Group Members:

1. Muhammad Izham Bin Norhamadi B032020039
2. Affendy Elyas bin Azhari Sharidan B032020024
3. Ahmad Sha Herizam Bin Tahir B032020009
4. Muhammad Imran Bin Rosli B032020043

Lab 6 & Lab 7 Vulnerability Scanning

1. Scanning Process of Windows 7

i. Turn on Automatic Update

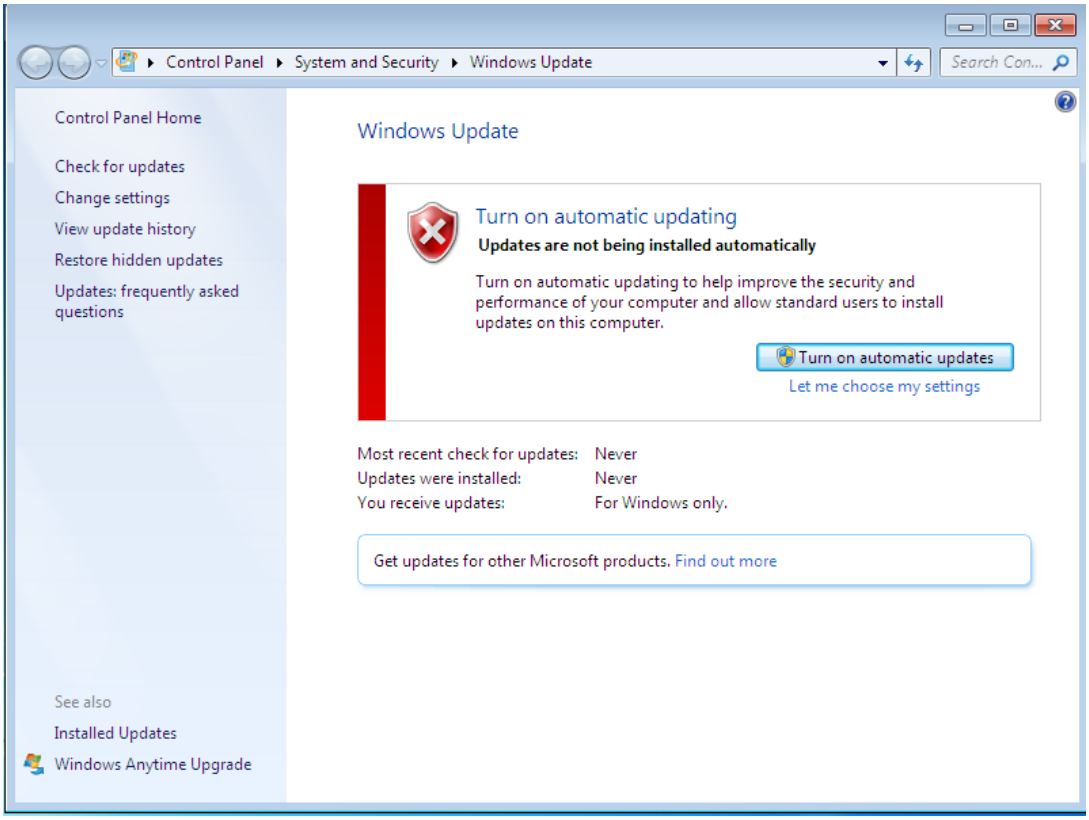

Figure 1 Turn on automatic update in Control Panel

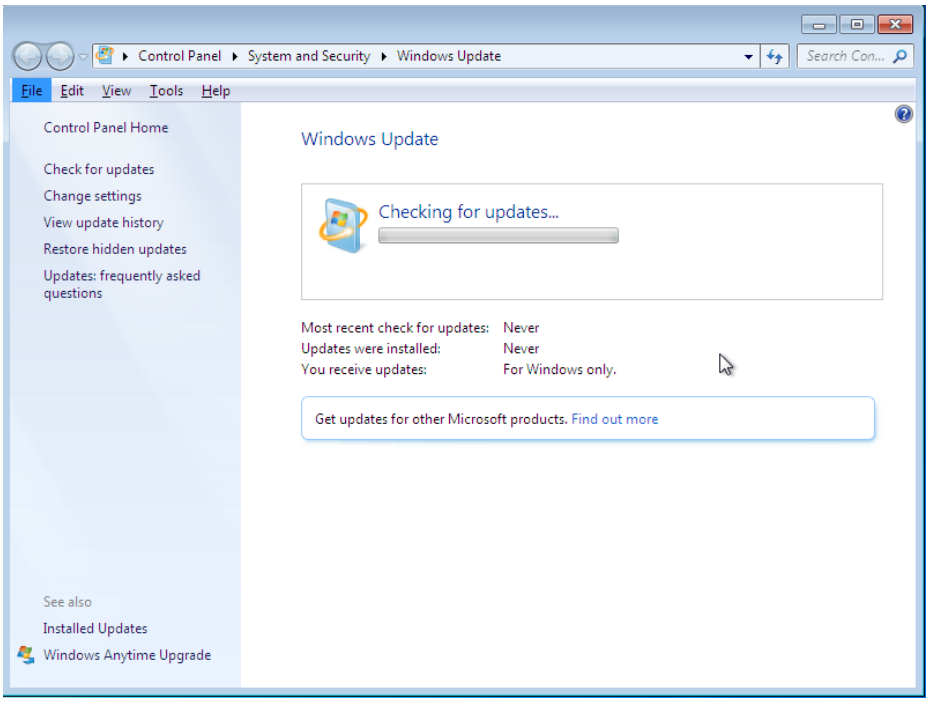

Figure 2 Wait for Windows Update to check for latest updates

ii. Enable System and Event log

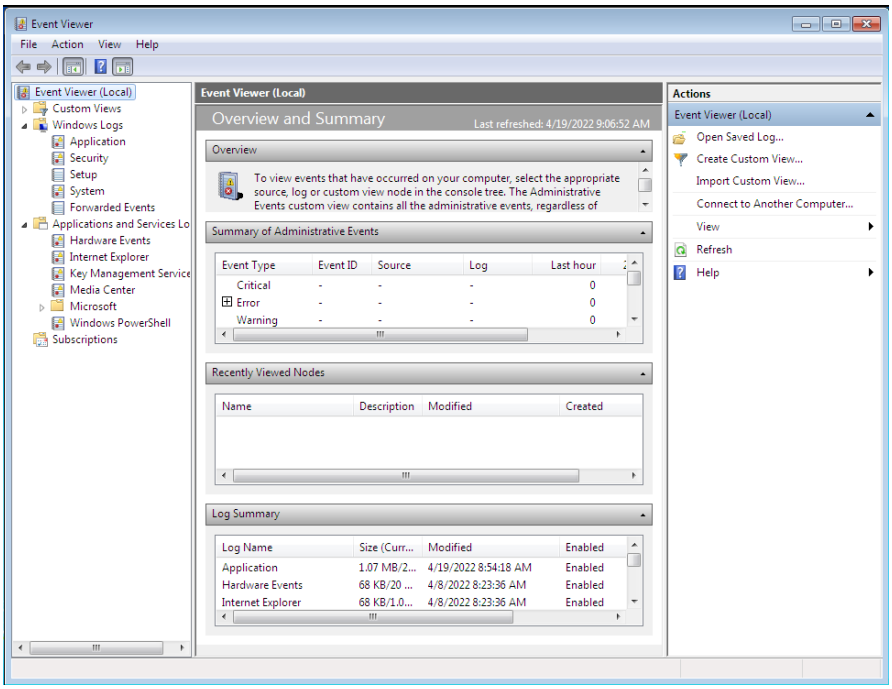

