CCF Lab 4 - Incident response and log management

In this lab, you will set up a complete environment for detecting and responding to security incidents using the Wazuh security platform. You will simulate real-world attacks, configure automated responses, and explore best practices for managing logs and system alerts. This hands-on exercise is designed to reinforce key concepts in incident detection, active response, and log retention.

Task 1 - Preparation

1. Deploy Wazuh central components (server, indexer, and dashboard) on your host machine or use an alternate method like Docker.
2. Set up a second machine with a Unix-like OS, install the Wazuh agent, and enroll it with the Wazuh manager. Enable SSH and create a test user account.
3. Prepare a third machine to act as the "attacker" endpoint to simulate cyber attacks.

   > You can collaborate with your colleagues to simulate attacks if you don't have enough hardware resources for three machines.

Task 2 - Configure active response

1. Enable the Wazuh active response feature to disable a user account for 10 minutes when a brute force attempt is detected.
2. Also configure it to block the attacker's IP address for 10 minutes.
3. Create `/home/<USERNAME>/malwarefiles/` on the monitored endpoint. Integrate malware detection (e.g., VirusTotal or YARA), and monitor this directory for malware.
   Configure Wazuh to automatically delete detected malware files.

Task 3 - Simulate attacks

1. Launch an SSH brute force attack from the attacker endpoint against the test user.
2. Show relevant alerts on the Wazuh dashboard.
3. Provide evidence that the user account was disabled and the attacker IP blocked. Include dashboard alerts and screenshots from the endpoint involved.
4. Download a malware sample into the `/home/<USERNAME>/malwarefiles/` directory.
   Confirm detection and show that it was automatically removed.

Task 4 - Log management

1. Define what a log retention policy is.
2. Explain how logs are rotated on Linux and how disk space is managed in relation to logs.
3. Create a configuration to automatically delete Wazuh alert log files older than 90 days.

Bonus

1. What are indices, and how do they differ from log files?
2. Create an index retention policy to delete Wazuh alert indices after 90 days.