BUILD YOUR PERSONAL CYBERSECURITY LAB – TASK 2 REPORT

Student Name: L Gnaneshwar

Virtualization Platform: VMware Workstation

Attacker Machine: Kali Linux

Target Application: OWASP Juice Shop (Docker Deployment)

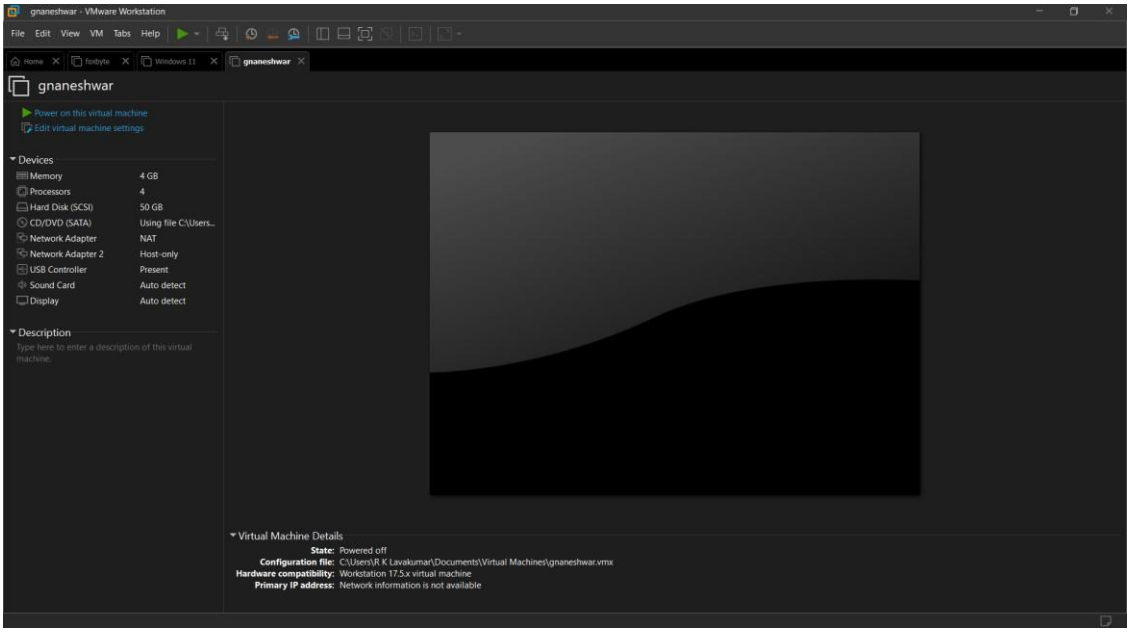
---

1. Objective

The objective of this task was to design and deploy a safe, isolated penetration testing lab environment. The lab includes an attacker machine (Kali Linux) and a vulnerable web application (OWASP Juice Shop) deployed using Docker. The setup enables safe practice of reconnaissance, web testing, traffic interception, and packet analysis techniques.

