Alex Lutz 5/17/2025

Exploiting a Vulnerable VM in a Safe Lab (Kali Linux + Metasploitable)

Lab Setup Overview

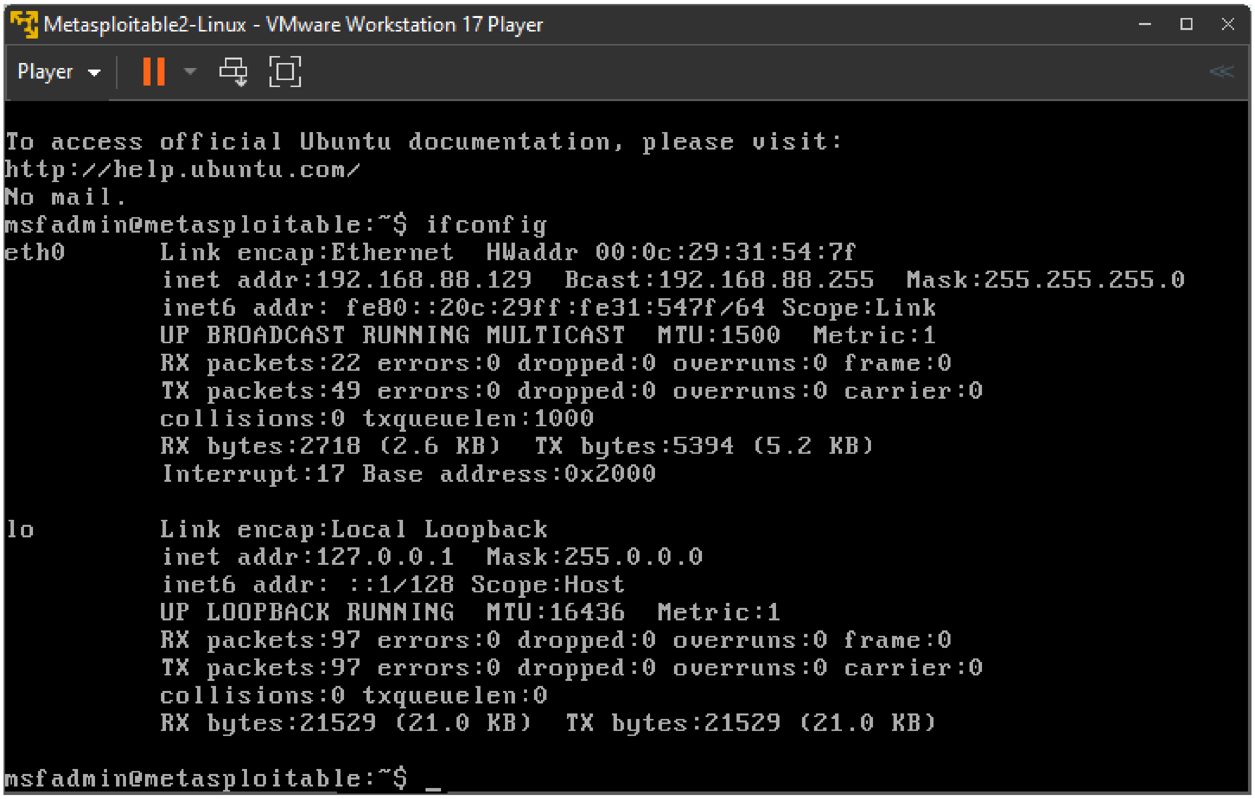
Host System	**Windows Surface Laptop**
Hypervisor	**VMware Workstation Player**
Attacker VM	**Kali Linux**
Target VM	**Metasploitable 2**

Lab Steps Taken

1. **Install and Configure Virtual Machines**

- Installed Kali Linux and Metasploitable
- Set both of the virtual machines to **Host-Only network adapter** which contains lab

