

Introduction - Cybersecurity

TP1 - Traffic Sniffing with Wireshark

Objectives

- Learn how to configure a virtual network.
- Learn how to filter data in Wireshark.
- Discover vulnerabilities in Telnet and HTTP services.

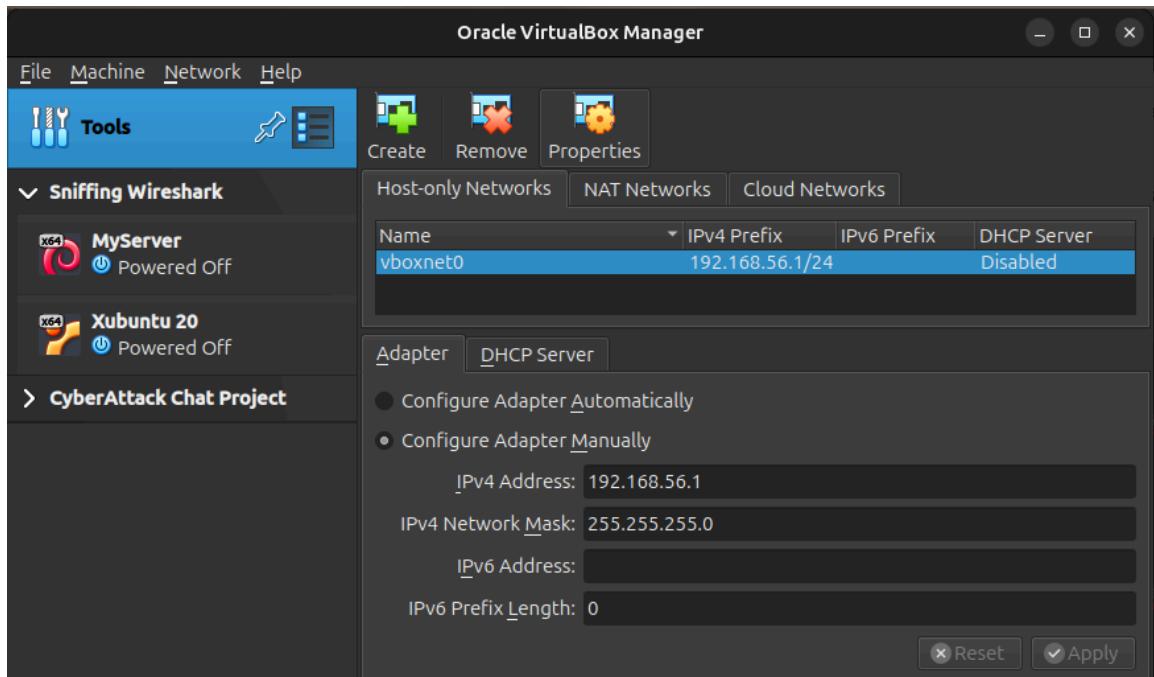
1. Virtualization Environment Setup

1. Download and install the latest version of **VirtualBox**.
2. Download and install **Oracle VM VirtualBox Extension Pack**.

2. Virtual Machine Preparation

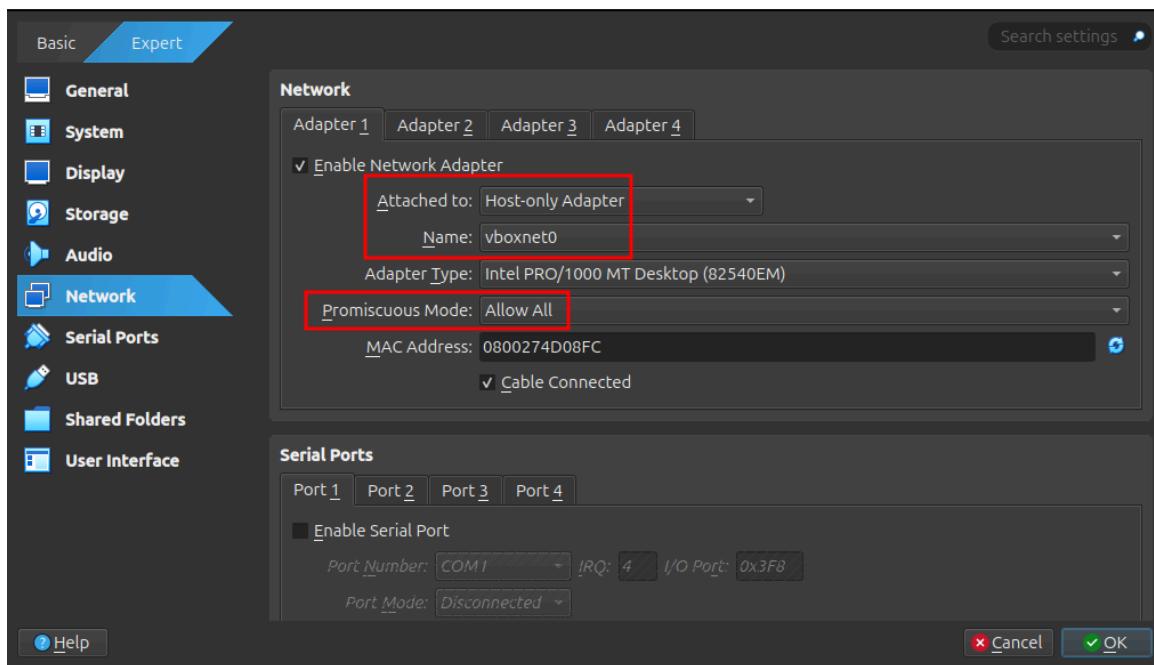
1. Download the two virtual machines "**Student.ova**" and "**MyServer.ova**" from [this platform](#).
2. Import these virtual machines into VirtualBox.
3. Discuss with your instructor how to set up the virtual network.

File > Tools > Network Manager:



{VM name} > Settings > Network:

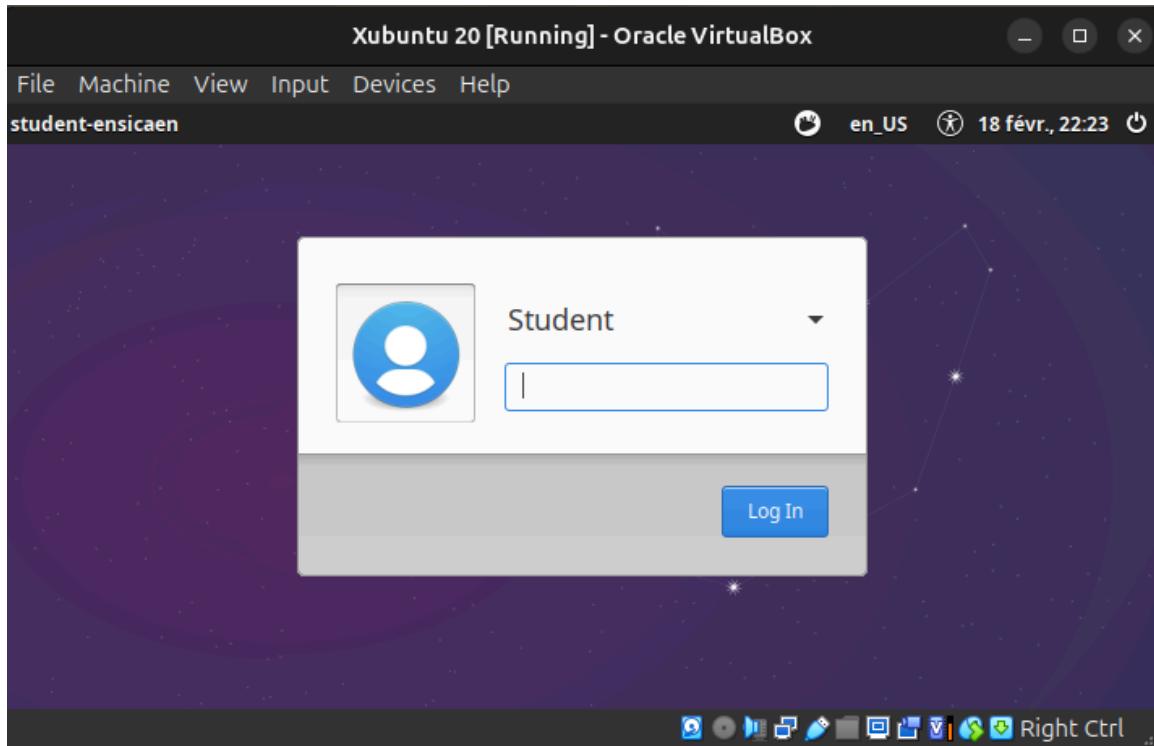
Do these configurations on both of the machines. This allow us to use the network we created which includes the host, making it possible the sniffing by the host.



