Refonte Cybersecurity & DevSecOps Exercise 1

The goal of this exercise is to set up a small network, capture its traffic using Wireshark from visiting an unsecure website, analyse if there are any vulnerabilities, such as clear-text passwords or insecure protocols.

The exercise commenced with creating two virtual machines on VirtualBox virtual machine (VM) environment – Ubuntu 24.04 Desktop and Ubuntu 24.04 Server. With each machine configured to have two interface cards one “Bridged Network” and the other “NAT” modes in the virtualisation software.

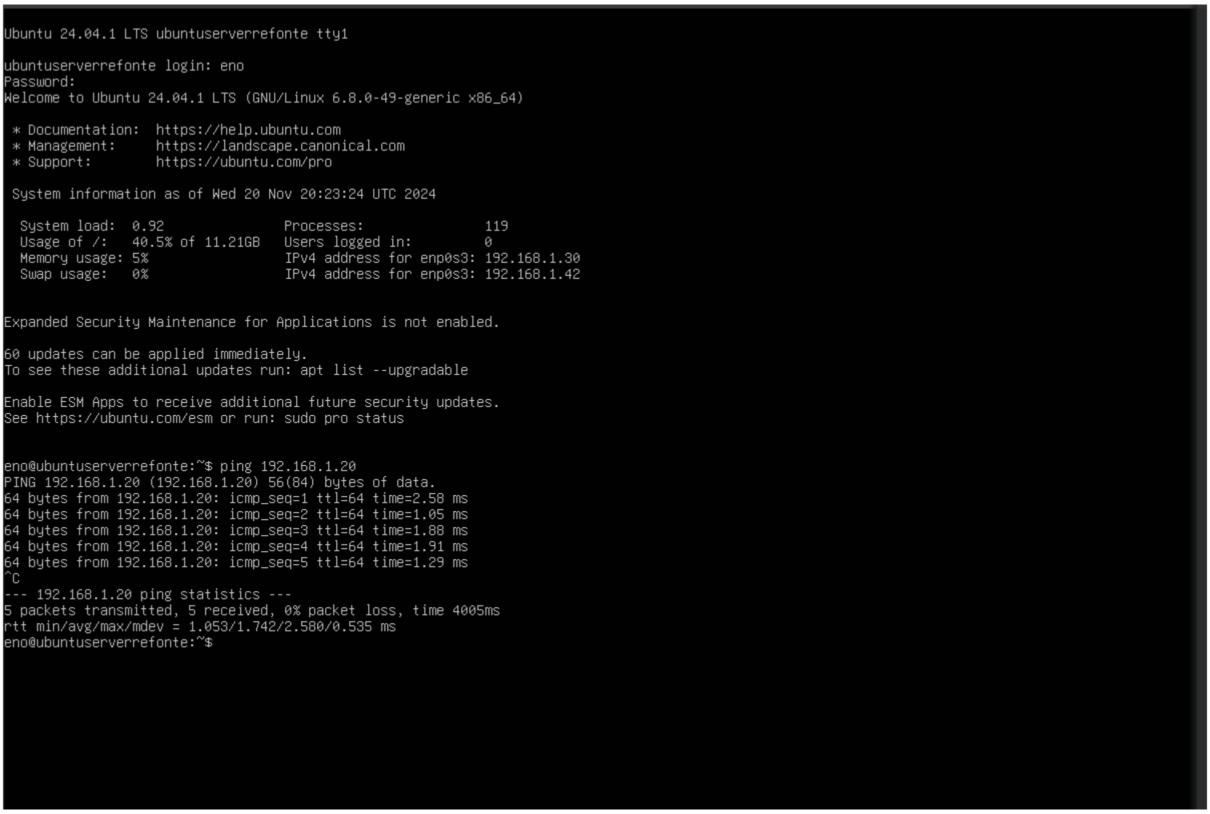
IP address for desktop is 192.168.1.20

IP address for server is 192.168.1.30

Testing for communication between both machines were then tested by pinging each other in the terminal command prompts – this succeeded perfectly.

