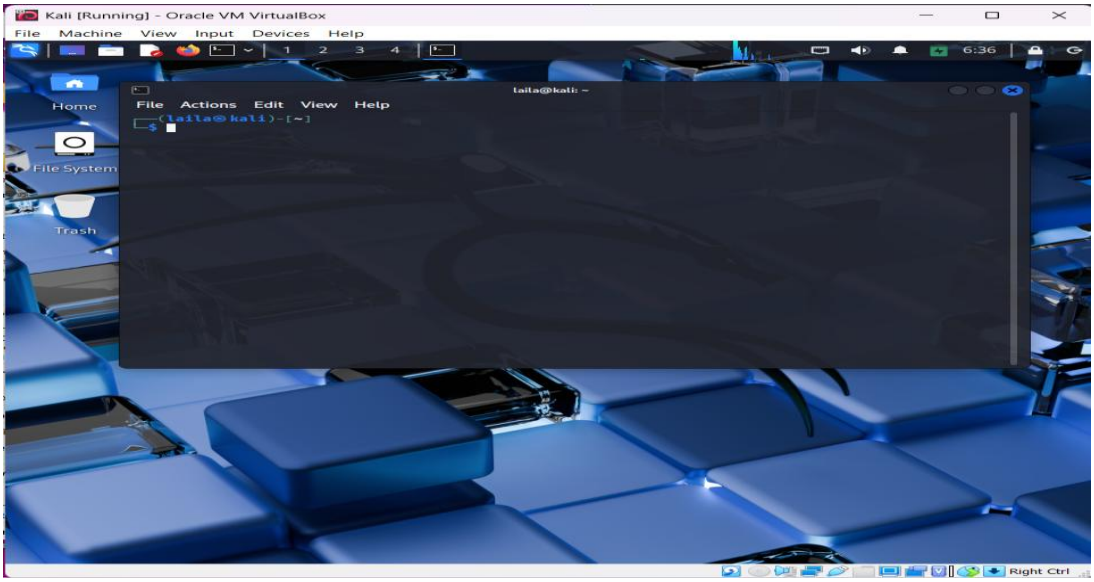
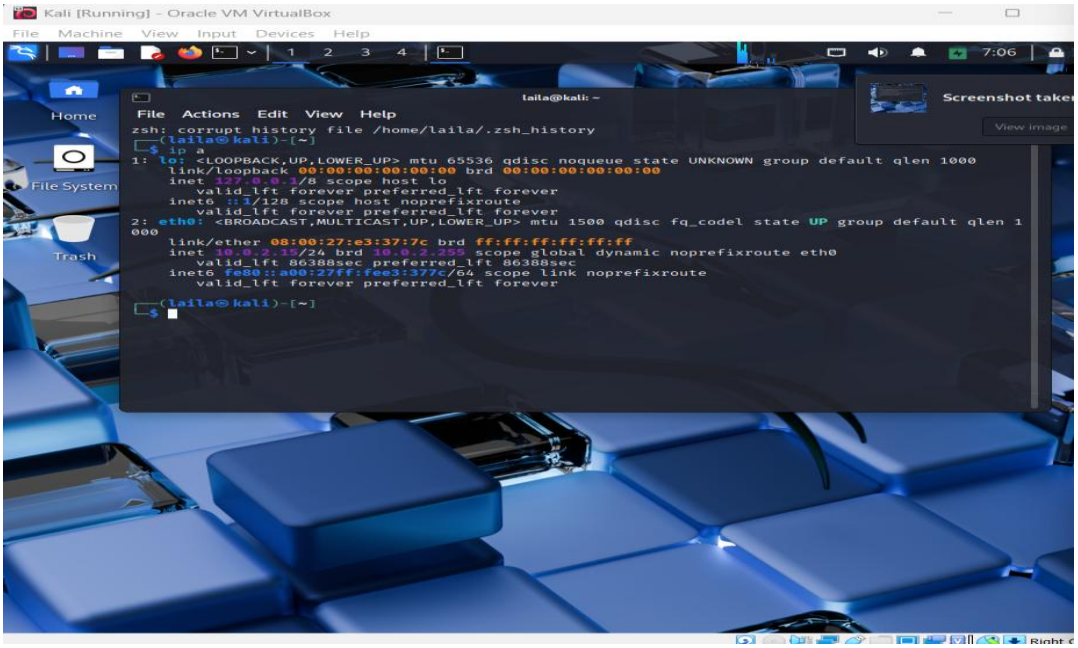
CyberSecurity Project

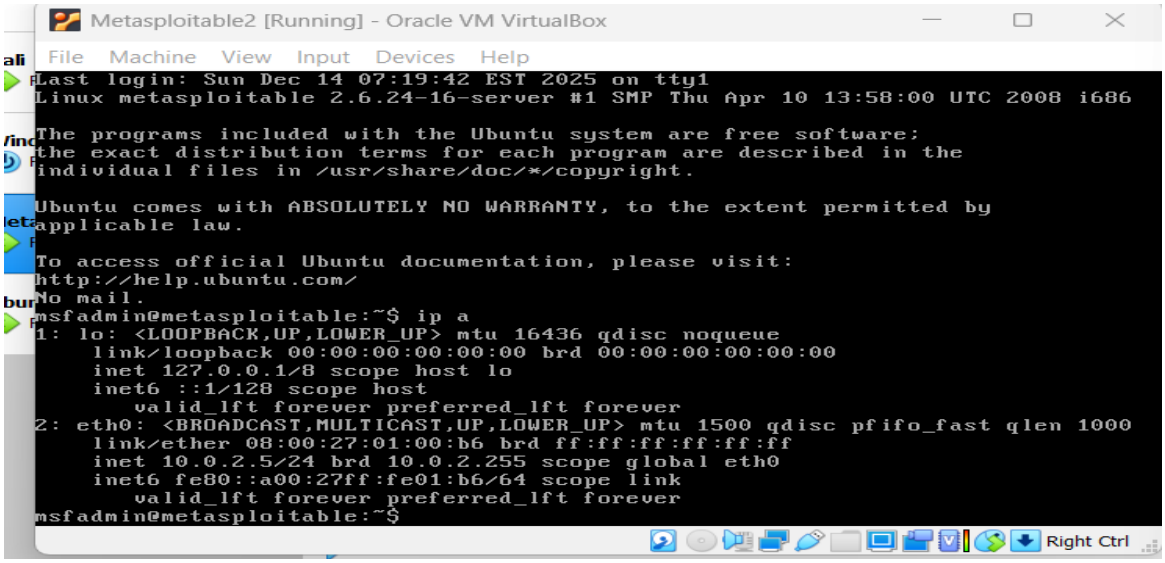
1. Network Setup & Discovery:



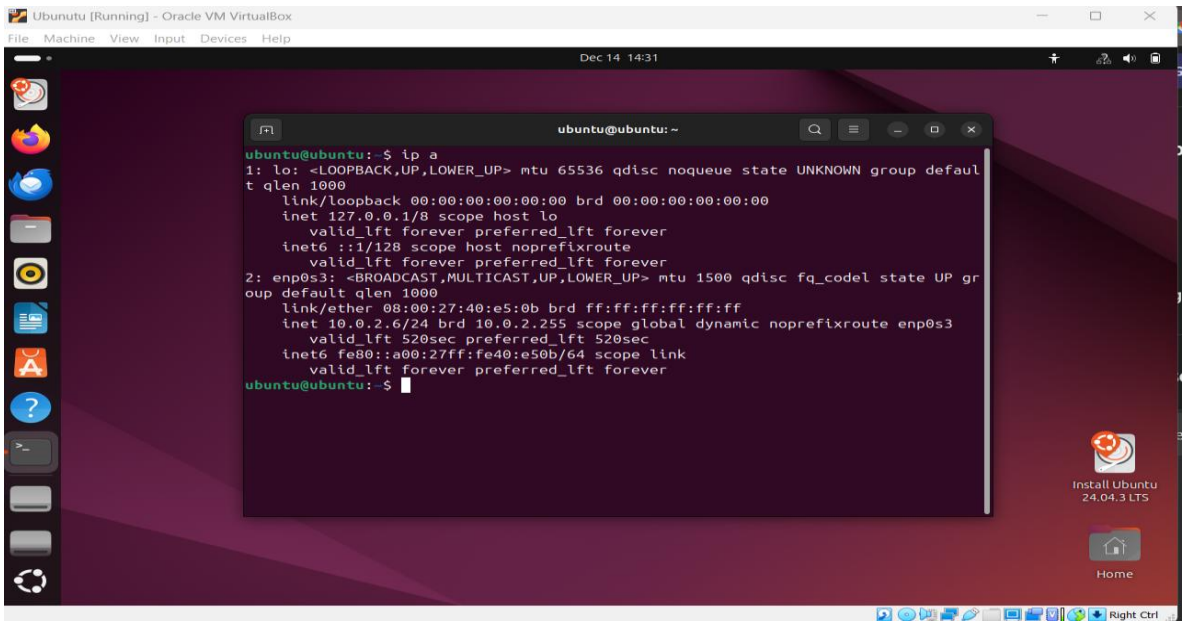
This is kali's terminal in each I will be writing commands to discover the networks , ips etc..



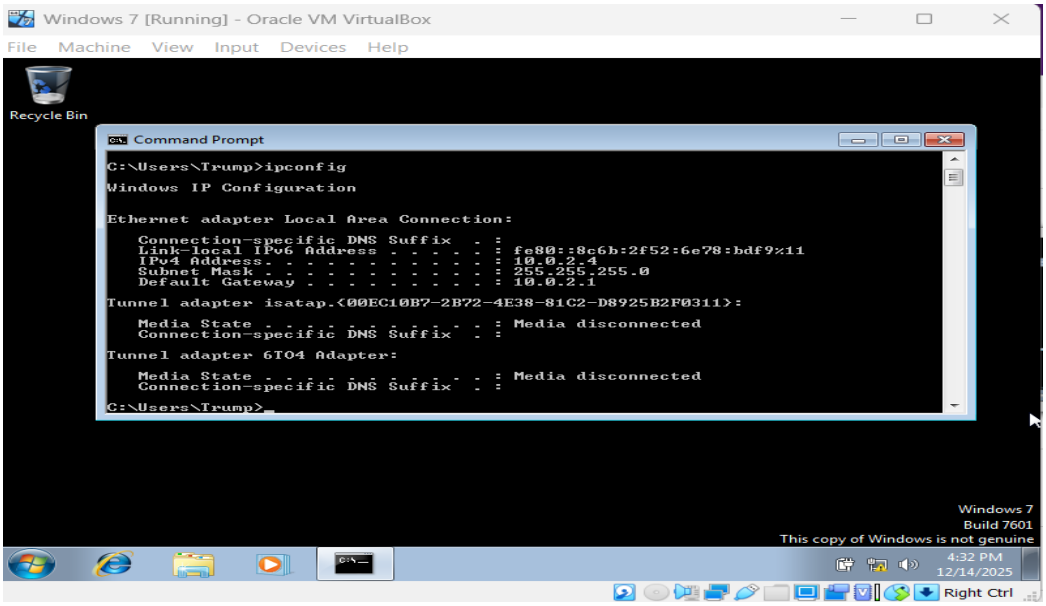
I configured kali's ip by changing the network in the setting (to NAT network that different vms takes different ips from the DHCP) so kali's ip is 10.0.2.15/24



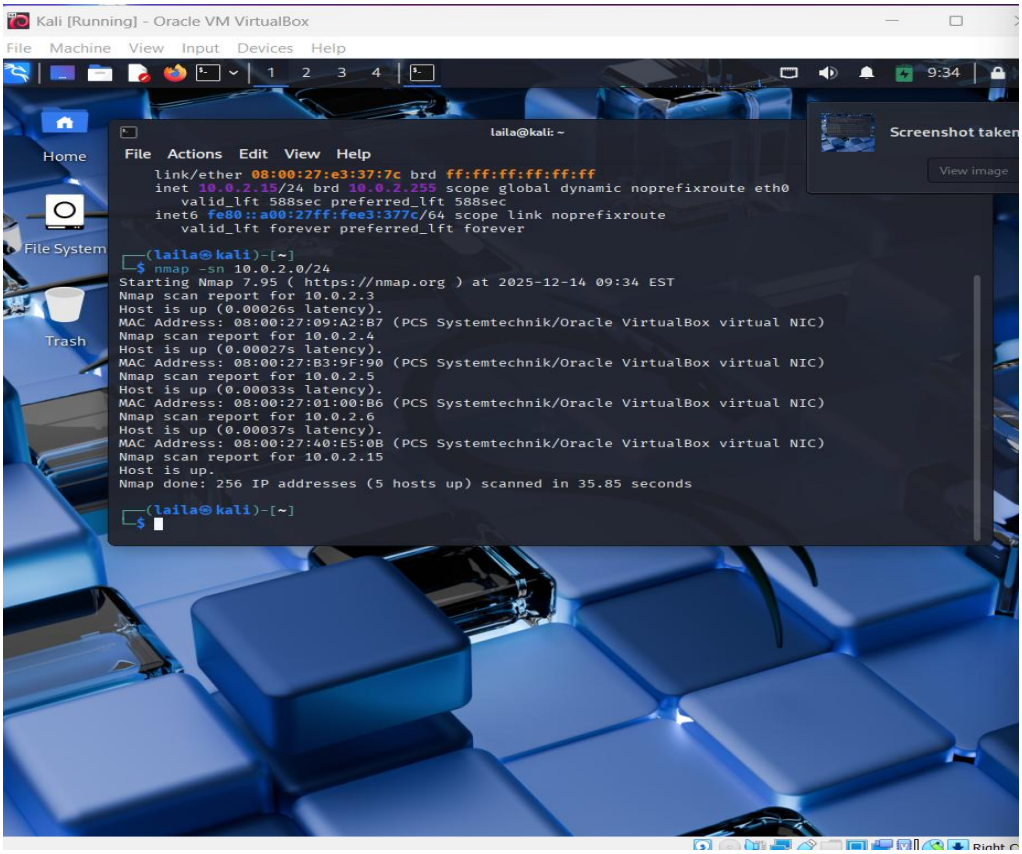
Same goes for metasploitable2/ubuntu/windows (it took its ip address from the DHCP) -> 10.0.2.5/24



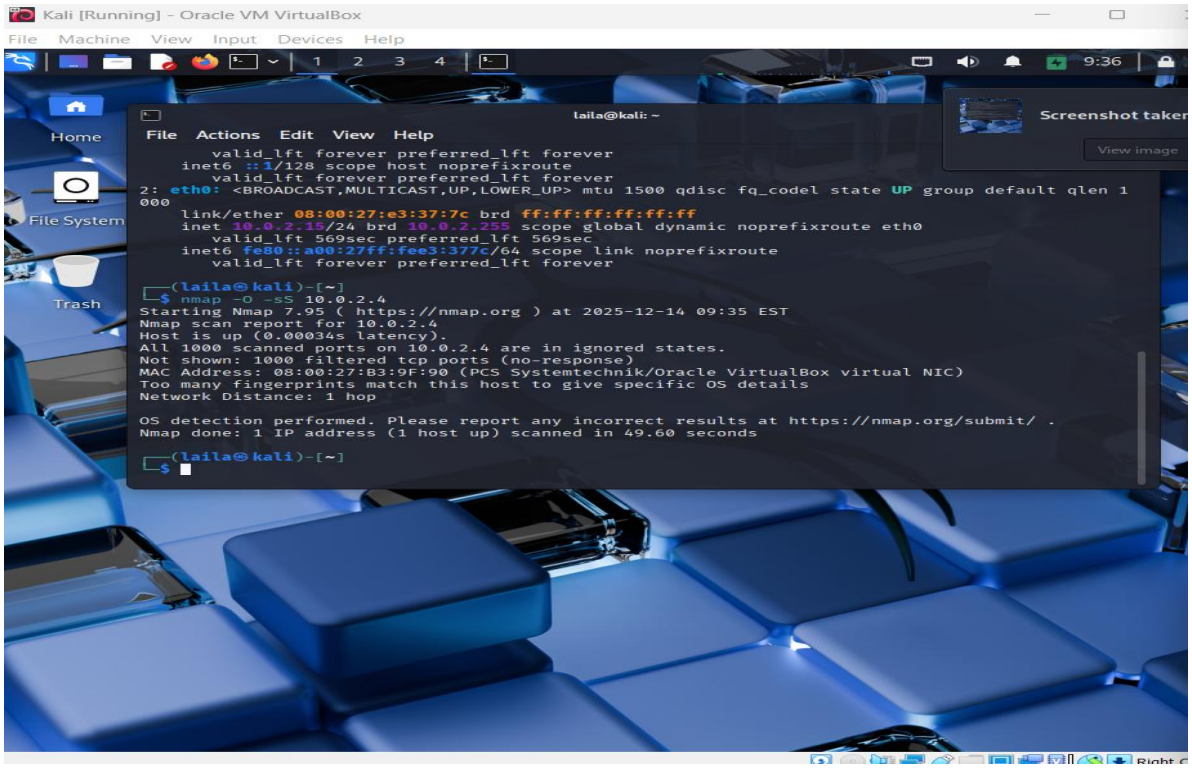
Ubuntu's ip is 10.0.2.6/24



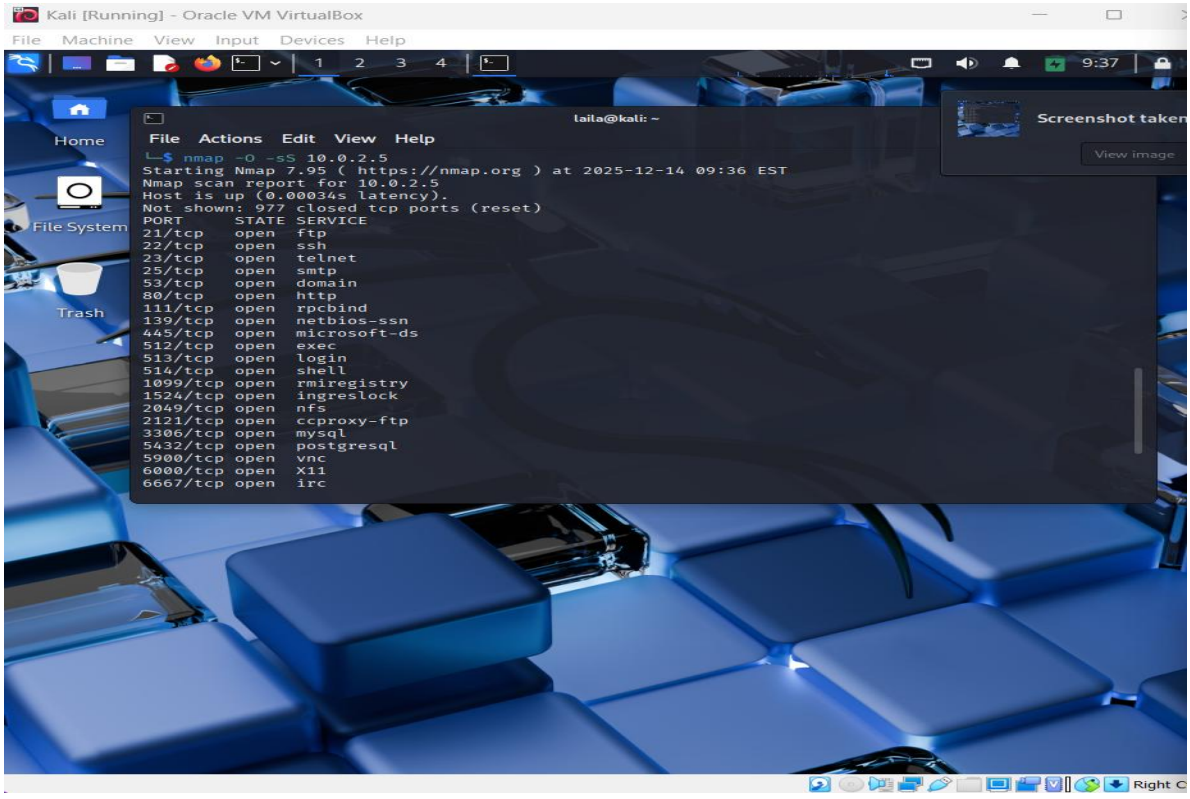
Windows ip is 10.0.2.4



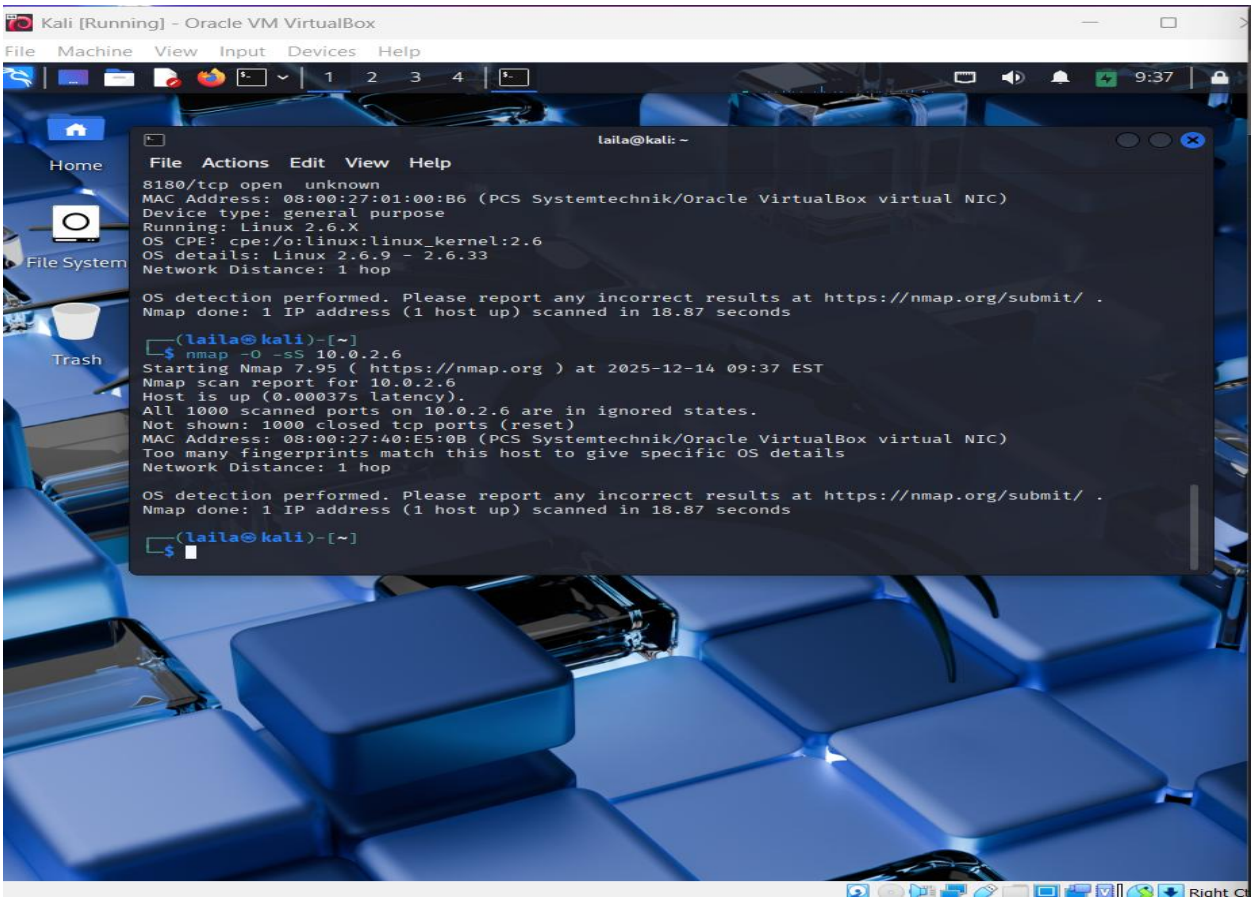
From kali I used nmap to discover which hosts are up and as we can see ubuntu , windows , metasploitable2 and another hot is up



Then I used nmap -O to see what are the available ports and what the hot is operating (windows) -> they are all in ignored state



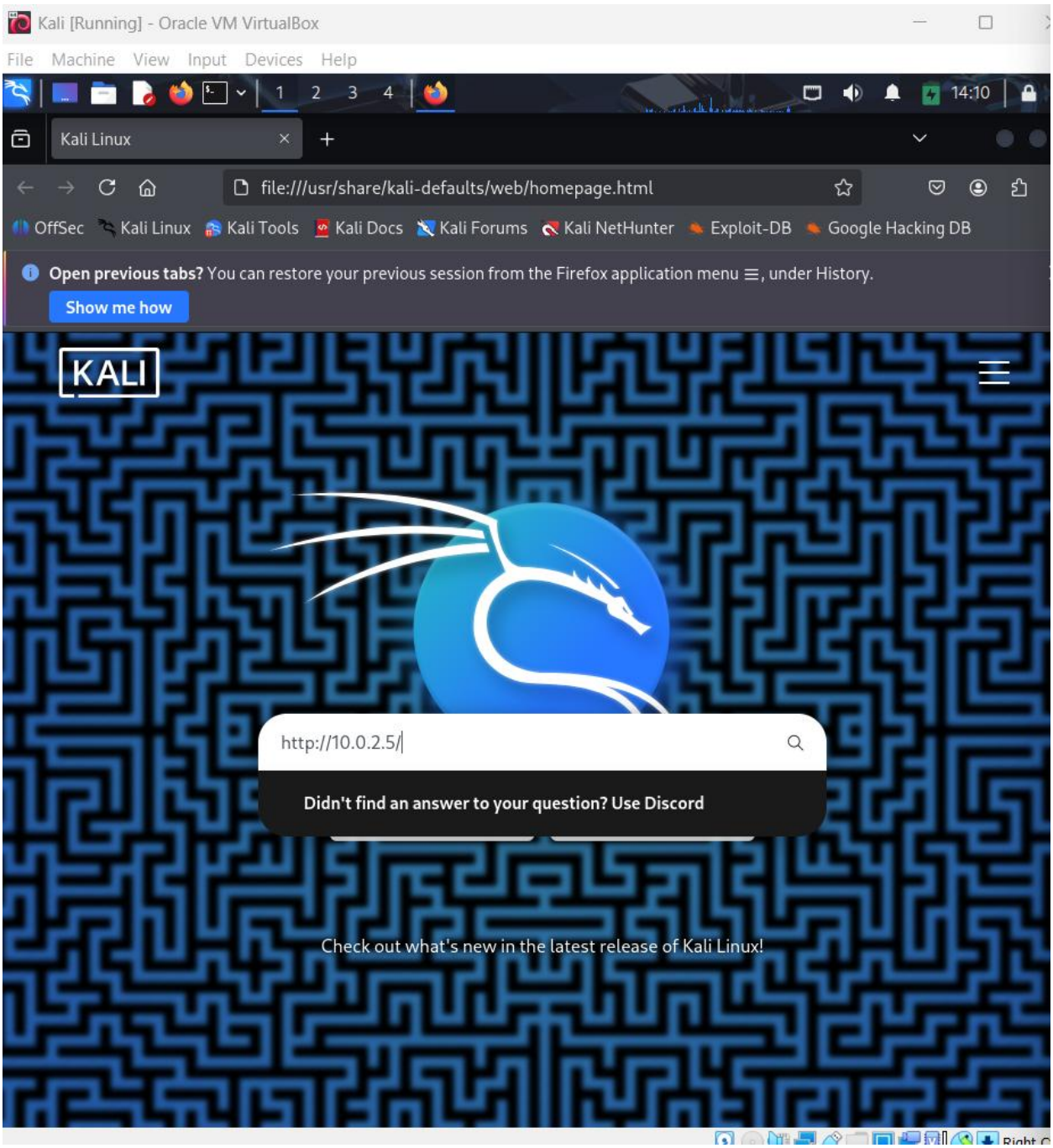
Then I used nmap -O to see what are the available ports and what the hot is operating (metasploitable2) ->tcp ports are opened like ftp ssh smtp etc..