Host's terminal:

```
sudo ip link set vboxnet0 promisc on # before starting VMs
```

4. Start the "**Student**" VM and log in with the credentials: **student | student**.



5. Start the "**MyServer**" VM and log in with: **student | ensicaen**.

MyServer [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
* Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.0.1 for ServerName [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

Client login:
```

6. Assign an **IP address** to each virtual machine.

Server's terminal:

```
sudo nano /etc/network/interfaces # add new ip based on our network
```

MyServer [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
student@Client:/$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:4d:08:fc
          inet addr:192.168.56.5 Bcast:192.168.56.255 Mask:255.255.255.0
              inet6 addr: fe80::a00:27ff:fe4d:8fc/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:11 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:856 (856.0 B) TX bytes:9140 (8.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:150 errors:0 dropped:0 overruns:0 frame:0
              TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:48049 (46.9 KB) TX bytes:48049 (46.9 KB)

student@Client:/$ _
```

Student's terminal:

```
sudo ip addr flush dev enp0s3 # clean up old ip
sudo ip addr add 192.168.56.2/24 dev enp0s3 # adding new ip/netmask ba
```

Xubuntu 20 [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
Terminal - student@student... 18 févr., 22:38
Terminal - student@student-ensicaen: ~
File Edit View Terminal Tabs Help
enp0s3: flags=4163<IP_BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.2 brd 192.168.56.255 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::dd2:233a:cc54:85fa brd ff02::1 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:5a:88:ab txqueuelen 1000 (Ethernet)
RX packets 56 bytes 8003 (8.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 51 bytes 5746 (5.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 78 bytes 6788 (6.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 78 bytes 6788 (6.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

student@student-ensicaen:~$ 

```

7. Verify connectivity between the two VMs.

- The **MyServer VM** should **not** have access to the internet.

Doing ping from server to student

MyServer [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help

Password:
Last login: Wed Feb 12 14:07:37 EST 2025 on pts/1
Linux Client 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No directory, logging in with HOME=/
student@Client:/$ ping 192.168.56.2
PING 192.168.56.2 (192.168.56.2) 56(84) bytes of data.
64 bytes from 192.168.56.2: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 192.168.56.2: icmp_seq=2 ttl=64 time=0.419 ms
64 bytes from 192.168.56.2: icmp_seq=3 ttl=64 time=0.564 ms
64 bytes from 192.168.56.2: icmp_seq=4 ttl=64 time=0.450 ms

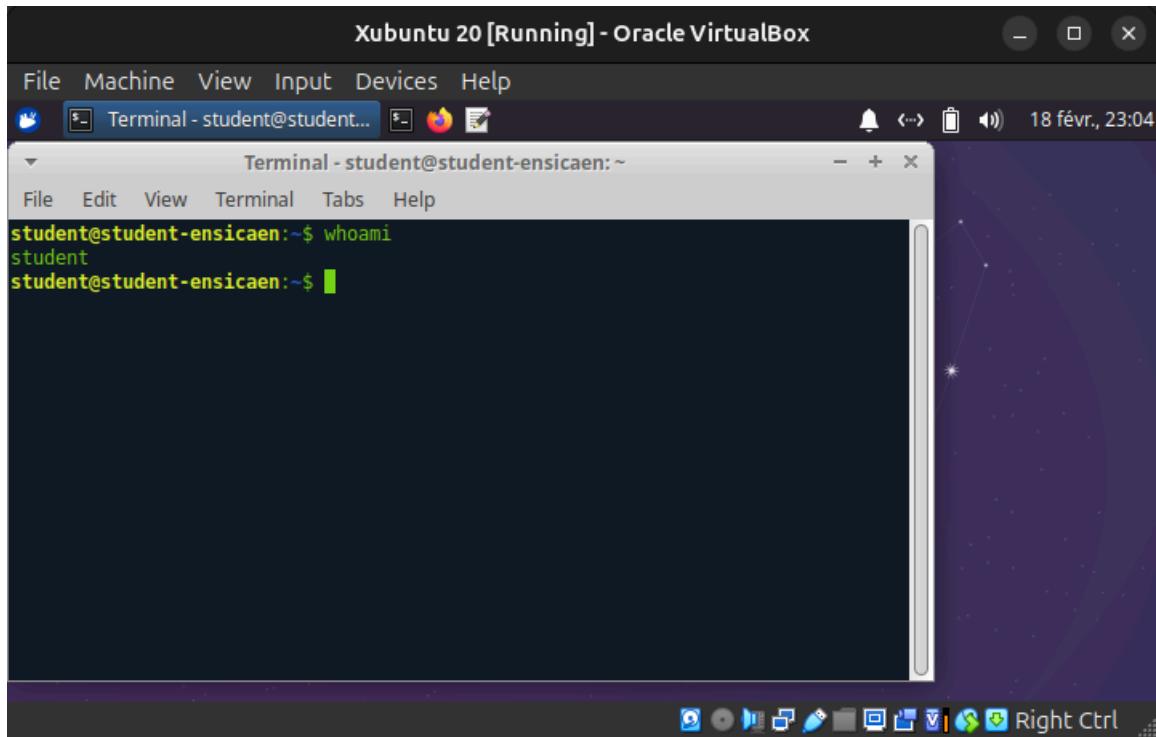
--- 192.168.56.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.419/1.666/5.234/2.060 ms
student@Client:/$ 

