Command and Control (C2) Traffic Generation and Detection Pentester

Table Of Contents

- 1. Executive Summary
- 2. Scope
- 3. Detailed Setup
- 4. Achieving Scalability
- 5. Setup Issues
- 6. Testing
- 7. Observations
- 8. Recommendations
- 9. Encrypted C2 Traffic: Detection Challenges and Enhancements
  - Overview
  - Detection Enhancements
    - Initial Assessment
    - JA4 Hash Integration
    - ALPN Protocol and TLS Certificate Analysis
    - Domain Name Analysis
  - Outcomes and Recommendations

1. Executive Summary

This white-box penetration test aims to assess BeCode's ability to detect and respond to a simulated Command and Control (C2) attack. The BeCode security team (blue team) will have full knowledge of the test objectives, methodology, and timeline. The test will leverage a controlled C2 infrastructure within the BeCode network, with Caldera agents simulating compromised endpoints. Network security monitoring and intrusion detection will be conducted using pfSense and Suricata, with Splunk serving as the central log analysis platform. Findings and recommendations from this engagement will guide BeCode in enhancing its security posture against sophisticated C2-based attacks.

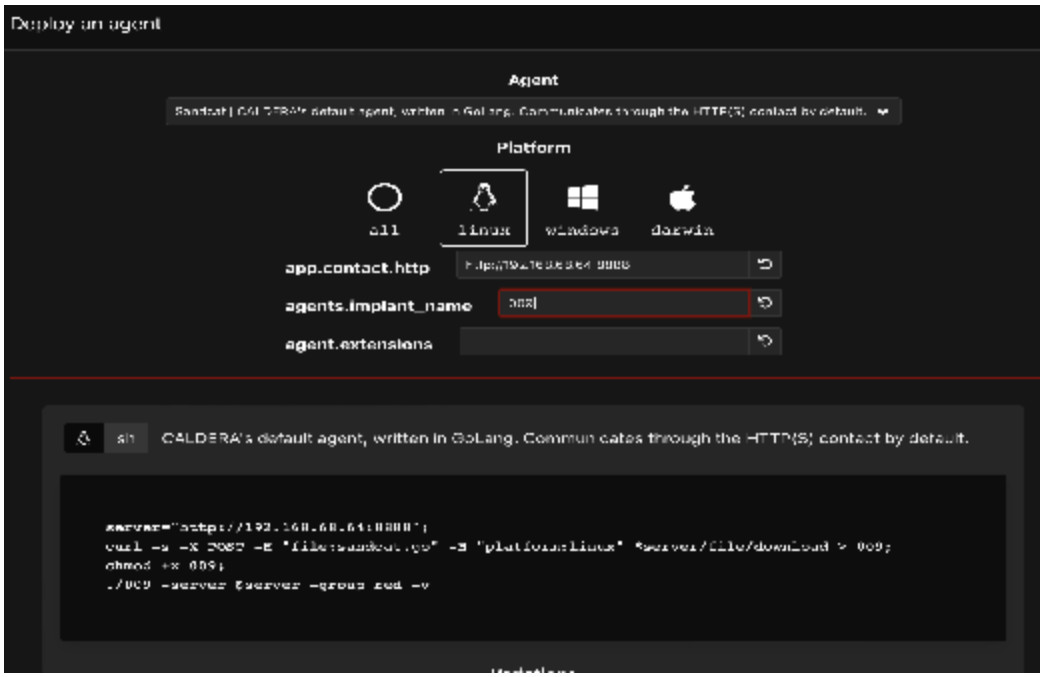
2. Scope

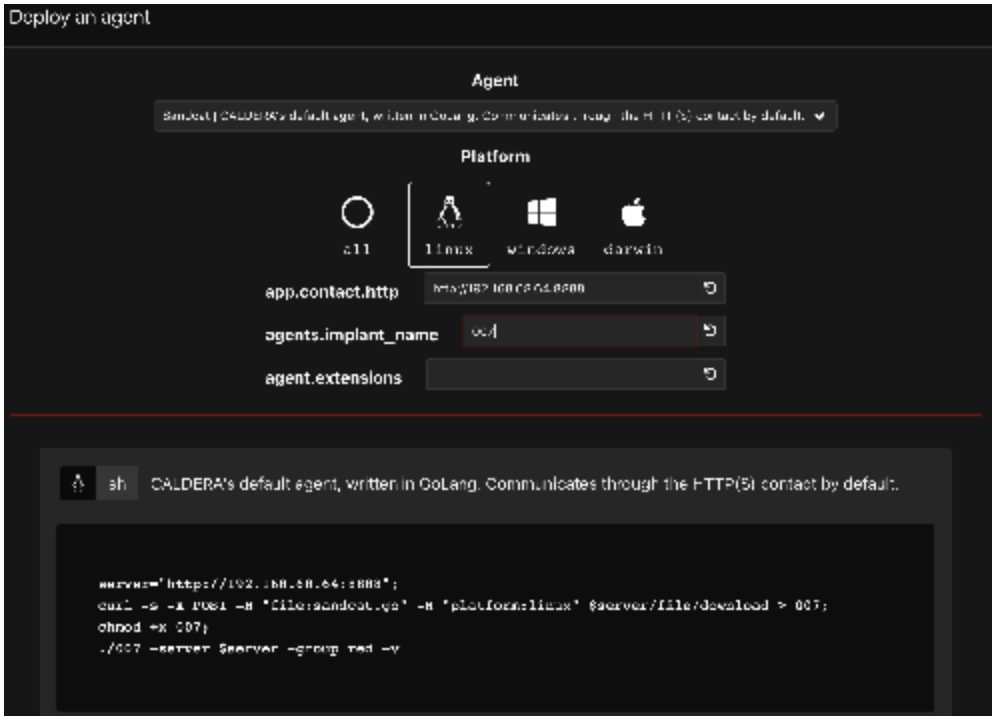
- In-Scope Activities:
  - Deployment and configuration of a C2 server within the BeCode network.
  - Simulation of compromised endpoints using Caldera agents, adhering to predefined C2 behavior rules.
  - Collection and analysis of logs from pfSense, Suricata, and other relevant security sources using Splunk.
  - Integration of threat intelligence feeds (abuse.ch) into Splunk for real-time detection.
  - Evaluation of pfSense firewall rules and Suricata IDS configurations in relation to C2 traffic detection and prevention.
  - Assessing the scalability of the C2 infrastructure and detection mechanisms.
- Out-of-Scope Activities:
  - Active exploitation of vulnerabilities to gain initial access.
  - Lateral movement or privilege escalation within the BeCode network.
  - Attempts to exfiltrate sensitive data.
  - Physical security assessments.

3. Detailed Setup

- **C2 Infrastructure: Caldera**
- Framework: Caldera, an open-source platform designed for adversary emulation, will serve as the C2 infrastructure for this pentester. Caldera's ability to automate attack simulations based on MITRE ATT&CK techniques will enable realistic and comprehensive testing of BeCode's security posture.
- Server Configuration:
  - Deployment: The Caldera server will be deployed on a dedicated virtual machine within the Proxmox environment.
