Activity File: Final Group Presentations

Overview

You are working as a Security Engineer for X-CORP, supporting the SOC infrastructure. The SOC Analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate.

Previously, you monitored live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

For the final part of this project, you will report back your findings to both the SOC manager and the Engineering Manager with appropriate analysis.

Instructions

Congratulations on making it through a comprehensive and demanding project! The tools and knowledge used to complete this week's tasks are a large chunk of offensive, defensive, networking, and system administration cybersecurity skills.

In the final part of this project, you will work with your fellow students to complete a group presentation. The presentation will contain analyses from one of the three perspectives: an offensive red team analysis, a defensive blue team analysis, or a network administration analysis.

In groups of three to six, divide responsibilities to complete **one** of the three presentations below:

- Offensive Presentation Template
- Defensive Presentation Template
- Network Presentation Template

Groups are expected to present **together**. One student will introduce the presentation. Then, each student will talk through the portion of the slides they were specifically responsible for.

Note that you can personalize these templates and include additional information as you see fit.

Example of an Offensive Presentation split between six students: Student A and B work on the "Network Topology" and "Critical Vulnerabilities" portion. Students C and D work on the "Exploits Used" section. Students E and F work on the "Avoiding Detection and Maintaining Access" sections.

This project and all of the deliverables created during this six-month course are valuable evidence of your skills and knowledge, which you can present during job searches and networking events. Make sure your project is complete, presentable, and free of errors.

The following is an overview of what each section covers. The slide templates provide the same information.

Offensive Security Presentation Option

The offensive red team section must include the following sections:

- **Exploits Used**
  - Choose three important exploits used during the assessment of the VMs.
  - Explain how each exploit works.
  - Provide the commands used to run them.
  - Add a screenshot confirming success (For example: a screenshot of a user shell if you ran a bind shell exploit).
- **Avoiding Detection**
  - For each exploit, explain which alerts in Kibana can detect it, if any.
  - Identify which metric the alert is responding to.
  - Suggest a technique for bypassing detection.
  - If possible, demonstrate your stealthier solution in action.
- **Maintaining Access**
  - Find a way to implement a backdoor on each target.
  - Provide an example or screenshot of the commands used.
  - Options include using Metasploit, dropping SSH keys, adding users, etc. You only need to choose one.

Defensive Security Presentation Option

The defensive blue team section must include the following sections:

- **Alerts Implemented**
    - Explain each alert implemented in Kibana and provide the metric it responds to.
    - Note the threshold it fires against.
    - Include a screenshot demonstrating that the alert indeed fired.
- **Hardening**
    - Choose three vulnerabilities or exploits.
    - For each, explain how it works, how it's delivered, and how to harden or patch the vulnerable VM against it.
- **Implementing and Distributing Fixes**
    - Create an Ansible playbook that implements all of the hardening steps specified above.
    - Include a README explaining what the playbook does and which vulnerabilities or exploits it mitigates.
    - If creating a functional playbook is too difficult or time-consuming, you can create just a README describing what it should do.

Network Security Presentation Option

The network security section must include the following sections:

- **Traffic Profile**
    - Fill out a table with information from the analysis, including data about top talkers, amount of traffic, type of traffic (protocols), and purpose of the observed network activity.
- **Normal Activity**
    - In this section, identify users who are participating in non-malicious traffic.
    - Explain what they're doing and include a screenshot of packets clarifying their behavior.
    - Elaborate on the packet, explaining how you know the traffic is not malicious.
- **Malicious Activity**
    - Identify which users are sending suspicious and malicious traffic.
    - For each, explain what kind of traffic they're sending.

  - Identify the IP addresses involved.
  - Identify and explain any interesting files in the conversation, such as malware, images, etc.
