Refonte Cybersecurity & DevSecOps Exercise 1

Network Security & Traffic Analysis

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

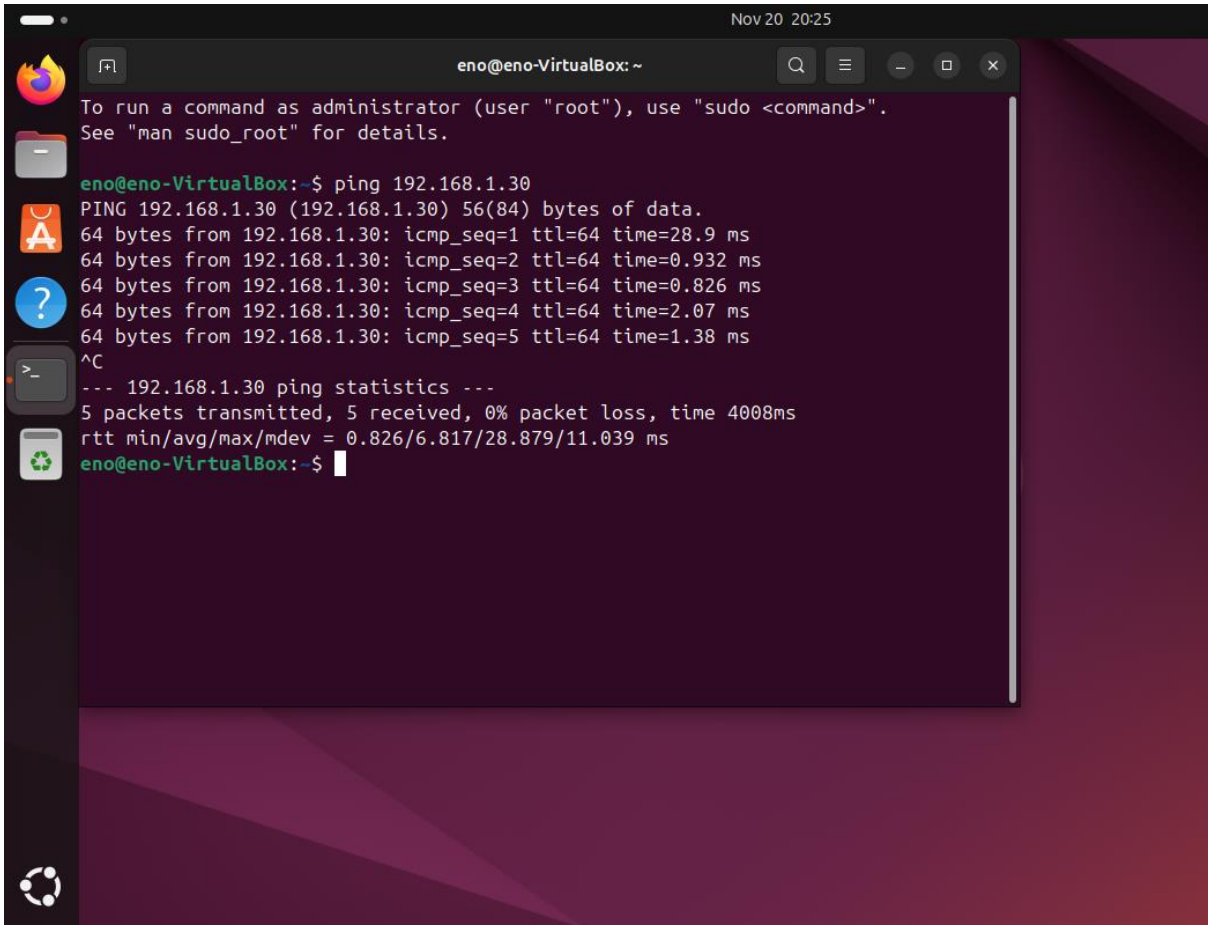
Testing for communication between both machines were then tested by pinging each other in the terminal command prompts – this succeeded perfectly.

Below is the screenshot of the successful pings.

