ICS 344: Information Security
Course Project

<ICS 344 Course Instructors 241>

Formally assigned: Oct 20, 2024
Due: Nov 20, 2024

Project Title

Offensive Security, Cyber Deception, and SIEM

Copyright and Usage Notice

1 Overview

This project provides hands-on experience in offensive security, cyber deception using honeypots, security event correlation and analysis through Security Information and Event Management (SIEM), and optionally defensive strategy formulation. Use a SIEM platform to collect and visualize data from both the victim and honeypot environments. Set up an attacker-victim environment, compromise a specific service, and replicate the attacks against a honeypot that mimics the service. Then, use a SIEM platform to collect and visualize data from both the victim and honeypot environments.

The deadline for forming groups of 3 to 4 members is on October 24.

2 Learning Outcomes

By the end of this project, students will:

1. Gain hands-on experience with offensive security tools.
2. Understand the value of honeypots in cybersecurity.
3. Develop skills in security event correlation using SIEM.
4. Explore and propose defensive strategies (Optional).

3 Project Phases

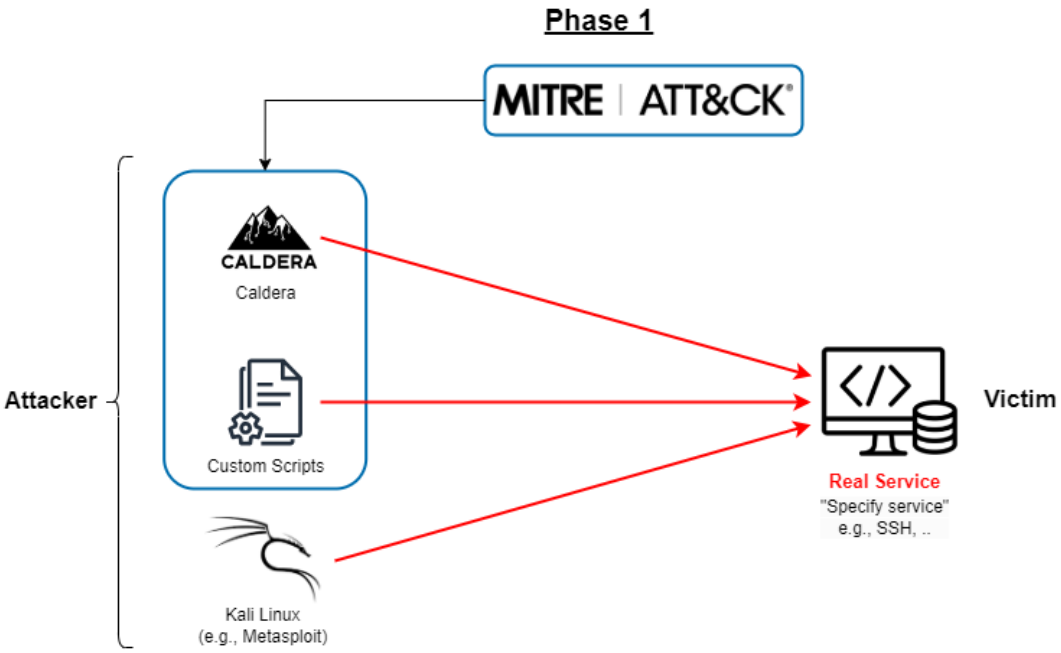
Phase 1: Setup and Compromise the Service

In this phase, you will create two virtual environments:

1. **Victim Environment:** Configure a machine hosting the target service.
2. **Attacker Environment:** Use various tools to compromise the service.

Examples of Target Services

- Web Server (e.g., Apache, Nginx)
- Database Server (e.g., MySQL, PostgreSQL)
- Remote Desktop Protocol (RDP)
- File Transfer Protocol (FTP) Server
- Email Service (e.g., Microsoft Exchange)
- SSH Service
- and more...



Tasks for Phase 1

- **Task 1.1:** Compromise the service using Caldera (an automated red-teaming framework).
- **Task 1.2:** Use Kali Linux and tools like Metasploit to compromise the service.
- **Task 1.3:** Write your own scripts/commands to compromise the service:
  - Guided by relevant MITRE ATT&CK TTPs for that specific service.
  - Or, create a novel TTP to demonstrate creativity and understanding.

The deadline for submitting phase 1 is on November 5.

