

College Name	University of Hertfordshire SEGi College Subang Jaya										
Programme Name	BACHELOR OF SCIENCE (HONS) COMPUTER SCIENCE (CYBER SECURITY AND NETWORKS)										
Module Name	CYBER SECURITY AND NETWORKS PROJECT	Module Code	6COM1040								
		Semester	September 2025								
Module Leader	Dr. Aneshkumar Thangaveloo										
Lecturer Name	Ms. Nur Diana Madinah Binti Ab Hadi										
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

4.0 Testing and Problem-Solving.....	4
4.1 Vulnerability Assessment and Penetration Testing Process	4
4.2 Intrusion Detection and Monitoring Results.....	5
4.3 Identified Vulnerabilities and Suggested Improvements	6
4.4 Summary	7

Table of Figures

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

4.0 Testing and Problem-Solving

A comprehensive testing and vulnerability assessment process was conducted to evaluate the robustness of the security measures implemented for A2Z Corporation's internet-facing infrastructure. The goal of this phase was to replicate realistic attack scenarios, identify weaknesses, validate detection and monitoring mechanisms, and ensure that the defence-in-depth design effectively mitigates external threats. All testing activities were performed from the admin-Kali-PC located within the internal LAN, simulating both insider and outsider attack vectors.

4.1 Vulnerability Assessment and Penetration Testing Process

The assessment began with baseline reconnaissance using Nmap, aimed at discovering open ports, accessible services, and potential system misconfigurations. A standard TCP SYN scan was executed to determine the attack surface exposed by the DMZ-Ubuntu-Server. The results revealed four open ports 22 (SSH), 80 (HTTP), 443 (HTTPS), and 3000 (Juice Shop application) indicating that only essential services were reachable from external networks. This aligned with the firewall policies configured earlier and confirmed that unnecessary ports remained secured by UFW's default deny rules.

```
(patrick㉿kali)-[~]
$ nmap 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 13:05 +08
Nmap scan report for 192.168.56.101
Host is up (0.00089s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3000/tcp  open  ppp
MAC Address: 08:00:27:98:E8:7B (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 18.29 seconds
```

Figure 1: Nmap Scan

To verify network visibility and packet flow monitoring, tcpdump was executed on the DMZ interface (enp0s8). The captured traffic logs confirmed that both normal application traffic and scanning attempts were detected at the packet level. This validated that packet capture capabilities were functioning correctly and that detailed traffic analysis could be performed during incidents.

```
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 2: TCPDump Traffic Capture

4.2 Intrusion Detection and Monitoring Results

Advanced intrusion attempts were simulated to test the responsiveness of the Suricata IDS deployed on the DMZ server. Tests included OS fingerprinting scans, aggressive SYN scanning, and service enumeration techniques commonly used by attackers during the reconnaissance phase. Suricata successfully detected these behaviours, generating alerts related to Nmap OS detection, suspicious SYN flag patterns, and possible brute-force attempts. The IDS loaded 46,603 detection rules during initialization and actively processed threat signatures against incoming traffic.

```
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

The detection summary demonstrated a total of 78 triggered alerts, confirming the IDS's effectiveness in recognising hostile traffic patterns. This validated that the network monitoring layer was functioning as intended, identifying malicious activity before exploitation could occur.

```
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

4.3 Identified Vulnerabilities and Suggested Improvements

Although the system performed strongly during testing, several vulnerabilities were identified that require remediation:

- **Unencrypted HTTP Traffic:** Port 80 remained accessible, making initial connections susceptible to man-in-the-middle (MITM) attacks. Improvement: Enforce HTTPS using a Nginx reverse proxy and automatically redirect all HTTP requests to port 443.
- **Direct Exposure of the Juice Shop Application (Port 3000):** This intentionally vulnerable application should not remain publicly reachable. Improvement: Restrict port 3000 to trusted internal IP addresses or protect it with a Web Application Firewall (WAF).
- **High Volume of IDS Alerts:** Although alerts indicate visibility, they may overwhelm administrators. Improvement: Integrate Suricata logs into a central SIEM to filter false positives, correlate events, and streamline incident response.
- **Software Version Disclosure:** Banner information from services may assist attackers in identifying exploit paths. Improvement: Mask software versions in Nginx and disable unnecessary headers.

4.4 Summary

The testing process confirmed that firewall rules, container isolation, and intrusion detection mechanisms were properly implemented and effective. While a few vulnerabilities were detected, all were manageable and accompanied by clear mitigation strategies. The combination of tools Nmap, Suricata IDS, and tcpdump demonstrated strong monitoring, restricted attack surface, and reliable detection capabilities, validating the security posture of A2Z Corporation's internet-facing infrastructure.