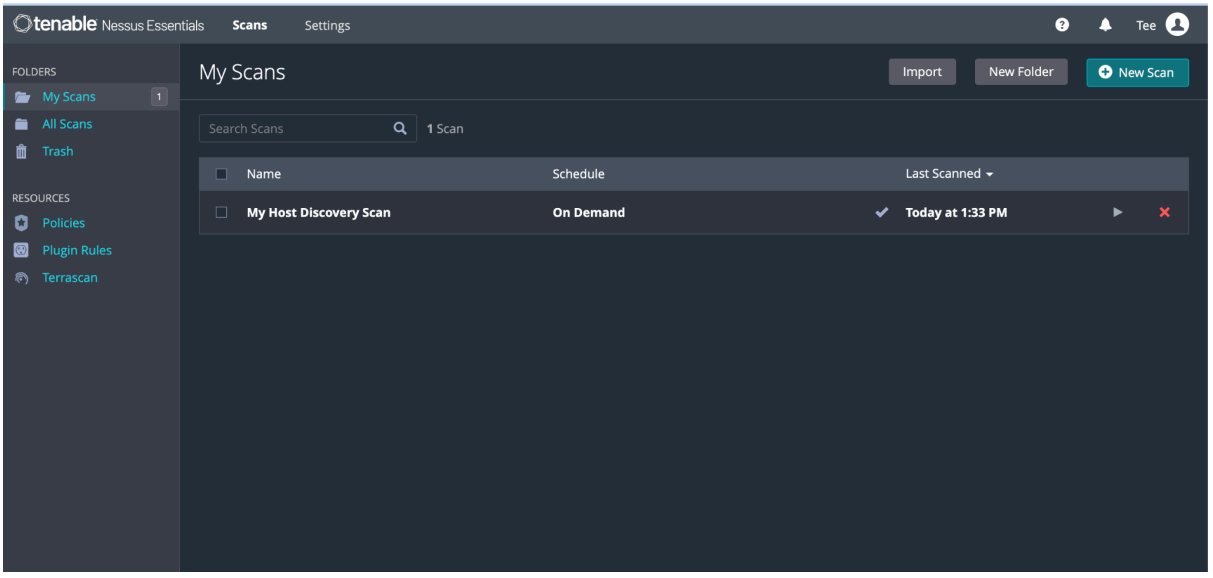
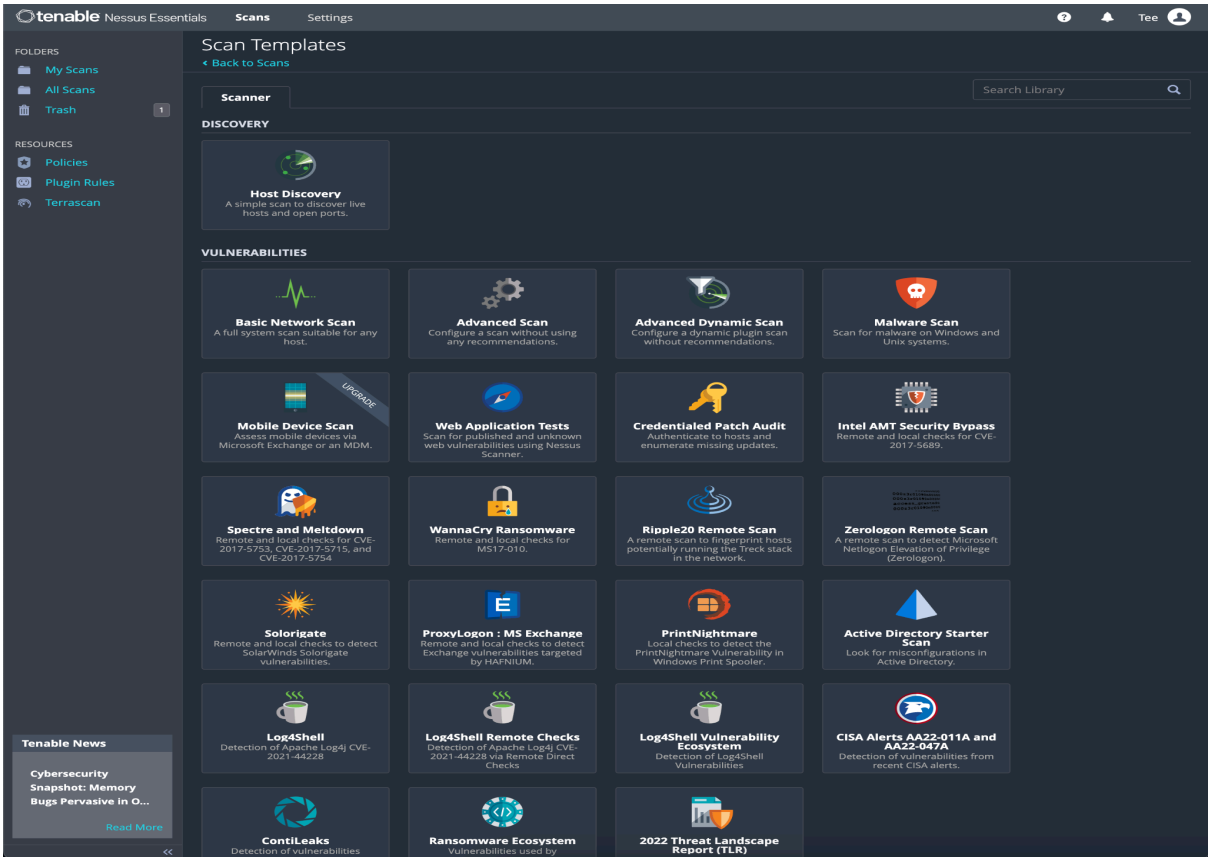
Vulnerability Scanning and Management