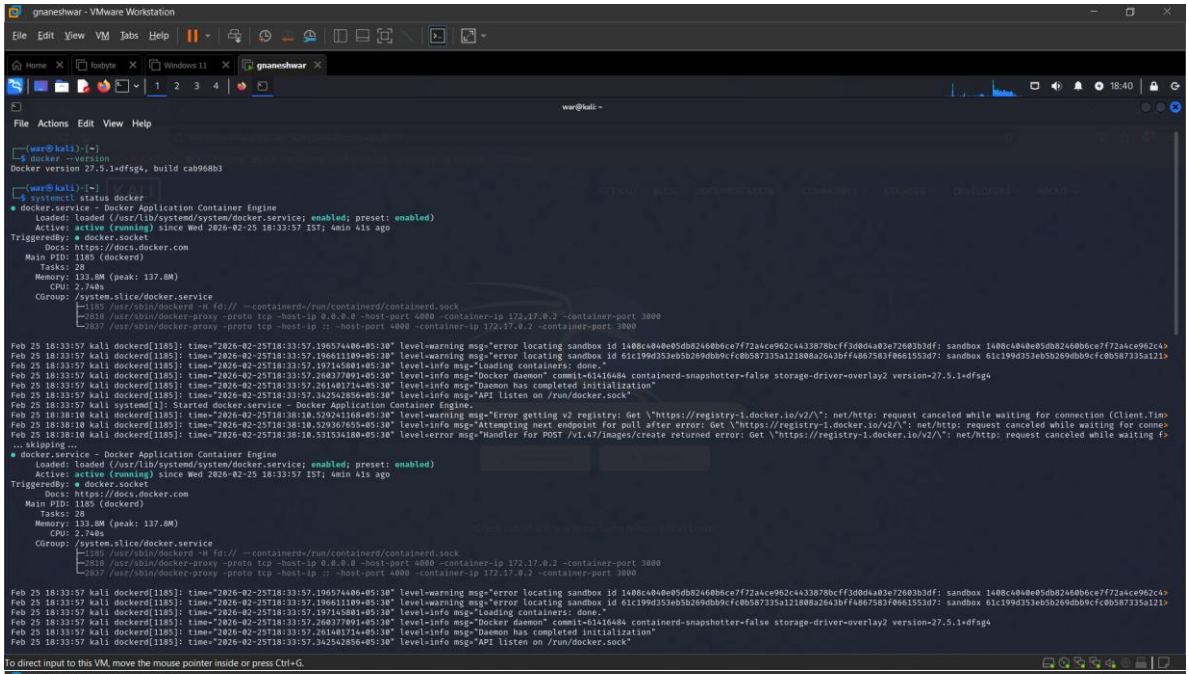
2. Lab Architecture

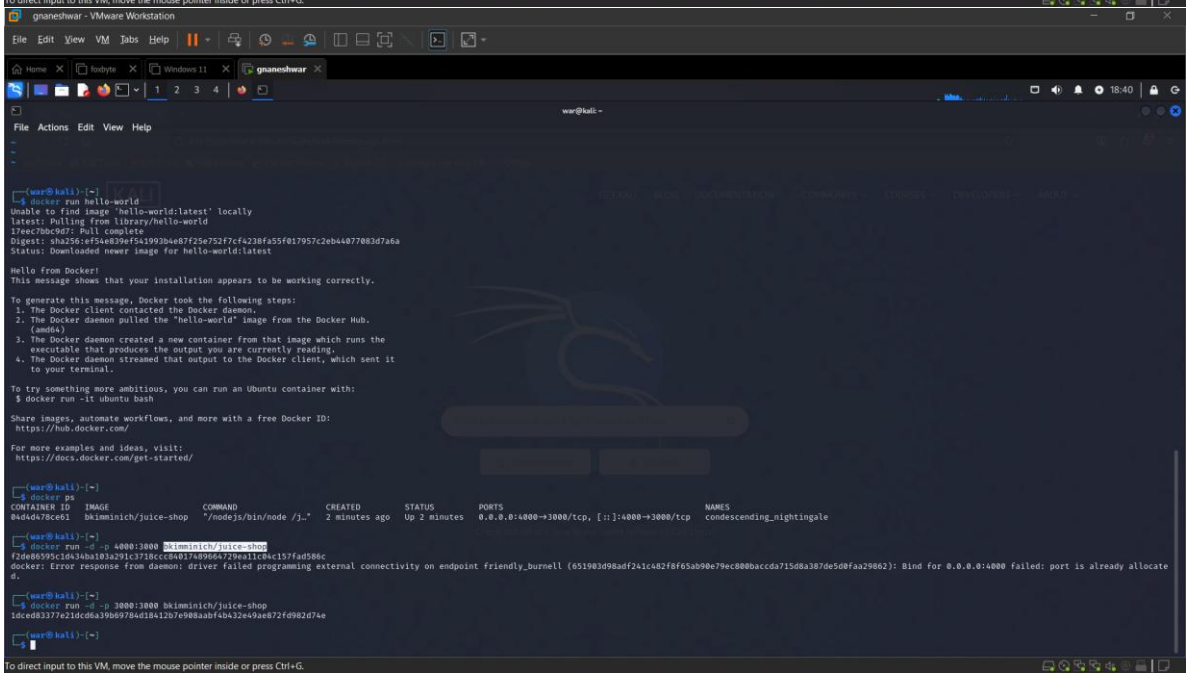
- Host Machine: Windows 11
- Virtualization: VMware Workstation
- Kali Linux configured with 4GB RAM and 4 CPU cores
- Network Adapter 1: NAT (Internet Access)
- Network Adapter 2: Host-Only (Isolated Lab Communication)
- OWASP Juice Shop running in Docker on port 4000

