

**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**

**1. Introduction**

1.1 Objective of the project

1.2 Description of the project

1.3 Scope of the project

**2. System Description**

2.1 Target system description

2.2 Assumptions and Dependencies (If applicable)

**3. Analysis Report**

3.1 System snapshots and full analysis report

**4. Reference**

**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. **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**

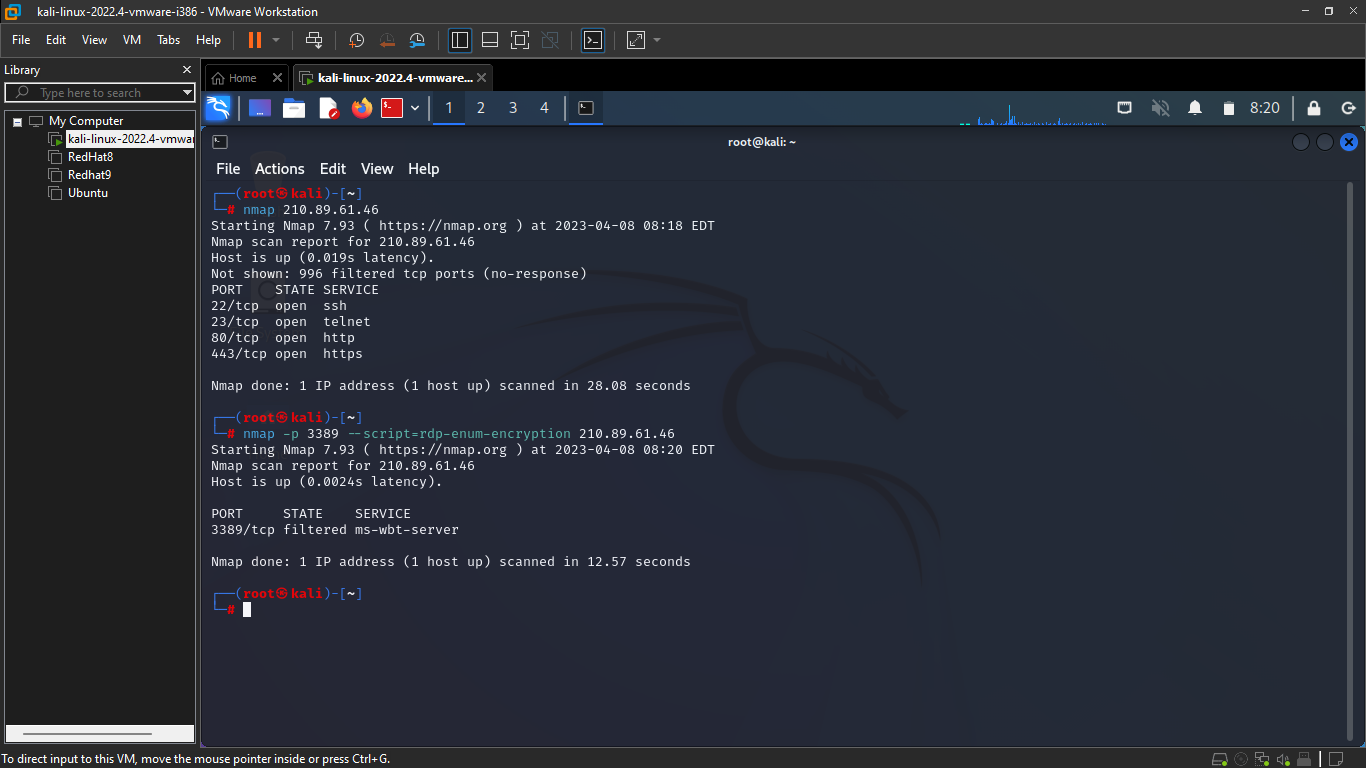
**3.1 System snapshots and full analysis report**

