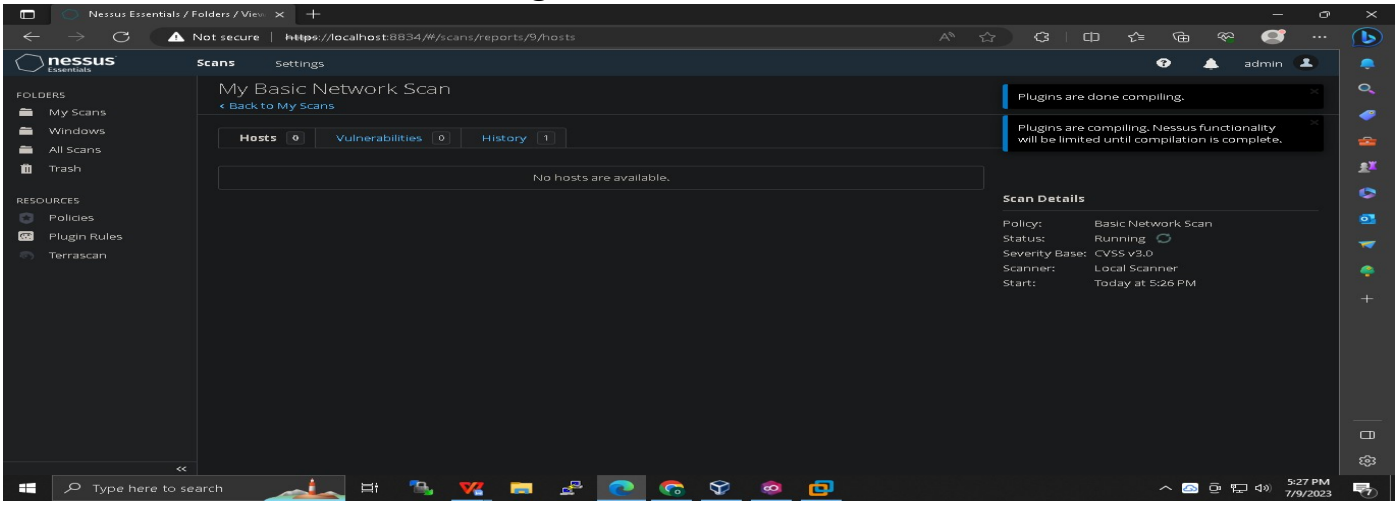
Nessus Scan :

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.

