Intruder Vulnerability Scanner

Submitted by – Harsh Sharma

Index Page

1. Introduction to Intruder ………………………………………………………2
   1. What is vulnerability scanning?
   2. What is proactive scanning?
2. Interacting with Intruder………………………………………………………3
   1. Dashboard
   2. Issues
   3. Scans
   4. Reports
   5. Targets
   6. Networks
3. How to scan our own endpoints……………………………………………7
   1. Adding target
   2. Installing Nessus agent
   3. Executing the agent
   4. Starting scan
4. Looking at more endpoints and services……………………………….11

4.1 Scanning website

1. Conclusion…………………………………………………………………………….11

**Introduction to Intruder**

Intruder is a web-based vulnerability scanner, used for exposing vulnerabilities within the network, operating systems, and cloud. It scans proactively as soon as a new vulnerability comes, this tool will recognize it.

Intruder can scan the following things:

1. Windows, MacOS, Linux, Fedora
2. Websites and Ip’s
3. Google cloud, Microsoft Azure, Amazon Web Services

**What is vulnerability scanning?**

It is a process also known as penetration testing in which malicious steps are performed intentionally to check the security weaknesses in a system.

In case of Intruder it does the same by executing scripts and attacks on the described target.

When the scanning gets completed, report is generated in a certain format reporting about the vulnerabilities, in which way it got vulnerable, suggestions of patching and recommended steps.

**What is proactive scanning?**

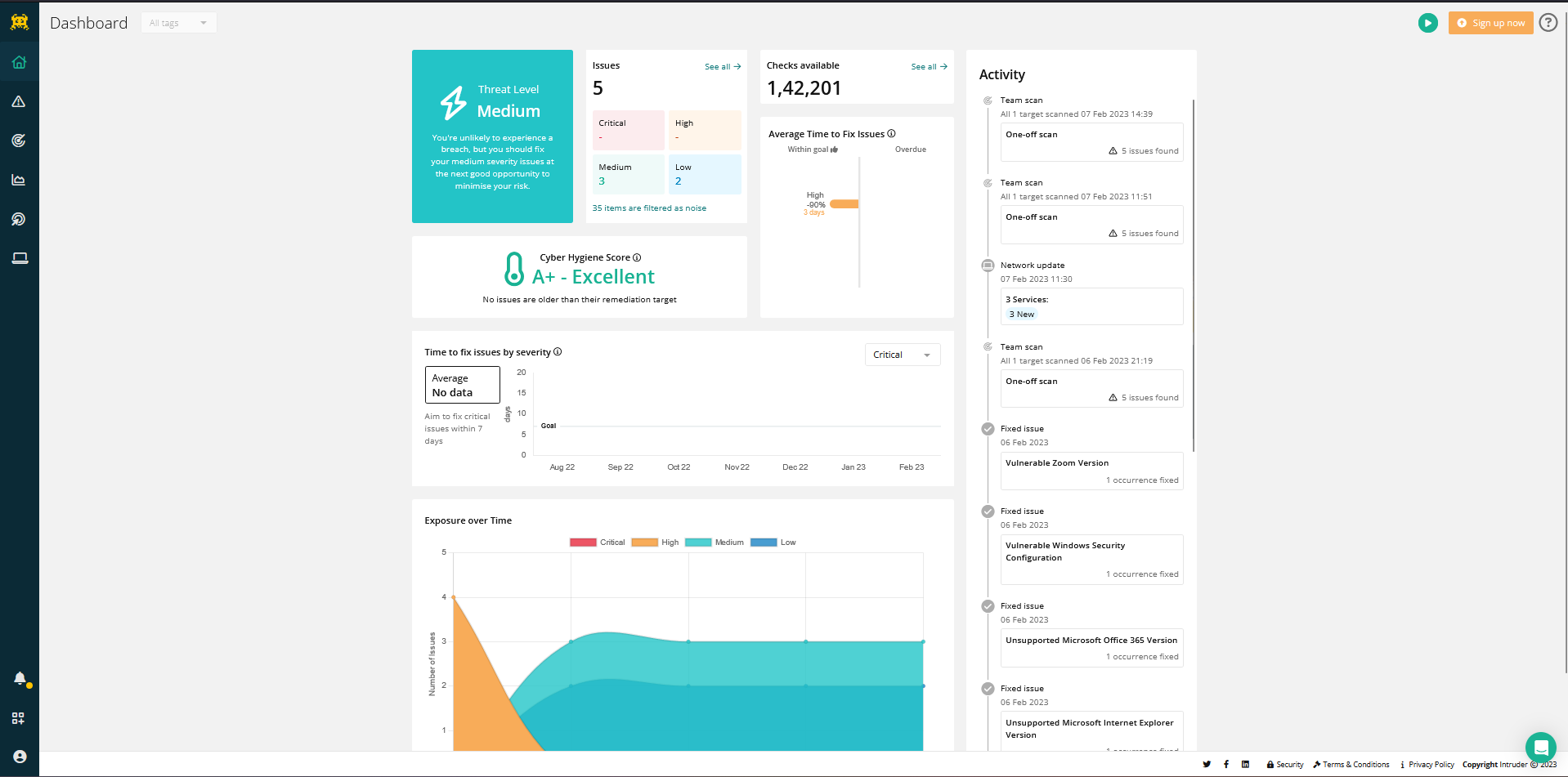
Proactive scanning technique scans your target when it is alive and working. Proactive scanning uses intelligent methods to check all executable files, library files and driver files for suspicious programs.

