**INT301**

**OPEN SOURCE TECHNOLOGIES**



**SUBMITTED BY:**

Yangoti Harsha Vardhan Reddy

**Reg. No. -** 11904858

**Roll. No. -** 40

**Section -** KE059

**ACADEMIC TASK**

1. **INTRODUCTION**
   1. **Objective of the Project**

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, a)RDP b) FTP c) SMTP d) Netbios e) SQL .

* 1. **Description of the Project**

According to the task given, we can use open source software tools such as Nmap, Wireshark to generate a report on information gathering for the listed services. These tools can help with the detection and collection of various details such as IP address, MAC address, port information, encryption information, banner information, and more.

Nmap can be used to search for open ports and retrieve RDP version and banner information. Wireshark can capture packets and aid in the identification of encryption protocols. Nmap can be used to scan for open ports and retrieve banner information for FTP, and Wireshark can be used to capture packets and identify any encryption protocols used. Similarly, we can use Nmap and Wireshark to scan for open ports, retrieve banner information, and so on for SMTP. For NetBIOS, we can use Nmap to scan for open ports and retrieve the version and banner information. Lastly, for SQL, as well we can use Nmap to gather the information such as ip address, port details.

The use of open source tools such as Nmap and Wireshark is widely known for retrieving information based on various services to filter the details. These details provide information about the enumeration of system over the network as well.

* 1. **Scope of the Project**

As there are many tools to do the information gathering and prepare a report for the services provided, including RDP, FTP, SMTP, NetBIOS, and SQL. These tools can help identify and enumerate information such as IP addresses, MAC addresses, port details, encryption details, and banner information, among other things. The tool such as Wireshark is best known for port details, packet transferring. For using the different services the prerequisites are need to be fulfilled to work without any errors. Though it is little hard to do these, the result of the analysis is very descriptive way and easily used to further analysis, making it a useful tool for security professionals who need to assess the security of their networks.

One popular tool for this purpose is Nmap, which is a free and open source tool that can be used to scan networks and identify hosts and services. Nmap can scan multiple protocols, including TCP, UDP, and ICMP, and can provide detailed information about the devices and services on a network. It can also be used to detect vulnerabilities and exploits, making it a useful tool for security professionals.

1. **System Description**
   1. **Target System Description**

To generate a report on information gathering for the services listed below (RDP, FTP, SMTP, NetBIOS, SQL), you can use open-source tools like Nmap, OpenVAS, and Metasploit. Here is a brief description of how you can gather the requested information using these tools:

To gather information about RDP, you can use Nmap, a free and open-source network scanner. You can scan the target IP address to check if the RDP port (3389) is open. You can also use a tool like rdpscan to gather information about the RDP service, such as the protocol version and the security settings. To gather information about FTP, you can use Nmap to scan the target IP address for open FTP ports (20 and 21). You can also use a tool like ftp-anon to check if anonymous FTP access is allowed, and use a tool like ftpmap to gather information about the FTP service, such as the banner information and encryption details.

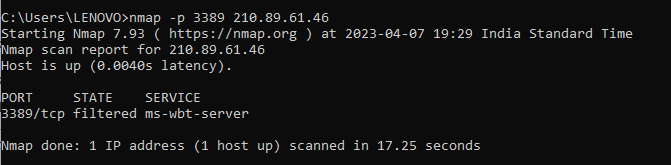
To gather information about SMTP, you can use Nmap to scan the target IP address for open SMTP ports (25, 587, or 465). You can also use a tool like smtp-user-enum to enumerate the valid email addresses on the target SMTP server and use a tool like smtpscan to gather information about the SMTP service, such as the banner information and encryption details. To gather information about NetBIOS, you can use Nmap to scan the target IP address for open NetBIOS ports (139 and 445). You can also use a tool like nbtscan to gather information about the NetBIOS service, such as the NetBIOS name, MAC address, and operating system information.