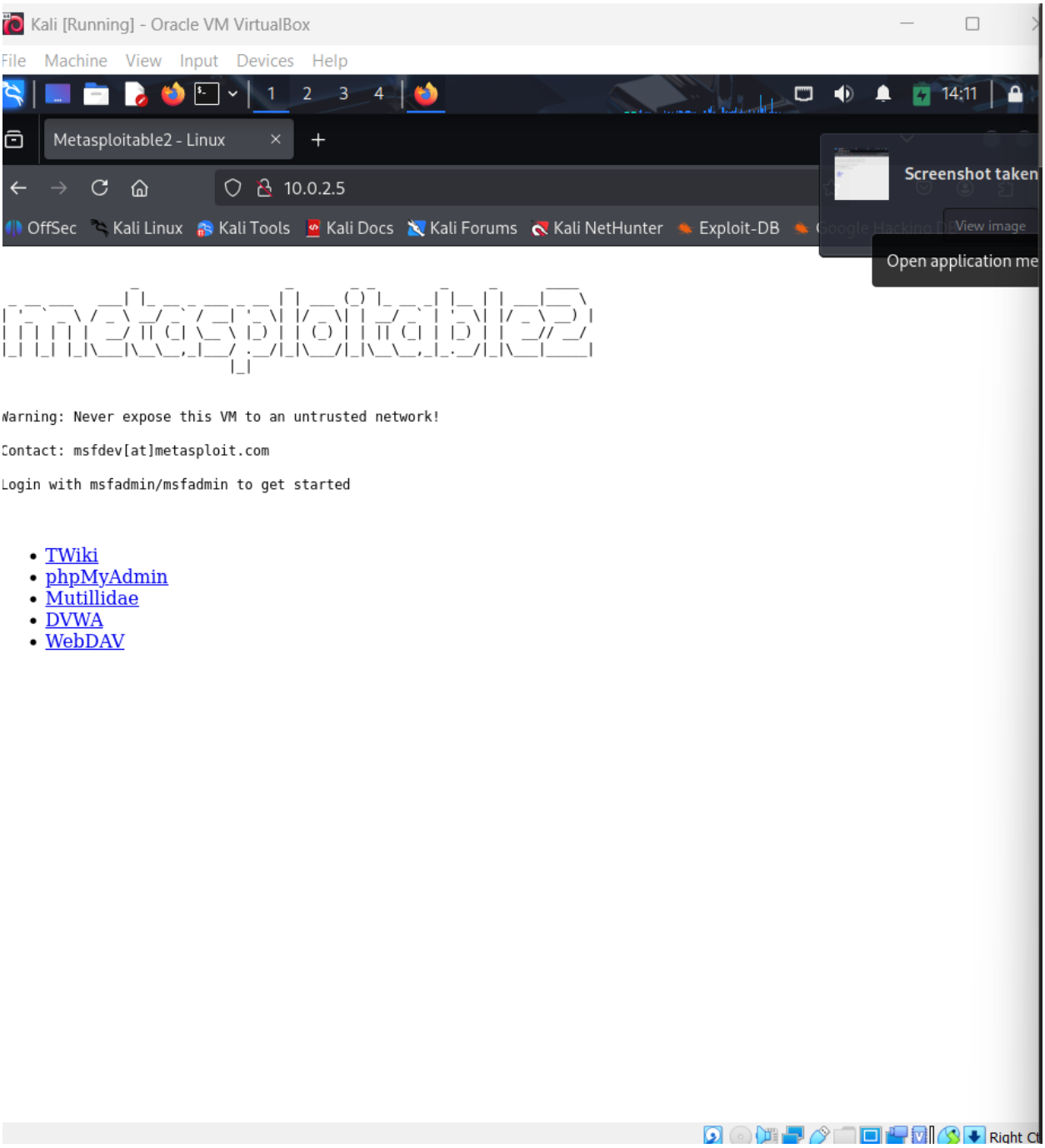
And for ubuntu -> the same as windows all of them are in ignored state

** all virtual machines (Kali Linux, Ubuntu, Windows, and Metasploitable) were configured on the same virtual network. The IP address of each machine was verified to ensure proper connectivity. Network discovery was performed from Kali Linux using Nmap to identify all active hosts on the subnet. Finally, operating system detection and port scanning were conducted for each host to enumerate open ports and running services.

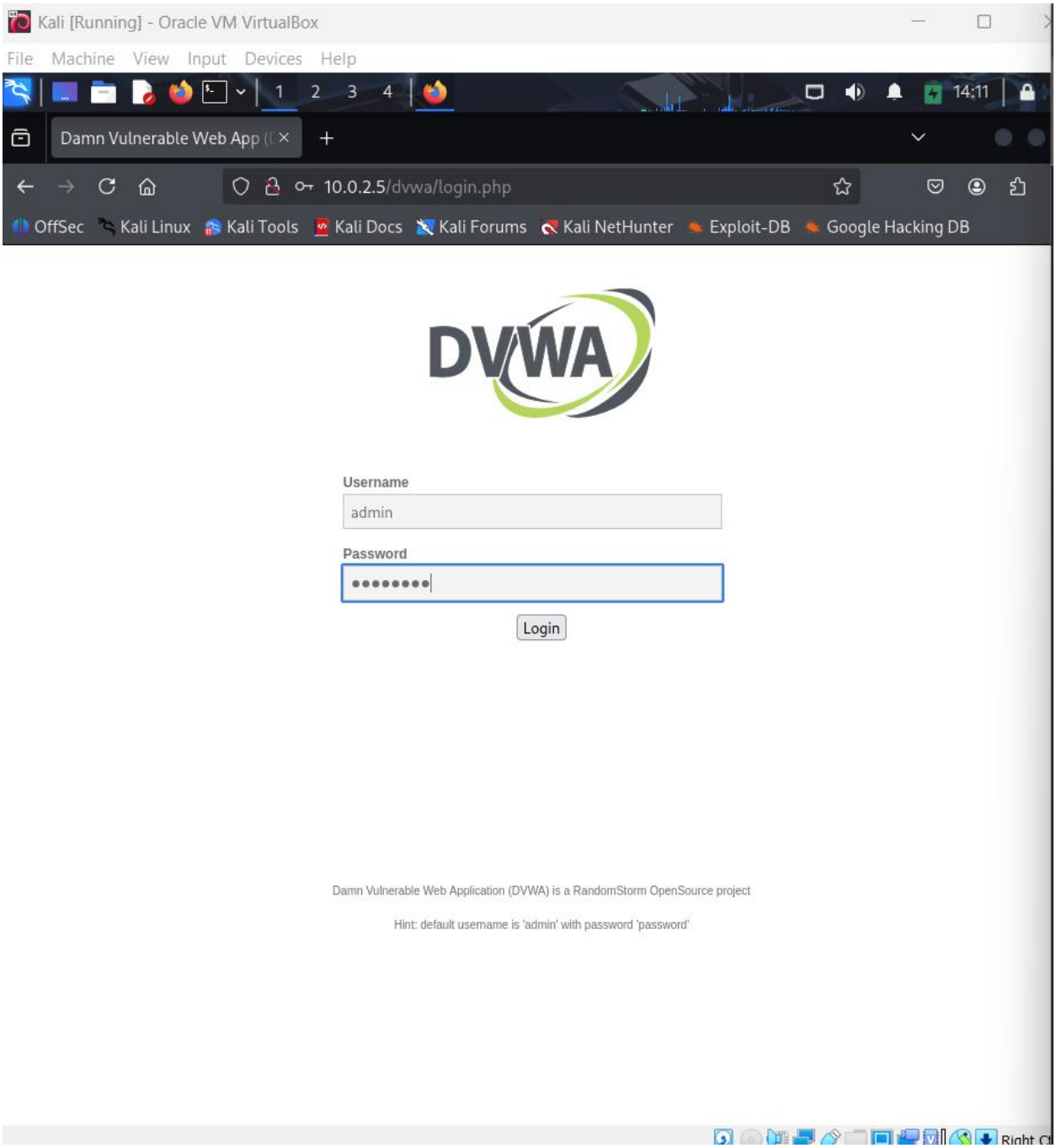
2. Man-in-the-middle attack:



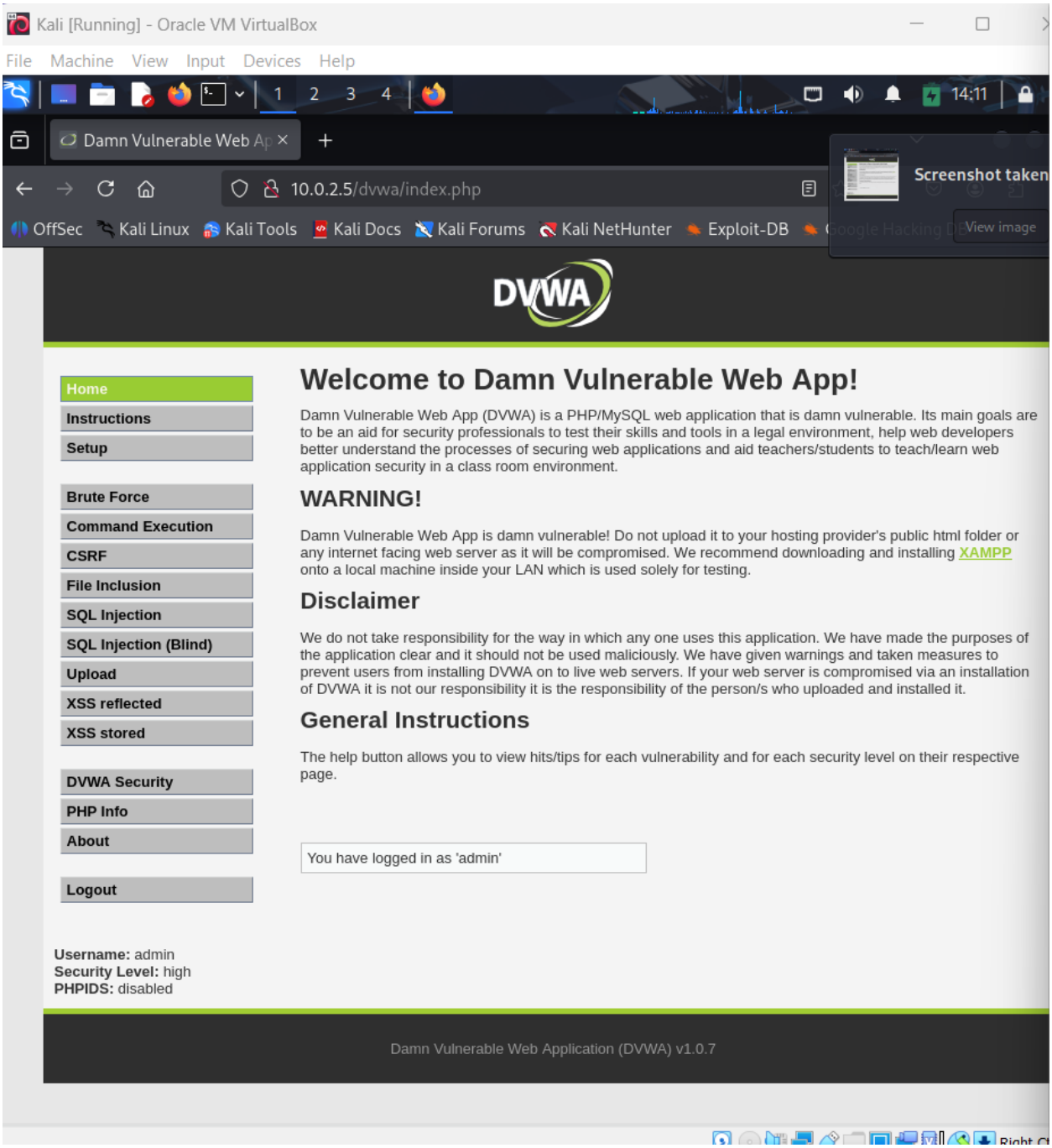
10.0.2.5 is the ip address of the metasploitable in which I will open the DVWA of firefox



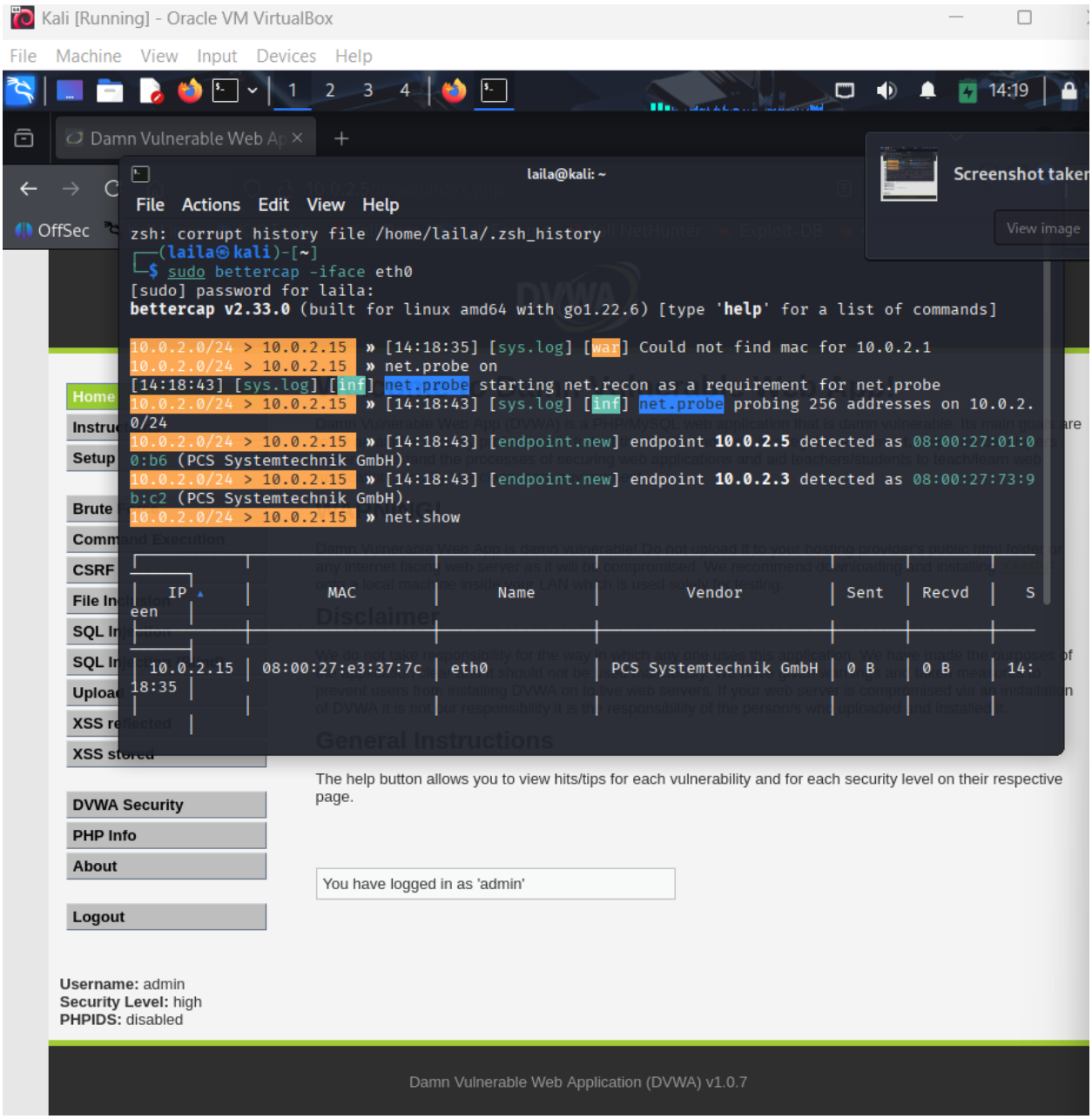
Opened metasploitable using it’s ip address



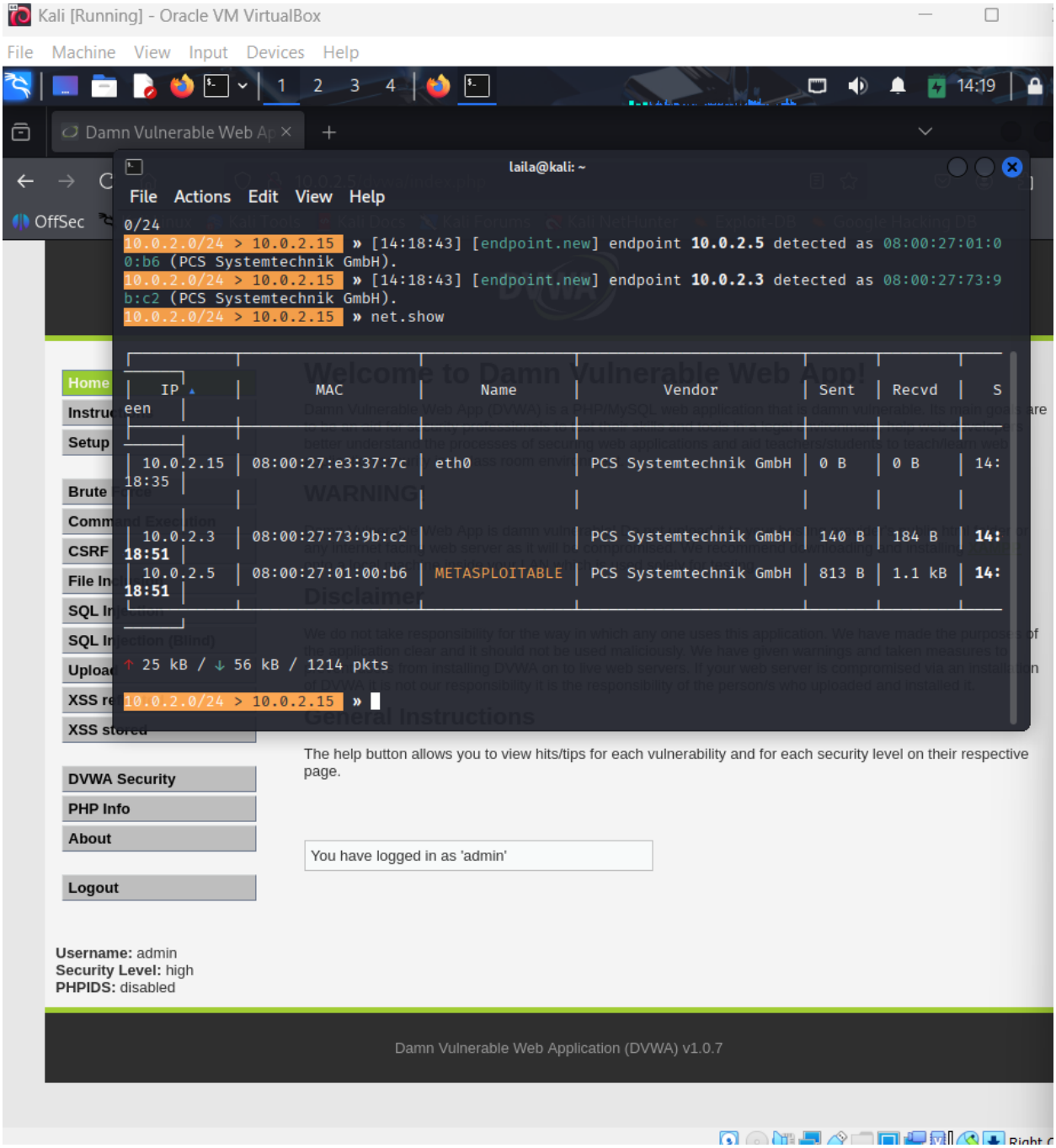
Logged in with username: admin and password: password



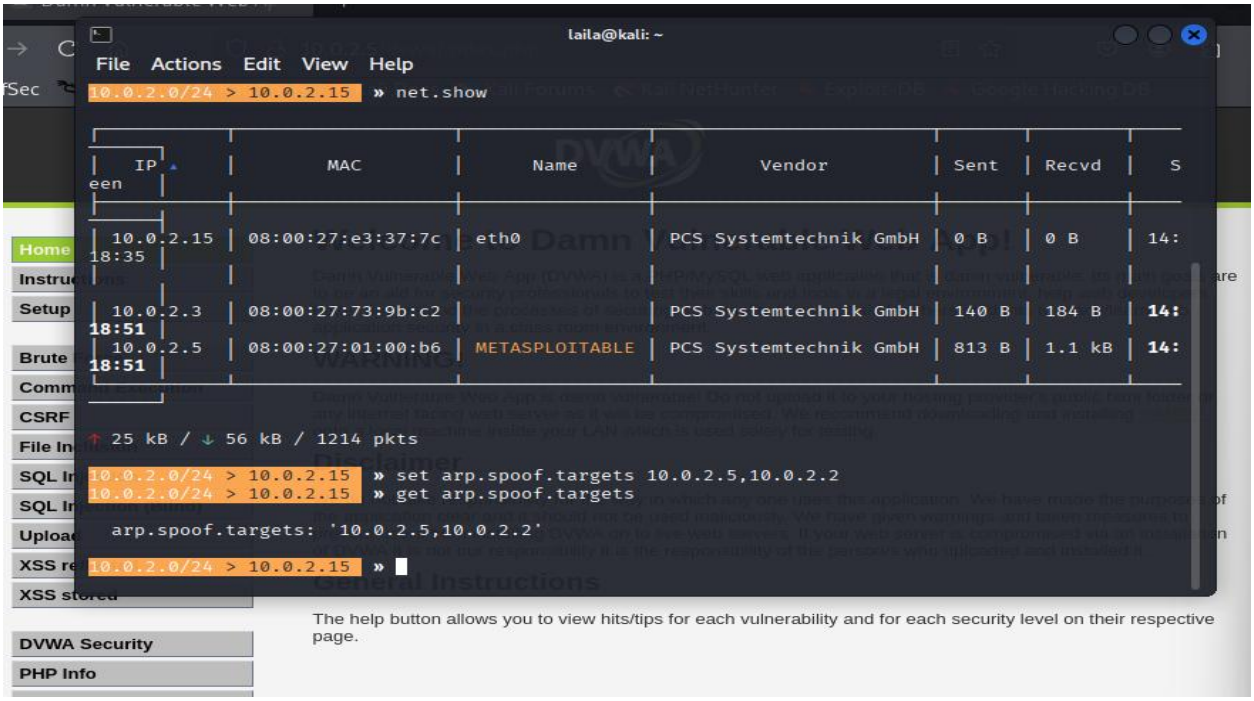
This is the html page that I will perform on it the attack