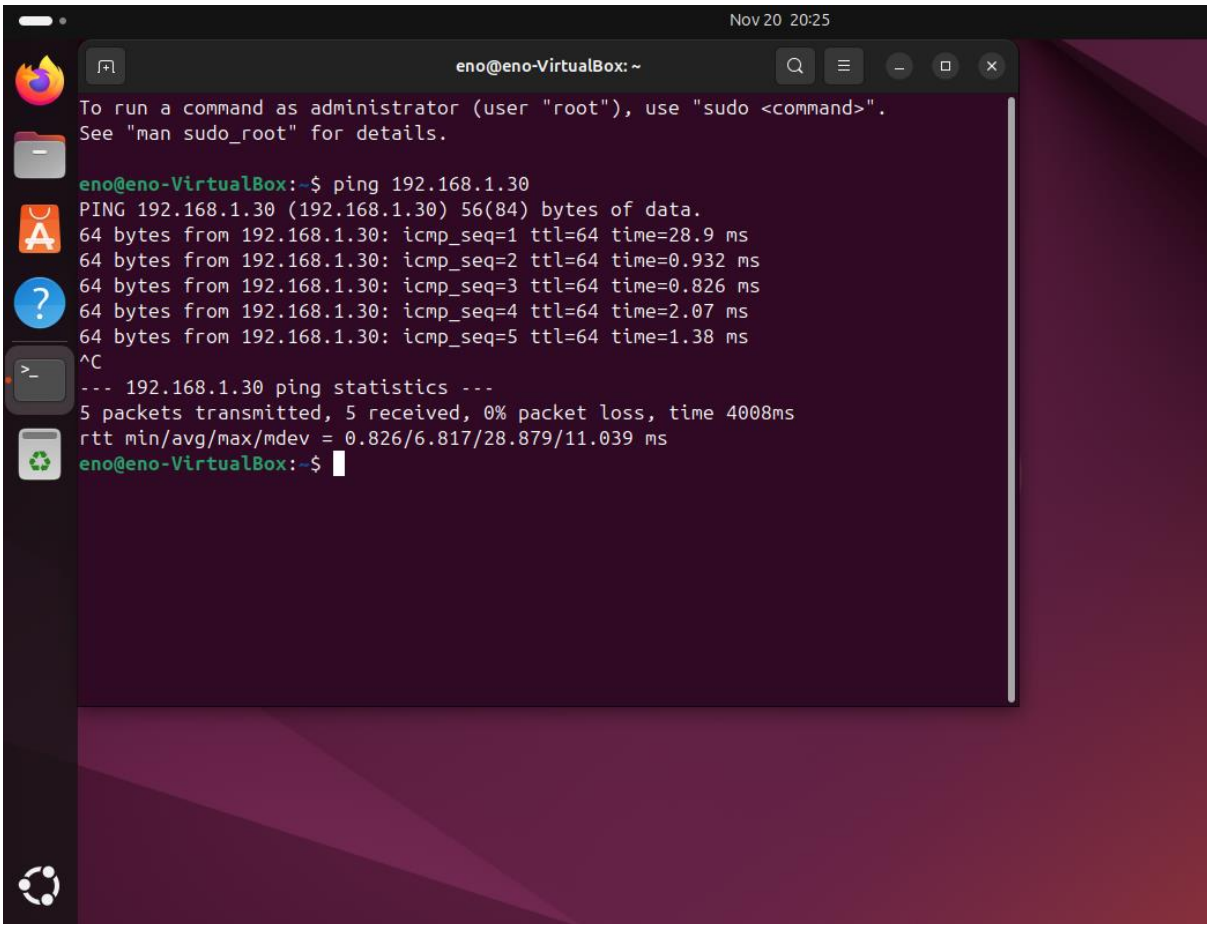
Below is the screenshot of the successful pings.

