Purple team bootcamp

IDS Detection System

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Mohammed baqer

2026/2/7

SCHOLARKAZIM

Contents

SCHOLARKAZIM

Introduction

- **Topic Focus:** Setting up detection on an IDS server (Intrusion Detection System).
- **Concept:** Treating the IDS as a monitoring agent, not as a full server.
- **Goal:** Understanding how to manage IDS in different environments, the importance of logging for detection, and the integration of IDS systems like Suricata in organizations.

Main Points & Concepts

1. **The Role of Documentation / دور التوثيق**
    - **Importance:** Documentation is vital for learning IDS products.
    - Engineers should refer to official documentation (installation, security considerations, and configuration) to understand the system thoroughly. Using interfaces like Sguil alone is insufficient; in-depth knowledge of rules and logic is required.
    - التوثيق أمر بالغ الأهمية لتعلمIDS ، ويجب أن يعود المهندسون إلى التوثيق الرسمي لفهم النظام بشكل شامل.
2. **Security Onion & Its Log Files / Security Onion**
    - **What is Security Onion:** An open-source IDS platform.
    - **Key Log Files:**
        - **fast.log:** Contains attack alerts.
        - **eve.json:** Detailed forensic data about events.
        - **suricata.log / start.log:** Service status and troubleshooting information.
    - Security Onion هو منصة مفتوحة المصدر، وتوفر ملفات السجل مثل fast.log و eve.jsonمعلومات حيوية عن الهجمات والأحداث.
3. **How IDS/IPS Works / كيفية عمل IDS/IPS**
    - **Header Inspection (Firewall/Network Policy):** Like checking a passport/ID (source/destination IP/port).
    - **Payload Inspection (IDS/IPS):** Like searching luggage for contraband (signatures/threats).
        - **IDS (Detection):** Alerts on suspicious traffic.
        - **IPS (Prevention):** Actively blocks malicious traffic.
    - فحص الهدر يشبه فحص جواز السفر، بينما فحص البيلود يشبه تفتيش الأمتعة للبحث عن التهديدات.
4. **Practical Traffic Analysis & Attack Detection / التحليل العملي لحركة المرور والكشف عن الهجمات**
    - **Reconnaissance:** Using Nmap to scan a web server (Apache on port 80).
    - **IDS Alert:** Detection of a web application attack in the fast.log.
    - **Deep Analysis:** Analyzing the eve.json log for granular details.
    - **Threat Intelligence:** Using frameworks like MITRE ATT&CK to understand the attacker's methodology.

SCHOLARKAM

- استخدام Nmap لفحص خادم ويبApache ، ثم تحليل سجلات fast.log و eve.jsonللكشف عن الهجمات.

5. **Incident Response & Packet Capture (PCAP) Analysis / الاستجابة للحوادث وتحليل التقاط الحزم (PCAP)**
    - **PCAP Files:** Network traffic captured for forensic analysis.
    - **Response Actions:**
        - **Isolation:** Disconnect the compromised machine.
        - **Containment:** Block the attacker's IP.
        - **Eradication:** Follow threat mitigation advice (e.g., from MITRE ATT&CK).
    - استخدام ملفات PCAP في التحقيقات والتحليل، مع الإجراءات الفورية مثل العزل والاحتواء.

Main Points Discussed

1. **IDS Basics and Configuration**
    - IDS detects suspicious activities within a network. Logs are essential in identifying and addressing potential threats.
    - IDS often integrates with other systems for effective detection.
2. **Suricata IDS Installation and Configuration**
    - Suricata is an open-source IDS system that also functions as an IPS. Installation includes security and performance configurations.
    - Documentation is critical for setting up Suricata and other IDS/IPS systems.
3. **Understanding Logs in IDS**
    - IDS logs (such as Suricata logs) are crucial for analyzing network anomalies.
    - **Log Types:**
        - **fast.log:** Alerts about detected activities.
        - **json.log:** Detailed data for deep analysis.
4. **Configuration and Use of Documentation**
    - Reading and understanding documentation is essential for effective use of IDS tools like Suricata.
    - Documentation includes setup guides, security tips, and configuration recommendations.
5. **Handling Alerts and Logs**
    - IDS generates alerts when suspicious activities are detected. These alerts need to be analyzed using logs like fast.log and json.log.
6. **Tools and Techniques**
    - **Nmap:** A network scanning tool used to detect open ports and services.
    - **Apache Server Setup:** Understanding web server setups and vulnerability scanning using Nmap.

SCHOLARKAZIM

Key Terminology and Concepts Explained

1. **IDS (Intrusion Detection System):** Detects and alerts on potential security breaches in the network.
2. **IPS (Intrusion Prevention System):** Detects and prevents attacks.
3. **Suricata:** An open-source IDS engine used for network monitoring and attack prevention.
4. **fast.log:** A log format used by Suricata to store brief alerts on detected activities.
5. **json.log:** A detailed log format used for deeper inspection and analysis.
6. **Nmap:** A tool used to scan networks for open ports and services.
7. **Log Correlation:** The process of analyzing and combining logs to gain deeper insights into network activity.

Examples Used in the Lecture

1. **Suricata Logs:**
   - Configuring Suricata, analyzing logs (fast.log, json.log), and correlating them to understand network anomalies.
2. **Real-Time Alerts:**
   - Demonstrating how Suricata triggers alerts in real-time based on unusual network patterns.
3. **Nmap Tool Example:**
   - Using Nmap to scan for open ports and services, demonstrating the risks associated with unsecured ports.
4. **Apache Web Server Setup:**
   - Setting up an Apache web server, scanning for open ports with Nmap, and ensuring correct server installation.

Introduction / المقدمة

- **Topic Focus:** Setting up detection on an IDS server, focusing on using IDS as a monitoring agent rather than a full server.
- **Concept:** The goal is to manage IDS systems based on the environment and focus on logging as a critical element in detecting and managing threats, particularly in organizations using Suricata IDS.

SCHOLARKAZIM

- الموضوع يركز على كيفية إعداد الكشف على خادم IDS واستخدامه كأداة مراقبة بدلاً من خادم كامل. الهدف هو إدارة أنظمة IDS بناءً على البيئة والتركيز على السجلات كعنصر رئيسي في اكتشاف وإدارة التهديدات، خصوصًا في المنظمات التي تستخدم سوركاتا.IDS

Main Points & Concepts / النقاط الرئيسية والمفاهيم

1. **The Role of Documentation / دور التوثيق**
    - **Importance:** Documentation is vital for learning IDS products and understanding their functionality. Engineers should always refer to official documentation, not just the product's interface.
    - التوثيق أمر بالغ الأهمية لتعلم منتجات IDS وفهم كيفية عملها. يجب على المهندسين دائمًا الرجوع إلى التوثيق الرسمي وليس فقط واجهة المنتج.
2. **Security Onion & Its Log Files / Security Onion وملفات السجلات الخاصة بها**
    - **What is Security Onion:** An open-source IDS platform that helps monitor network traffic for intrusions.
    - **Key Log Files:**
        - **fast.log:** Contains potential attack alerts.
        - **eve.json:** Provides detailed forensic data.
        - **suricata.log / start.log:** Contains service status and startup information.
    - Security Onion هو منصة IDS مفتوحة المصدر تساعد في مراقبة حركة مرور الشبكة لاكتشاف التسللات. تشمل الملفات الرئيسية fast.log و eve.json و suricata.log.
3. **How IDS/IPS Works / كيفية عمل IDS/IPS**
    - **Header Inspection:** Checking source and destination IPs/ports.
    - **Payload Inspection:** Searching for known threats (signatures).
    - **IDS (Detection):** Alerts on suspicious traffic.
    - **IPS (Prevention):** Prevents attacks by blocking malicious traffic.
    - فحص الهدر وفحص البيلود يساعدان في الكشف عن التهديدات. يقوم IDS بالكشف والتنبيه، بينما يمنع IPSالهجمات.
4. **Practical Traffic Analysis & Attack Detection / التحليل العملي لحركة المرور والكشف عن الهجمات**
    - **Reconnaissance:** Using tools like Nmap to scan a server.
    - **IDS Alert:** An alert for a web application attack in fast.log.
    - **Deep Analysis:** Using eve.json to analyze the attack details.
    - **Threat Intelligence:** Mapping detected activity to frameworks like MITRE ATT&CK to understand the attacker's tactics.
    - استخدم Nmap لفحص الخوادم، وتحليل التنبيهات مثل "هجوم على تطبيق ويب" باستخدام سجلات fast.logو eve.json.

SOHOLARKAZIM

5. **Incident Response & Packet Capture (PCAP) Analysis / الاستجابة للحوادث وتحليل التقاط الحزم (PCAP)**
    - **PCAP Files:** Network traffic captured for analysis.
    - **Response Actions:**
        - **Isolation:** Disconnect compromised machines.
        - **Containment:** Block the attacker's IP address.
        - **Eradication:** Follow threat intelligence advice.
    - استخدام ملفات PCAP للتحقيقات وتحليل الهجمات مع اتخاذ إجراءات مثل العزل والاحتواء.

Main Points Discussed / النقاط الرئيسية التي تم مناقشتها

1. **IDS Basics and Configuration / أساسيات IDS والإعدادات**
    - IDS detects suspicious network activity. Logs are essential for detecting threats and understanding network behavior.
    - نظام IDS يكتشف الأنشطة الشبكية المشبوهة. السجلات أساسية لاكتشاف التهديدات وفهم سلوك الشبكة.
2. **Suricata IDS Installation and Configuration / إعداد وتكوين سوركاتا IDS**
    - Suricata is an open-source IDS that also acts as an IPS. Installation involves configuring multiple aspects, including security.
    - سوركاتا هو نظام IDS مفتوح المصدر يعمل أيضًا كنظام IPS. يشمل التثبيت تكوين جوانب متعددة، بما في ذلك الأمان.
3. **Understanding Logs in IDS / فهم السجلات في IDS**
    - IDS logs like **fast.log** and **json.log** are crucial for detecting and analyzing intrusions.
    - سجلات IDS مثل fast.log و json.logمهمة جدًا للكشف عن التسللات وتحليلها.
4. **Configuration and Use of Documentation / التوثيق والاستخدام الفعّال**
    - Understanding documentation is crucial for setting up IDS like Suricata.
    - فهم الوثائق أمر بالغ الأهمية عند إعداد IDS مثل سوركاتا.
5. **Handling Alerts and Logs / التعامل مع التنبيهات والسجلات**
    - Alerts generated by IDS need to be analyzed using logs like **fast.log** and **json.log** for severity and correlation.
    - التنبيهات التي يولدها IDS يجب تحليلها باستخدام سجلات مثل fast.log و json.logلتحديد شدتها وربط الأحداث.
6. **Tools and Techniques / الأدوات والتقنيات**
    - **Nmap:** Scanning tool for detecting open ports and services.
    - **Apache Server Setup:** Understanding web server setups and vulnerabilities.

SCHOLARKAZIM

Nmap أداة لفحص الشبكة لاكتشاف البورتات المفتوحة والخدمات. تم شرح إعداد خوادم Apache وكيفية مسحها للكشف عن الثغرات.

Key Terminology and Concepts Explained / شرح المصطلحات والمفاهيم الرئيسية

1. **IDS:** Intrusion Detection System - Detects and alerts on potential security breaches.
2. **IPS:** Intrusion Prevention System - Detects and prevents attacks.
3. **Suricata:** Open-source IDS engine.
4. **fast.log:** A log format for quick alerts.
5. **json.log:** Detailed log format for deep analysis.
6. **Nmap:** A tool for network scanning.
7. **Log Correlation:** Analyzing and combining logs to understand deeper network activities.

- IDS: نظام كشف التسلل، IPS: نظام منع التسلل، سوركاتا: محرك IDS مفتوح المصدر، Nmap: أداة مسح الشبكة، Rبط السجلات: عملية دمج وتحليل السجلات لاكتشاف الأنشطة.

Examples Used / الأمثلة التي تم استخدامها

1. **Suricata Logs / سجلات سوركاتا**
   - Practical example of configuring Suricata and analyzing its logs to detect network anomalies.
   - المثال العملي حول كيفية تكوين سوركاتا وتحليل سجلاته لاكتشاف الأنماط المشبوهة في الشبكة.
2. **Real-Time Alerts / التنبيهات في الوقت الفعلي**
   - Demonstration of how Suricata triggers real-time alerts based on network traffic patterns.
   - عرض كيفية تشغيل سوركاتا للتنبيهات في الوقت الفعلي بناءً على أنماط حركة المرور الشبكية.
3. **Nmap Tool Example / مثال على أداة Nmap**
   - Nmap used to scan for open ports and detect vulnerabilities.
   - استخدم Nmap لفحص الشبكة واكتشاف البورتات المفتوحة.
4. **Apache Web Server Setup / إعداد خادم Apache**
   - Setting up Apache web server and using Nmap to scan open ports and services.
   - إعداد خادم Apache ثم استخدام Nmap لمسح البورتات المفتوحة والخدمات.

SCHOLARKAZIM

```
kazim@kazim:~$ sudo apt install apache2
[sudo] password for kazim:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0
  ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 2 not upgraded.
Need to get 2,090 kB of archives.
After this operation, 8,113 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure (1) shows installing apatche 2

we will run **Nmap scripts**, in network security they refer to prewritten scripts that automate tasks such as information gathering, vulnerability scanning, and exploitation. These scripts are essential for identifying potential weaknesses in a network or web application of the given Ip address over ubuntu server port 80

```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-enum -p 80 192.168.100.44
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-07 05:26 EST
Nmap scan report for 192.168.100.44
Host is up (0.00060s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:8F:67:A8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Figure (2) shows simple network scanning

Log Analysis and HTTP Requests

Now, after running the enumeration scripts, we need to analyze the logs generated by the system. In this case, using **sudo cat** to view the logs in **/var/log/fast.log** is one way to inspect the activities taking place.

For example, if Nmap detects a port scan or an HTTP request, the log will show the source IP address (e.g., 192.168.1.270), indicating that someone is probing your server.

A common classification for this type of behavior is **Web Application Attacks**. If an attacker is scanning the server for vulnerabilities, the log will indicate an attempt to exploit the system.

When monitoring network traffic, especially when dealing with large log files, it's important to use filtering commands to manage the data effectively. For instance, the **tail command** can help us focus on the most recent entries in the log files, such as using `tail -f fast.log`.

When analyzing network traffic, we use tools like *Wireshark*. These tools help monitor data traveling in and out of the network. Think of it like a traffic camera watching cars (data packets) traveling through a street (network).

Packet Capture Files (PCAP):

We can use *PCAP files* to analyze specific traffic. These files contain data about network activity, including the source, destination, and protocol used. For example, if we want to investigate an incident, we use the PCAP file to track the movement of suspicious traffic.

```
02/07/2026-11:18:53.218744  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47304 -> 192.168.100.44:80
02/07/2026-11:18:53.218744  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47304 -> 192.168.100.44:80
02/07/2026-11:18:53.218744  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47304 -> 192.168.100.44:80
02/07/2026-11:18:53.218744  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47304 -> 192.168.100.44:80
02/07/2026-11:18:53.218744  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47304 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
02/07/2026-11:18:53.230419  [**] [1:2024364:5] ET SCAN Possible Nmap User-Agent Observed [**] [Classification: Web Application Attack]
 [Priority: 1] {TCP} 192.168.100.38:47312 -> 192.168.100.44:80
```

Figure (3) shows fast.log Socrata

Example log line:

```
02/07/2026-11:18:53.218744 [**] [Priority: 1] {TCP}
192.168.100.41:40434 -> 192.168.100.48:80 Nmap User-Agent
Observed [**] [Classification: Web Application Attack]
```

1. **Date and Time:**

```
02/07/2026-11:18:53.218744
```

^: This is the **timestamp** when the event was recorded. It includes the **date** (02/07/2026) and **time** (11:18:53) with **microsecond precision** (218744).

2. **Priority Level:**

```
[Priority: 1]
```

^: **Priority 1** indicates the **severity level** of the event, with "1" representing a **critical event** that requires immediate attention.

3. **Protocol Type:**

```
{TCP}
```

^: This shows that the **protocol used** for this communication is **TCP** (Transmission Control Protocol), which ensures reliable delivery of data across networks.

4. **Source IP and Port:**

```
192.168.100.41:40434
```

^: This is the **source IP address** (192.168.100.41) and **source port** (40434) from which the network traffic originated. It shows where the request is coming from.

5. **Destination IP and Port:**

```
-> 192.168.100.48:80
```

^: This part indicates the **destination IP address** (192.168.100.48) and **destination port** (80). Port 80 is commonly used for HTTP traffic, which suggests the request is targeting a web server.

SCHOLARKAZIM

6. **Action/Alert Message:**

Nmap User-Agent Observed
^: This part indicates that a **network scan** using **Nmap** was observed, specifically a probe for the **User-Agent** (often related to identifying a web application). It is part of the detection that recognizes this as a potential attack attempt.

7. **Event Classification:**

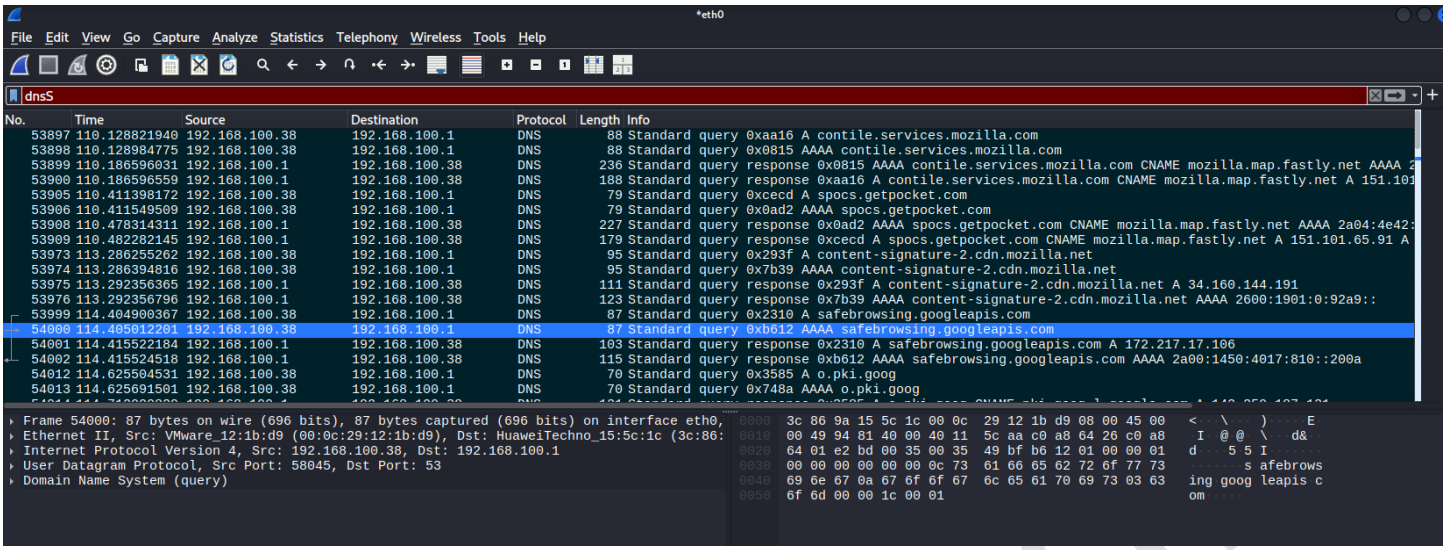
[Classification: Web Application Attack]
^: This indicates the **classification** of the event, marking it as a **Web Application Attack**, which suggests that the network scan is aimed at finding vulnerabilities in a web application.

Full Explanation:

1. The log captures a **network scanning event** at a specific time (02/07/2026-11:18:53.218744), marked as a **critical event** (priority 1).
2. The scan is coming from the source IP (192.168.100.41) and port (40434), targeting the destination IP (192.168.100.48) at port 80 (standard for HTTP services).
3. The scan is identified as coming from a **User-Agent** that was observed in the logs, which is indicative of an **Nmap scan**, a tool used for discovering open ports and vulnerabilities.
4. This type of scan is classified as a **Web Application Attack**, which often involves probing the web server for weaknesses.

Network Traffic Analysis with Wireshark and Packet Capturing

SCHOLARKAZIM



Figure(4) shows DNS queries being captured. This indicates that you are monitoring the network traffic, which is essential for understanding the data being exchanged over the network.

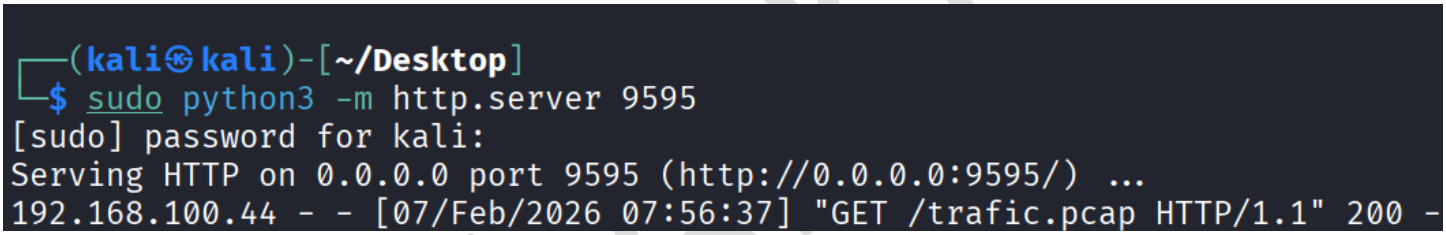


Figure (5) shows using Python's built-in HTTP server to transform files

attempting to transfer a trafic.pcap file over an HTTP server running on port 9000 using Python's built-in HTTP server. Despite successfully analyzing the file with the Suricata Intrusion Detection System (IDS), an error stating "Scheme missing" arises during the attempt to download the file using wget. This report investigates the root cause of the issue and suggests corrective actions to resolve it.

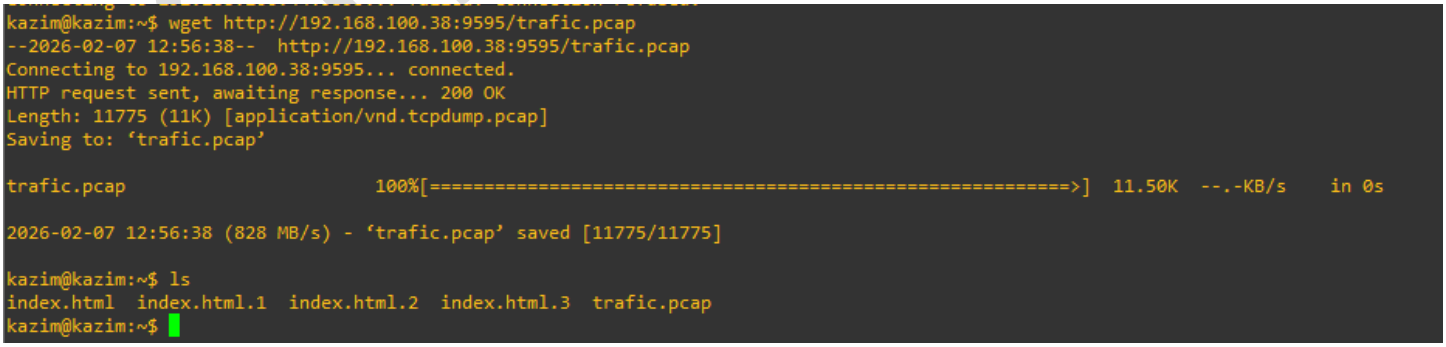


Figure (6) shows the file has been transferred

The Suricata Intrusion Detection System successfully parsed the trafic.pcap file, detecting 40 alerts related to network traffic anomalies. This confirms that the file is intact and can be

processed by network security tools. The IDS executed the analysis without errors, but the issue arises during the file transfer process.

```
kazim@kazim:~$ sudo suricata -r trafic.pcap
[sudo] password for kazim:
Notice: suricata: This is Suricata version 8.0.3 RELEASE running in USER mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: suricata: Preparing unexpected signal handling
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 48236 rules successfully loaded, 0 rules failed, 0 rules skipped
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 48240 signatures processed. 1257 are IP-only rules, 4467 are inspecting packet payload, 42281 inspect application layer,
 110 are decoder event only
Notice: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable: 113
Info: pcap: Starting file run for trafic.pcap
Info: pcap: pcap file trafic.pcap end of file reached (pcap err code 0)
Notice: threads: Threads created -> RX: 1 W: 2 FM: 1 FR: 1   Engine started.
Notice: suricata: Signal Received.  Stopping engine.
Info: suricata: time elapsed 0.184s
Notice: pcap: read 1 file, 80 packets, 10471 bytes
Info: counters: Alerts: 40
kazim@kazim:~$
```

Figure (7) the Suricata IDS has successfully processed the trafic.pcap file and detected 40 alerts

SCHOLARKA