

College Name	<b>University of Hertfordshire SEGi</b> <b>College Subang Jaya</b>										
Programme Name	<b>BACHELOR OF SCIENCE (HONS) COMPUTER SCIENCE (CYBER SECURITY AND NETWORKS)</b>										
Module Name	<b>CYBER SECURITY AND NETWORKS PROJECT</b>	Module Code	<b>6COM1040</b>								
		Semester	<b>September 2025</b>								
Module Leader	<b>Dr. Aneshkumar Thangaveloo</b>										
Lecturer Name	<b>Ms. Nur Diana Madinah Binti Ab Hadi</b>										
Student's declaration	<p>I hereby certify that this assignment is my own work and where materials have been used from other resources, they have been properly acknowledged. I also understand I will face the possibility of failing the module if the content of this assignment is plagiarized.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>No.</th> <th>Name</th> <th>Student ID</th> <th>Signature / Initial</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>PATRICK ROGERS</td> <td>SCSJ2100424</td> <td>PAT</td> </tr> </tbody> </table> <p>Date:</p>			No.	Name	Student ID	Signature / Initial	1	PATRICK ROGERS	SCSJ2100424	PAT
	No.	Name	Student ID	Signature / Initial							
	1	PATRICK ROGERS	SCSJ2100424	PAT							
Release Date	Submission Due Date	Marks obtained:									
Date Received	Student's work assessed by / date	<input type="text"/>									

**Module Leader's Feedback.**

Module Leader's comments / feedback	
Student's comments	

## Table of Contents

1.0 Testing and Problem-Solving.....	4
1.1 Nmap Scanning.....	4
1.2 Intrusion Detection Logs.....	5
1.3 Suricata Alerts and Detection Summary .....	6
1.4 Traffic Capture Verification .....	7
1.5 Vulnerability Assessment and Recommended Improvements .....	7
1.6 Conclusion of Assessment .....	8

## Table of Figures

Figure 1 Nmap Scan.....	4
Figure 2 Service Version Scan .....	5
Figure 3 Suricata IDS Running.....	6
Figure 4 Suricata Detection Summary .....	6
Figure 5 TCPDump Traffic Capture .....	7

## 1.0 Testing and Problem-Solving

A thorough testing process was conducted to validate the security measures and identify potential vulnerabilities. Testing was performed from the Kali administrative machine, simulating realistic attacks against the Ubuntu server.

### 1.1 Nmap Scanning

Nmap is a network scanning tool that detects open ports, running services, and system fingerprints. Several scans were performed:

Basic Scan: Identified open ports (80, 3000).

```
(patrick@kali)-[~]
$ nmap 192.168.56.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 02:48 +08
Nmap scan report for 192.168.56.16
Host is up (0.0028s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   closed https
3000/tcp  open   ppp
MAC Address: 08:00:27:4F:5C:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.96 seconds
```

Figure 1 Nmap Scan

**Service Version Scan:** Revealed software versions such as nginx 1.29.3 and Juice Shop application, enabling assessment of outdated or vulnerable services.

```
SF-Port3000-TCP:V=7.95%I=7%D=12/5%Time=6931D816%P=x86_64-pc-linux-gnu%r(Ge
SF:Request,3890,"HTTP/1.1\x20200\x200K\r\nAccess-Control-Allow-Origin:\x
SF:20\*\r\nContent-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SAMEO
SF:RIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#/jo
SF:bs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=0
SF:\r\nLast-Modified:\x20Thu, \x2004\x20Dec\x202025\x2016:36:48\x20GMT\r\nE
SF:Tag:\x20W/"1252f-19aea3934c0"\r\nContent-Type:\x20text/html;\x20chars
SF:et=UTF-8\r\nContent-Length:\x2075055\r\nVary:\x20Accept-Encoding\r\nDat
SF:et:\x20Thu,\x2004\x20Dec\x202025\x2018:51:02\x20GMT\r\nConnection:\x20cl
SF:ose\r\n\r\n!— \n\x20\x20\x20Copyright\x20(c)\x202014-2026\x20Bjoern
SF:\x20Kimmich\x20\x20the\x20WASP\x20Juice\x20Shop\x20contributors.\n
SF:\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20→\n\n<doctype>
SF:<html>\n<html\x20lang="en"\x20data-beasties-container>\n<head>\n\x2
SF:<meta\x20charset="utf-8">\n<x20>\n<title>OWASP\x20Juice\x20Shop
SF:</title>\n<x20>\n<meta\x20name="description"\x20content="Probably\x
SF:\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x20a
SF:pplication">\n<x20>\n<meta\x20name="viewport"\x20content="width=de
SF:vice-width,\x20initial-scale=1">\n<x20>\n<link\x20id="favicon"\x20r
SF:el="icon"\x20"$(Help,2F,"HTTP/1.\x20400\x20Bad\x20Request\r\nConn
SF:ection:\x20close\r\n\r\n")$(NCP,2F,"HTTP/1.\x20400\x20Bad\x20Request
SF:r\r\nConnection:\x20close\r\n\r\n")$(HTTPOptions,EA,"HTTP/1.\x20204\x
SF:20No\x20Content\r\nAccess-Control-Allow-Origin:\x20\*\r\nAccess-Control
SF:-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-Co
SF:ntrol-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2004\x2
SF:0Dec\x202025\x2018:51:02\x20GMT\r\nConnection:\x20close\r\n\r\n")$(RTS
SF:PRequest,EA,"HTTP/1.\x20204\x20No\x20Content\r\nAccess-Control-Allow-
SF:Origin:\x20\*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,PO
```

