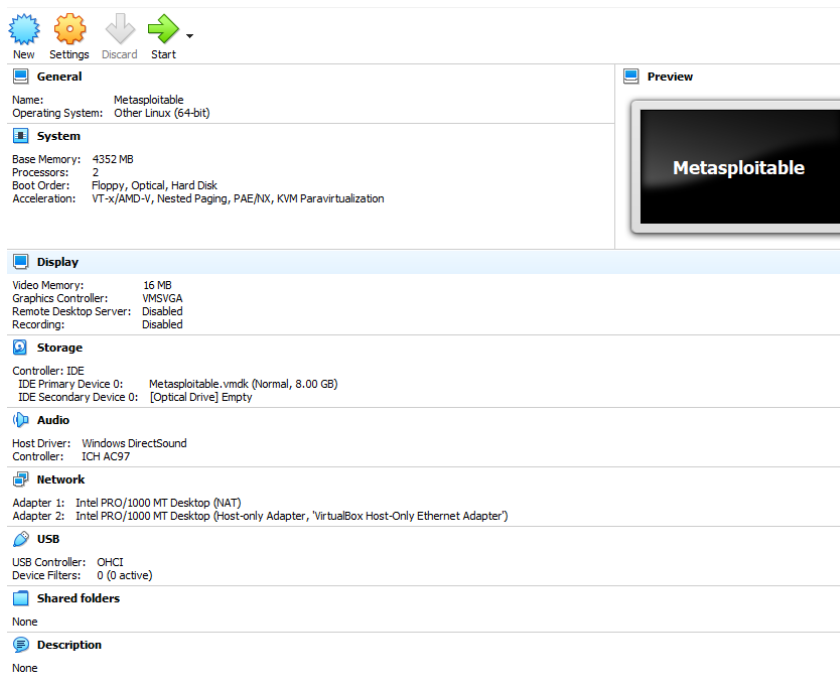


a. Objectives: I will be simulating a man-in-the-middle attack to collect information that a user puts into the computer and transmitted over the network. In the process I learn how to collect net traffic across a network and how to do ARP Poisoning. I exploit that a script could runs this attack on a network after being inserted into it and being run by itself or the hacker.

b. Lab Environment: I used an intentionally vulnerable Linux virtual machine called Metasploitable which hosts a vulnerable web application. This is to have a place for the Windows VM to communicate with so that the Ubuntu VM can commit a man-in-the-middle attack.



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





metasploitable login: msfadmin
Password:
Last login: Fri Sep 16 01:13:48 EDT 2022 on tty1
Linux metasploitable 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 mail.
msfadmin@metasploitable:~$ _
```

On the Ubuntu VM I ran Ettercap which Conducts a man-in-the-middle attack by ARP Poisoning the network. I also ran Wireshark on Ubuntu to capture the network traffic from the Windows VM. I made no change the Windows VM or to the network adaptor.








General


Name: Ubuntu
Operating System: Ubuntu (64-bit)


System


Base Memory: 7684 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization


Display


Video Memory: 92 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled


Storage


Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 80.00 GB)


Audio


Host Driver: Windows DirectSound
Controller: ICH AC97


Network


Adapter 1: Intel PRO/1000 MT Desktop (NAT)


USB


USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)



Shared folders

None


Description

None


Preview



c. Tool details:

- Ettercap is from Alberto Ornaghi, Marco Valleri, Emilio Escobar, Alexander Koeppel, Gianfranco Costamagna, and Ali Abdulkadir. Its located at <https://www.ettercap-project.org/downloads.html>.
- Current version is 0.8.3.1-Bertillon released on August 1, 2020
- It can run on Linux and MacOSX (Snow Leopard & Lion)
- Ettercap is a comprehensive suite for man-in-the -middle attacks. It features sniffing of live connections, content filtering on the fly. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

d. Scenario:

I will be using a Windows VM as the attacked machine and also the Mutillidae web app in the Metasploitable VM so that the Windows VM transmits data of the network so that I can then use a Ubuntu VM running Ettercap and Wireshark to intercept and to capture that web traffic that is being sent over the network. My expected outcome is to collect valuable info about the user that inputs information into the Windows VM which is their username and password.

e. Experiment:

After launching the Metasploitable VM what until it says “metasploitable login:” then type “msfadmin” as the username and password.

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Sep 16 01:13:48 EDT 2022 on tty1
Linux metasploitable 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.

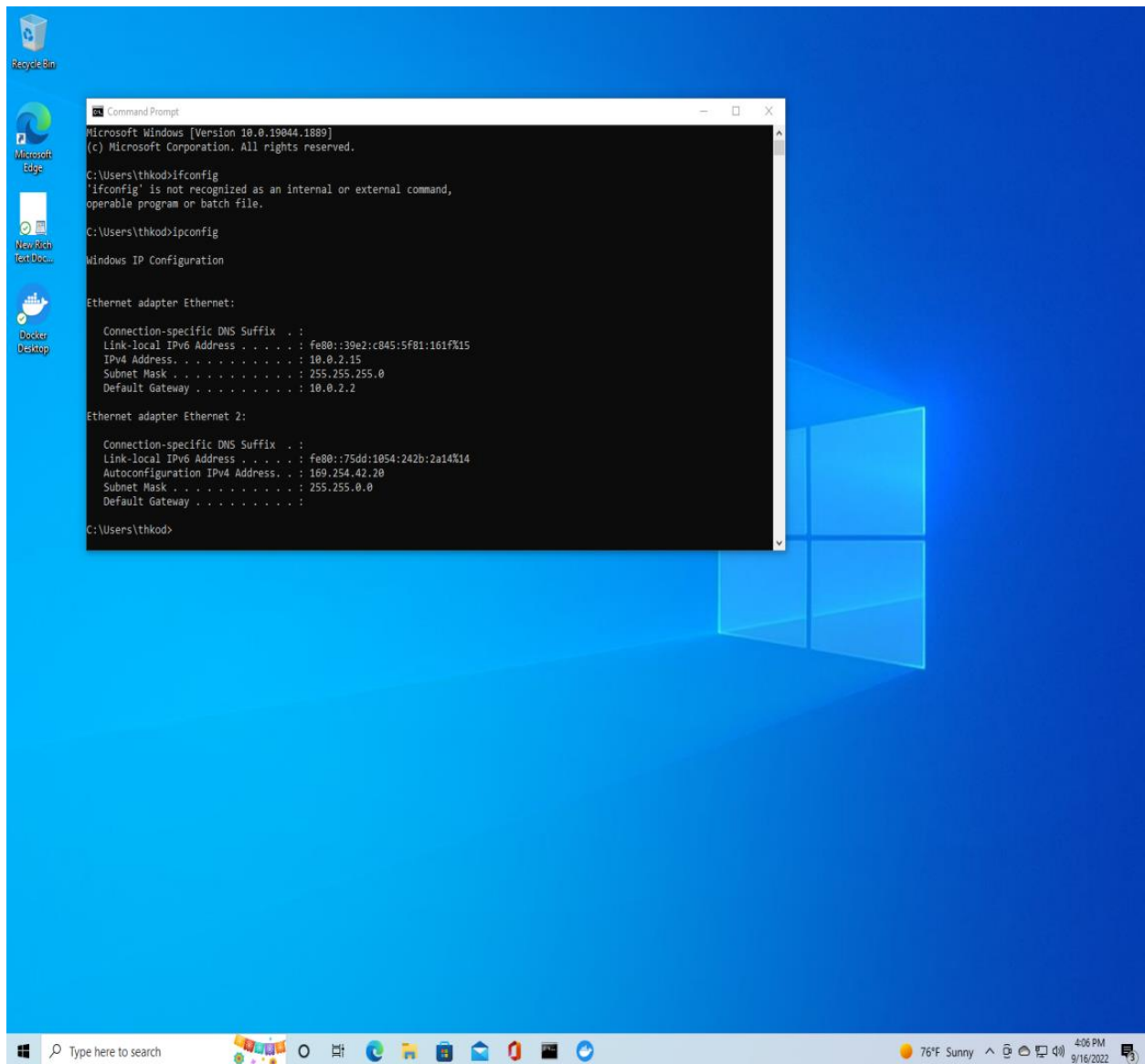
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Then at the next prompt type “ifconfig” to get the IP address to connect to the web portal which is the first listed as “int addr:”, it’s going to be a 192.168.x.x IP address.