Server pinging desktop

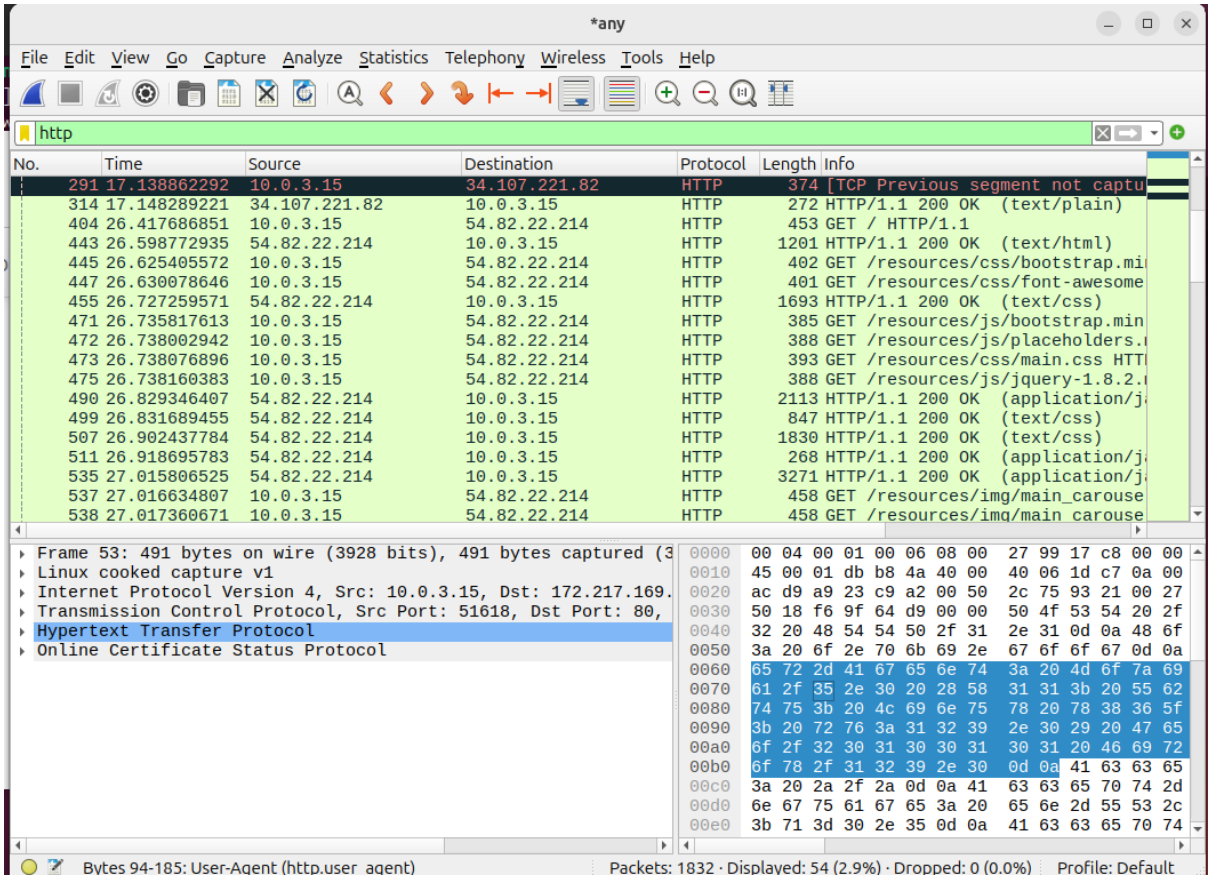
```
Ubuntu 24.04.1 LTS ubuntuserverrefonte tty1

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



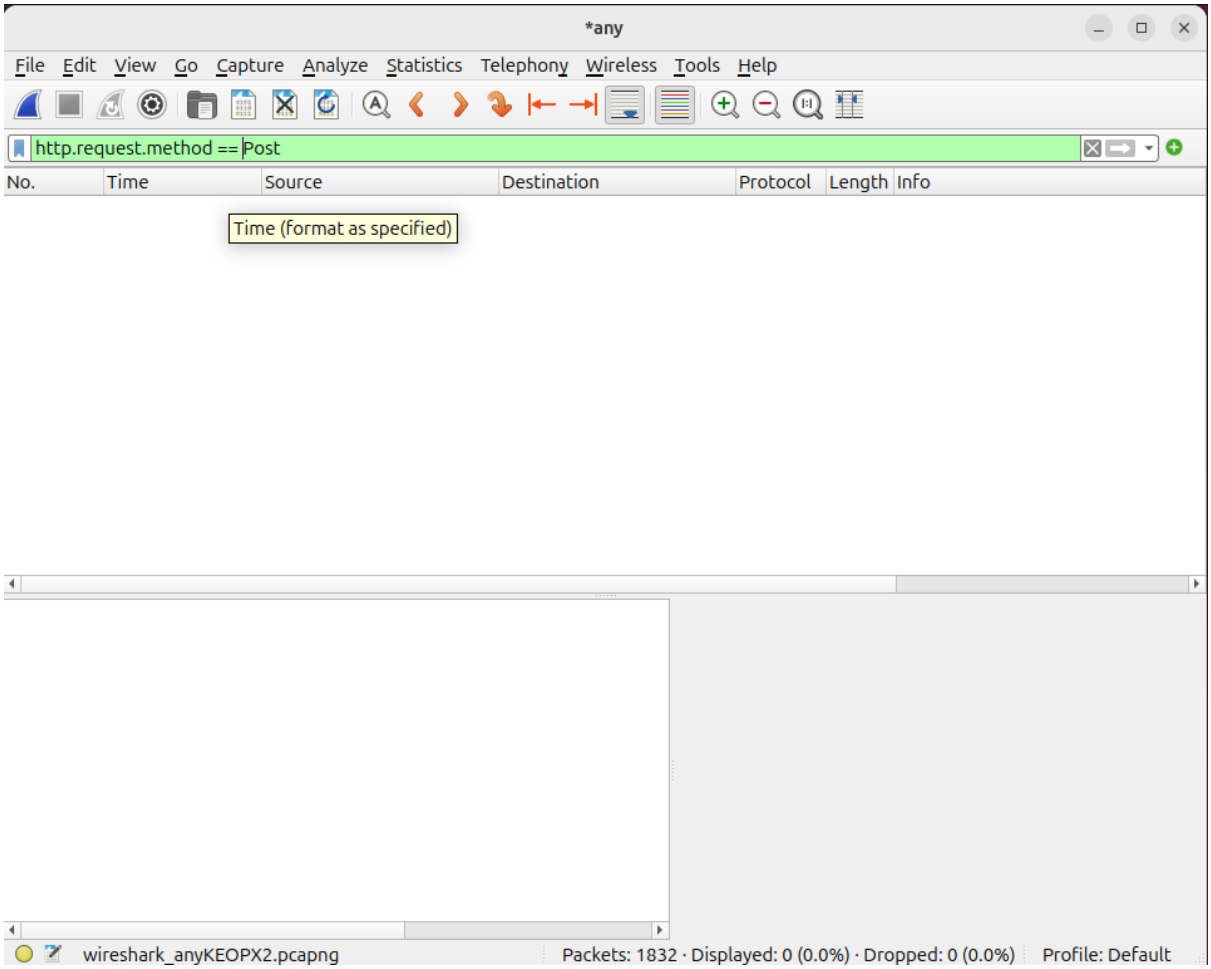
Capturing Packets using Wireshark

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



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 were no successful logins to the website with existing credentials, the credentials were not captured but the website is definitely not secure.



It is not advisable to apply HTTP (HyperText Transfer Protocol) for accessing the web as it is insecure and deprecated, lacking security for the data being transmitted through it on web browsers. As HTTP allows communications between the client and web browser, data transmitted are in plaintext and not encrypted therefore information such as login credentials can be intercepted and used to perform cyber exploits such as Man-In-The-Middle (MITM) attacks and impersonation attack due to lack of authentications.

Alternatively HTTPS (HyperText Transfer Protocol Secure) is better recommended for web browsing. This is due to the fact that it provides a layer of security of encrpytion, it uses SSL/TLS

(Secure Sockets Layer/Transport Layer Security) to encrypt commninucation which ensures confidentiality and integrity. HTTPS allows clients to verify the identity of the server using digital certificates ensuring users are commnunicating with the intended website and not a fraudulent site such as s phishing site designed to steal users sensitive information.