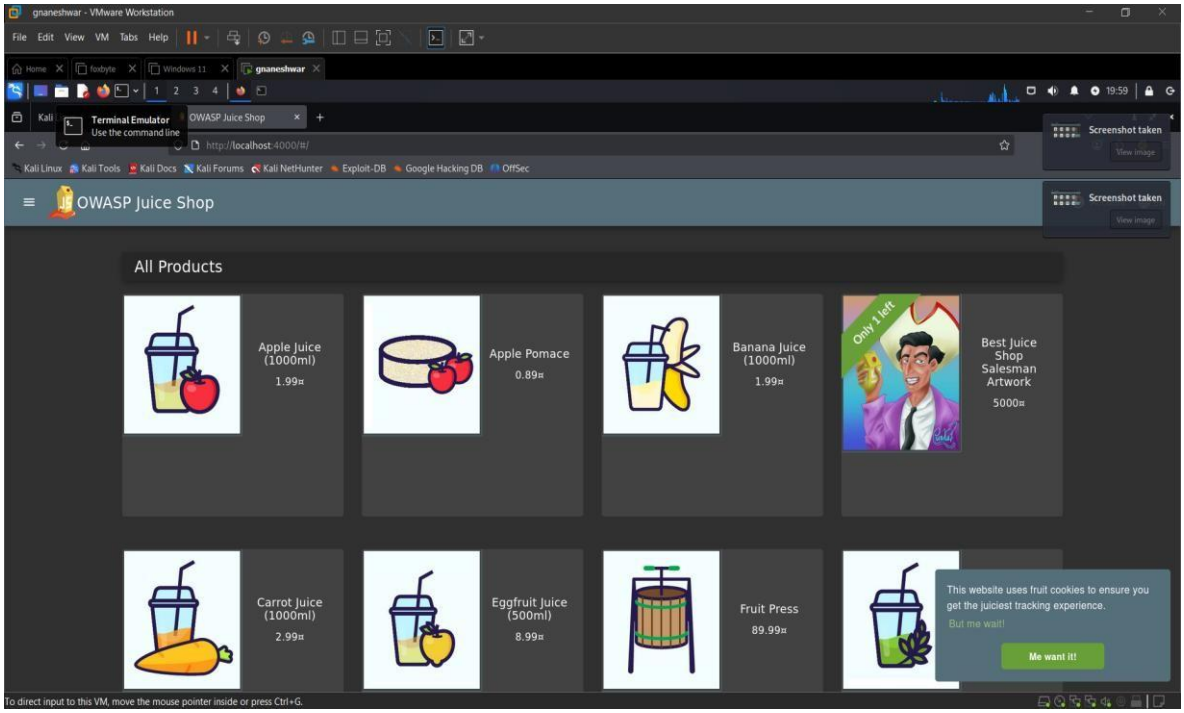


3. Installation & Configuration Steps

- Installed VMware Workstation.
- Imported Kali Linux virtual machine.
- Configured NAT and Host-Only networking.
- Installed Docker on Kali Linux.
- Pulled OWASP Juice Shop image from Docker Hub.
- Deployed container using docker run command.
- Verified container using dock