**Interacting with Intruder**

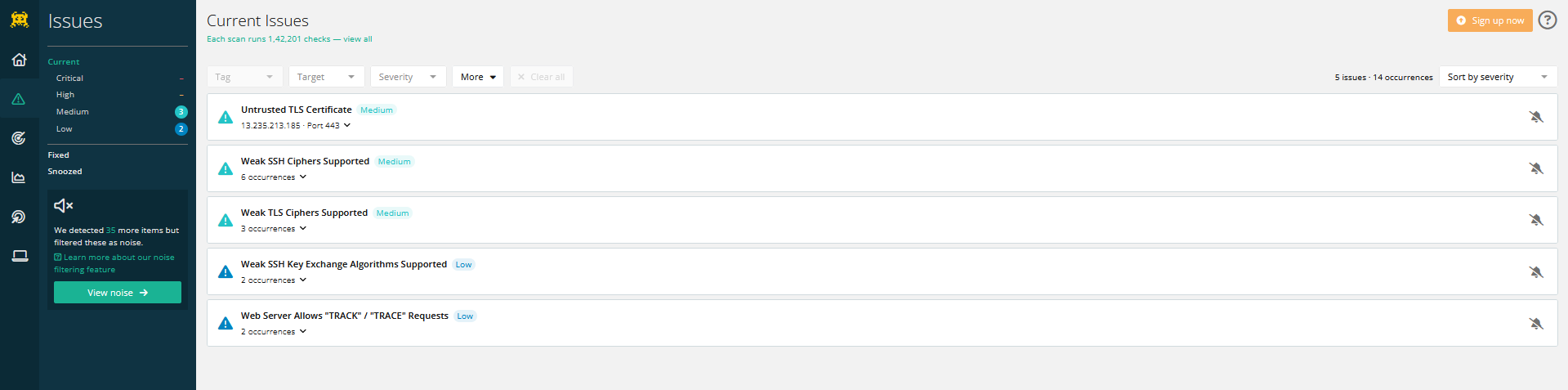
At left side of the intruder there are 6 icons:

1. Dashboard
2. Issues
3. Scans
4. Reports
5. Targets
6. Network

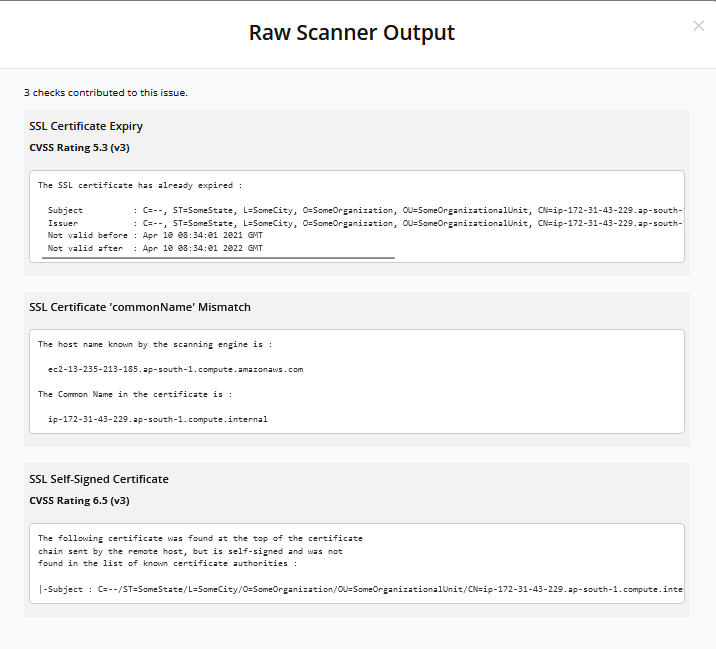
We will see the above in detail in this report.

**Dashboard**

Dashboard gives brief of every activity done and security status of recently scanned system indicating risks and severity. No of issues is also shown in the form of graph.

