Assignment 8

Intrusion Detection System (IDS)

Objectives

By the end of this lab, you should be able to:

- Analyze PCAP files to identify malicious traffics, inputs and malwares
- Understand Suricata alerts and rules used to improve incident response

System

- Any Linux machine

1. Infrastructure Setup

For Windows users only:

Use the following instructions to install and configure suricata

- sudo apt-get install software-properties-common
- sudo add-apt-repository ppa:oisf/suricata-stable
- sudo apt-get update
- sudo apt-get install suricata
- sudo su (to login as superuser)
- Change the directory to /etc/suricata and open suricata.yaml file.
  - Replace the content of the file with content in the "suricata_windows_yaml.txt " file provided in the edimension
  - Create a new directory called "rules" and change the directory to rules
  - Inside rules, create a new file called "custom.rules". Use the content provided in "custom_rules.txt" file provided in the edimension
- Restart *suricata*
  - sudo systemctl restart suricata
  - sudo systemctl status suricata

Note*: If the above command shows failed. Reach out to the TA.

For MAC or Kali users only:

Use the following instructions to install and configure suricata

- sudo apt install suricata
- Change the directory to /etc/suricata and open suricata.yaml file.
  - Replace the content of the file with content in the “suricata_mac_yaml.txt ” file provided in the edimension
  - Change the directory to “rules ” and create a new file called “custom.rules”. Use the content provided in “custom_rules.txt” file provided in the edimension
- Restart *suricata*
  - sudo systemctl restart suricata
  - sudo systemctl status suricata

2. Analyze PCAP

In real life scenarios, SOC analyst will use tools like *wazuh* and suricata will be integrated with *wazuh* where the alerts will be triggered in a designated dashboard which helps to investigate and respond to the incident happens in the network or host or both.

In this setup *suricata* act as network intrusion detection system (NIDS) and it will be used to store alerts in logs which can be retrieved later. To simplify, we have provided the PCAP files which you can analyze using wireshark to understand what type of attack is performed and create the specific rules for suricata to trigger the alert.

Use the below command to send *pcap* files which trigger alert if it matches with rules specified by *suricata* inside “custom.rules”

- sudo suricata –r <pcap_file> -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

To verify whether the rule detects the attack you can check in the logs using this command

- sudo cat /var/log/suricata/eve.json | grep -a "<<description of the attack>>"

  #for highlighted text use your own description which you used to detect the attack

To remove previous alerts, you can remove the log file using the following command

- sudo rm /var/log/suricata/eve.json

3. Attack 1

Download all the *pcap* files and put it inside SeedVM. Send the attack1.pcap file to suricata using the following command and check whether it triggers an alert in the log files

- sudo suricata –r attack1.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a “Suspicious”

Since the rule is provided to you already you should be able to see one response in the log which shows the bruteforce attack is detected successfully.

Associated Rule

- **Destination (any any)**: The destination IP address and port are also set to any, meaning the rule applies to traffic directed to any destination IP and port.
- **Message (msg: "Suspicious Attempts")**: This is the message that will appear in the alert when rule is triggered. The message indicates an "Attempted brute force" attack.
- **Flags (flags)**: The rule looks for **SYN** packets. The SYN flag in TCP is used to initiate a connection. A high volume of SYN packets may indicate a brute-force attempt or denial-of-service attack.
- **Threshold (threshold both, track by_src, count 20, seconds 60)**: This threshold configuration defines the condition that triggers the alert:
    - **type both**: The rule will alert on both the source and destination.
    - **track by_src**: It tracks packets by the source IP address.
    - **count 20**: If 20 SYN packets are sent within the time frame, an alert is triggered.
    - **seconds 60**: The time window in which the 20 SYN packets must be seen is 60 seconds.
- **Class type (classtype)**: This classifies the event as an "attempted-user" attack, which is a general classification for brute-force or unauthorized access attempts.
- **Signature ID (sid:1000020)**: This is a unique identifier for the rule, in this case, 1000020.
- **Revision (rev:1)**: This is the revision number of the rule, which is set to 1, meaning it's the first version of this specific rule.