**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>*

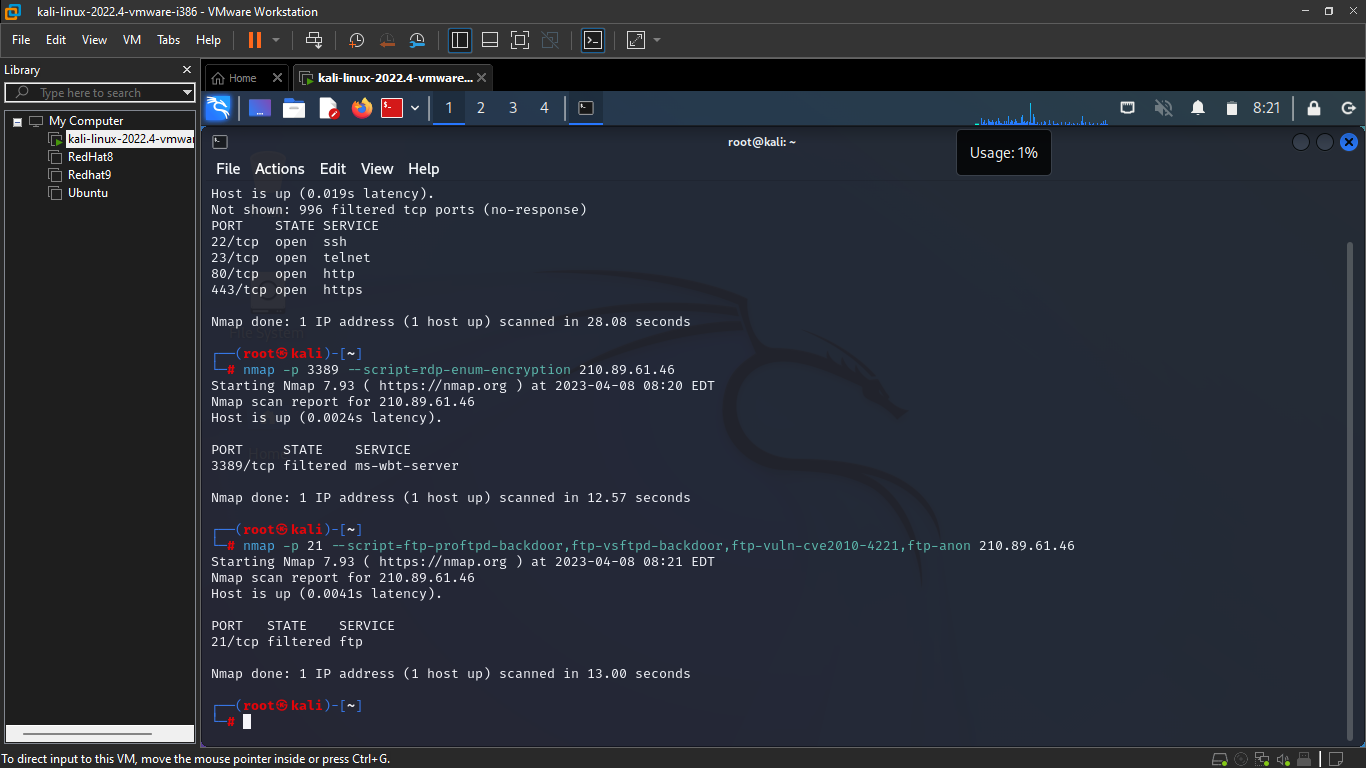
*Obtained operating system and banner information.*