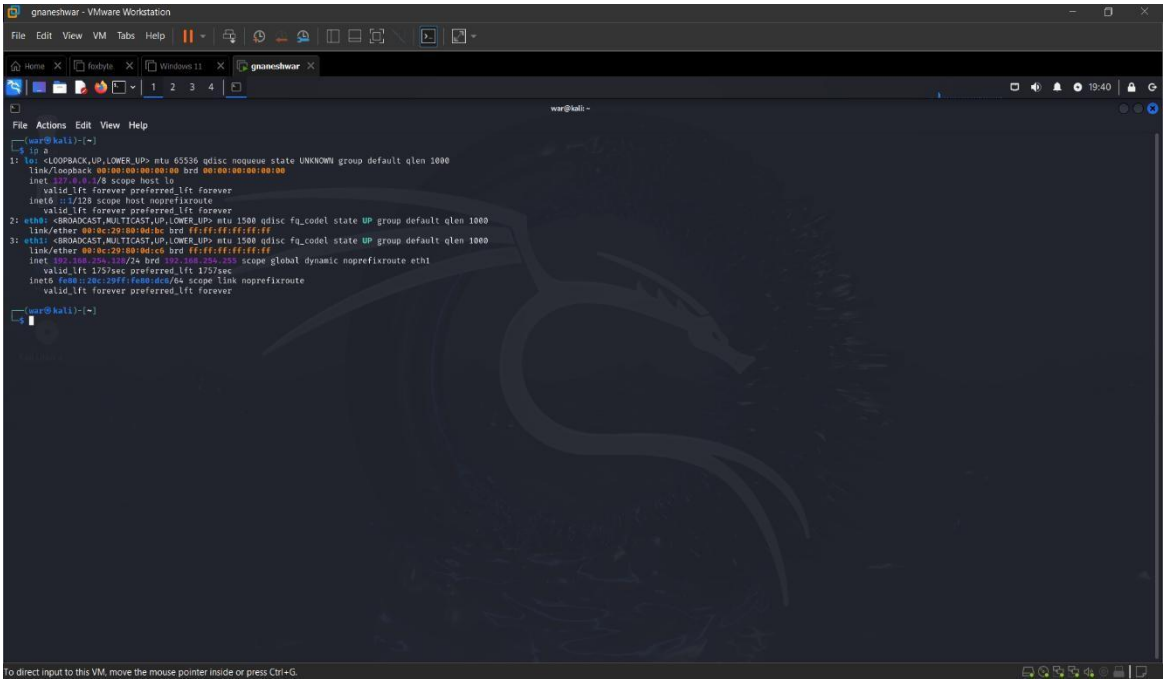

gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Home
foxbyte
Windows 11
gnaneshwar
18:40
war@kali: ~
File Actions Edit View Help
┌──(war㉿kali)-[~]
└─$ docker --version
Docker version 27.5.1+dfsg4, build cab968b3
┌──(war㉿kali)-[~]
└─$ systemctl status docker
● docker.service - Docker Application Container Engine
Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
Active: active (running) since Wed 2026-02-25 18:33:57 IST; 4min 41s ago
TriggeredBy: ● docker.socket
Docs: https://docs.docker.com
Main PID: 1185 (dockerd)
Tasks: 28
Memory: 133.8M (peak: 137.8M)
CPU: 2.740s
CGroup: /system.slice/docker.service
├─1185 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
├─2810 /usr/sbin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 4000 -container-ip 172.17.0.2 -container-port 3000
└─2837 /usr/sbin/docker-proxy -proto tcp -host-ip :: -host-port 4000 -container-ip 172.17.0.2 -container-port 3000
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.196574406+05:30" level=warning msg="error locating sandbox id 1408c404e05db82460b6ce7f72a4ce962c4433878bcff3d0d4a03e72603b3df: sandbox 1408c404e05db82460b6ce7f72a4ce962c4>
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.196611109+05:30" level=warning msg="error locating sandbox id 61c199d353eb5b269dbb9cfc0b587335a121808a2643bff4867583f0661553d7: sandbox 61c199d353eb5b269dbb9cfc0b587335a121>
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.197145801+05:30" level=info msg="Loading containers: done."
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.260377091+05:30" level=info msg="Docker daemon" commit=61416484 containerd-snapshotter=false storage-driver=overlay2 version=27.5.1+dfsg4
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.261401714+05:30" level=info msg="Daemon has completed initialization"
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.342542856+05:30" level=info msg="API listen on /run/docker.sock"
Feb 25 18:33:57 kali systemd[1]: Started docker.service - Docker Application Container Engine.
Feb 25 18:38:10 kali dockerd[1185]: time="2026-02-25T18:38:10.529241168+05:30" level=warning msg="Error getting v2 registry: Get \"https://registry-1.docker.io/v2/\": net/http: request canceled while waiting for connection (Client.Tim>
Feb 25 18:38:10 kali dockerd[1185]: time="2026-02-25T18:38:10.529367655+05:30" level=info msg="Attempting next endpoint for pull after error: Get \"https://registry-1.docker.io/v2/\": net/http: request canceled while waiting for conne>
Feb 25 18:38:10 kali dockerd[1185]: time="2026-02-25T18:38:10.531534180+05:30" level=error msg="Handler for POST /v1.47/images/create returned error: Get \"https://registry-1.docker.io/v2/\": net/http: request canceled while waiting f>
... skipping ...
● docker.service - Docker Application Container Engine
Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
Active: active (running) since Wed 2026-02-25 18:33:57 IST; 4min 41s ago
TriggeredBy: ● docker.socket
Docs: https://docs.docker.com
Main PID: 1185 (dockerd)
Tasks: 28
Memory: 133.8M (peak: 137.8M)
CPU: 2.740s
CGroup: /system.slice/docker.service
├─1185 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
├─2810 /usr/sbin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 4000 -container-ip 172.17.0.2 -container-port 3000
└─2837 /usr/sbin/docker-proxy -proto tcp -host-ip :: -host-port 4000 -container-ip 172.17.0.2 -container-port 3000
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.196574406+05:30" level=warning msg="error locating sandbox id 1408c404e05db82460b6ce7f72a4ce962c4433878bcff3d0d4a03e72603b3df: sandbox 1408c404e05db82460b6ce7f72a4ce962c4>
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.196611109+05:30" level=warning msg="error locating sandbox id 61c199d353eb5b269dbb9cfc0b587335a121808a2643bff4867583f0661553d7: sandbox 61c199d353eb5b269dbb9cfc0b587335a121>
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.197145801+05:30" level=info msg="Loading containers: done."
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.260377091+05:30" level=info msg="Docker daemon" commit=61416484 containerd-snapshotter=false storage-driver=overlay2 version=27.5.1+dfsg4
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.261401714+05:30" level=info msg="Daemon has completed initialization"
Feb 25 18:33:57 kali dockerd[1185]: time="2026-02-25T18:33:57.342542856+05:30" level=info msg="API listen on /run/docker.sock"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