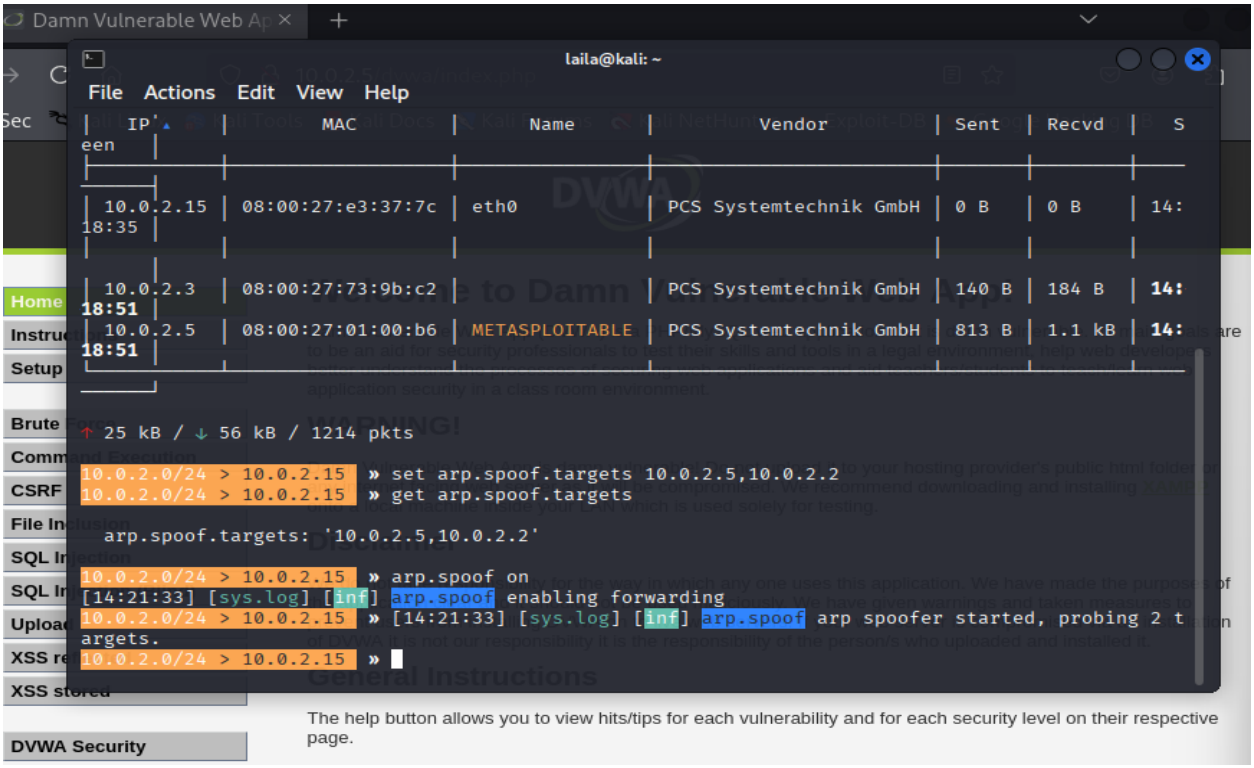
Started bettercap using sudo bettercap -iface eth0 then I did net.probe on this detects the endpoints (spoofing)



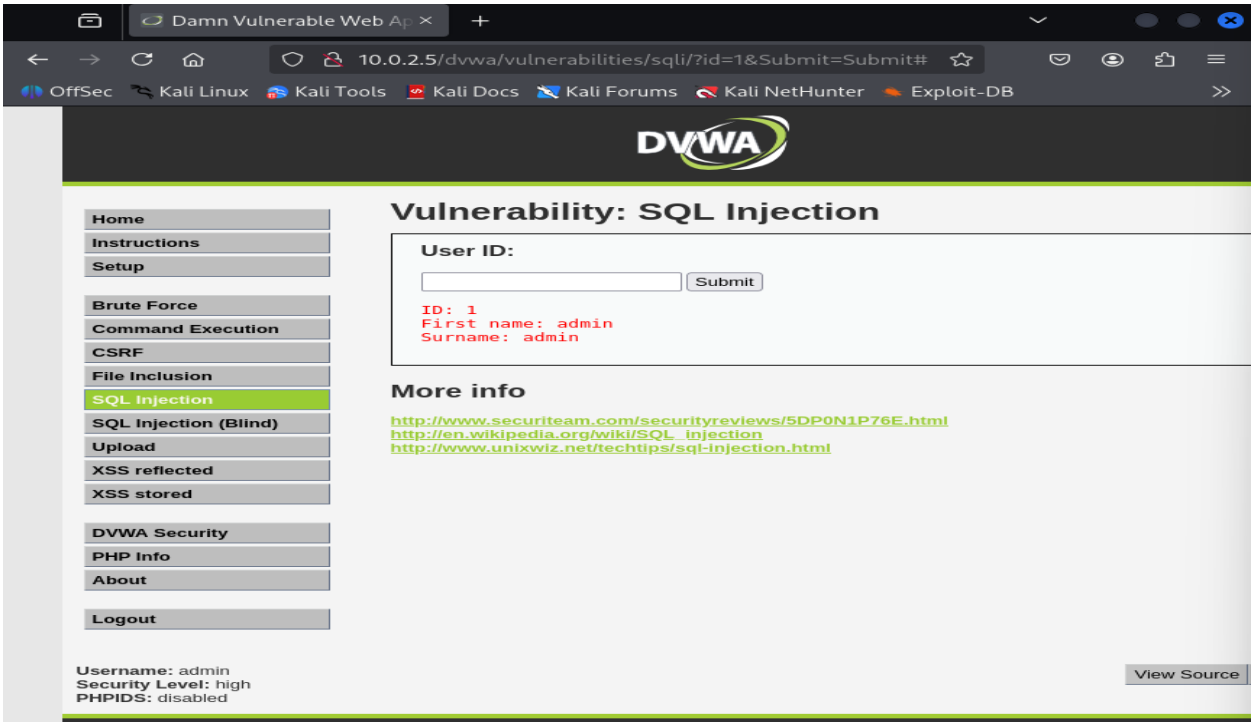
By the net.show I saw that there is the ip address of the metaspoitable which says that its open



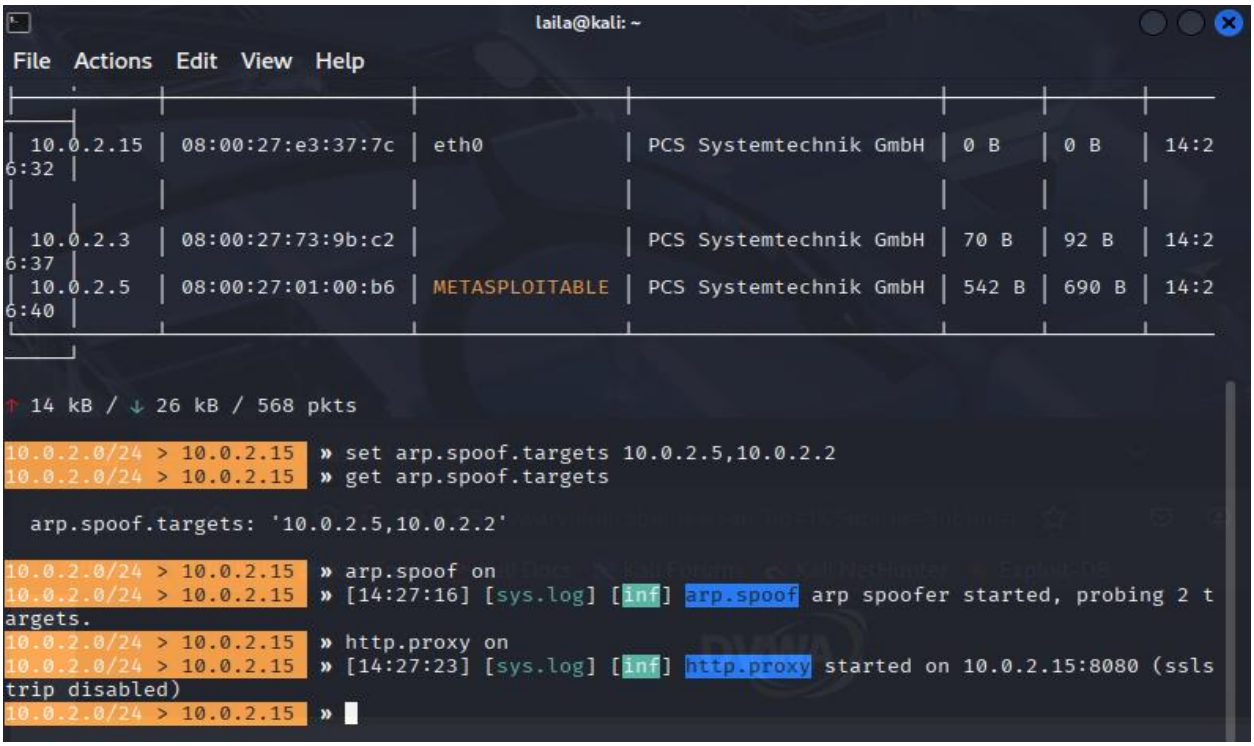
Then I set the arp target (in which I will attack) will be the metasploitable Ip address an it gateway which is 10.0.2.2 , and we spoofed it



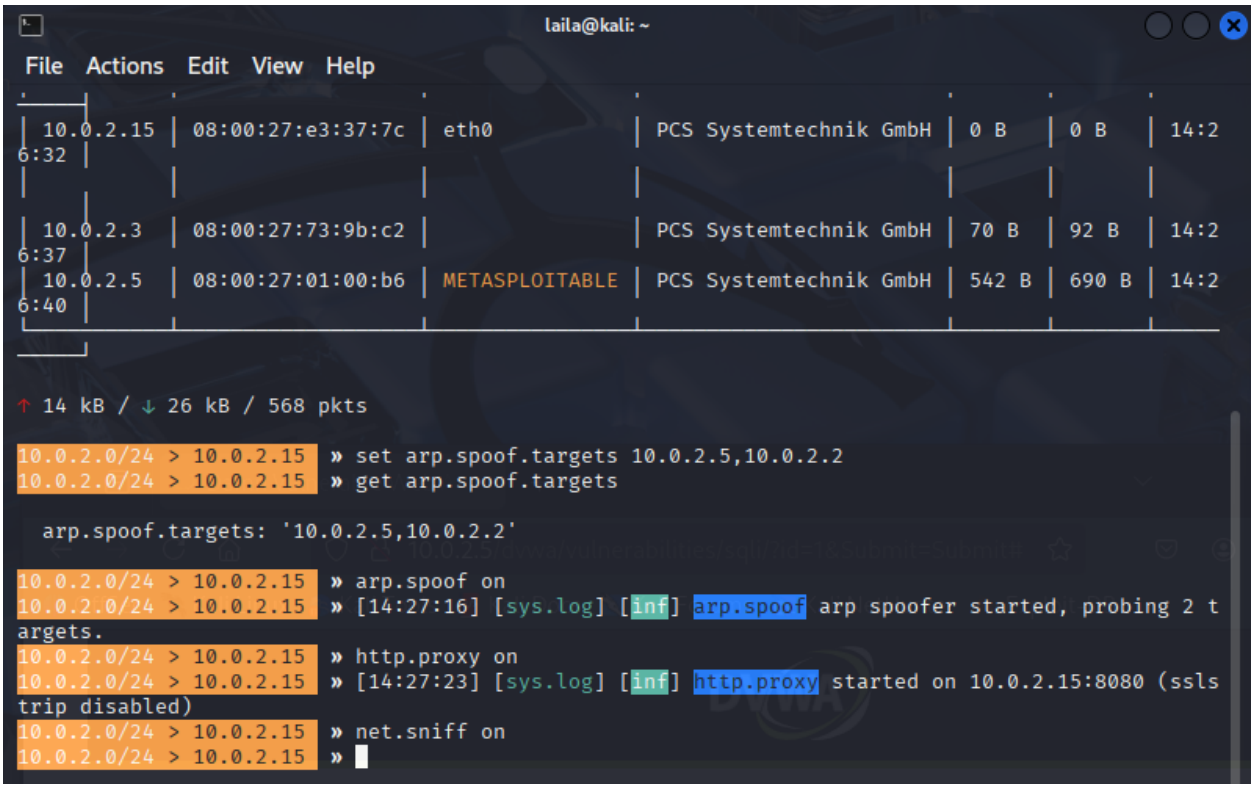
Done spoofing now we will see if we entered a username in the DVWA

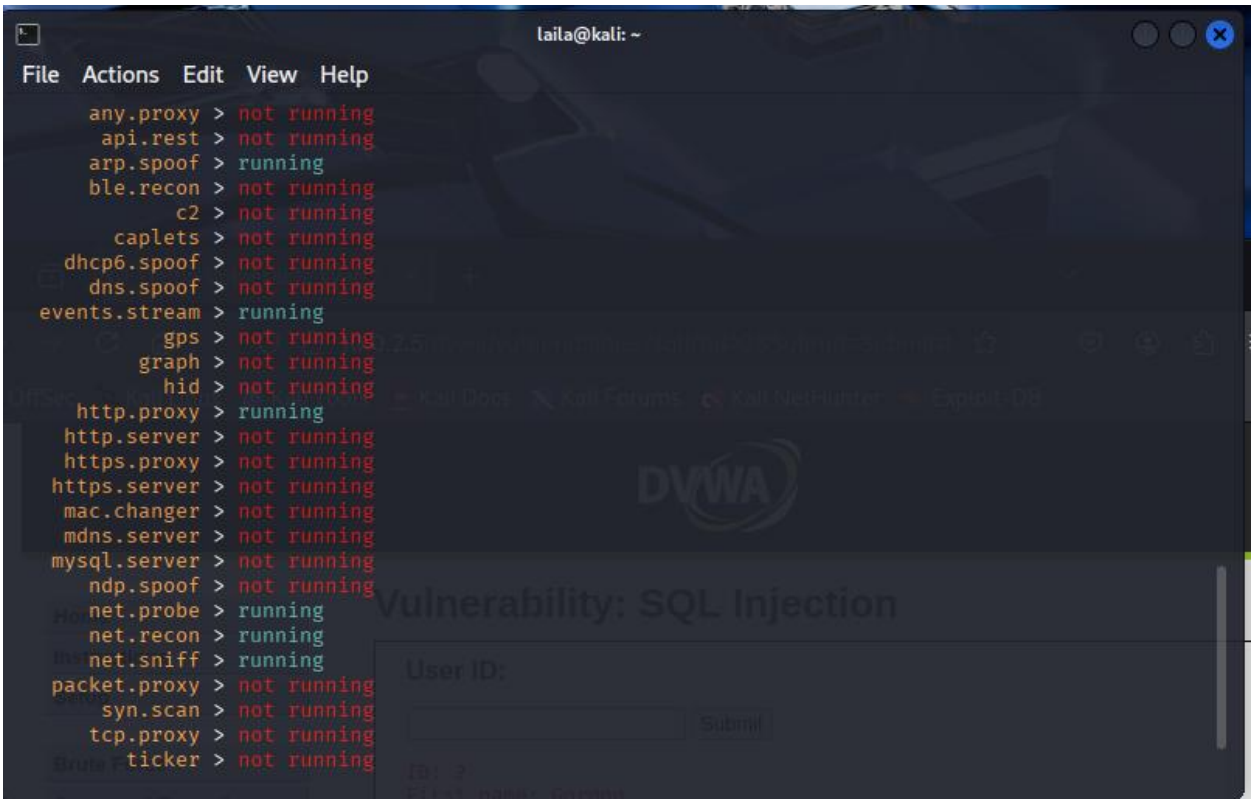


I entered user 1 with first name : admin and last name : admin

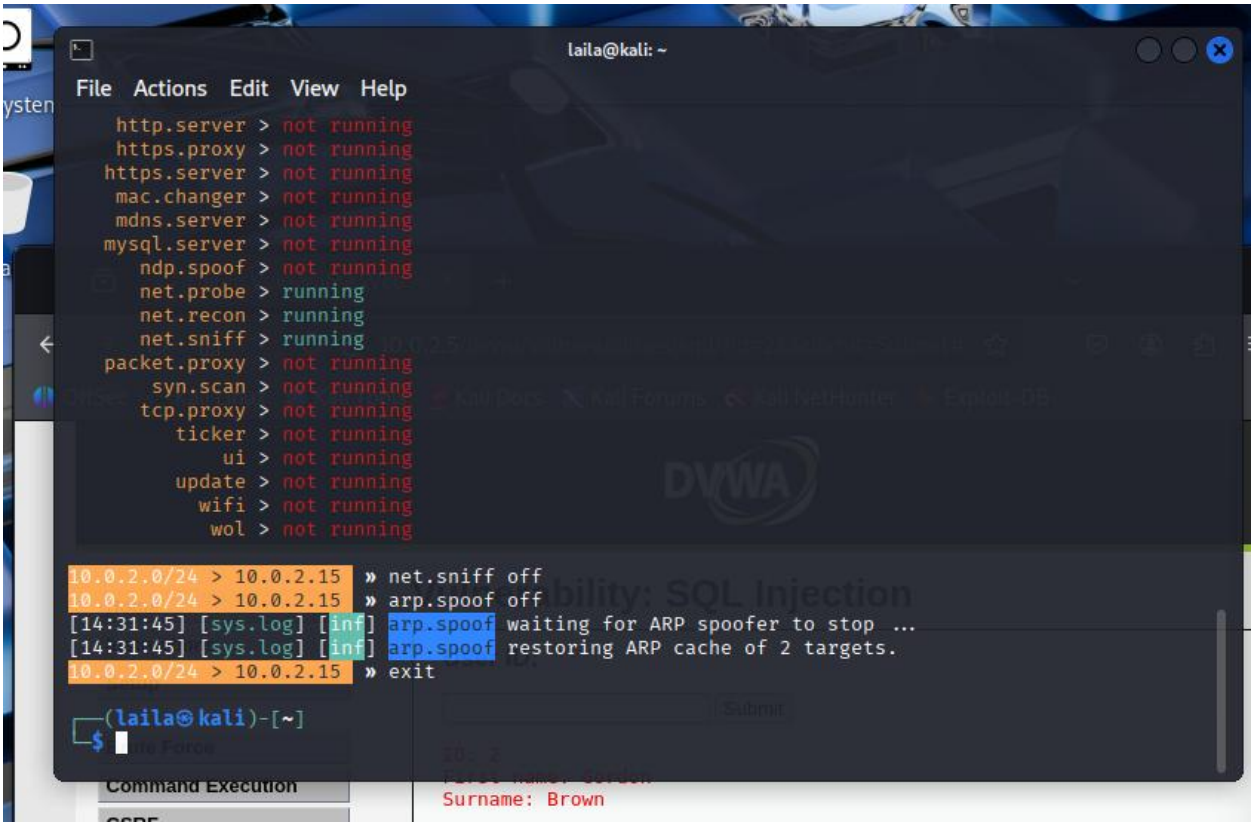


Then I did proxy on because when I did the spoof on and submitted the user .. it didn't show on kali terminal so I did proxy mode on to see what is running



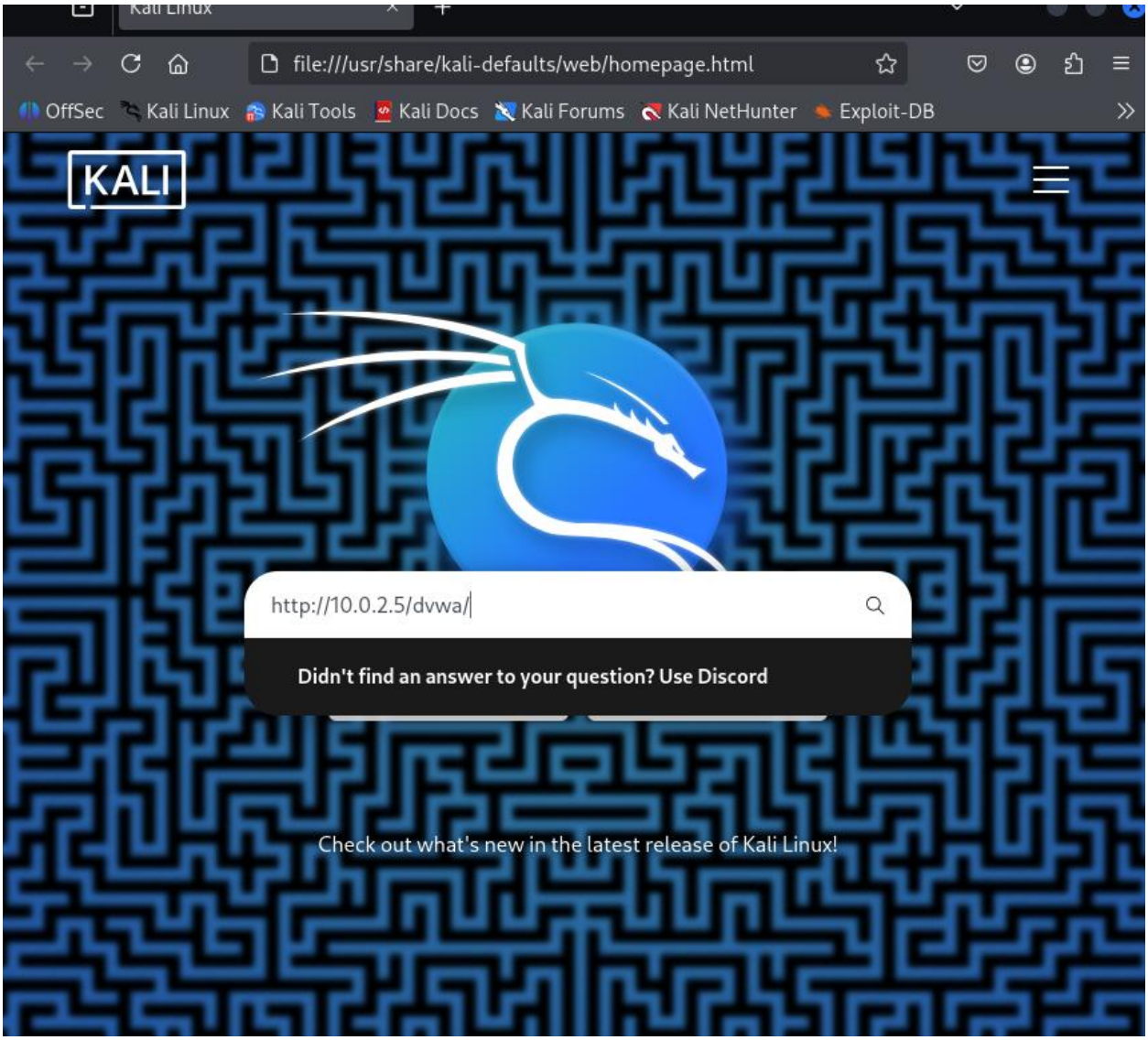


Task is done : arp spoofing, stream,proxy,probe, recon,sniff is running



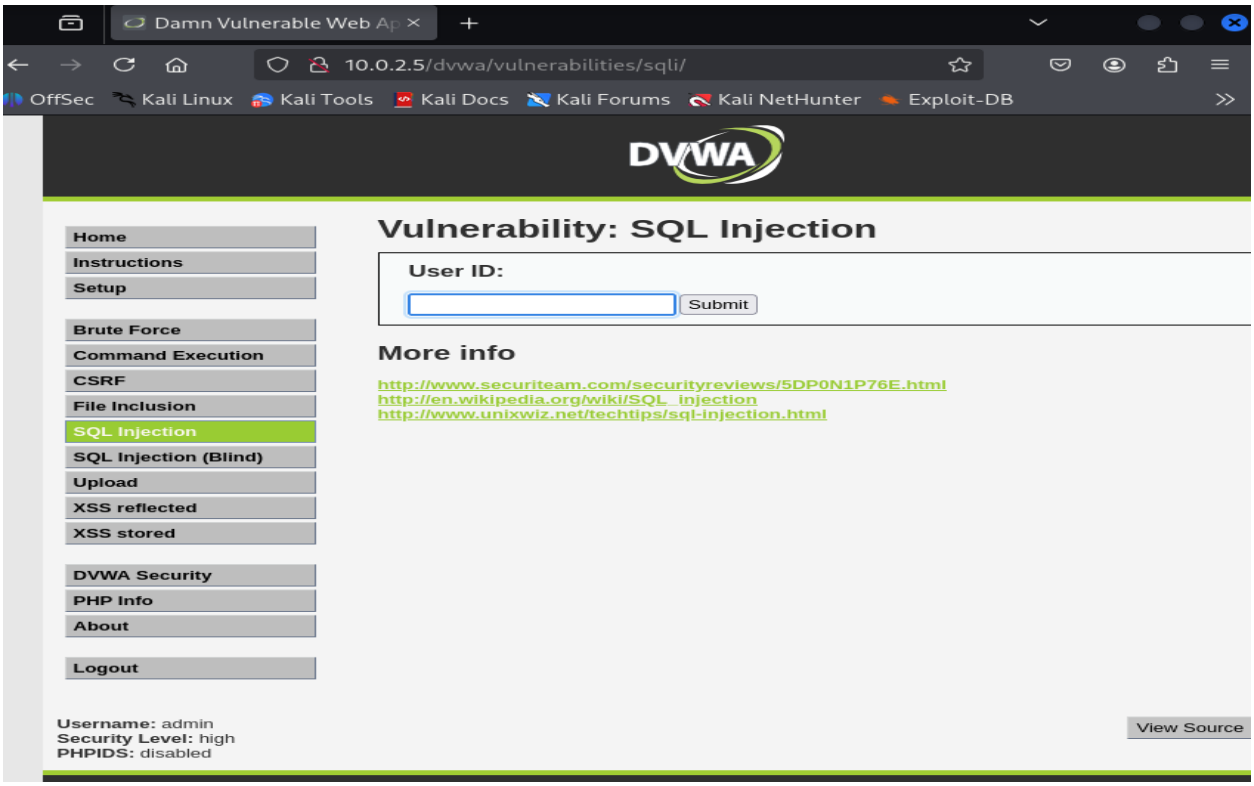
Done with this task so I turned off everything