2. **Get IP Address of Metasploitable**

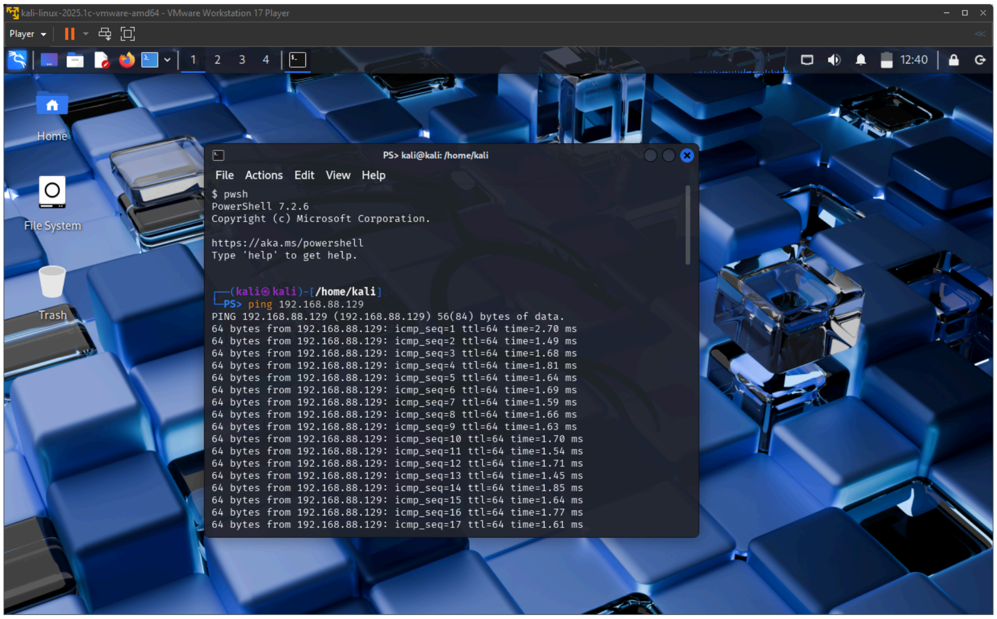


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:54:7f
          inet addr:192.168.88.129  Bcast:192.168.88.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe31:547f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2718 (2.6 KB)  TX bytes:5394 (5.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$ _
```

- Booted Metasploitable
- Logged in with **Username: msfadmin**

  Password: msfadmin
- Ran the **ifconfig** command

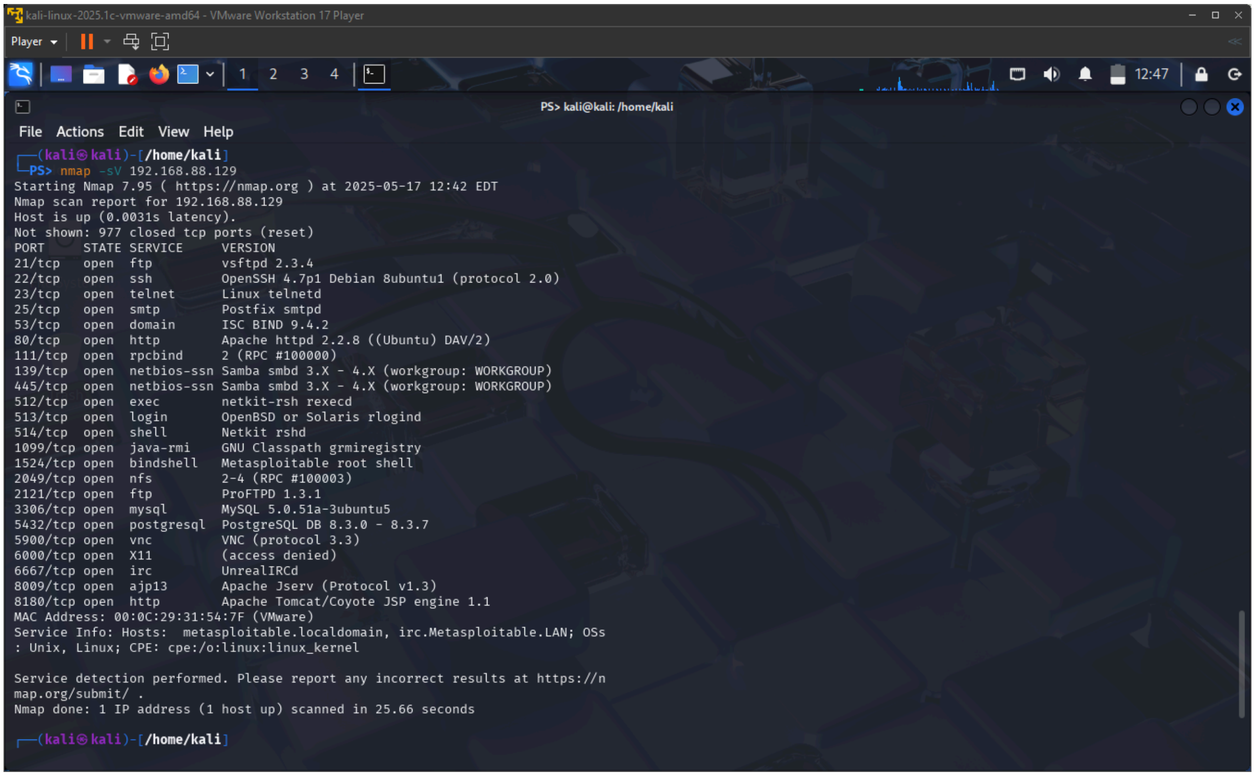
3. **Ping Target from Kali Linux**


kali-linux-2025.1c-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
12:40
Home
File System
Trash
PS> kali@kali: /home/kali
File Actions Edit View Help