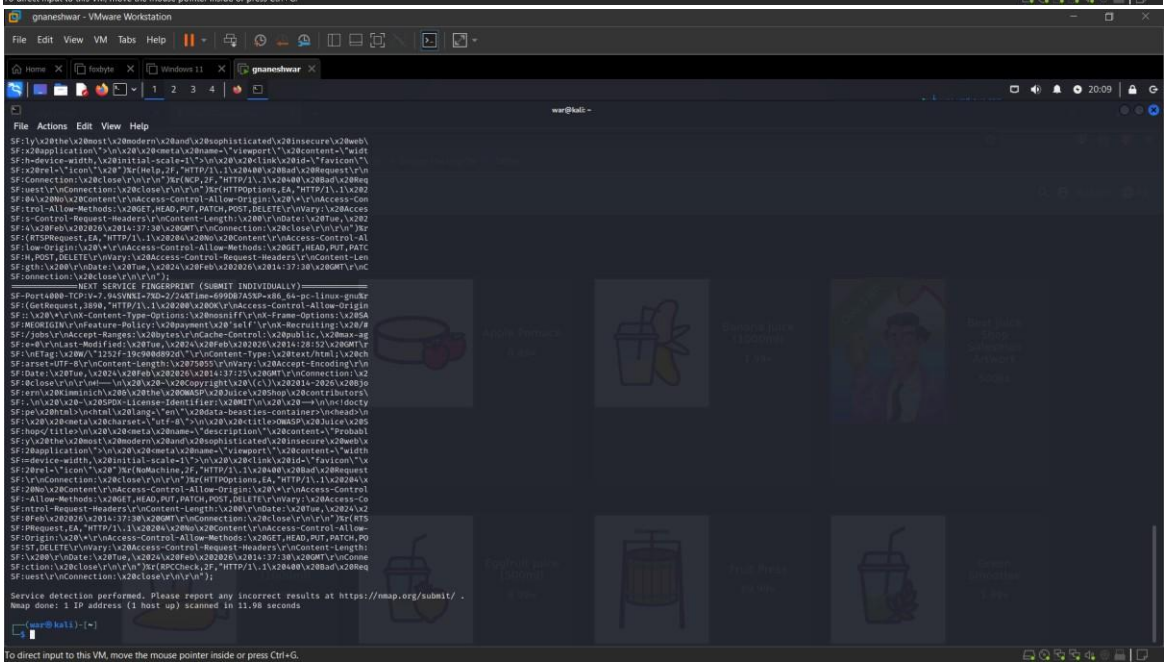

gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Home
foxbyte
Windows 11
gnaneshwar
18:40
war@kali: ~
File Actions Edit View Help
┌──(war㉿kali)-[~]
└─$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
17eec7bbc9d7: Pull complete
Digest: sha256:ef54e839ef541993b4e87f25e752f7cf4238fa55f017957c2eb44077083d7a6a
Status: Downloaded newer image for hello-world:latest
Hello from Docker!
This message shows that your installation appears to be working correctly.
To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
(amd64)
3. The Docker daemon created a new container from that image which runs the
executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
to your terminal.
To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash
Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/
For more examples and ideas, visit:
https://docs.docker.com/get-started/
┌──(war㉿kali)-[~]
└─$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
04d4d478ce61 bkimminich/juice-shop "/nodejs/bin/node /j…" 2 minutes ago Up 2 minutes 0.0.0.0:4000→3000/tcp, [::]:4000→3000/tcp condescending_nightingale
┌──(war㉿kali)-[~]
└─$ docker run -d -p 4000:3000 bkimminich/juice-shop
f2de86595c1d434ba103a291c3718ccc840174899664729ea11c04c157fad586c
docker: Error response from daemon: driver failed programming external connectivity on endpoint friendly_burnell (651903d98adf241c482f8f65ab90e79ec800baccda715d8a387de5d0faa29862): Bind for 0.0.0.0:4000 failed: port is already allocate
d.
┌──(war㉿kali)-[~]
└─$ docker run -d -p 3000:3000 bkimminich/juice-shop
1dced83377e21dcd6a39b69784d18412b7e908aabf4b432e49ae872fd982d74e
┌──(war㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