****

**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*

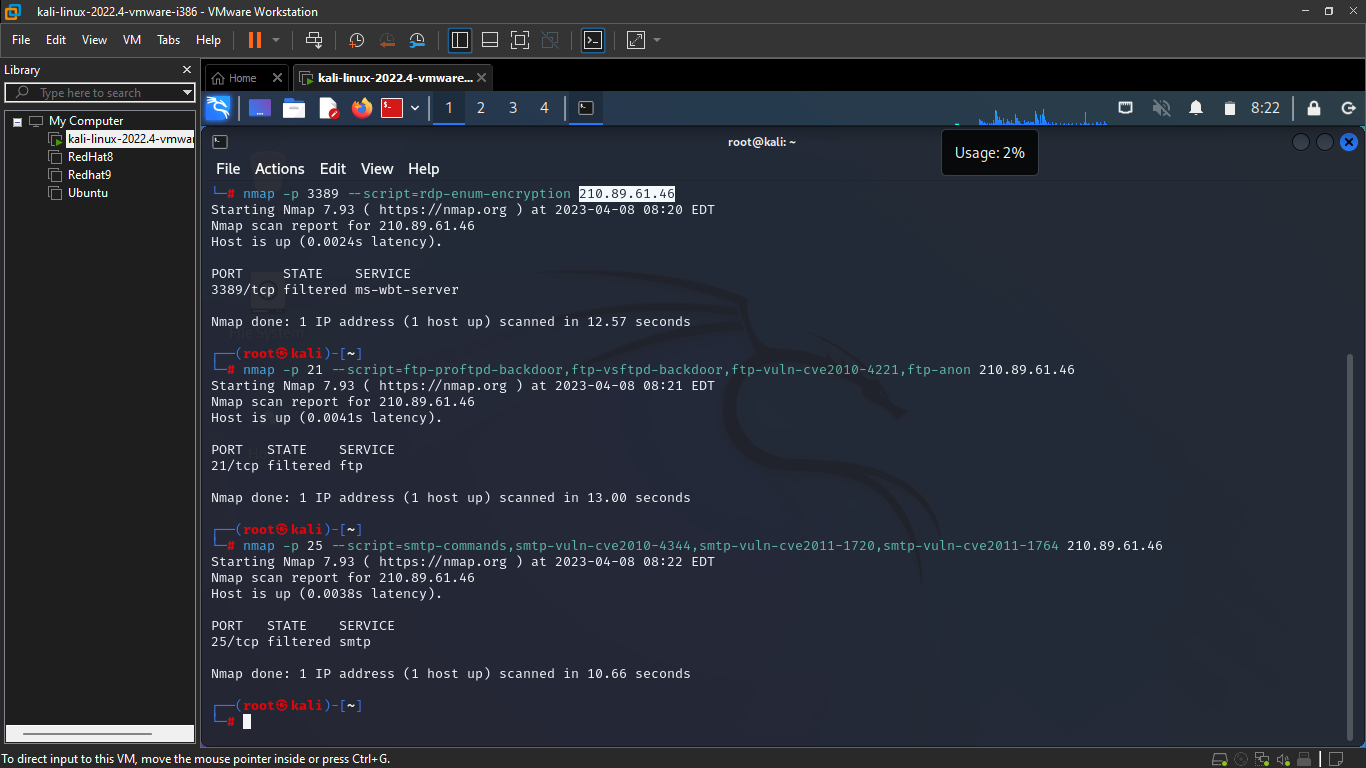


**SMTP:**

*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*

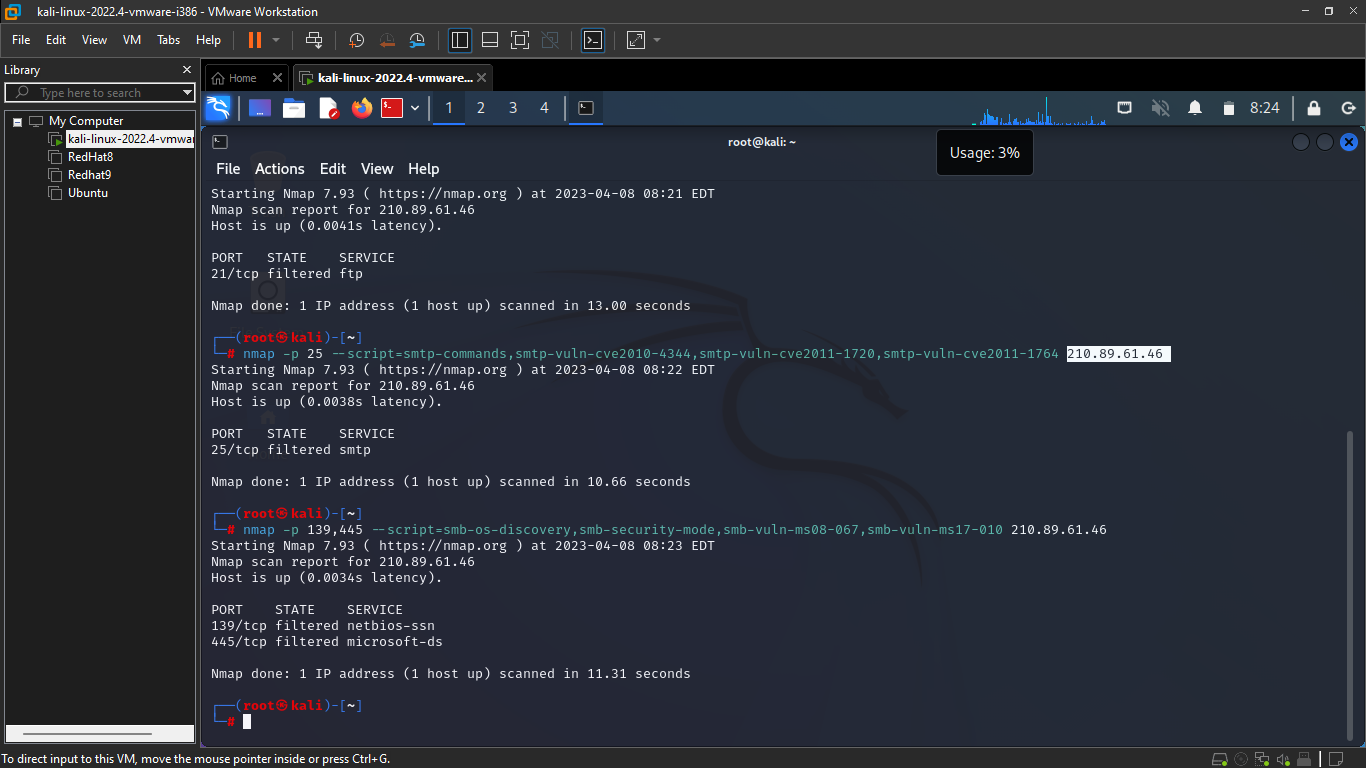
*Analyzed the captured traffic to identify the IP address of the SMTP service, banner information, and more.*



