NEW YORK INSTITUTE OF TECHNOLOGY

Lab 3 –NIDS Rule Development

Introduction

In this lab, you will engage in the process of developing Network Intrusion Detection System (NIDS) rules aimed at identifying and detecting malicious patterns within network traffic. By implementing these rules and testing them against network traffic, you will gain hands-on experience in identifying and responding to potential security threats. This lab comprises of analyzing a specific malware's traffic and preparing the rules for its detection.

Lab Environment

In this lab, we are working with the following tools, each serving a specific purpose:

- **Wireshark**: Used for the analysis of malicious network traffic.
- **VSCode** (or your preferred text editor): Functions as the editor for writing NIDS rules, allowing you to customize your work environment for rule development.
- **Suricata**: This Network Intrusion Detection System (NIDS) is employed to assess the performance of NIDS rules against potentially malicious network traffic.

Task 1: Creating NIDS Rules for Previous Attacks

This task focuses on crafting Network Intrusion Detection System (NIDS) rules to identify patterns associated with attacks previously conducted in the previous lab. The objective is to run these rules in Suricata and determine their effectiveness in detecting malicious patterns within the captured traffic (pcap file). For example, If you went with option 2 in lab 3, You should use pcap files associated with option 2 and create rules accordingly to detect the malicious packets.

Instructions:

1. Use Previous Pcap Files: Utilize the pcap files from earlier labs (lab 3).
2. Develop a minimum of two Suricata rules to pinpoint the malicious patterns linked to distinct attacks you have previously executed.
    a. Ensure your rules are specific and comprehensive, incorporating an array of relevant keywords to precisely target the particular attack you conducted.

    b. Employ suitable metadata in your rules.

3. Alert Message in Your Rule: In the alert message segment of your rule, start with your name. Subsequently, specify the explicit attack name and/or CVE number, followed by a brief title to the CVE.
4. Test Your Rules: Apply your developed rules to the captured traffic file using Suricata.

Evaluate the functionality of your rules by testing them against the traffic.

This task sharpens your ability to create NIDS rules and gauge their effectiveness when applied to network traffic. Your crafted rules should be highly specific, well-structured, and capable of accurately detecting the intended attack patterns.

Task 2: Develop NIDS Rules for Detecting Cross-Site-Scripting Attempts

In this lab, you will take on the role of a security analyst from CyberFortify Inc., investigating suspicious network traffic. A network capture (.pcap) has been provided, containing potential security threats, including XSS attack attempts and hidden flags. Your task is to analyze the traffic, identify malicious patterns, and create Suricata rules to detect these threats effectively. The final goal is to uncover four hidden flags and analyze four different XSS payloads before making a final rule to detect all of those XSS payloads.

💡 **What is XSS?**

Cross-site scripting (XSS) is when an attacker injects malicious scripts (usually JavaScript) into a website or request.

These payloads often look like this:

- *<script>alert(1)</script>*
- *"><img src=x onerror=alert(1)>*
- *';alert(1)//<script>alert(1)</script>*
- *"><img src=x onerror=alert(1)>*
- *';alert(1)//*

Look for weird tags, quotes, <script>, or anything trying to pop up an alert.

Task 2.1: Flag Detection Using Suricata

1. Identify the first flag, which follows the pattern **fl_g**.
2. Create a Suricata rule to detect the packet containing this flag.
3. Open the matched packet in Wireshark.
4. Each flagged packet contains: A **hint** for the next flag, An **XSS payload**.
5. Repeat the process until all **4 flags** are found.
6. Create and document a Suricata rule for each flag (4 rules in total).

Task 2.2: XSS Payload Rule Creation

1. **Collect** the XSS payloads found during Task 2.1
2. Analyze patterns or similarities across all four payloads.

3. Write **one** Suricata rule that can detect **all four** XSS payloads.
4. Explain your logic and approach for designing this detection rule.
5. Your rules don’t need to be overly generic or overly specific.

You need to create a total of five rules: four for the individual flags and one for the XSS detection based on the encountered payloads.

Deliverables

This lab simulates a real-world cybersecurity investigation, requiring a methodical approach to detecting hidden attack patterns in network traffic. By uncovering XSS payloads and tracking hidden flags, you will gain insight into threat detection techniques, attack evasion methods, and the importance of adaptive security rules in an intrusion detection system.

Your final report should include:

- A step-by-step explanation of how each flag and XSS payload was identified and detected with the rules and Wireshark analysis.
- All the Suricata rules you created and the reasoning behind creating those rules, including the final XSS detection rule.
- Screenshots of flagged packets in Wireshark.

Submit all your rules in a single .txt rule file, along with your report.