NESSUS VULNERABILITY SCANNER

Vulnerability Assessments and Reverse Engineering LABTASK

APRIL 16, 2023

SARDAR MUHAMMAD ZEESHAN KHAN
27969 Teacher: SIR HASEEB

CONTENTS

Differences between Nessus 4 and Nessus 10.5.1

Nessus 4: The Nessus vulnerability scanner was first introduced in 2006, which is a very old version known as Nessus 4. It was a popular open-source vulnerability scanner that many security experts used. The organization that now owns Nessus, Tenable, stopped providing support for Nessus 4 in 2010.

Nessus 10.5.0: In contrast, Nessus version 10.5.0 is a current version of the Nessus vulnerability scanner that was released in 2021. It is a commercial product that is widely used by security professionals to scan and assess the security of network systems.

Differences

i. **GUI:** The user interface of Nessus version 10.5.0 is much more modern and user-friendly compared to version 4. The new interface provides better visibility into the scan results and allows users to quickly identify critical vulnerabilities.

ii. **Performance:** Nessus version 10.5.0 offers better speed and efficiency than version 4. The Nessus 10.5.0 version now scan extensive networks more accurately and quickly.

iii. **Features:** Nessus Version 10.5.0 of Nessus introduces additional functionality not found in version 4. Improved compliance checks, enhanced cloud support, and more capable reporting tools are a few of them.

iv. **Security:** Version 4 of Nessus has less effective security features than version 10.5.0. Nessus 10.5.0 includes stronger authentication methods, better integration with existing security products, and improved support for encryption protocols.

v. **Licensing:** Nessus version 10.5.0 employs a different licensing scheme than version 4, in terms of ownership. Instead of counting IP addresses, the new licensing scheme counts the assets being scanned. Organizations may manage their licenses more easily and only pay for what they need as a result.

vi. **Architecture:** Nessus version 10.5.0 features a redesigned architecture that increases its scalability and capacity to manage huge, complicated networks. Moreover, it offers distributed scanning and is cross-platform compatible.

vii. **Plugins:** Nessus version 10.5.0 can identify a greater range of vulnerabilities and threats because it has a significantly larger library of plugins than version 4. Also, the plugins are updated more regularly, ensuring that the tool can identify the most recent threats.

viii. **Integration:** Better integration with other security products, such as SIEMs and vulnerability management platforms, is provided by Nessus version 10.5.0. As a result, businesses can gain a more complete picture of their security posture and make better choices.

SCANNING WITH NESSUS 4 on Windows 2K

1st Step:

As a First step I opened the Nessus 4 on Windows 2k, by **going to the start menu** or by searching for it.