3. Database Attack using SQLmap:

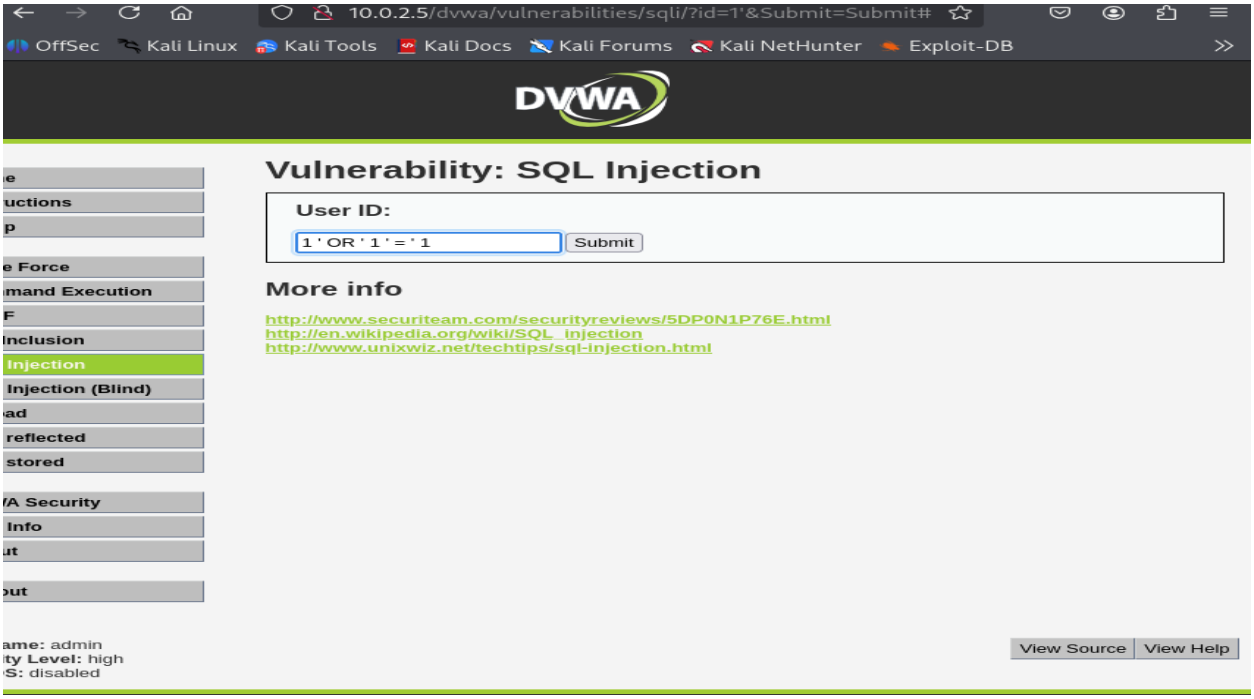


Re entered DVWA

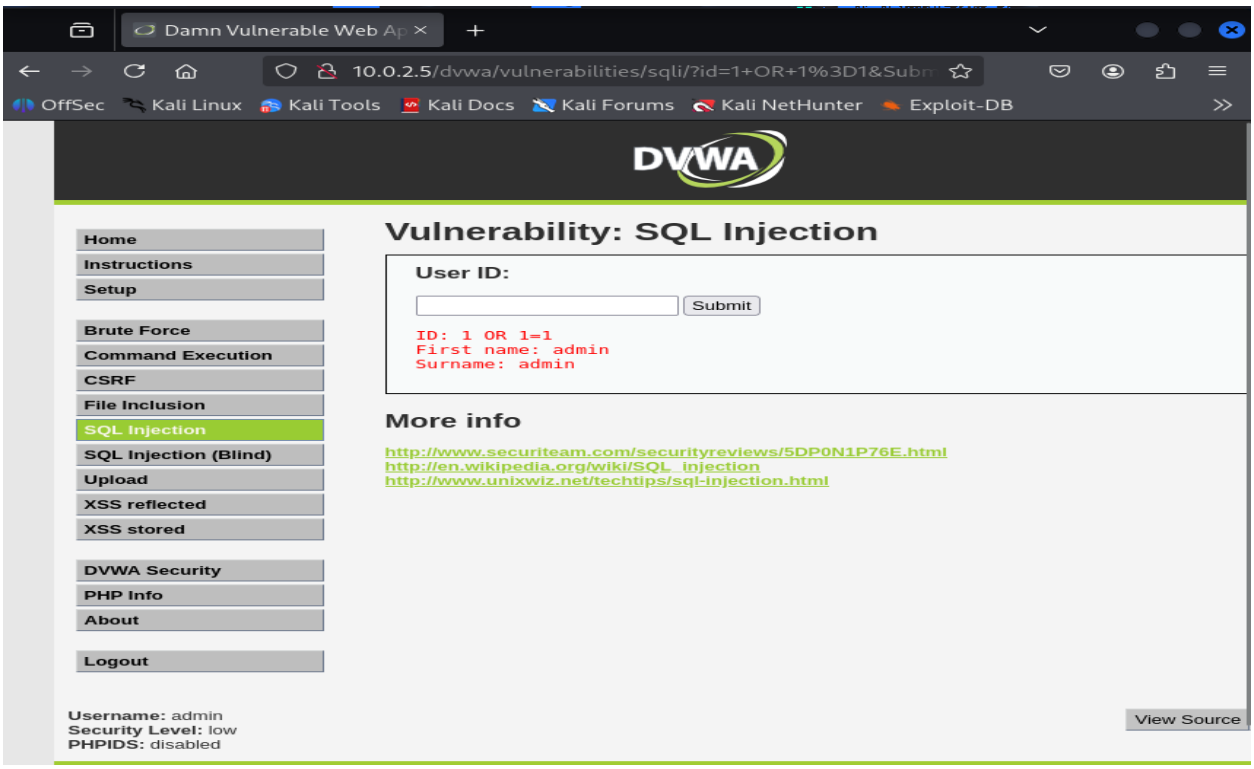
Here I set the security low -> so I can attack because if the security is high then I can't attack because of the firewall



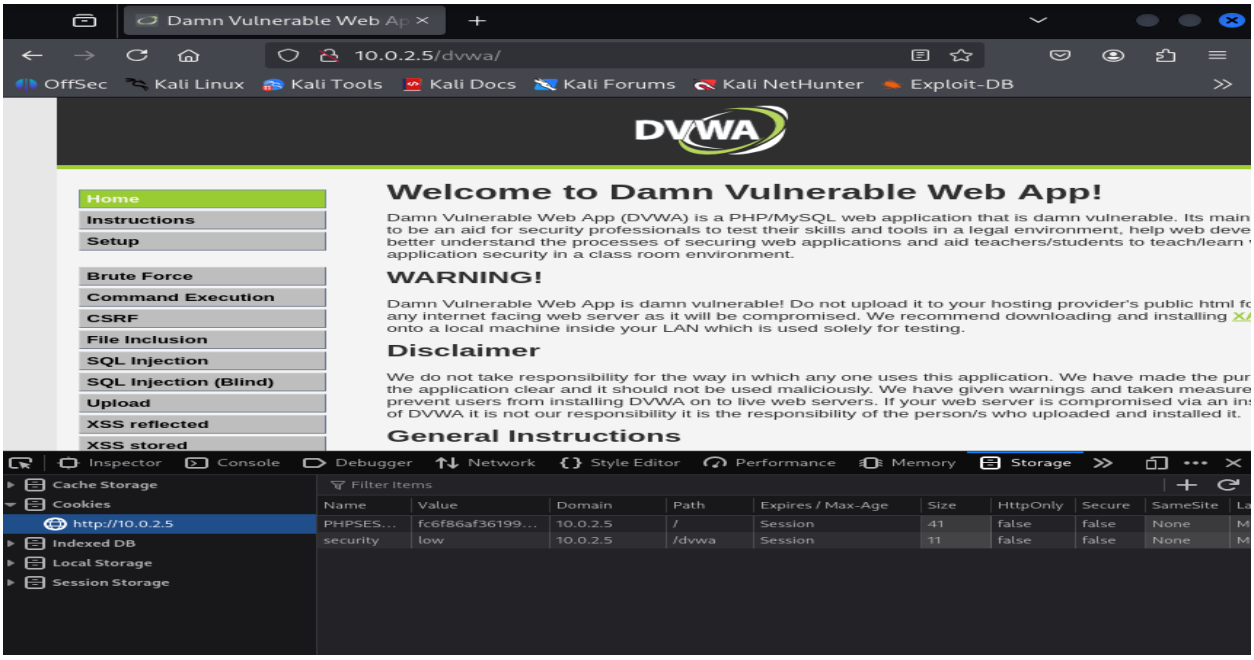
Here I have to enter the user id which can be 1 OR 1=1 to be able to enter to the database and attack it



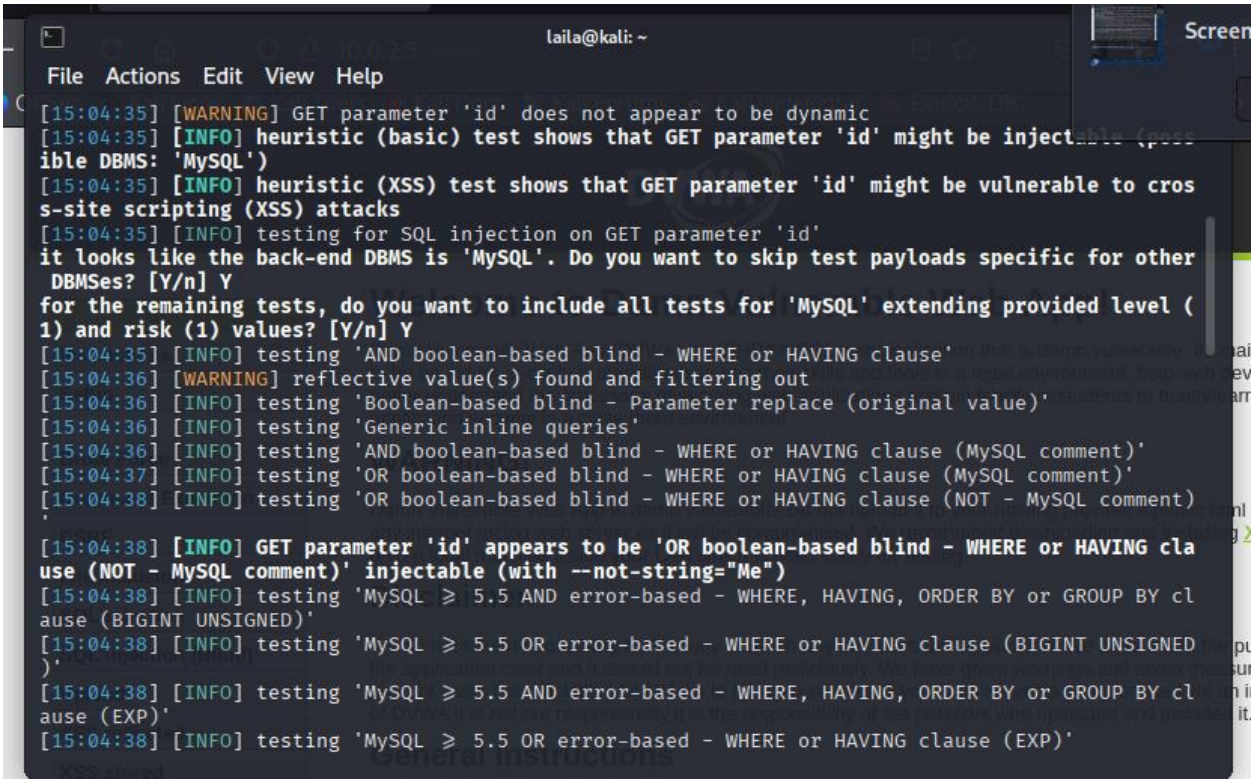
That's what I entered so I can attack the database



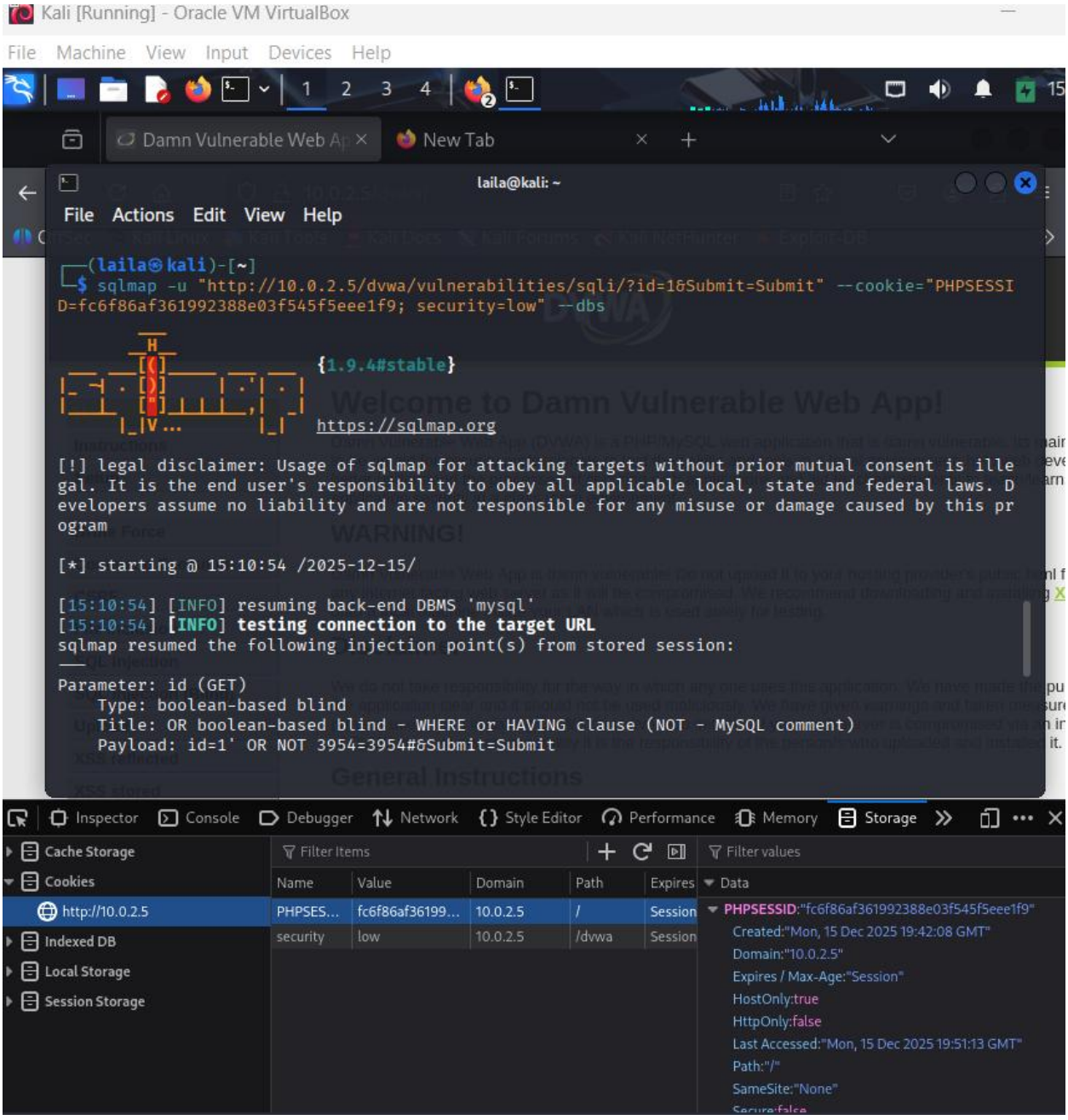
It displayed the first one in the database



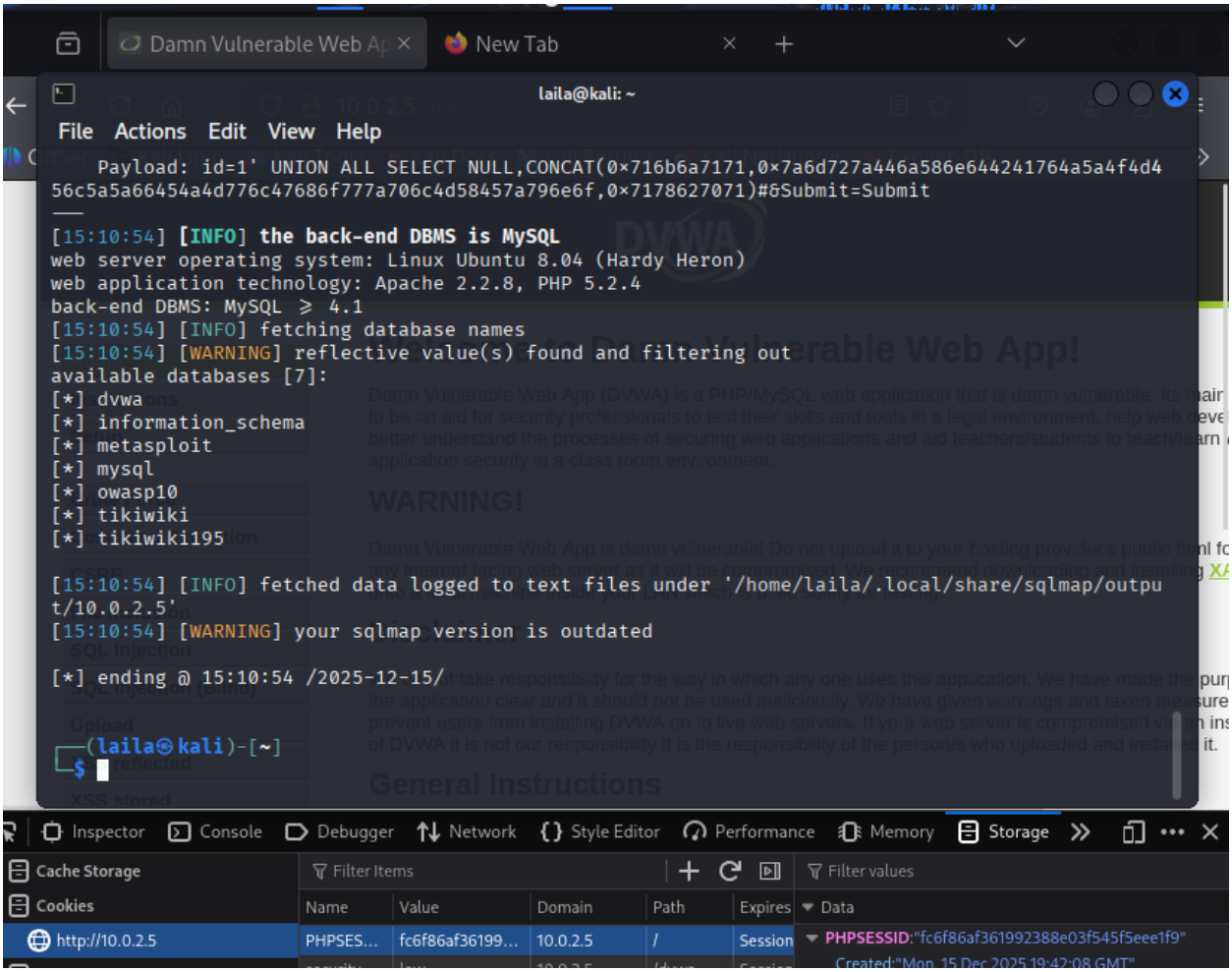
Here I need to steal the cookies session so I can log in to the databae with the PHPSESSID



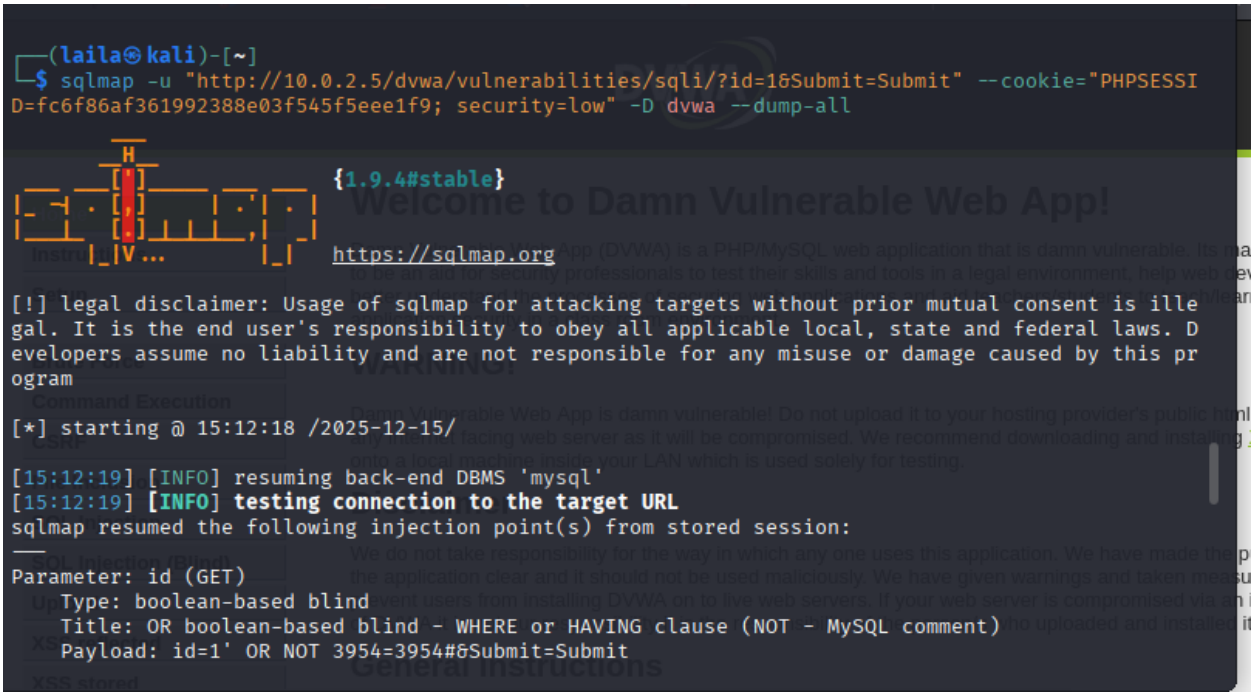
This is to see that the id is vulnerable to I can attack based on it

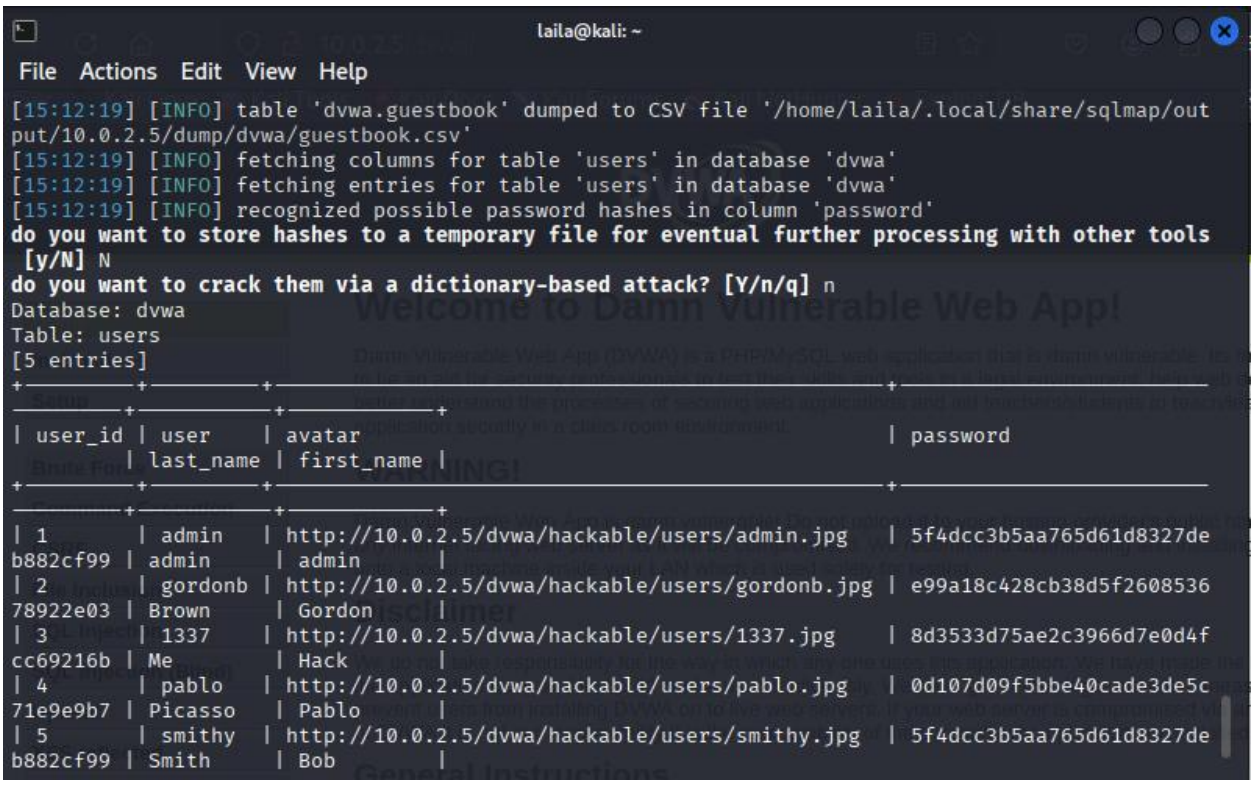


Taking the session id



And replace it on kali when the current one (above -> PHPSESSID)