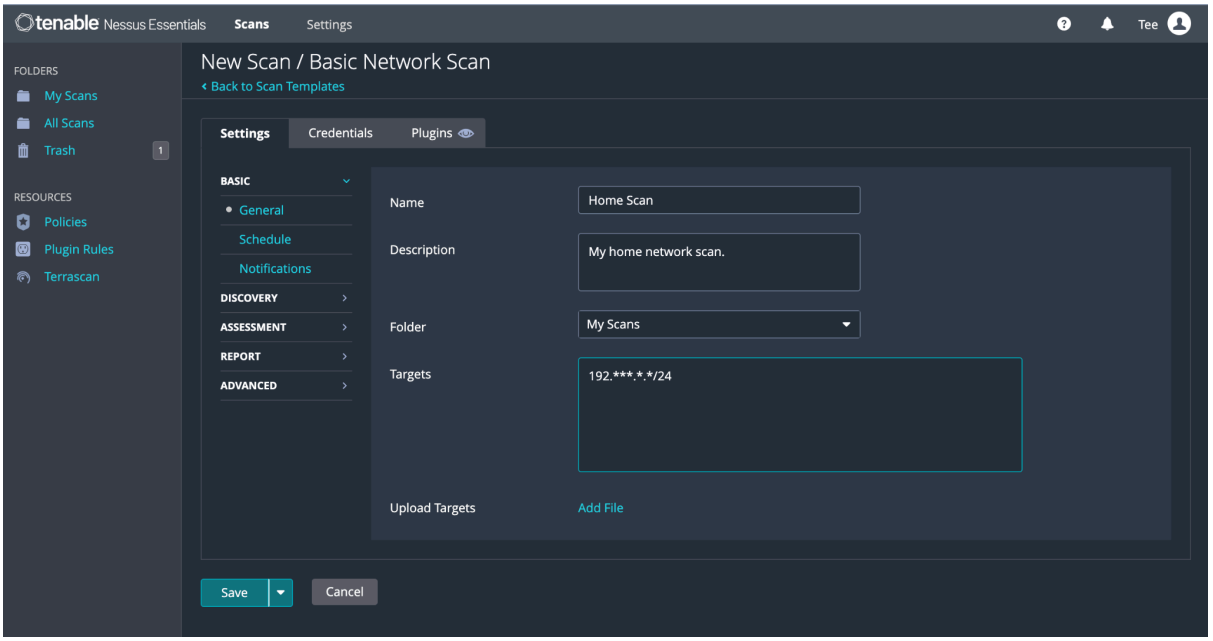
The aim of this demo is to create a step by step guide on how to conduct a vulnerability scan using **Tenable Nessus.** The first step is to navigate to the homepage of the **Tenable Nessus** vulnerability scanner to create a new scan. On getting to the homepage, locate and click on the '**new scan'** option on the top-right corner of the screen as indicated below:



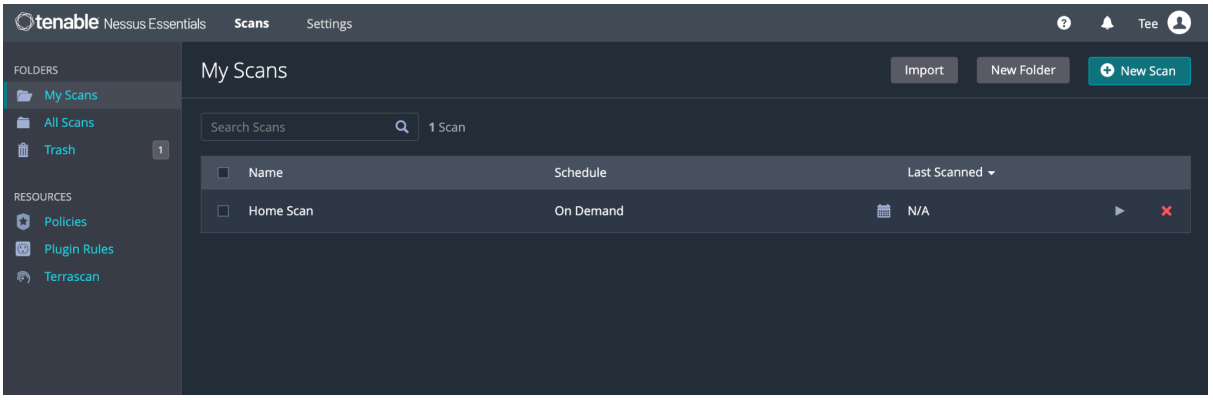
The next page will display a variety of possible scans provided by **Nessus.** For the sake of this demo, I'll be doing a basic network scan. Hence the next step is to click on the '**basic network**' scan option as illustrated below:



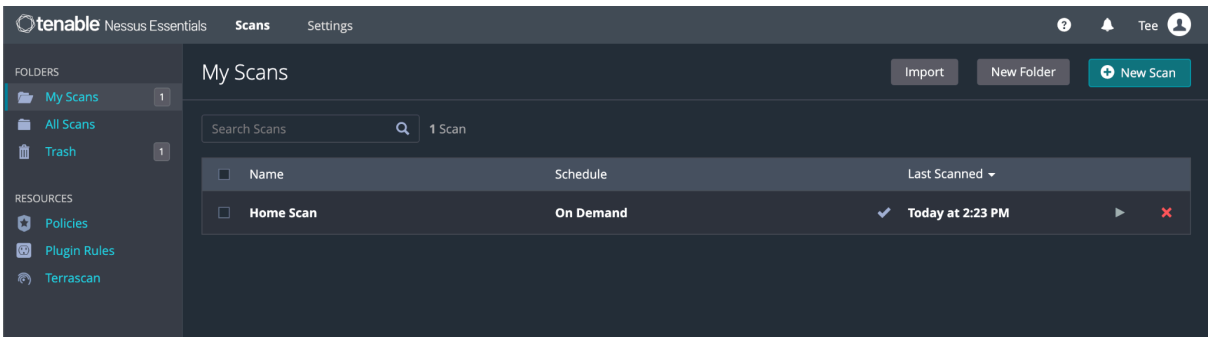
Clicking on the **'basic discovery scan'** option displays a window asking for basic descriptions such as name, description, folder, and targets. When the required fields have been filled, click on the save option. This is illustrated below:



