Week 1: Introduction to Cybersecurity and Virtualization

Name: V. Risvanth

1. Virtualisation Software Setup:

To enable the execution of multiple operating systems, virtualization platform was installed. The following software options were considered:

Installation Steps:

1. Downloaded VirtualBox from the official website (https://www.virtualbox.org/).
2. Installed VirtualBox and ensured all necessary extensions were added for compatibility.

2. Kali Linux Setup:

Steps to Install Kali Linux:

1. Downloaded the **Kali Linux ISO** from the official website (https://www.kali.org/get-kali/).
2. Created a new virtual machine in VirtualBox:
    - **RAM:** 4GB
    - **Storage:** 50GB (Dynamically Allocated)
3. Attached the **Kali Linux ISO** to the virtual machine.
4. Installed Kali Linux with default settings.
5. Updated the system and installed necessary tools:

3. **Metasploitable 2 Setup:**

Steps to Install Metasploitable 2:

1. Downloaded **Metasploitable 2** from https://sourceforge.net/projects/metasploitable/.
2. Created a new virtual machine in VirtualBox:
    - **RAM:** 512MB
    - **Storage:** 8GB (Dynamically Allocated)
3. Attached the **Metasploitable 2 VMDK file** to the VM.

4. Logged in using the default credentials:
    - **Username:** msfadmin
    - **Password:** msfadmin

4. Network Configuration:

To allow communication between Kali Linux and Metasploitable, the following networking setup was used:

- **Network Adapter Type:** Bridged Adapter (Preferred) or NAT Network
- Ensured both VMs received IP addresses in the same subnet.

5. Initial Reconassiance:

Using **Nmap**, a scan was performed to identify open ports and services:
Key Findings:

- Open Ports: **21 (FTP), 22 (SSH), 80 (HTTP), 3306 (MySQL)**
- Detected **vsFTPd 2.3.4**, known to have a backdoor vulnerability.

6. Security Assessment & Exploitation:

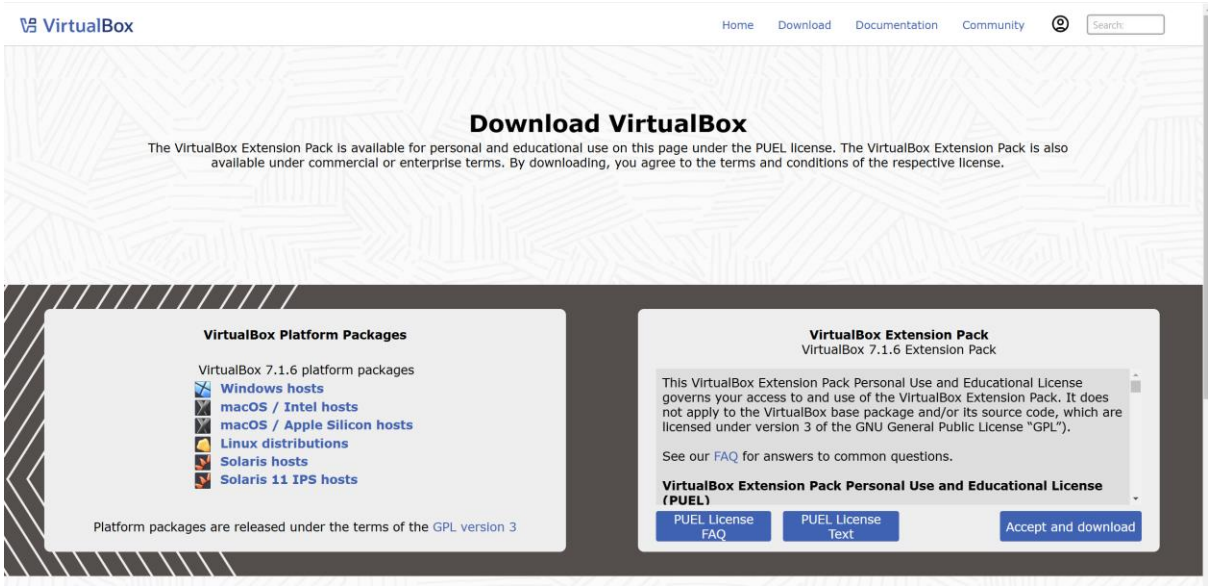
Using Metasploit, an attempt was made to exploit vsFTPd 2.3.4:
Step 1: Launch Metasploit Framework
Step 2: Select and Configure Exploit
Step 3: Verify Exploitation

