Purple team bootcamp

Cybersecurity and Attack Detection

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Mohammed baqer

2026/2/4

Table of Contents

Introduction

The lecture focuses on detection and analysis. This phase is crucial for identifying and responding to threats before they cause significant damage. The concept of "Attacker Dwell Time," which refers to the time an attacker stays undetected in a network.

Key Points Covered (النقاط الرئيسية التي تم تناولها):

Attacker Dwell Time (وقت تواجد المهاجم):

- **Imagine your house has been broken into, but you don't notice until 280 days later. This is similar to the concept of "Attacker Dwell Time" in cybersecurity, which is the amount of time it takes to detect an intrusion. On average, it takes organizations 280 days to realize they've been breached. This is far too long, and the goal is to reduce this time by detecting attackers early.**
- **تخيل أن منزلك قد تم اختراقه ولكنك لا تلاحظ ذلك إلا بعد 280 يومًا. هذا مشـــابه لمفهوم "وقت تواجد المهاجم" في الأمن السيبراني، وهو الوقت الذي يستغرقه اكتشاف الاختراق. في المتوسط، تستغرق الشركات 280 يومًا حتى تدرك أنها تعرضت للاختراق، وهذا وقت طويل للغاية. الهدف هو تقليل هذا الوقت بالكشف المبكر عن المهاجمين.**

Scenario - Smoke Detector Analogy (السيناريو - تشبيه كاشف الدخان):

- **Think of detection like a smoke detector in your house. It doesn't stop the fire, but it alerts you to act before it spreads. Similarly, strong detection systems in cybersecurity help spot attackers early, preventing further damage.**
- **فكر في الاكتشـاف مثل جهاز كشـف الدخان في منزلك. هو لا يوقف الحريق، لكنه ينبهك للتحرك قبل أن ينتشـر. بالمثل، تسـاعد أنظمة الكشف القوية في الأمن السيبراني في اكتشاف المهاجمين مبكرًا، مما يمنع المزيد من الأضرار.**

Detection Engineering (هندسة الكشف):

- **Detection is all about knowing what to look for and how to find it. Imagine being a detective looking for clues at a crime scene. You need to know what kind of clues to search for and how to analyze them. In cybersecurity, this involves creating rules to identify suspicious activity and continually refining them as attackers evolve.**

- الاكتشاف يتعلق بمعرفة ما الذي يجب البحث عنه وكيفية العثور عليه. تخيل أنك محقق تبحث عن أدلة في مسرح الجريمة. تحتاج إلى معرفة نوع الأدلة التي تبحث عنها وكيفية تحليلها. في الأمن السيبراني، يشمل ذلك إنشاء قواعد لتحديد الأنشطة المشبوهة وصقلها باستمرار مع تطور أساليب المهاجمين.

Detection Levels (مستويات الكشف):

- **There are multiple layers of detection, similar to having different security cameras around a building. These levels are:**

0. **Network Perimeter Level: Like a firewall acting as a guard checking IDs.**
1. **Endpoint Perimeter Level: Like an antivirus acting as a doorman checking for unauthorized access.**
2. **Endpoint System Level: Like a security guard monitoring internal activity.**
3. **Application Level: Monitoring who accesses specific applications or systems.**

- هناك مستويات متعددة من الكشف، مثل وجود كاميرات أمان مختلفة حول المبنى. هذه المستويات هي:

0. مستوى محيط الشبكة :مثل جدار الحماية الذي يعمل كحارس للتحقق من الهويات.
1. مستوى محيط النقطة النهائية :مثل برنامج مضاد الفيروسات الذي يعمل كحارس للتحقق من الوصول غير المصرح به.
2. مستوى نظام النقطة النهائية :مثل الحارس الأمني الذي يراقب الأنشطة الداخلية.
3. مستوى التطبيق :مراقبة من يدخل إلى تطبيقات أو أنظمة معينة.

What is Suricata? (ما هو سوركاتا؟):

- **Suricata is an open-source security tool that monitors network traffic, detects suspicious activity, and can block intrusions. It acts like a guard dog, watching over your network and alerting you when something suspicious happens.**
- سوركاتا هو أداة أمنية مفتوحة المصدر تراقب حركة المرور على الشبكة، وتكتشف الأنشطة المشبوهة، ويمكنها حظر التسللات. إنه يعمل مثل الكلب الحارس الذي يراقب شبكتك وينبهك عندما يحدث شيء مريب.