Server pinging desktop



```
Ubuntu 24.04.1 LTS ubuntuserverrefonte tty1

ubuntuserverrefonte login: eno
Password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed 20 Nov 20:23:24 UTC 2024

  System load:  0.92               Processes:               119
  Usage of /:   40.5% of 11.21GB   Users logged in:         0
  Memory usage: 5%                 IPv4 address for enp0s3: 192.168.1.30
  Swap usage:   0%                 IPv4 address for enp0s3: 192.168.1.42


Expanded Security Maintenance for Applications is not enabled.

60 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


eno@ubuntuserverrefonte:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=2.58 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=64 time=1.88 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=64 time=1.91 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=64 time=1.29 ms
^C
--- 192.168.1.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.053/1.742/2.580/0.535 ms
eno@ubuntuserverrefonte:~$
```

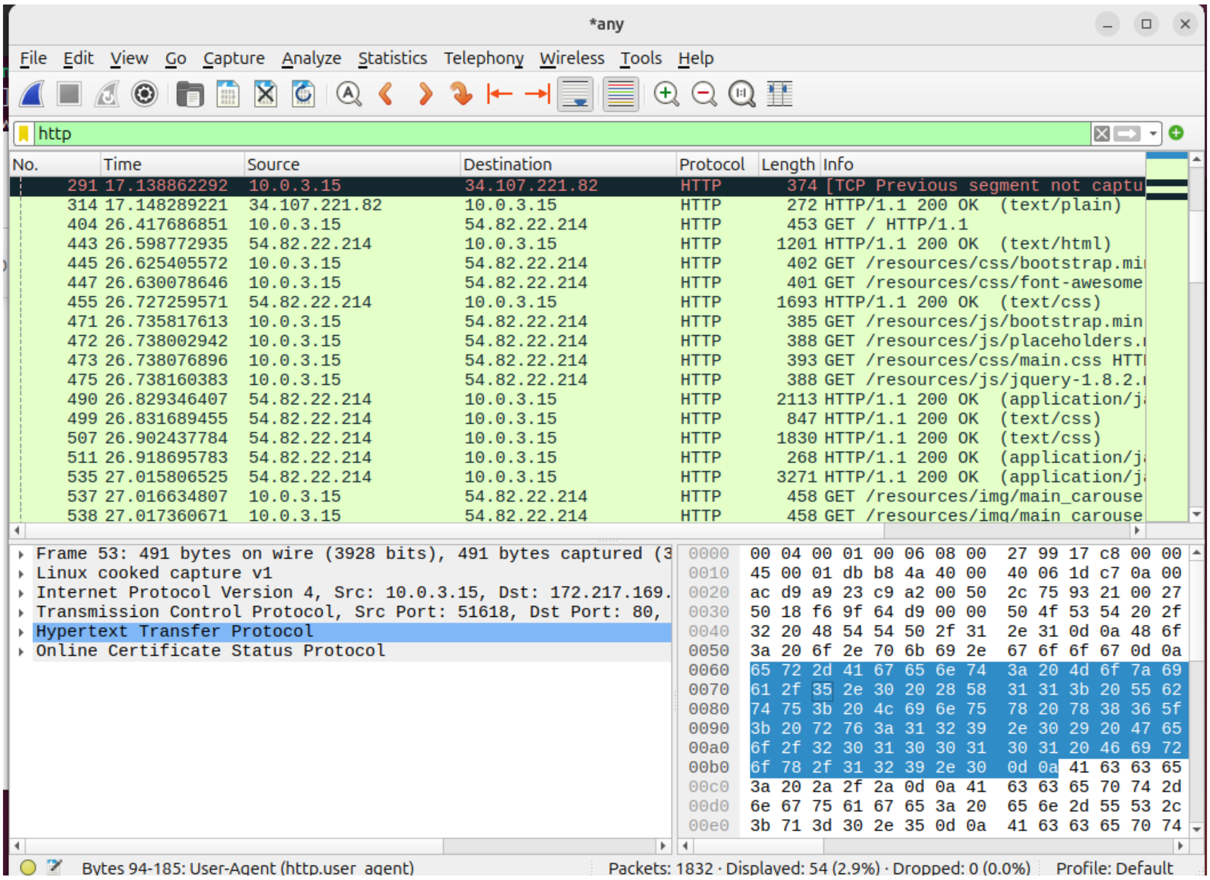
Desktop pinging server



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

eno@eno-VirtualBox:~$ ping 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=28.9 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=0.932 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=0.826 ms
64 bytes from 192.168.1.30: icmp_seq=4 ttl=64 time=2.07 ms
64 bytes from 192.168.1.30: icmp_seq=5 ttl=64 time=1.38 ms
^C
--- 192.168.1.30 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 0.826/6.817/28.879/11.039 ms
eno@eno-VirtualBox:~$
```

Capturing Packets using Wireshark

A traffic capture was started and then browsed to an unsecure http website as well as sending messages in an online form. A filter on http shows the results in the screenshot below



http