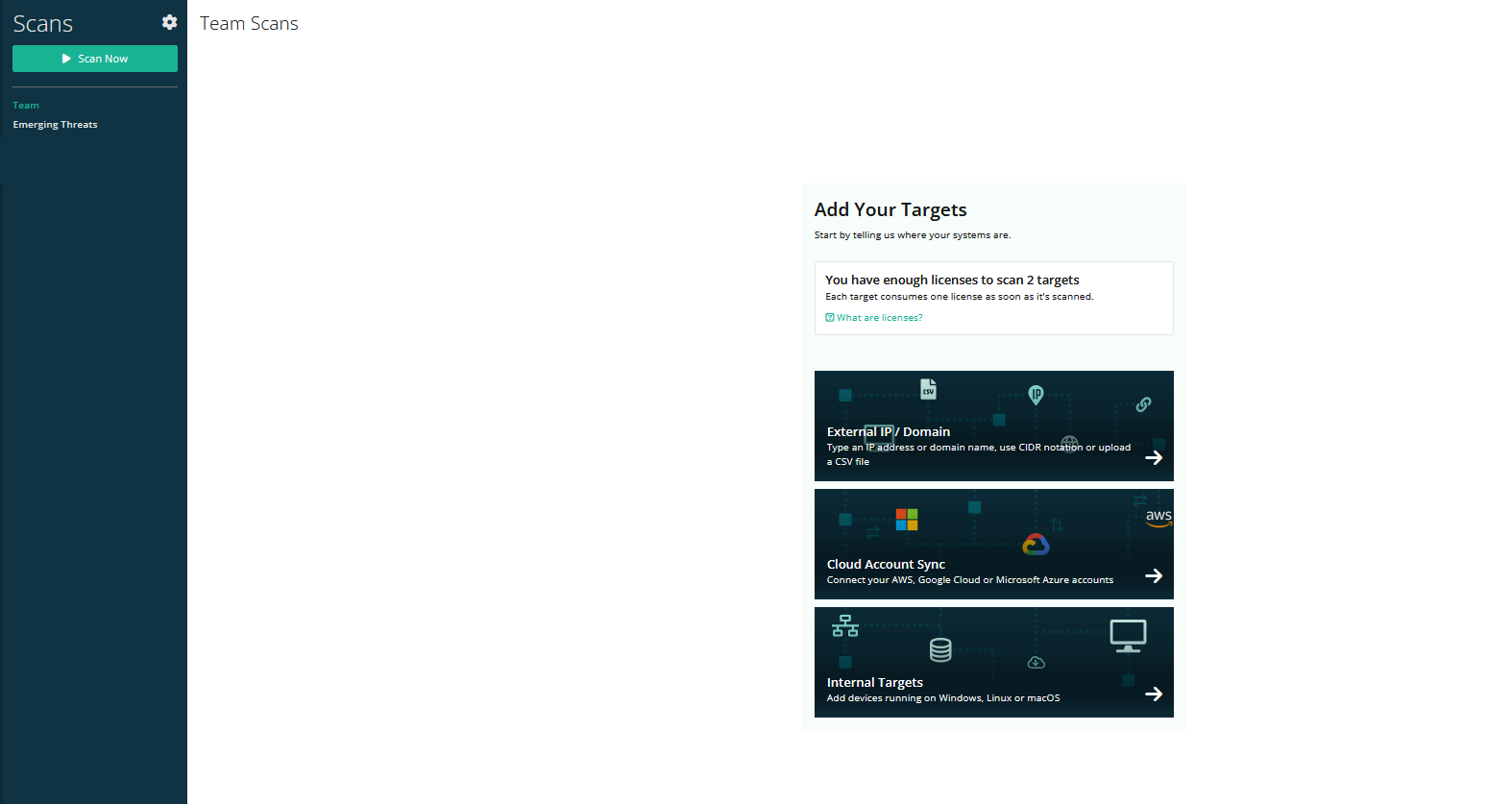
**Issues**

After scanning gets completed, security concerns of the target are directed to issues corner of the intruder. Issues are ranked with low, medium, high, and critical issues. By clicking, on the issue we can get the details of the issues.



We can see the result and vulnerability that raised the issue in the **show raw scanner output option** in a particular issue.

**Scans**



Scans is where the whole process starts , by adding targets we can start our scan.

NOTE : We can add multiple targets at same time but starting scan on all the targets can be time consuming , refer to the link below:

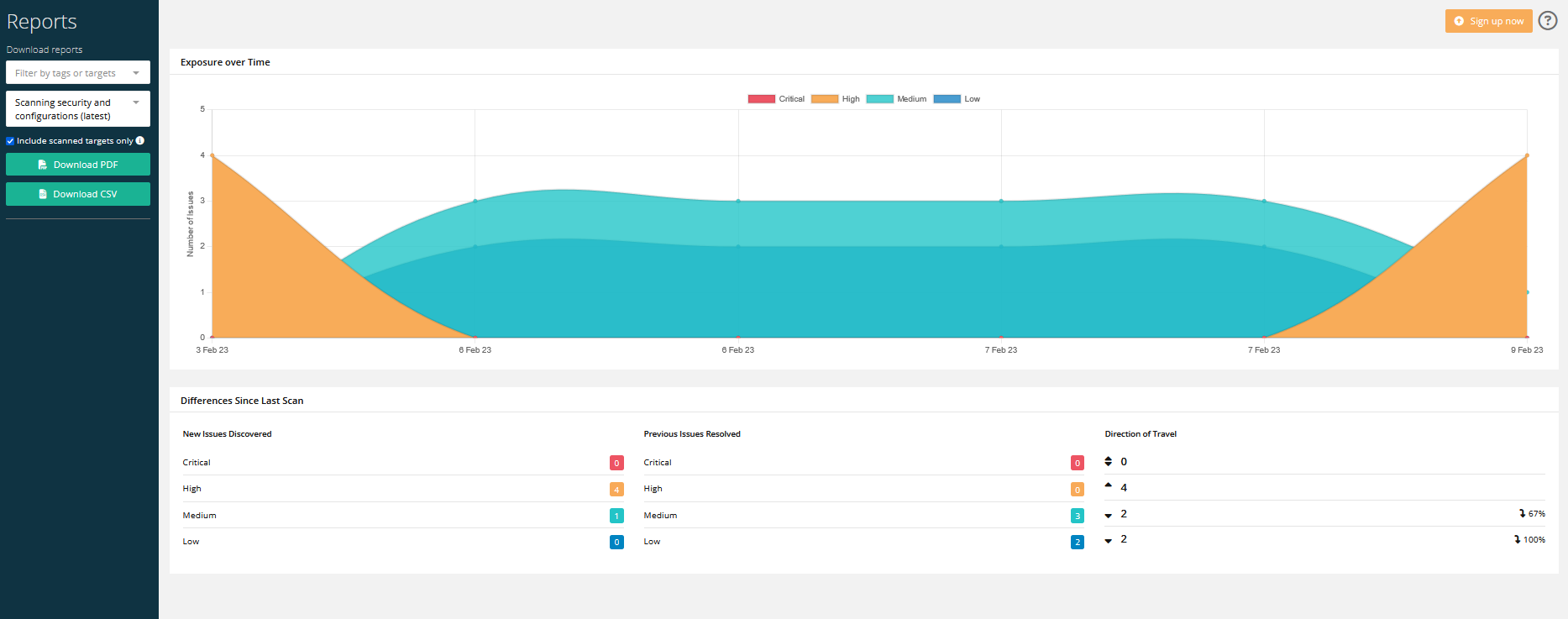
[https://help.intruder.io/en/articles/1844315-how-long-will-my-scans-take#h\_74ac9d75e2](https://help.intruder.io/en/articles/1844315-how-long-will-my-scans-take%23h_74ac9d75e2)