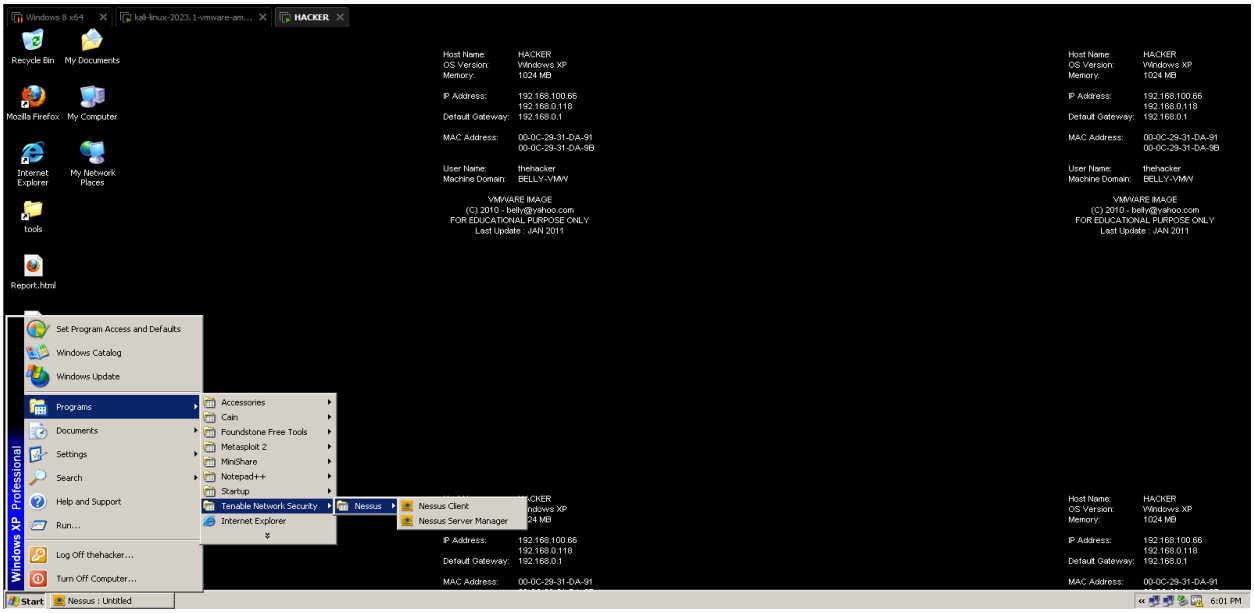

Figure: Searching for Nessus Client.

2nd Step:

Next step would be when the Nessus is opened, **insert the IP address** of the network, you want to scan using Nessus.

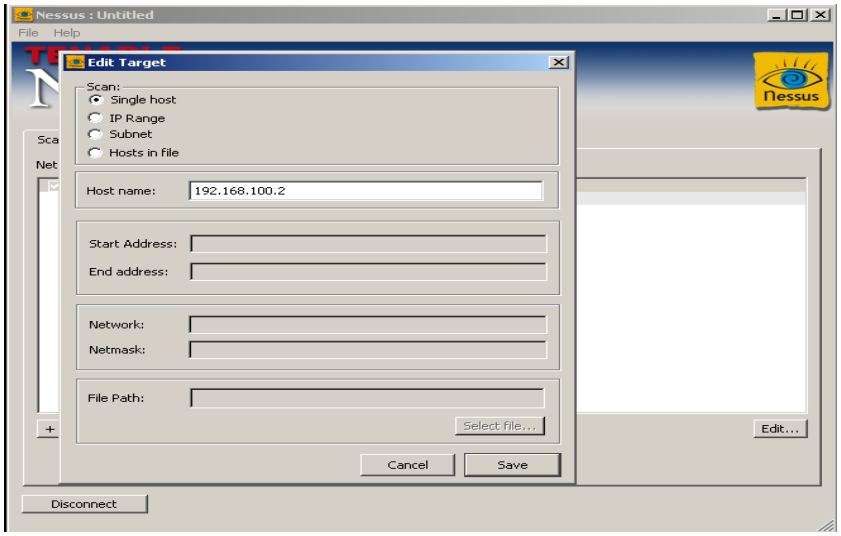

Figure: Inserting IP address in NESSUS 4.

3rd Step:

Third step would be to **set the Policy In the Nessus Scan**. Policy means the options or advance settings you want to check in or not. E.g. Do you want to save the scan results, which plugins you want to use for the scan, or what type of scans do you want to perform.

