Cybersecurity

Activity File

Module 12 Day 2: 07 Security Onion and NSM

Activity File: Security Onion and NSM Overview

In this activity, you will continue your role as an SOC Analyst for the California DMV.

- You've implemented a new security control as part of your network security monitoring (NSM) program.
- Your NSM program will help your organization understand the limits of what it can detect, adversarial tactics, and how to quickly apply lessons learned to mitigate security vulnerabilities.
- Your CISO has advocated for using Security Onion as your open source NSM system to detect and analyze all intrusion attempts.
- Your CISO provided the following questions to help you test your knowledge of Security Onion and NSM before launching the new system.

Instructions

Open the Security Onion Console

1. Pick one alert and answer the following questions:
    - What is the alert status? allowed
    - What are the source and destination IP addresses? 192.168.10.128 -> 200.223.236.53
    - What are the source and destination ports? 1615-> 51275
    - In the IP resolution section, perform a reverse DNS lookup of the attacker. What information is revealed? Non existent domain
    - What is the alert ID for the alert you chose? 20000334
2. Define the IDS (Suricata) rule that triggers the alert you chose:
    - Action alert
    - Protocol tcp
    - Source IP $HOME_NET
    - Source port any
    - Direction outbound

- Destination IP $EXTERNAL_NET
- Destination port !7680
- Message msg:"ET P2P BitTorrent peer sync"; flow:established; content:"|00 00 00 0d 06 00|"; depth:6; threshold: type limit, track by_dst, seconds 300, count 1; reference:url,bitconjurer.org/BitTorrent/protocol.html; classtype:policy-violation; sid:2000334; rev:13; metadata:created_at 2010_07_30, updated_at 2019_07_26;

Bonus Questions

True or false:

1. NSM is vulnerability-centric, with its primary focus on the vulnerability and not the adversary. False
2. The strength of NSM is its focus on the visibility of an attack, not its control. True
3. NSM can see inside encrypted traffic. False
4. Alerts in Security Onion's console are the equivalent of an Indicator of Attack, or IOA. True
5. NSM allows organizations to track and uncover malware.True
6. The Suricata IDS engine drives much of the functionality of the Security Onion analyst's console. True

Answer the following:

1. Name two methods for physically connecting an IDS to a network. Mirrored or tapping
2. Name the two stages of NSM and their processes. Escalation and resolution

---

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