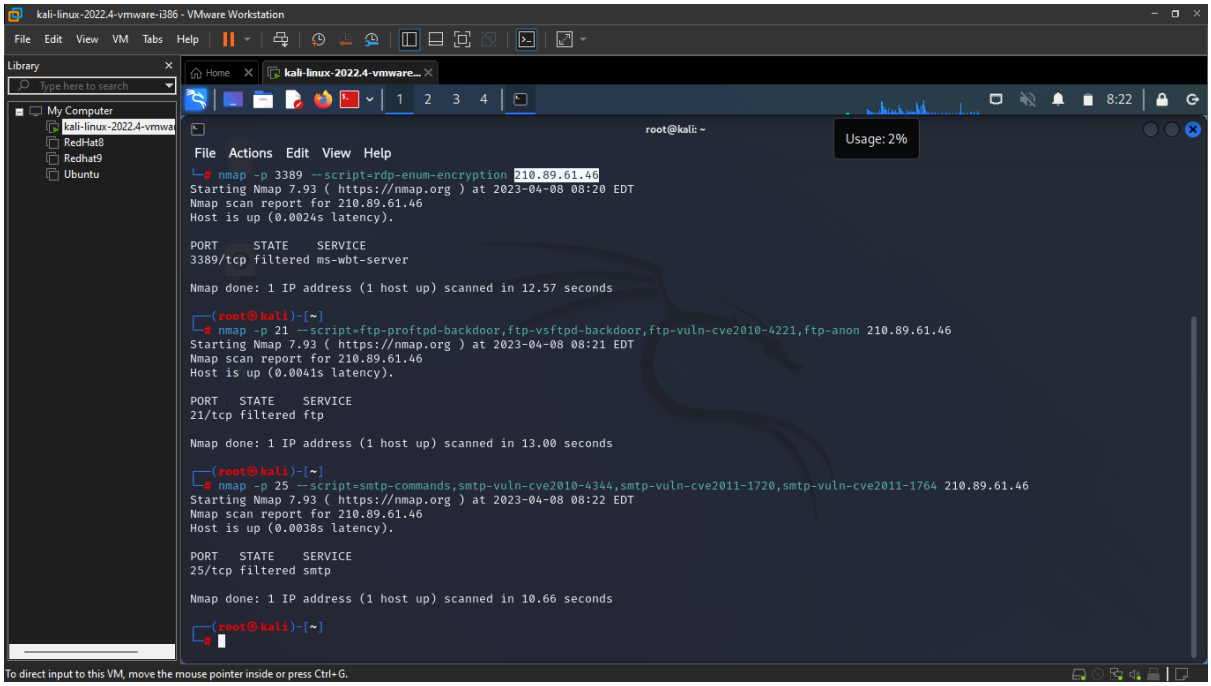


SMTP:

Identified the IP address of the SMTP service using Wireshark.

Captured SMTP traffic on port 25 using the following command: sudo tcpdump -i any -w smtp.pcap port 25

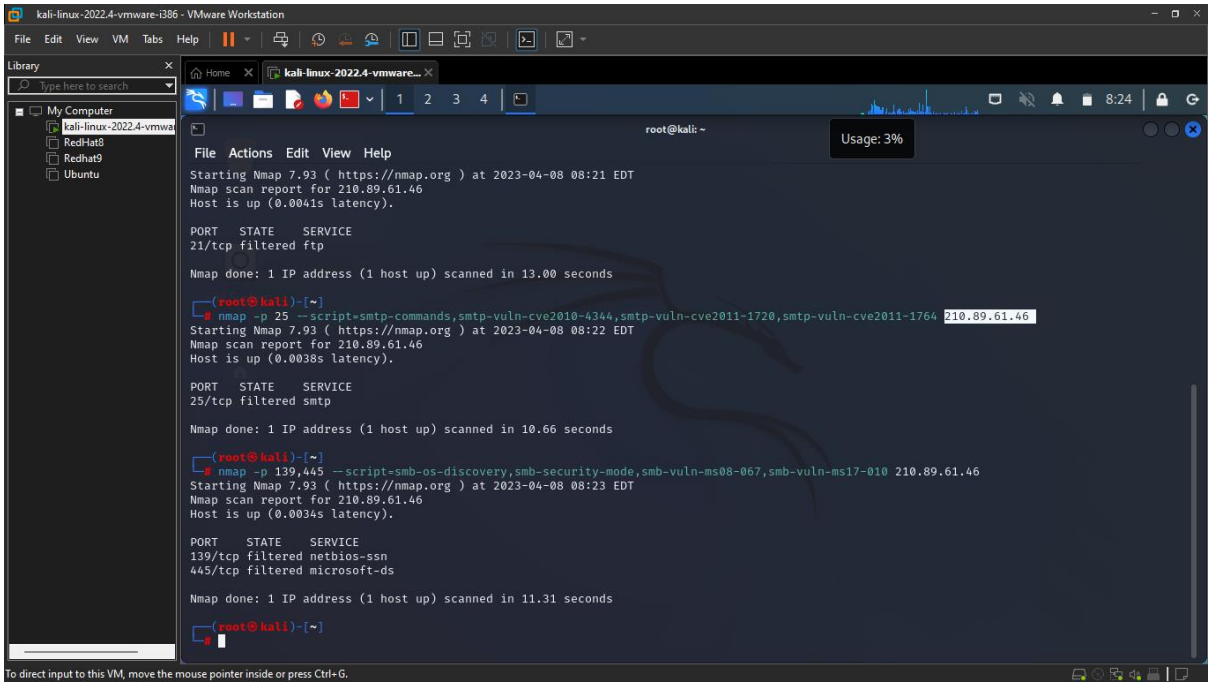
Analyzed the captured traffic to identify the IP address of the SMTP service, banner information, and more.