```

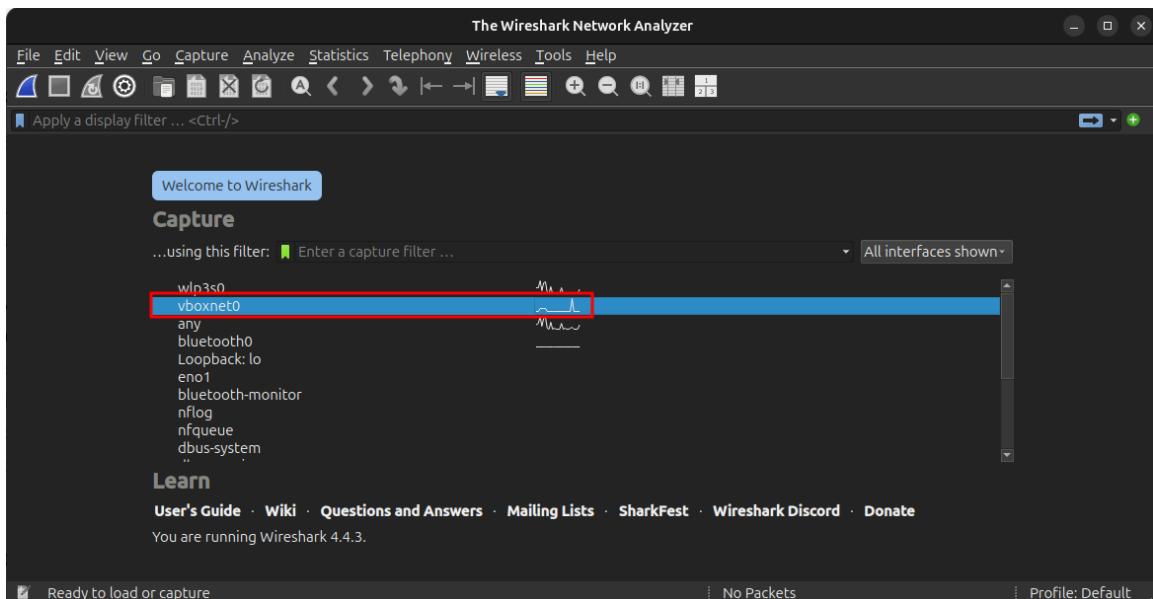
3. Capturing Telnet Passwords

1. On the **Student** machine, open a terminal and run the command:

```
whoami
```



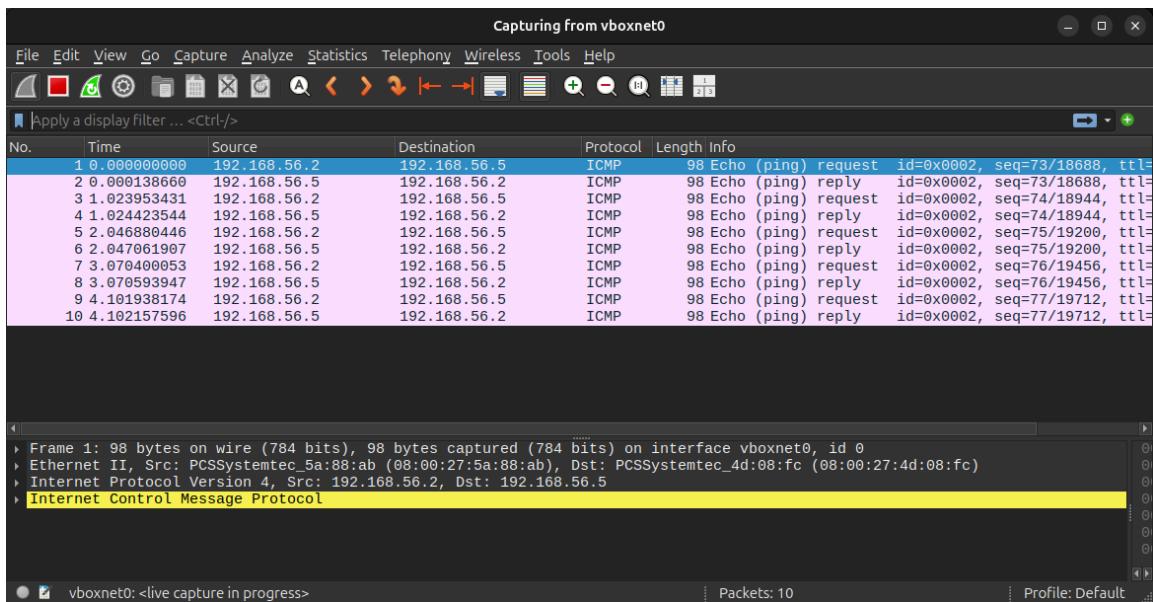
2. Open **Wireshark** and select the correct network interface for traffic capture.



3. Start packet capture in Wireshark.

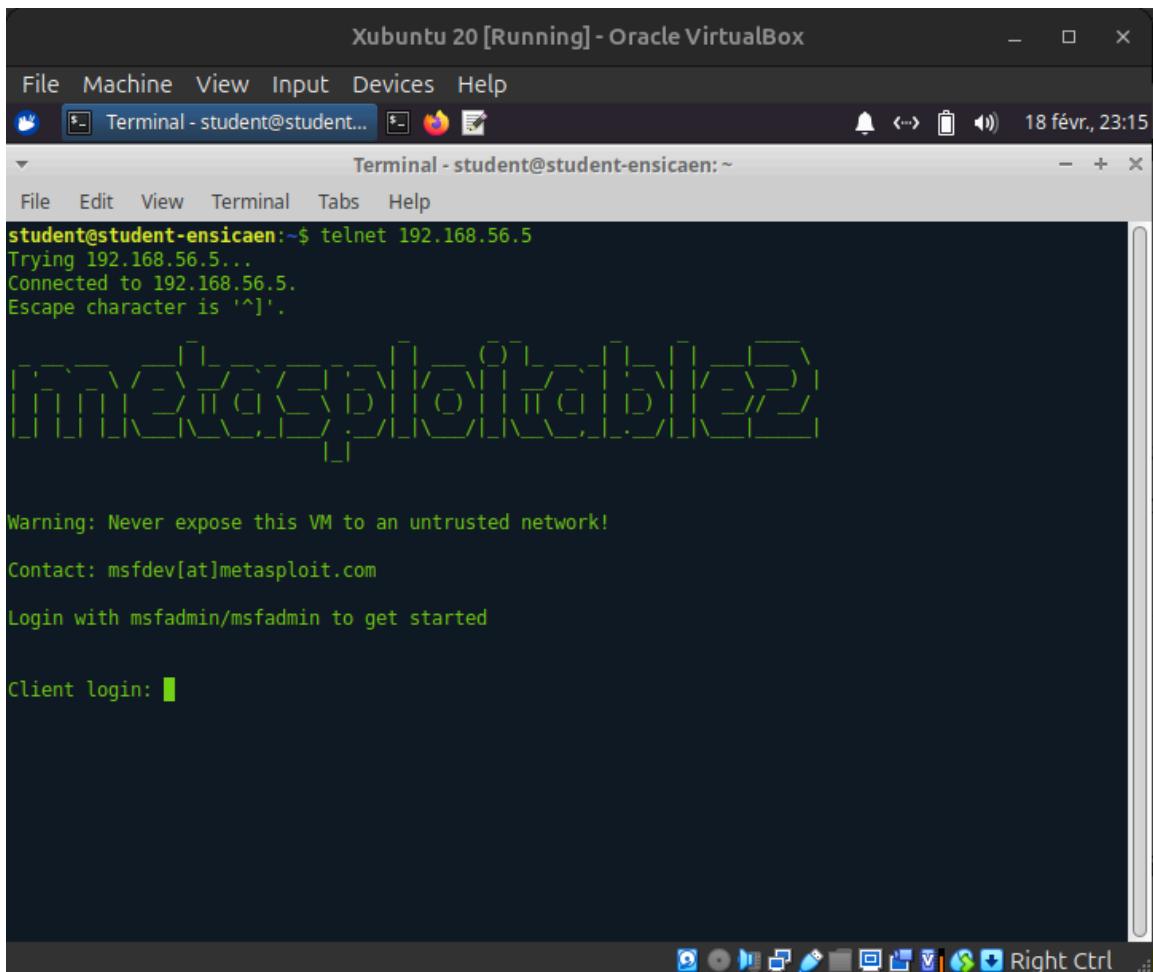
Testing packet capture with our network

```
student@student-ensicaen:~$ ping 192.168.56.5
PING 192.168.56.5 (192.168.56.5) 56(84) bytes of data.
64 bytes from 192.168.56.5: icmp_seq=1 ttl=64 time=0.421 ms
64 bytes from 192.168.56.5: icmp_seq=2 ttl=64 time=0.421 ms
64 bytes from 192.168.56.5: icmp_seq=3 ttl=64 time=0.357 ms
64 bytes from 192.168.56.5: icmp_seq=4 ttl=64 time=0.485 ms
64 bytes from 192.168.56.5: icmp_seq=5 ttl=64 time=0.359 ms
64 bytes from 192.168.56.5: icmp_seq=6 ttl=64 time=0.280 ms
64 bytes from 192.168.56.5: icmp_seq=7 ttl=64 time=0.334 ms
64 bytes from 192.168.56.5: icmp_seq=8 ttl=64 time=0.286 ms
64 bytes from 192.168.56.5: icmp_seq=9 ttl=64 time=0.355 ms
64 bytes from 192.168.56.5: icmp_seq=10 ttl=64 time=0.741 ms
64 bytes from 192.168.56.5: icmp_seq=11 ttl=64 time=0.402 ms
64 bytes from 192.168.56.5: icmp_seq=12 ttl=64 time=0.419 ms
```



