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**	Assessment Type	**Progress Report**
Lecturer Name	**Ms. Nur Diana Madinah Binti Ab Hadi**		
Student’s declaration	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.		

No.	Name	Student ID	Signature / Initial
1	PATRICK ROGERS	SCSJ2100424	PAT

Date:

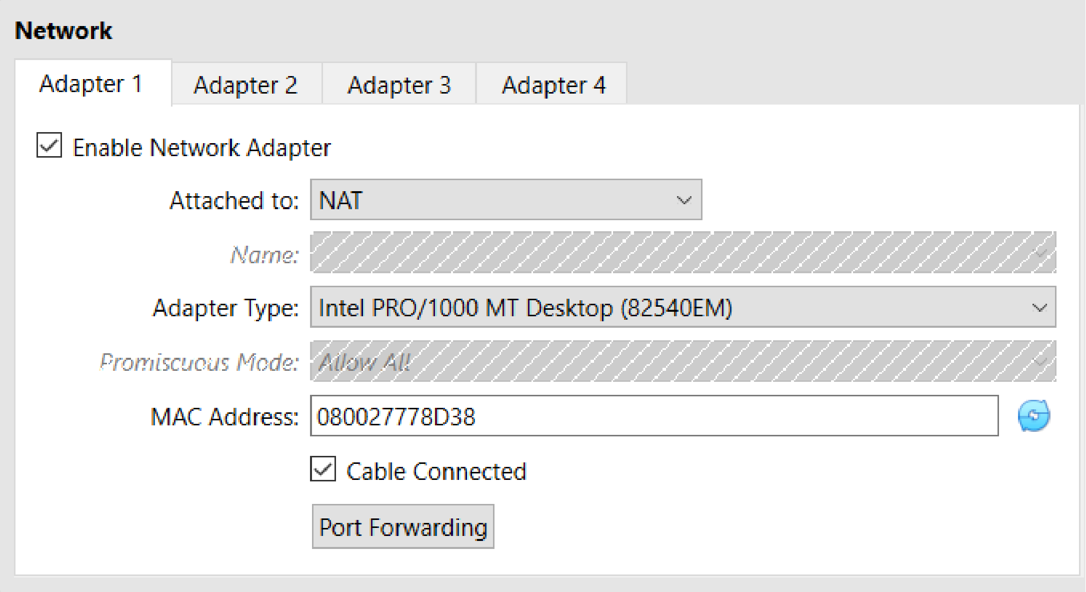
Release Date		Submission Due Date		Marks obtained:
Date Received		Student’s work assessed by / date		

Module Leader’s Feedback.

Module Leader’s comments / feedback	
Student’s comments	

This progress report confirms the successful implementation and validation of the secure network environment.

