Johannes Castellano

Research Summary

Metasploit Framework

Metasploit boasts several key features that contribute to its widespread adoption.

1. **Exploit modules** contain the necessary code to exploit specific vulnerabilities found in systems or applications, ultimately aiming to gain unauthorized access.
2. **Payload modules** define the shellcode executed on the target system after successful exploitation, specifying how the attacker will interact with and control the compromised system.
3. **Auxiliary modules** encompass a broad range of tools that perform tasks unrelated to direct exploitation, such as scanning networks, fuzzing applications, and gathering information about targets.
4. **Post-exploitation modules** are designed to be run after a system has been successfully compromised, enabling further actions like gathering credentials, escalating privileges, or maintaining persistence.
5. Lastly, **NOP generator modules** produce sequences of no-operation bytes that can be used to pad memory buffers, potentially helping bypass intrusion detection and prevention systems.

Cobalt Strike

Cobalt Strike offers a suite of key features tailored for advanced adversary simulation.

1. **Covert communication**, primarily facilitated through its **Beacon** payload, is a central aspect. Beacon establishes stealthy communication channels designed to bypass network defenses and maintain persistent access to compromised systems. It supports various protocols, including HTTP, HTTPS, and DNS, allowing for flexible and covert communication with the attacker's command and control server.
2. **Cobalt Strike leverages Beacon Object Files (BOFs)** for post-exploitation activities. These are compiled C programs that can be executed within a Beacon process, extending its capabilities for advanced tasks while potentially offering greater stealth compared to traditional DLL injection techniques.
3. A particularly notable feature is **Malleable C2**, which allows operators to extensively customize the network indicators of Beacon traffic. This customization includes modifying user-agent strings, HTTP headers, and URIs to blend in with legitimate network

traffic or mimic the communication patterns of specific known malware, significantly complicating detection efforts.

4. **Browser pivoting** is another powerful feature that enables operators to bypass two-factor authentication mechanisms and access websites as compromised users through the attacker's own browser. This technique is invaluable for lateral movement and gaining access to protected resources.
5. For team-based operations, Cobalt Strike's **team servers** allow for real-time communication and shared control over compromised systems among multiple red team members, enhancing collaboration and efficiency during complex engagements.
6. **Process injection** is a critical capability, and Cobalt Strike employs various sophisticated techniques to inject malicious code into legitimate processes. This allows for the execution of malicious code within the context of trusted processes, aiding in evasion and potentially privilege escalation.

Empire

Several key features drive Empire's functionality.

1. It utilizes **PowerShell/Python/C# agents** that can be deployed across Windows, Linux, and macOS environments to establish communication with the C2 server. These agents enable the remote execution of commands and the deployment of various modules for post-exploitation.
2. The framework has a massive library of **modular post-exploitation capabilities**. These modules range from simple tools like *keyloggers* to more advanced ones like Mimikatz for credential theft, as well as modules for *privilege escalation*, *lateral movement* within the network, and *data exfiltration*.
3. Like Cobalt Strike, Empire offers adaptable communication profiles, often called **Malleable C2 profiles**. These profiles allow operators to customize the network traffic generated by the agents to evade detection by network security monitoring tools, making the C2 communication appear less conspicuous.
4. Empire also supports **multi-user operations**, enabling multiple attackers to simultaneously manage and interact with a network of compromised systems through a centralized interface. This feature enhances the efficiency and effectiveness of red team operations.
5. To maintain a persistent presence on compromised systems, Empire provides various **persistence mechanisms**, such as creating scheduled tasks and modifying *registry keys*, ensuring that the agents continue to run even after system reboots.

Comparison Table

Feature	Metasploit	Cobalt Strike	Empire
Supported Platforms	Windows, Linux, macOS, Android, others	Windows, Linux, macOS (Teamserver) (Implied)	Windows, Linux, macOS
Primary Programming Language	Ruby	Java	Python 3 (Server), PowerShell, Python, C# (Agents)
Licensing Model	Open-source (BSD 3-clause)	Commercial (Annual License)	Open-source (Archived GitHub repo, forks exist)
Key C2-related Features	Meterpreter, Auxiliary Modules (Scanners, Sniffers), Post-Exploitation Modules, Resource Scripts	Beacon, Malleable C2, BOFs, Browser Pivoting, Redirectors	Agents (PowerShell, Python, C#), Malleable C2, Persistence Modules, Lateral Movement Modules

Disclaimer

To effectively manage the extensive literature, Gemini Deep Research was utilized to conduct research and to organize the material. Grammarly was also used to ensure that the message was being conveyed clearly and concisely.