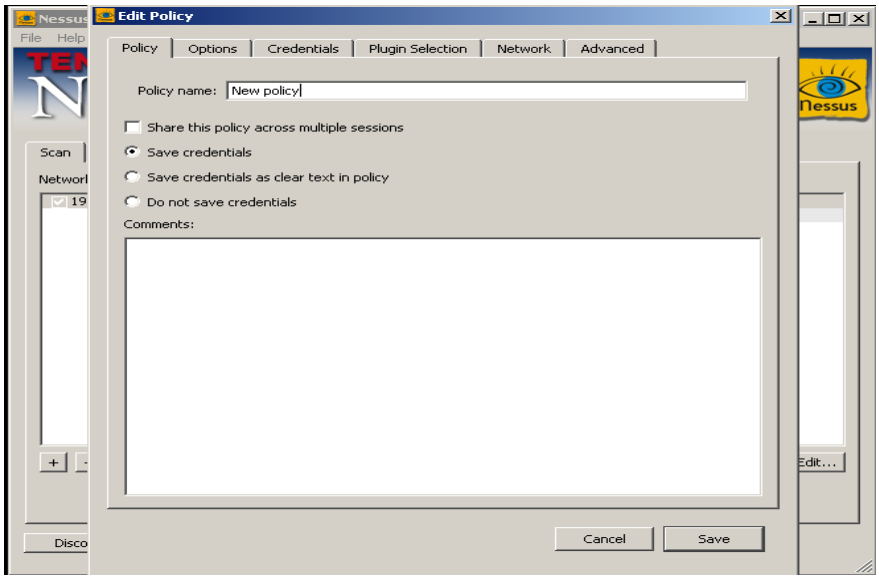

Figure: Policy tab of New Policy of Nessus 4

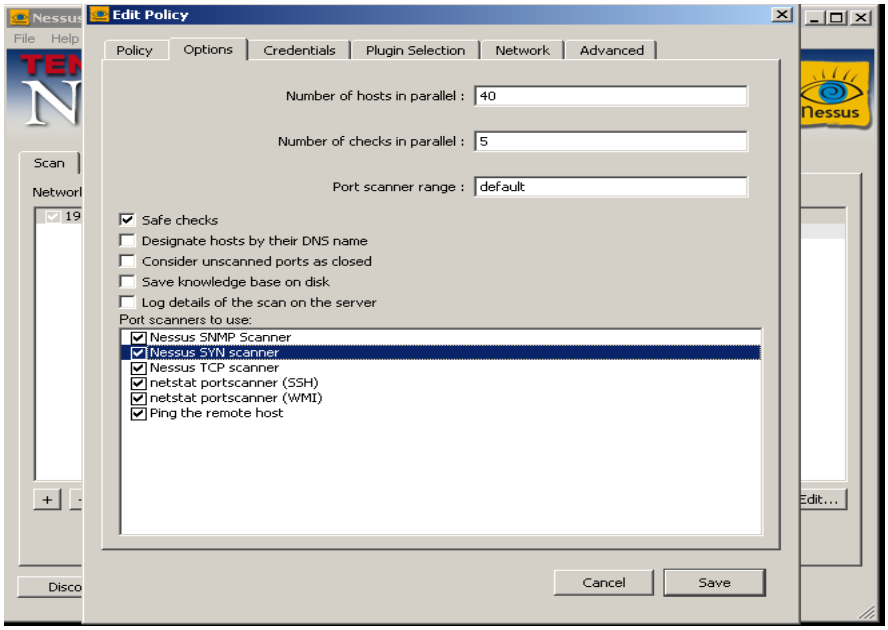

Figure: Scanner options in the New policy of Nessus 4

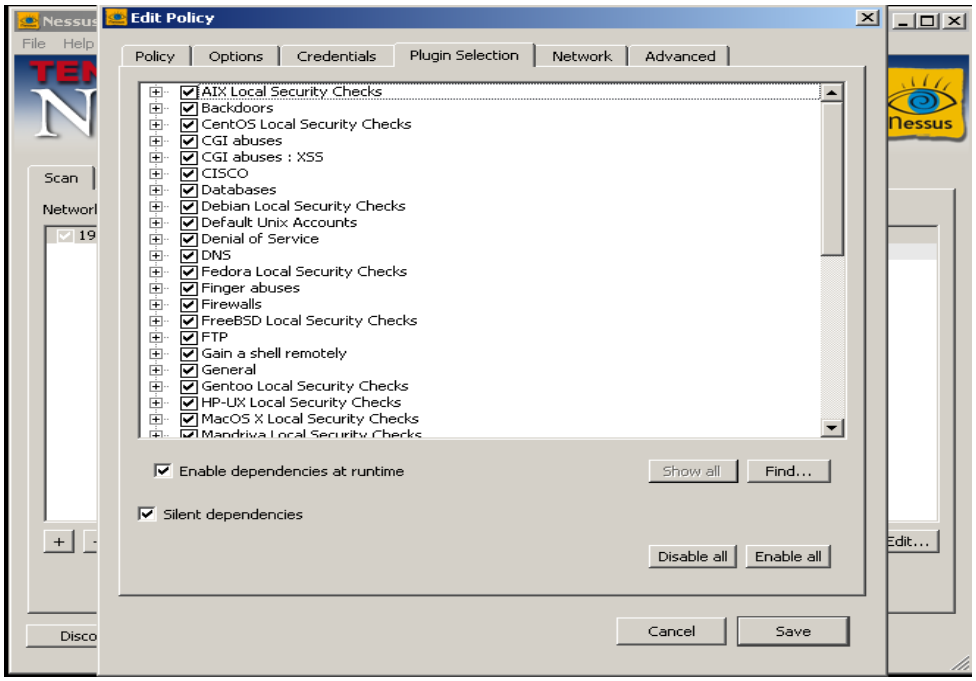

Figure: Plugin Selections in the New policy of Nessus 4.

4th Step:

The Second Last step would be to perform the scan by tapping on the **SCAN NOW** button.