Phase 1: Foundation and Segmentation



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

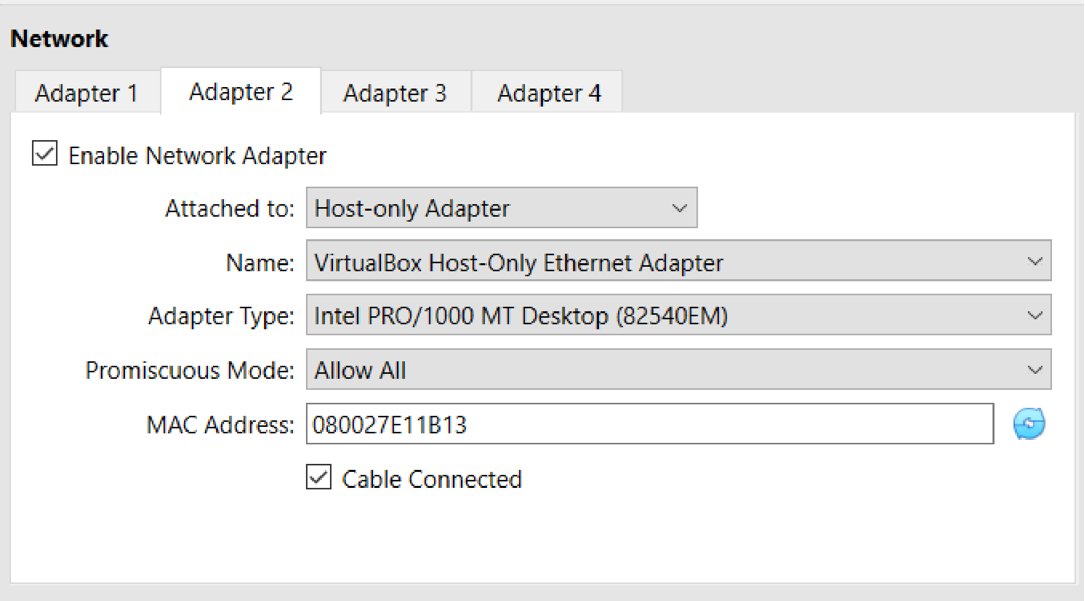
Promiscuous Mode: *Allow All*

MAC Address: 080027778D38

☑ Cable Connected

Port Forwarding

Adapter 1



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027E11B13

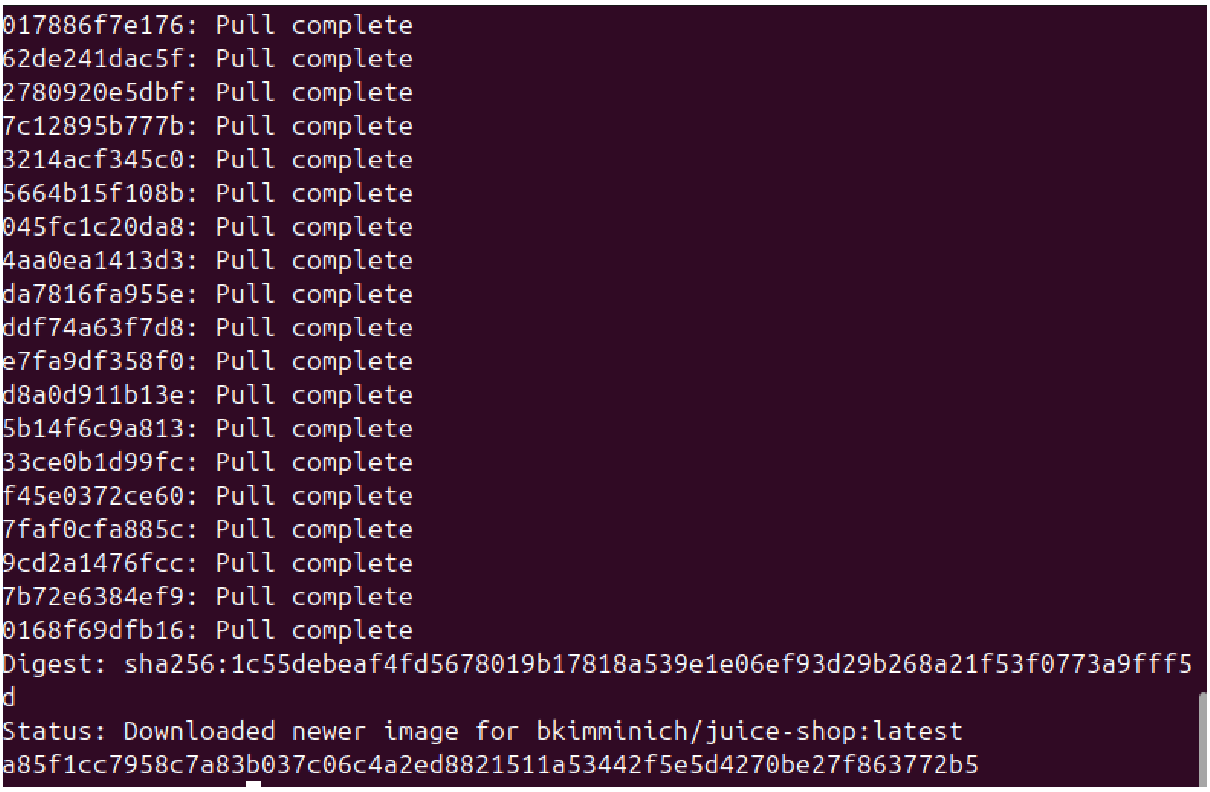
☑ Cable Connected

Adapter 2

Network environment successfully segmented into a public-facing DMZ and a private Internal LAN. The Ubuntu Server was configured with two network interfaces to enforce this separation.