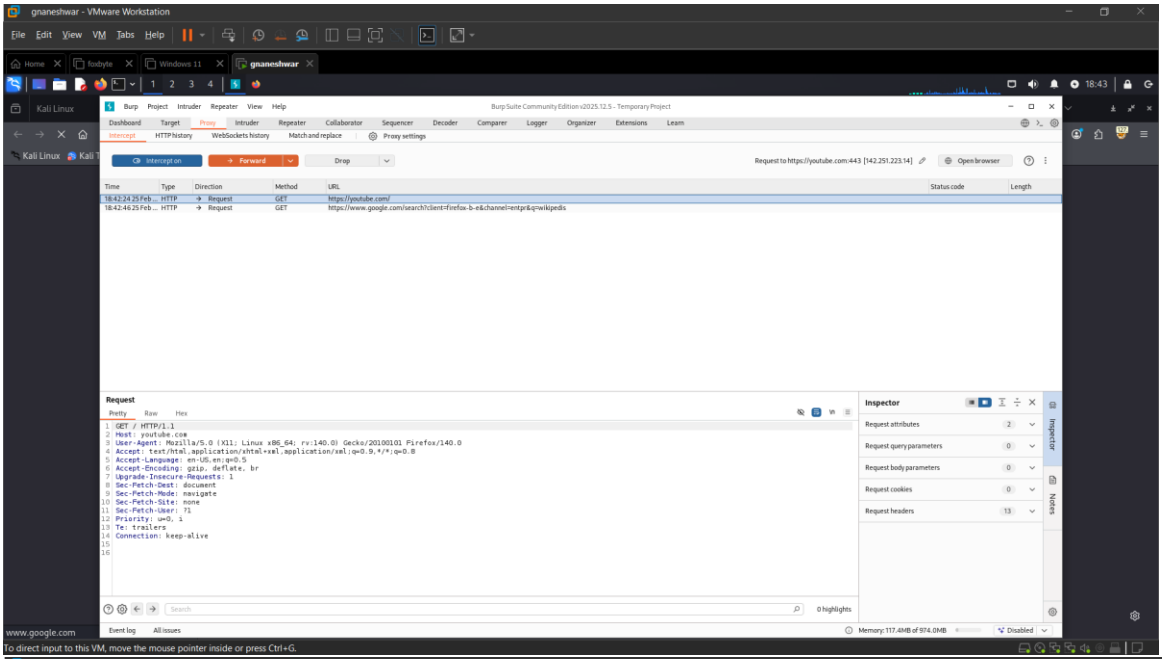
4. Validation & Testing

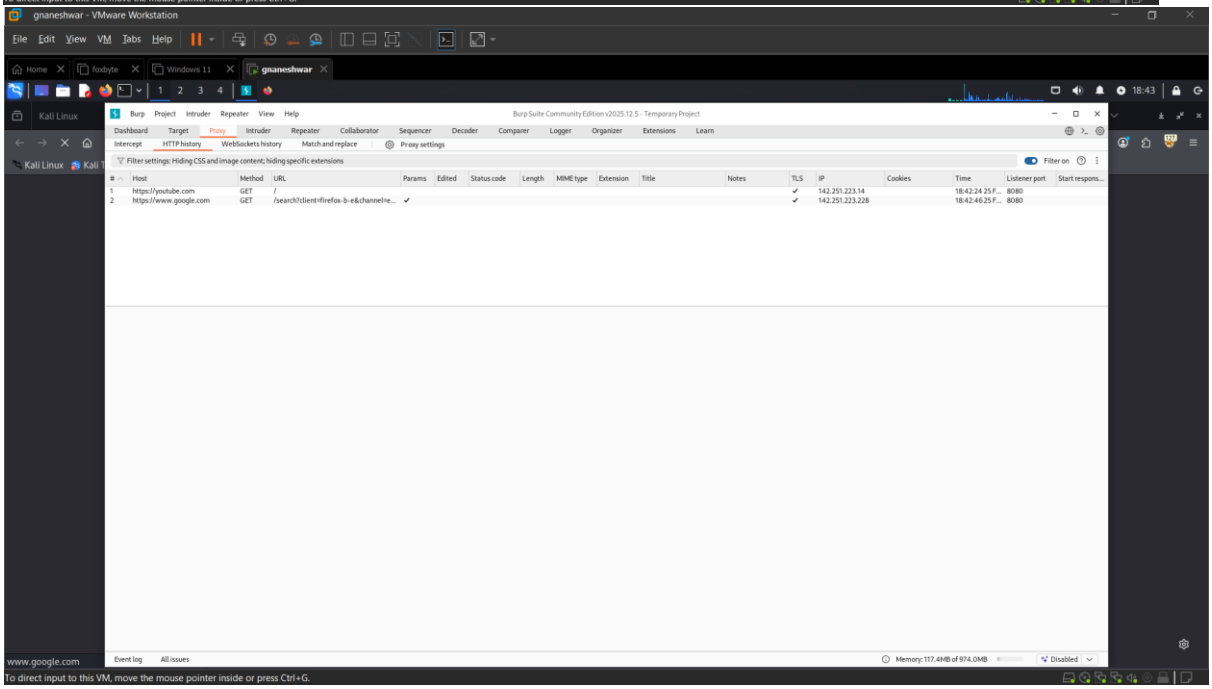
- Verified IP configuration using 'ip a'.
- Confirmed container running using 'docker ps'.
- Accessed OWASP Juice Shop via http://localhost:4000.
- Performed Nmap scan to identify open ports.
- Intercepted HTTP traffic using Burp Suite.
- Captured network packets using Wireshark.