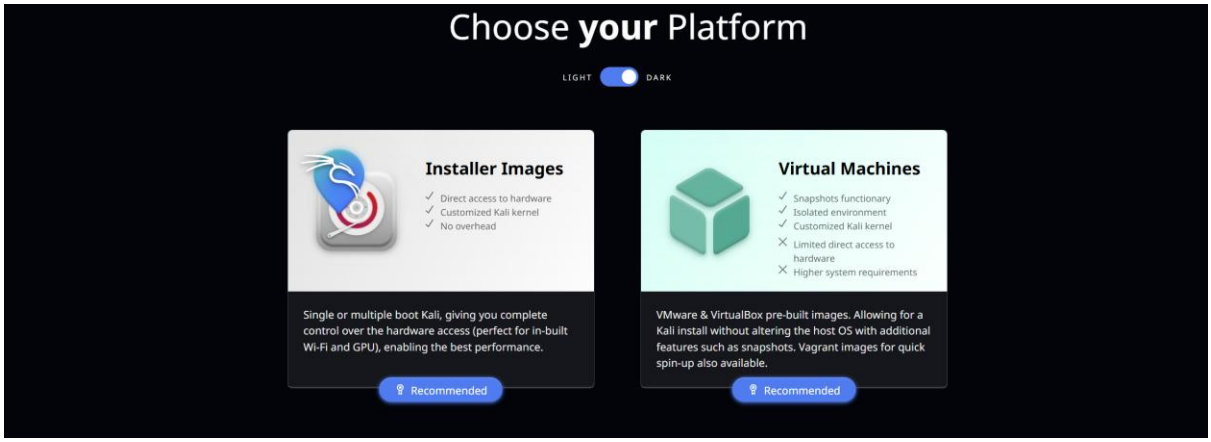
7. Clean Up and Backup:

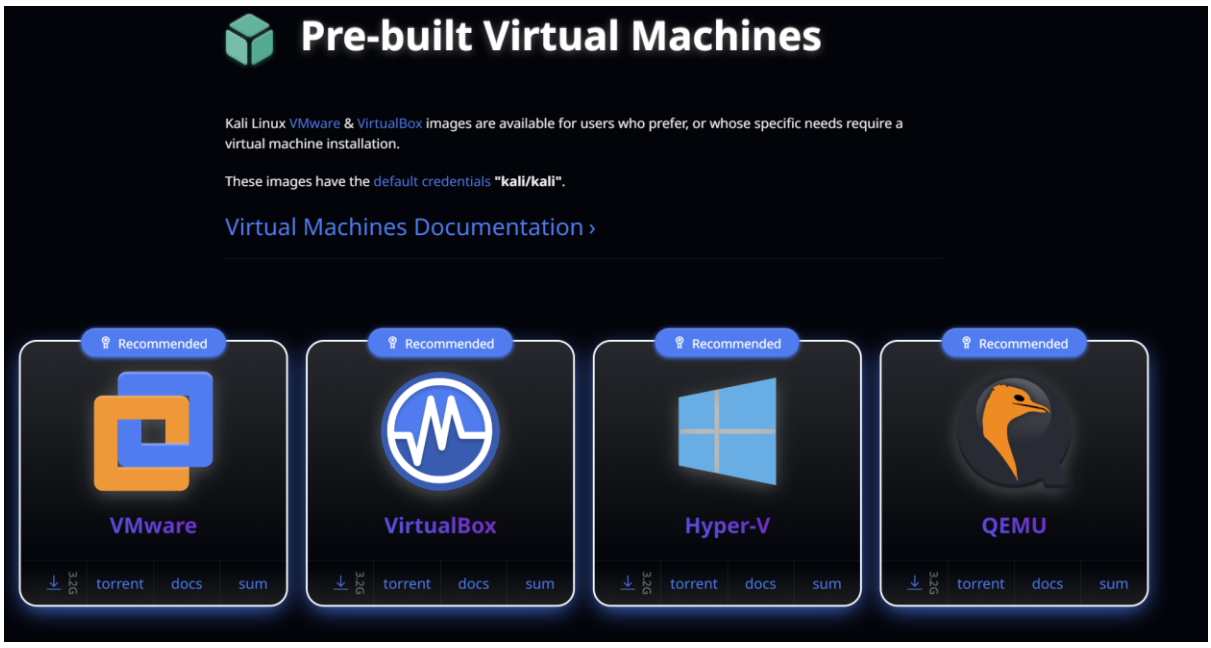
● Regularly take snapshots of your virtual machines to preserve the lab state.