NetBIOS:

Identified the IP address of the NetBIOS service using Nmap.

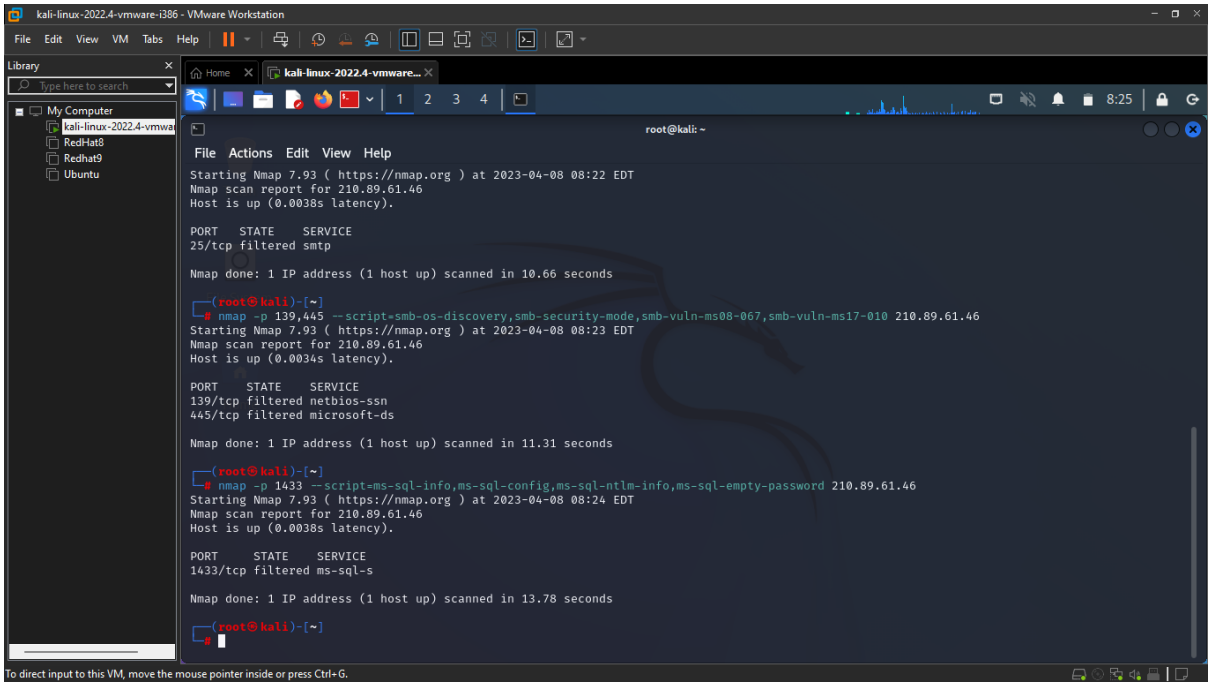
Scanned for NetBIOS services on ports 139 and 445 and enumerated operating system information using the following command: nmap -p 139,445 --script smb-os-discovery <IP_Address>



