CEH - SCANNING

Configuration:

Your machine is HACKER, running Windows XP Professional.
The IP address of your machine is **192.168.100.66/24**.
Your target machines are :

1. WIN2000, running Windows 2000
   IP address is **192.168.100.2/24**.
2. WIN2003, running Windows 2003
   IP address is **192.168.100.1/24**.

Objectives:

1. Gather some vital information from your target system that will help you to proceed to the next steps in hacking.
2. Identify your target system and find any vulnerability related.

Tools:

Nmap v5.0
Nessus v4.0

Preparation:

Ensure that HACKER, WIN2003 and WIN2000 virtual machines are connected.

Logon to HACKER virtual machine and test connectivity between these machines by using PING command.

I. PORT SCANNING

Scanning with Nmap

Detailed Steps:

1. On the HACKER virtual machine, open a command prompt. Navigate to **C:\tools\Nmap** directory and run this command:

```
C:\tools\Nmap> nmap 192.168.100.2

Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-08 23:49
SE Asia Standard Time

Interesting ports on 192.168.100.2:
Not shown: 989 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1033/tcp open  netinfo
3372/tcp open  msdtc
MAC Address: 00:0C:29:62:C0:70 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.34 seconds
```

2. Now try to run Nmap without any option to see commands explanation. Use other Nmap scanning options, examines the results and see the differences.
   Examples:

```
C:\tools\Nmap> nmap | more
C:\tools\Nmap> nmap –O 192.168.100.2
C:\tools\Nmap> nmap –A 192.168.100.2
C:\tools\Nmap> nmap –sS –O 192.168.100.2
```

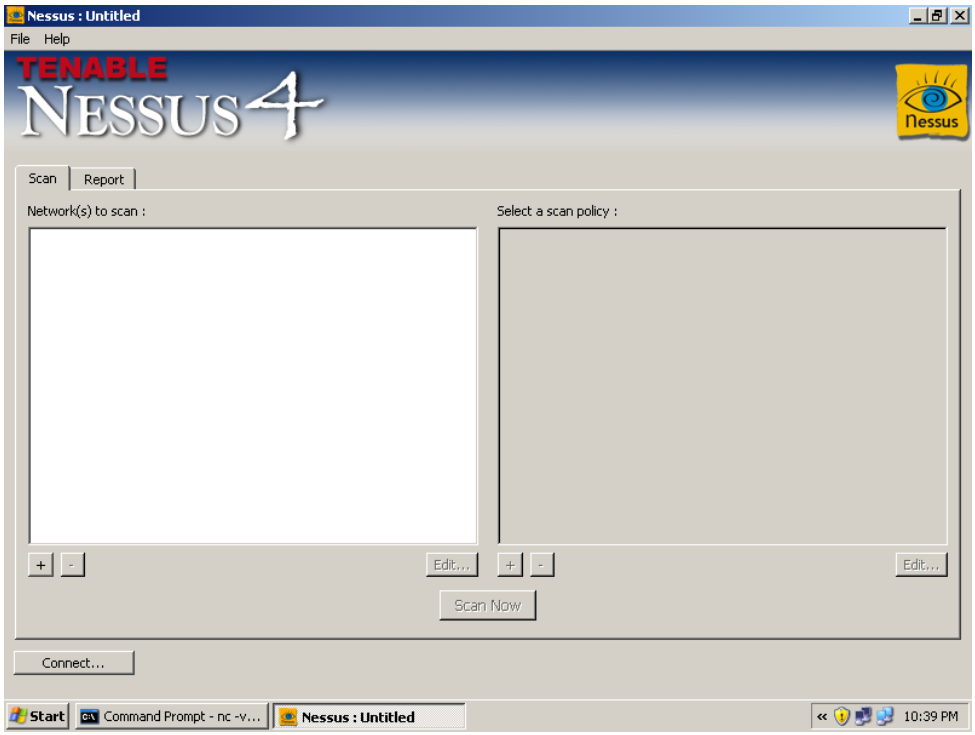
3. Try to scan WIN2003 machine.

