Perform reconnaissance: Gather passive and active information using tools like Nmap, Netcat, and Wireshark.

Identify vulnerabilities: Analyze gathered data to find weaknesses in the target system or network.

Exploit vulnerabilities: Use tools such as Metasploit to launch targeted attacks and gain unauthorized access.

Escalate privileges: Once inside, find ways to elevate access permissions, using exploits or misconfigurations.

Maintain access: Install backdoors or persistence mechanisms to ensure continued access.

Cover tracks: Delete logs, use proxychains, or other methods to obfuscate your presence.

Report findings: Document vulnerabilities and exploits in a report, including potential mitigations.