Figure 3 Open Event Viewer in Admin Tools, check if everything is in order

iii. Install Greenbone Vulnerability Manager

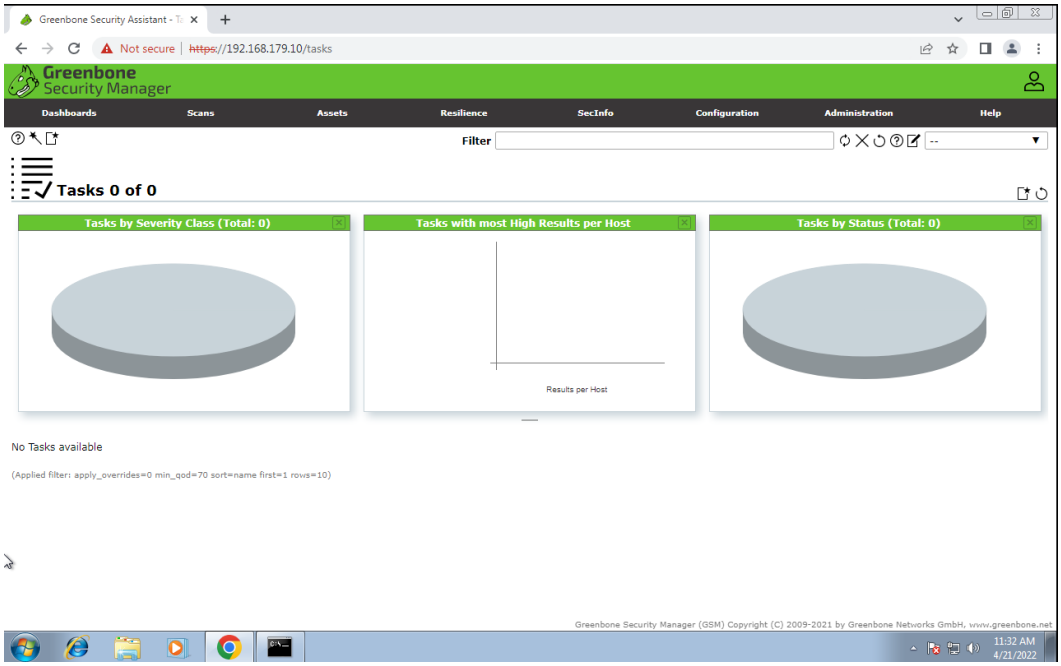

Figure 4 Install and launch Greenbone Security Manager

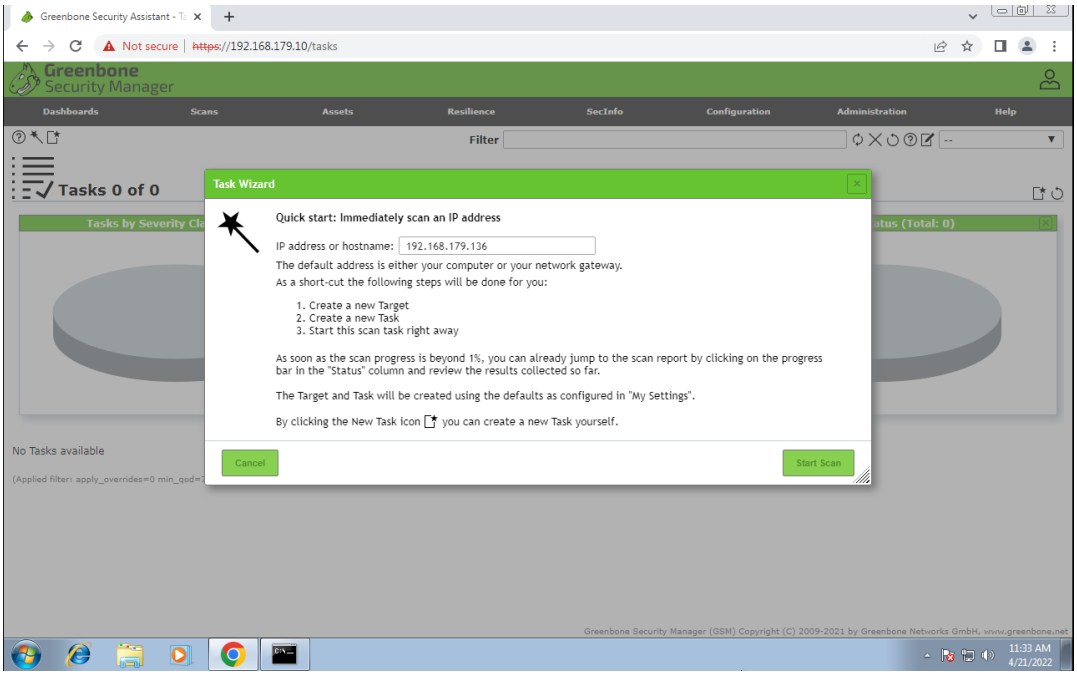

Figure 5 Use Task Wizard to scan for vulnerabilities

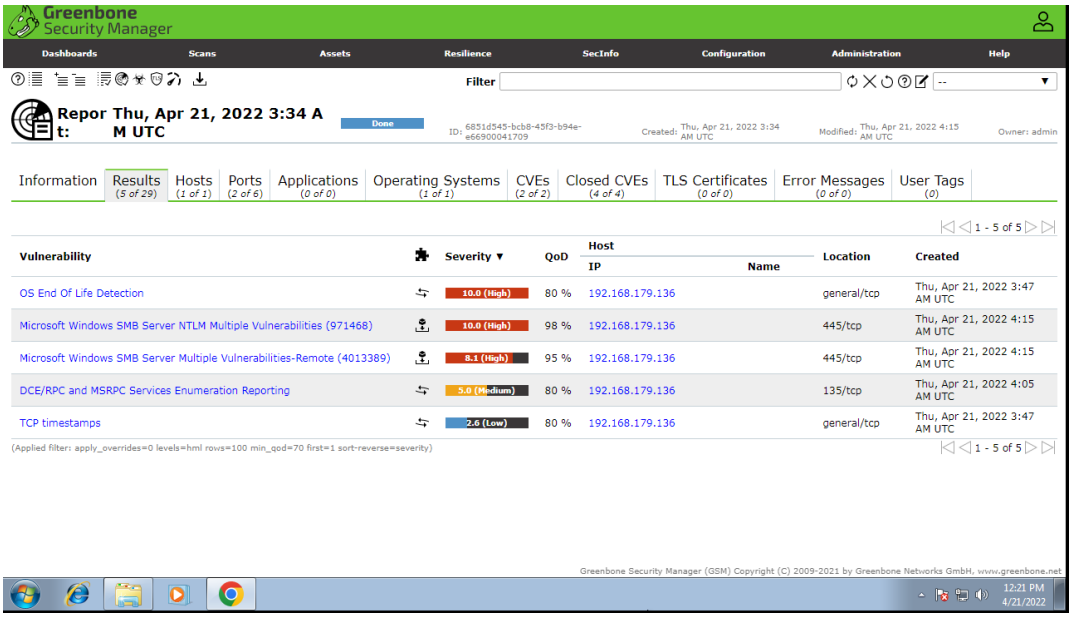

Figure 6 Wait for Security Manager to produce report

iv. Review Firewall filters

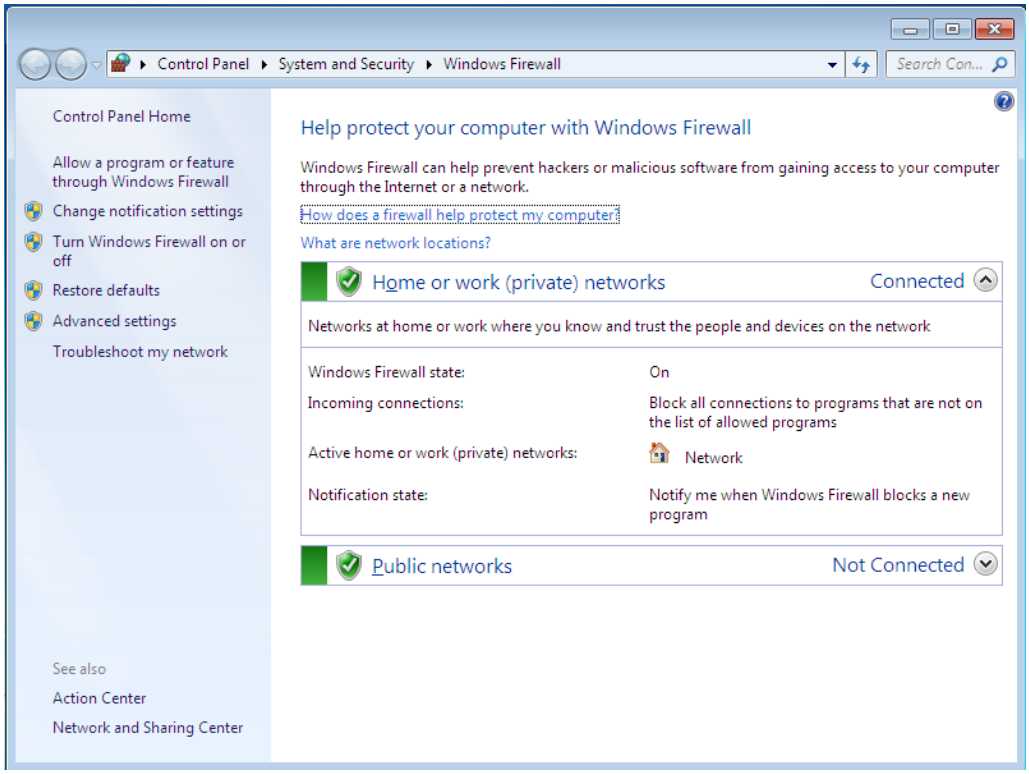

Figure 7 Open Windows Firewall to check its status

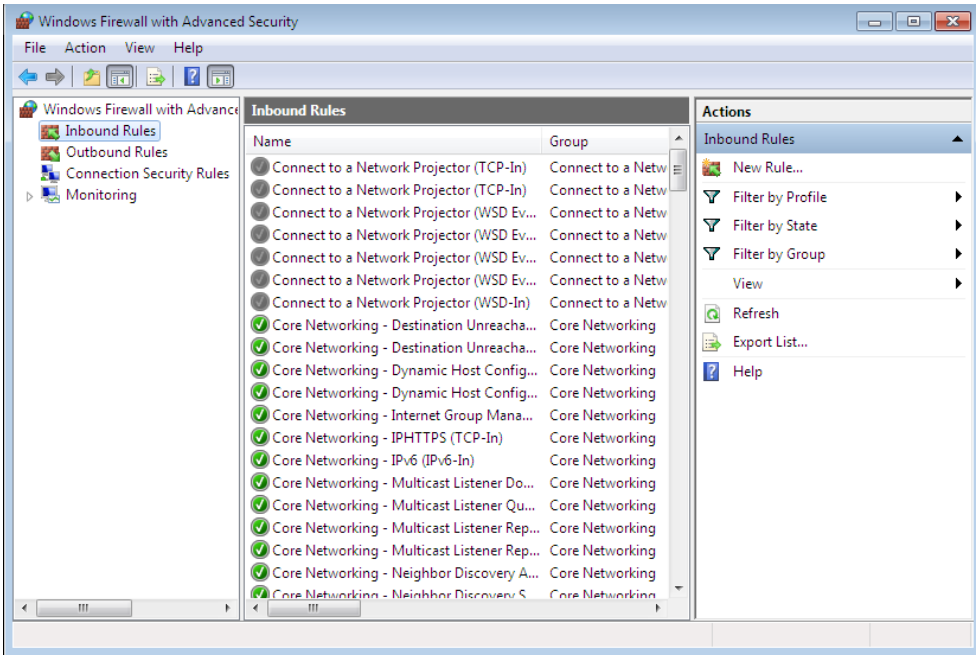