II. VULNERABILITY SCANNING

Scanning with Nessus

Detailed Steps:

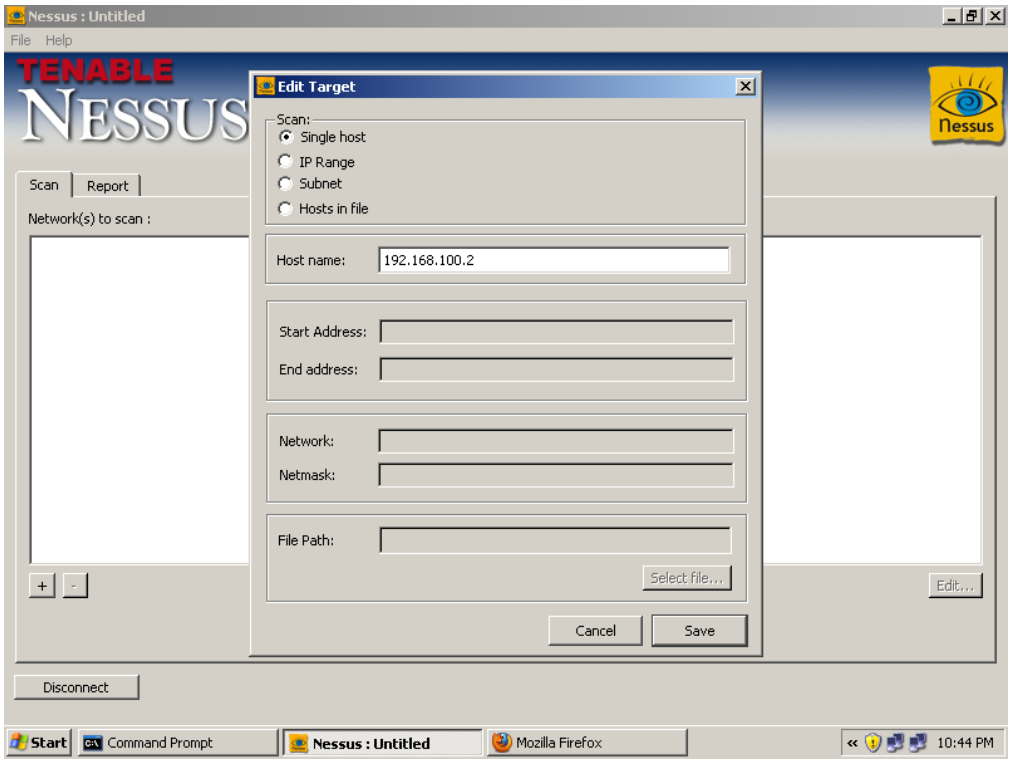
1. In the HACKER machine, navigate to **" Start - Programs - Tenable Network Security - Nessus - Nessus Client "**



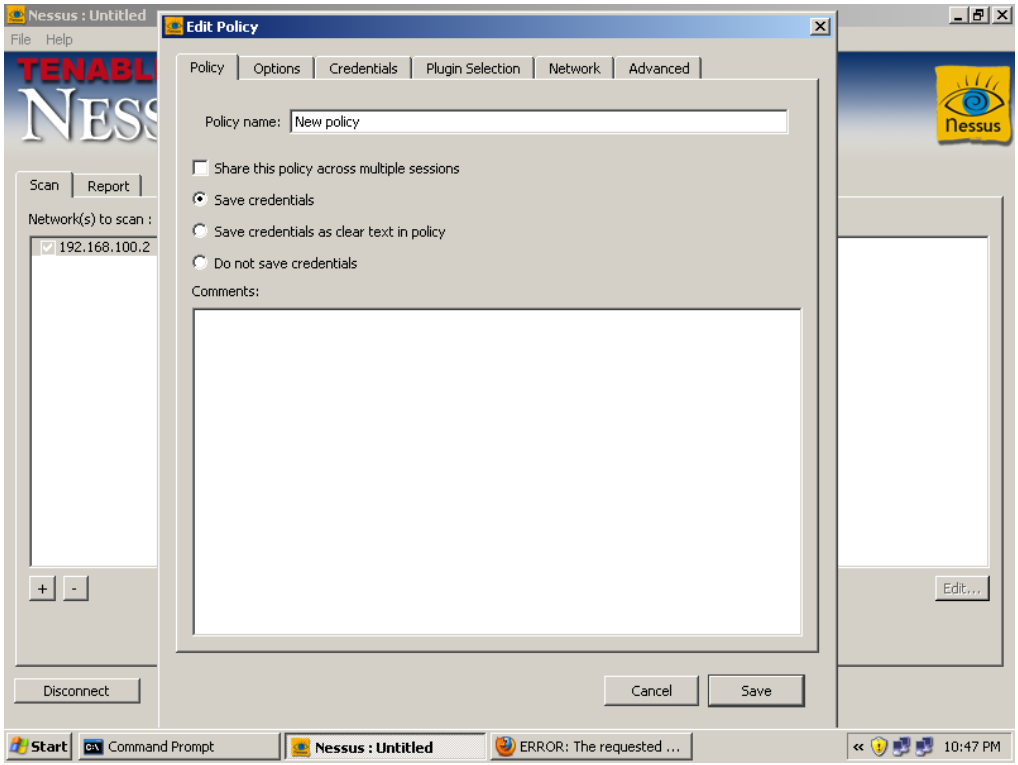
2. Click on the ' Connect… ' button to connect to nessus server, then select 'localhost', then press 'Connect'.