```
No.      Time          Source          Destination     Protocol Length Info
     291 17.138862292  10.0.3.15       34.107.221.82   HTTP      374 [TCP Previous segment not captu
     314 17.148289221  34.107.221.82   10.0.3.15       HTTP      272 HTTP/1.1 200 OK  (text/plain)
     404 26.417686851  10.0.3.15       54.82.22.214    HTTP      453 GET / HTTP/1.1
     443 26.598772935  54.82.22.214    10.0.3.15       HTTP     1201 HTTP/1.1 200 OK  (text/html)
     445 26.625405572  10.0.3.15       54.82.22.214    HTTP      402 GET /resources/css/bootstrap.mi
     447 26.630078646  10.0.3.15       54.82.22.214    HTTP      401 GET /resources/css/font-awesome
     455 26.727259571  54.82.22.214    10.0.3.15       HTTP     1693 HTTP/1.1 200 OK  (text/css)
     471 26.735817613  10.0.3.15       54.82.22.214    HTTP      385 GET /resources/js/bootstrap.min
     472 26.738002942  10.0.3.15       54.82.22.214    HTTP      388 GET /resources/js/placeholders.
     473 26.738076896  10.0.3.15       54.82.22.214    HTTP      393 GET /resources/css/main.css HTT
     475 26.738160383  10.0.3.15       54.82.22.214    HTTP      388 GET /resources/js/jquery-1.8.2.
     490 26.829346407  54.82.22.214    10.0.3.15       HTTP     2113 HTTP/1.1 200 OK  (application/j
     499 26.831689455  54.82.22.214    10.0.3.15       HTTP      847 HTTP/1.1 200 OK  (text/css)
     507 26.902437784  54.82.22.214    10.0.3.15       HTTP     1830 HTTP/1.1 200 OK  (text/css)
     511 26.918695783  54.82.22.214    10.0.3.15       HTTP      268 HTTP/1.1 200 OK  (application/j
     535 27.015806525  54.82.22.214    10.0.3.15       HTTP     3271 HTTP/1.1 200 OK  (application/j
     537 27.016634807  10.0.3.15       54.82.22.214    HTTP      458 GET /resources/img/main_carouse
     538 27.017360671  10.0.3.15       54.82.22.214    HTTP      458 GET /resources/img/main_carouse
```

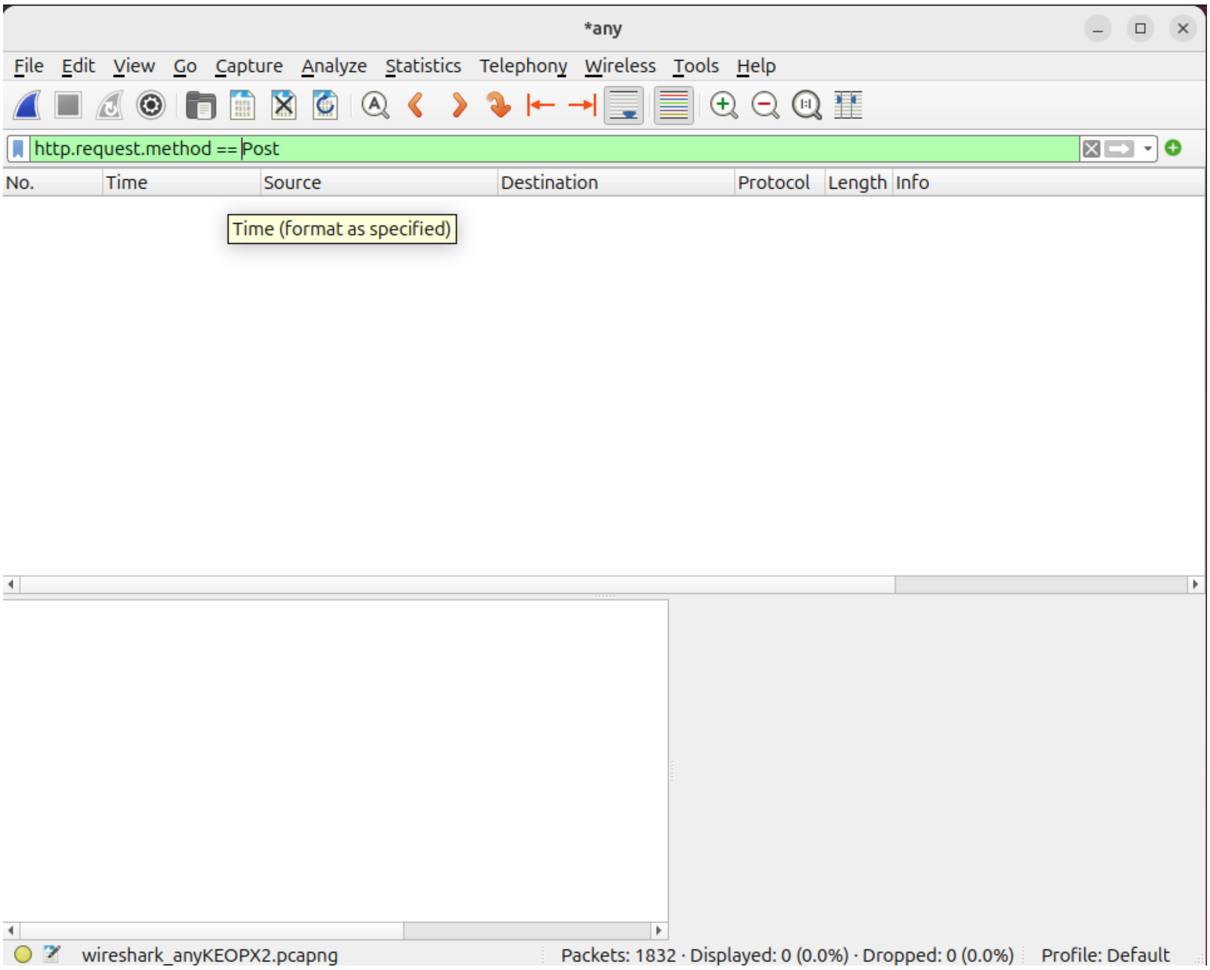
```
▸ Frame 53: 491 bytes on wire (3928 bits), 491 bytes captured (3
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.0.3.15, Dst: 172.217.169.
▸ Transmission Control Protocol, Src Port: 51618, Dst Port: 80,
▸ Hypertext Transfer Protocol
▸ Online Certificate Status Protocol
```