4. Open a terminal and run:

```
telnet <MyServer IP>
```

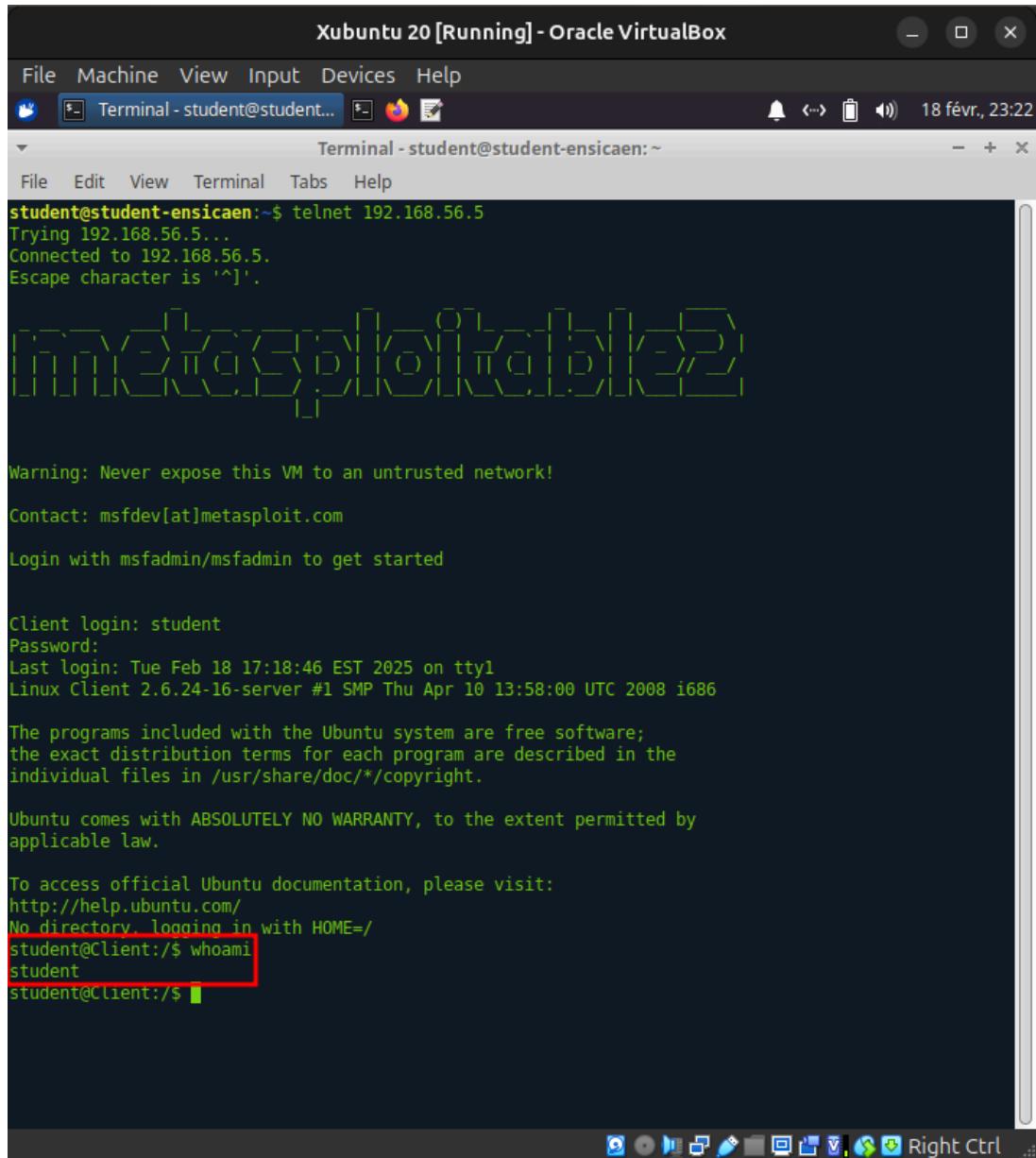


5. Log in using the **MyServer** credentials.

6. Run `whoami` again and explain the output.

After connecting to the **MyServer** machine via **Telnet** and running the `whoami` command, the terminal will display the authenticated user on MyServer.

- **If the login is successful**, the output will be:



The screenshot shows a terminal window titled "Terminal - student@student-ensicaen:~". The window is part of an Oracle VirtualBox instance named "Xubuntu 20 [Running]". The terminal content is as follows:

```
student@student-ensicaen:~$ telnet 192.168.56.5
Trying 192.168.56.5...
Connected to 192.168.56.5.
Escape character is '^['.

[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

Client login: student
Password:
Last login: Tue Feb 18 17:18:46 EST 2025 on ttym
Linux Client 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No directory, logging in with HOME=/
student@Client:/$ whoami
student
student@Client:/$
```

This confirms that authentication was successful and that the user "student" has access to the remote system.

7. Stop the traffic capture in Wireshark.

Capturing from vboxnet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length Info
88	22.524069308	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
90	22.750583274	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
91	22.750929377	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
93	22.991044987	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
94	22.991308264	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
96	23.488955124	192.168.56.2	192.168.56.5	TELNET	68 2 bytes data
97	23.489190919	192.168.56.5	192.168.56.2	TELNET	68 2 bytes data
99	23.490931380	192.168.56.5	192.168.56.2	TELNET	75 9 bytes data
101	23.491258026	192.168.56.5	192.168.56.2	TELNET	84 18 bytes data
107	41.228419030	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
108	41.228711091	192.168.56.5	192.168.56.2	TELNET	187 121 bytes data
110	41.266413104	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
111	41.266806516	192.168.56.5	192.168.56.2	TELNET	187 121 bytes data
113	41.303757362	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
114	41.364046648	192.168.56.5	192.168.56.2	TELNET	188 122 bytes data
116	41.359330119	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
117	41.359640173	192.168.56.5	192.168.56.2	TELNET	188 122 bytes data
119	41.396925360	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
120	41.397288485	192.168.56.5	192.168.56.2	TELNET	188 122 bytes data
122	41.522361155	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
123	41.522622959	192.168.56.5	192.168.56.2	TELNET	189 123 bytes data
125	42.451634478	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
126	42.451902404	192.168.56.5	192.168.56.2	TELNET	186 120 bytes data
128	42.578932323	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
129	42.579170342	192.168.56.5	192.168.56.2	TELNET	186 120 bytes data
131	42.641795464	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
132	42.642100639	192.168.56.5	192.168.56.2	TELNET	186 120 bytes data
134	42.710549290	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
135	42.710843816	192.168.56.5	192.168.56.2	TELNET	185 119 bytes data
137	43.068191397	192.168.56.2	192.168.56.5	TELNET	75 Suboption Negotiate About Window Size
138	43.068447790	192.168.56.5	192.168.56.2	TELNET	186 120 bytes data

Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface vboxnet0, id 0
Ethernet II, Src: PCSSystemtec_5a:88:ab (08:00:27:5a:88:ab), Dst: PCSSystemtec_4d:08:fc (08:00:27:4d:08:fc)
Internet Protocol Version 4, Src: 192.168.56.2, Dst: 192.168.56.5
Transmission Control Protocol, Src Port: 38042, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
Telnet

8. Analyze the captured traffic and apply filters to isolate **Telnet** data.

9. Identify and extract the **username and password** exchanged during the session.

Login ✓

*vboxnet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length Info
16	9.994774358	192.168.56.2	192.168.56.5	TELNET	173 Suboption Negotiate About Window Size
18	9.996807041	192.168.56.5	192.168.56.2	TELNET	69 Do Echo
20	9.996998943	192.168.56.2	192.168.56.5	TELNET	69 Won't Echo
21	9.997100033	192.168.56.5	192.168.56.2	TELNET	69 Will Echo
23	9.997195343	192.168.56.2	192.168.56.5	TELNET	69 Do Echo
24	9.997242592	192.168.56.5	192.168.56.2	TELNET	678 612 bytes data
27	*REF*	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
29	0.000315745	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
31	1.350204725	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
32	1.350469986	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
34	1.661676926	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
35	1.661903423	192.168.56.5	192.168.56.2	TELNET	67 1 byte data
37	1.917884052	192.168.56.2	192.168.56.5	TELNET	67 1 byte data
38	1.918180921	192.168.56.5	192.168.56.2	TELNET	67 1 byte data

Frame 27: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface vboxnet0, id 0
Ethernet II, Src: PCSSystemtec_5a:88:ab (08:00:27:5a:88:ab), Dst: PCSSystemtec_4d:08:fc (08:00:27:4d:08:fc)
Internet Protocol Version 4, Src: 192.168.56.2, Dst: 192.168.56.5
Transmission Control Protocol, Src Port: 38042, Dst Port: 23, Seq: 141, Ack: 670, Len: 1
Telnet
Data: s

wireshark_vboxnet0FD9J22.pcapng

Packets: 143 · Displayed: 76 (53.1%) · Dropped: 0 (0.0%) · Profile: Default

```

▼ Telnet
  Data: t

▼ Telnet
  Data: u

▼ Telnet
  Data: d

▼ Telnet
  Data: e

▼ Telnet
  Data: n

▼ Telnet
  Data: t

```

Password ✓

*vboxnet0

No.	Time	Source	Destination	Protocol	Length	Info
50	3.662642747	192.168.56.5	192.168.56.2	TELNET	68	2 bytes data
52	3.662911695	192.168.56.5	192.168.56.2	TELNET	76	10 bytes data
54	4.519117135	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
56	4.851450122	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
58	5.785814372	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
60	6.156563925	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
62	6.552315339	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
64	7.004314217	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
66	7.389276793	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
68	7.735454825	192.168.56.2	192.168.56.5	TELNET	67	1 byte data
70	8.180403622	192.168.56.2	192.168.56.5	TELNET	68	2 bytes data
72	8.189949011	192.168.56.5	192.168.56.2	TELNET	68	2 bytes data
74	8.190232846	192.168.56.5	192.168.56.2	TELNET	582	516 bytes data
76	8.200507001	192.168.56.5	192.168.56.2	TELNET	64	10 bytes data

► Frame 54: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface vboxnet0, id 0
 ► Ethernet II, Src: PCSSystemtec_5a:88:ab (08:00:27:5a:88:ab), Dst: PCSSystemtec_4d:08:fc (08:00:27:4d:
 ► Internet Protocol Version 4, Src: 192.168.56.2, Dst: 192.168.56.5
 ► Transmission Control Protocol, Src Port: 38042, Dst Port: 23, Seq: 150, Ack: 689, Len: 1
 ▼ Telnet
 Data: e

wireshark_vboxnet0FD9J22.pcapng | Packets: 143 · Displayed: 76 (53.1%) · Dropped: 0 (0.0%) | Profile: Default

```

▼ TRANSMISSION CONTROL PROTOCOL, SRC PORT: 38042, DST PORT: 23, SEQ: 151, ACK: 689, LEN: 1
  ▼ Telnet
    Data: n

```

```

▼ TRANSMISSION CONTROL PROTOCOL, SRC PORT: 38042, DST PORT: 23, SEQ: 152, ACK: 689, LEN: 1
  ▼ Telnet
    Data: s

```

```

▼ Telnet
  Data: i

```

```

▼ Telnet
  Data: c

```

```
▼ Telnet  
Data: a
```



```
▼ Telnet  
Data: e
```



```
▼ Telnet  
Data: n
```

10. Type "**quit**" to exit the Telnet session.

11. What solution can be implemented to **secure authentication data**?

The **Telnet** protocol does not provide encryption, making it highly vulnerable to sniffing attacks.

Replace Telnet with SSH:

- **SSH (Secure Shell)** encrypts communications, preventing credential capture.
- SSH supports **public key authentication**, eliminating the need to send passwords over the network.