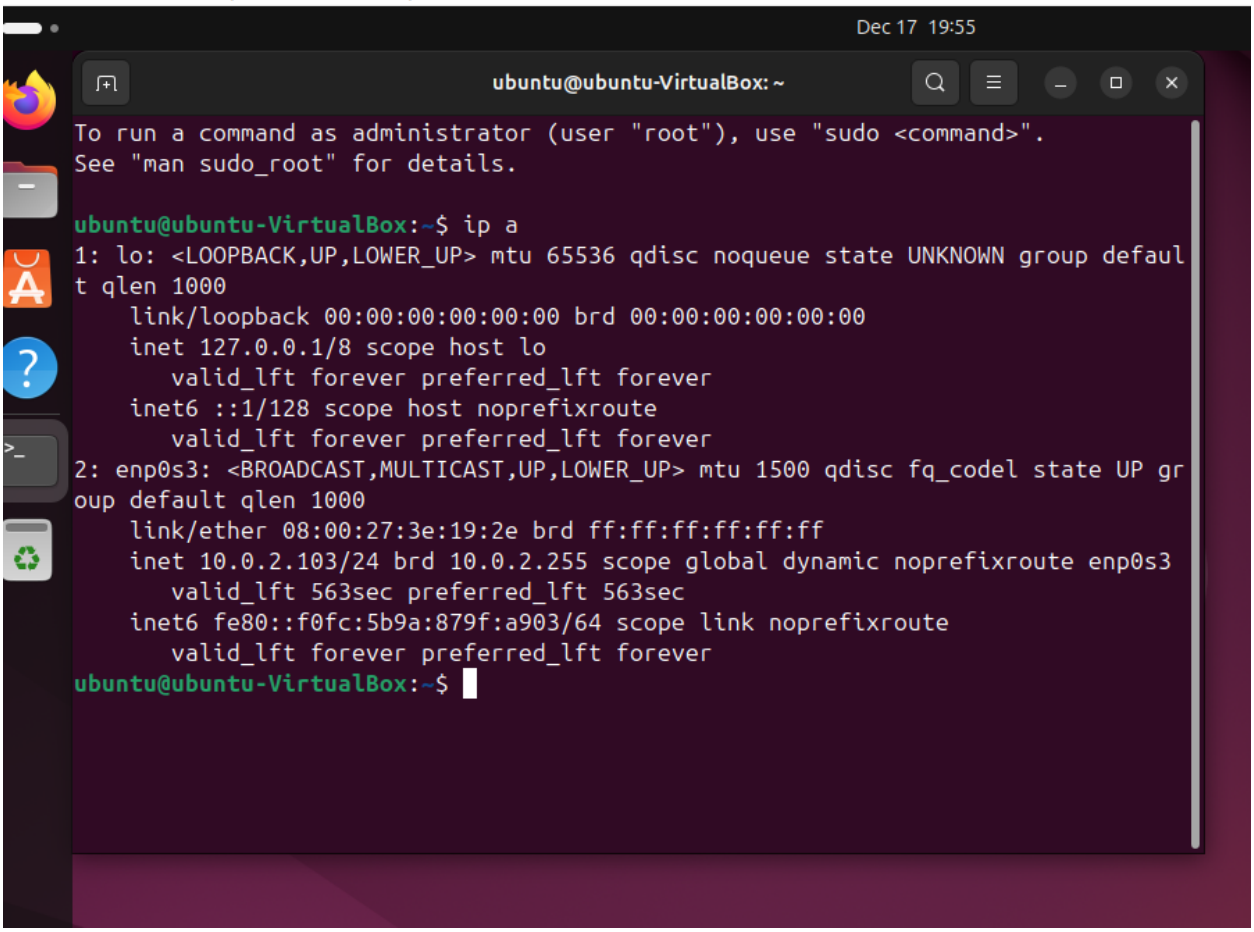




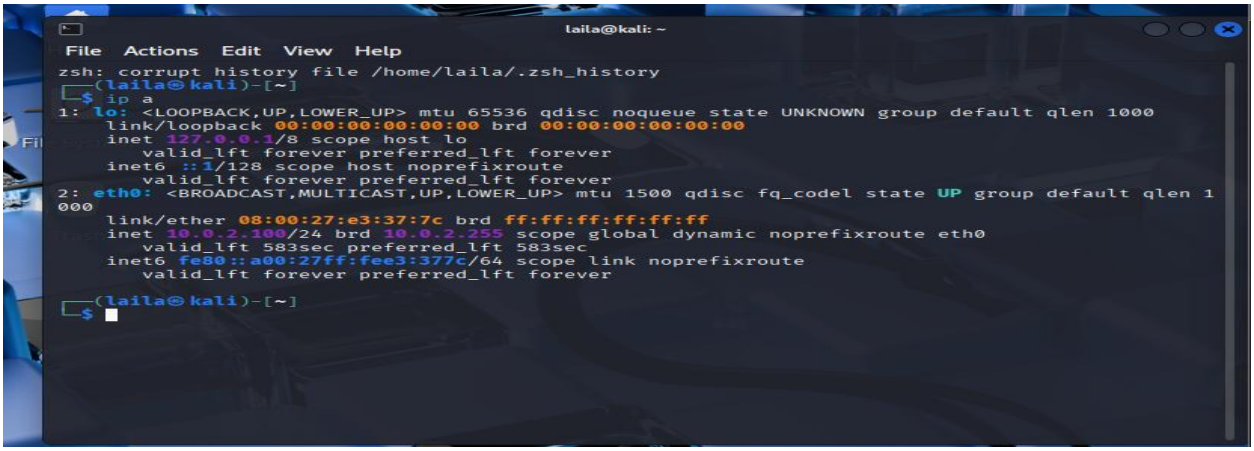
I have all the database with all the passwords

4. Logon attack on ubuntu using Hydra:

I had a problem with the ip configuration (the NAT network) that I did so I changed all of the vms network to host-only adapter (in which I also enable the dhcp) so all of the ips changed

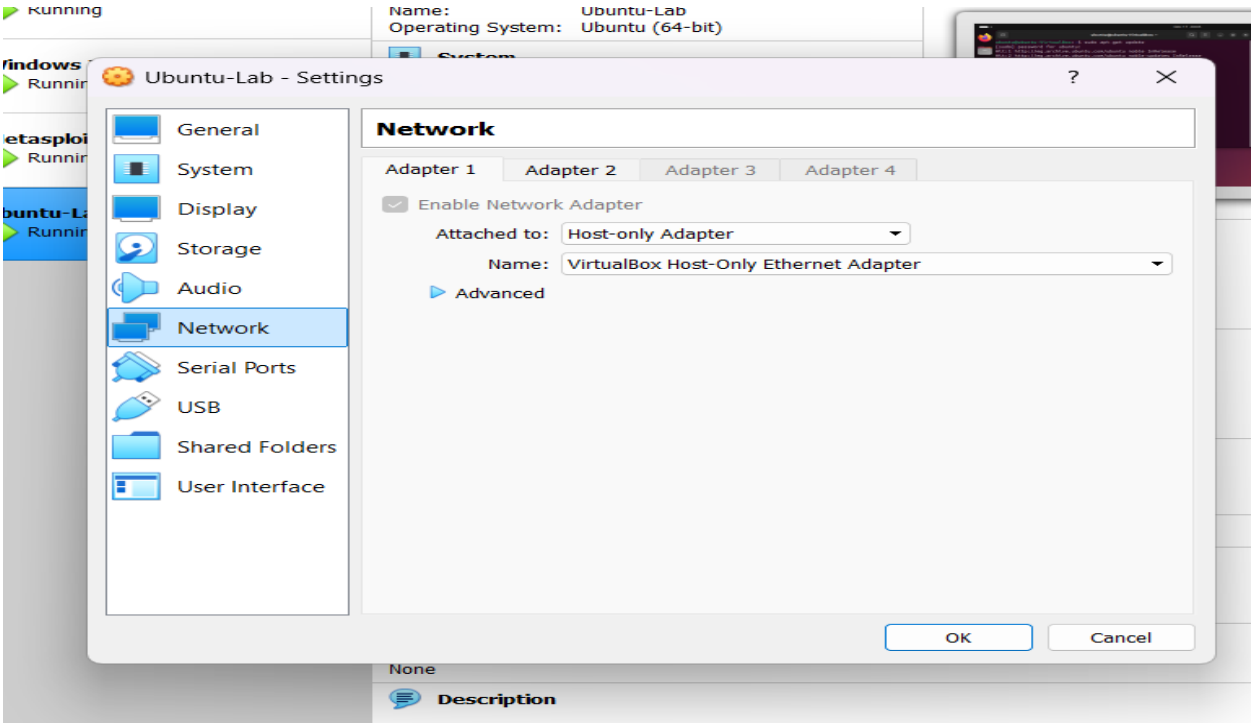


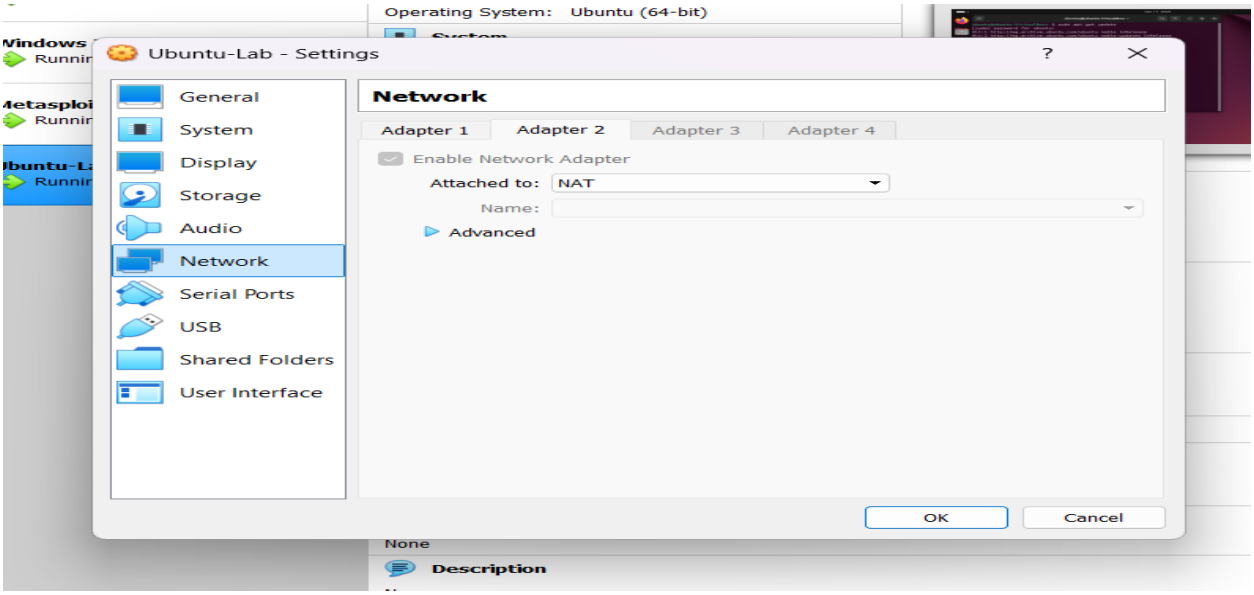
The new ip address of ubuntu : 10.0.2.103



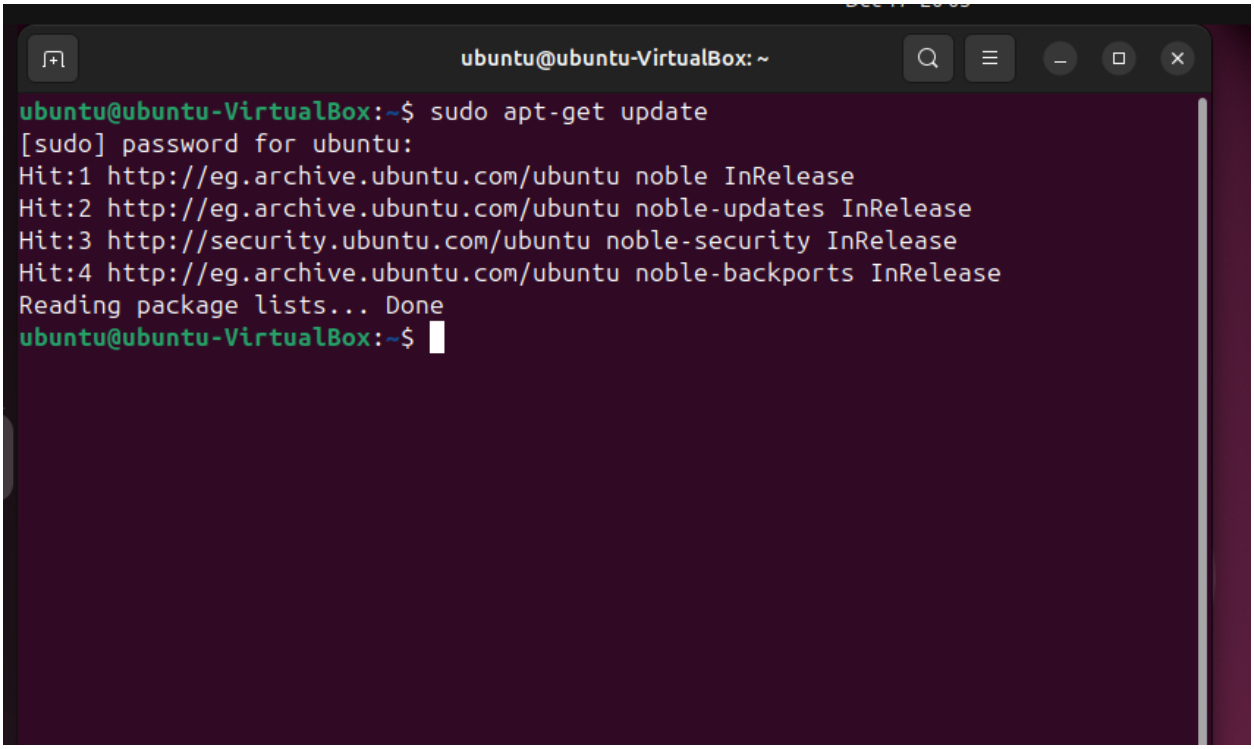
and this is kali's ip address: 10.0.2.100

Another problem appeard the ssh port didn't want to open on ubuntu (on the host-only adapter) so I added another adapter but instead of using host-only I used NAT and after updating and installing the ssh I will remove it and keep only adapter 1 which is host-only adapter