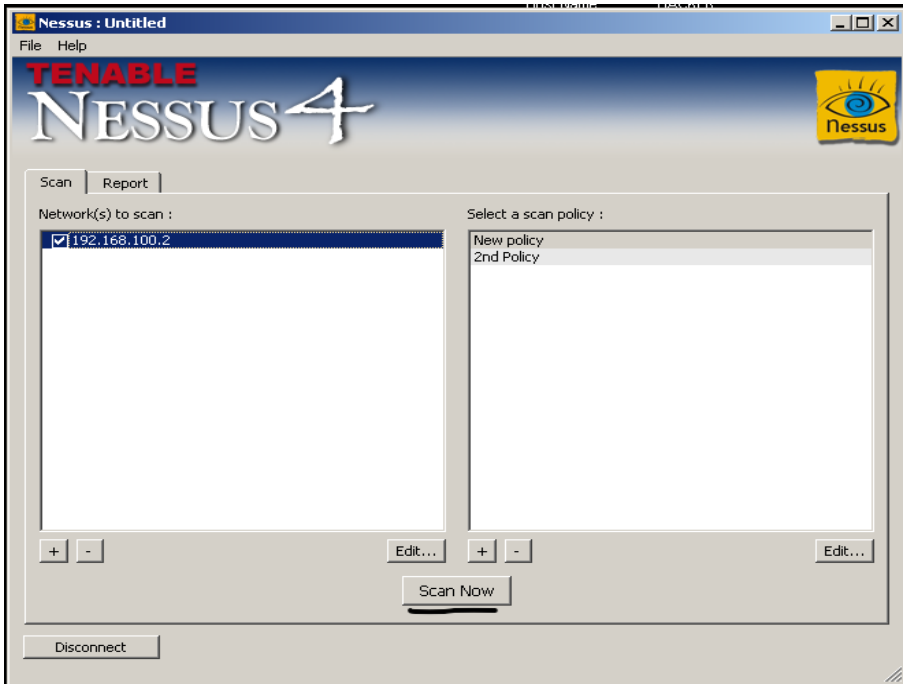

Figure: Scan to be started by tapping on the Scan Now button.

5th STEP:

The Final Step would be to look at the results of the Scan by going to the **Report Section** and then tapping on the **View Template button** which will open the LIST of CVEs in the Browser that can be exploited in Windows 2k to take access of the Windows 2k.