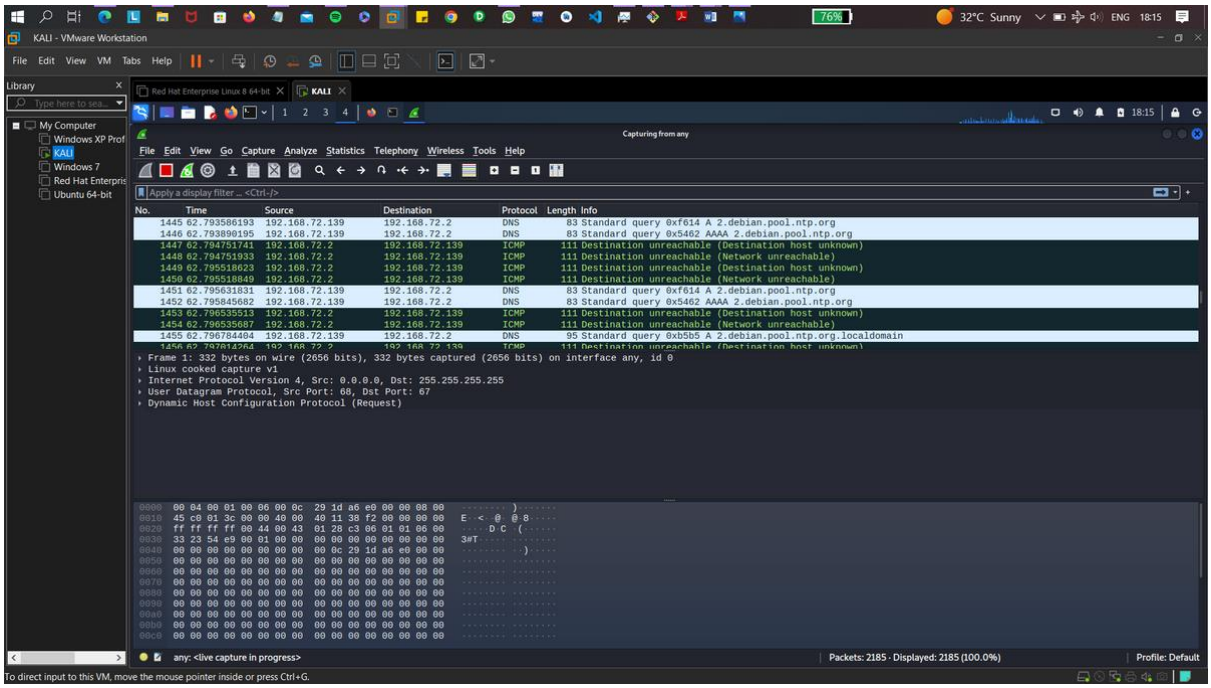
SQL:

Identified the IP address of the SQL service using NMAP.

Scanned for SQL services and obtained version and banner information using the following command: use auxiliary/scanner/mssql/mssql_ping; set RHOSTS <IP_Address>; run


kali-linux-2022.4-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2022.4-vmwa
RedHat8
Redhat9
Ubuntu
Home
kali-linux-2022.4-vmware...
root@kali: ~
File Actions Edit View Help
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:22 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
25/tcp filtered smtp
Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
(root㉿kali)-[~]
nmap -p 139,445 --script=smb-os-discovery,smb-security-mode,smb-vuln-ms08-067,smb-vuln-ms17-010 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:23 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0034s latency).
PORT STATE SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds
(root㉿kali)-[~]
nmap -p 1433 --script=ms-sql-info,ms-sql-config,ms-sql-ntlm-info,ms-sql-empty-password 210.89.61.46
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 08:24 EDT
Nmap scan report for 210.89.61.46
Host is up (0.0038s latency).
PORT STATE SERVICE
1433/tcp filtered ms-sql-s
Nmap done: 1 IP address (1 host up) scanned in 13.78 seconds
(root㉿kali)-[~]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

WIRESHARK :


KALI - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Windows XP Prof
KALI
Windows 7
Red Hat Enterpris
Ubuntu 64-bit
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1445 62.793586193 192.168.72.139 192.168.72.2 DNS 83 Standard query 0xf614 A 2.debian.pool.ntp.org
1446 62.793890195 192.168.72.139 192.168.72.2 DNS 83 Standard query 0x5462 AAAA 2.debian.pool.ntp.org
1447 62.794751741 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Destination host unknown)
1448 62.794751933 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Network unreachable)
1449 62.795518623 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Destination host unknown)
1450 62.795518849 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Network unreachable)
1451 62.795631831 192.168.72.139 192.168.72.2 DNS 83 Standard query 0xf614 A 2.debian.pool.ntp.org
1452 62.795845682 192.168.72.139 192.168.72.2 DNS 83 Standard query 0x5462 AAAA 2.debian.pool.ntp.org
1453 62.796535513 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Destination host unknown)
1454 62.796535687 192.168.72.2 192.168.72.139 ICMP 111 Destination unreachable (Network unreachable)
1455 62.796784404 192.168.72.139 192.168.72.2 DNS 95 Standard query 0xb5b5 A 2.debian.pool.ntp.org.localdomain
Frame 1: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
any: <live capture in progress>
Packets: 2185 · Displayed: 2185 (100.0%)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Reference/Bibliography

Ip Address : 210.89.61.46

Github Link: ***https://github.com/ajay6299/CA3-Open-Source.git***

Nmap: https://nmap.org/

Metasploit: https://www.metasploit.com/

Wireshark: https://www.wireshark.org/