Scan can be done on:

1. Operating Systems
2. Websites and Ip’s
3. Clouds such as Microsoft Azure, AWS, and Google Cloud

For the scanning procedure we must download an agent which is required to initialize and to perform the scan.(for operating systems only)

**Reports**



When the scans are completed, we can download the vulnerability assessment report in the Reports section of the intruder. Report can be downloaded in following formats:

1. PDF format
2. CSV format

A brief of vulnerabilities is also shown here in the reports.

**Targets**

All the targets are added here for the scanning procedure to add targets.

**Networks**

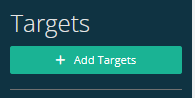
Here we can, add cloud network, website and ips. The procedure is same as adding targets.

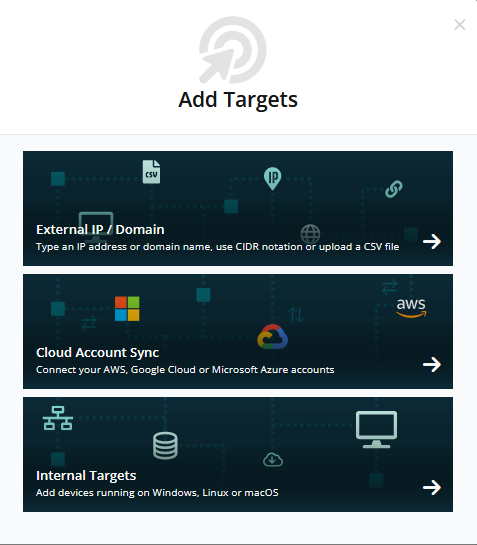
**How to scan our own endpoints**

Now we have all the knowledge required to use Intruder.

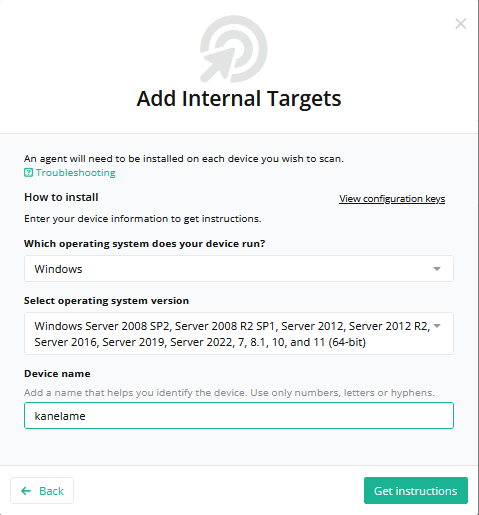
To scan endpoints we have to follow these steps:

**Adding Target**

****Click on add targets.



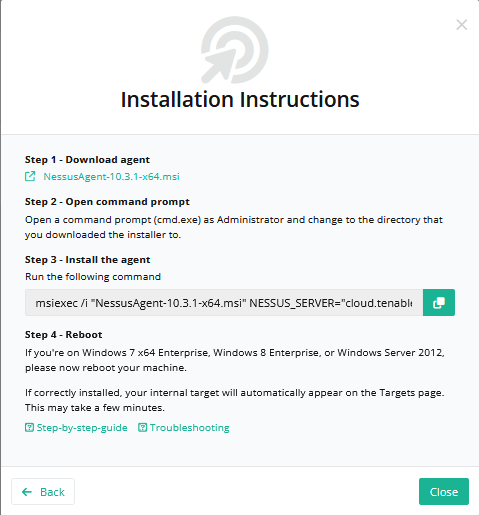
Select your endpoint, I am choosing Internal targets as I am scanning my windows machine.