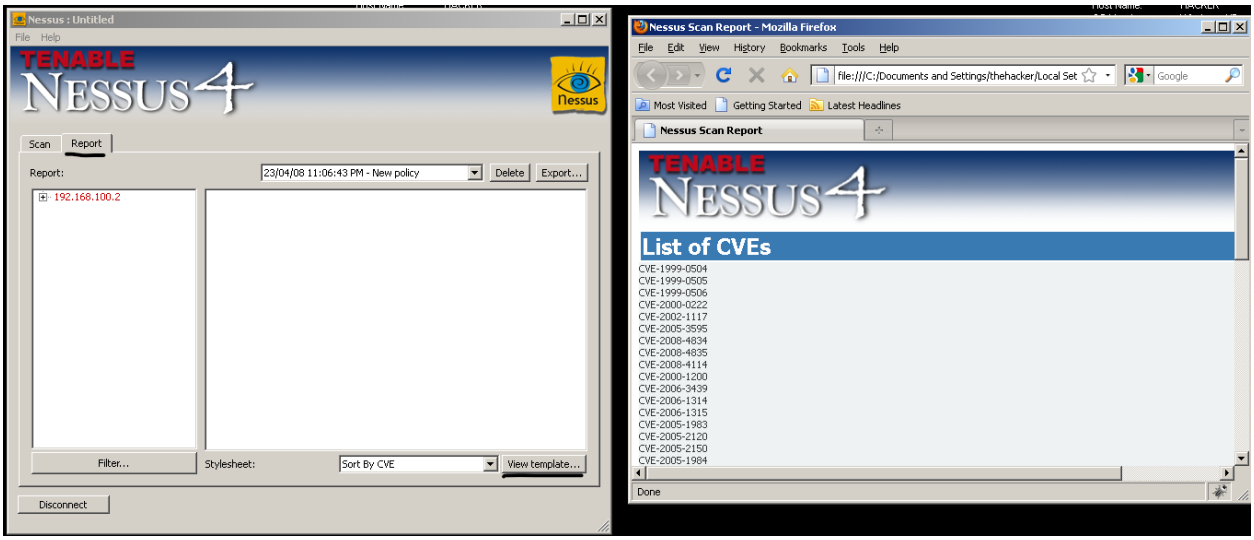

Figure: List of Vulnerabilities/CVEs available in the Windows 2k.

SCANNING WITH NESSUS 10.5.1 on KALI LINUX

1st Step:

The first step would be to install the Nessus and then start the Nessus Services by going to the CMD and typing **" Service Nessusd Start & hit enter"** and then "**insert your password"** and it will start running.

The Nessus will start running on your **port 8834**. After setting up the Nessus and logging in successfully in the Nessus. Go to the scan templates in the Scan sections you will a lot of variety of scans in that section. I have chosen to scan "Basic Network Scan".