```
0000  00 04 00 01 00 06 08 00  27 99 17 c8 00 00
0010  45 00 01 db b8 4a 40 00  40 06 1d c7 0a 00
0020  ac d9 a9 23 c9 a2 00 50  2c 75 93 21 00 27
0030  50 18 f6 9f 64 d9 00 00  50 4f 53 54 20 2f
0040  32 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f
0050  3a 20 6f 2e 70 6b 69 2e  67 6f 6f 67 0d 0a
0060  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69
0070  61 2f 35 2e 30 20 28 58  31 31 3b 20 55 62
0080  74 75 3b 20 4c 69 6e 75  78 20 78 38 36 5f
0090  3b 20 72 76 3a 31 32 39  2e 30 29 20 47 65
00a0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72
00b0  6f 78 2f 31 32 39 2e 30  0d 0a 41 63 63 65
00c0  3a 20 2a 2f 2a 0d 0a 41  63 63 65 70 74 2d
00d0  6e 67 75 61 67 65 3a 20  65 6e 2d 55 53 2c
00e0  3b 71 3d 30 2e 35 0d 0a  41 63 63 65 70 74
```

Bytes 94-185: User-Agent (http.user_agent)   Packets: 1832 · Displayed: 54 (2.9%) · Dropped: 0 (0.0%)   Profile: Default

The website visited is unsecured as it uses only http and if it required login credentials to access the system behind it, the username passwords will definitely be captured.

Filtering for usernames and passwords revealed no results as seen in the screenshot below. Since there was no successful logins to the website with existing credentials, the credentials were not captured but the website is definitely not secure.



http.request.method == Post

No.	Time	Source	Destination	Protocol	Length	Info

wireshark_anyKEOPX2.pcapng Packets: 1832 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%) Profile: Default