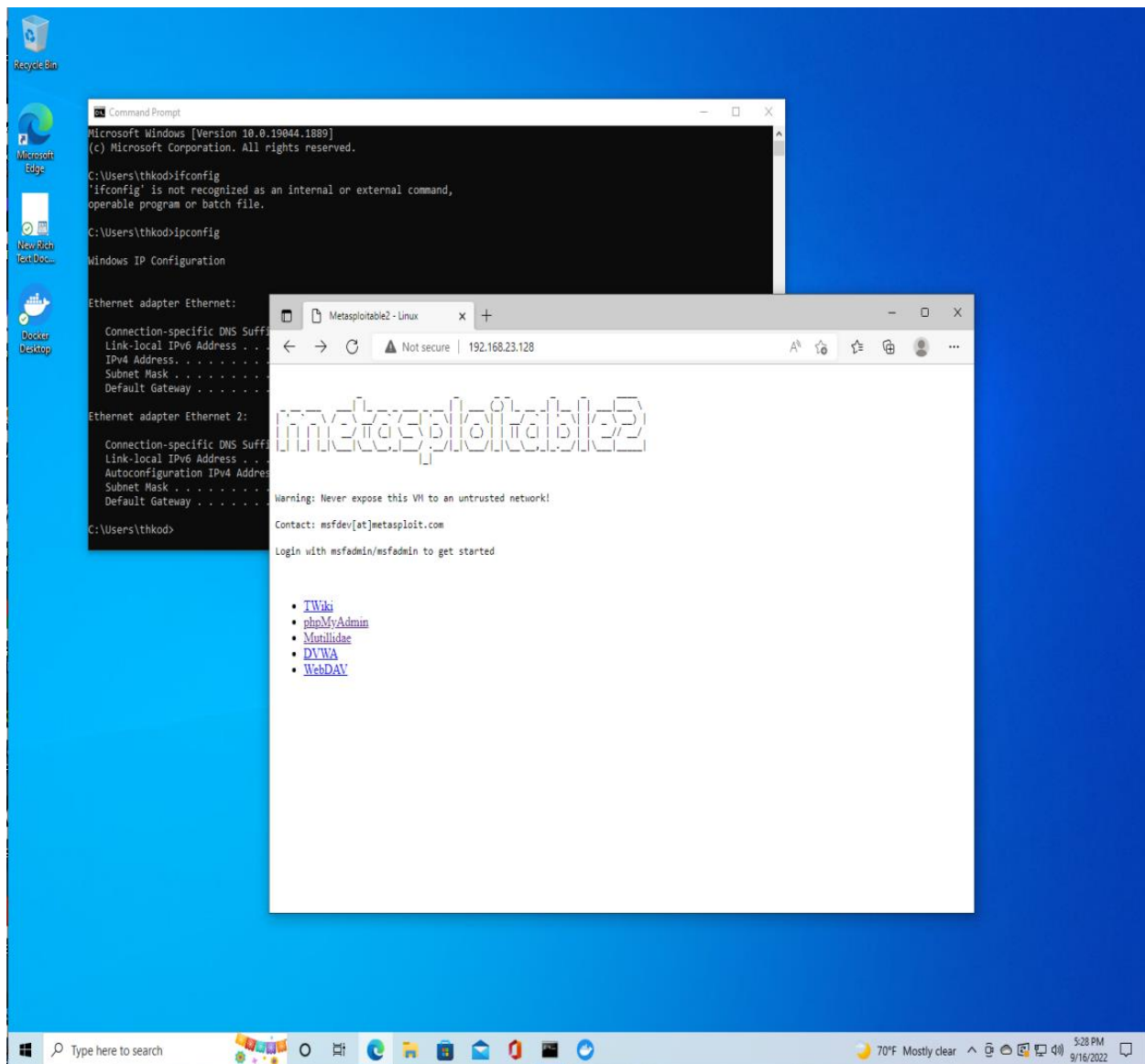
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:32:a8:d5
          inet addr:192.168.23.128  Bcast:192.168.23.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:a8d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4129 (4.0 KB)  TX bytes:7402 (7.2 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

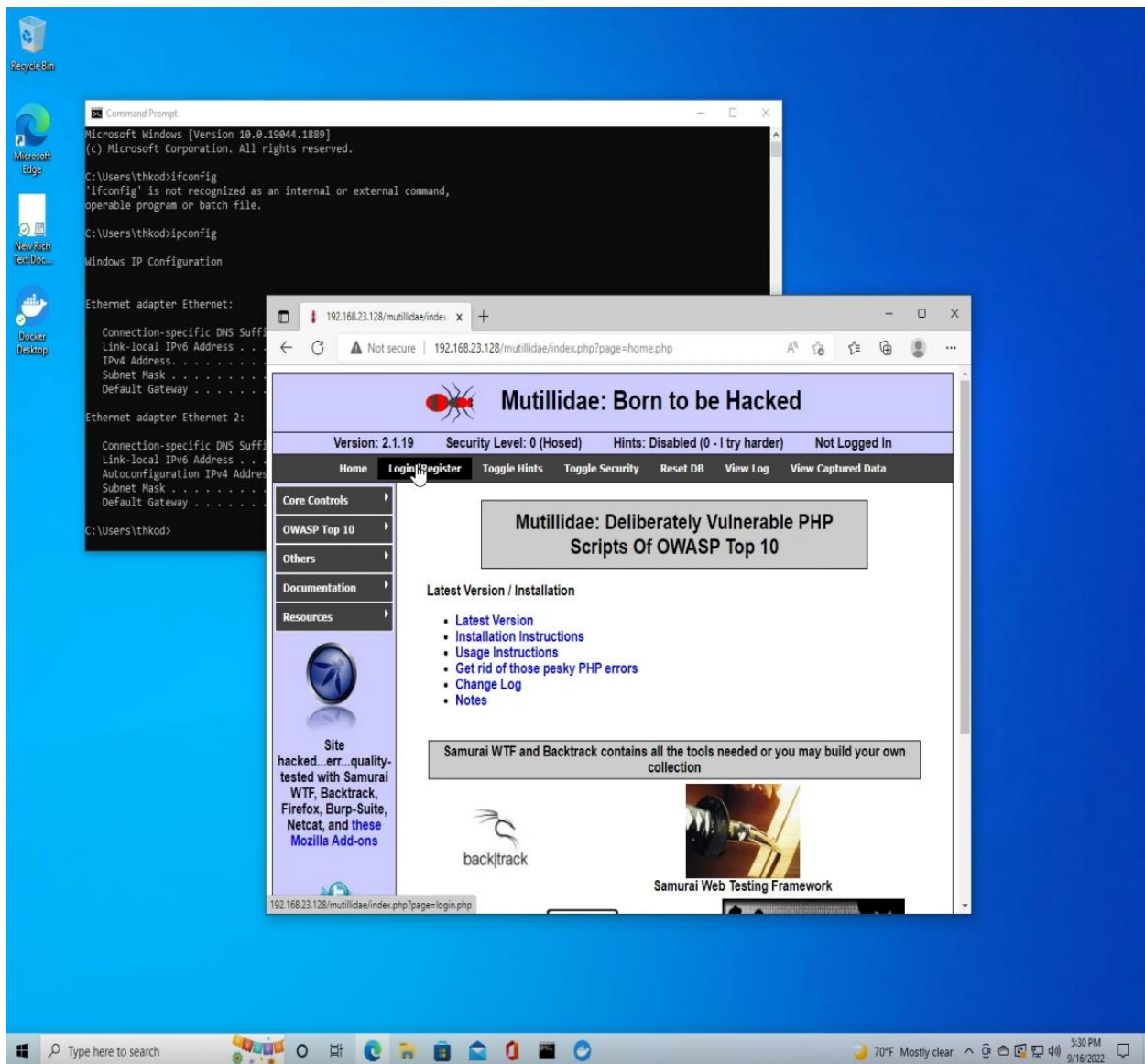


Then, launch the Windows VM and login to the home screen. Next, open the command prompt and run “ipconfig” to get the IP address of the Windows VM.