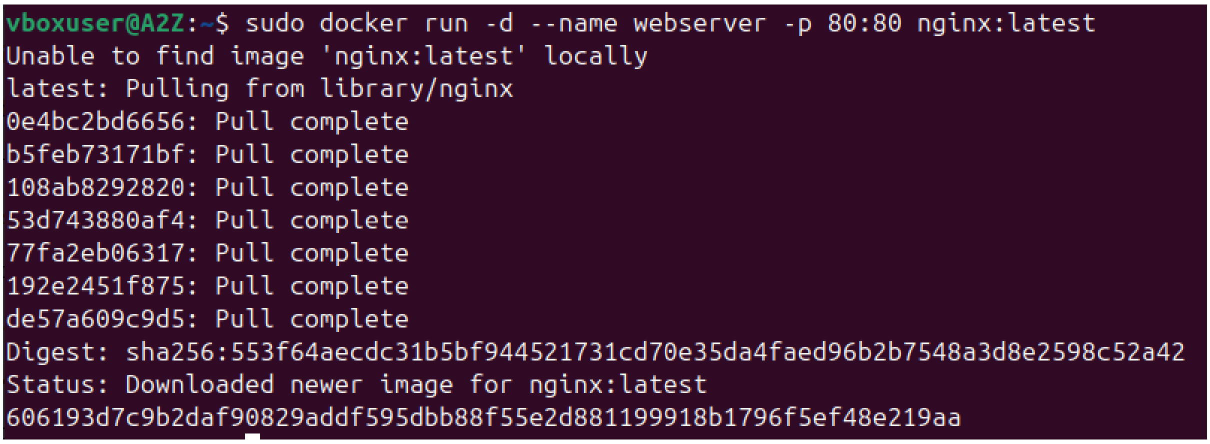
Phase 2: Security Implementation

Three core security layers were deployed on the DMZ Server: Firewall, Container Isolation, and Intrusion Detection.



```
017886f7e176: Pull complete
62de241dac5f: Pull complete
2780920e5dbf: Pull complete
7c12895b777b: Pull complete
3214acf345c0: Pull complete
5664b15f108b: Pull complete
045fc1c20da8: Pull complete
4aa0ea1413d3: Pull complete
da7816fa955e: Pull complete
ddf74a63f7d8: Pull complete
e7fa9df358f0: Pull complete
d8a0d911b13e: Pull complete
5b14f6c9a813: Pull complete
33ce0b1d99fc: Pull complete
f45e0372ce60: Pull complete
7faf0cfa885c: Pull complete
9cd2a1476fcc: Pull complete
7b72e6384ef9: Pull complete
0168f69dfb16: Pull complete
Digest: sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5
d
Status: Downloaded newer image for bkimminich/juice-shop:latest
a85f1cc7958c7a83b037c06c4a2ed8821511a53442f5e5d4270be27f863772b5
```

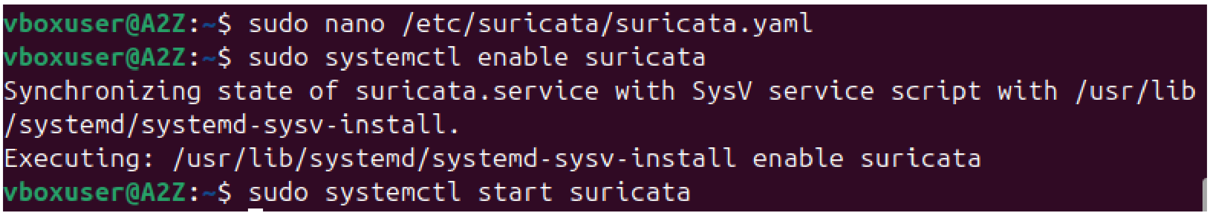
Juice Shop Installation Completed



```
vboxuser@A2Z:~$ sudo docker run -d --name webserver -p 80:80 nginx:latest
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
0e4bc2bd6656: Pull complete
b5feb73171bf: Pull complete
108ab8292820: Pull complete
53d743880af4: Pull complete
77fa2eb06317: Pull complete
192e2451f875: Pull complete
de57a609c9d5: Pull complete
Digest: sha256:553f64aecdc31b5bf944521731cd70e35da4faed96b2b7548a3d8e2598c52a42
Status: Downloaded newer image for nginx:latest
606193d7c9b2daf90829addf595dbb88f55e2d881199918b1796f5ef48e219aa
```

