Lightning Talk 4
Testing

Project: Grid-SIEM

Fall 2023 | Group 29

Ella Cook, Trent Bickford, Westin Chamberlain, Daniel Ocampo

Unit and Interface Testing

- Unit Testing: The process of testing the smallest components used to build the overall project. In our case that could be ensuring that a virtual machine is up on the network. Or testing our cyber security defense measures from a specific subset of OT attacks.
- Interface Testing: This type of testing procedure is done to ensure that different units or components within our project are communicating successfully and are adhering to the project goals outlined in the design phase.
- What units are being tested? How? Tools?
  - The different types of virtual machines that are used to attack, defend and create the PowerCyber infrastructure. In addition to the Machine Learning algorithms and learning models we produce later in the project.
  - We will test the VMs by making sure that they have the hardware resources required, to verify this we will use Wireshark to observe network traffic and train our ML capabilities with the appropriate datasets.
- What are the interfaces in your design?
  - The most important interfaces in our design include the data channels of VMs sending system traffic into the two SIEM frameworks and machine learning data parsers that will be set up. Security Onion's Test Data Generator can help generate realistic test data, including logs and security events, to simulate various security scenarios.

Integration and System Testing

- Integration testing – testing units and interfaces together
  - Gathering traffic > parsing > machine learning
- System testing – testing a completed system as a unified whole
  - Penetration testing
  - Uptime, attack detection, power fluctuations
- Tools
  - Pytest – python testing framework
  - Command prompt
    - Ping, traceroute, nmap, mitre caldera

Regression and Acceptance Testing

- Regression Testing: In our project, the main requirements that cannot be broken are implementing a SIEM tool, using machine learning to assist the SIEM tool, and running attacks to test the defense.
  - To prevent the breaking of our SIEM tool we will use the snapshot feature on VMs.
  - To prevent the machine learning component of our project breaking, we will code adjustments.
  - There does not seem to be an issue with the attack portion of our project breaking due to updates.
- Acceptance Testing: To show that the requirements are being met, we will run an attack script against the PowerCyber testbed environment for functional requirements and receive client feedback for non-functional requirements.
  - Functional Requirements: We will run a demo where we show an off-network computer running an attack script against the PowerCyber testbed environment, then we will show how the SIEM tool that we implemented catches the attack script and sends an alert from a sensor node to the master node while utilizing the machine learning component to better group the attack.
  - Non-functional Requirements: We will track things like uptime and receive client feedback on design aspects like the usability of the interface for our SIEM tool as well as the responsiveness and performance from a users' perspective.

Security Testing and Results

- Security Testing
  - Determine how effective Security Onion and Gravwell are at detecting, analyzing, and mitigating threats
  - Assessing the added value of custom machine-learning script
  - We will
    - Employ Mitre Caldera
    - Replicate real-world scenarios like network intrusions, data breaches, and system exploits
    - Conduct scans using Security Onion and Gravwell tools
    - Our custom machine learning script will be evaluated based on its ability to learn from the simulated attacks
- Results
  - Our results phase is expected to have
    - A high efficacy in detecting brute force attacks and power fluctuations
    - Enhanced attack detection capabilities
    - A near 99% uptime of the SIEM system
    - ICS systems within PowerCyber to exhibit a 99.999% availability
    - Integrate ML/DL analytics to help detect and triage incidents