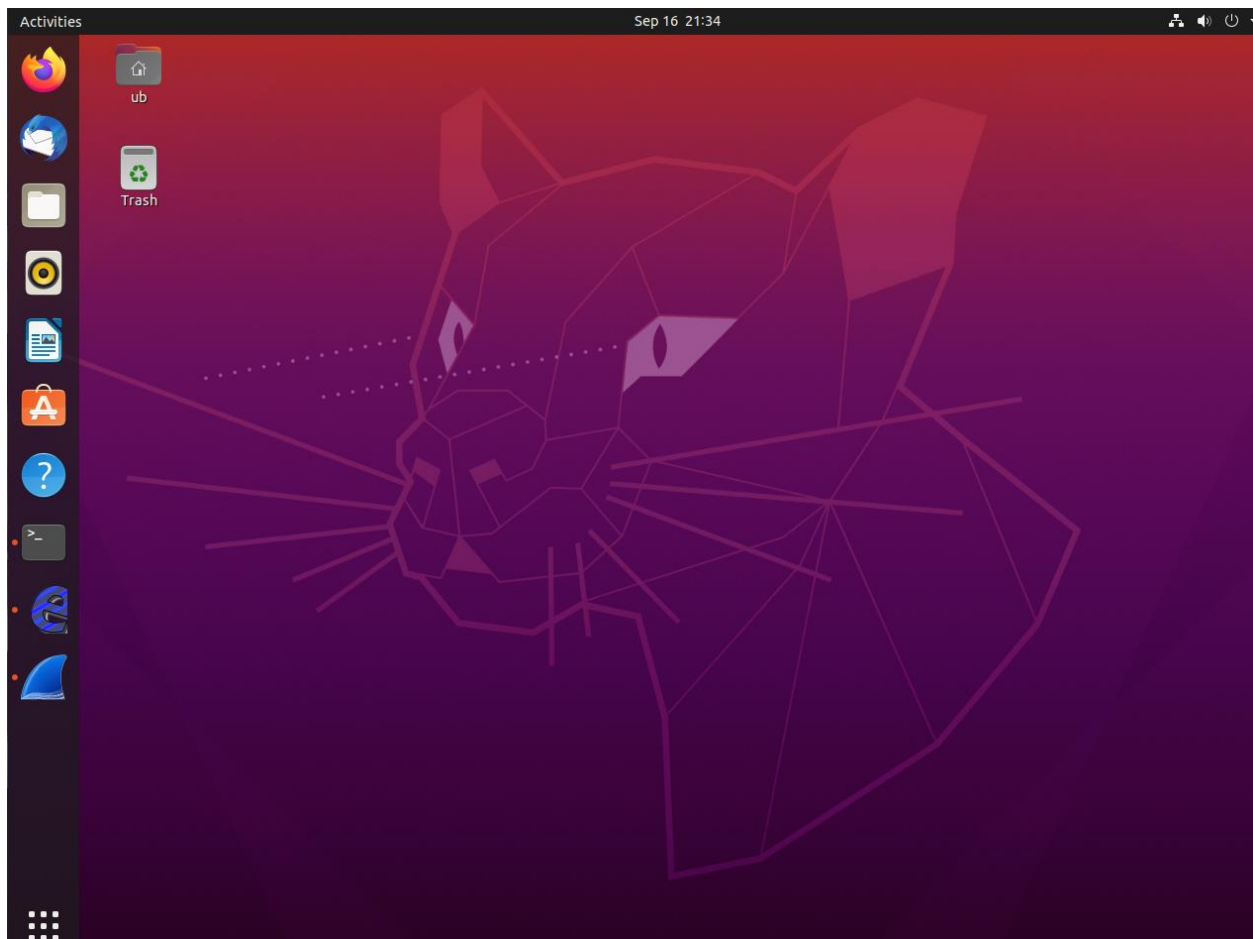


Then, open Edge web browser and go to 192.168.x.x address that was found on the other VM.

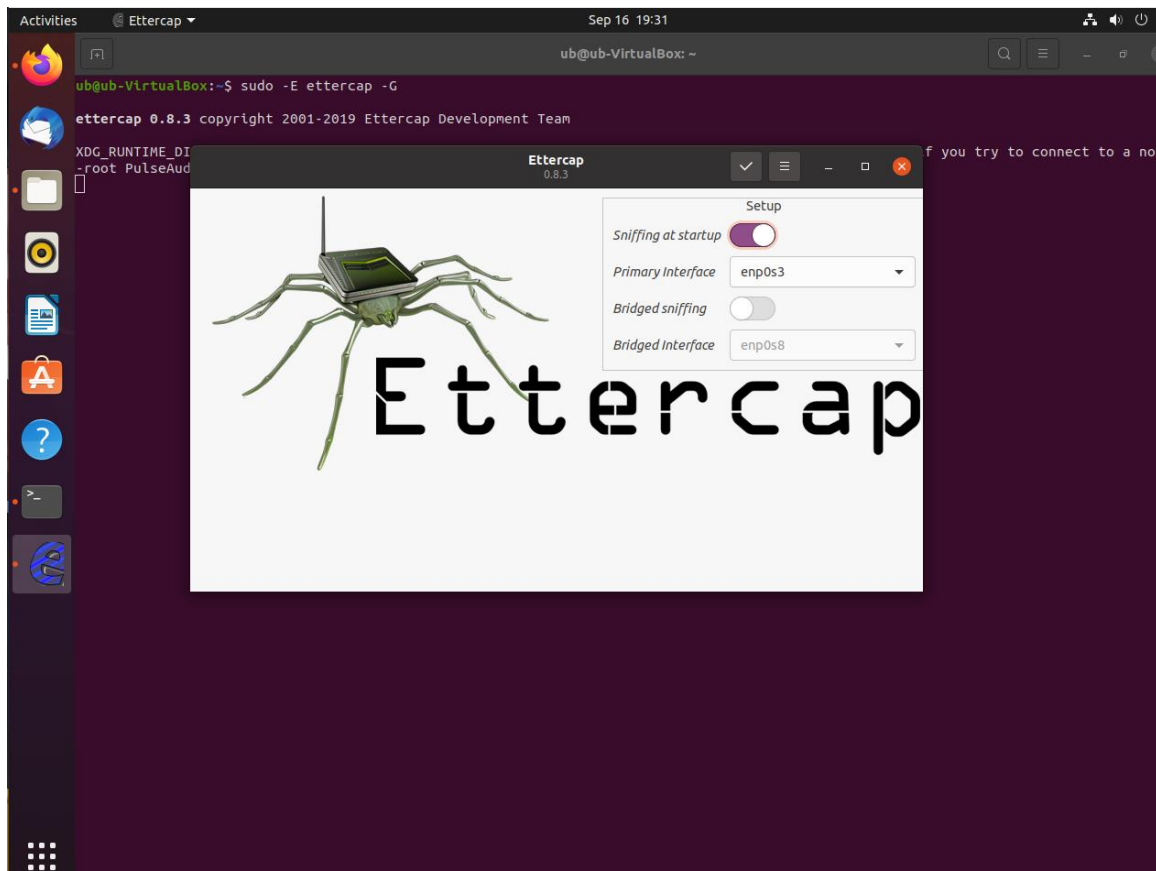
Next, Click on “Mutillidae” in the bulleted list to continue.



Then, navigate the directory and on the top left side of the page click on “Login/Register” where you will then be taken to a Login screen.



Then Open the Ubuntu VM and login to the home screen.

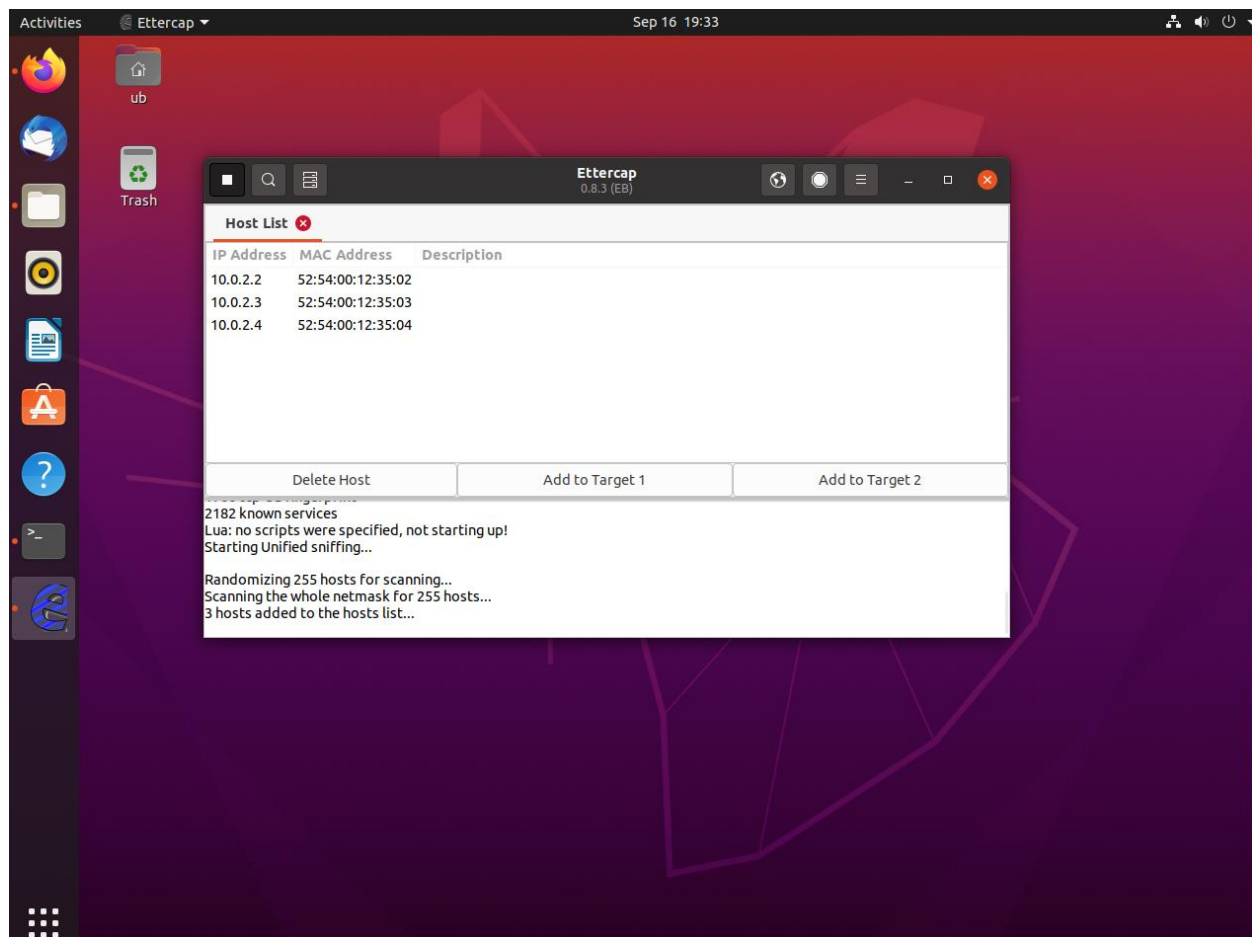


Next, Open the Terminal and run “sudo -E Ettercap -G” or find it in the list of apps on the bottom left of the screen. This will open Ettercap as a graphical interface, if this were to take place in the real world the GUI would be found so only the CLI version would be used.