Answer the following questions from analyzing the pcap files using wireshark

- Does the attacker is successful in gaining the information? If so, what is the username and password?

4. Attack 2

Analyze attack2.pcap using wireshark and try to understand what type of attack has been done.

Hint: It is a type of network-based attack which is used for reconnaissance*

Previous rule can detect this attack as well, but you need to create your own rule that is specific to this attack.

- sudo gedit /etc/suricata/rules/custom.rules

After updating the rules make sure to restart the suricata using the following command.

- sudo systemctl restart suricata

Send the attack2.pcap file to suricata and see whether it triggers an alert in the logs based on the rules created

- sudo suricata –r attack2.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a "*<<description of the attack>>*"

Paste the screenshot of the alert trigger in logs in the report.

Answer the following questions from analyzing the pcap files using wireshark

- What is the attack performed by the attacker in this scenario?

5. Attack 3

Analyze attack3.pcap using wireshark and try to understand what type of attack has been done.

Hint: Focus on the HTTP packets*

Based on the attack create the rule in suricata to detect the attack.

- sudo gedit /etc/suricata/rules/custom.rules

After updating the rules make sure to restart the suricata using the following command.

- sudo systemctl restart suricata

Send the attack3.pcap file to suricata and see whether it triggers an alert in the logs based on the rules created

- sudo suricata –r attack3.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a "*<<description of the attack>>*"

Paste the screenshot of the alert trigger in logs in the report.

Answer the following questions from analyzing the pcap files using wireshark

- What is the attack performed by the attacker in this scenario?

6. Attack 4

Analyze attack4.pcap using wireshark and try to understand what type of attack has been done.

Hint: It is also another type of injection*

Based on the attack create the rule in suricata to detect the attack.

- sudo gedit /etc/suricata/rules/custom.rules

After updating the rules make sure to restart the suricata using the following command.

- sudo systemctl restart suricata

Send the attack4.pcap file to suricata and see whether it triggers an alert in the logs based on the rules created

- sudo suricata –r attack4.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a "*<<description of the attack>>*"

Paste the screenshot of the alert trigger in logs in the report.

Answer the following questions from analyzing the pcap files using wireshark

- What is the attack performed by the attacker in this scenario?
- What is the confidential information gained by the attacker?

7. Attack 5 (Trickbot Trojan)

Trickbot is a sophisticated banking trojan that has evolved into a modular malware platform capable of various malicious activities, including credential theft, lateral movement within networks, data exfiltration, and delivering other malware.

Open attack4.pcap in wireshark to analyze it. Filter the post requests packets using *http.request.method == "POST"* as malware often uses POST requests to exfiltrate data like credentials, system information or files.

Select the packet where the user-agent is *"test"*

'user-agent' is one of the method used by attackers in injecting malwares to camouflage their activity. Right click and select Follow-> HTTP Stream to understand the operations the packet is trying to perform. And you can see it is trying to gain information like process list and system info.

You need to create rules to detect this trojan. After updating make sure restart suricata and send the *pcap* file to trigger alert in *logs* using the following command.

- sudo suricata –r attack5.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a *"<<description of the attack>>"*

Paste the screenshot of the alert trigger in logs in the report.

From the wireshark answer the following questions

- What is the IP address of the infected windows client?
- What is the domain name of the infected windows client?
- What is the name of the malware (windows executable) file you can extract from the pcap file?

8. Attack 6

Open attack6.pcap in wireshark to analyze it.

You need to create rules to detect this malware. After updating make sure restart suricata and send the *pcap* file to trigger alert in *logs* using the following command.

- sudo suricata –r attack6.pcap -c /etc/suricata/suricata.yaml -l /var/log/suricata -k none

Filter the log(s) based on the description which is used to trigger the alert using the following command

- sudo cat /var/log/suricata/eve.json | grep -a *"<<description of the attack>>"*

Paste the screenshot of the alert trigger in logs in the report.

From the wireshark answer the following question

- What type of file is used by the attacker in this attack to camouflage that it is a normal file the client is downloading/accessing and not a malware (like is it a text/zip/image/audio/video file)? Show the wireshark screenshot as proof to your observation?