4. Capturing HTTP Data

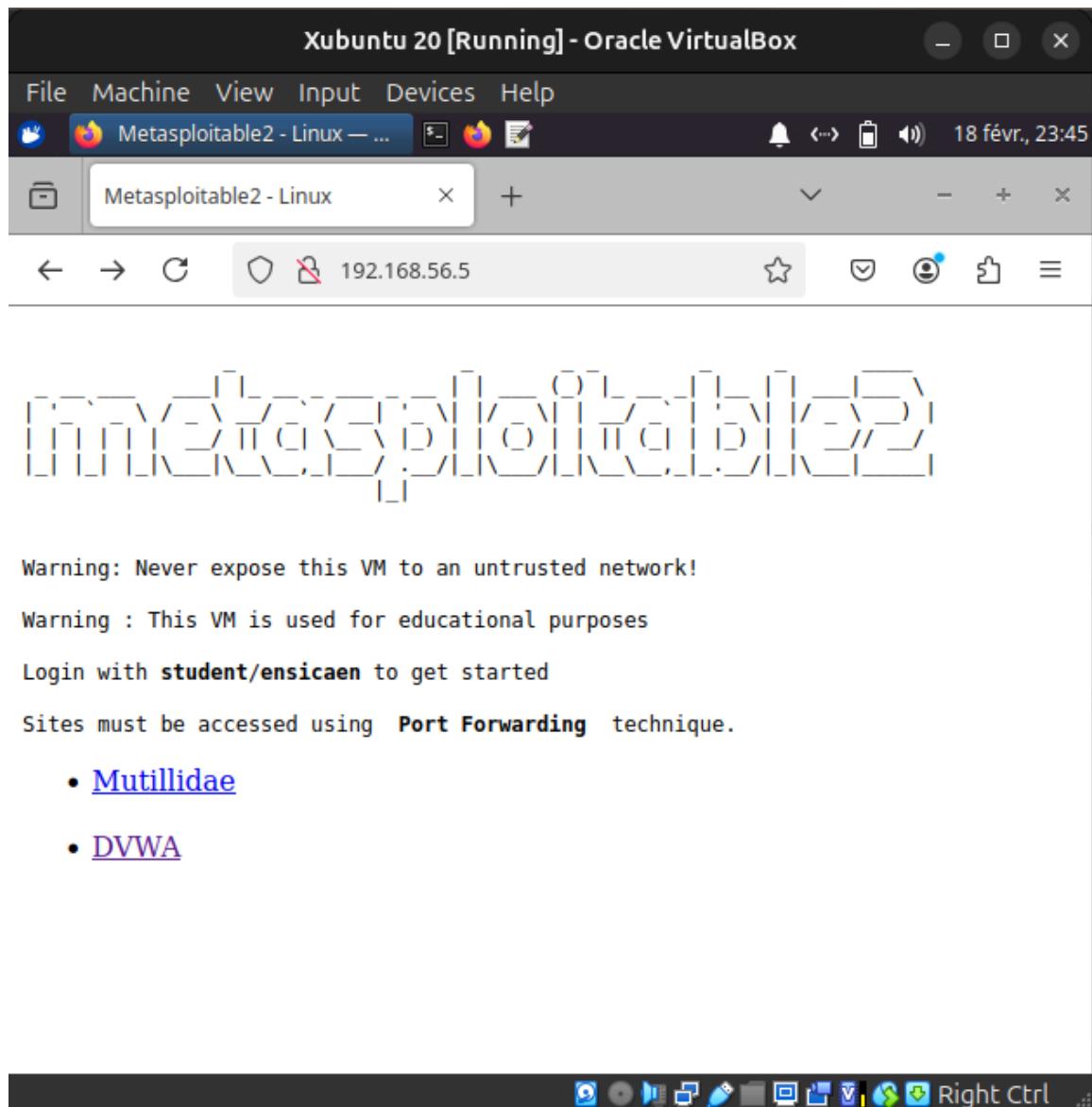
1. Start a **new capture** in Wireshark.