```
$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


┌──(kali㉿kali)-[/home/kali]
└─PS> ping 192.168.88.129
PING 192.168.88.129 (192.168.88.129) 56(84) bytes of data.
64 bytes from 192.168.88.129: icmp_seq=1 ttl=64 time=2.70 ms
64 bytes from 192.168.88.129: icmp_seq=2 ttl=64 time=1.49 ms
64 bytes from 192.168.88.129: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.88.129: icmp_seq=4 ttl=64 time=1.81 ms
64 bytes from 192.168.88.129: icmp_seq=5 ttl=64 time=1.64 ms
64 bytes from 192.168.88.129: icmp_seq=6 ttl=64 time=1.69 ms
64 bytes from 192.168.88.129: icmp_seq=7 ttl=64 time=1.59 ms
64 bytes from 192.168.88.129: icmp_seq=8 ttl=64 time=1.66 ms
64 bytes from 192.168.88.129: icmp_seq=9 ttl=64 time=1.63 ms
64 bytes from 192.168.88.129: icmp_seq=10 ttl=64 time=1.70 ms
64 bytes from 192.168.88.129: icmp_seq=11 ttl=64 time=1.54 ms
64 bytes from 192.168.88.129: icmp_seq=12 ttl=64 time=1.71 ms
64 bytes from 192.168.88.129: icmp_seq=13 ttl=64 time=1.45 ms
64 bytes from 192.168.88.129: icmp_seq=14 ttl=64 time=1.85 ms
64 bytes from 192.168.88.129: icmp_seq=15 ttl=64 time=1.64 ms
64 bytes from 192.168.88.129: icmp_seq=16 ttl=64 time=1.77 ms
64 bytes from 192.168.88.129: icmp_seq=17 ttl=64 time=1.61 ms
```

- Started Kali Linux and confirmed connectivity in the terminal
- Ran a ping command using the Metasploitable custom IP

4. **Scan Metasploitable for Vulnerabilities**


kali-linux-2025.1c-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
12:47
PS> kali@kali: /home/kali
File Actions Edit View Help

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -sV 192.168.88.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 12:42 EDT
Nmap scan report for 192.168.88.129
Host is up (0.0031s 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: 00:0C:29:31:54:7F (VMware)
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds

┌──(kali㉿kali)-[/home/kali]
```

- Ran the command to scan, **nmap -sV [Metasploitable IP]**

5. **Launch Metasploit Framework**

- Opened Metasploit in Kali Linux with the **msfconsole** command

6. **Using a Known Backdoor Exploit**

- Attempted to use **exploit/unix/ftp/vsftpd_234_backdoor** using the **RHOSTS** value
- While the exploit did not result in an active session, it provided exposure to the workflow of module selection by setting payload options and executing exploit attempts using Metasploit

Post Lab Completion Recap

While I wasn't able to successfully run the exploits on the target system, this lab provided great hands-on experience with penetration testing, setting up virtual environments, and simulating ethical hacking. This can be applied to proper configuration within network infrastructure and is essential to have a foundation in identifying vulnerabilities before they become exploited by real attackers. The entire process also encouraged me to continue troubleshooting as I came across errors in my commands, maintaining persistence which is a crucial skill for any Cybersecurity professional to have in this field.

Overall, this exercise strengthened my practical understanding of attack vectors and identifying risks while providing me experience with real-world security tools like Kali Linux and Metasploit. I look forward to building on this practice for the future as I continue to grow with these projects.