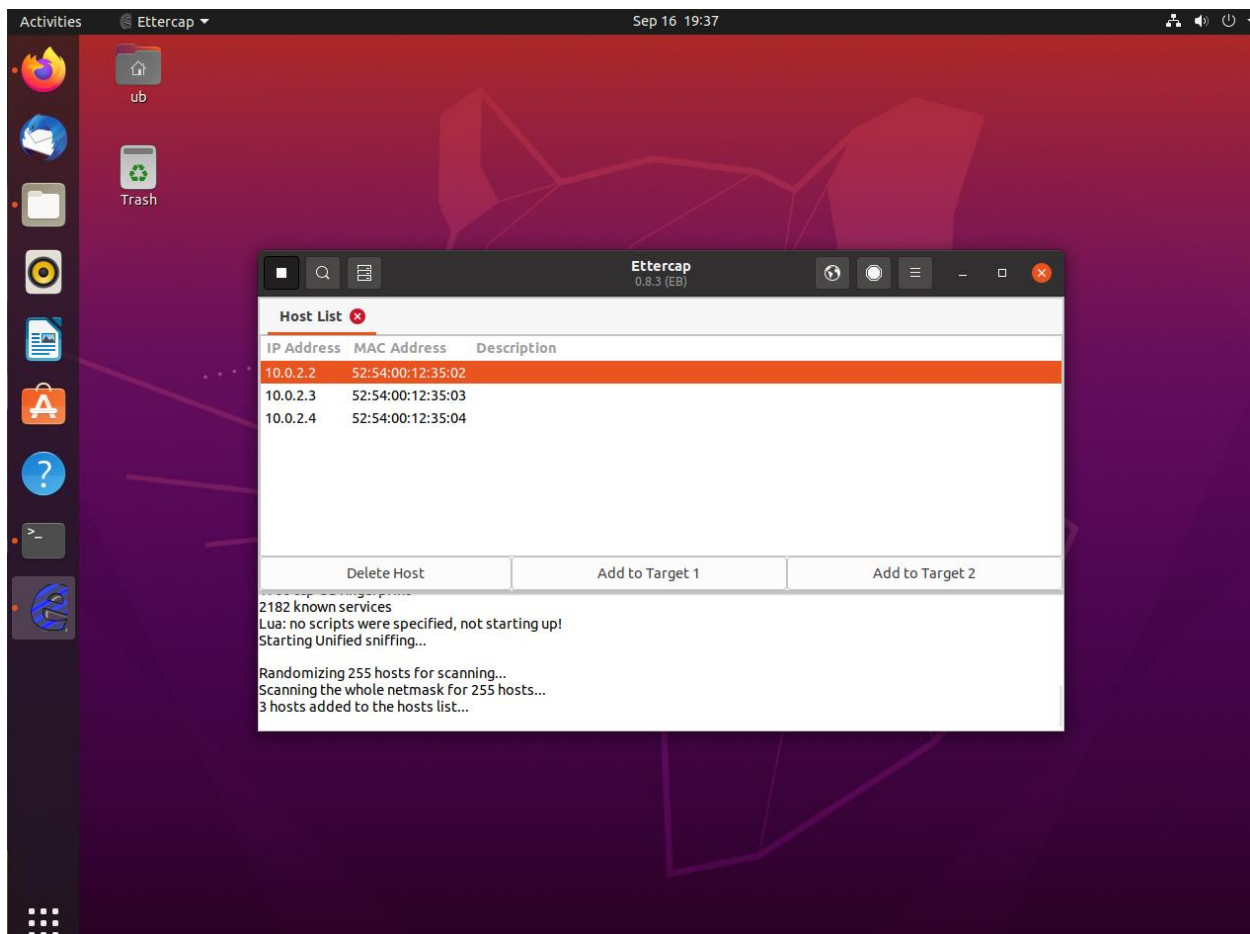
Then, make sure “Sniffing at startup is selected” and the “Primary Interface” from the dropdown box is set to “enp0s3”. Click the checkmark on the top of the window to continue.



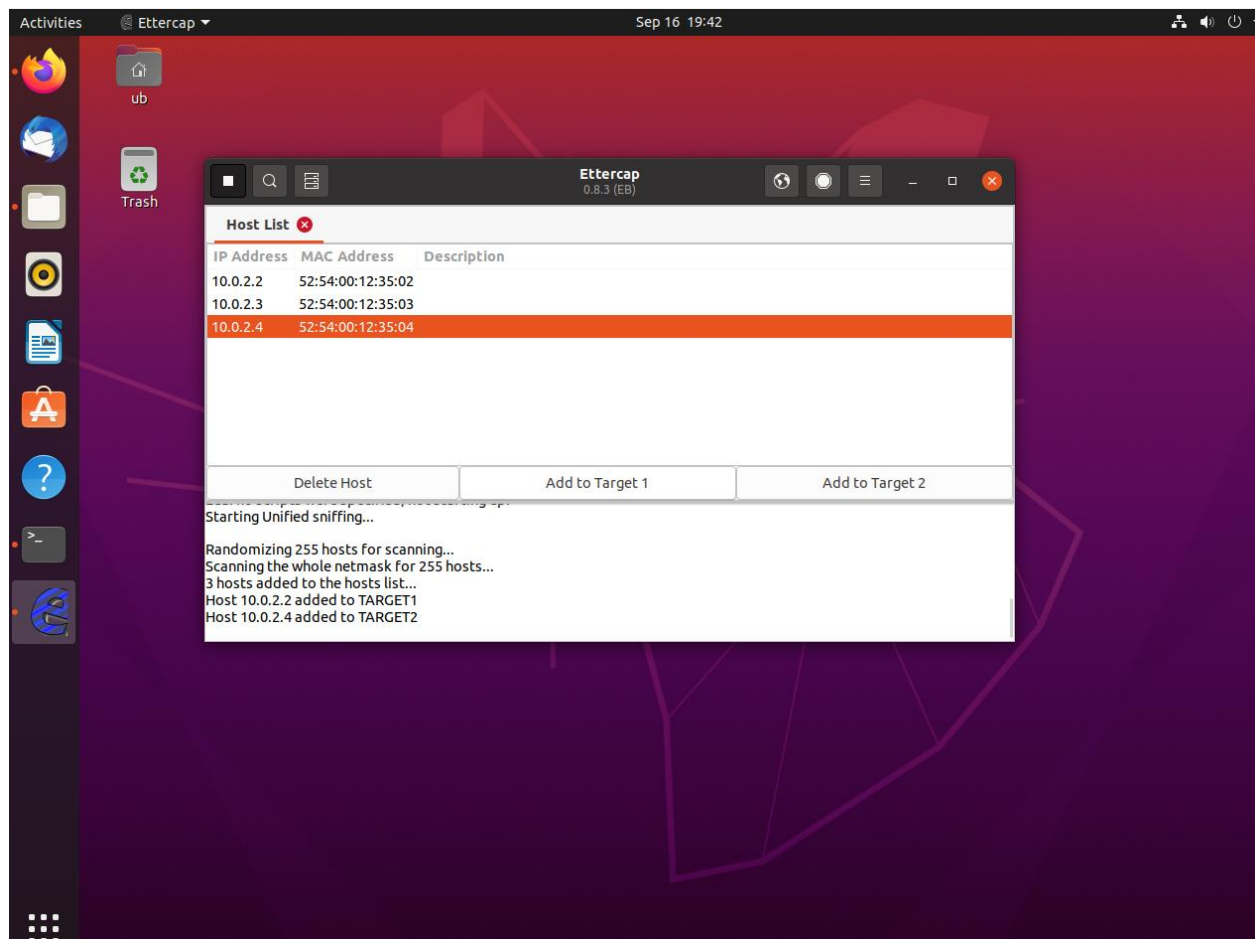
Next, Click the magnifying glass on the top left to scan the sub-network for hosts connected to the network. After it finishes click on the three bars next to the magnifying glass to open the window to show you list of hosts found on the network.