  - Communication: Caldera primarily utilizes HTTP for C2 communication, ensuring secure and encrypted channels between the server and the agents.
  - Abilities: Caldera's capabilities include executing various adversary behaviors (abilities) on compromised systems, such as reconnaissance, lateral movement, and data exfiltration.
  - Plugins: We will leverage plugins within Caldera to customize and extend its functionality, enabling us to tailor the attack simulations to BeCode's specific environment and potential threats.
- **Endpoint Simulation: Caldera Agents**

- Deployment: Two virtual machines within the Proxmox environment will be designated as compromised endpoints. Caldera agents will be deployed on these VMs to simulate adversary presence and execute commands from the C2 server.
- Configuration: The Caldera agents will be configured to communicate with the Caldera server over HTTP.
- Adversary Behavior: We will use Caldera's adversary emulation capabilities to define and execute specific attack scenarios, mimicking the tactics, techniques, and procedures (TTPs) of real-world adversaries





- **Network Security & Monitoring**

- pfSense Firewall: pfSense will be configured as the network perimeter, acting as the first line of defense.Firewall rules will be implemented to control and monitor network traffic, potentially including restrictions on outbound connections to known malicious domains or IP addresses.
- Suricata IDS: Suricata, an open-source intrusion detection system, will be integrated with pfSense to analyze network traffic in real-time. Suricata rules and signatures will be customized to detect C2 communications,anomalous network behavior, and other indicators of compromise.
- Splunk: Splunk will serve as the centralized log management and analysis platform. It will ingest logs from pfSense, Suricata, the Caldera server, and other relevant security sources. Custom dashboards and alerts will be created within Splunk to facilitate the detection and investigation of C2 activity.
- Threat Intelligence Integration: Threat intelligence feeds from abuse.ch will be incorporated into Splunk to enhance its detection capabilities. This will enable the identification of known malicious C2 infrastructure and associated indicators.
- **Note:**
- Specific technical details regarding the Caldera server configuration, agent deployment, pfSense rules, Suricata signatures, and Splunk queries will be further elaborated upon as the setup progresses and specific attack scenarios are defined.