To gather information about SQL, you can use Nmap to scan the target IP address for open SQL ports (1433, 1434, 3306, or 5432). You can also use a tool like sqlmap to perform automated SQL injection attacks to gather information about the SQL service, such as the database schema and the user accounts. Once you have gathered the requested information for each of the services, you can compile it into a report that includes the IP address, MAC address, port details, encryption details, and banner information for each service. The report should also include a description of the tools used and the methodology used to gather the information.

1. **Analysis Report**
   1. **System snapshots and full analysis report**

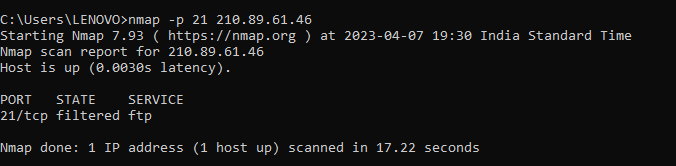
**RDP:**

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that allows users to connect to and control another computer over a network. Some of the information that can be gathered about an RDP service include:

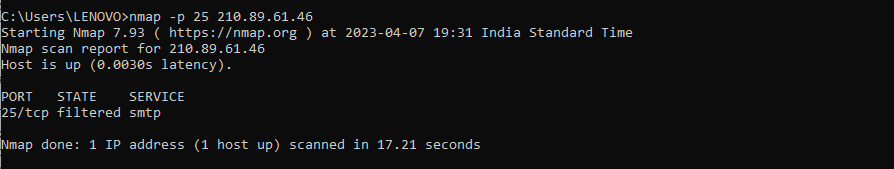


**FTP:**

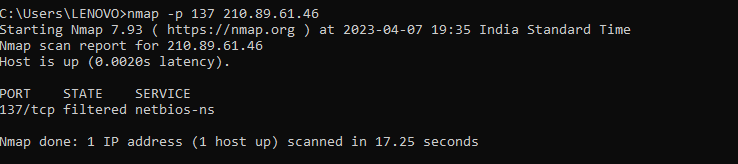
File Transfer Protocol (FTP) is a standard protocol used for transferring files over a network. Some of the information that can be gathered about an FTP service include:



**SMTP:**

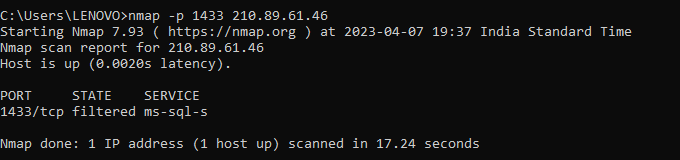
 Simple Mail Transfer Protocol (SMTP) is a standard protocol used for sending and receiving email messages over a network. Some of the information that can be gathered about an SMTP service include,