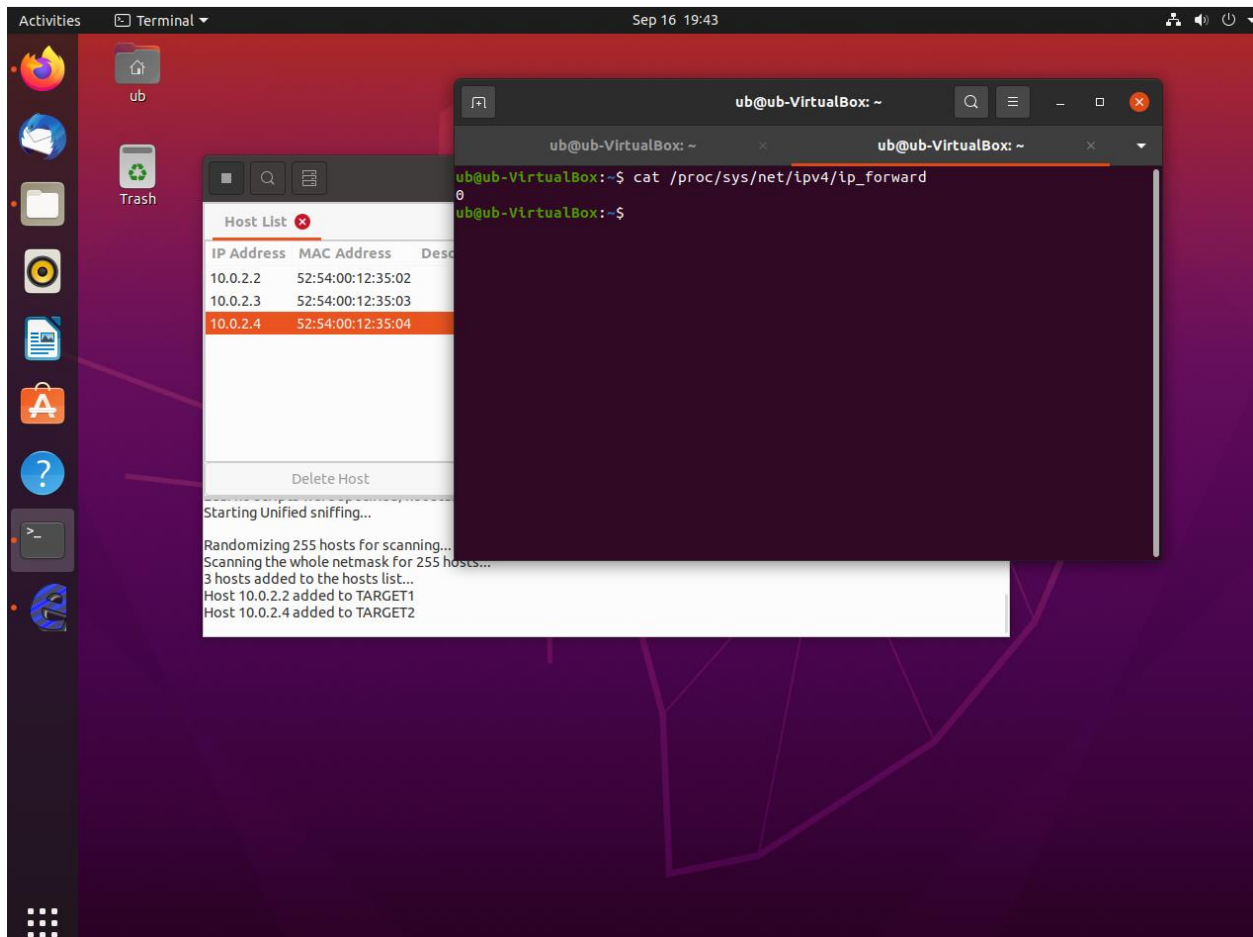
This is the list of hosts found on the network.



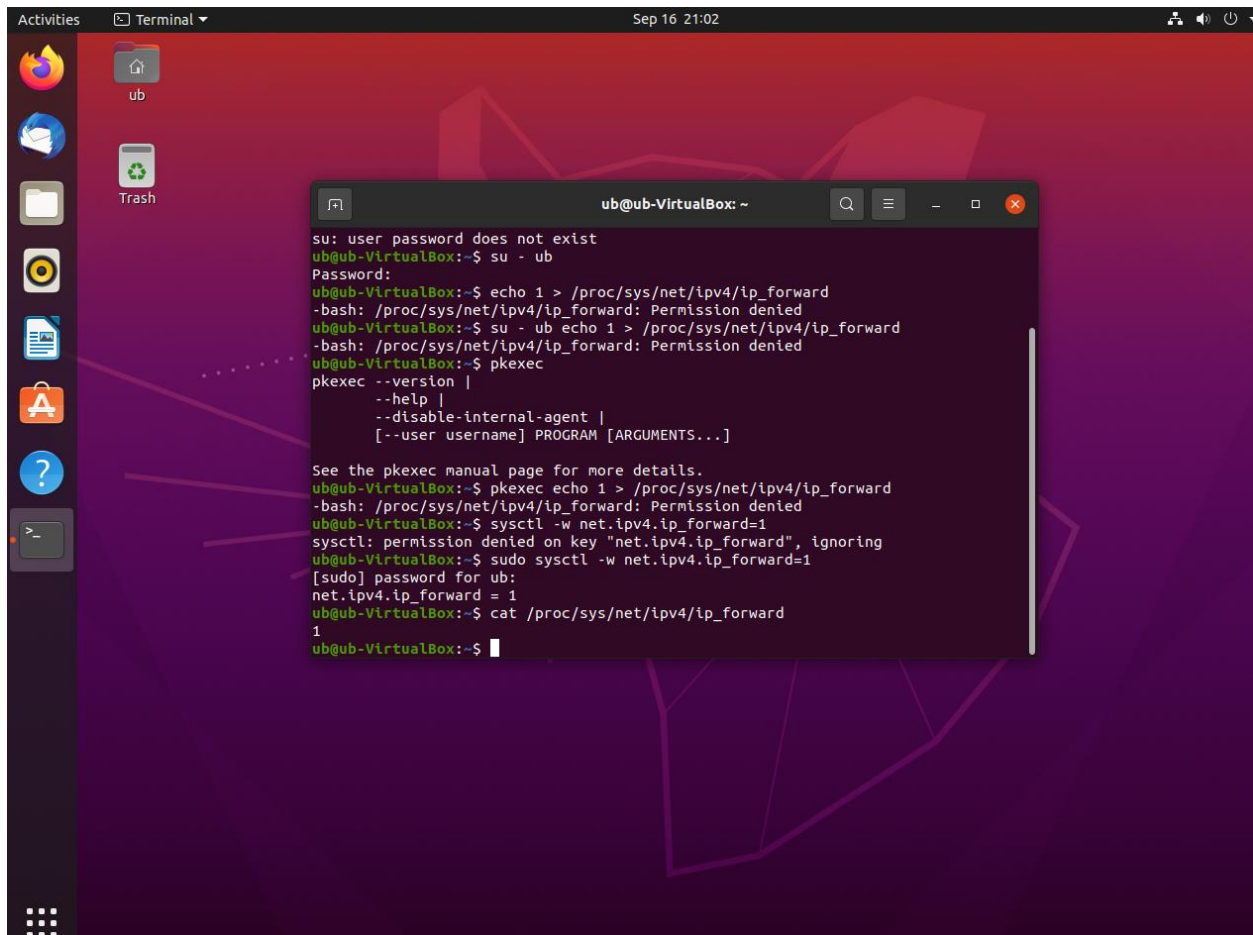
Next, click on the IP address for the host that was the Windows VM which was 10.0.2.2 and click “Add to Target 1” which is the hosts that Ettercap collects traffic from.



Next, click on the IP address for the host that was the Metasploitable VM which was 10.0.2.4 and click “Add to Target 2” which is the hosts that Ettercap sends the intercepted trafficto.



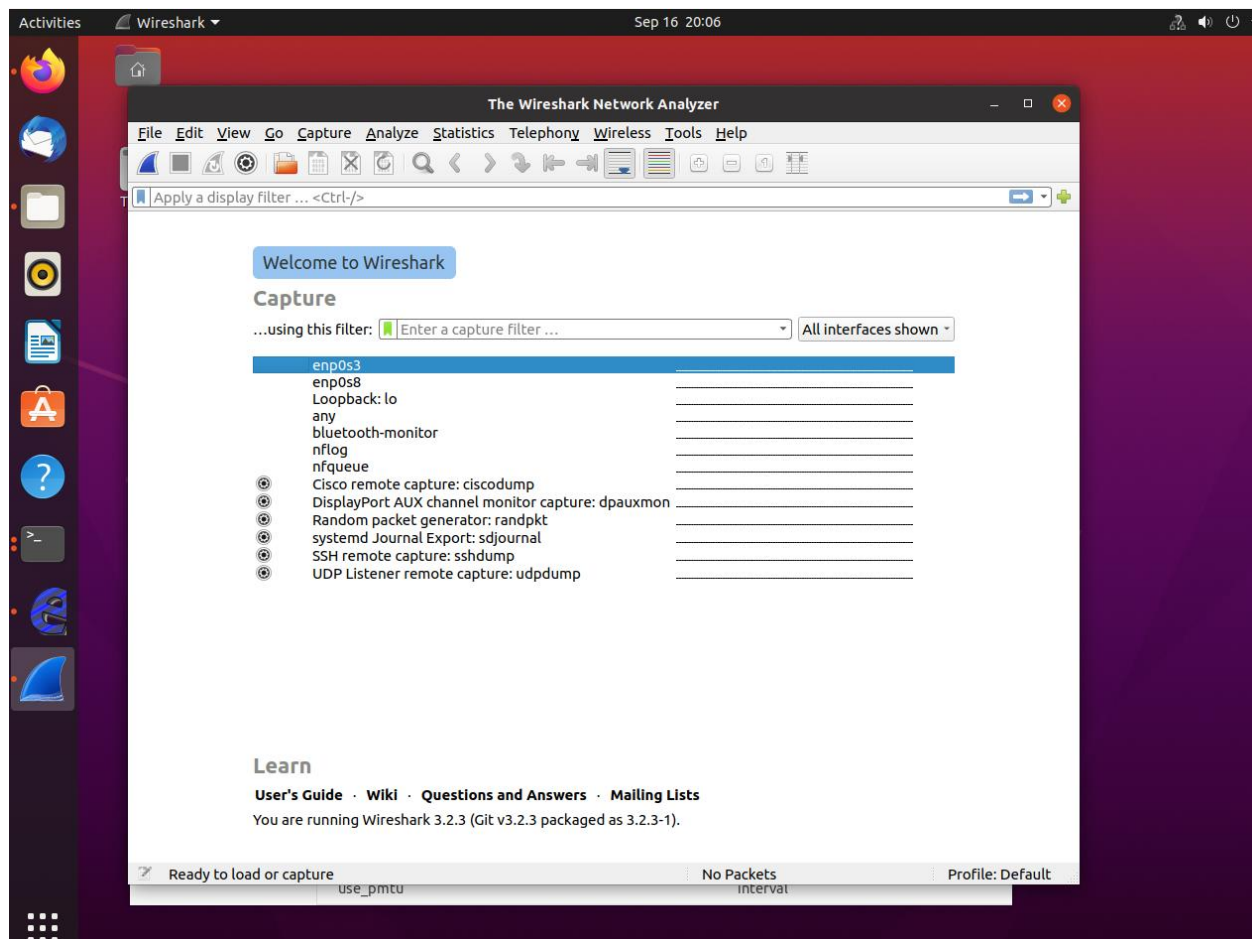
Next open a new Terminal window “cat /proc/sys/net/ipv4/ip_forward” the default value is 0. To capture network traffic the value needs to be changed to 1.