Suricata Lab Overview (نظرة عامة على مختبر سوركاتا):

- **In this lab, you will set up Suricata, analyze suspicious activities (like a backdoor attack), and learn how to write your own rules for detecting specific threats.**
- في هذا المختبر، ستقوم بإعداد سوركاتا، وتحليل الأنشطة المشبوهة (مثل هجوم الباب الخلفي)، وتعلم كيفية كتابة قواعدك الخاصة لاكتشاف التهديدات المحددة.

Simplified Suricata Logs (السجلات المبسطة لسوركاتا):

- **Suricata generates several types of logs to monitor and analyze activities:**

0. **suricata.log: General log of all activities.**
1. **fast.log: Quick alerts for detected threats.**
2. **eve.json: Detailed logs in JSON format for suspicious activities.**

- **يولد سوركاتا عدة أنواع من السجلات لمراقبة وتحليل الأنشطة:**

0. **suricata.log: سجل عام لجميع الأنشطة.**
1. **fast.log: تنبيهات سريعة للتهديدات المكتشفة.**
2. **eve.json: سجلات مفصلة بتنسيق JSON للأنشطة المشبوهة.**

The Importance of Reducing Attacker Dwell Time (أهمية تقليل وقت تواجد المهاجم):

- **the longer an attacker remains undetected, the more damage they can do. This concept of "Attacker Dwell Time" is critical in measuring the effectiveness of your security operations. Reducing this time is crucial for minimizing data loss and reputational damage.**
- **كلما طال بقاء المهاجم دون اكتشاف، كلما زادت الأضرار التي يمكن أن يسببها. يعتبر مفهوم "وقت تواجد المهاجم" أمرًا بالغ الأهمية في قياس فعالية عمليات الأمان الخاصة بك. تقليل هذا الوقت أمر بالغ الأهمية لتقليل فقدان البيانات والأضرار التي تلحق بالسمعة.**

Testing Suricata for Intrusion Detection (اختبار سوركاتا لاكتشاف التسلل):

- **You can test Suricata's configuration using the terminal to ensure it is correctly set up. Once properly configured, Suricata will be ready to monitor your network for intrusions, alerting you to any suspicious activities.**
- **يمكنك اختبار تكوين سوركاتا باستخدام الطرفية لضمان أنه تم إعداده بشكل صحيح. بمجرد تكوينه بشكل صحيح، سيكون سوركاتا جاهزًا لمراقبة شبكتك لاكتشاف التسللات، وتنبيهك إلى أي أنشطة مشبوهة.**

Phases of Detection in Incident Response (مراحل الكشف في استجابة الحوادث):

- **Detection and analysis are among the most challenging stages in incident response (IR). Without effective detection, an organization cannot respond to incidents, making this phase**

indispensable. Preparation is key, but detection is where incidents are first noticed and contained.

- **يعتبر الكشف والتحليل من بين المراحل الأكثر تحديًا في استجابة الحوادث (IR). دون الكشف الفعال، لا يمكن للمنظمة الاستجابة للحوادث، مما يجعل هذه المرحلة أمرًا لا غنى عنه. التحضـــير مهم، لكن الكشـــف هو المكان الذي يتم فيه ملاحظة الحوادث لأول مرة واحتواؤها.**

Practical Lab

The purpose of this lab was to install and configure **Suricata**, an open-source intrusion detection system (IDS) and intrusion prevention system (IPS) on an Ubuntu Server. The lab involved the step-by-step process of downloading and installing Ubuntu Server, configuring network settings, and setting up Suricata for network traffic monitoring and security analysis. This report outlines the installation procedure, configuration, and the steps taken to ensure the proper functioning of Suricata.

1. Downloading Ubuntu Server

The first step in the process involved downloading the **Ubuntu Server ISO** file. The ISO was obtained from the official **Ubuntu website** to ensure the latest stable version was used for the installation. The file was saved locally and prepared for use in a virtual machine (VM) environment.

2. Choosing the Installation Type

For the purpose of this lab, a **virtualized environment** was used to install Ubuntu Server. We chose **VMware** as the virtualization software, although **VirtualBox** could also be utilized as an alternative. A new virtual machine was created, and the **Ubuntu Server ISO** was loaded to initiate the installation.

3. Installing Ubuntu Server

Once the installation media was loaded into VMware, the process began by selecting the **Ubuntu Server ISO** and configuring the virtual machine's settings:

- **Storage Configuration:** The virtual disk size was set to allocate space for the server installation.
- **Network Configuration:** The network settings were configured to ensure the server would have network access during and after installation.
- **Partitioning:** The system was configured to automatically partition the disk for the installation of the operating system.

During the installation, the system prompted for a **username** and **password** to create a user account that would have administrative (sudo) privileges for managing the server.

4. Confirming the Installation

Once the installation was completed, the system prompted for the user credentials, including the **username** and **password**. This user account would be used for logging into the server post-installation. After the system restarted, we logged in using the newly created credentials.

5. Connecting to the Server via SSH

To manage the server remotely, **SSH (Secure Shell)** was used. The following steps were performed:

- The **IP address** of the server was obtained by executing the command:

ip addr show

Figure (1) shows the Ip address of the ubuntu server used to connect via ssh into putty

- With the IP address in hand, we used **Putty**, an SSH client, to establish a remote connection to the server. We entered the IP address of the server in Putty, provided the **username** and **password**, and gained access to the server's terminal remotely.

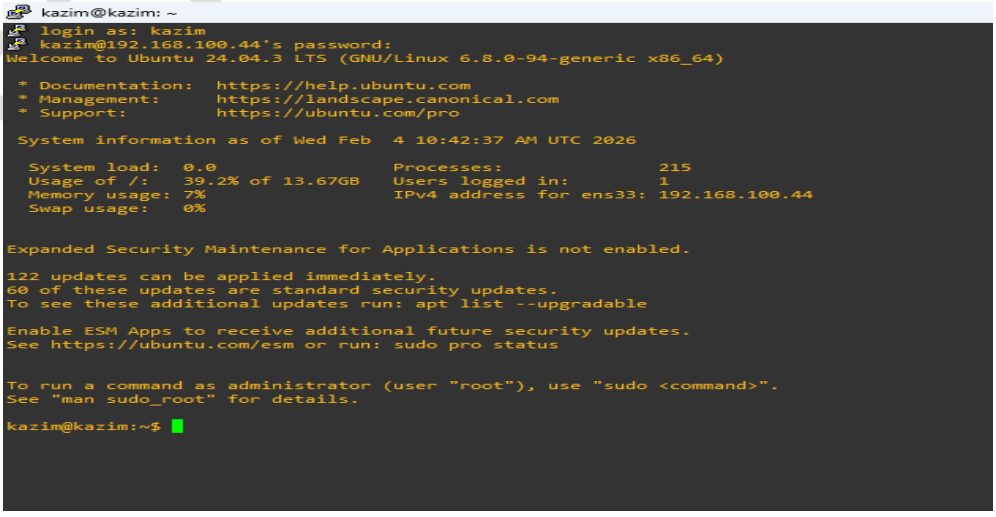

Figure (2) shows successful connection after inputting credentials

6. Installing Suricata IDS/IPS

Once connected to the server, we proceeded to install **Suricata**. Suricata is an advanced IDS/IPS used for network monitoring and security analysis. To install Suricata, we used the following commands:

```
sudo apt-get update

sudo apt-get install suricata
```

This process downloaded and installed the latest stable version of Suricata from the Ubuntu repositories.

7. Configuring Suricata

After installation, we needed to configure Suricata to ensure it monitored the correct network interface and that all necessary rules were loaded for detection:

- The **configuration file** for Suricata (`/etc/suricata/suricata.yaml`) was edited to update the **network interface** from **eth0** to the correct interface **ens33** (based on the server's network settings).
- We also ensured that Suricata's rule files were properly installed and updated. Suricata requires rule sets to detect and prevent network threats, and the rule files were downloaded and verified using the following command:

  ```
  sudo nano /etc/suricata/suricata.yaml
  ```

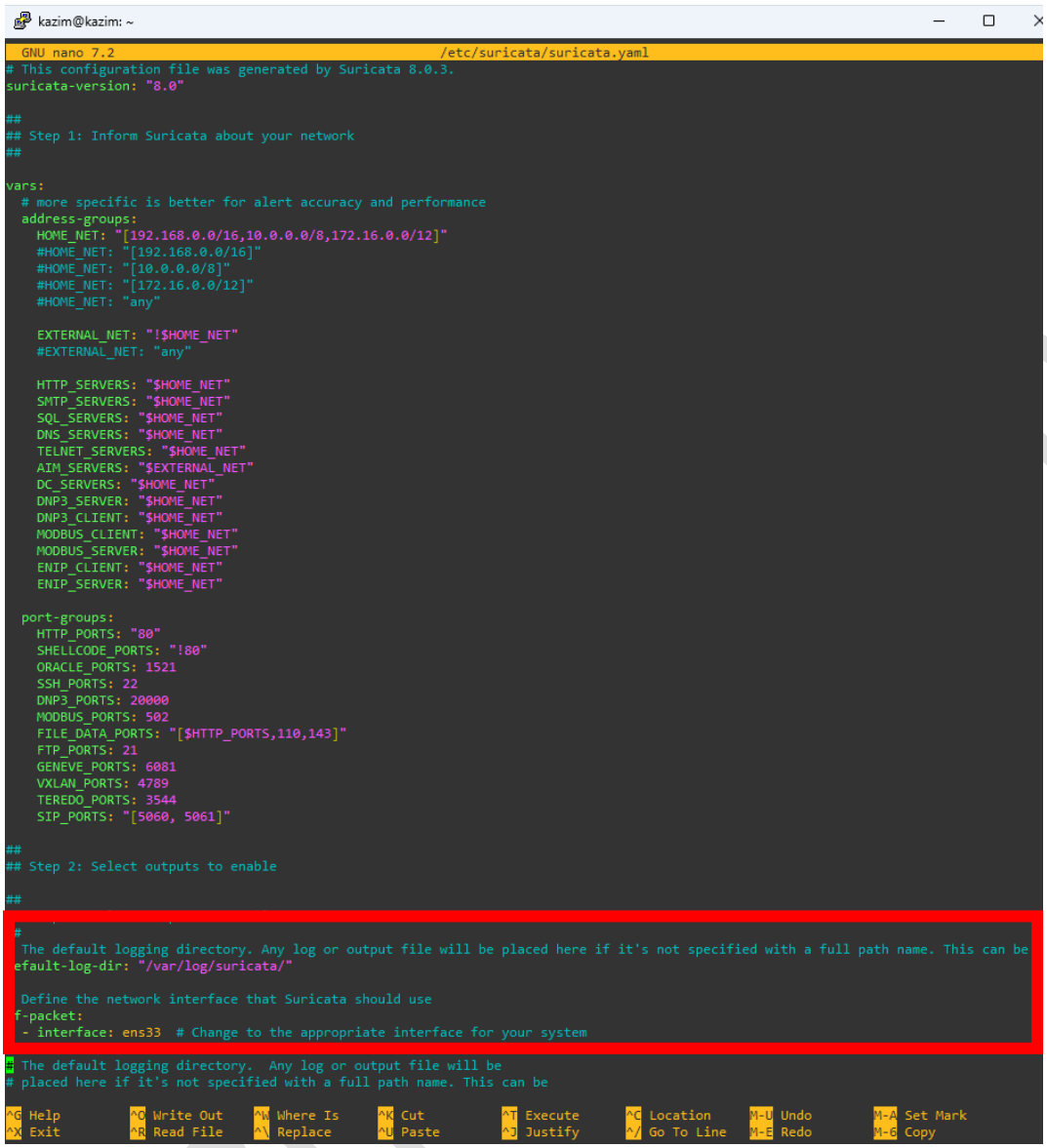

Figure (3) shows the modification we implemented to the network interface

Following the steps outlined, **Suricata** was successfully installed and configured on the **Ubuntu Server**. The service was running without errors, and the system was set to monitor the designated network interface for any potential security threats.

Conclusion

This lab successfully demonstrated the installation, configuration, and deployment of **Suricata** on an **Ubuntu Server** in a virtualized environment. The key tasks involved downloading and installing Ubuntu Server, configuring SSH access, installing Suricata, and ensuring the system was properly configured to monitor network traffic for security threats. The process culminated in a running Suricata service that was able to detect potential intrusions, ensuring the server's security.

Future work may involve further customization of Suricata's rule sets, as well as testing its effectiveness by simulating network attacks. Additionally, continuous monitoring of system logs and Suricata's alerts would be critical for maintaining server security.