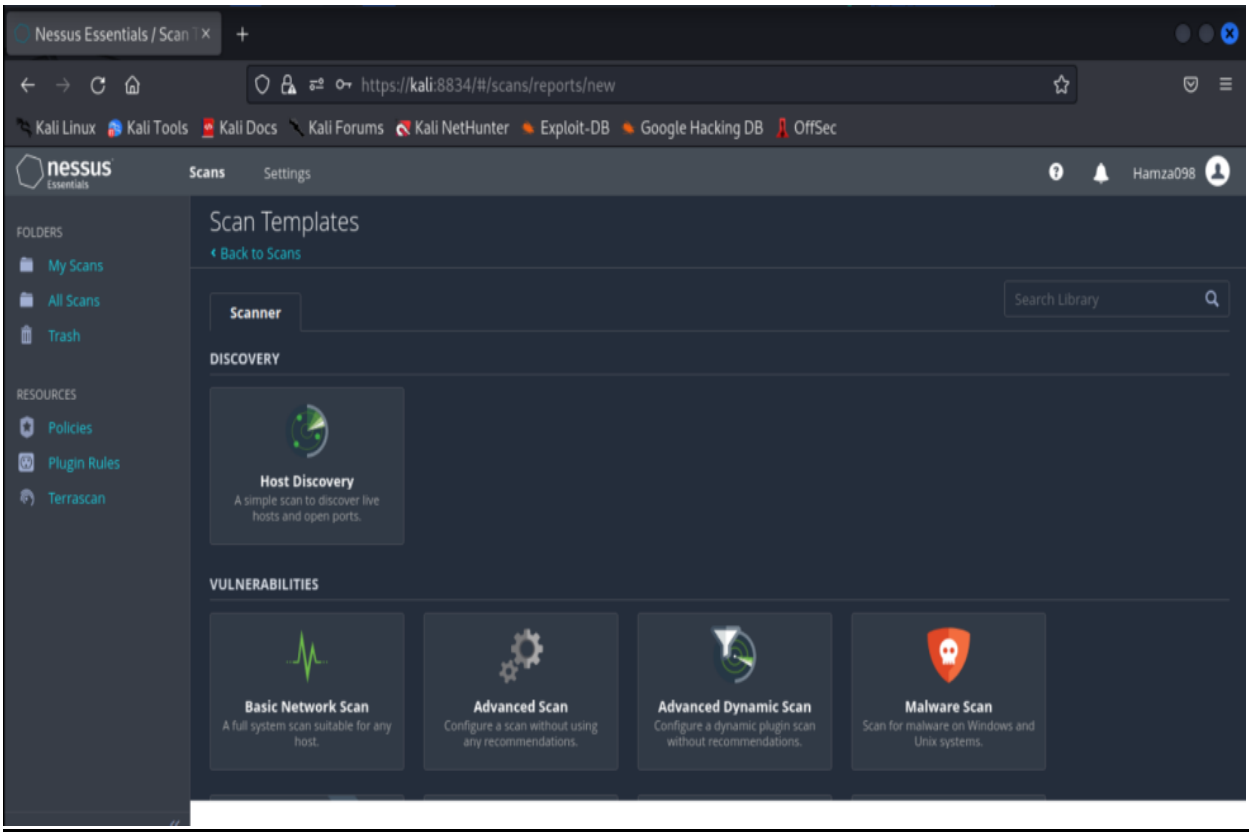

Figure: General Screenshot of Scans Template in The Nessus

2nd Step:

Next step would be after selecting the scan, is to **add the IP address** of the Network you want to scan. As you can see I have added the IP address in the below screenshot of the Windows 2K.

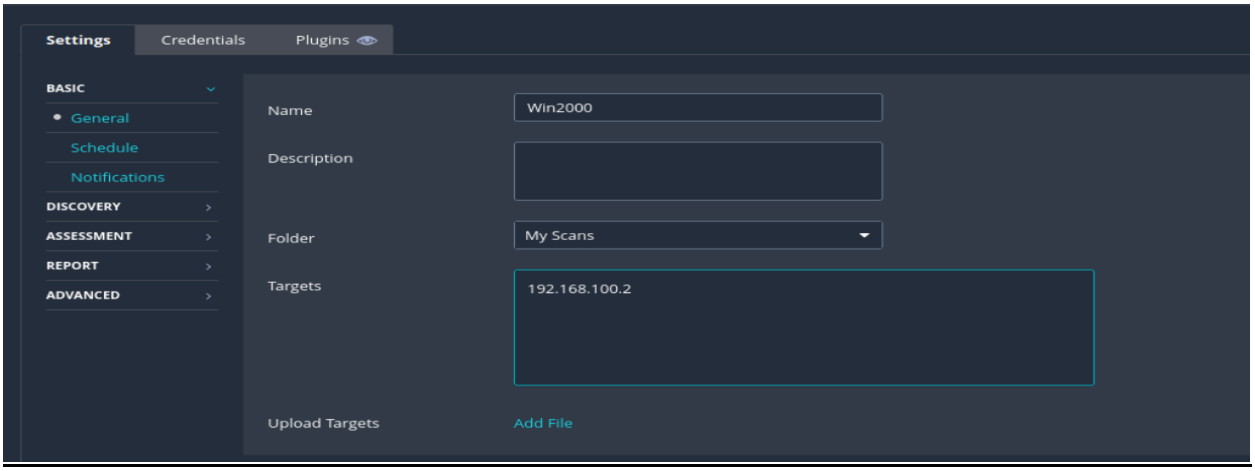

Figure: Adding the IP Address in the Basic Network Scanner

3rd Step:

After finishing setting up the scanner we will save the scan and perform the scan. As you can see in below screenshot the scan has been completed as It shows TICK MARK to show completion.