**NetBIOS:**

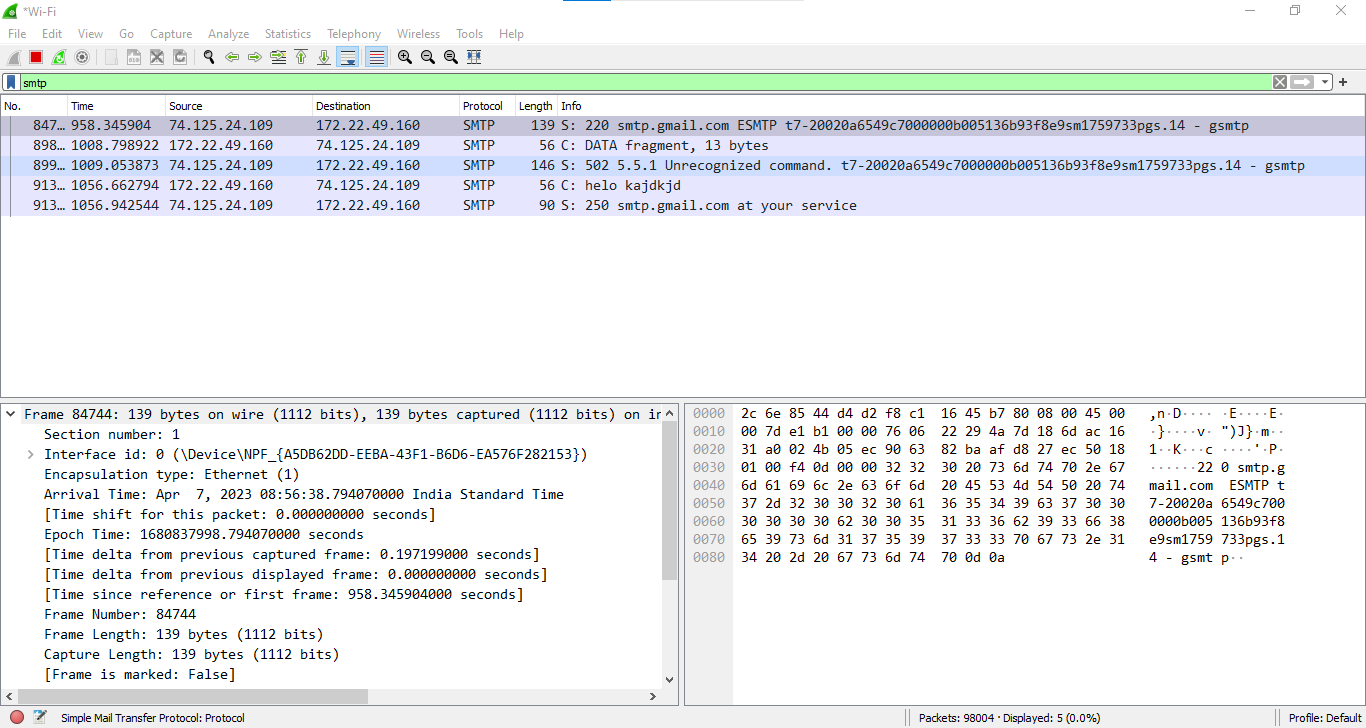
 NetBIOS is a legacy protocol used for communication between computers on a local network. Some of the information that can be gathered about NetBIOS include:

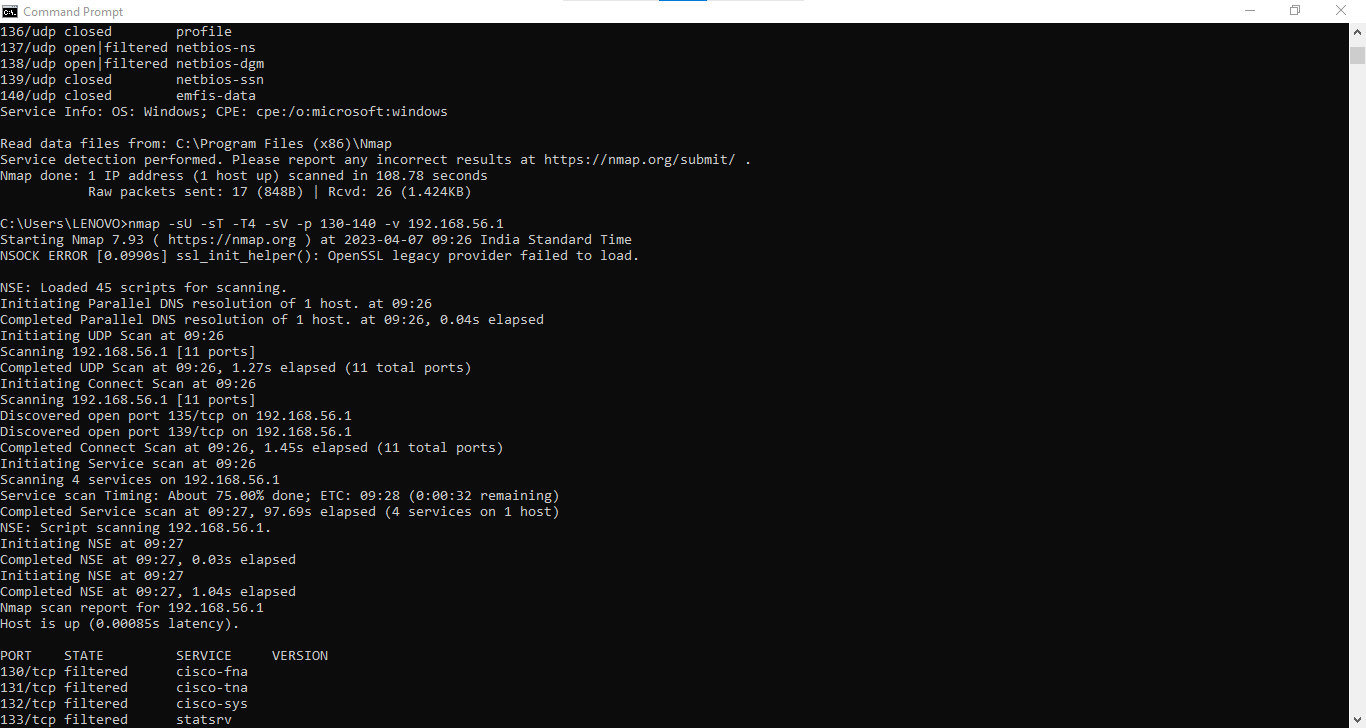
**SQL:**

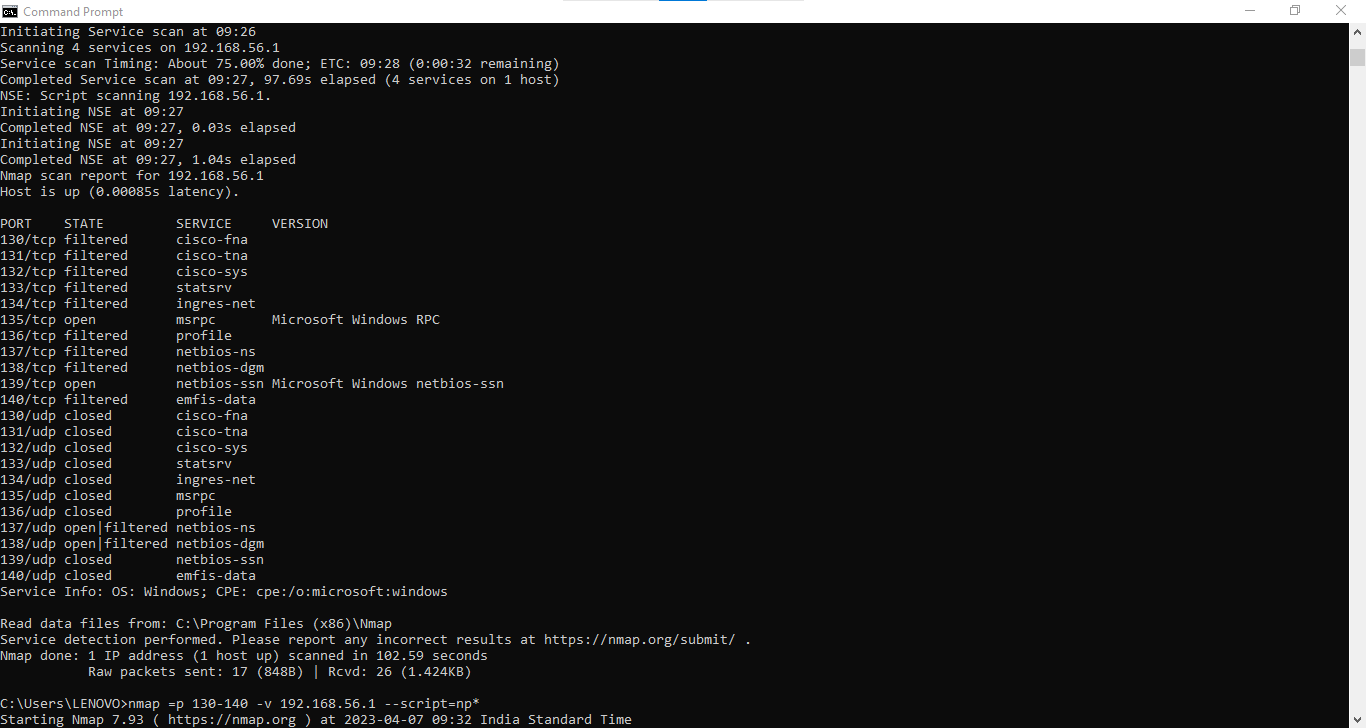
Structured Query Language (SQL) is a standard language used for managing relational databases. Some of the information that can be gathered about SQL include,