Give the required information of your operating system, I have chosen **Windows 11** and **kanelame** as my system name.

Click on get instructions.

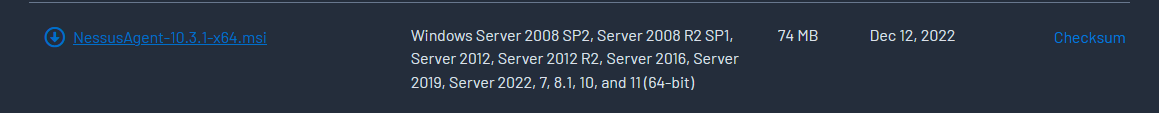
**Installing Nessus Agent**



Before initializing the scan, we need to install an agent for further process. Download the agent by clicking on the link shown in the image.

Copy the following command.

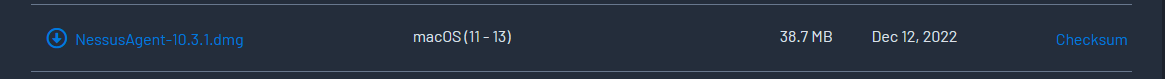
For windows:



For linux:



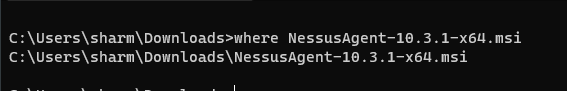
For macOS:



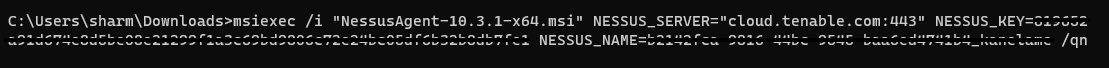
Versions can be different, so the best practice is to install the agent with latest version.

**Executing the agent**

**(Open command prompt as administrator)**

****

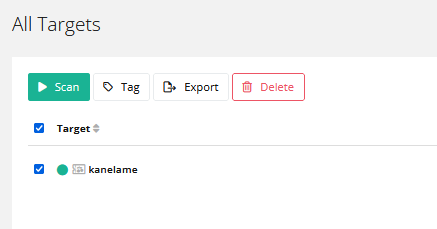
Navigate to your downloads folder (location of your downloaded files)



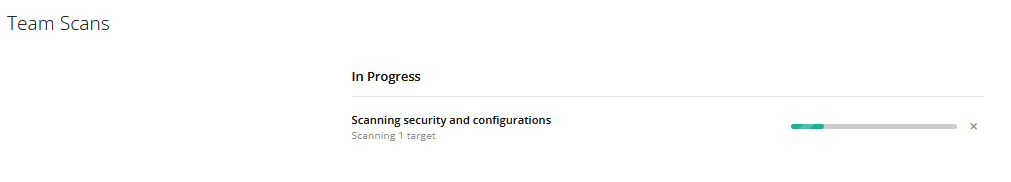
Paste the command copied before and execute it.

Wait for sometime and then refresh intruder web page to get your target.