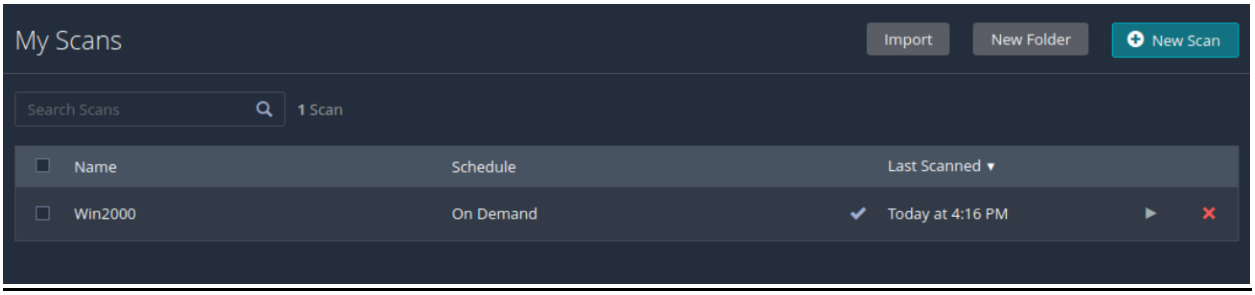

Figure: Shows that Scan has been completed on windows 2000.

4th Step:

After the completion of Scan The final step would be to tap on the scan results and they will show you the vulnerabilities that have been scanned out for you from that system. As you can see in the below screenshot.

Figure: shows all the vulnerabilities that exists in Win 2K.

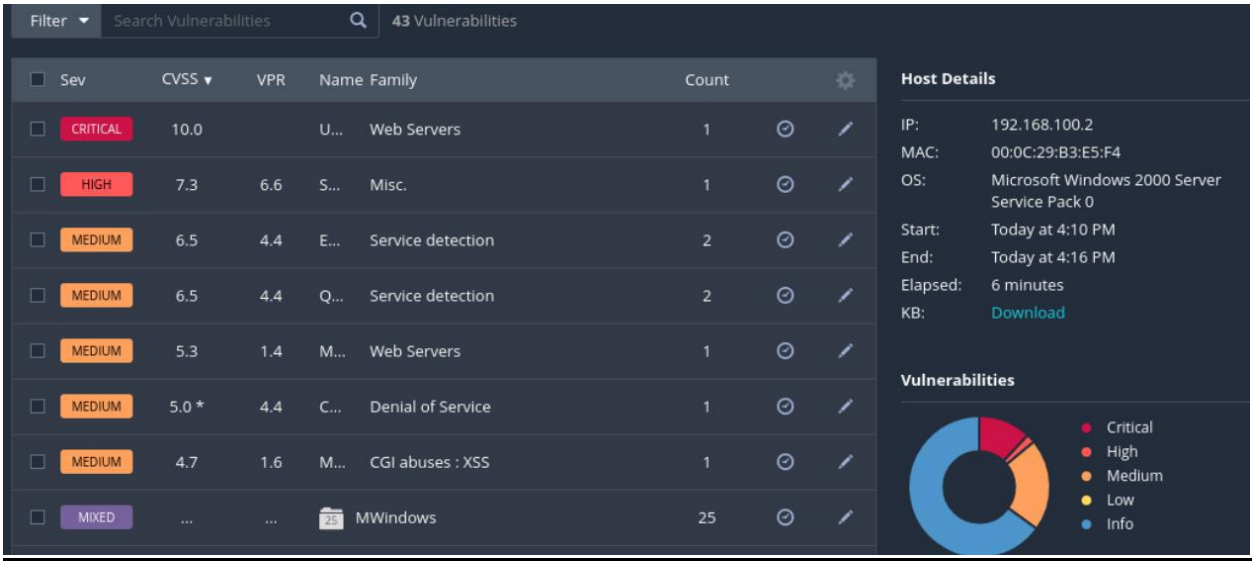

Figure: Detailed view of individual vulnerabilities along with their CVSS score.