2. Open **Firefox** browser.

3. In the address bar, enter:

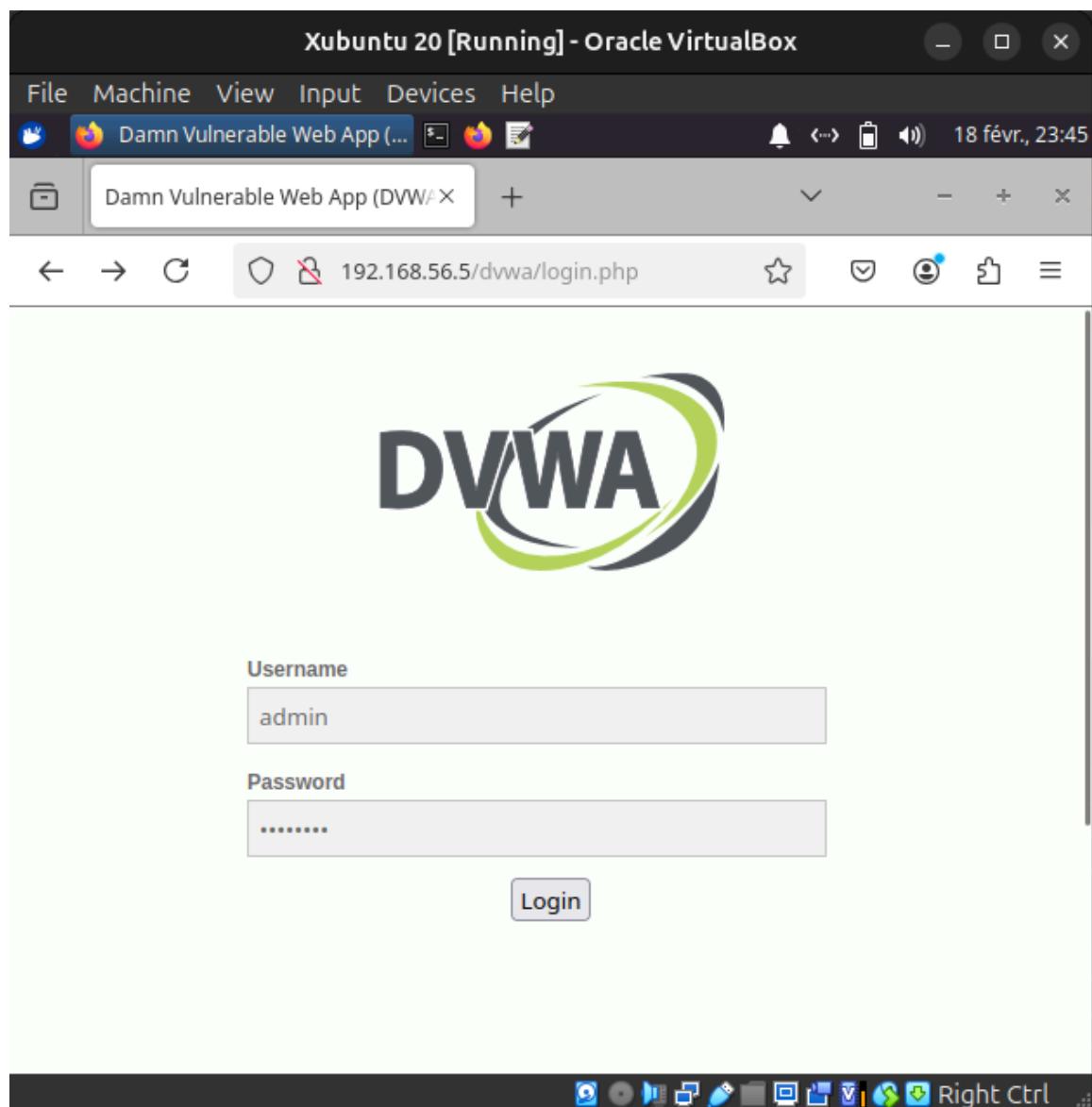
```
http://<MyServer IP>
```

4. Click on the "**DVWA**" link.

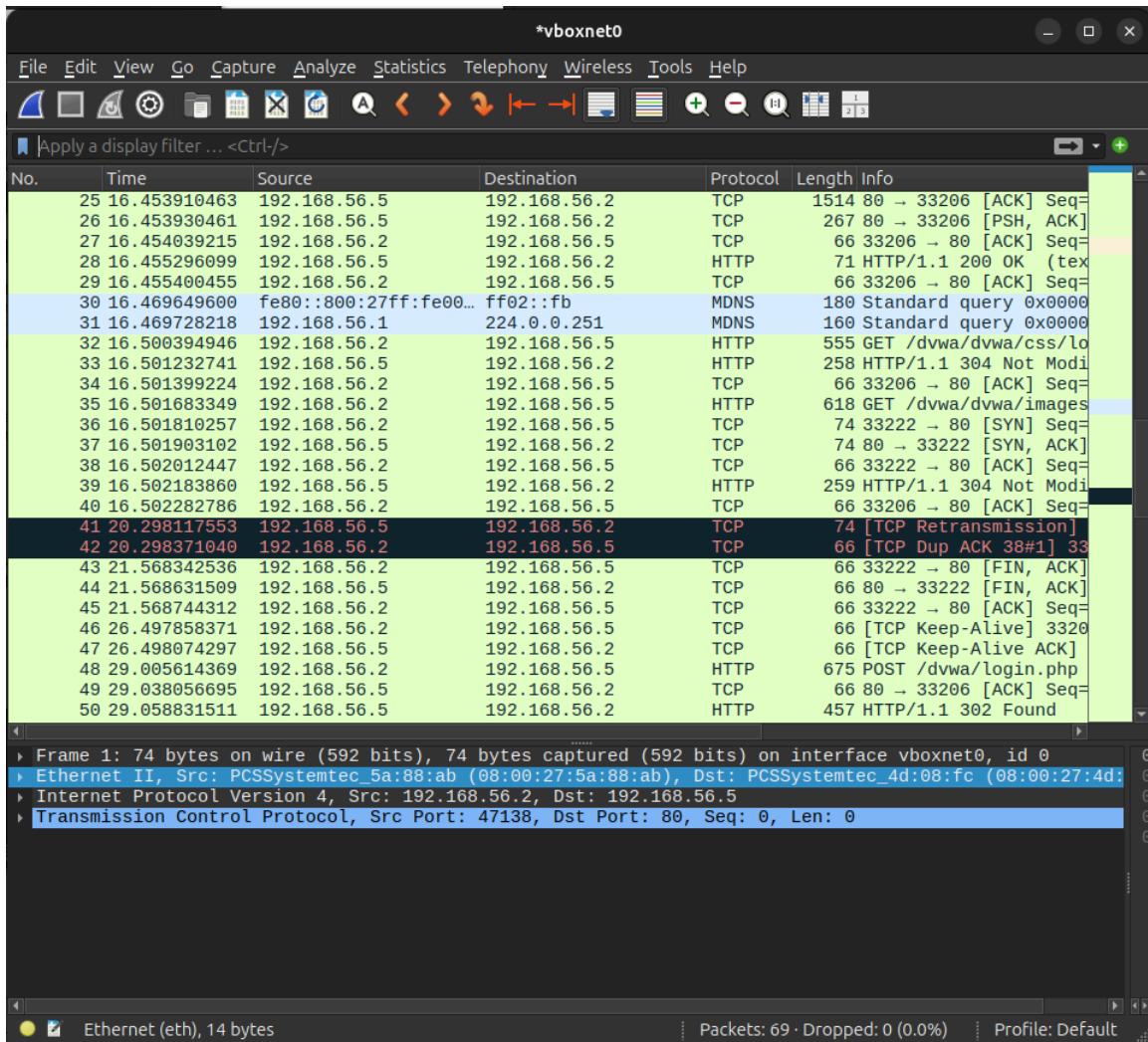


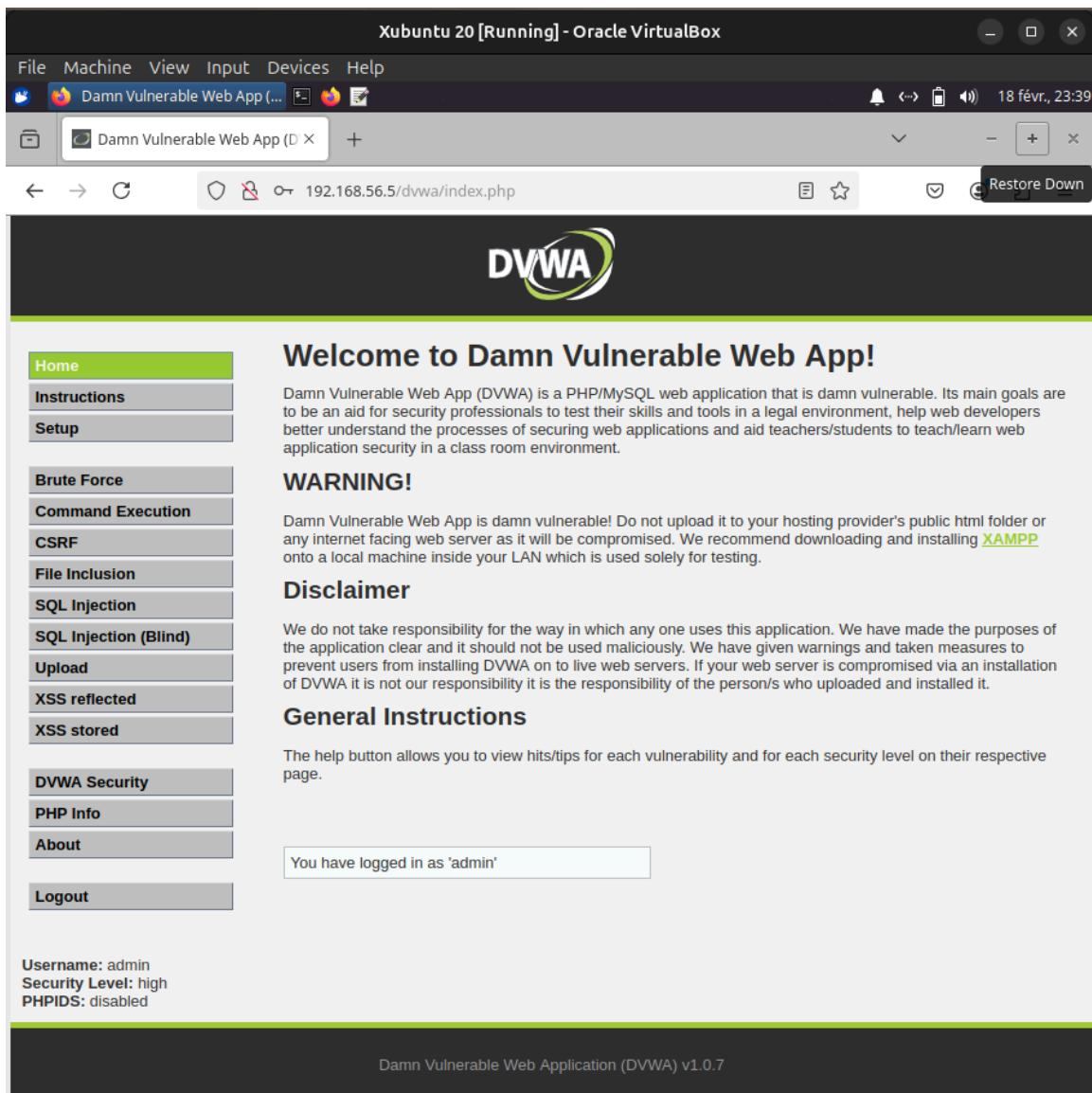
5. On the login page, enter the credentials:

admin | password

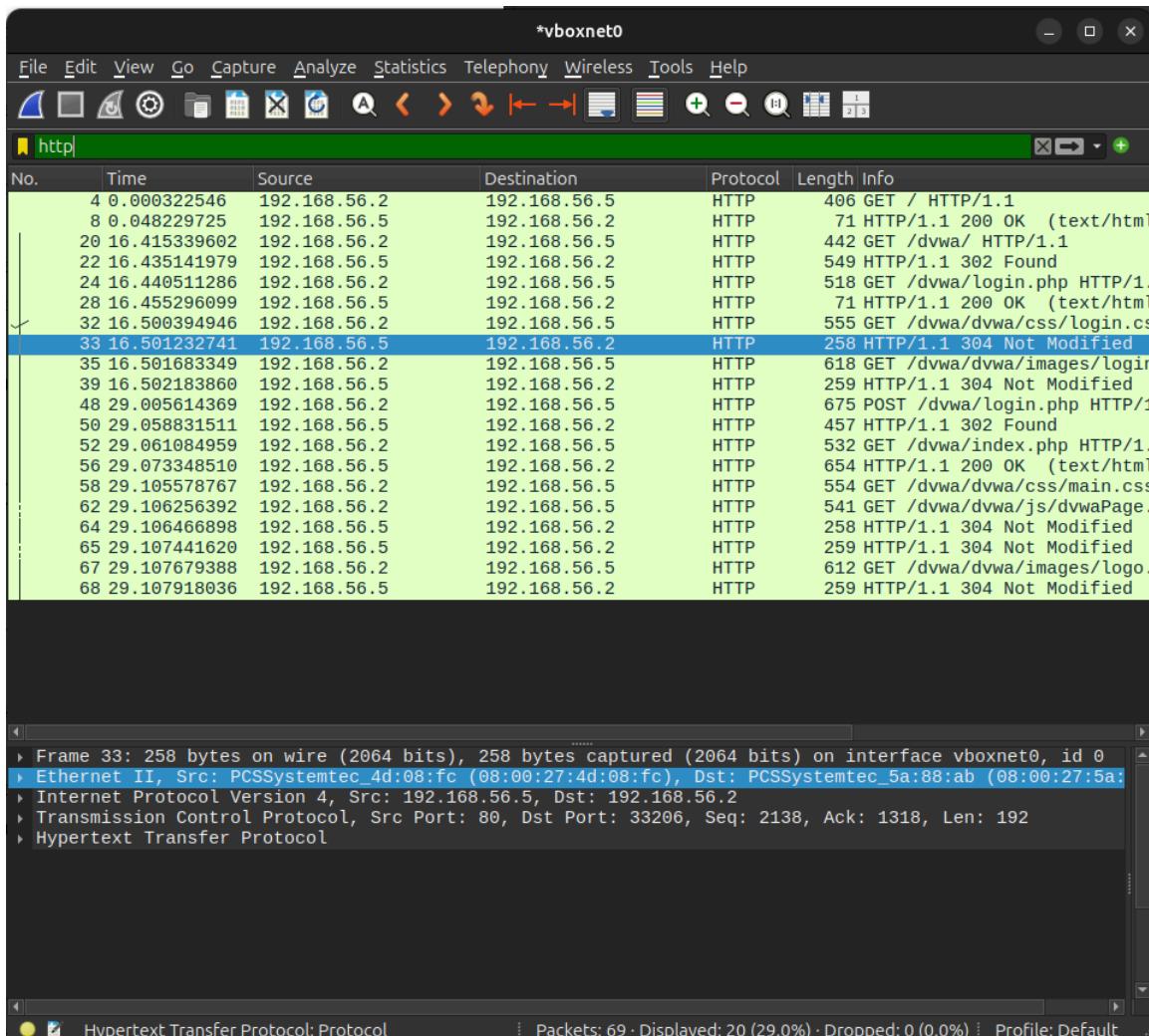


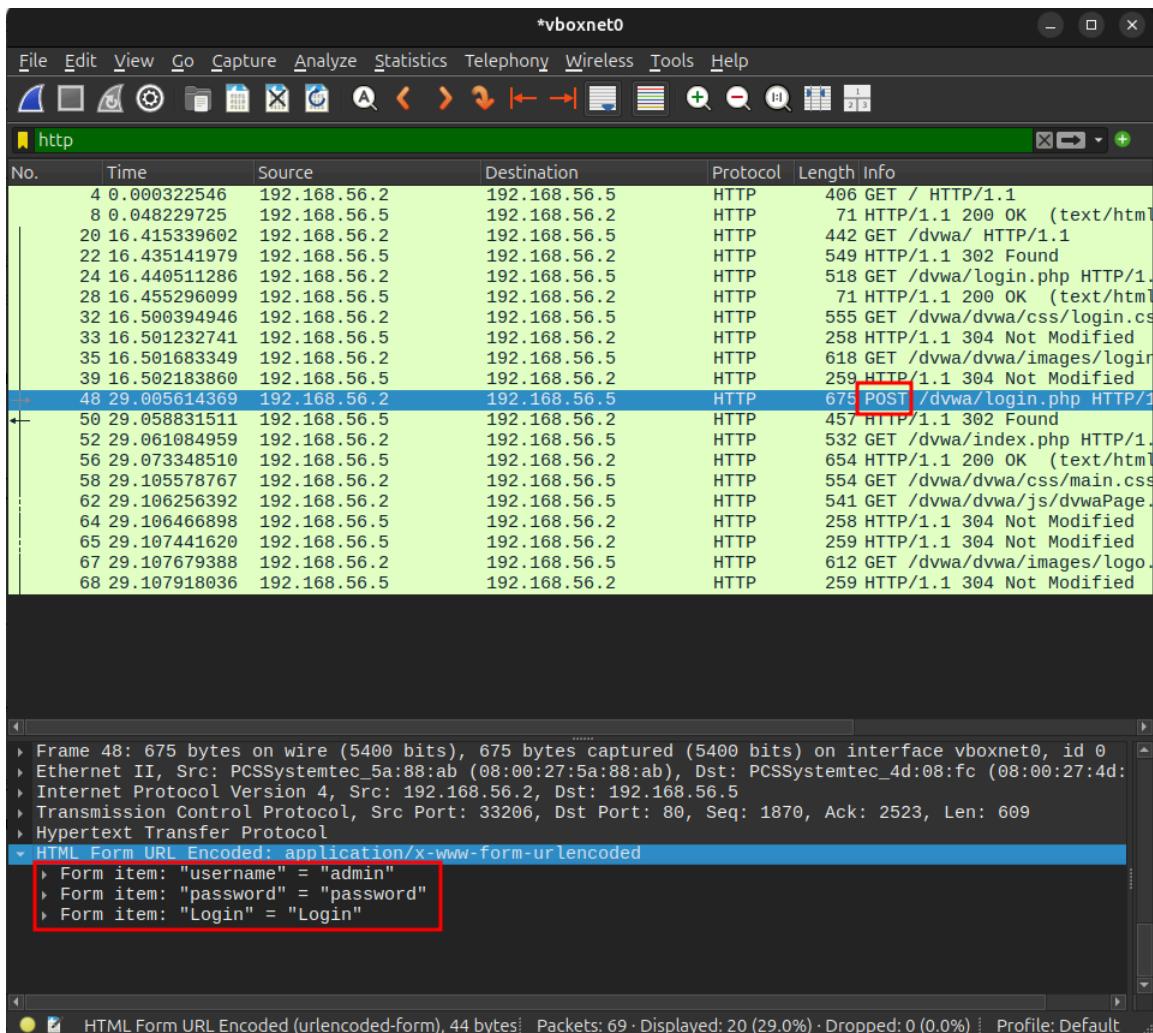
6. Once logged in, stop the packet capture.





7. Analyze the captured traffic and apply filters for **HTTP traffic**.





8. What solution can be implemented to **secure authentication data**?

The **HTTP** protocol also transmits data in **plaintext**, meaning credentials can be easily intercepted. Solutions to protect authentication data include:

1 - Use HTTPS (HyperText Transfer Protocol Secure)

- HTTPS uses **TLS/SSL** to encrypt data between the client and the server.

2 - Implement token-based authentication

- Methods like **OAuth**, **JWT (JSON Web Token)**, or **encrypted session cookies** prevent credentials from being repeatedly sent.

3 - Enable HSTS (HTTP Strict Transport Security)

- HSTS forces browsers to always use HTTPS when communicating with the server.

Troubleshooting Errors

If you encounter errors such as:

```
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is another process using it?
```

Try running the following commands:

```
sudo rm /var/lib/apt/lists/lock
sudo rm /var/cache/apt/archives/lock
sudo rm /var/lib/dpkg/lock*
sudo dpkg --configure -a
sudo apt update
```