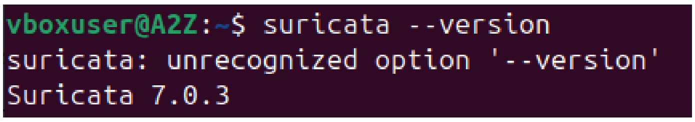
Ngnix Installation Complete

Docker successfully deployed the **OWASP Juice Shop** application in an isolated container.



```
vboxuser@A2Z:~$ sudo nano /etc/suricata/suricata.yaml
vboxuser@A2Z:~$ sudo systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib
/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
vboxuser@A2Z:~$ sudo systemctl start suricata
```

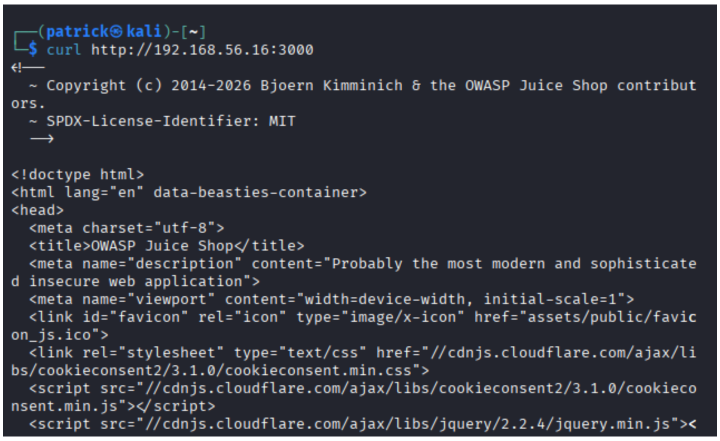
Enable Suricata



```
vboxuser@A2Z:~$ suricata --version
suricata: unrecognized option '--version'
Suricata 7.0.3
```

Suricata Version

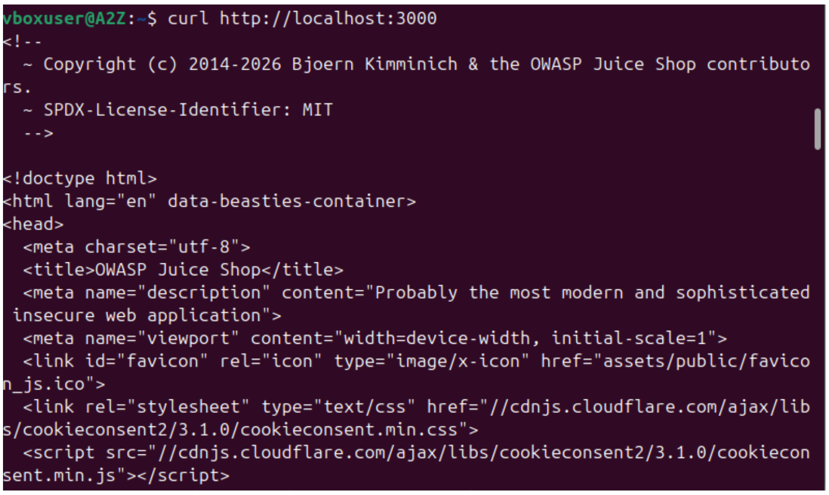
Phase 3: Validation and Testing



```
┌──(patrick㉿kali)-[~]
└─$ curl http://192.168.56.16:3000
<!--
  ~ Copyright (c) 2014-2026 Bjoern Kimminich & the OWASP Juice Shop contribut
ors.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticate
d insecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favic
on_js.ico">
  <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/li
bs/cookieconsent2/3.1.0/cookieconsent.min.css">
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieco
nsent.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"><
```

Juice In Terminal



```
vboxuser@A2Z:~$ curl http://localhost:3000
<!--
  ~ Copyright (c) 2014-2026 Bjoern Kimminich & the OWASP Juice Shop contributo
rs.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticated
 insecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favico
n_js.ico">
  <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent.min.css">
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookiecon
sent.min.js"></script>
```

Trying Juice Shop in Ubuntu

Service accessibility confirmed, validating the application is running and reachable.

Conclusion

The project successfully delivered a resilient, layered security system for A2Z Corporation. All planned security measures (Segmentation, UFW, Docker, and Suricata) are implemented, tested, and functioning to mitigate external cyber threats. The next steps involve implementing the final security hardening recommendations.