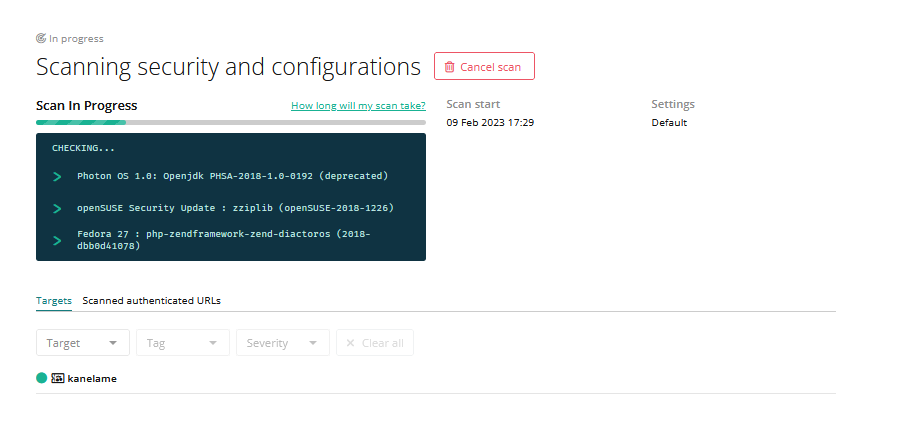
**Starting Scan**

****Click on scan to launch the assessment.

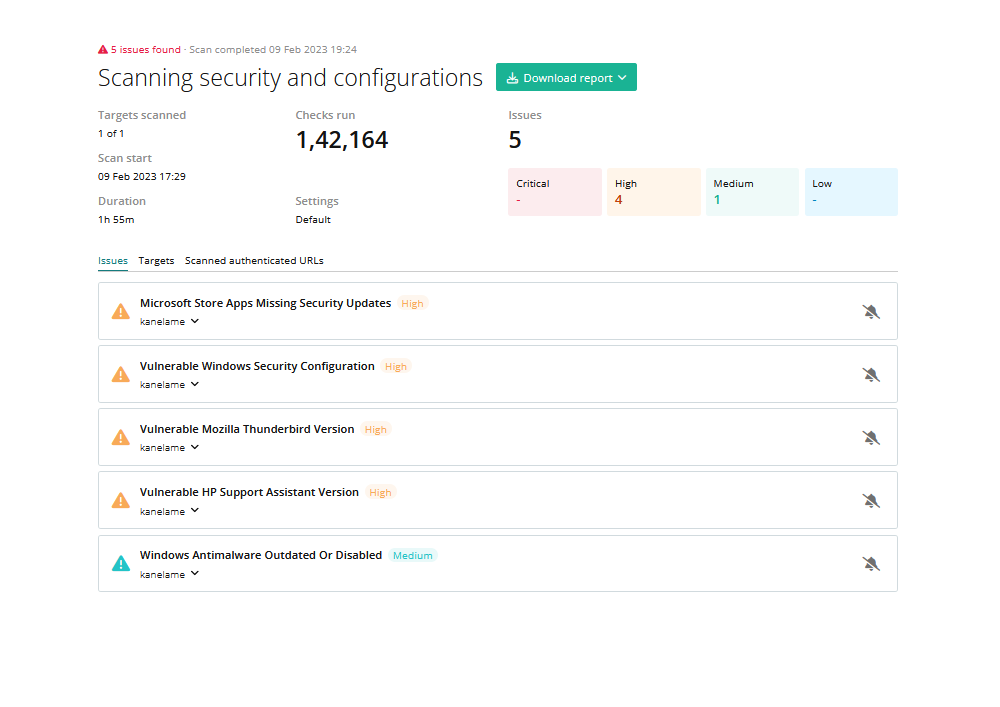
Scanning assessment will take time.



Click on scans tab to check the progress.



Further clicking on the scan progress, we can see the scanning process and the security status.



When the scanning gets completed , a list of vulnerabilities will appear according to their severity.

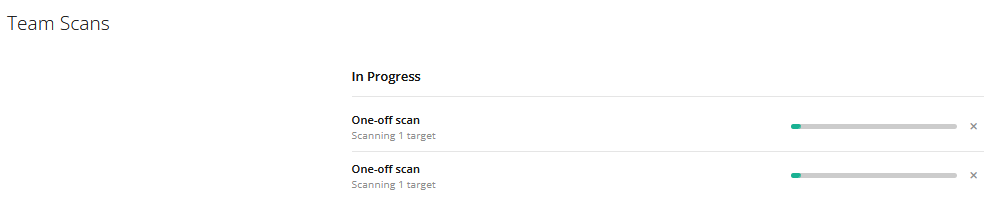
To get the whole report, go to reports tab to download the report.

**Looking at more endpoints and services**

**Scanning a website**

To start the scan of a website, we have to do the same steps while declaring the target but this time we have to select **External Ip/Domain** option.

Then add all the details such as website name, here I am testing <testphp.vulnweb.com> .

Go to scans page to check the progress. 

It will take time ,to check the reports we have to check the reports tab.

**Conclusion**

It is important to check your system security weaknesses time to time. Intruder vulnerability scanner is one of the best scanners out there in the market. Talking about its scanning efficiency and UI anyone can use it with proper guidance. Companies should perform vulnerability assessment regularly.