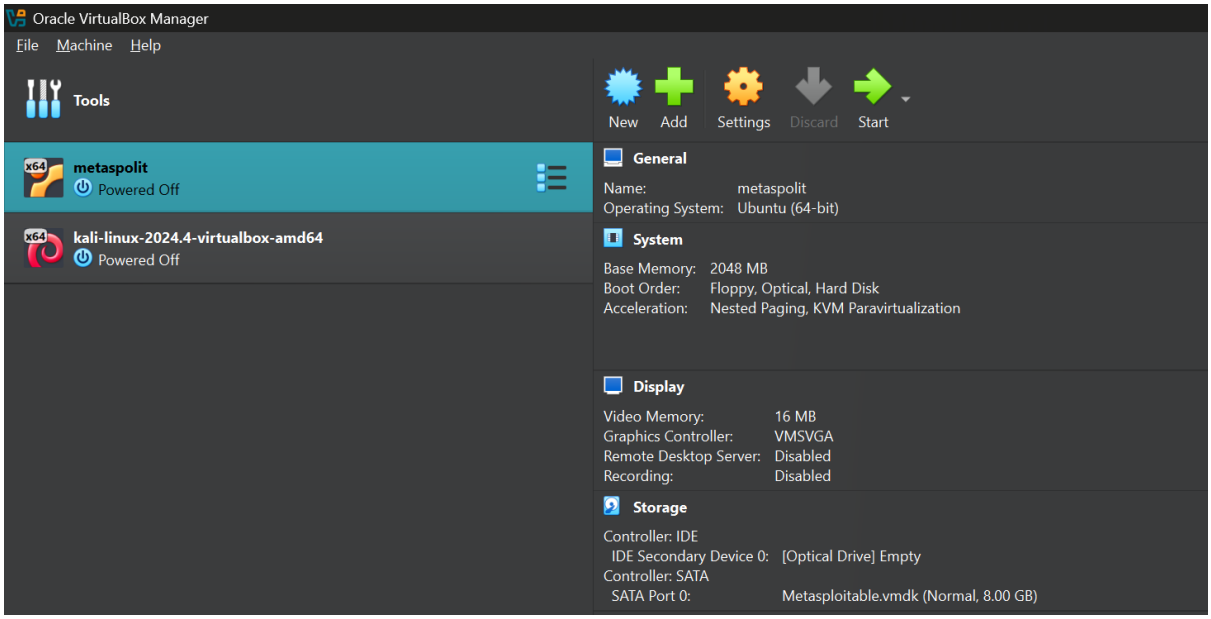
● Clean up any unnecessary files or data to keep your lab environment organized.

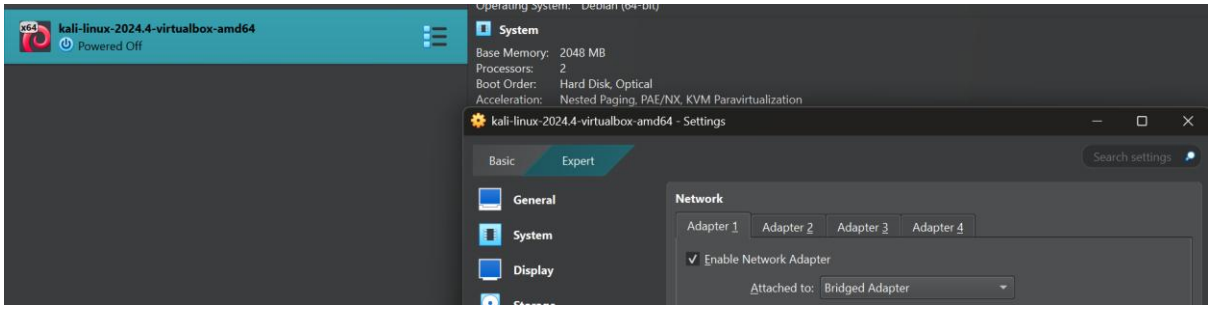
Screenshots:

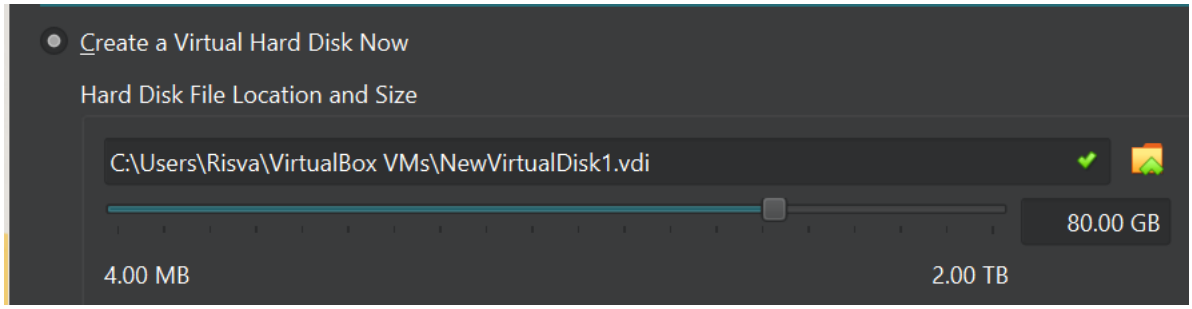







Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
metaspolit
Powered Off
kali-linux-2024.4-virtualbox-amd64
Powered Off
General
Name: metaspolit
Operating System: Ubuntu (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)