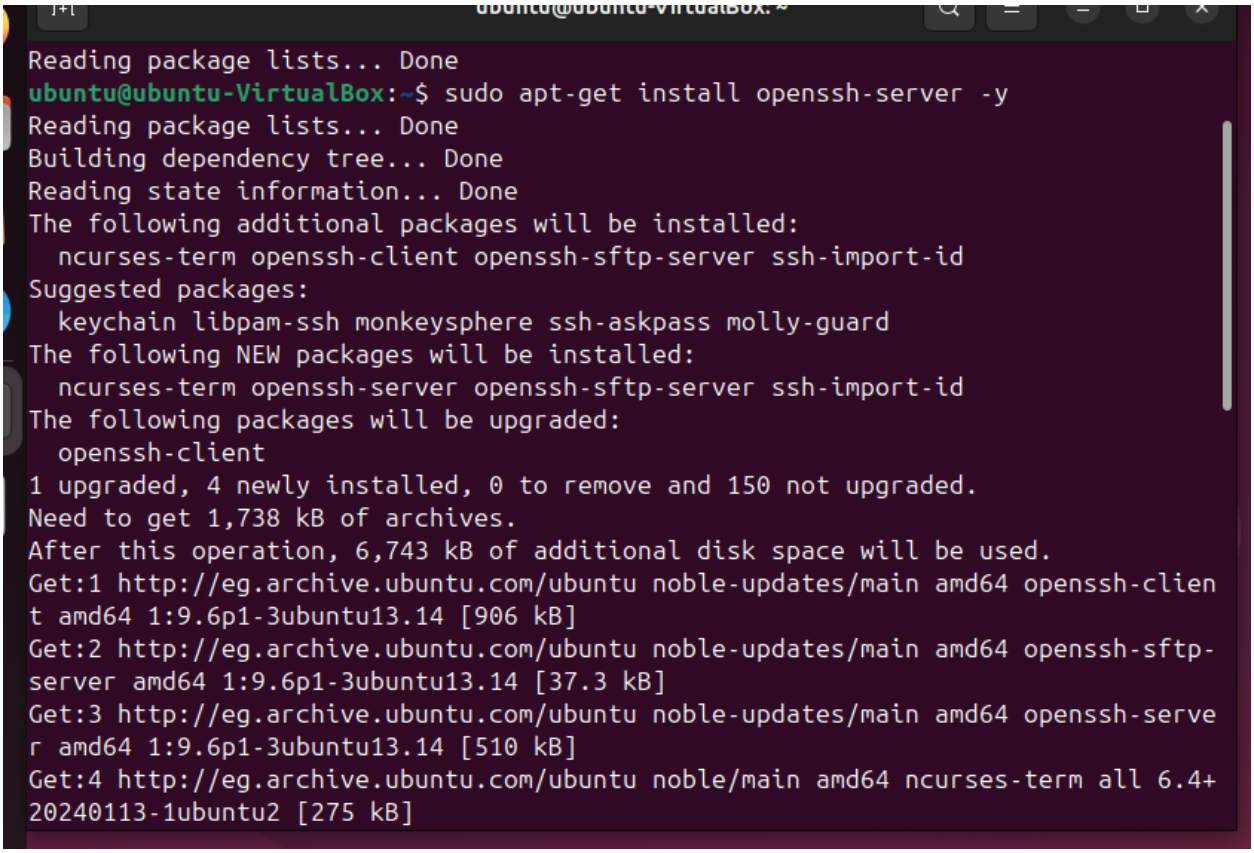




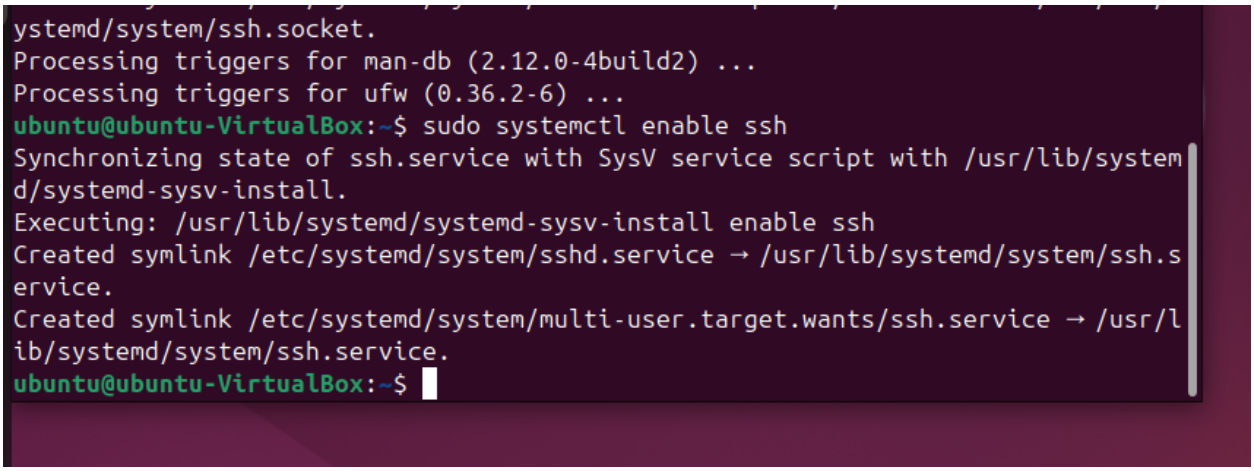
Done



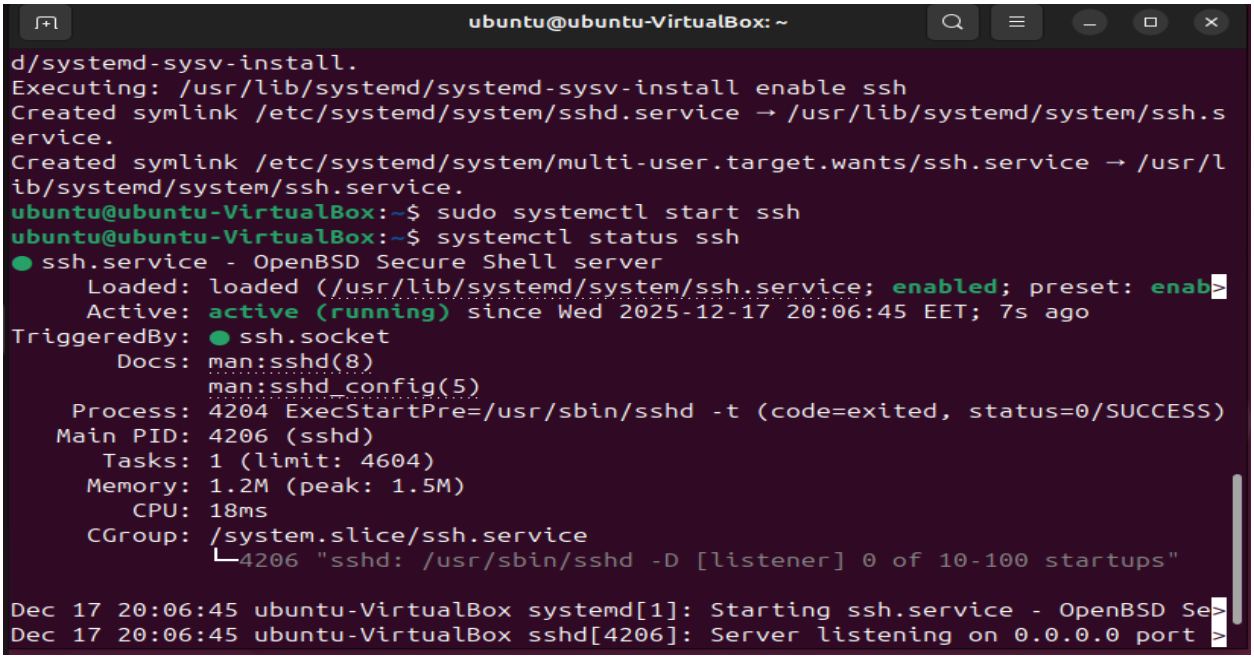
Update done



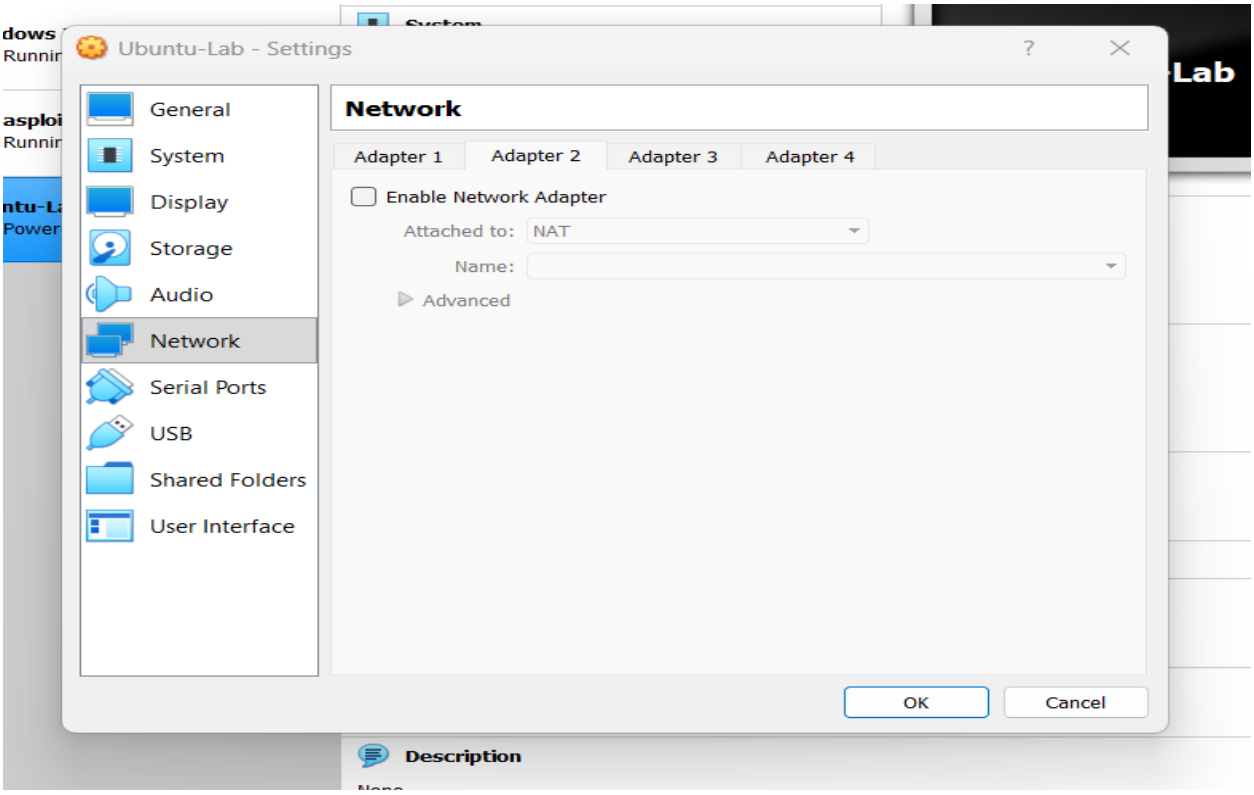
Done installing the ssh server

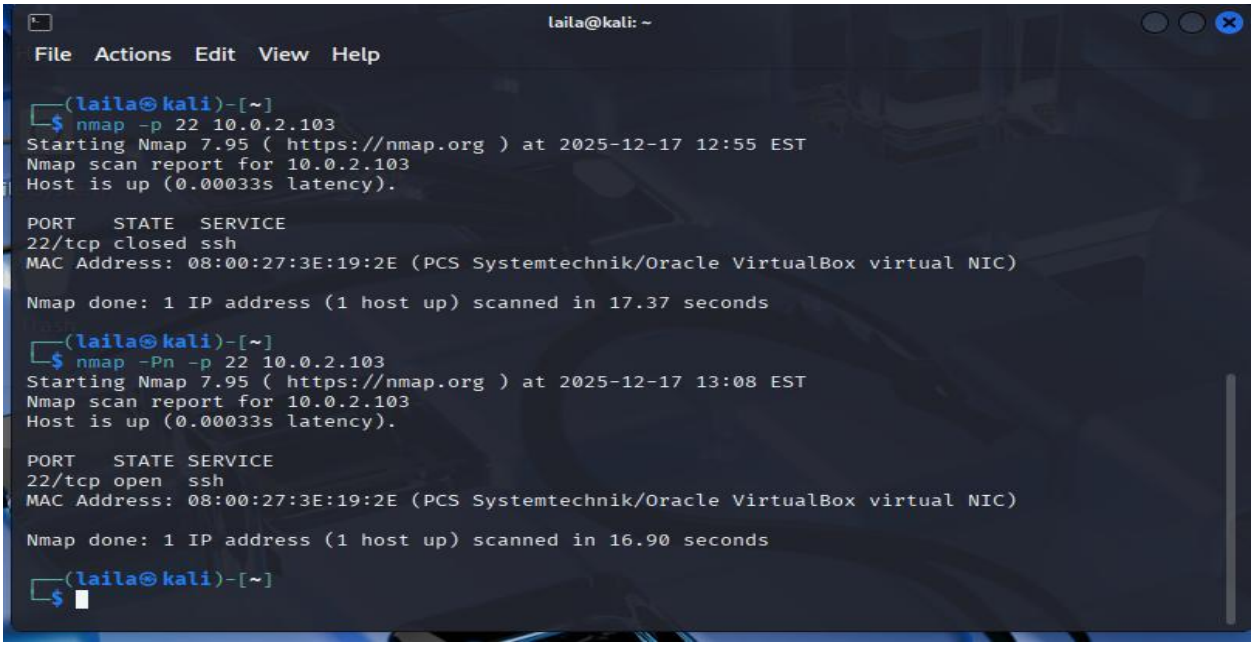


Then I enabled the ssh

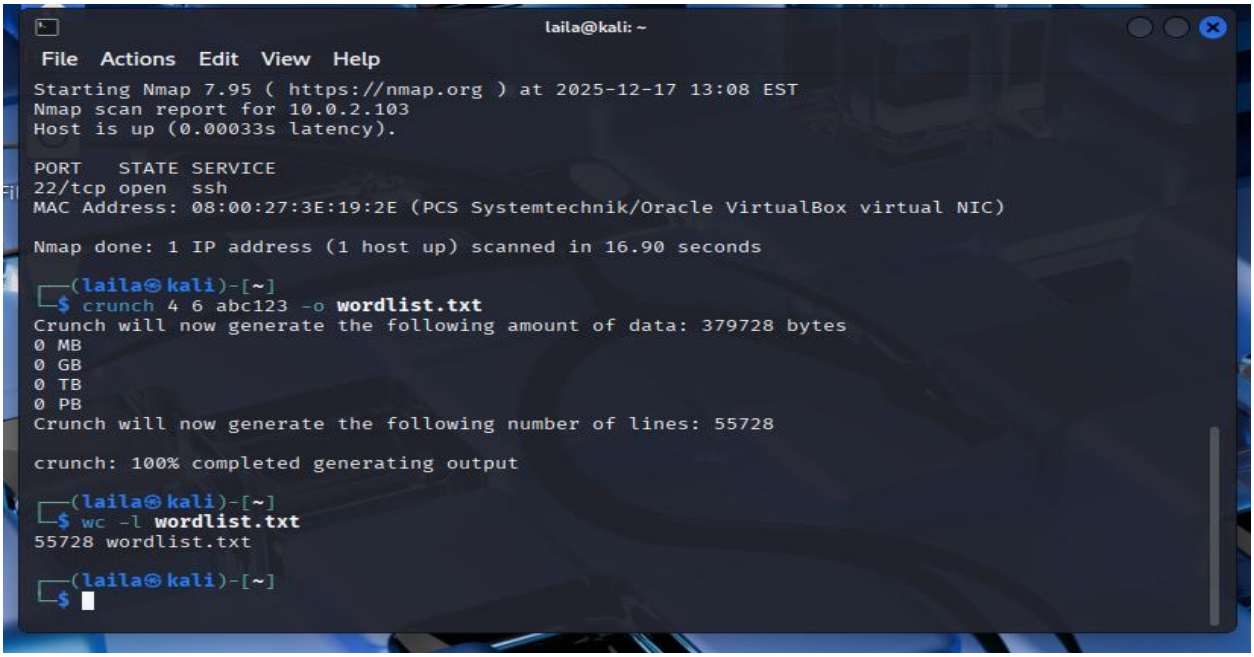


Made sure that the port is active .. rn I will disable adapter 2



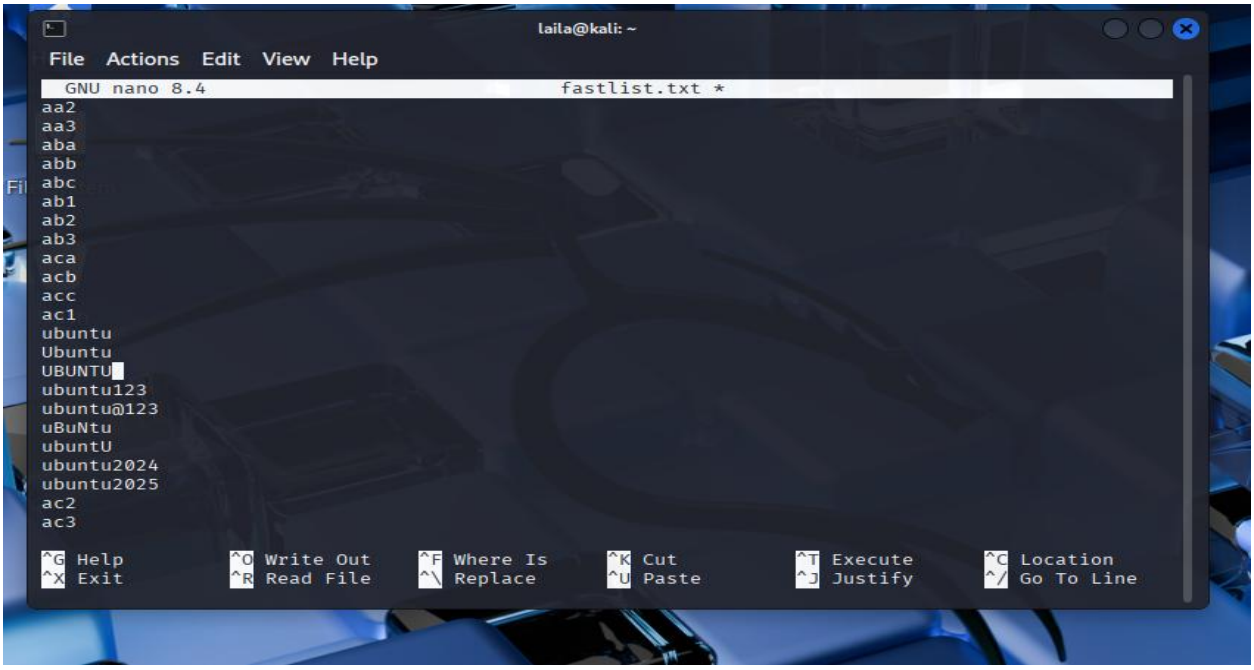


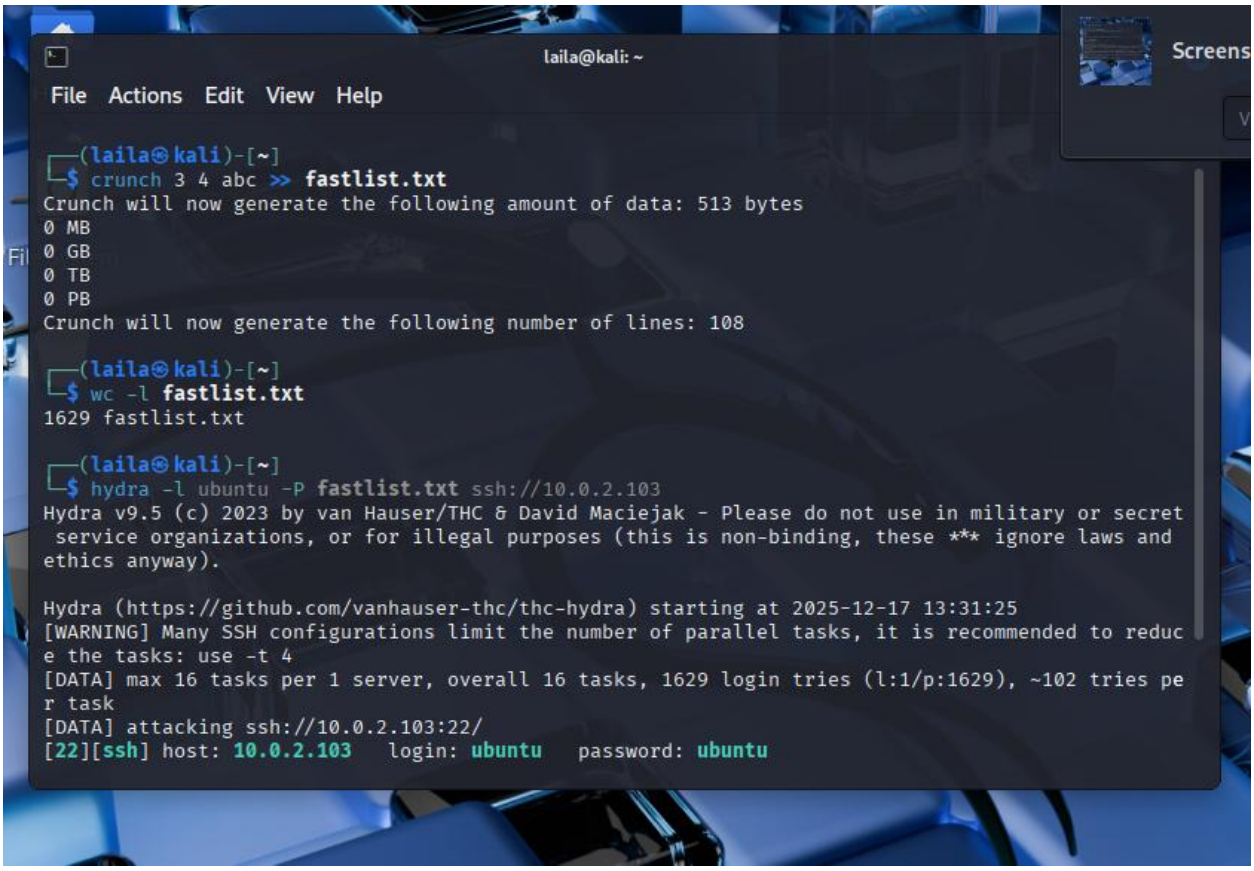
As we can see the port 22 is open -> ready for attack



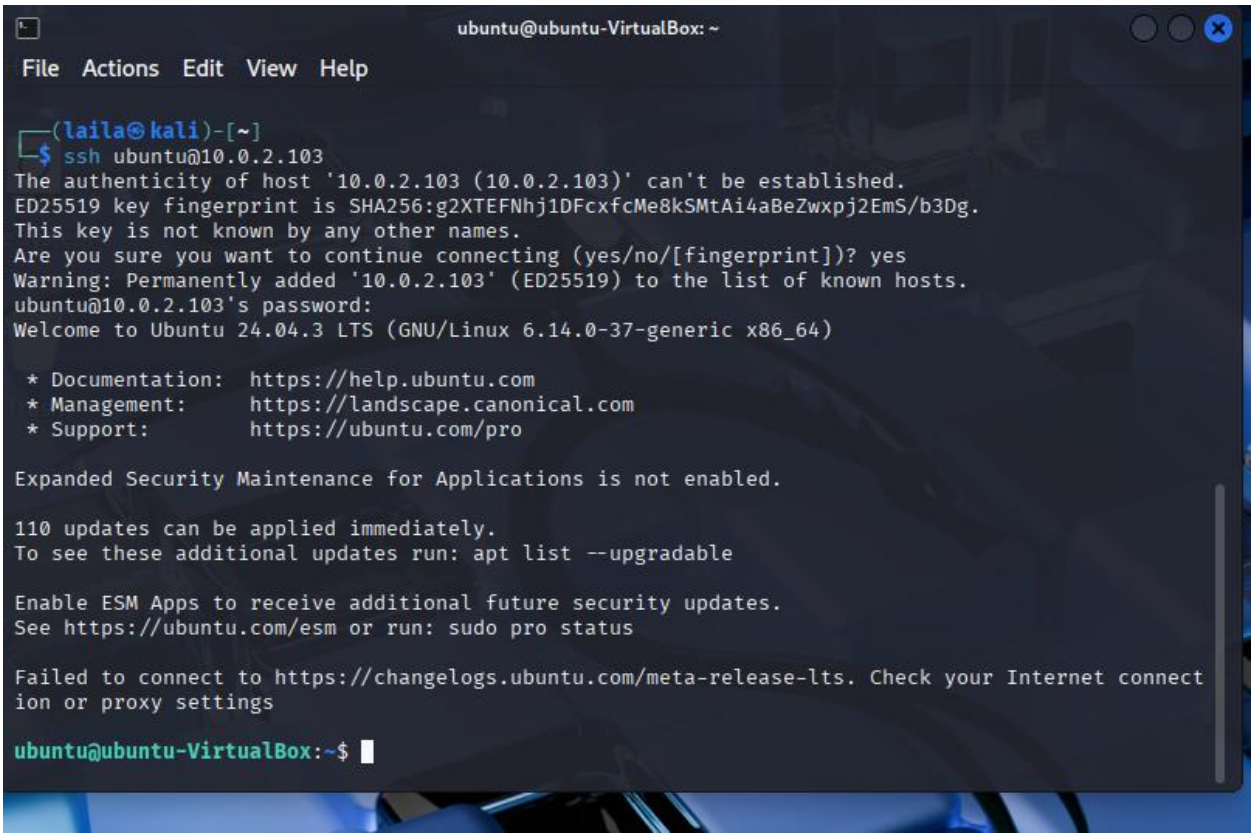
Here I tried the wordlist.txt (crunch password that hydra will use) but the amount of possibilities are so much so I will use instead fastlist.txt

And also there is problem that all the passwords are abc etc.. and my password is ubuntu so I needed to add these password in the fastlist.txt


laila@kali: ~
File Actions Edit View Help
GNU nano 8.4 fastlist.txt *
aa2
aa3
aba
abb
abc
ab1
ab2
ab3
aca
acb
acc
ac1
ubuntu
Ubuntu
UBUNTU
ubuntu123
ubuntu@123
uBuNtu
ubuntU
ubuntu2024
ubuntu2025
ac2
ac3
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

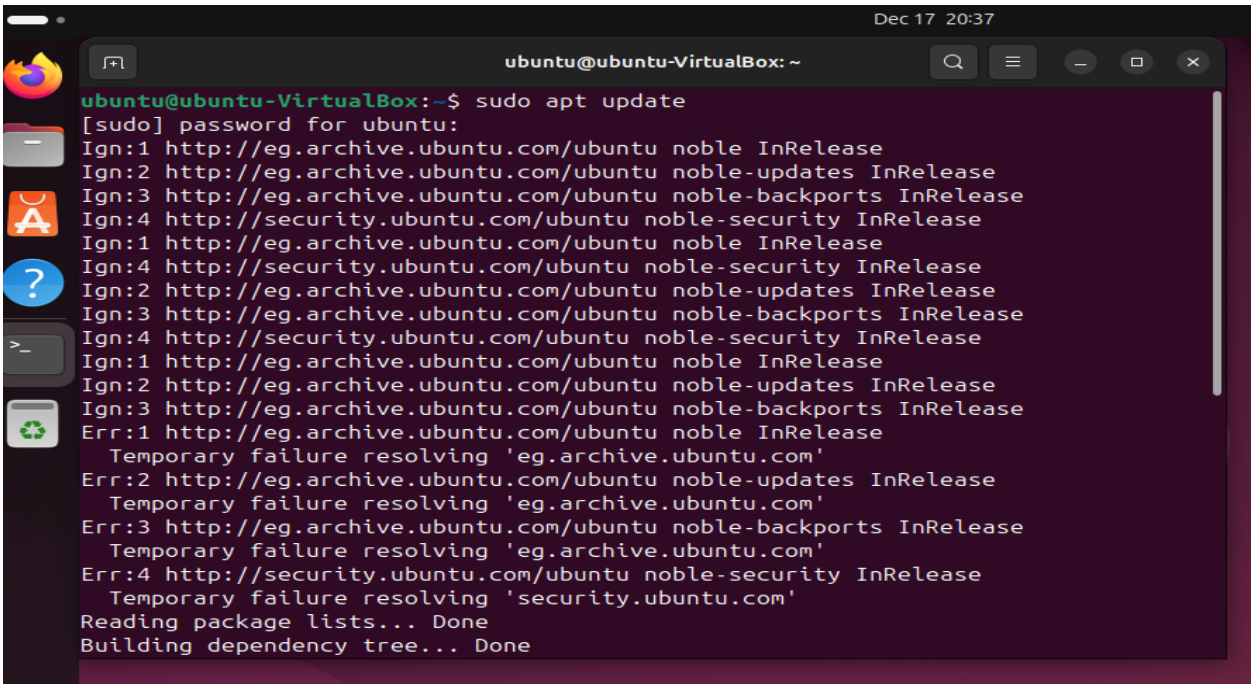

laila@kali: ~
File Actions Edit View Help
Screens
(laila㉿kali)-[~]
$ crunch 3 4 abc >> fastlist.txt
Crunch will now generate the following amount of data: 513 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 108
(laila㉿kali)-[~]
$ wc -l fastlist.txt
1629 fastlist.txt
(laila㉿kali)-[~]
$ hydra -l ubuntu -P fastlist.txt ssh://10.0.2.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-17 13:31:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1629 login tries (l:1/p:1629), ~102 tries per task
[DATA] attacking ssh://10.0.2.103:22/
[22][ssh] host: 10.0.2.103 login: ubuntu password: ubuntu

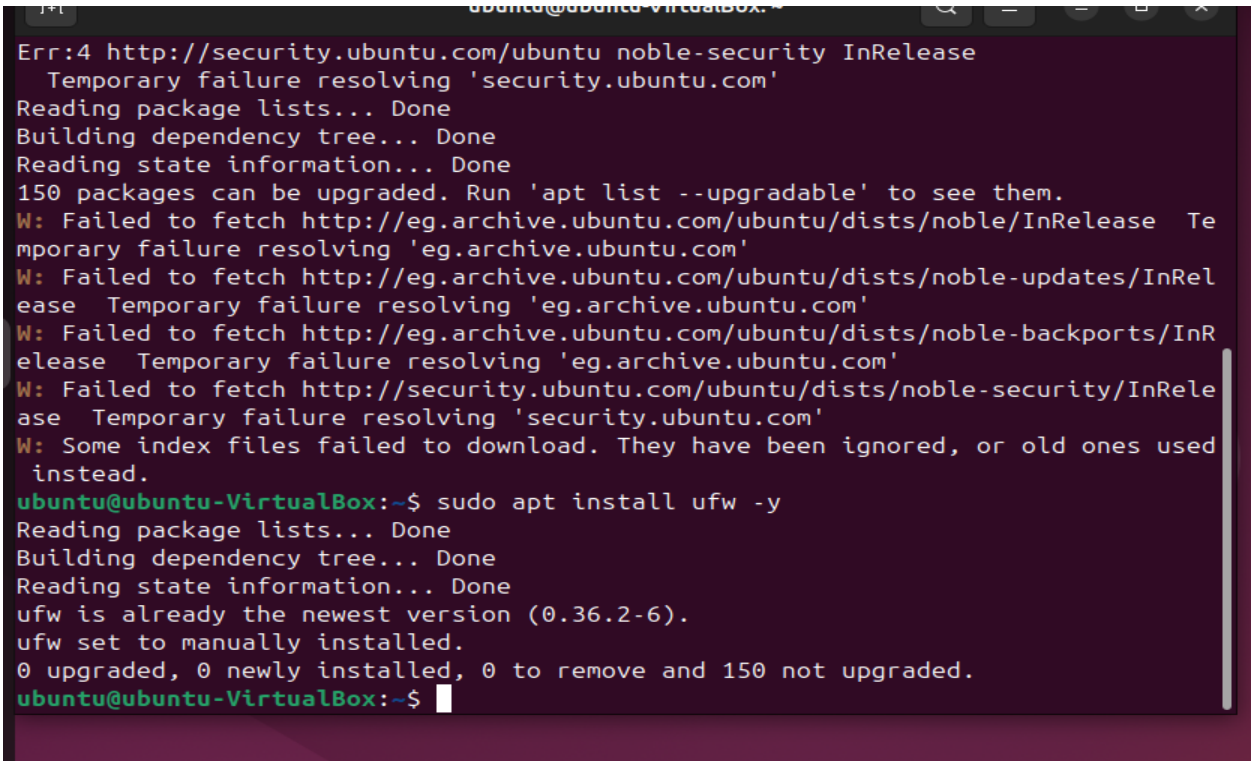
Done



Tested the password and logged in ubuntu from kali

5. Install firewall (ufw) on ubutnu:

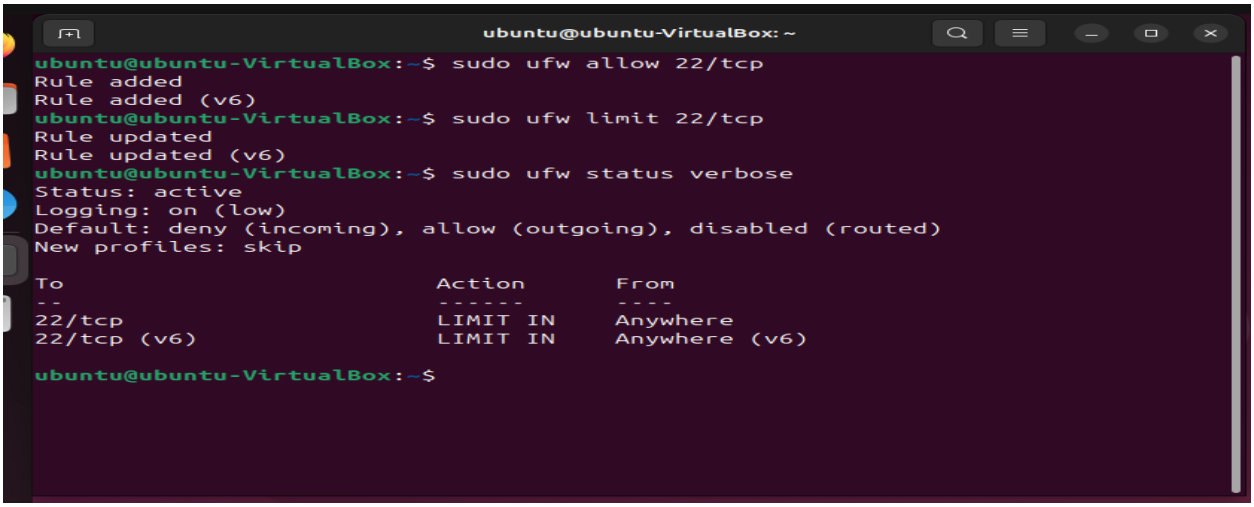




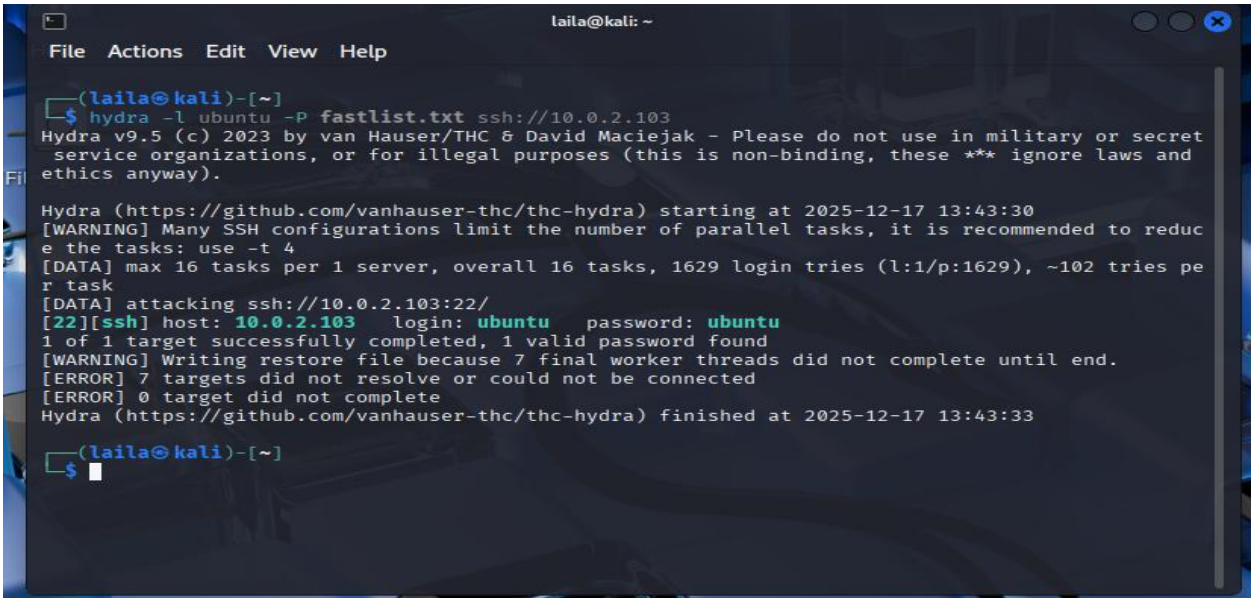
The Uncomplicated Firewall (UFW) package was installed on the Ubuntu system.

