**WEB APPLICATION PENTESTING**

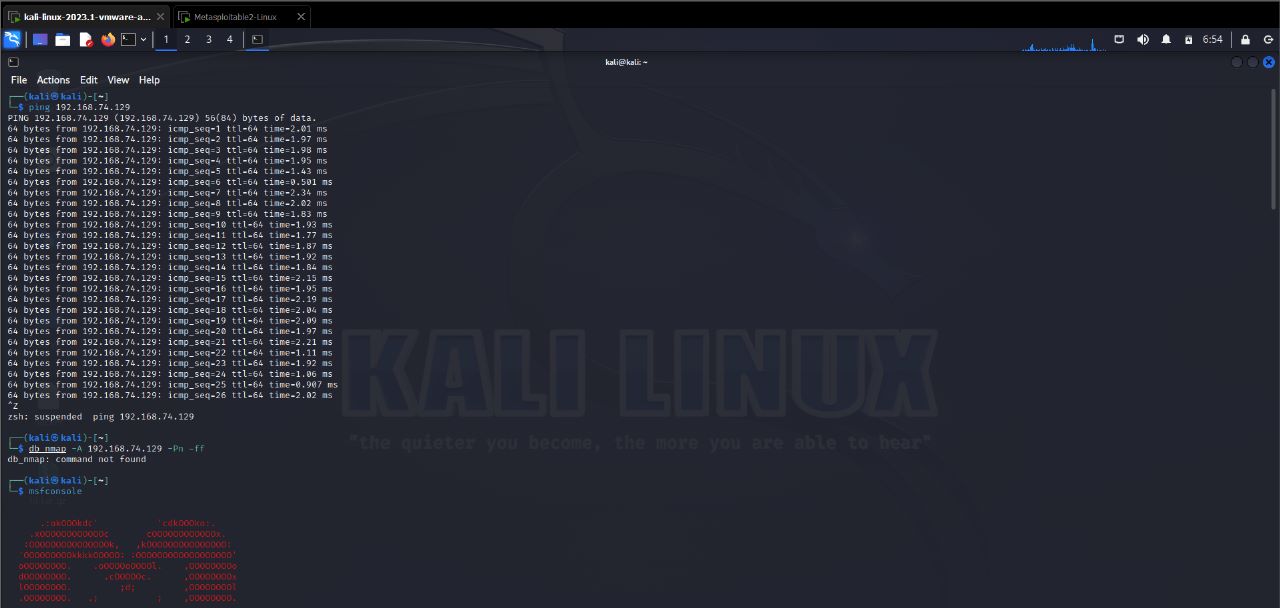
**GROUP – 2.6**

*M.SURYATEJA-20BCN7021*

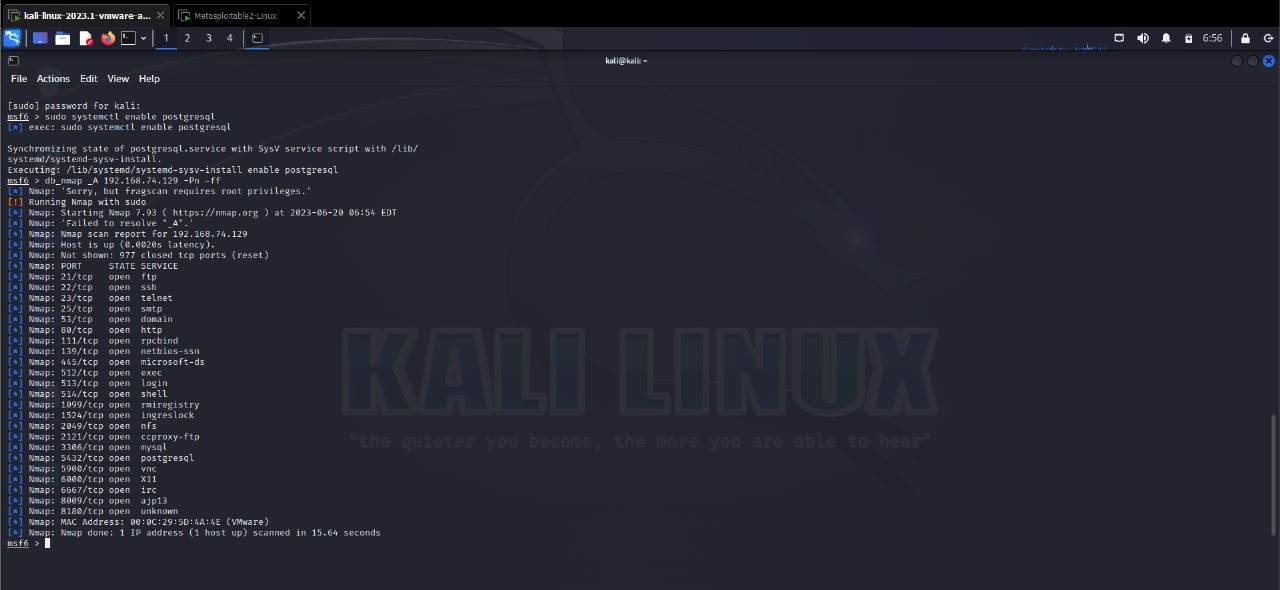
*G. PUSHKAR – 20BCN7119*

*G. KARTHIK – 20BCN7008*

**TARGET: METASPLOITABLE 2**







Open ports Information:

1. Port 21 (FTP - File Transfer Protocol):

- FTP is a standard network protocol used for transferring files between a client and a server.

- Port 21 is dedicated to FTP control traffic, which handles commands and responses between the client and server.

- It is commonly used for uploading and downloading files to and from a server.

- FTP can be vulnerable to attacks such as brute-forcing, command injection, or unauthorized access if not properly secured.

2. Port 22 (SSH - Secure Shell):

- SSH is a cryptographic network protocol that provides secure remote access to systems over an unsecured network.

- Port 22 is the default port used by SSH for establishing secure shell connections.

- It is commonly used for secure remote administration and file transfers.

- SSH provides strong encryption and authentication mechanisms, making it a more secure alternative to protocols like Telnet.

3. Port 23 (Telnet):

- Telnet is an unencrypted network protocol used for remote access to systems.

- Port 23 is the default port used by Telnet for establishing connections.

- Telnet transmits data in plain text, which makes it insecure, as credentials and other sensitive information can be intercepted.

4. Port 25 (SMTP - Simple Mail Transfer Protocol):

- SMTP is a protocol used for sending and receiving email messages between mail servers.

- Port 25 is the default port used for SMTP traffic.

- It handles the transmission of email messages from the sender's mail server to the recipient's mail server.

- SMTP can be vulnerable to attacks such as email spoofing, relay abuse, or unauthorized access if not properly secured.

5. Port 3306 (MySQL):

- MySQL is an open-source relational database management system.

- Port 3306 is the default port used for MySQL database traffic.

- It is used for client-server communication, query execution, and database administration tasks.

- MySQL databases can be targeted for attacks such as SQL injection, unauthorized access, or privilege escalation if not properly secured.

6. Port 8180:

- Port 8180 is often used as an alternative HTTP port.

- It can be used for web servers or applications that require a non-standard HTTP port.

- The specific usage or application running on this port may vary depending on the system's configuration.

7. Port 139 (NetBIOS - Network Basic Input/Output System):

- NetBIOS is an older networking protocol used for file sharing, print services, and network browsing in Windows systems.

- Port 139 is used for NetBIOS Session Service, which facilitates communication between devices on a network.

- It can be involved in certain types of attacks like NetBIOS enumeration or SMB (Server Message Block) exploitation if not properly secured.

8. Port 514:

- Port 514 is commonly associated with the Syslog protocol.

- Syslog is a standard protocol used for logging and collecting system events from network devices and servers.

- It is typically used for centralized logging and analysis of system logs.

- Syslog data can provide valuable insights into the security and operational status of systems.

9. Port 5432 (PostgreSQL):

- PostgreSQL is an open-source relational database management system.

- Port 5432 is the default port used for PostgreSQL database traffic.

- It is used for client-server communication, query execution, and database administration tasks.

- PostgreSQL databases can be targeted for attacks such as SQL injection, unauthorized access, or privilege escalation if not properly secured.

**VULNERABILITY:**

1. Port 21 (FTP):

- Weak authentication: FTP may suffer from weak or insecure authentication mechanisms, making it susceptible to brute force attacks or credential theft.

- Command injection: Improper handling of user-supplied input can lead to command injection vulnerabilities, allowing attackers to execute arbitrary commands on the FTP server.

2. Port 22 (SSH):

- Weak passwords: If SSH is configured with weak or easily guessable passwords, it can be vulnerable to brute force attacks.

- Misconfigured access controls: Improperly configured SSH access controls can result in unauthorized access or privilege escalation.

- SSH protocol vulnerabilities: older versions of the SSH protocol may have known vulnerabilities, so it's important to keep SSH software up to date.

3. Port 23 (Telnet):

- Lack of encryption: Telnet transmits data in plain text, allowing attackers to intercept sensitive information, including login credentials.

- Weak authentication: Telnet may use weak or insecure authentication mechanisms, making it vulnerable to password-based attacks.

4. Port 25 (SMTP):

- Email spoofing: SMTP can be abused to send forged or malicious emails, leading to phishing attacks or the spread of malware.

- Open mail relays: Misconfigured SMTP servers can be exploited as open relays, allowing attackers to use them for sending spam emails.

- Vulnerable mail server software: Outdated or unpatched mail server software can have known vulnerabilities that can be exploited by attackers.

5. Port 3306 (MySQL):

- SQL injection: If web applications or systems using MySQL do not properly sanitize user input, they can be vulnerable to SQL injection attacks.

- Weak or default credentials: MySQL databases can be at risk if default or weak credentials are used, allowing unauthorized access.

- Inadequate access controls: Improperly configured user permissions in MySQL can lead to unauthorized access or privilege escalation.

6. Port 8180:

- The vulnerabilities associated with Port 8180 can vary depending on the specific application or service running on that port. It is important to consider common web application vulnerabilities like XSS, SQL injection, or insecure direct object references (IDOR) if applicable to the service running on Port 8180.

7. Port 139 (NetBIOS) and 514 (Syslog):

- Misconfigured access controls: Improperly configured access controls on these ports can allow unauthorized access or information disclosure.

- Vulnerabilities in associated services: NetBIOS and Syslog services may have known vulnerabilities in their implementations, so it's important to keep them patched and updated.

8. Port 5432 (PostgreSQL):

- SQL injection: Just like with MySQL, PostgreSQL databases can be vulnerable to SQL injection attacks if user input is not properly sanitized.

- Weak or default credentials: Using weak or default credentials for PostgreSQL can lead to unauthorized access or privilege escalation.

- Inadequate access controls: Improperly configured user permissions in PostgreSQL can result in unauthorized access or data leakage.