<table>
<tr><td>College Name</td><td colspan="3">University of Hertfordshire SEGi
College Subang Jaya</td></tr>
<tr><td>Programme Name</td><td colspan="3">BACHELOR OF SCIENCE (HONS) COMPUTER SCIENCE (CYBER SECURITY AND NETWORKS)</td></tr>
<tr><td rowspan="2">Module Name</td><td rowspan="2">CYBER SECURITY AND NETWORKS PROJECT</td><td>Module Code</td><td>6COM1040</td></tr>
<tr><td>Semester</td><td>September 2025</td></tr>
<tr><td>Module Leader</td><td>Dr. Aneshkumar Thangaveloo</td><td rowspan="2">Assessment Type</td><td rowspan="2">Vulnerability Assessment Report</td></tr>
<tr><td>Lecturer Name</td><td>Ms. Nur Diana Madinah Binti Ab Hadi</td></tr>
<tr><td>Student’s declaration</td><td colspan="3">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.

<table><tr><th>No.</th><th>Name</th><th>Student ID</th><th>Signature / Initial</th></tr><tr><td>1</td><td>PATRICK ROGERS</td><td>SCSJ2100424</td><td>PAT</td></tr></table>Date:</td></tr>
<tr><td>Release Date</td><td></td><td>Submission Due Date</td><td></td><td rowspan="2">Marks obtained:</td></tr>
<tr><td>Date Received</td><td></td><td>Student’s work assessed by / date</td><td></td></tr>
</table>

Module Leader's Feedback.

Module Leader's comments / feedback	
Student's comments	

Table of Contents

Table of Figures

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.

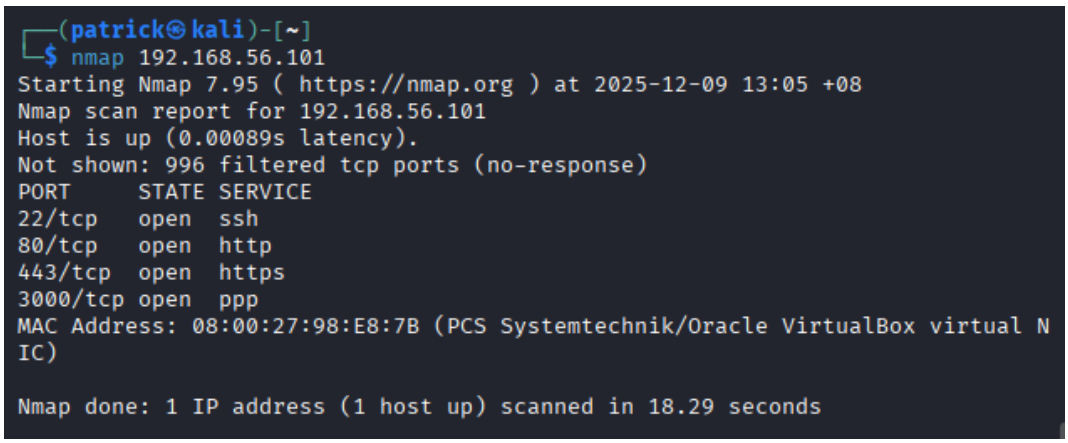

Figure 1: Nmap Scan

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.

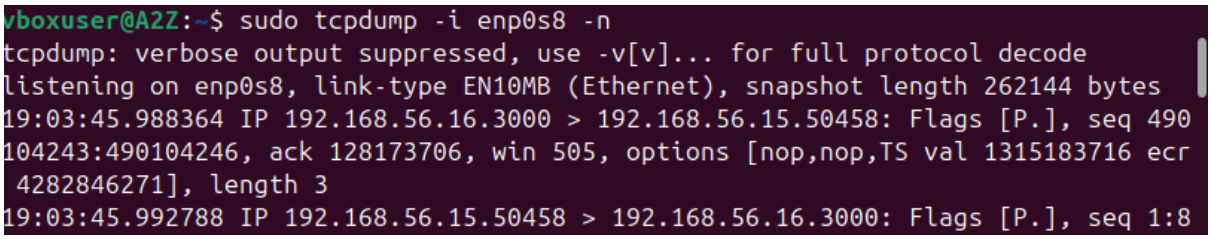

Figure 2: TCPDump Traffic Capture

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.

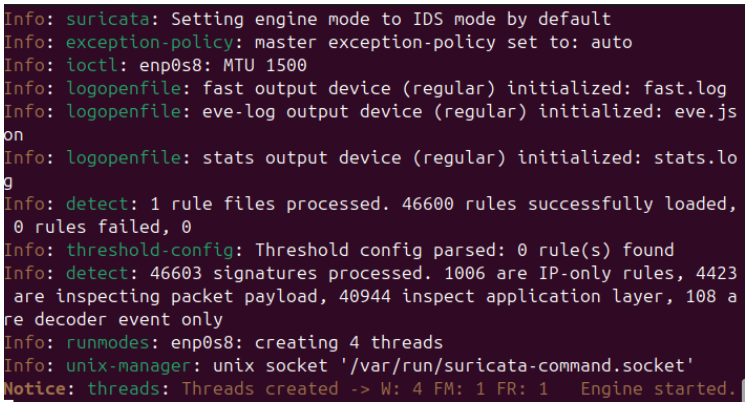

Figure 3 Suricata IDS Running

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.

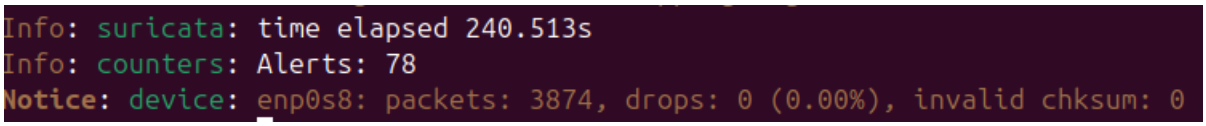

Figure 4: Suricata Detection Summary

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.