Week 4: Hacking using Metasploitable 2

Install virtual box in Windows

1. Go to the official website and download the latest version of Virtual box.
2. Select path to install virtual box.
3. Tick create entries and shortcut option.
4. Click ready to install
5. Select install files and packages
6. Select install certificate
7. Finish Installation

Install Kali Linux in Virtual Box

1. Open VirtualBox and select "New".
2. Configure Settings under "Advanced Tab" -> "Hard Disk" ->Increase number of CPU cores and RAM size for smooth function.
3. After clicking on "Create", the wizard is complete.
4. Then select start to start the kali linux.
   Username: kali
   Password: kali

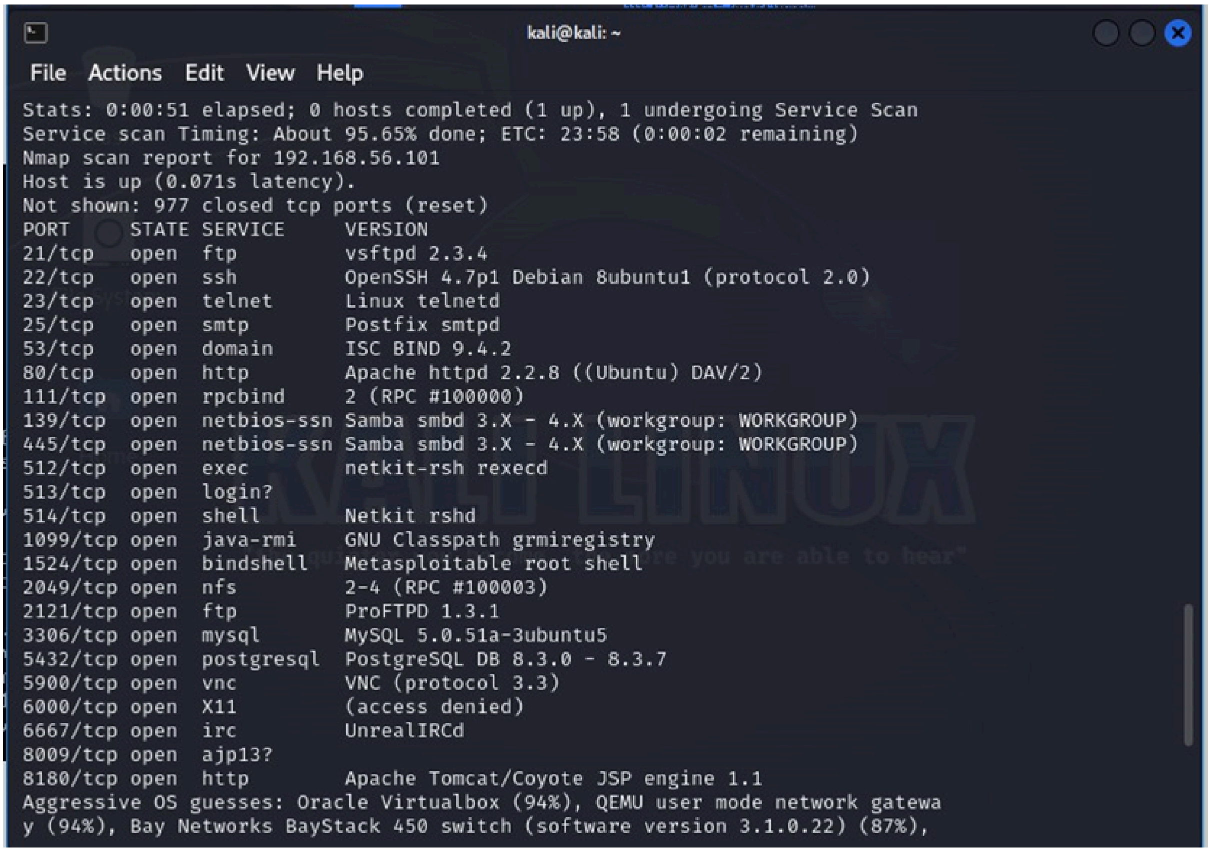
Installing Metasploit 2 in Virtual Box

1. Import the Metasploitable 2 VM image, adjust setting if necessary,
2. Configure Settings: Change network adapter to "Host-Only" click "OK" to save changes.
3. To start Metasploitable 2, select the VM in VirtualBox and click the "Start" button, initiating the boot process and displaying a console window with the VM's startup sequence.

4. After the boot process finishes, a login screen will appear where the username: "msfadmin" and password: "msfadmin".

Nmap scan using Metasploitable 2

1. Open the Kali VM, launch the VirtualBox and start the Kali VM instance.
2. In Kali VM, open a terminal and execute either "***sudo dhclient***" or "***ifconfig***" command to obtain the IP address of the Metasploitable 2 system.
3. First, obtain the IP address of the Metasploitable 2 system. Then, open a terminal on the Kali VM. Next, scan using Nmap command "***sudo nmap -sV -O <ipaddress>*** ".
    - ❖ "-O" option is used to determine the operating system of the target system.
    - ❖ "-sV" option is to know the version of services running on the scanned ports.



```
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 23:58 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.071s 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  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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gatewa
y (94%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%),
```