4. Achieving Scalability

To ensure the scalability of the C2 simulation and detection environment, several strategies could be implemented:

- Modular Setup: The infrastructure was designed with modularity in mind, allowing for the easy addition or removal of components like C2 servers, endpoint agents, and monitoring tools. This modular approach facilitates scaling the environment up or down as needed.
- Automated Deployment potential: Automated scripts could be used to deploy and configure Caldera agents, the C2 server, and the network security infrastructure. This automation ensures consistency in setup and enables rapid scaling across multiple virtual machines if required.
- Cloud Integration Potential: Although the current setup utilized an on-premises Proxmox environment, the infrastructure could be migrated to a cloud-based platform, offering enhanced scalability, flexibility, and resource allocation based on demand.

5. Setup Issues

During the setup phase of the penetration test, we encountered a challenge related to the firewall configuration that impacted the initial communication between the Caldera C2 server and the deployed agents.

Issue:

- Firewall Restrictions: The pfSense firewall, initially configured with a default deny-all policy for outbound traffic, blocked the Caldera agents' attempts to establish a connection with the C2 server. This resulted in communication failures and hindered the execution of Caldera abilities.

Solution:

- Collaborative Resolution: We collaborated with the BeCode security team (blue team) to identify and resolve the issue. Together, we analyzed the firewall logs and configuration and determined that the defa ult deny-all policy was preventing the necessary outbound traffic.
- Firewall Rule Adjustment: In collaboration with the blue team, we created rules on pfSense to allow outbound traffic from the Caldera agents (using their shared IP address: 192.168.68.64) to the C2 server on the designated ports (e.g., 443 for HTTP communication).
- Verification: After implementing the firewall rule changes, we re-tested the communication between the agents and the C2 server, confirming successful connectivity and the ability to execute Caldera abilities.

Lessons Learned:

- Proactive Communication: Early communication and collaboration with the blue team is crucial to identify and address any potential conflicts or restrictions imposed by the existing security infrastructure.
- Firewall Rule Review: A thorough review of firewall rules before initiating the pentest, ideally in collaboration with the blue team, can help prevent unexpected communication issues and streamline the setup process.
- Flexibility and Adaptation: Be prepared to adapt the test environment and configurations as needed to overcome challenges and ensure the successful execution of the pentest objectives.

Note:

- The specific firewall rule adjustments made will be documented in detail in the final pentest report.
- This experience highlights the importance of clear communication and collaboration between the red team and blue team to effectively navigate potential obstacles and ensure a successful pentest engagement.

6. Testing

The testing phase was conducted to evaluate the effectiveness of our test platform’s network security measures in detecting and responding to C2 communications.

- Simulated C2 Communications: The Caldera agents, deployed on virtual machines within the Proxmox environment, were configured to initiate regular beaconing to the C2 server over HTTP (port 8888). The frequency and behavior of these communications were designed to mimic realistic adversary activities.
- Log Analysis and Correlation: Logs collected by Splunk from pfSense and Suricata were analyzed. Custom search queries and dashboards were used to identify and correlate indicators of compromise (IOCs) associated with the simulated C2 activity.

7. Observations

Throughout the testing phase, several key observations were made:

- Firewall and IDS Effectiveness: The pfSense firewall and Suricata IDS were effective in detecting and logging C2-related activities. The custom rules and signatures tailored to the Caldera simulation proved valuable in identifying malicious traffic.
- Log Management and Analysis: Splunk's centralized log management system was instrumental in aggregating and correlating data from multiple sources. The use of custom dashboards and queries facilitated rapid detection and response.
- Potential Evasion Techniques: While the current setup successfully detected the simulated C2 activities, it was observed that more sophisticated adversaries could potentially evade detection by employing techniques such as encrypted communications, domain fronting, or more subtle beaconing intervals.
- Team Coordination: Effective communication between the red team (pentesters) and the blue team was crucial in navigating setup challenges and ensuring the success of the test. This collaboration also highlighted areas for potential improvement in operational procedures.