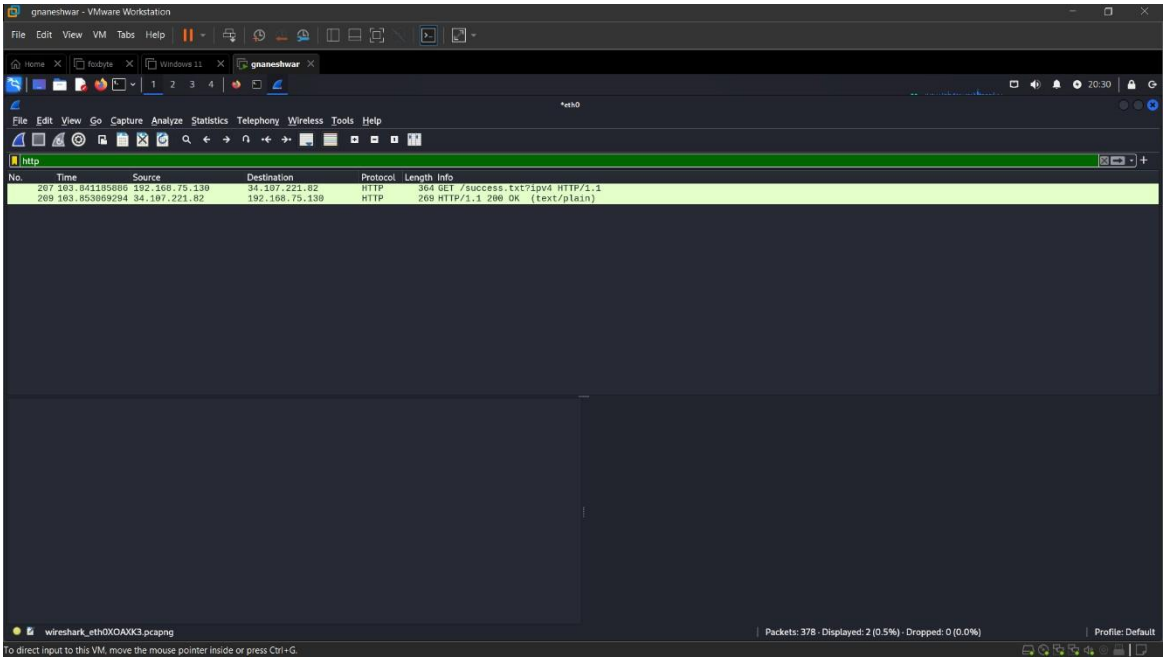

gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Home
foxbyte
Windows 11
gnaneshwar
1 2 3 4
19:40
war@kali: ~
File Actions Edit View Help
(war㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:80:0d:bc brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:80:0d:c6 brd ff:ff:ff:ff:ff:ff
inet 192.168.254.128/24 brd 192.168.254.255 scope global dynamic noprefixroute eth1
valid_lft 1757sec preferred_lft 1757sec
inet6 fe80::20c:29ff:fe80:dc6/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(war㉿kali)-[~]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