3. Click on the **+** sign , in the 'network(s) to scan' column.

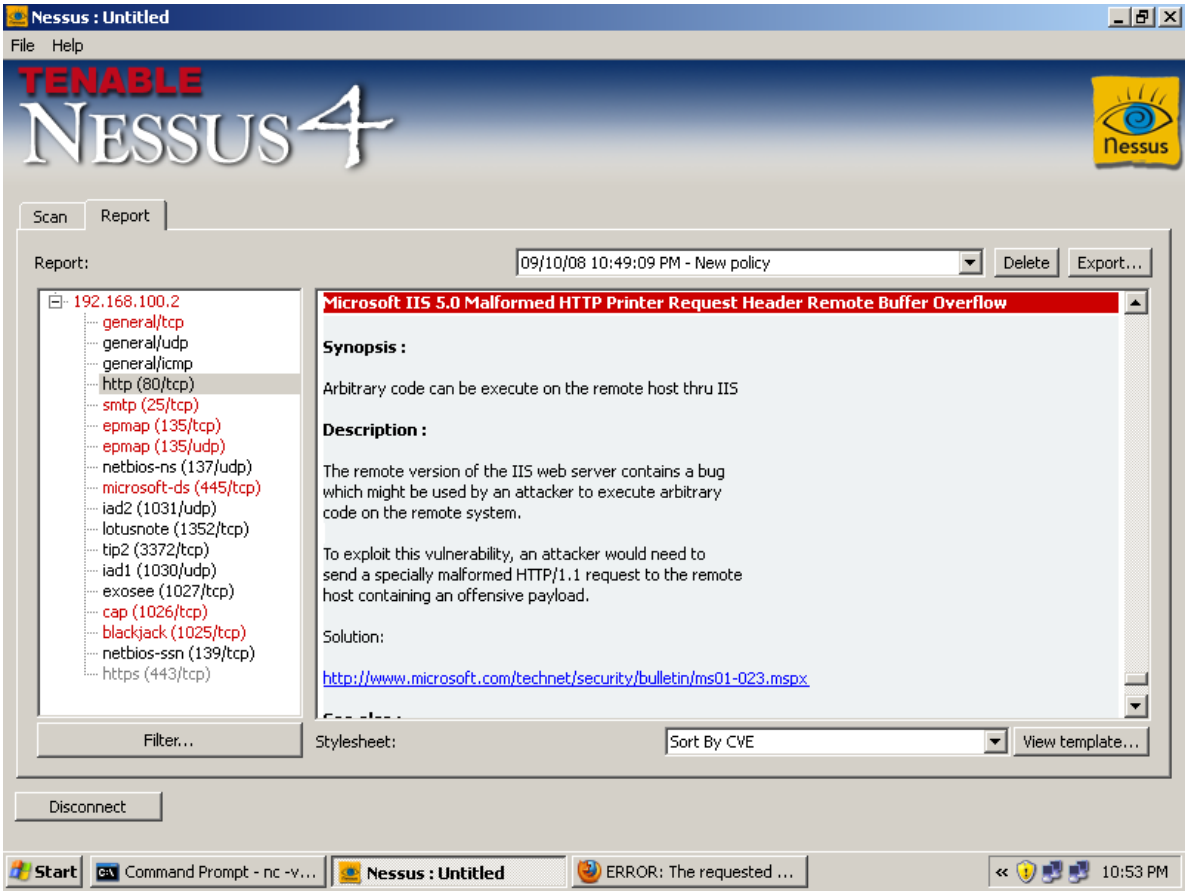
4. Select 'Single host' scan, then type: **192.168.100.2** in the hostname field, then save.



5. Click on the **+** sign , in the 'Select a scan policy' column, and then just click on 'save' button.



6. Then just click on ‘ Scan Now’ button. Wait until scan is finished ☺



7. Do some researches regarding to the vulnerabilities found, and try to scan WIN2003 machine.