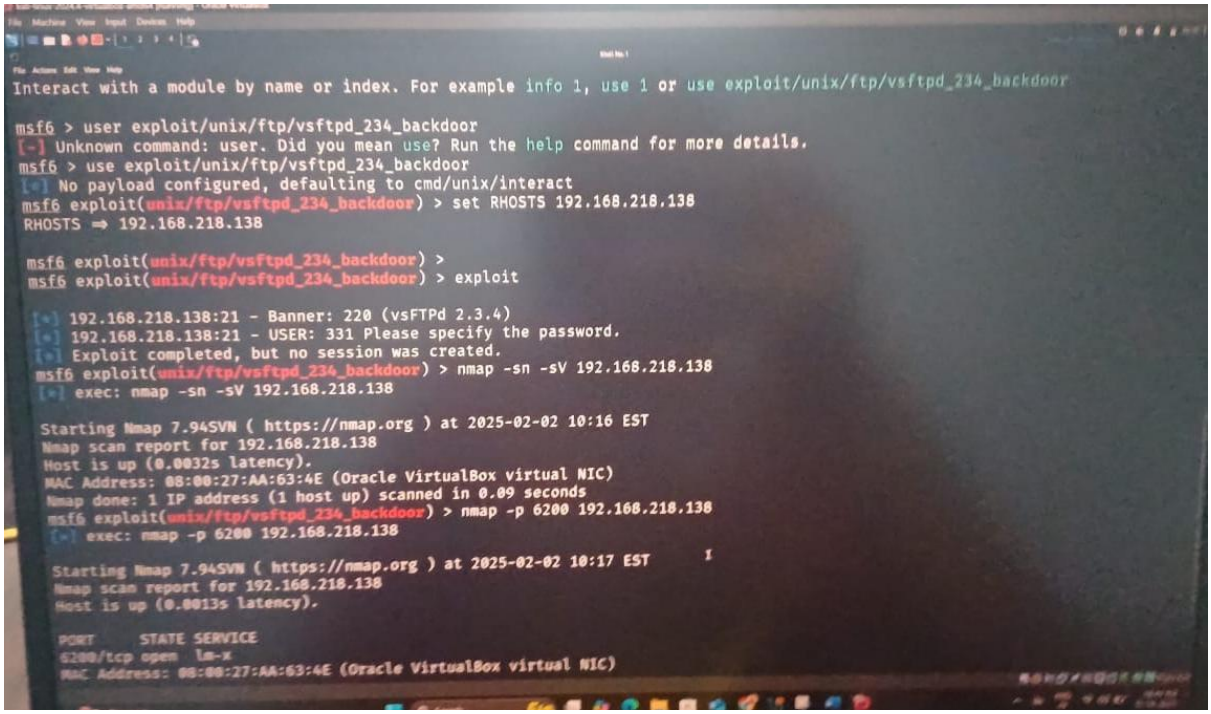

kali-linux-2024.4-virtualbox-amd64
Powered Off
System
Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
kali-linux-2024.4-virtualbox-amd64 - Settings
Basic Expert
Search settings
General
System
Display
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter

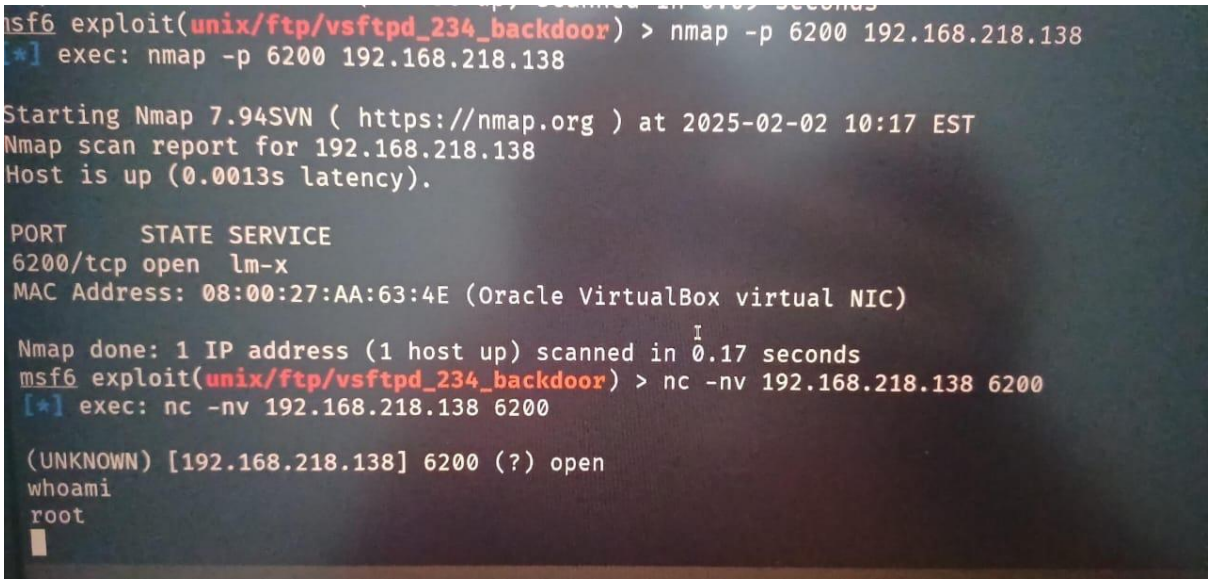

Create a Virtual Hard Disk Now
Hard Disk File Location and Size
C:\Users\Risva\VirtualBox VMs\NewVirtualDisk1.vdi
80.00 GB
4.00 MB
2.00 TB

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:aa:63:4e
          inet addr:192.168.218.138  Bcast:192.168.218.255  Mask:255.255.255.0
          inet6 addr: 2401:4900:4ded:752d:a00:27ff:feaa:634e/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feaa:634e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4782 (4.6 KB)  TX bytes:7554 (7.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ _
```

```
msf6 > nmap -sV 192.168.218.138
[*] exec: nmap -sV 192.168.218.138

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-02 10:13 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 10:13 (0:00:00 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 10:14 (0:00:02 remaining)
Nmap scan report for 192.168.218.138
Host is up (0.011s 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
514/tcp  open  tcpwrapped
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
```

```
Matching Modules

#  Name                                  Disclosure Date  Rank       Check  Description
-  ----                                  ---------------  ----       -----  -----------
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 Exe
```





Conclusion:

This report outlines the successful setup of a penetration testing lab, including virtualization, network configuration, reconnaissance, and exploitation

---