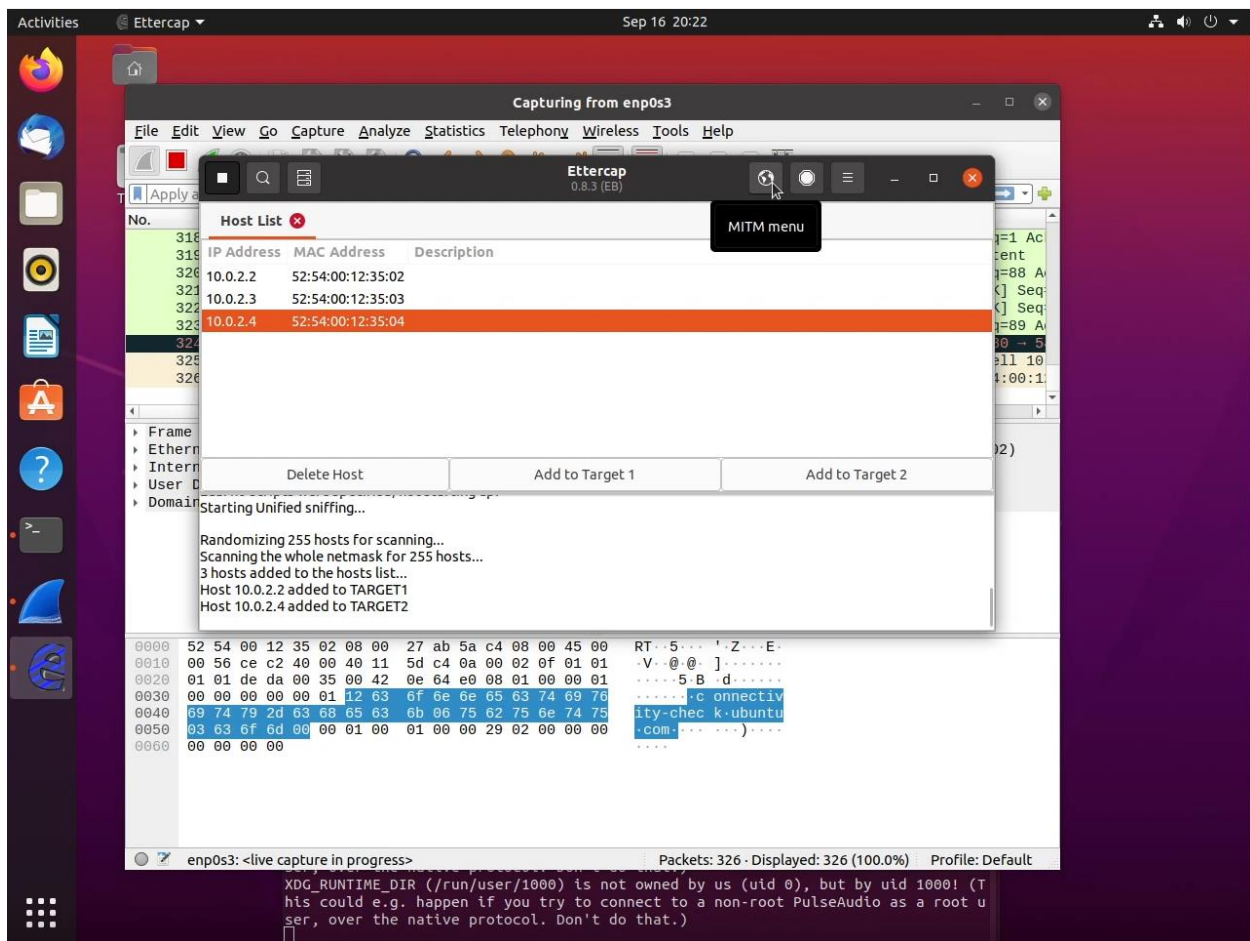
```
ub@ub-VirtualBox: ~
su: user password does not exist
ub@ub-VirtualBox:~$ su - ub
Password:
ub@ub-VirtualBox:~$ echo 1 > /proc/sys/net/ipv4/ip_forward
-bash: /proc/sys/net/ipv4/ip_forward: Permission denied
ub@ub-VirtualBox:~$ su - ub echo 1 > /proc/sys/net/ipv4/ip_forward
-bash: /proc/sys/net/ipv4/ip_forward: Permission denied
ub@ub-VirtualBox:~$ pkexec
pkexec --version |
--help |
--disable-internal-agent |
[--user username] PROGRAM [ARGUMENTS...]

See the pkexec manual page for more details.
ub@ub-VirtualBox:~$ pkexec echo 1 > /proc/sys/net/ipv4/ip_forward
-bash: /proc/sys/net/ipv4/ip_forward: Permission denied
ub@ub-VirtualBox:~$ sysctl -w net.ipv4.ip_forward=1
sysctl: permission denied on key "net.ipv4.ip_forward", ignoring
ub@ub-VirtualBox:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for ub:
net.ipv4.ip_forward = 1
ub@ub-VirtualBox:~$ cat /proc/sys/net/ipv4/ip_forward
1
ub@ub-VirtualBox:~$
```

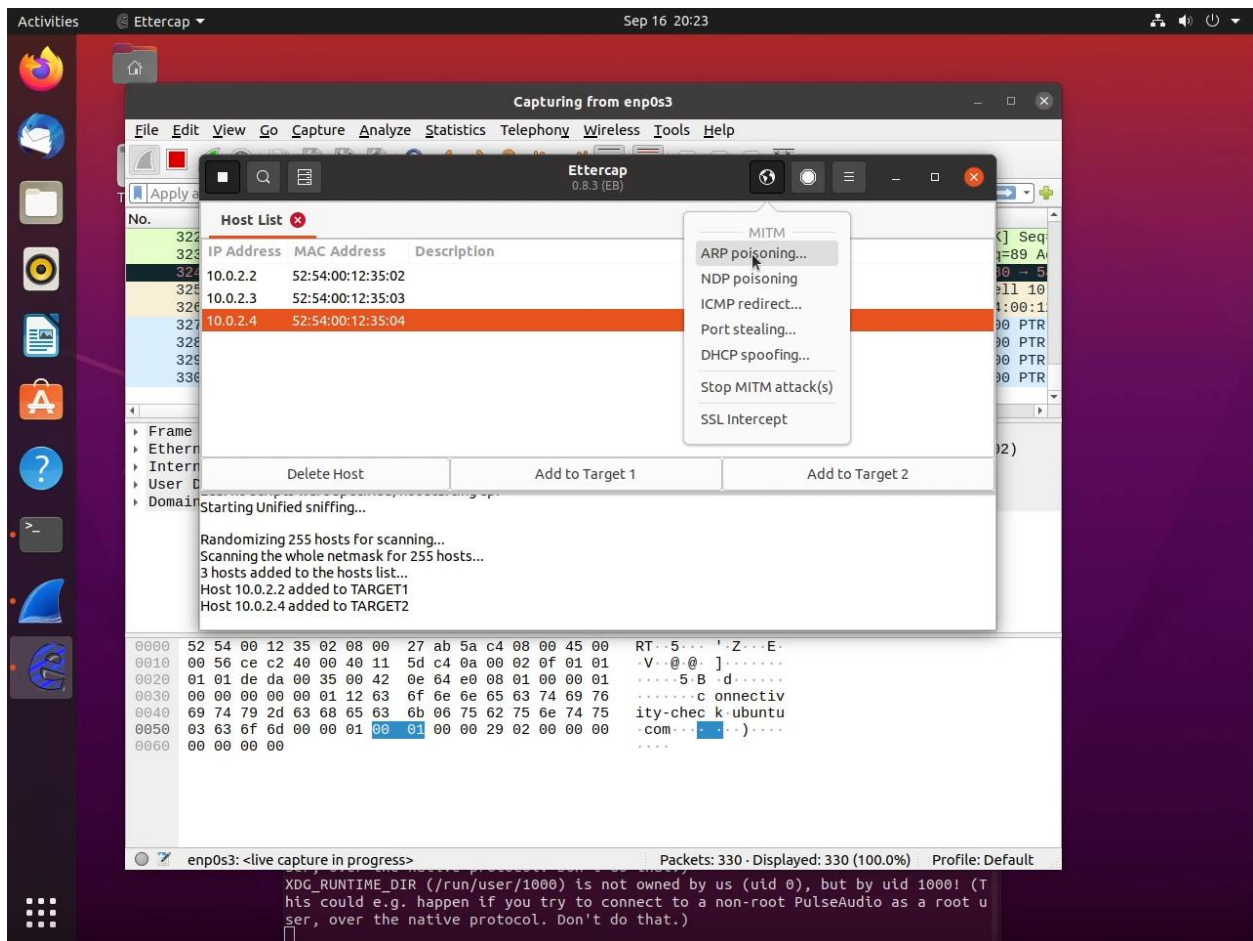
There are many ways to change that value one way is typing “echo 1 > cat /proc/sys/net/ipv4/ip_forward” but you may not have permission to change that file because of the lack of executable permissions. In that case enter “sudo sysctl -w.net.ipv4.ip_foward=1” this gives the user elevated permissions to make that change. By running “cat /proc/sys/net/ipv4/ip_forward” you can see the 0 is now a 1.