Figure 8 Make sure the Inbound Rules only allow for essential programs

2. List FOUR (4) vulnerabilities which can be found in your Windows, identify the vulnerability scores or CVEs for each vulnerability and discuss the impact of such vulnerability.

1. OS End Of Life Detection

   Vulnerability Scores: 10.0
   Impact: The OS on the remote server has reached the end of life and cannot be used anymore.

2. Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

   Vulnerability Scores: 10
   CVE: CVE-2017-0144
   Impact: Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique

3. Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
   Vulnerability Scores: 8.1
   Impact: Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

4. DCE/RPC and MSRPC Services Enumeration Reporting
   Vulnerability Scores: 5.0
   Impact: An attacker may use this fact to gain more knowledge about the remote host.

3. Give ONE (1) solution to EACH vulnerability which has been highlighted in question (2).

1. Make sure operating systems and third-party software are up to date.

   Due to the organization inconsistency on update practices because of the difficulty of timely patching of software, attackers can attack outdated vulnerabilities. Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

2. Update Windows 7 Service Pack 1 with latest patch

The host is missing a critical security update according to Microsoft Bulletin MS17-010. This was patched in a later version of Service Pack.

3. Update Windows 7 Service Pack 1 with latest patch

   The NULL pointer deference vulnerability was caused by caused by a pointer being incorrectly validated before being used. This was patched in a later version of Service Pack.

4. Filter incoming traffic to TCP ports