UFW was successfully enabled with default rules that deny incoming connections and allow outgoing traffic.

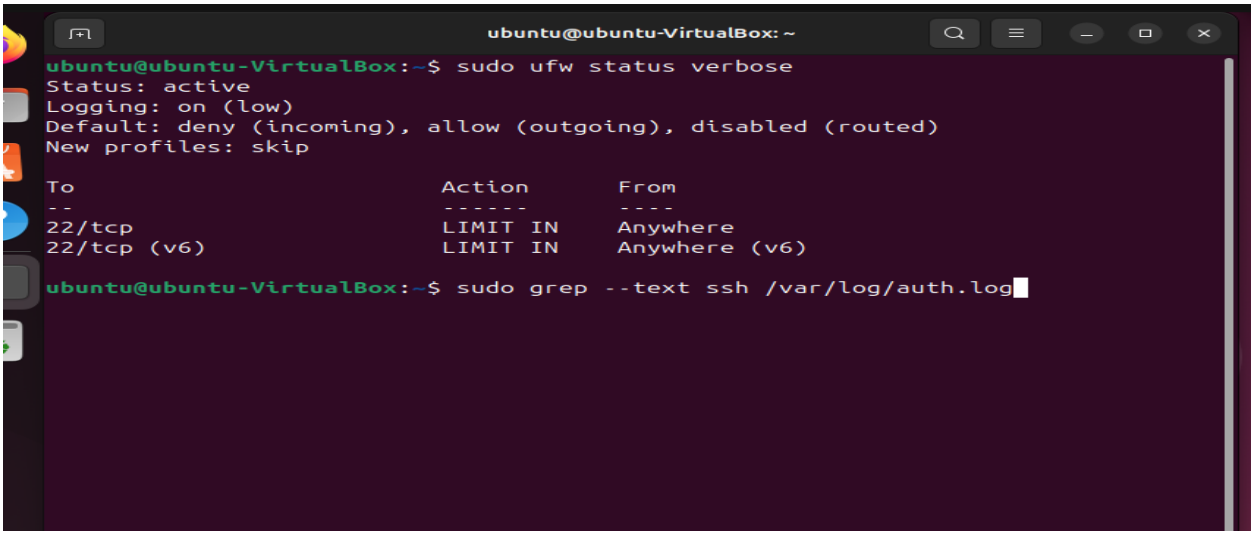
6. Secure the ubuntu ssh:

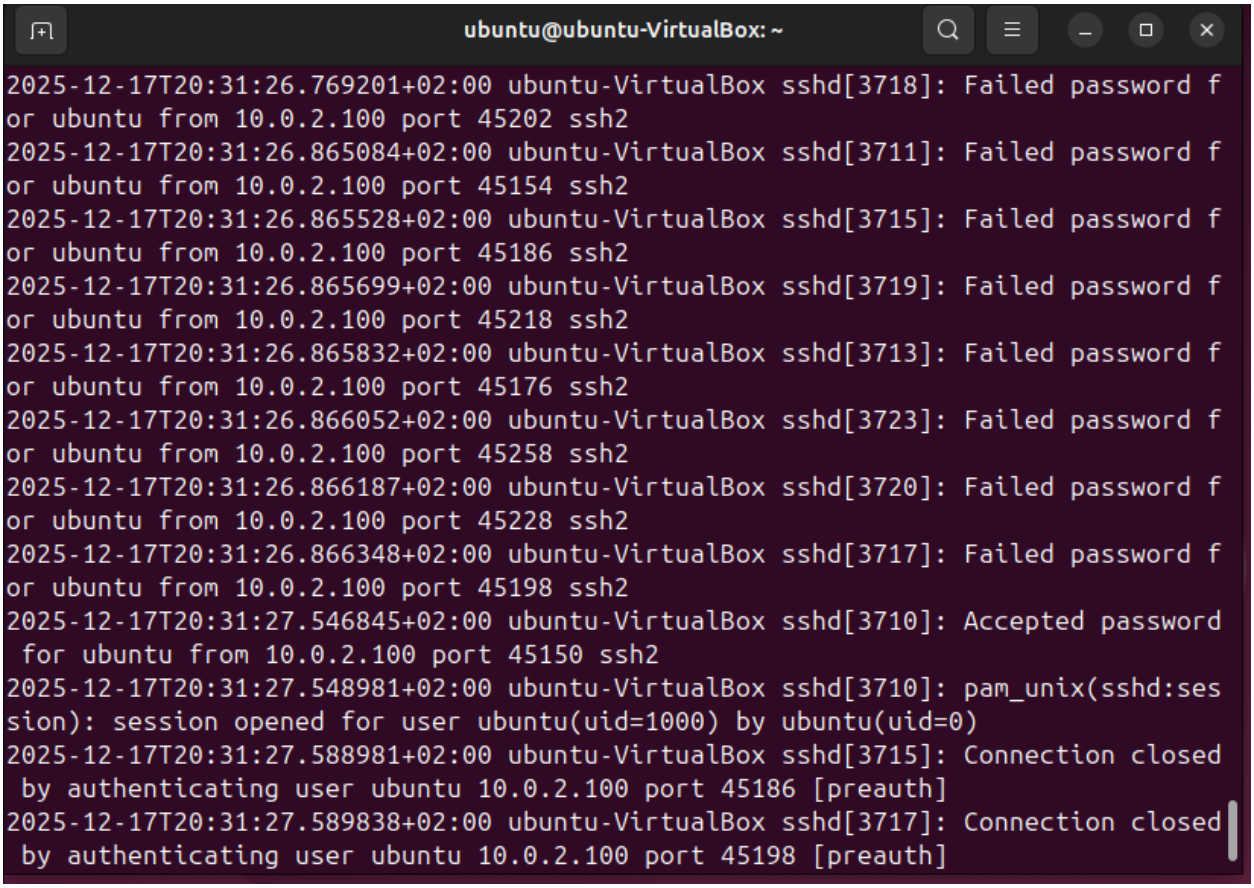


7. Re-perform the logon attack and show how UFW prevented it + check auth.log:



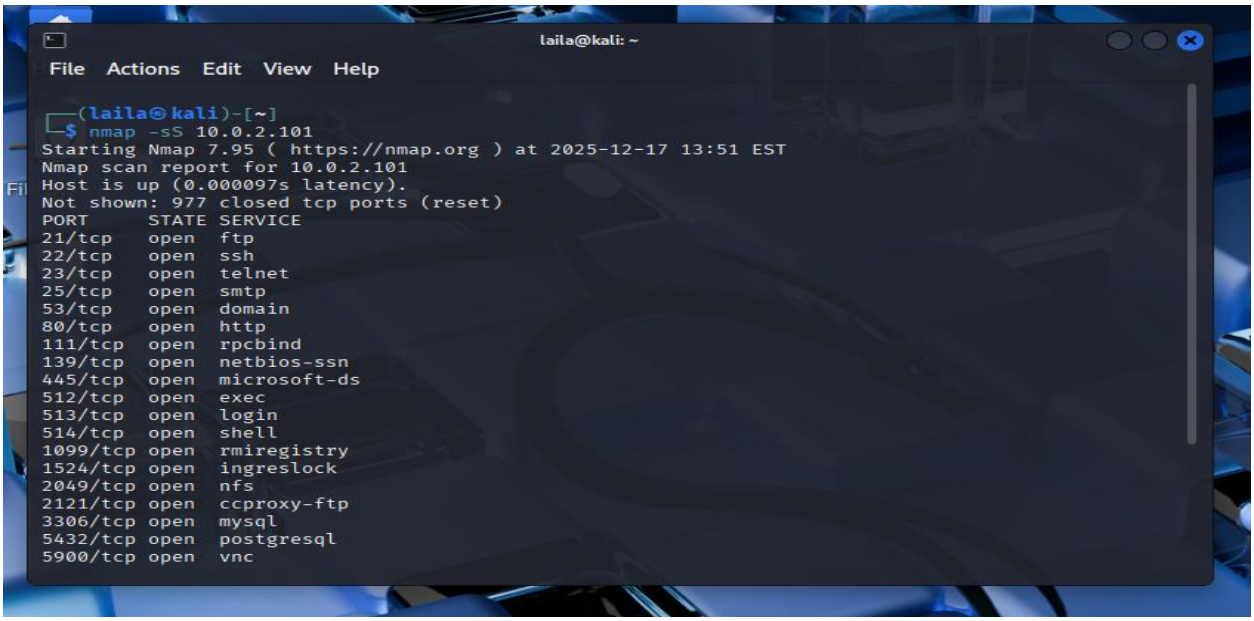
After enabling UFW and limiting SSH connections, the Hydra brute-force attack failed due to connection rate limiting.



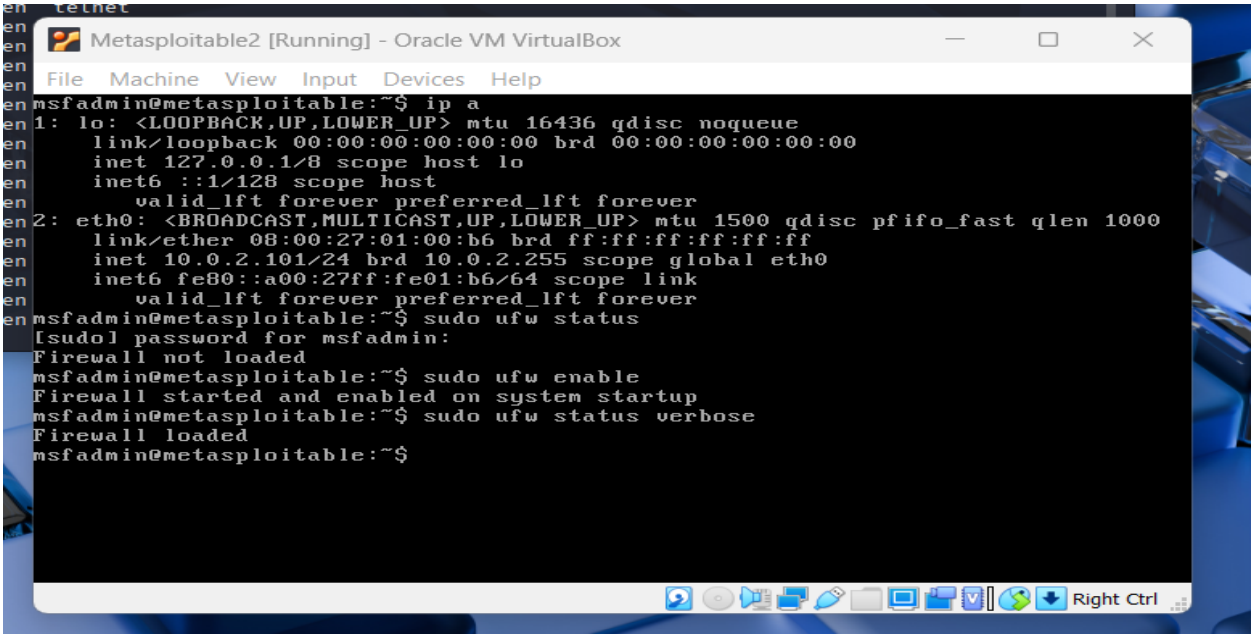


After enabling UFW and applying rate limiting on port 22, the SSH brute-force attack was re-performed using Hydra.
Unlike the previous attempt, the attack failed due to firewall restrictions. Authentication logs from /var/log/auth.log showed multiple failed SSH login attempts originating from the Kali machine, confirming that the firewall successfully limited and prevented the brute-force attack.

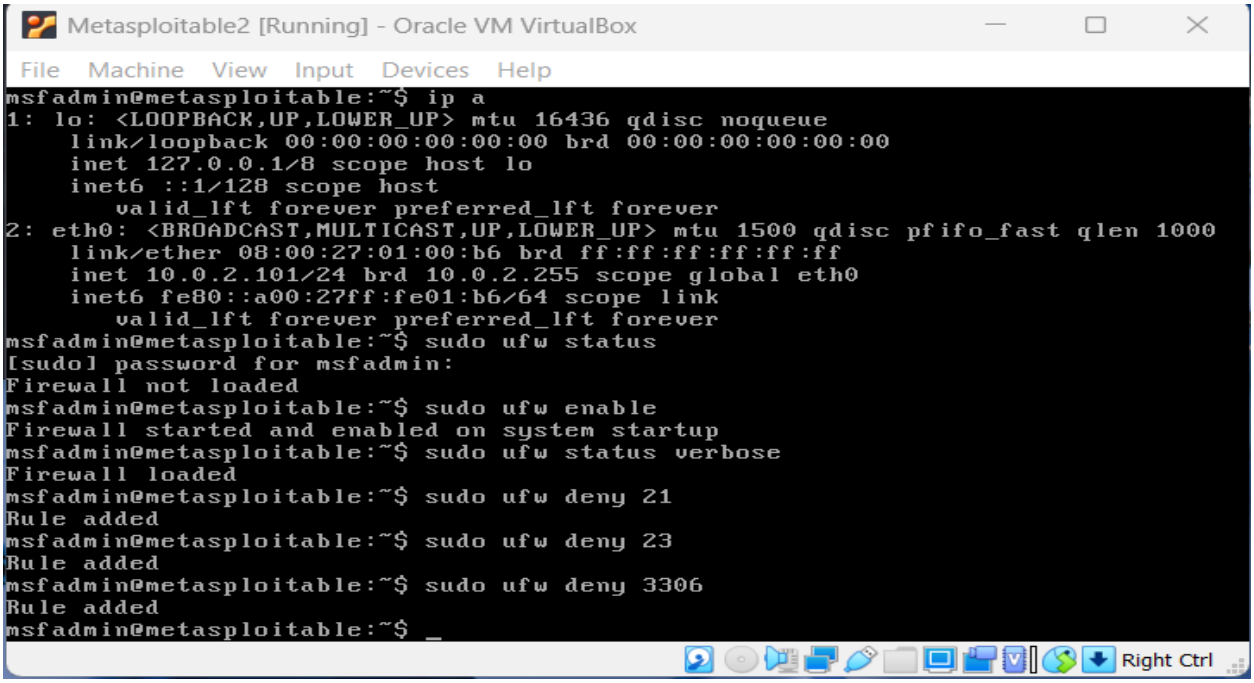
8. Secure some ports on Metasploitable and verify using Nmap:



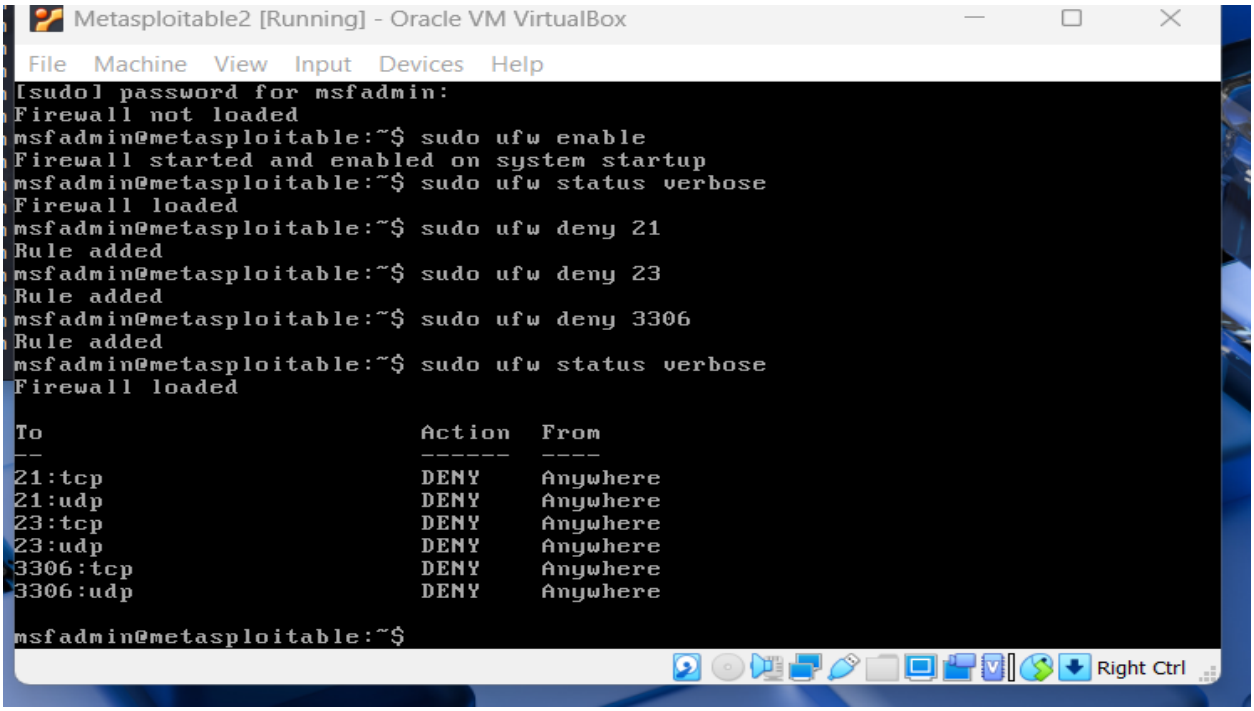
I nmaped the metasploitable and all of the ports where open



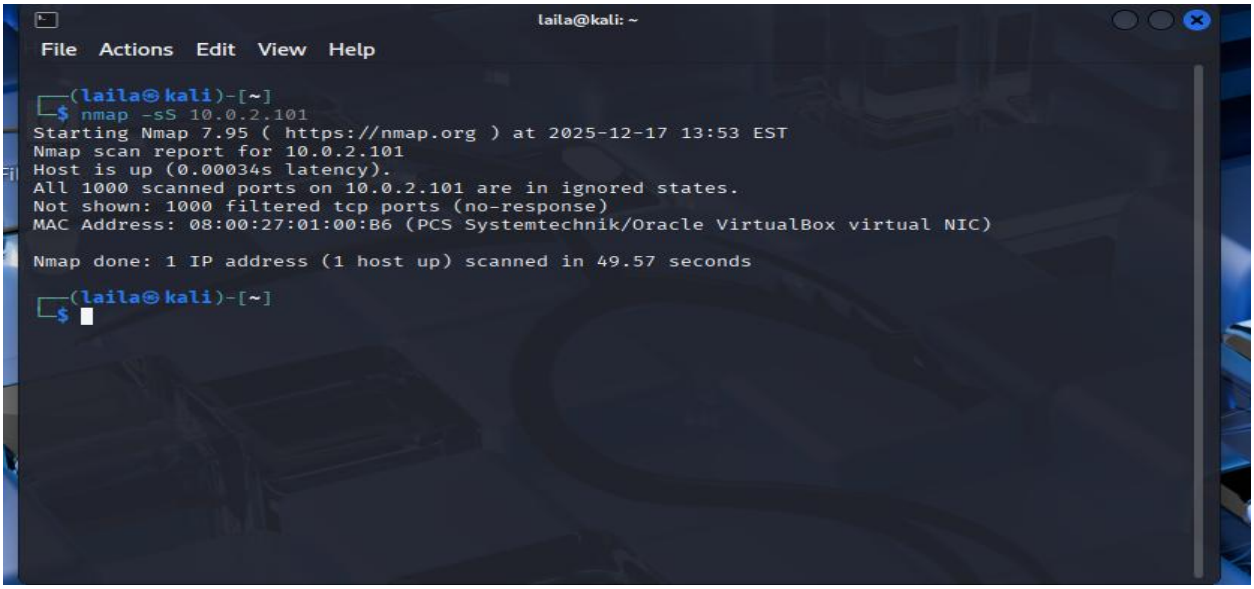
At first the firewall wasn't loaded but after that I started it



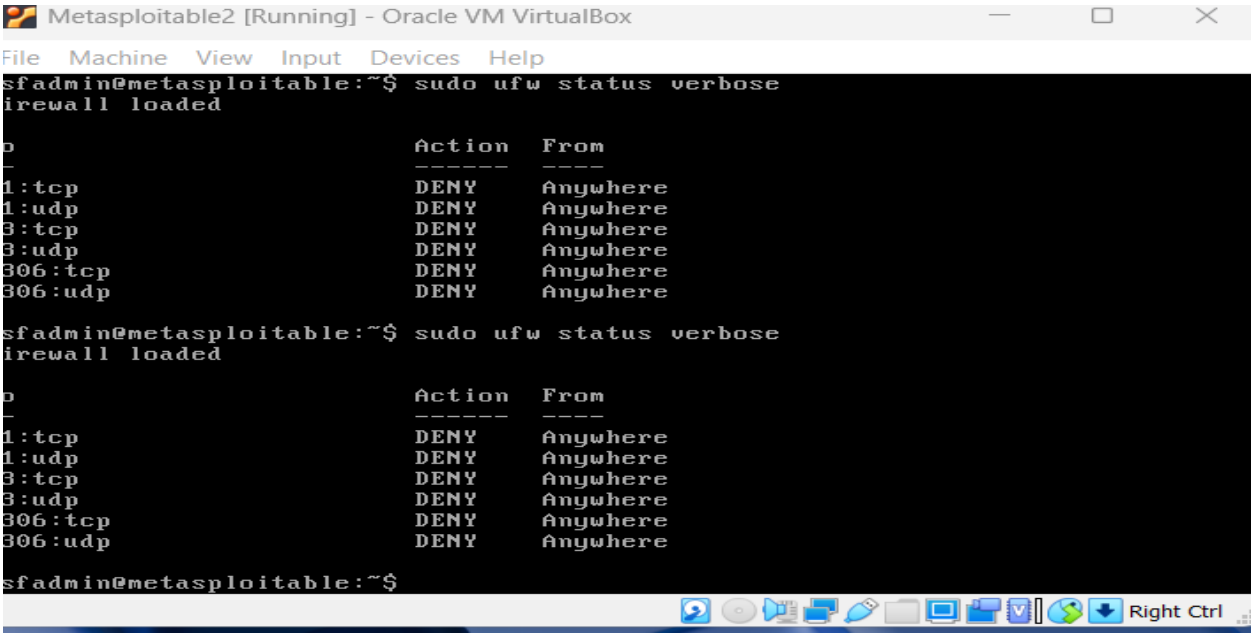
And to make sure I also added some rules for port 21,23 and 3306



And saw its status verbose : all of them their action are deny



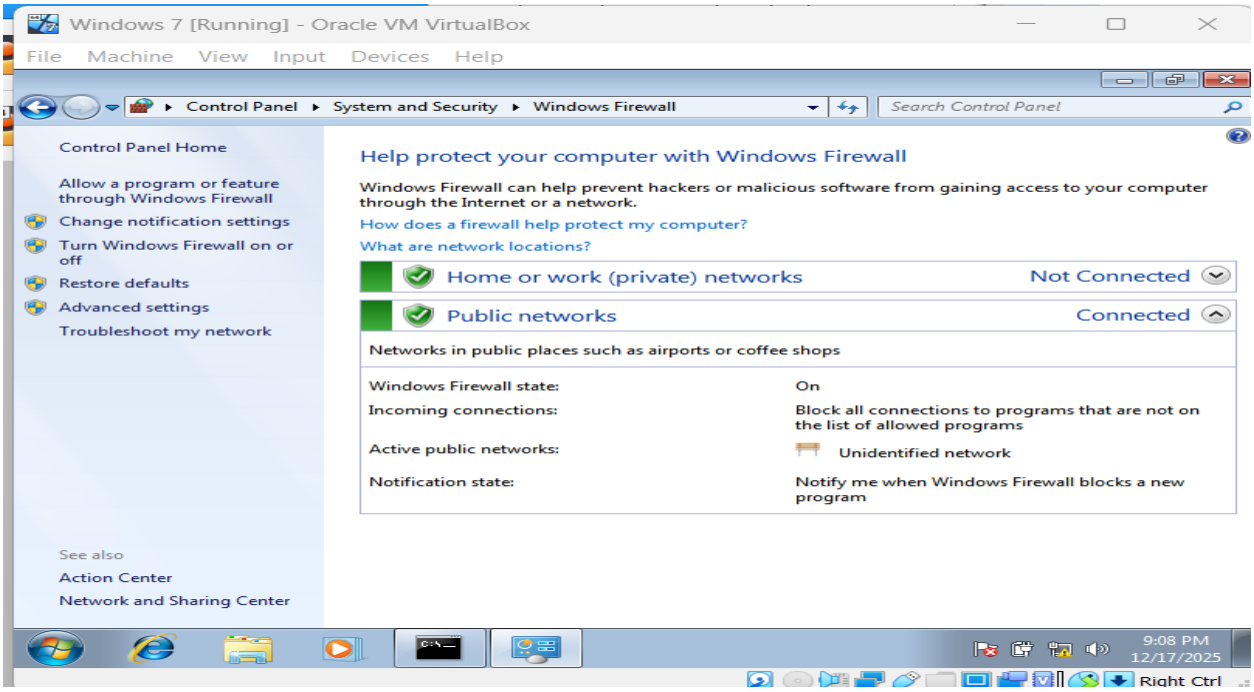
When I nmaped again from kali nth was opened!