8. Recommendations

Based on the findings from the C2 simulation exercise, the following recommendations are made to enhance security posture:

- Enhance Detection Capabilities:
- Advanced IDS Rules: Implement more advanced Suricata rules that account for obfuscated or encrypted C2 traffic. Regularly update these rules to incorporate the latest threat intelligence.
- Machine Learning: Consider integrating machine learning-based anomaly detection into Splunk to identify deviations from normal network behavior, which could indicate sophisticated C2 activities.
- Improve Network Segmentation:

- Micro-Segmentation: Enhance network segmentation by implementing micro-segmentation within the network. This would limit lateral movement opportunities for adversaries and contain potential breaches.
- Harden Endpoint Security:
- Endpoint Detection and Response (EDR): Deploy EDR solutions on all endpoints to provide deeper visibility into endpoint activities and enable rapid response to detected threats.
- Host-Based Firewalls: Configure host-based firewalls on endpoints to restrict unnecessary outbound communications, particularly those directed to unknown external IPs.
- Continuous Threat Intelligence Integration:
- Expand Intelligence Feeds: Incorporate additional threat intelligence feeds into Splunk to broaden the scope of detected threats. This includes integrating commercial threat intelligence services that offer more extensive coverage of C2 infrastructure.
- Regular Updates: Ensure that threat intelligence feeds are regularly updated and that Splunk queries and dashboards are modified accordingly to reflect the latest threat landscape.
- Ongoing Training and Exercises:
- Blue Team Training: Provide ongoing training for the blue team in advanced detection techniques, including recognizing and responding to evasion tactics used by sophisticated adversaries.
- Regular Red Team Exercises: Conduct regular red team exercises to continuously test and improve our detection and response capabilities.
- Investigate Firewall Rule Management:
- Firewall Rule Review Process: Establish a regular review process for firewall rules to ensure they are optimized for both security and functionality.

9. Encrypted C2 Traffic: Detection Challenges and Enhancements

Overview

In this red team exercise, Caldera agents were deployed using HTTPS encryption for their command-and-control (C2) communications, simulating the tactics of advanced adversaries who use encrypted channels to conceal their activities. The objective was to challenge and enhance the blue team’s ability to detect such encrypted C2 traffic.

Detection Enhancements

Initial Assessment

To emulate adversarial behavior, the blue team integrated a new correlation search into the Splunk environment aimed at detecting HTTPS-based beaconing activity. However, the initial efforts revealed a significant challenge—distinguishing between legitimate HTTPS traffic and malicious beaconing, as indicated by a high rate of false positives. This highlighted the inherent complexity in detecting encrypted threats, a core objective of the red team exercise.

JA4 Hash Integration

In response to the initial difficulties, the blue team incorporated JA4 hashes into their detection strategy. By leveraging Zeek on the pfSense firewall, which provides native support for JA4 hash generation, the blue team was able to create unique fingerprints for TLS client configurations. These fingerprints were then analyzed to identify suspicious patterns potentially indicative of red team operations or actual threats.

ALPN Protocol and TLS Certificate Analysis

In addition to JA4 hash analysis, the blue team scrutinized the Application-Layer Protocol Negotiation (ALPN) used in HTTPS connections. The presence of uncommon or custom ALPN protocols was flagged as a potential indicator of beaconing, simulating the techniques adversaries use to evade detection. Furthermore, the blue team conducted an in-depth analysis of TLS certificates, focusing on anomalies such as self-signed certificates or certificates issued by unrecognized authorities, which are often employed in red team scenarios to bypass security controls.

Domain Name Analysis

Lastly, the blue team analyzed the domain names associated with HTTPS connections for signs of malicious activity. This included checking for typosquatting, unusual patterns, or links to known threat actors—methods adversaries often use to obscure their C2 infrastructure.

Outcomes and Recommendations

The enhancements implemented by the blue team during this phase significantly improved their ability to detect encrypted beaconing activity, including traffic from the Caldera C2 server. However, the exercise also highlighted the ongoing challenge of balancing detection accuracy with the risk of false positives. Notably, some legitimate applications, such as Splunk and Tailscale, exhibited behavior similar to malicious beaconing, which complicated the detection process.

To further enhance detection capabilities and reduce false positives, the following recommendations are proposed:

- **Baseline Development:** The blue team should establish a baseline of trusted JA4 hashes for known good applications within the network. This baseline will help filter out benign traffic, allowing for more focused detection of potential threats.
- **Contextual Analysis:** The blue team should adopt a contextual approach when analyzing JA4 hashes, ALPN protocols, and other indicators. Factors such as source and destination IPs, traffic patterns, and other contextual information should be considered to better distinguish between benign and malicious activity.
- **Threat Intelligence Integration:** The blue team should integrate threat intelligence feeds to identify known malicious JA4 hashes, ALPN protocols, or domain names, improving the ability to filter out non-threatening traffic.
- **Continuous Monitoring and Updates:** The blue team should regularly review and update detection methodologies to stay ahead of evolving threats. This includes refreshing threat intelligence, refining detection rules, and continually assessing the effectiveness of current techniques.

By implementing these recommendations, the blue team can significantly improve the accuracy of detecting encrypted C2 traffic, enhancing the network's resilience against sophisticated adversarial attacks.