**NetBIOS:**

*Identified the IP address of the NetBIOS service using Nmap.*

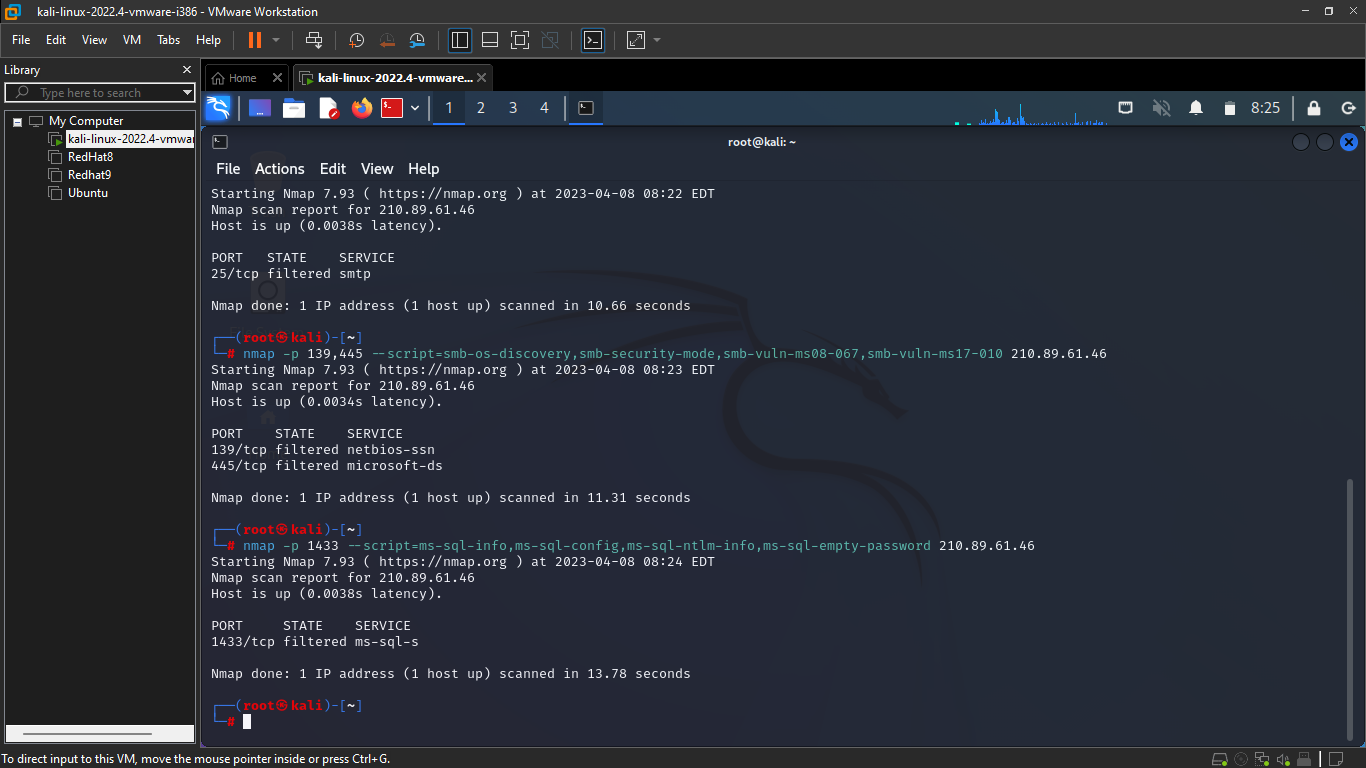
*Scanned for NetBIOS services on ports 139 and 445 and enumerated operating system information using the following command: nmap -p 139,445 --script smb-os-discovery <IP\_Address>*