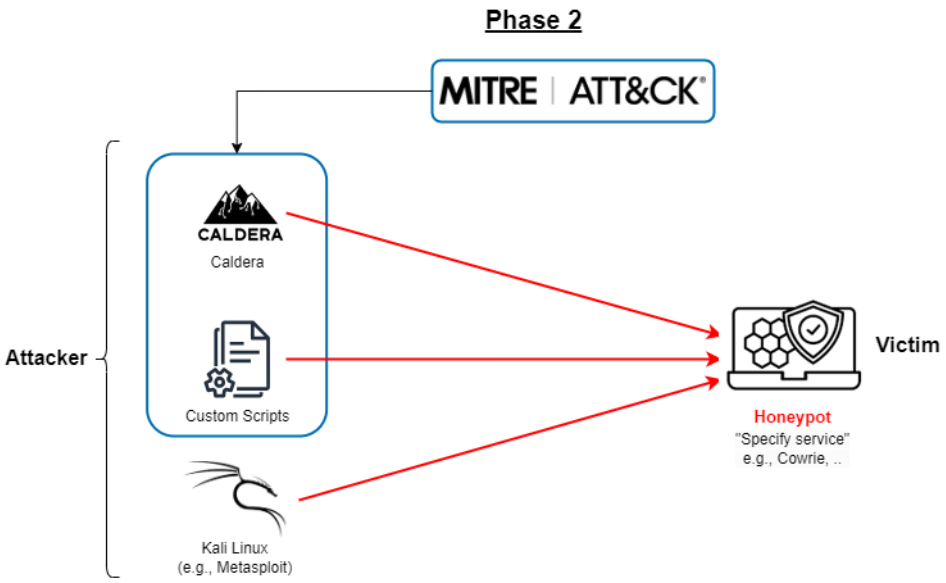
Phase 2: Honeypot Setup and Realism Evaluation

In this phase, you will replicate the victim environment using a honeypot that mimics the service attacked in Phase 1. Your task is to compare the honeypot's behavior against the actual service under identical attacks.

Tasks for Phase 2

- Replicate the attacks (Tasks 1.1–1.3) on the honeypot.
- Evaluate the honeypot's realism by considering:
  - How closely it mimics the actual service.
  - The time required to complete each attack.
  - The resource usage (CPU, memory, etc.) during each test.

The deadline for submitting phase 2 is on November 12.



Phase 3: Visual Analysis with a SIEM Dashboard

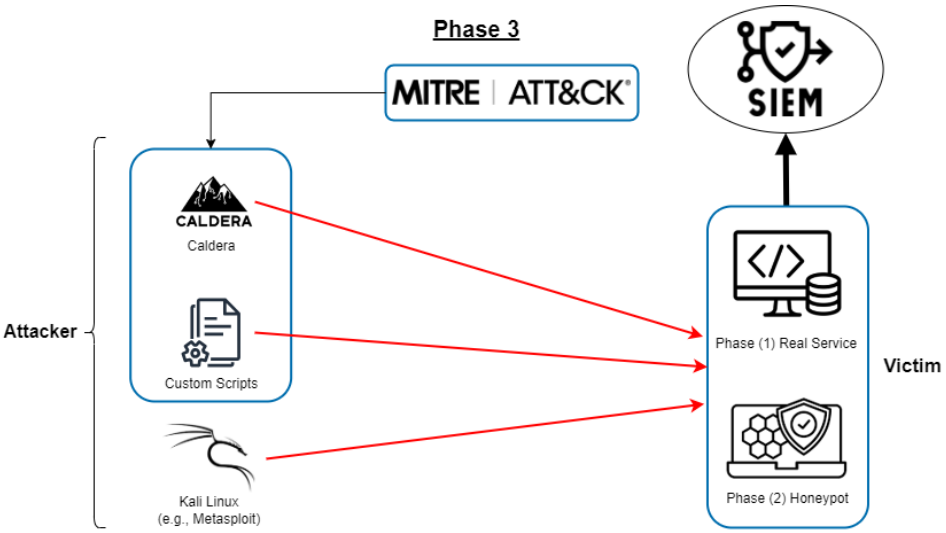
Use a SIEM platform to collect and visualize data from both the victim and honeypot environments.

Tasks for Phase 3

- Integrate logs and metrics from both environments into the SIEM platform.
- Visualize the attacks and compare the data from the victim and honeypot environments.
- Analyze and document key insights, such as detection, event correlation, and any differences between the victim and honeypot.

Recommended SIEM Tools

- Wazuh (Open Source Security Platform)
- Splunk
- ELK Stack
- Graylog
- and more...



Phase 4 (Optional): Defensive Strategy Proposal

In this optional phase, propose a defense mechanism for the service:

1. Use Caldera to implement automated defenses.
2. Develop your own defensive scripts, enhancing or creating new techniques beyond existing MITRE ATT&CK TTPs.

4 Report Guidelines

Each team must submit a structured report covering the following:

1. Technical Knowledge

Describe the technical aspects of your project setup in detail, including:

- **Setup Configuration:**
  - How did you configure Caldera, the honeypot, and the SIEM platform?
  - What TTPs did you select and how were they applied?
  - Which Kali tools and custom scripts did you use, and how were they integrated into the attack?
- **Service Selection:**
  - Which services did you target and why?
  - Why did you select these specific services for this project?
- **Challenges and Bugs:**
  - What challenges or bugs did you encounter during the setup and attack execution?
  - How did you overcome these issues?
- **Best Practices and Recommendations:**
  - Based on your experience, what best practices would you recommend for future students working on a similar project?
- **Project Feedback:**
  - How much did you learn from this project? Provide a brief reflection on your experience?
  - Do you recommend this project for use in future course cycles?
- **Learning Resources:**
  - What learning resources did you rely on during the project?
  - Specify the exact platforms or materials you used, such as `edX`, `Coursera`, `YouTube`, official documentation, or other relevant sources.