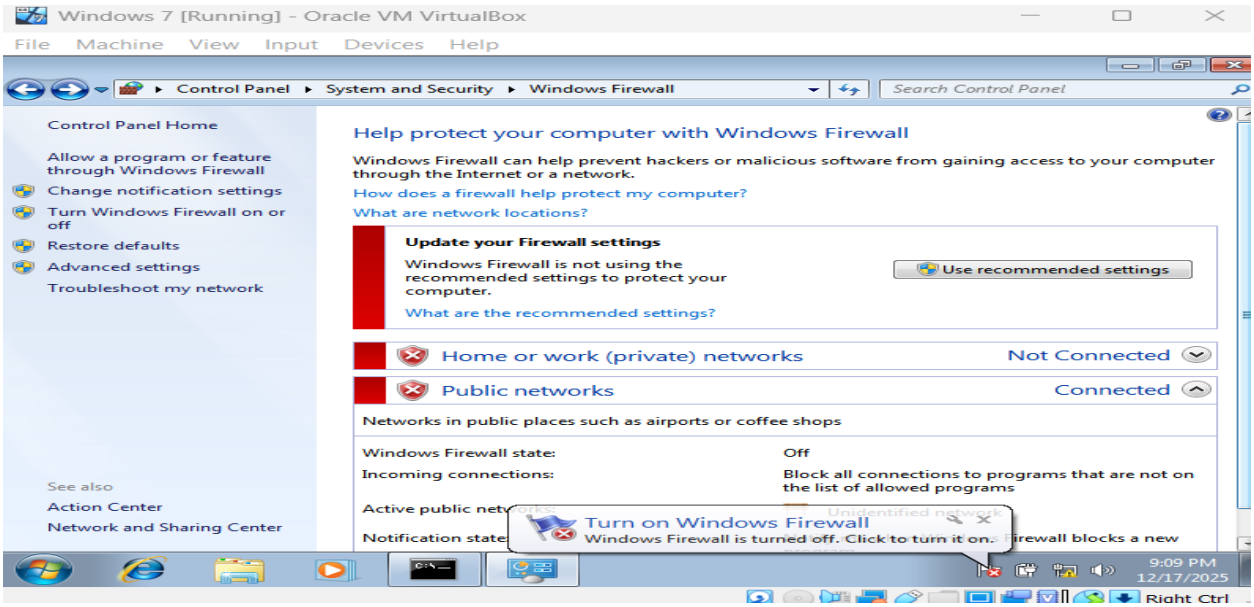


After I namped on kali I saw the status again it’s still denied

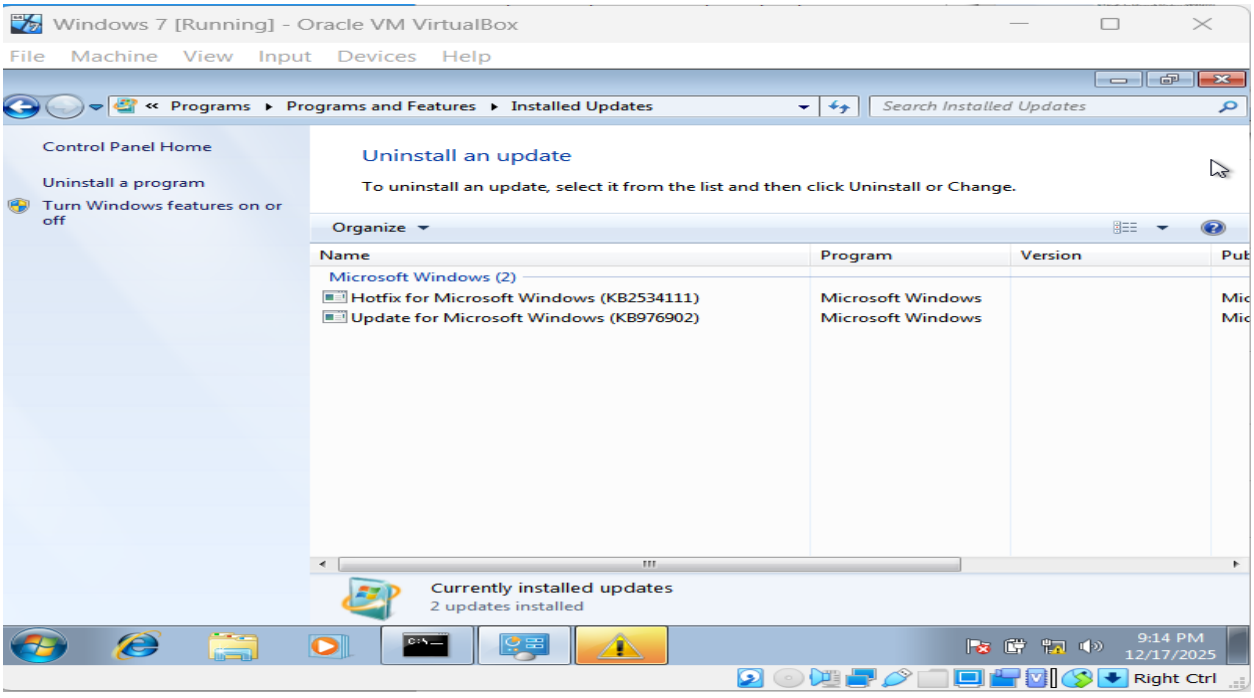
After enabling and configuring the firewall on the Metasploitable machine, a follow-up Nmap scan was performed from the Kali system. The scan results showed that all scanned ports were in a filtered state, indicating that the firewall was actively blocking incoming connections. This confirms that the applied firewall rules successfully secured the system services.

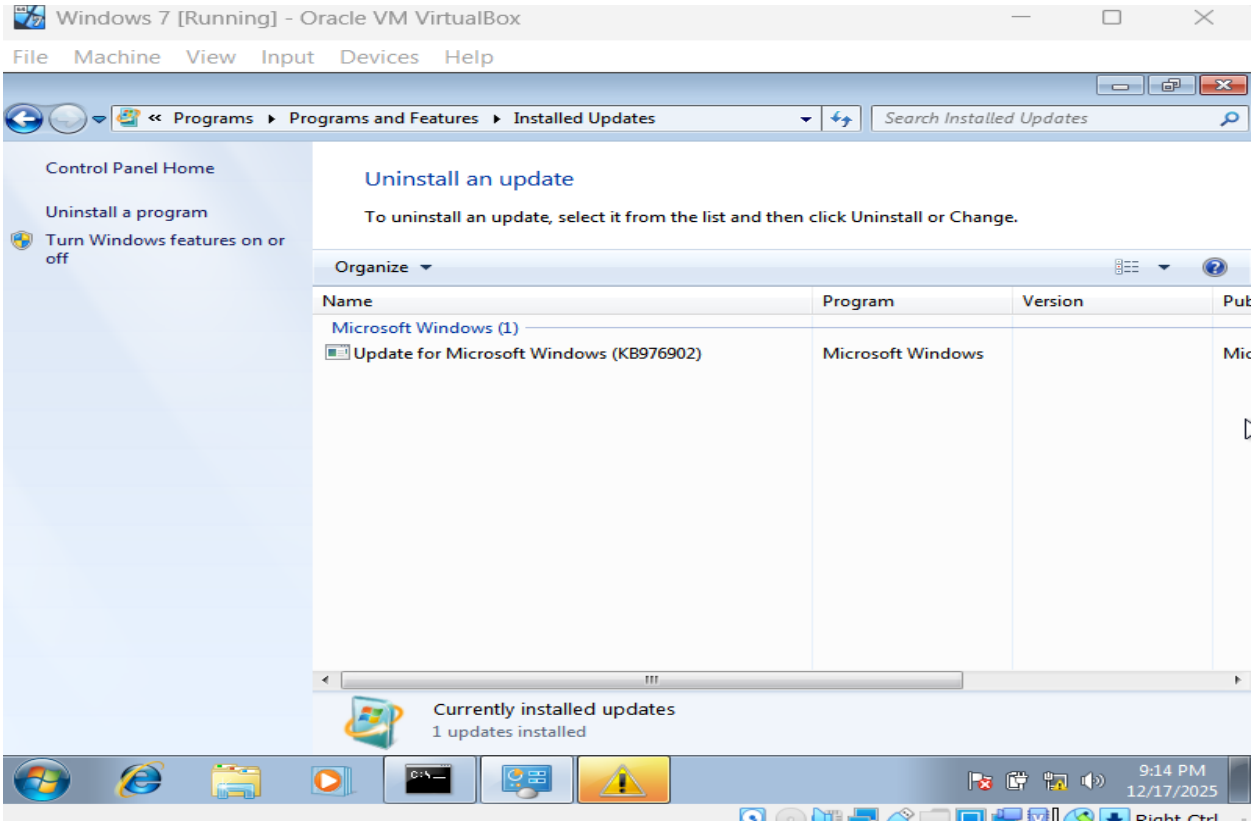
9. Apply the CVE-2017-0144 (EternalBlue):

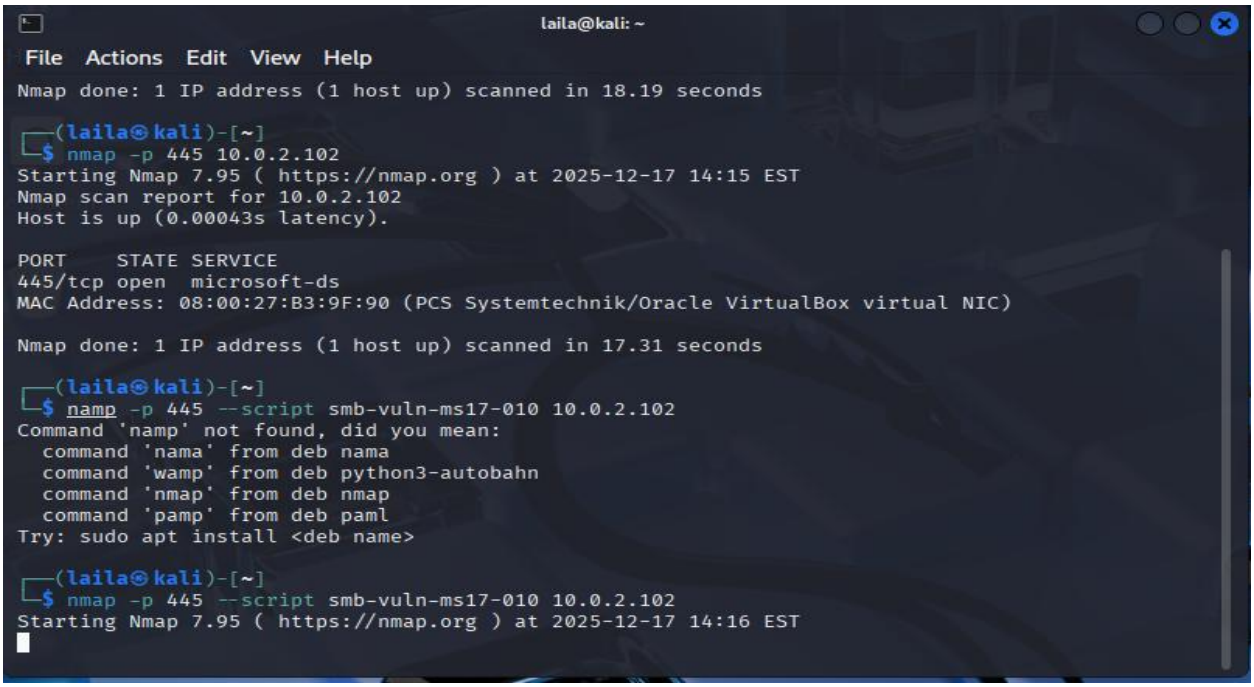


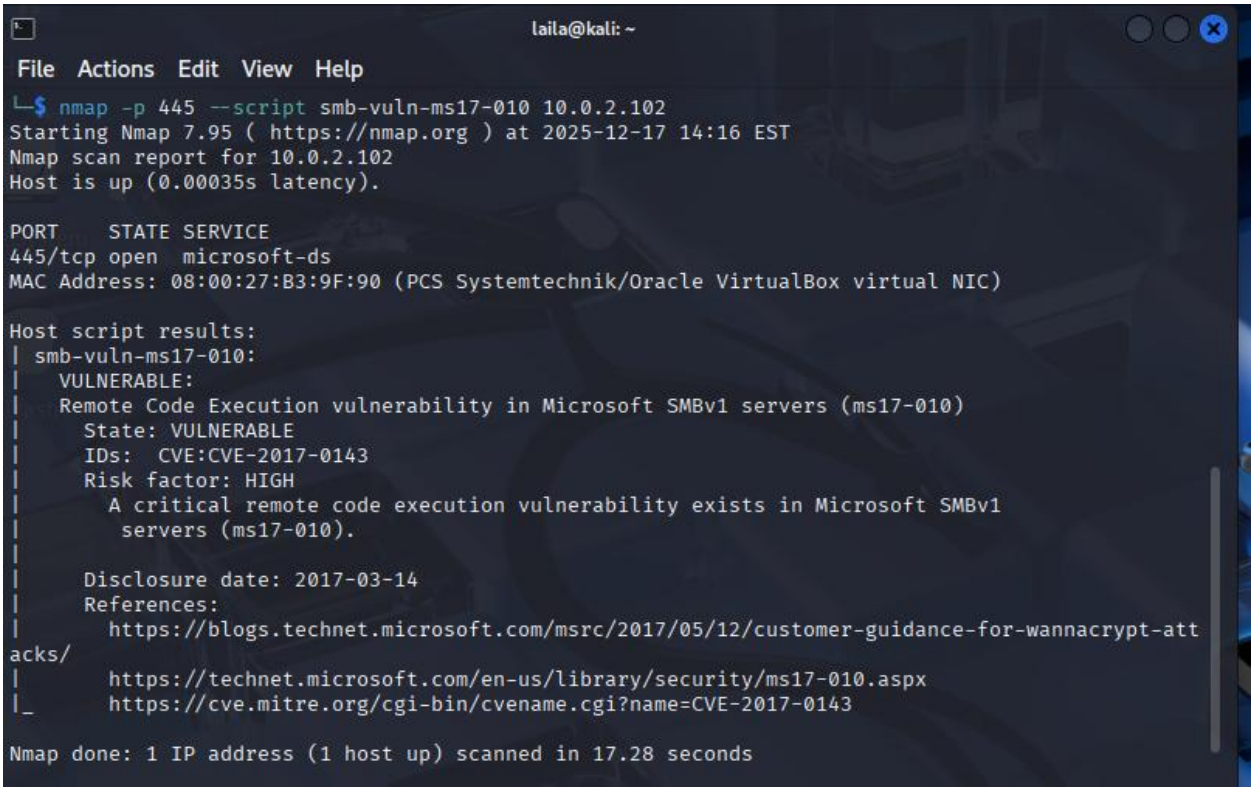


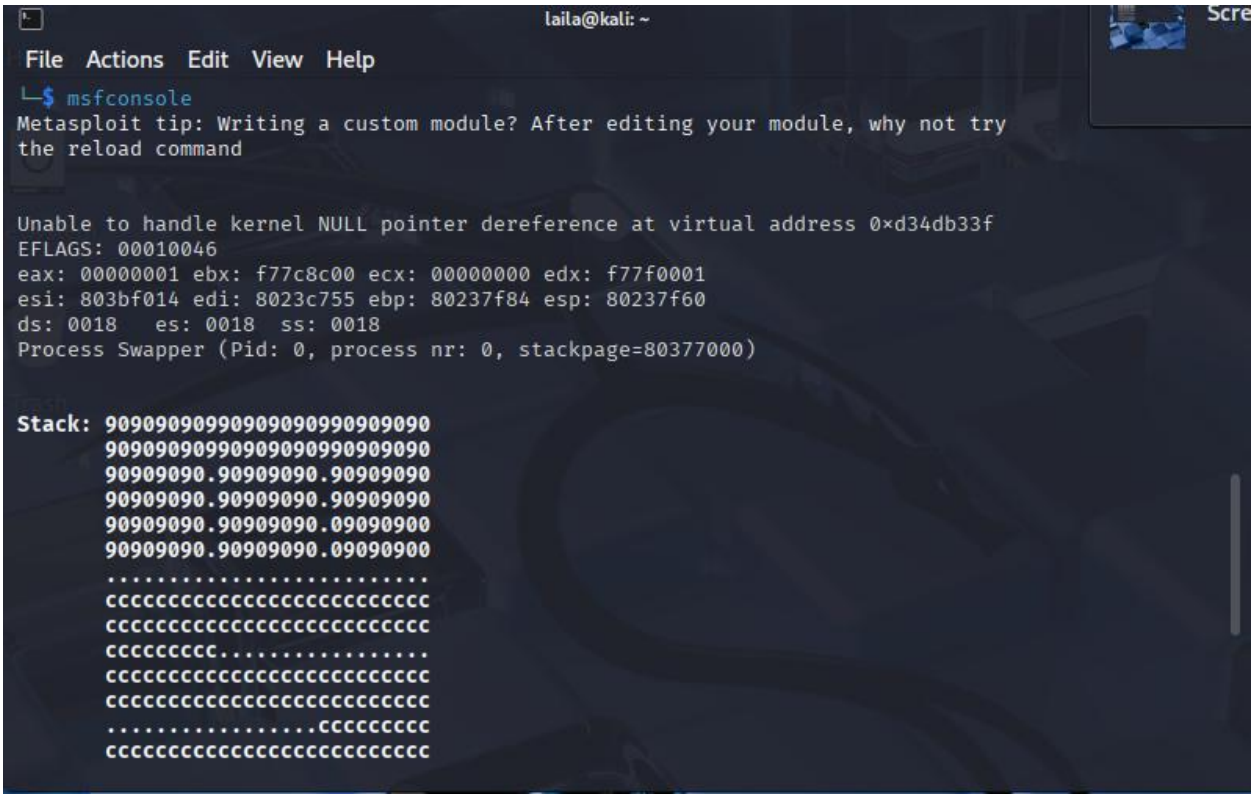

About Windows
Windows 7 Ultimate
Microsoft Windows
Version 6.1 (Build 7601: Service Pack 1)
Copyright © 2009 Microsoft Corporation. All rights reserved.
The Windows 7 Ultimate operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries.
This product is licensed under the Microsoft Software License Terms to:
Trump
OK

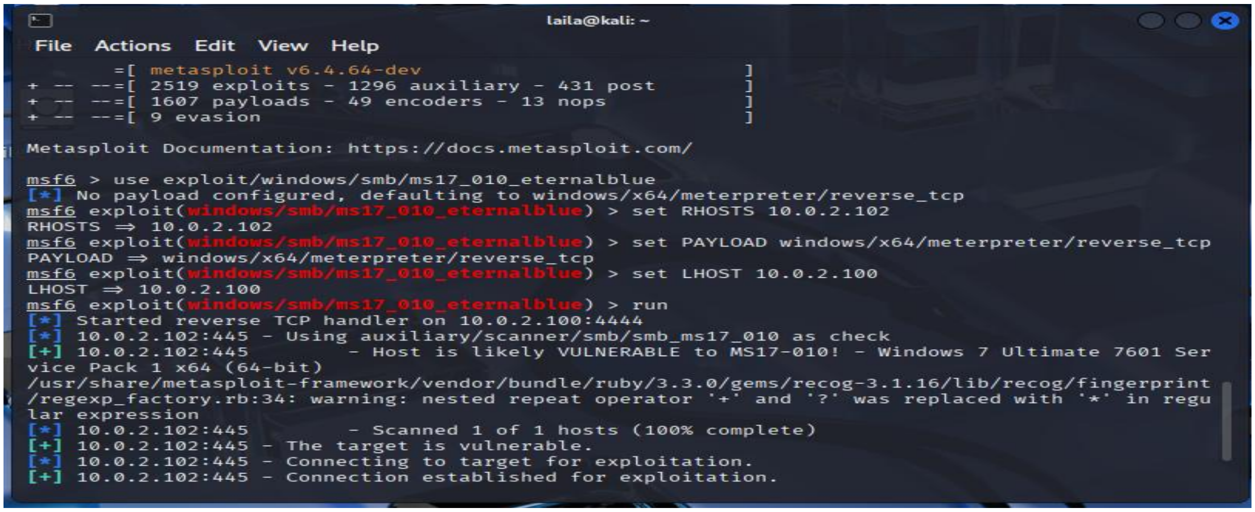

Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Programs ▸ Programs and Features ▸ Installed Updates
Search Installed Updates
Control Panel Home
Uninstall a program
Turn Windows features on or off
Uninstall an update
To uninstall an update, select it from the list and then click Uninstall or Change.
Organize
Name
Program
Version
Microsoft Windows (2)
Hotfix for Microsoft Windows (KB2534111)
Microsoft Windows
Update for Microsoft Windows (KB976902)
Microsoft Windows
Currently installed updates
2 updates installed
9:14 PM
12/17/2025
Right Ctrl

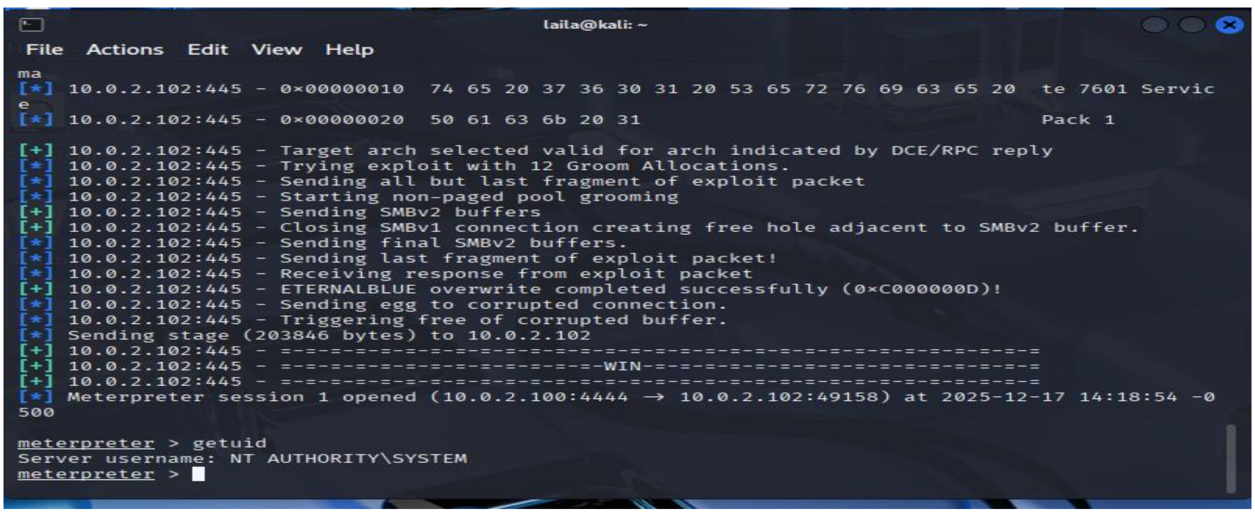

Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
« Programs ▸ Programs and Features ▸ Installed Updates
Search Installed Updates
Control Panel Home
Uninstall a program
Turn Windows features on or off
Uninstall an update
To uninstall an update, select it from the list and then click Uninstall or Change.
Organize
Name
Program
Version
Microsoft Windows (1)
Update for Microsoft Windows (KB976902)
Microsoft Windows
Currently installed updates
1 updates installed
9:14 PM
12/17/2025


laila@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 18.19 seconds
(laila㉿kali)-[~]
$ nmap -p 445 10.0.2.102
Starting Nmap 7.95 (https://nmap.org) at 2025-12-17 14:15 EST
Nmap scan report for 10.0.2.102
Host is up (0.00043s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:00:27:B3:9F:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
(laila㉿kali)-[~]
$ namp -p 445 --script smb-vuln-ms17-010 10.0.2.102
Command 'namp' not found, did you mean:
command 'nama' from deb nama
command 'wamp' from deb python3-autobahn
command 'nmap' from deb nmap
command 'pamp' from deb paml
Try: sudo apt install <deb name>
(laila㉿kali)-[~]
$ nmap -p 445 --script smb-vuln-ms17-010 10.0.2.102
Starting Nmap 7.95 (https://nmap.org) at 2025-12-17 14:16 EST


laila@kali: ~
File Actions Edit View Help
└─$ nmap -p 445 --script smb-vuln-ms17-010 10.0.2.102
Starting Nmap 7.95 (https://nmap.org) at 2025-12-17 14:16 EST
Nmap scan report for 10.0.2.102
Host is up (0.00035s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:00:27:B3:9F:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds


laila@kali: ~
File Actions Edit View Help
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
Stack: 90909090990909090990909090
90909090990909090990909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
ccccccccccccccccccccccccc
ccccccccccccccccccccccccc
cccccccccc.....
ccccccccccccccccccccccccc
ccccccccccccccccccccccccc
.....cccccccccc
ccccccccccccccccccccccccc





Using the Metasploit Framework, the MS17-010 (CVE-2017-0144 – EternalBlue) vulnerability was exploited against a Windows 7 Ultimate machine. After disabling the firewall and confirming SMB service availability on port 445, the system was found to be vulnerable. The exploit successfully resulted in a Meterpreter session with NT AUTHORITY\SYSTEM privileges, demonstrating complete system compromise. This confirms the severity of the EternalBlue vulnerability on unpatched Windows systems.