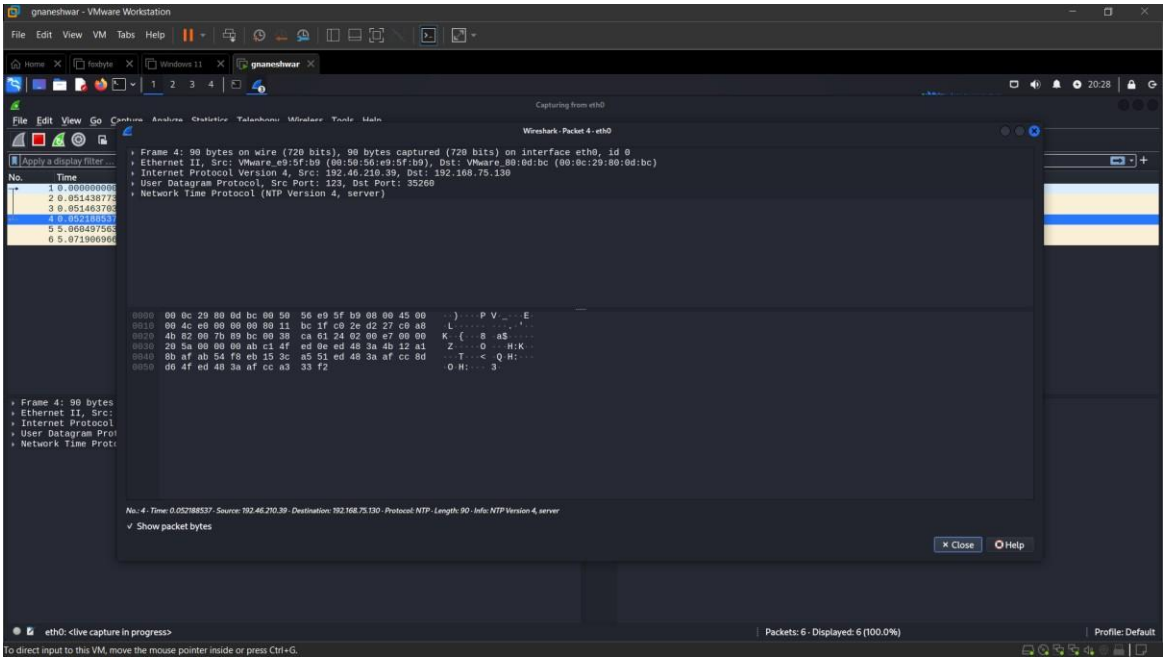

gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Home
foxbyte
Windows 11
gnaneshwar
1 2 3 4
20:09
war@kali: ~
File Actions Edit View Help
SF:ly\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\
SF:x20application\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"widt
SF:h=device-width,\x20initial-scale=1\">\n\x20\x20<link\x20id=\"favicon\"\
SF:x20rel=\"icon\"\x20")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Connection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x202
SF:0\x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Con
SF:trol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Acces
SF:s-Control-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Tue,\x202
SF:4\x20Feb\x202026\x2014:37:30\x20GMT\r\nConnection:\x20close\r\n\r\n")%r
SF:(RTSPRequest,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Al
SF:low-Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATC
SF:H,POST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Len
SF:gth:\x200\r\nDate:\x20Tue,\x2024\x20Feb\x202026\x2014:37:30\x20GMT\r\nC
SF:onnection:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port4000-TCP:V=7.94SVN%I=7%D=2/24%Time=699DB7A5%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,3890,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin
SF::\x20*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SA
SF:MEORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#
SF:/jobs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-ag
SF:e=0\r\nLast-Modified:\x20Tue,\x202\x20Feb\x202026\x2014:28:52\x20GMT\r
SF:\nETag:\x20W/\"1252f-19c9d0d092d\"\r\nContent-Type:\x20text/html;\x20ch
SF:arset=UTF-8\r\nContent-Length:\x2075055\r\nVary:\x20Accept-Encoding\r\n
SF:Date:\x20Tue,\x2024\x20Feb\x202026\x2014:37:25\x20GMT\r\nConnection:\x2
SF:0close\r\n\r\n<!--\n\x20\x20-\x20Copyright\x20\(c\)\x202014-2026\x20Jo
SF:ern\x20Kimminich\x20and\x20the\x20OWASP\x20Juice\x20Shop\x20contributors
SF:.\n\x20\x20-\x20SPDX-License-Identifier:\x20MIT\n\x20\x20-->\n\n<!docty
SF:pe\x20html>\n<html\x20lang=\"en\"\x20data-beasties-container>\n<head>\n
SF:\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20<title>OWASP\x20Juice\x205
SF:hop</title>\n\x20\x20<meta\x20name=\"description\"\x20content=\"Probabl
SF:y\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x
SF:20application\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"width
SF:=device-width,\x20initial-scale=1\">\n\x20\x20<link\x20id=\"favicon\"\x
SF:20rel=\"icon\"\x20")%r(NoMachine,2F,"HTTP/1\.1\x20400\x20Bad\x20Request
SF:\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.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:\x20Tue,\x2024\x2
SF:0Feb\x202026\x2014:37:30\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTS
SF:PRequest,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Allow-
SF:Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,PO
SF:ST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Length:
SF:\x200\r\nDate:\x20Tue,\x2024\x20Feb\x202026\x2014:37:30\x20GMT\r\nConne
SF:ction:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
(war㉿kali)-[~]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.12.5 - Temporary Project
Request
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
www.google.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.12.5 - Temporary Project
www.google.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
gnaneshwar
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
207 103.841185806 192.168.75.130 34.107.221.82 HTTP 364 GET /success.txt?ipv4 HTTP/1.1
209 103.853069294 34.107.221.82 192.168.75.130 HTTP 269 HTTP/1.1 200 OK (text/plain)
wireshark_eth0XOAXK3.pcapng
Packets: 378 · Displayed: 2 (0.5%) · Dropped: 0 (0.0%)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


gnaneshwar - VMware Workstation
File Edit View VM Tabs Help
gnaneshwar
Capturing from eth0
Wireshark · Packet 4 · eth0
Frame 4: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
Ethernet II, Src: VMware_e9:5f:b9 (00:50:56:e9:5f:b9), Dst: VMware_80:0d:bc (00:0c:29:80:0d:bc)
Internet Protocol Version 4, Src: 192.46.210.39, Dst: 192.168.75.130
User Datagram Protocol, Src Port: 123, Dst Port: 35260
Network Time Protocol (NTP Version 4, server)
0000 00 0c 29 80 0d bc 00 50 56 e9 5f b9 08 00 45 00
0010 00 4c e0 00 00 00 80 11 bc 1f c0 2e d2 27 c0 a8
0020 4b 82 00 7b 89 bc 00 38 ca 61 24 02 00 e7 00 00
0030 28 5a 00 00 00 ab c1 4f ed 0e ed 48 3a 4b 12 a1
0040 8b af ab 54 f8 eb 15 3c a5 51 ed 48 3a af cc 8d
0050 d6 4f ed 48 3a af cc a3 33 f2
No.: 4 · Time: 0.052188537 · Source: 192.46.210.39 · Destination: 192.168.75.130 · Protocol: NTP · Length: 90 · Info: NTP Version 4, server
Show packet bytes
Close
Help
eth0: <live capture in progress>
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Learning Outcomes

This task improved my understanding of virtualization, secure lab setup, network segmentation (NAT vs Host-Only), Docker container deployment, basic reconnaissance using Nmap, HTTP interception using Burp Suite, and packet analysis using Wireshark. The lab environment provides a safe foundation for future penetration testing and vulnerability assessment tasks.

End of Report