2. Attack Details (Tools, TTPs Used, etc.)

Here, you are required to compare the different approaches and tools used in Tasks 1.1 - 1.3. Critically evaluate the strengths, weaknesses, and practical implications of using Caldera, Kali tools, and custom scripts/commands guided by MITRE ATT&CK TTPs. To conduct the comparison, address the following questions:

- **Effectiveness and Success Rate:**
  - Which tool/approach was most effective at compromising the service?
  - Were there any limitations in one method that other methods overcame?
  - How successful were you in replicating a real-world attack scenario?
- **Ease of Use and Automation:**
  - How easy or difficult was it to use Caldera compared to Kali tools and manual scripting?
  - How did the level of automation in Caldera affect the overall process?
  - Which approach required the most manual intervention or expertise?
- **Time and Effort:**
  - Which task took the least/most time to execute?
  - How does automation (Caldera) compare with manual efforts in terms of efficiency?
  - Did the use of custom scripts require significant debugging or trial-and-error?
- **Learning Curve and Skill Requirements:**
  - Which approach was the easiest to learn and apply?
  - How did previous experience (e.g., with Kali or scripting) impact the outcomes?
  - What new skills or insights did each task provide?

- **Flexibility and Creativity:**
  - How flexible were Caldera and Kali tools in supporting creative/novel techniques?
  - Were there limitations in using pre-built tools that custom scripting could overcome?
  - How did your novel TTPs compare to the predefined MITRE ATT&CK techniques?
- **Detection and Stealth:**
  - Which approach was most likely to bypass detection mechanisms?
  - How easily would each method be detected by a SIEM or honeypot?
  - Were certain methods noisier or stealthier than others?
- **Alignment with MITRE ATT&CK Framework:**
  - How well did each approach map to the MITRE ATT&CK TTPs?
  - Were there any gaps or deviations in existing tools when compared to the desired TTPs?
  - How did developing your own TTP contribute to a better understanding of adversary behavior?
- **Impact on the Target System:**
  - Which approach caused the most/least disruption to the service?
  - Were any unintended consequences (e.g., service crash, instability) observed?
- **Future Application and Improvement:**
  - Which method would you recommend for a future red-teaming engagement and why?
  - What could be improved in each approach to make it more effective or efficient?
- **Show Snapshots:**
  - Provide snapshots of system logs, reports, and dashboards generated during your experiments.
  - Ensure the snapshots are annotated to highlight key findings and observations.

3. Honeypot Comparison Results

- Include a detailed evaluation of time, realism, and resource usage when the honeypot was subjected to the same attacks as the victim environment.
- Discuss how closely the honeypot mimicked the real service and any differences observed.

4. SIEM Dashboard Screenshots and Analysis

- Provide screenshots from your SIEM platform showing logs and metrics from both the victim and honeypot environments.
- Document key insights from attack visualizations, including event correlation and detection differences between environments.
- Ensure the snapshots are annotated to highlight key findings and observations.

5. Defense Techniques (Optional)

If participating in Phase 4, propose a defense mechanism using either Caldera or custom scripts, along with reasoning and technical details.

5 Deliverables

- **Format:** Submit a PDF report including relevant screenshots, graphs, and code snippets.
- **Length:** The report should be well-organized and concise (around 10-20 pages).
- **Presentation:** Teams should present key findings.
- **Demo:** Teams should show a demo.
- **Source:** Teams may be asked to submit the source and setup.

The deadline for submitting deliverables is on November 20.

6 Grading Criteria

- **Phase 1:** Setup and Attacks – 40%
- **Phase 2:** Honeypot Replication and Comparison – 20%
- **Phase 3:** SIEM Analysis – 20%
- **Report Quality and Documentation:** 20%

- **Phase 4 (Optional):** Defense Proposal – 20%

7 Resources and Tools

- **Caldera Framework:** https://caldera.mitre.org
- **Kali Linux:** https://www.kali.org
- **Metasploit Framework:** https://www.metasploit.com
- **MITRE ATT&CK Framework:** https://attack.mitre.org
- **SIEM Tools:**
  - **Wazuh:** https://wazuh.com
  - **Splunk:** https://www.splunk.com
  - **ELK Stack:** https://www.elastic.co/elk-stack
  - **Graylog:** https://www.graylog.org

8 Technical Support

The Teaching Assistants (TAs) are here to guide you through the stages of your project, providing support, clarifications, and feedback. However, the responsibility for completing tasks and meeting deadlines rests with you. Start early, stay engaged, and manage your time effectively to ensure successful project completion.