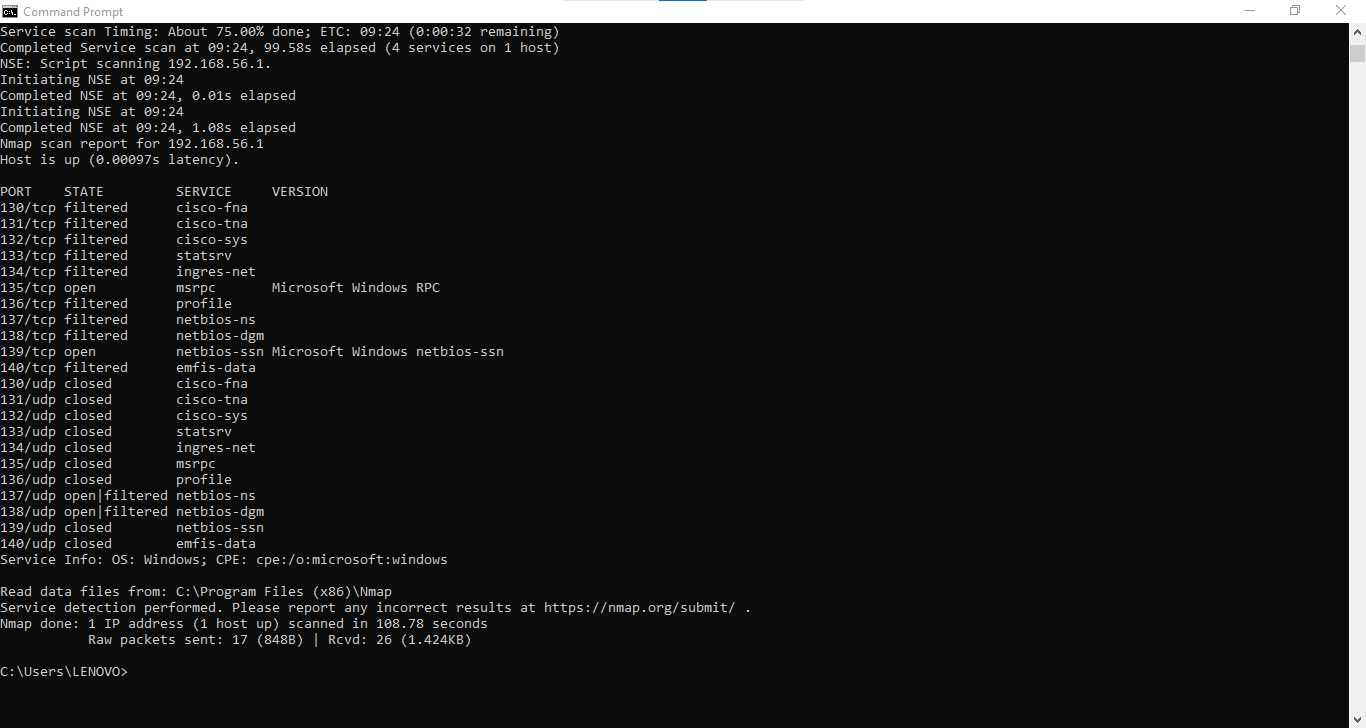


Below are the images of using the services filters in the wireshark application and using nmap on command line interface









**4. Reference/ Bibliography**

* Nmap: <https://nmap.org/>
* Wireshark: https://www.wireshark.org/
* Green, B., & Davis, J. (2017). Metasploit: The Penetration Tester's Guide. San Francisco, CA: No Starch Press.
* Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. San Francisco.
* Fyodor. (2018). Nmap: Network Exploration and Security Auditing Cookbook - Second Edition. Birmingham, UK: Packt Publishing.

GitHub Link: