ops-201d12 Team Phamtom System Selection

Team Members:

- Bradley Baack
- Cody Blahnik
- Ethan Pham
- Julian Pena

Scenario

Your MSSP has been contracted to perform a one-time adversary emulation engagement for SimCorp, a financial asset management company. The CTO is concerned with the security posture of the company's cloud systems, after having already experienced sensitive data exposure as a result of misconfiguration of an employee's instance. Depending on the quality of your company's findings, SimCorp may consider a long term agreement to have your MSSP defend its cloud systems.

You've been tasked with enumerating the target network from a "black box" position (minimal knowledge of the target environment) starting with a foothold on a single endpoint. One of your goals is discovering as many vulnerabilities as you can and documenting them in accordance with community resources such as CWE and CVSS. You'll also get to apply TTPs you've learned throughout this course and perform exploits as the opportunities present themselves. Document how you went about executing TTPs and whether they were successful or not.

Red Team Staging

You will be provided with a single compromised endpoint instance as well as VPN access to its LAN to facilitate tool execution. For example, if you wanted to perform attacks from Kali Linux, you would activate an OpenVPN connection from Kali Linux to the target network.

Red Team Objectives (RTOs)

- **RTO1:** Enumerate the target network, gleaning as much information as possible about the various hosts and their configurations. Document in detail what tools were used and how much you were able to reveal.
  - **RTO1a:** Create a professional network topology of the target environment for inclusion in your final report.

- **RTO2:** Discover vulnerabilities on targets hosts on the network. There will be at least one web application for you to discover and test against, in addition to several other instances running various operating systems with unknown configurations.
- **RTO3:** Build/customize and utilize at least one custom Python tool to aid in your team's offensive efforts.
- **RTO4:** Exploit and gain access to as many host instances as possible, and as deeply as possible.

While hacking is great fun, be sure to take plenty of screenshots and document what worked and didn't work in order to produce a high quality report deliverable. Remember the goal is to help your client understand their risks.

Systems Selection

1. Kali Linux

Fit into Scenario: Kali Linux is a versatile penetration testing platform that provides a wide range of tools for network enumeration, vulnerability scanning, and exploitation, which are crucial for our red team objectives.

Problem/Pain Point Solved: It enables comprehensive security assessments by offering a centralized platform for running different tools and scripts, ensuring efficient and effective penetration testing.

MVP Definition:

- Installation and configuration of Kali Linux.
- Successful VPN connection to the target network.
- Basic enumeration using tools like Nmap and Nikto.

2. OpenVPN

Fit into Scenario: OpenVPN will be used to establish a secure connection to the target network, allowing us to perform remote penetration testing as if we were directly connected to the internal network.

Problem/Pain Point Solved: It ensures secure and encrypted communication between our testing environment and the target network, maintaining the confidentiality and integrity of our testing activities.

MVP Definition:

- Setup and configuration of OpenVPN on the Kali Linux instance.
- Successful connection to the target network.
- Verification of network access through the VPN.

3. Metasploit Framework

Fit into Scenario: Metasploit is an essential tool for discovering and exploiting vulnerabilities. It will be used for vulnerability scanning, exploitation, and post-exploitation tasks.

Problem/Pain Point Solved: Provides a comprehensive suite of tools for exploiting vulnerabilities, automating the process of gaining access to target systems, and conducting post-exploitation activities.

MVP Definition:

- Installation and setup of Metasploit.
- Successful exploitation of at least one vulnerability on a target host.
- Documentation of the exploitation process and results.

4. Custom Python Tool

Fit into Scenario: A custom Python tool will be developed to automate specific tasks or create tailored exploits, enhancing our offensive capabilities.

Problem/Pain Point Solved: It allows for flexibility and customization in our penetration testing efforts, enabling us to address unique challenges and exploit scenarios specific to the target environment.

MVP Definition:

- Development of a basic custom Python tool.
- Successful execution of the tool in a relevant context (e.g., enumeration, exploitation).
- Documentation of the tool's purpose and functionality.

Minimum Viable Product (MVP) Definition

The minimum required for demo day includes:

- Basic installation and configuration of essential tools (Kali Linux, OpenVPN, Metasploit).
- Successful enumeration of the target network with initial findings documented.
- At least one successful exploitation documented with screenshots.
- A custom Python tool developed and utilized in the engagement.
- A professional network topology diagram.
- A draft of the penetration test report with preliminary findings and documentation of TTPs.