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:-

1. RDP

2. FTP

3. SMTP

4. Netbios

5. SQL

Nmap is our Preferd Opensource Software

nmap is a powerful and widely-used network exploration and security auditing tool. The -Pn, -sV, and -sC options are used to customize the scan and perform various types of tests.

Here's a breakdown of what each option does:

- -Pn (no ping): By default, nmap will use ping to determine if a host is up or not. This option disables ping probes and assumes that the host is up, allowing nmap to attempt a scan regardless of whether the host is responding to ping requests.
- -sV (version detection): This option instructs nmap to attempt to determine the version of any services that are running on the scanned hosts. nmap will send a series of probes to each open port to try to identify the service, its version number, and any associated information that can be used to fingerprint the system.
- -sC (default script scan): This option tells nmap to run a set of default scripts against the target hosts. These scripts are designed to identify common vulnerabilities and security issues. The -sC option is a shorthand way to run a set of scripts that are commonly used for basic vulnerability assessment.

By combining these options, nmap will perform a scan that attempts to identify the version of services running on the target hosts and look for vulnerabilities using a set of default scripts. This can be a useful way to quickly identify potential security issues on a network.

a) RDP

To gather information about an RDP service, we can use a tool called "Nmap" which is a free and open-source network scanner. Nmap can help us to identify open ports, service versions, and OS details. To use Nmap, we can run the following command:

```
nmap -Pn -sV -sC <service-IP>
```

b) FTP

To gather information about an FTP service, we can use a tool called "Nmap" which is a free and open-source network scanner. Nmap can help us to identify open ports, service versions, and OS details. To use Nmap, we can run the following command:

```
nmap -Pn -sV -sC <service-IP>
```

c) SMTP

To gather information about an SMTP service, we can use a tool called "Nmap" which is a free and open-source network scanner. Nmap can help us to identify open ports, service versions, and OS details. To use Nmap, we can run the following command:

```
nmap -Pn -sV -sC <service-IP>
```

d) NetBIOS

To gather information about an NetBIOS service, we can use a tool called "Nmap" which is a free and open-source network scanner. Nmap can help us to identify open ports, service versions, and OS details. To use Nmap, we can run the following command:

```
nmap -Pn -sV -sC <service-IP>
```

e) SQL

To gather information about an SQL service, we can use a tool called "Nmap" which is a free and open-source network scanner. Nmap can help us to identify open ports, service versions, and OS details. To use Nmap, we can run the following command:

```
nmap -Pn -sV -sC <service-IP>
```

Overall Report

Service Name	Ip	Ports	Encryption	Banner	Netbios
RDP	65.0.89.91	3389	SSL	ms-wbt-server	EC2AMAZ-6QTV5EA
FTP	112.196.62.12	21	SSL2_RC4_128_WITH_MD5, SSL2_RC4_128_WITH_MD5	Microsoft ftpd	LPU
SMTP	49.156.110.205	587	SSL	Exim smtp	netbios-ssn
SQL	112.196.62.12	1433	SSL2_RC4_128_WITH_MD5, SSL2_RC4_128_WITH_MD5	Microsoft SQL Server 2012 SP4	LPU