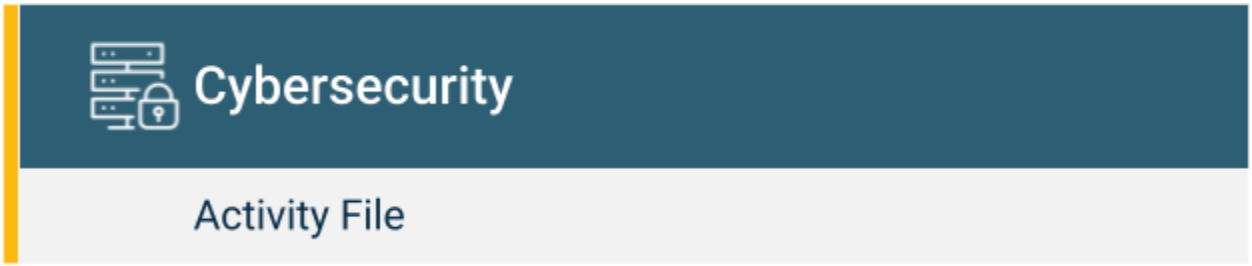

Module 12 Day 2: 04 Intrusion Detection Systems and Snort

Activity File: Intrusion Detection Systems and Snort

In this activity, you will play the role of an SOC analyst for the California Department of Motor Vehicles (DMV).

- In preparation for the California Consumer Privacy Act (CCPA), your CISO has advised you to implement new security controls to further protect the driving records of all state citizens.
- This new law includes serious penalties for failing to provide adequate protection of private citizen data. As a result, you've decided to strengthen your layered defenses by adding both network-based (NIDS) and host-based intrusion detection systems (HIDS).
- You decided to deploy Snort as your newly added security control. You've also decided to deploy Snort at three layers of the defense-in-depth (DiD) model: Perimeter (NIPS), Network (NIDS), and Host (HIDS).
- In preparation for the launch, your CISO prepared a review document to determine who needs additional training.

Instructions

Read and answer each question.

1. What are the two main differences between a firewall and an IDS system?

A firewall is a perimeter defense. It blocks traffic based on rules ports. An IDS is a bit more complex as it does not block traffic but it monitors it and sends alerts based on malicious signatures.

2. What's the best physical placement for an IDS on a network: Inline or mirrored port?

The best physical placement is on a mirrored port. It is a packet sniffer that does not need to interact with the packets only read them.

3. An IDS placed at the perimeter layer of the DiD model is referred to as what?

A perimeter IDS

4. Define each part of the following Snort alert:
    - `alert ip any any -> any any {msg: "IP Packet Detected";}`
        - `Alert = any rule that is broken that triggers the IDs`
        - `Ip = the rule applies to IP traffic`
        - `any any = any source IP and any source port`
        - `-> = inbound vs. outbound`
        - `any any = any destination IP and any destination port`
        - `{msg: "IP Packet Detected";} = the predefined msg for the analyst when the rule is triggered`
5. An intrusion system that can act on an alert by blocking traffic is referred to as what?

Intrusion prevention system

6. Name the two types of detection techniques used by intrusion detection systems.

Signature based and anomaly based

7. What type of IDS establishes its rules using a baseline?

Anomaly based IDS

8. True or false: Signature-based IDS systems are not effective against zero-day attacks.

True they are not able to detect due to no signature

9. When used together, which should be placed farthest from the data: A firewall, an IDS, or an IPS?

Firewall should be farthest as it is the outer perimeter of defense.

Bonus Questions

10. What part of this Snort alert is the "rule header"?
    - `alert ip any any -> any any {msg: "IP Packet Detected";}`
11. Name and define the three Snort configuration modes.

Sniffer reads network packets, Packet logger performs packet captures, NIDS analyzes traffic and performs actions based on rules

12. What is the difference between an IDS and an IPS?

IDS is only able to detect traffic but and IPS can prevent certain traffic based on rules.

13. True or false: An indicator of attack (IOA) occurs at some previous point in time, and an indicator of compromise (IOC) occurs in real time.

False, IOA occurs in real time and an IOC occurs at a previous point in time.

14. True or false: An IOA is "proactive" and an IOC is "reactive."

True

15. True or false: An IPS is physically connected "inline" with the flow of traffic, processes entire subnets of data, and requires more robust hardware.

True

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.