Figure 2 Service Version Scan

The scan identified the OWASP Juice Shop application running on port 3000 and a web server on port 80. Enumerating these service versions is critical for identifying potential vulnerabilities and focusing subsequent security testing.

## 1.2 Intrusion Detection Logs

**Suricata IDS Running Status:** To show that Suricata was actively monitoring the DMZ interface, you would use the screenshot that proves the engine started successfully and loaded the detection rules.

```
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: ioctl: enp0s8: MTU 1500
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.js
on
Info: logopenfile: stats output device (regular) initialized: stats.lo
g
Info: detect: 1 rule files processed. 46600 rules successfully loaded,
0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 46603 signatures processed. 1006 are IP-only rules, 4423
are inspecting packet payload, 40944 inspect application layer, 108 a
re decoder event only
Info: runmodes: enp0s8: creating 4 threads
Info: unix-manager: unix socket '/var/run/suricata-command.socket'
Notice: threads: Threads created -> W: 4 FM: 1 FR: 1   Engine started.
```

Figure 3 Suricata IDS Running

Confirmed that the Suricata engine was successfully initialized and running in IDS mode, monitoring the DMZ network interface (enp0s8) and processing 46603 detection rules. During testing, Suricata captured various suspicious activities, including Nmap OS detection, SYN scans, and service enumeration.

### 1.3 Suricata Alerts and Detection Summary

```
Info: suricata: time elapsed 240.513s
Info: counters: Alerts: 78
Notice: device: enp0s8: packets: 3874, drops: 0 (0.00%), invalid checksum: 0
```

Figure 4 Suricata Detection Summary

- During testing, Suricata captured various suspicious activities, including Nmap OS detection, SYN scans, and service enumeration.
- The alert counters confirmed that the Intrusion Detection System successfully generated a total of 78 alerts against the target traffic, demonstrating the IDS's ability to identify probing attempts.
- These logs demonstrate that the IDS can detect attempts to probe system vulnerabilities, allowing timely intervention before an attacker can exploit any service. By monitoring

both payload content and network patterns, Suricata ensures that even subtle reconnaissance attempts are logged.

#### 1.4 Traffic Capture Verification

```
vboxuser@A2Z:~$ sudo tcpdump -i enp0s8 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:03:45.988364 IP 192.168.56.16.3000 > 192.168.56.15.50458: Flags [P.], seq 490
104243:490104246, ack 128173706, win 505, options [nop,nop,TS val 1315183716 ecr
4282846271], length 3
19:03:45.992788 IP 192.168.56.15.50458 > 192.168.56.16.3000: Flags [P.], seq 1:8
```

Figure 5 TCPDump Traffic Capture

Traffic Capture Verification tcpdump was executed on the Ubuntu server's DMZ interface to capture and inspect raw network packets. This process confirmed that all traffic, including scanning attempts and normal web requests to the Juice Shop on port 3000, was being logged at the network layer. This validates that the monitoring infrastructure is functional and capable of capturing detailed traffic for analysis, supporting both reactive incident response and proactive security measures.

#### 1.5 Vulnerability Assessment and Recommended Improvements

Vulnerability	Impact/Risk	Recommended Improvement
Unencrypted HTTP Traffic	High - vulnerable to MITM attacks	Enforce HTTPS with Nginx reverse proxy
Direct Exposure of Juice Shop	High - intentionally vulnerable app	Restrict port 3000 to trusted IPs / use WAF
Software Version Disclosure	Medium - helps attackers find exploits	Mask Nginx version numbers
High IDS Alert Volume	Low - operational risk	Integrate Suricata logs with SIEM

## **1.6 Conclusion of Assessment**

The testing confirmed that the implemented defence-in-depth model (UFW, Docker, Suricata) is fundamentally functional and prevents unauthorized services from being exposed. The immediate next steps must focus on hardening the application access plane by enforcing encryption and limiting the exposure of the vulnerable application to maintain the security posture required by A2Z Corporation.