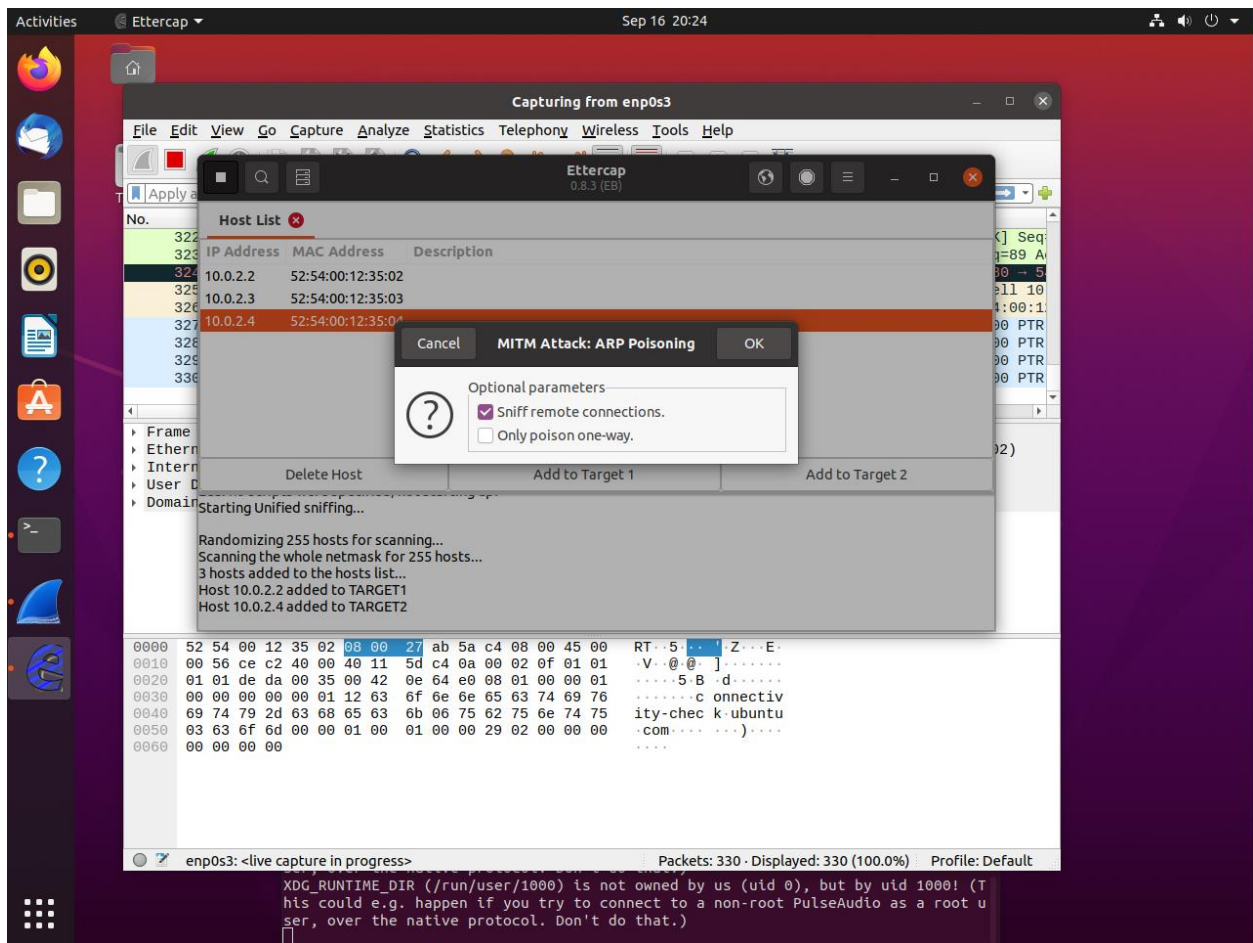
Next open Wireshark so that network traffic can be captured. Then click on “enp0s3” to connect to the right network.



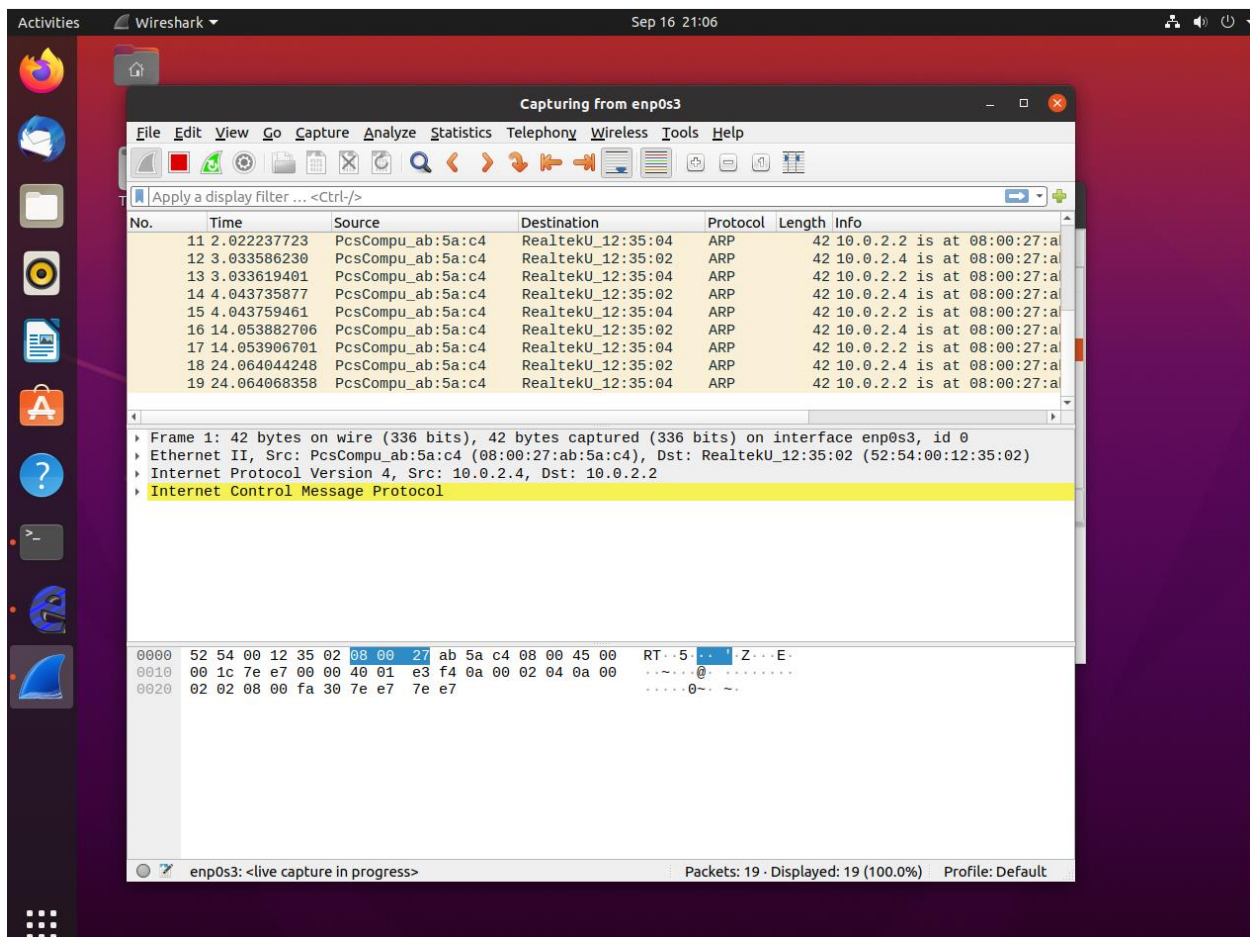
Next, go back to Ettercap and click on the globe or "MITM menu" button.