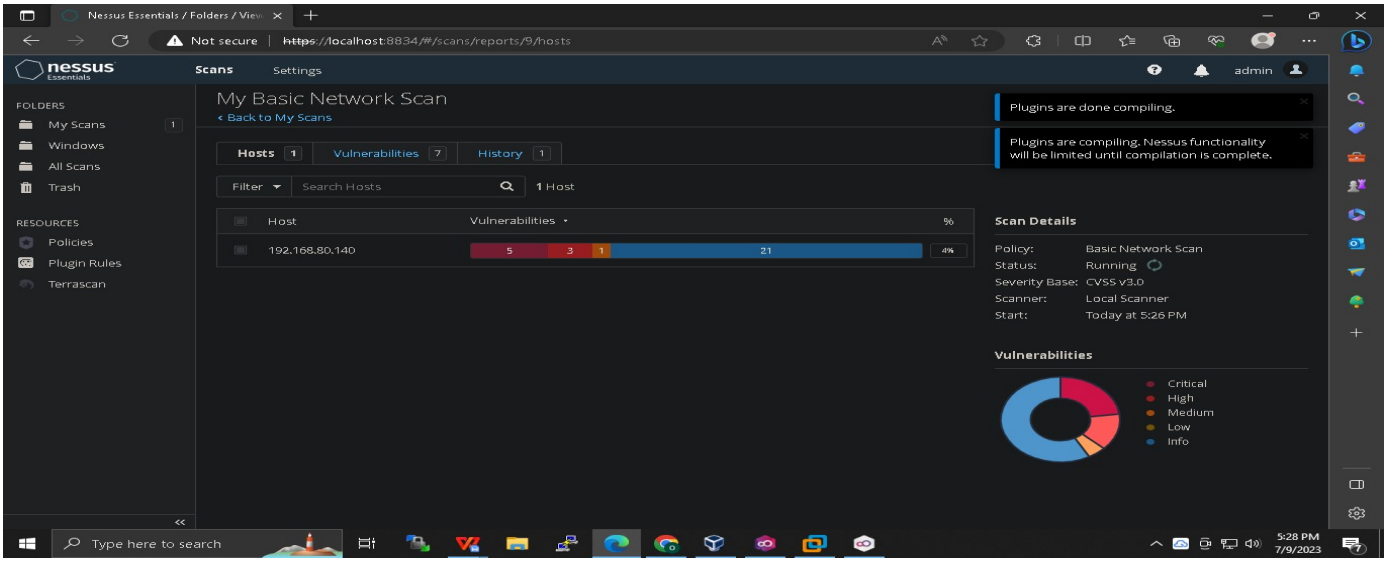
Download tenable nesus : port 8834
1. Detick offline
2. Nessus essentials
3. Create a new scan -> basic n/w scan-> generate report -> to proof show impact as well By performing task for example if there is remote desktop vuln show the impact . by doing remote login . downloa exploit code form internet , run it on another machine and show how you can take remote access of vulnerable machine .

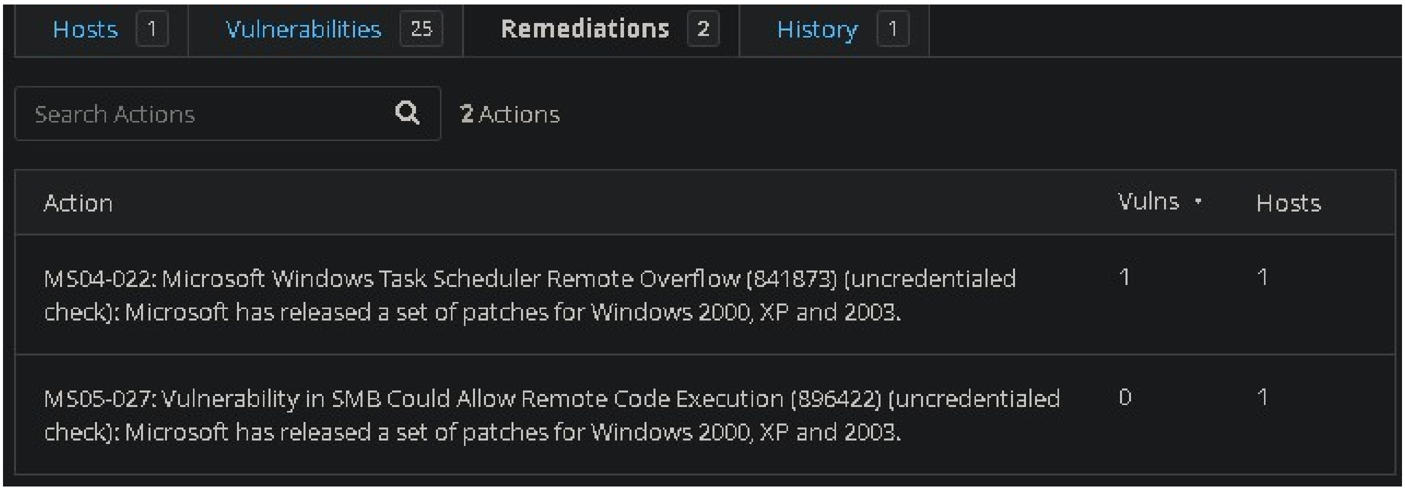
Exploit development : these are those peope who do testing like virologist who do research and write code to exploit , vulnerable assesment people are like doctors . Corelan training .

