Task 6: HIDS

Objectives:

- To get you acquainted with host-based intrusion detection systems (HIDS)
- Explore how to utilize **Alerts** interface to investigate host based intrusion scenario
- Explore which pre-existing rules in the Security Onion we are using
- Try two HIDS attack scenarios: Login failure on the server and unauthorized accessing files

HIDS

HIDS stands for Host-based Intrusion Detection System. It is a security mechanism that monitors and analyzes activity on a specific host or endpoint to detect potential security breaches or malicious activity.

Usage

Security Onion utilizes Wazuh as a Host Intrusion Detection System (HIDS) on each of the Security Onion nodes.
While using the Wazuh to collect the log file for Security Onion, we are supposed to install a Wazuh agent in each of the Virtual Machines that we want to monitor and connect the Wazuh agent with the Wazuh manager. Since the connection is not built successfully, you only need to know about it and there is no task given.

Wazuh

The Wazuh agent runs on the hosts that you want to monitor. It is multi-platform and provides the following capabilities:

- Log and data collection
- File integrity monitoring
- Rootkit and malware detection
- Security policy monitoring.
- Configuration assessments
- Software inventory

Task 6.1: Login Failure Exploration

Task 6.1.1: Performing login failure
Make sure that the attacker machine and the Security Onion are in the same network to perform the login failure to Security Onion.
Open a terminal and SSH to the Security Onion machine by type in the following command:

- ssh admin@<IP address of your Security Onion Machine>

You should be able to see a message that says “Are you sure you want to continue

connecting (yes/no/[fingerprint])? ” Type “yes” and click [Enter].

You will be asking to enter a password for the Security Onion machine. Entering a random password three times.

Wait for 1-2 minutes and then open the dashboard of Security Onion, and click on “Alert.” You should be able to see there is a medium level alert showing there are authentication failed and user login failure. Take a screenshot of the alerts. Using the **[Drilldown]** to see more information of each alert and tell us what you find.

Task 6.1.2: In the previous Snort lab, you are not able to see alerts on the console prompt to run Snort. The actual alert log file will be stored under the /var/log/snort directory. Explain the reason why we are able to visualize the alert now.

Task 6.1.3: From the information that you explore from the alerts and the information associated with these alerts. Please show the rule that detects the login failure.

Task 6.2: Sensitive File Accessing Exploration

Task 6.2.1: Performing Sensitive File Accessing
In your Analyst VM, open a terminal and type in the following command:

- echo “This is sensitive information like credit card numbers, social security numbers, or passwords” > sensitive.txt

- sudo mv sensitive.txt /var/log/my_monitored_directory/

  Replace "/var/log/my_monitored_directory/" with the directory path you want to monitor.

In your attacker VM, open a terminal and type in the following command:

- wget --no-check-certificate http://<Security Onion IP Address>/var/log/my_monitored_directory/sensitive.txt

[**Hint**: If you are not able to connect to the Security Onion, you can try this command in the Analyst VM to visualize the alert.]

After waiting for a few minutes, open the dashboard of Security Onion, and click on “Alert.” You should be able to see an alert showing that the host unblocked. Using the **[Drilldown]** to see more information of each alert and tell us what you find.

Task 6.2.2: From the information that you explore from the alerts and the information associated with these alerts. Please show the rule message that detects the login failure.