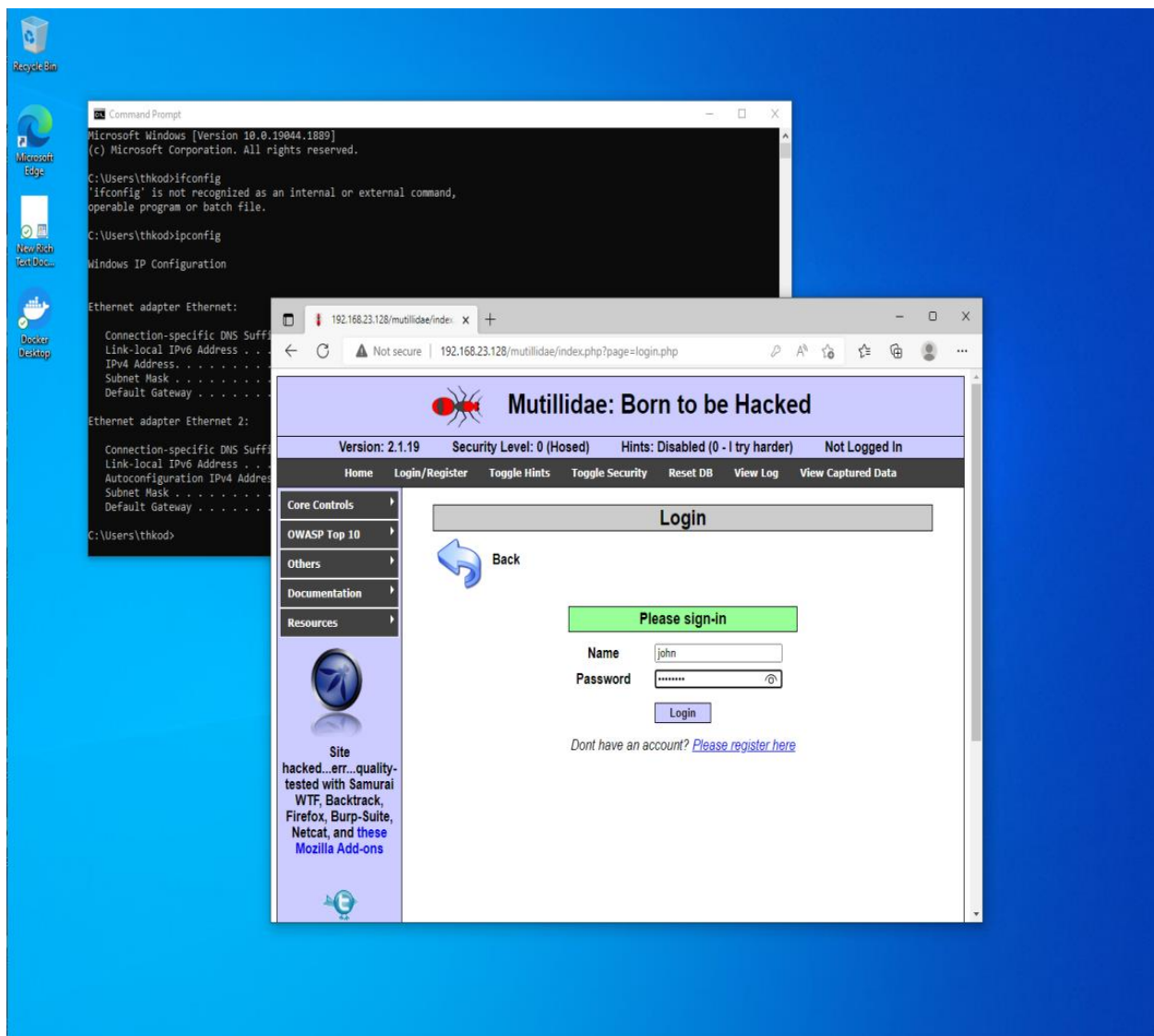
Next, click on "ARP poisoning".



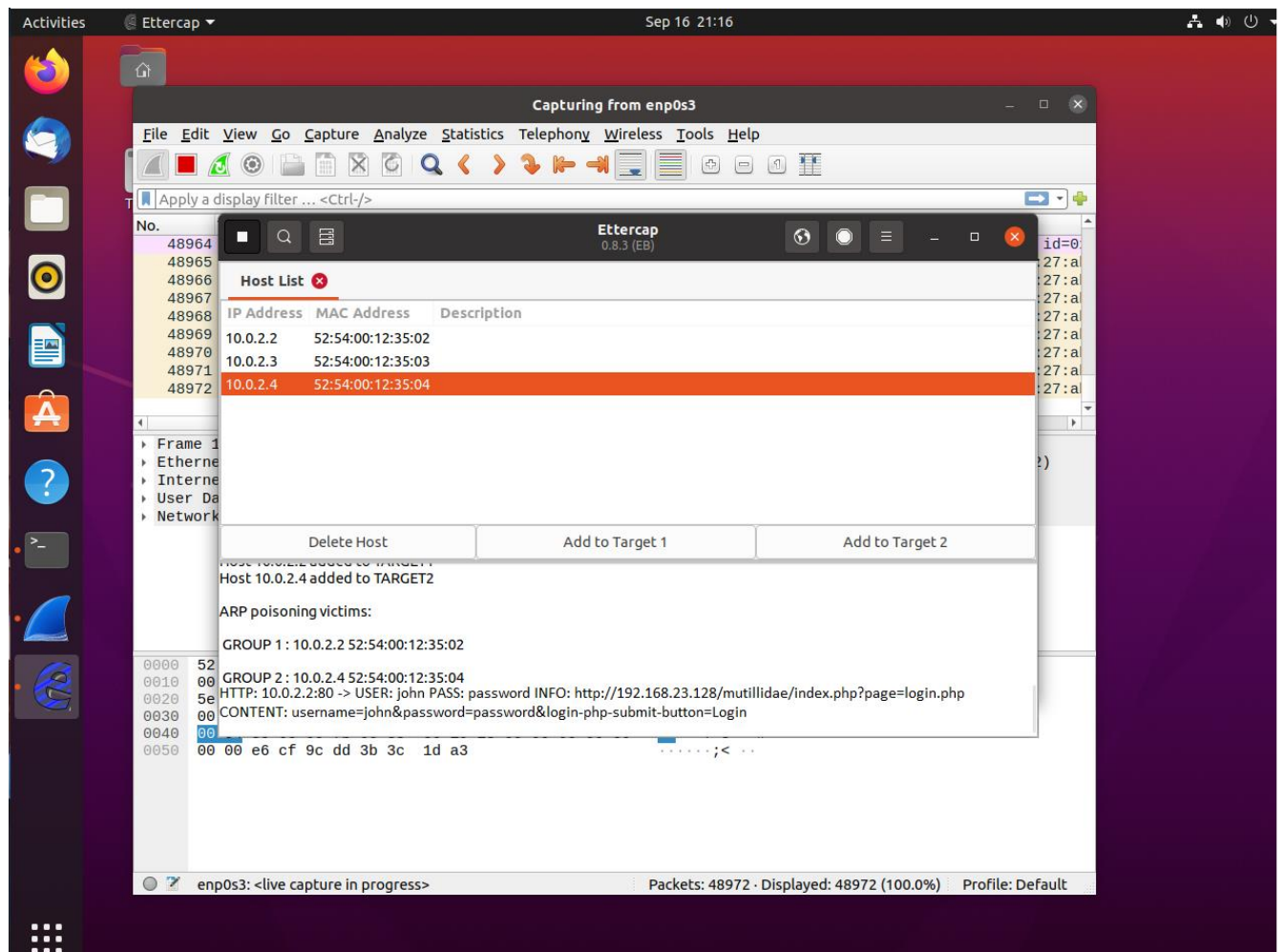
Next, make sure “sniff remote connections.” Is the only box selected and press “OK”.



By going back to wireshark we can see that ARP data is being sent across the network to confuse the connected IP address. This confuses the ARP caches of the different machines on the network.



Next, go back to the Windows VM and in the login page enter “john” as Name and “password” as password. Then press Login or press enter on the keyboard.



Next go back to the Ubuntu VM and in the Ettercap window we can see the data that was sent from the Windows VM to the Metasploitable VM. The username john and the password password were sent across the network and captured by the Ubuntu VM. We now have the username and password of the user who is using the Windows VM.

f. Analysis of your experiment:

I was successfully able to view the username and passwords of the users who enter data that passes through the network. With this data I can login as john, and I also have the user's password that I can try on this website to gain more info and on other websites to gain access to the user's other accounts.

g. Discussion and conclusion:

Ettercap is a good tool to use when securing a network by having it run on the sub-network and having the intended devices find it and block it from the network. Because Ettercap is free anyone can download and use it. This means an attacker needs a remote connection to a device on a sub-network, a downloadable script, and Network Analyzer like Wireshark to run the attack or they can use the CLI to run the attack themselves to collect the information.