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



Now we have come to know about vulnerabilities :





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

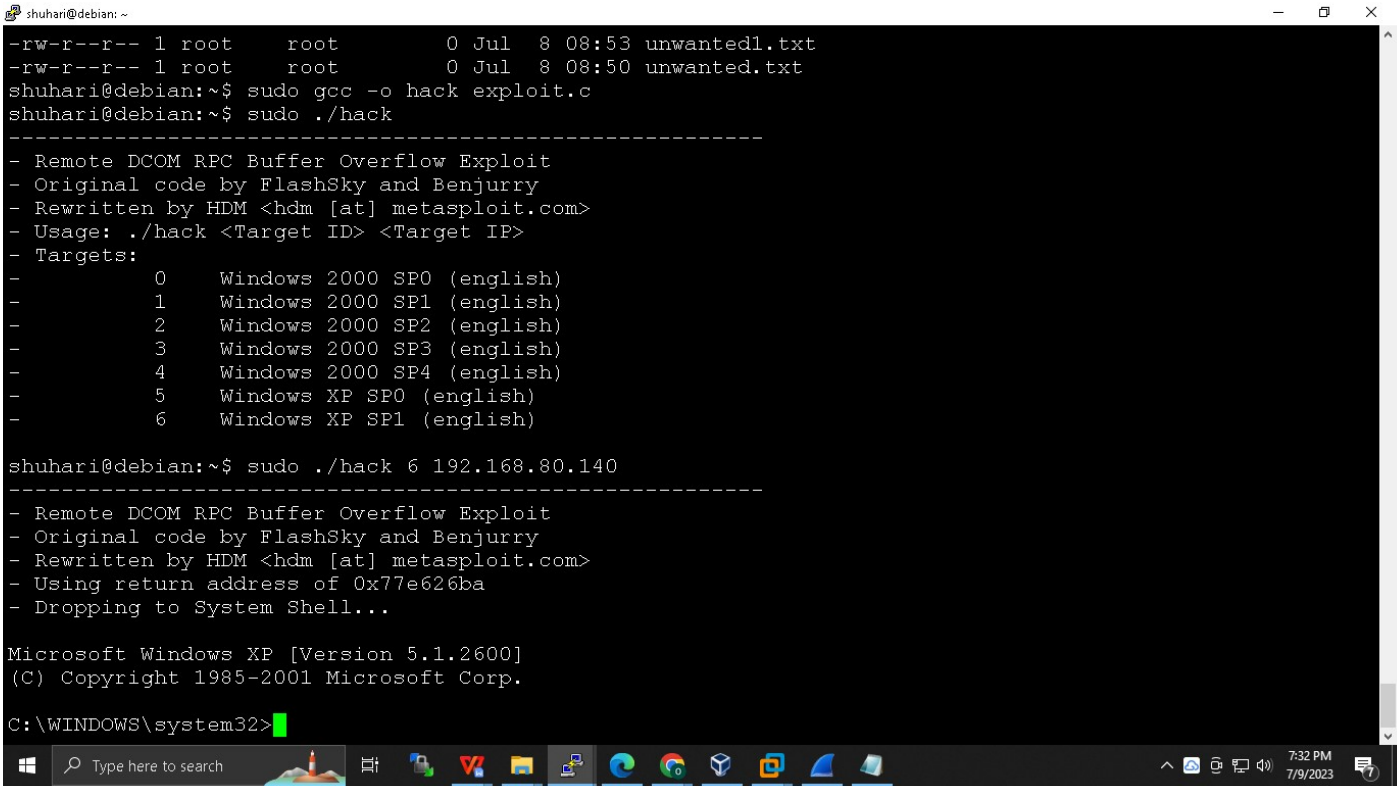
$ sudo apt-get install libc6-dev build-essential gcc

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)



***********************************_***********************************