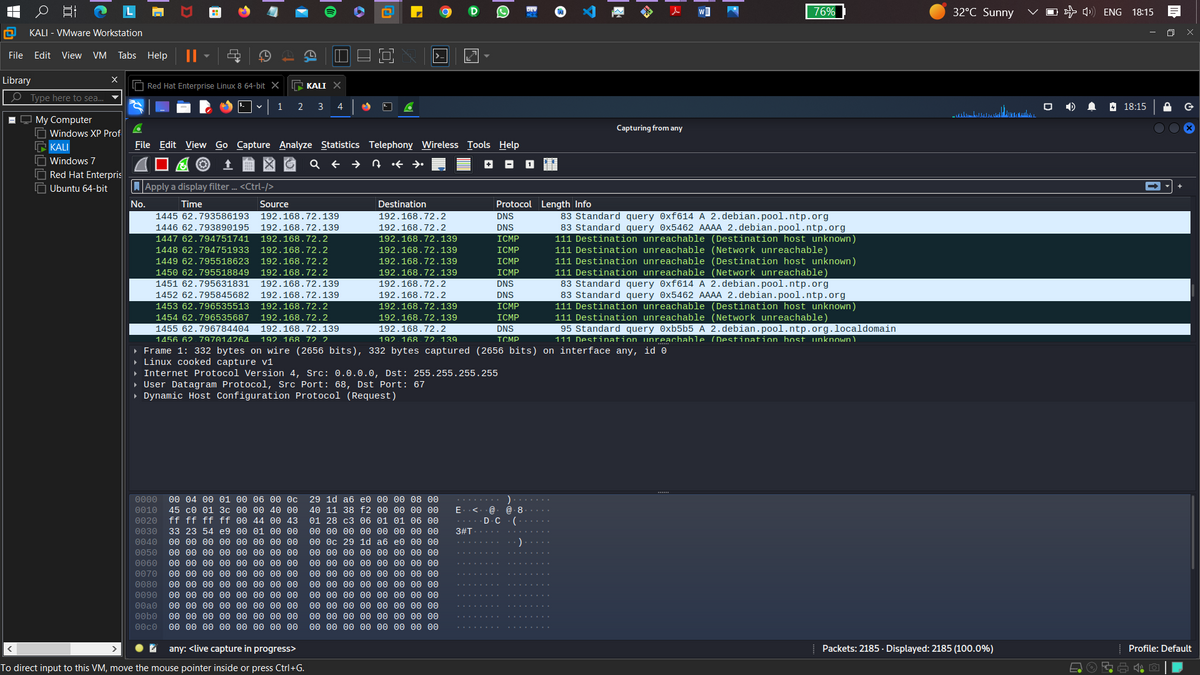
**SQL:**

*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*



**WIRESHARK :**

****

**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/>