After saving, the window illustrated below pops up. The next step is to click on the play button '►' at the end of the newly created scan line.

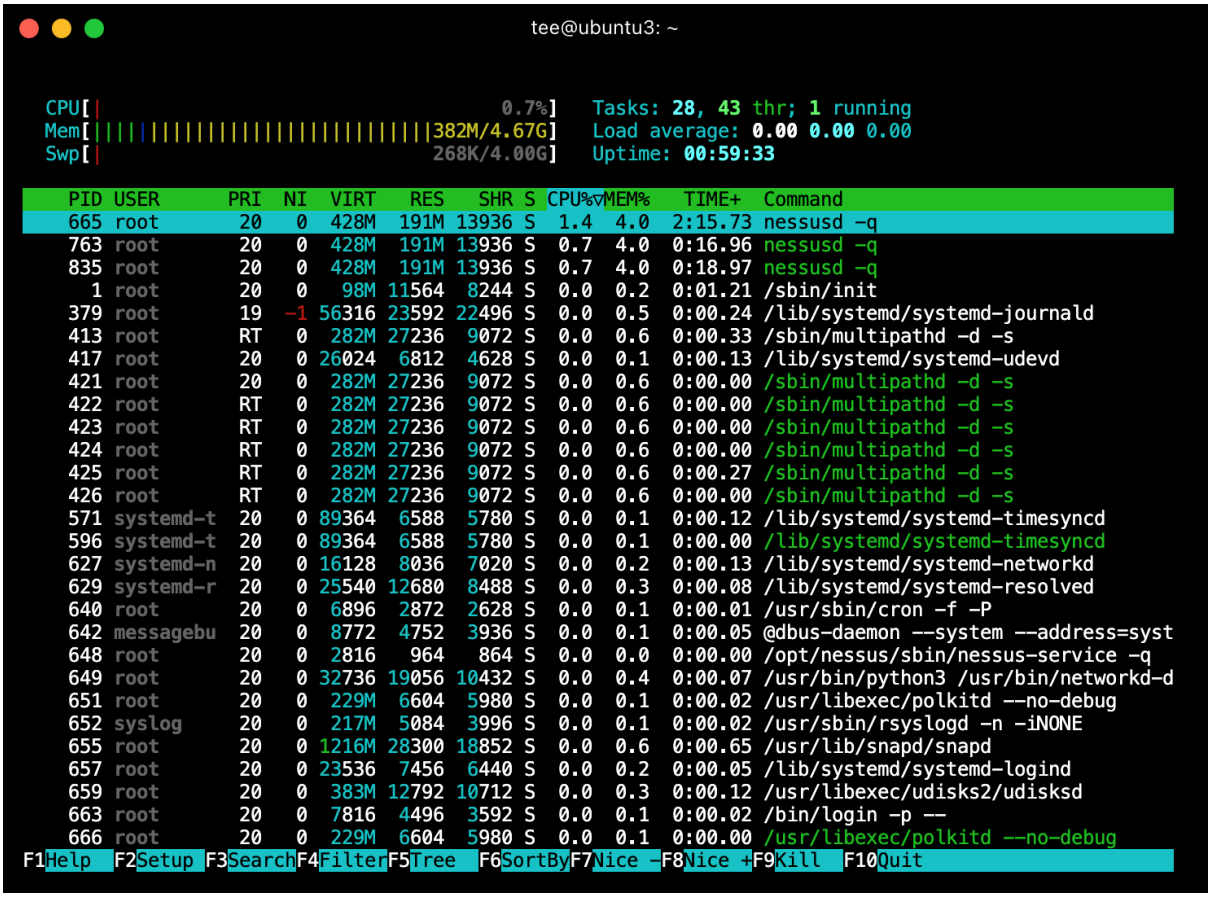


When the scan is completed, the **'last scanned'** tab of the scan shows when the scan was last completed as illustrated below:

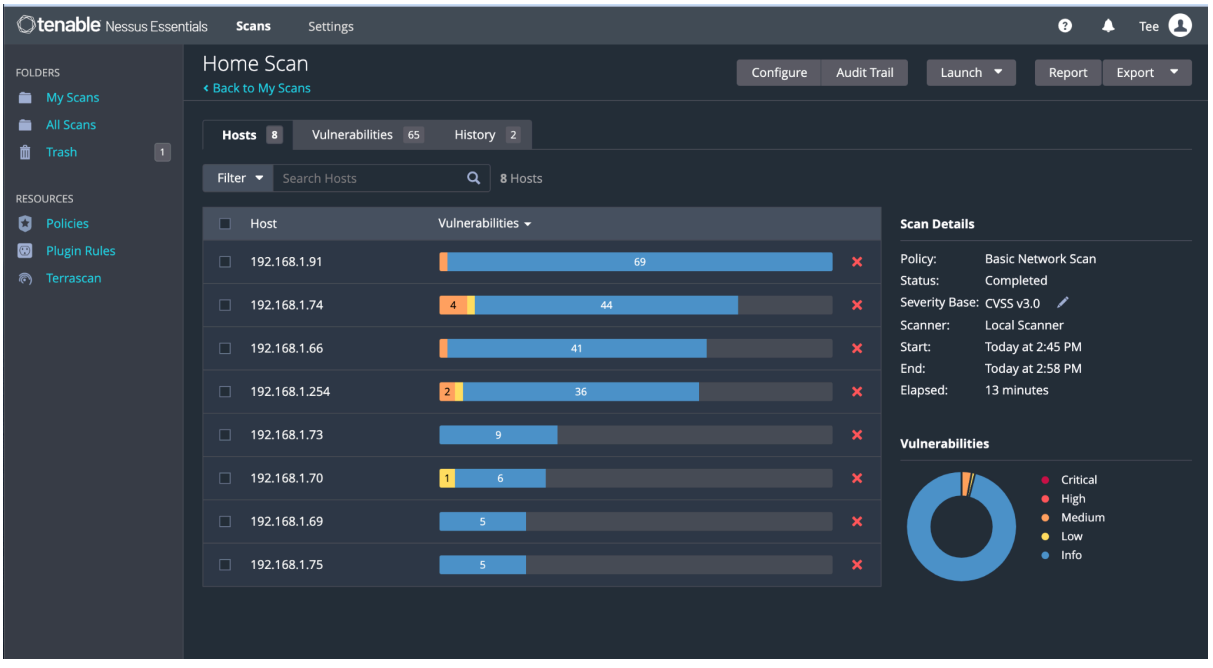


The image above shows that the scan was last scanned today at 2:23pm.

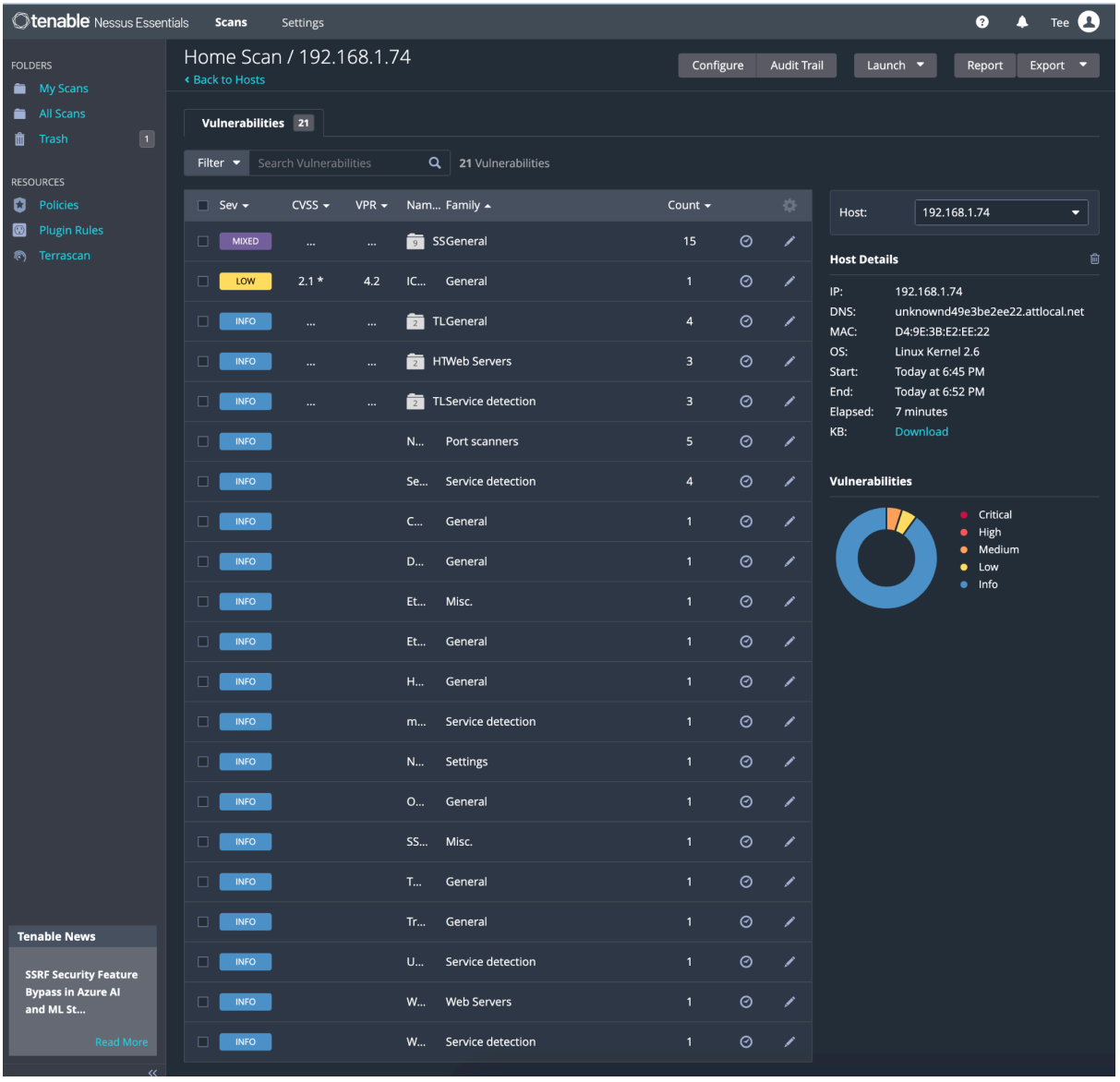
Running the '**htop**' command via the CLI will display the processor as shown below:



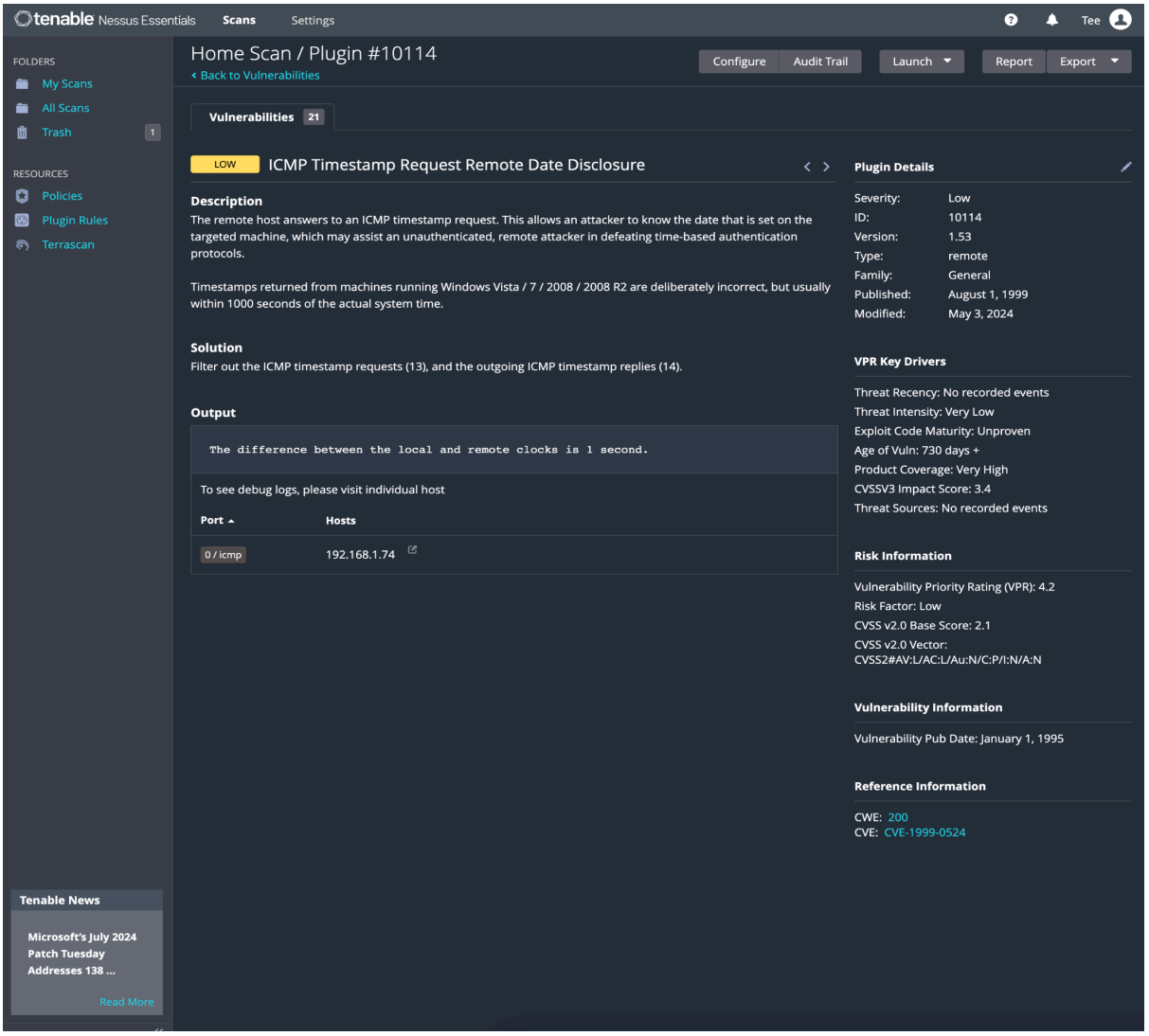
To view the output of the just completed scan, click on the **Home Scan** tab on the **My Scans** window. The output is shown below:



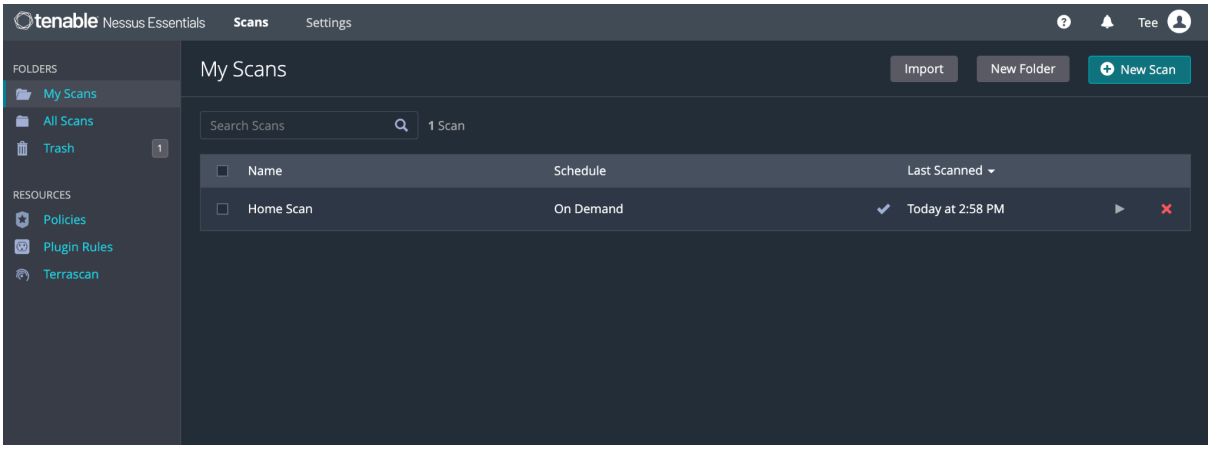
As shown in the scan result, host 192.168.1.74 has the most critical vulnerabilities. To show more details about the output of this host, click on it. This is illustrated below:


tenable Nessus Essentials
Scans
Settings
Tee
FOLDERS
My Scans
All Scans
Trash 1
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
SSRF Security Feature Bypass in Azure AI and ML St...
Read More
Home Scan / 192.168.1.74
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 21
Filter
Search Vulnerabilities
21 Vulnerabilities
Sev
CVSS
VPR
Nam...
Family
Count
MIXED ... ... SSGeneral 15
LOW 2.1 * 4.2 IC... General 1
INFO ... ... TLGeneral 4
INFO ... ... HTWeb Servers 3
INFO ... ... TLService detection 3
INFO N... Port scanners 5
INFO Se... Service detection 4
INFO C... General 1
INFO D... General 1
INFO Et... Misc. 1
INFO Et... General 1
INFO H... General 1
INFO m... Service detection 1
INFO N... Settings 1
INFO O... General 1
INFO SS... Misc. 1
INFO T... General 1
INFO Tr... General 1
INFO U... Service detection 1
INFO W... Web Servers 1
INFO W... Service detection 1
Host: 192.168.1.74
Host Details
IP: 192.168.1.74
DNS: unknownd49e3be2ee22.attlocal.net
MAC: D4:9E:3B:E2:EE:22
OS: Linux Kernel 2.6
Start: Today at 6:45 PM
End: Today at 6:52 PM
Elapsed: 7 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

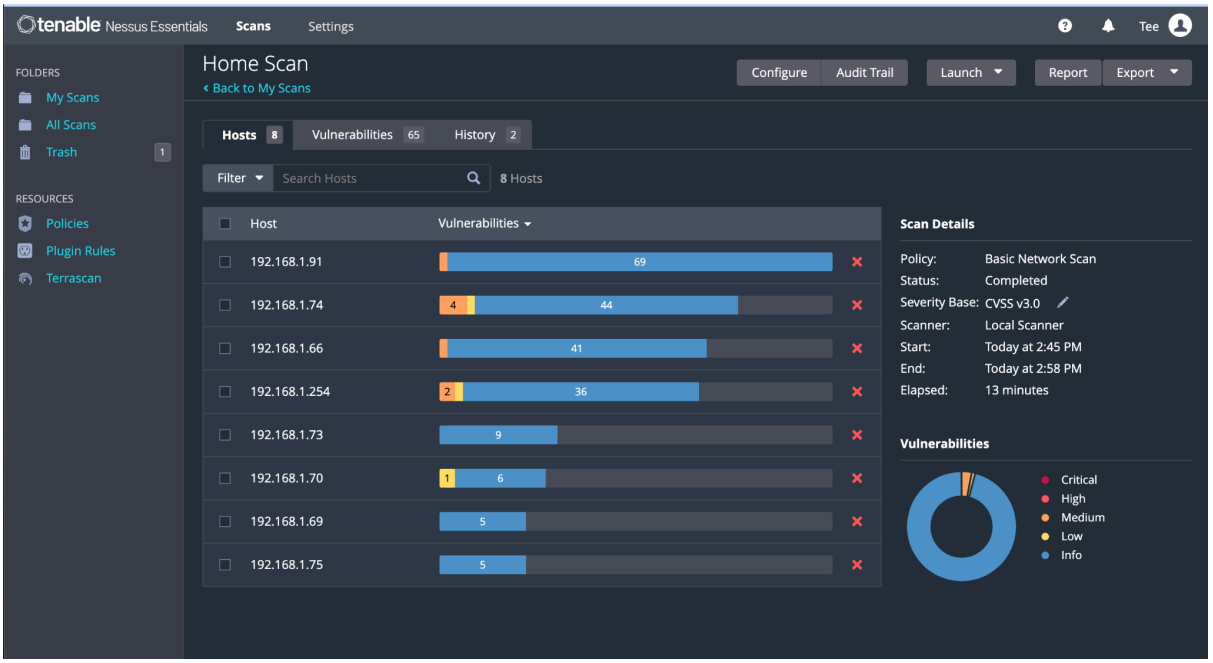
To further dive into this vulnerability, I'll click on the **Low** tab since that is the highest rated vulnerability on my network. Clicking on this provides more insight into this vulnerability as illustrated below:



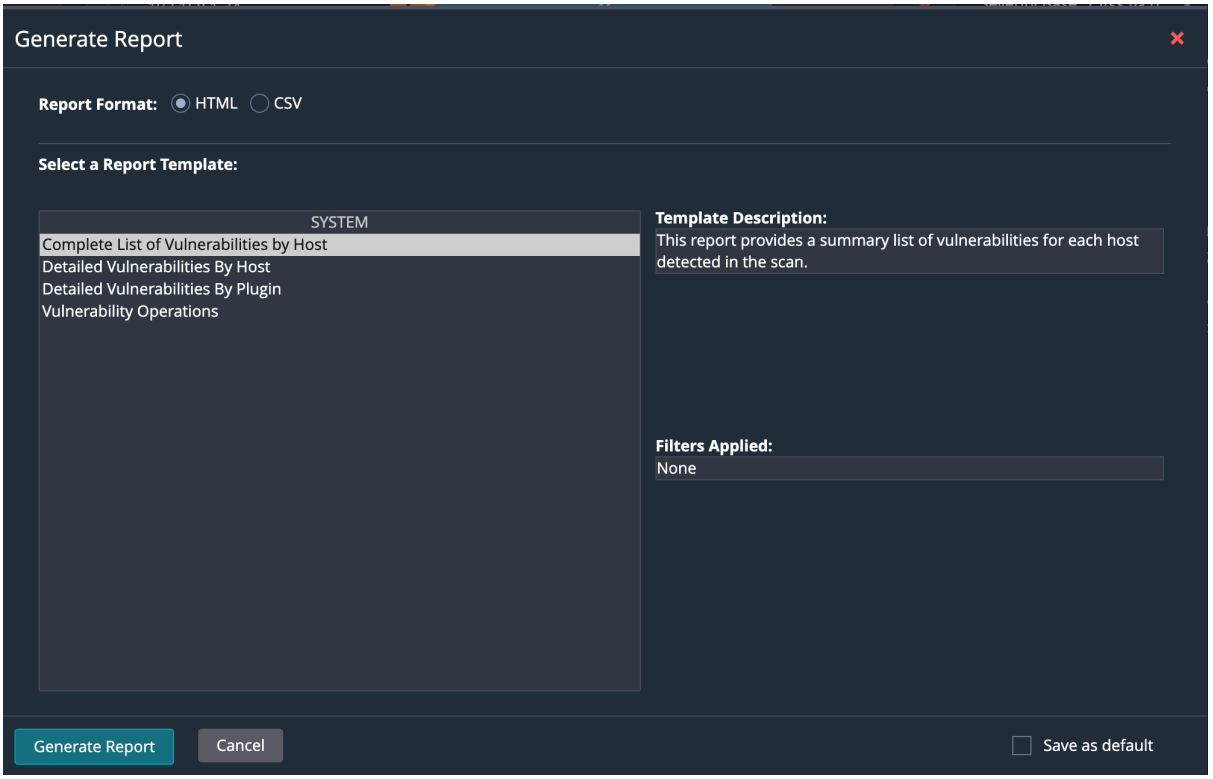
After looking over this vulnerability, the next step is to generate a report. To do this, I have to return to the **My Scans** folder by clicking on it at the top-left corner of the screen. This is illustrated below:

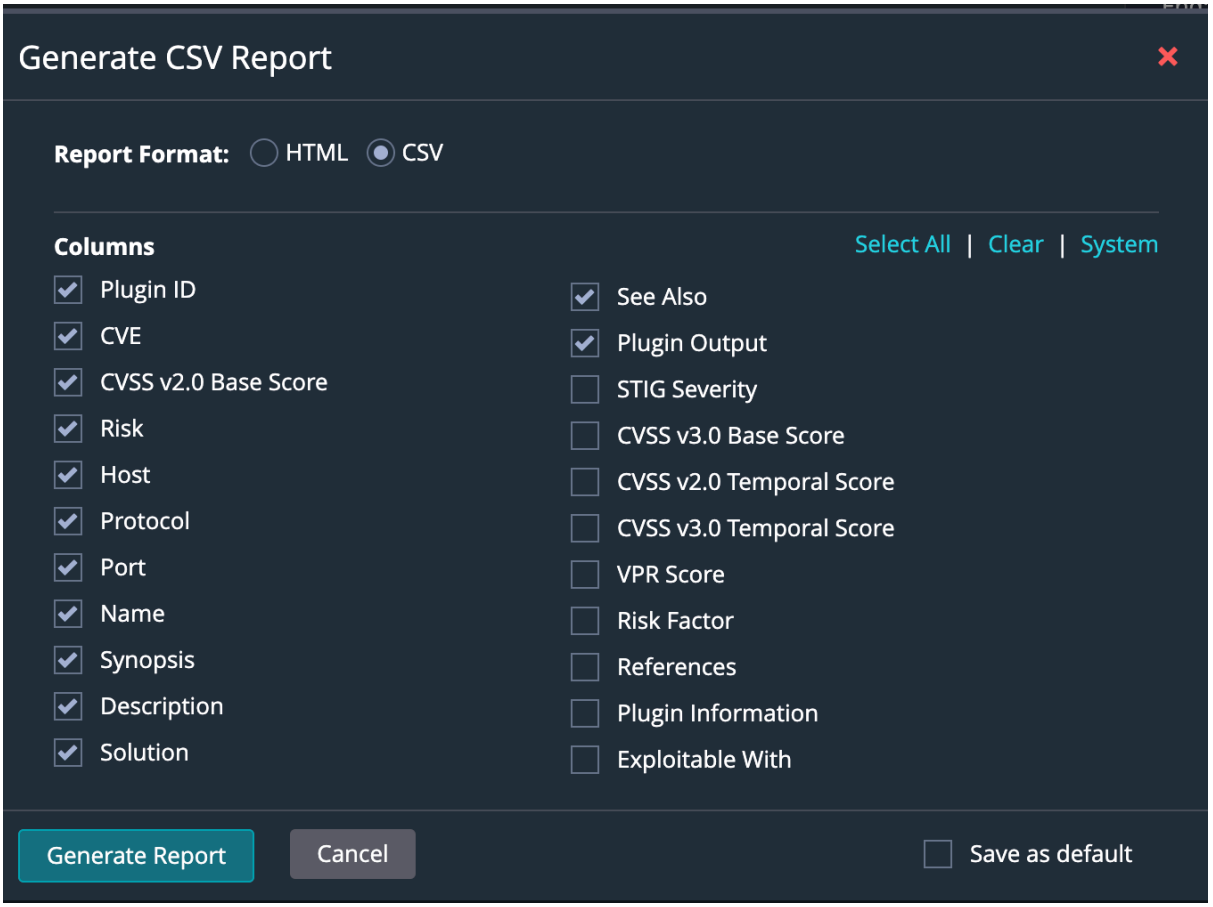


When in this folder, click on the desired scan, in this case that will be the **Home Scan.** When in the **Home Scan** folder, click on the **report** tab at the top-right corner of the screen to generate a report as shown in the illustration below:

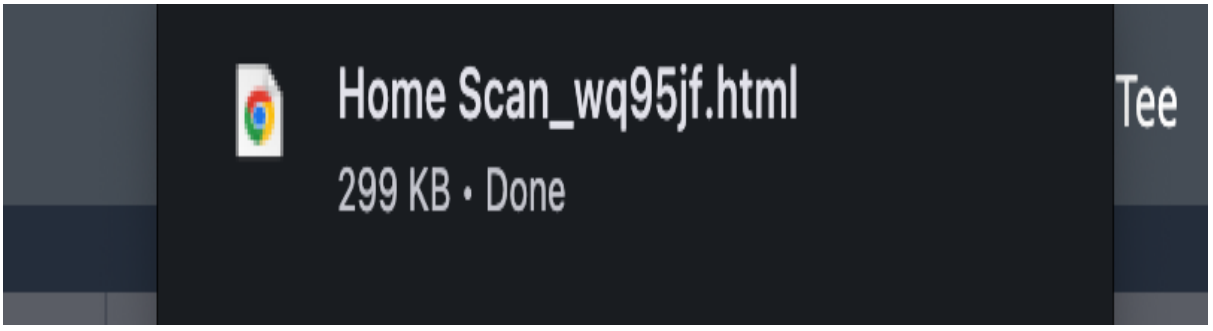


Upon clicking on the **report** option, there is provision to choose in what format one would like their report. The two options provided by **Nessus** are **HTML** and **CSV** as illustrated below:

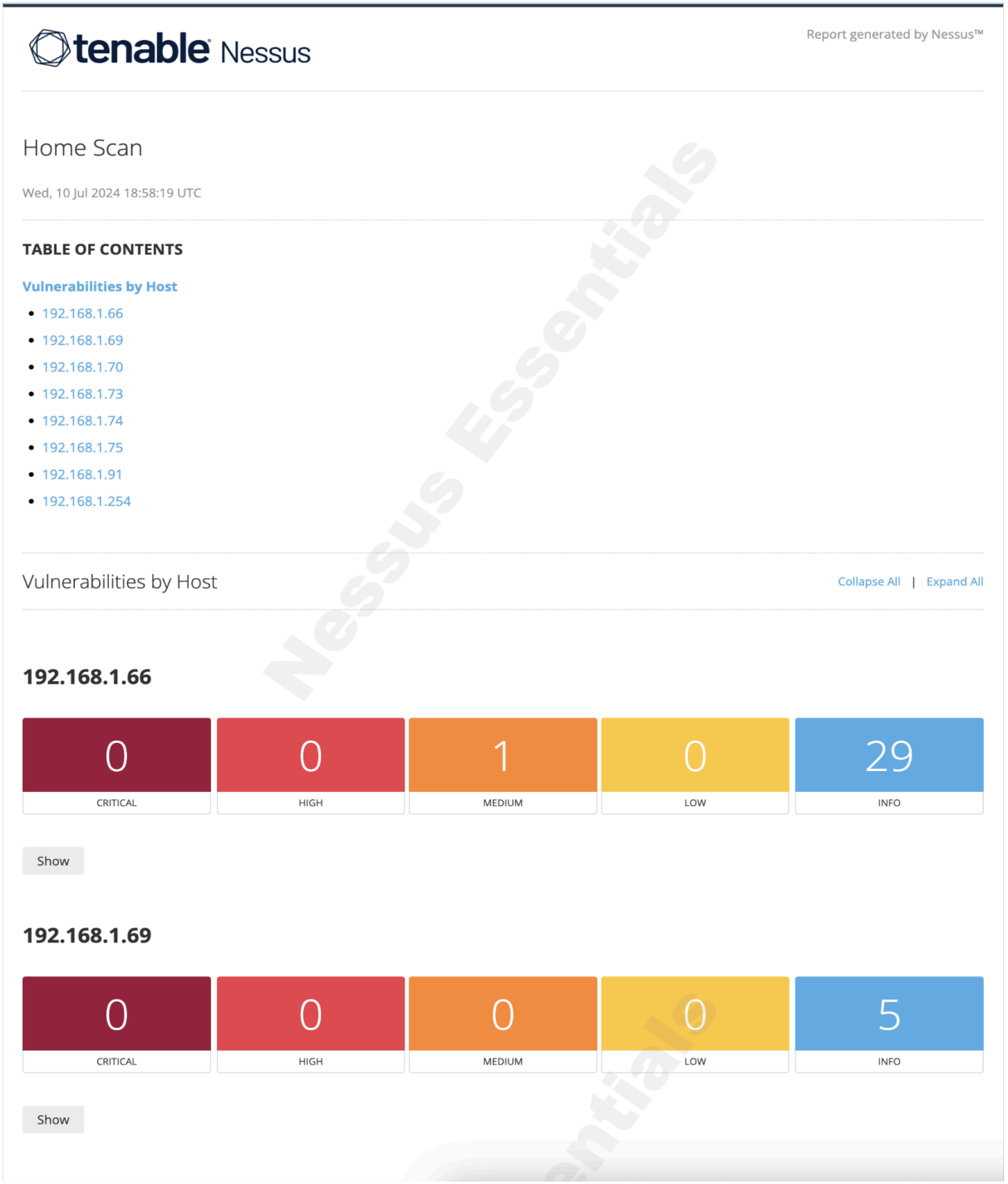




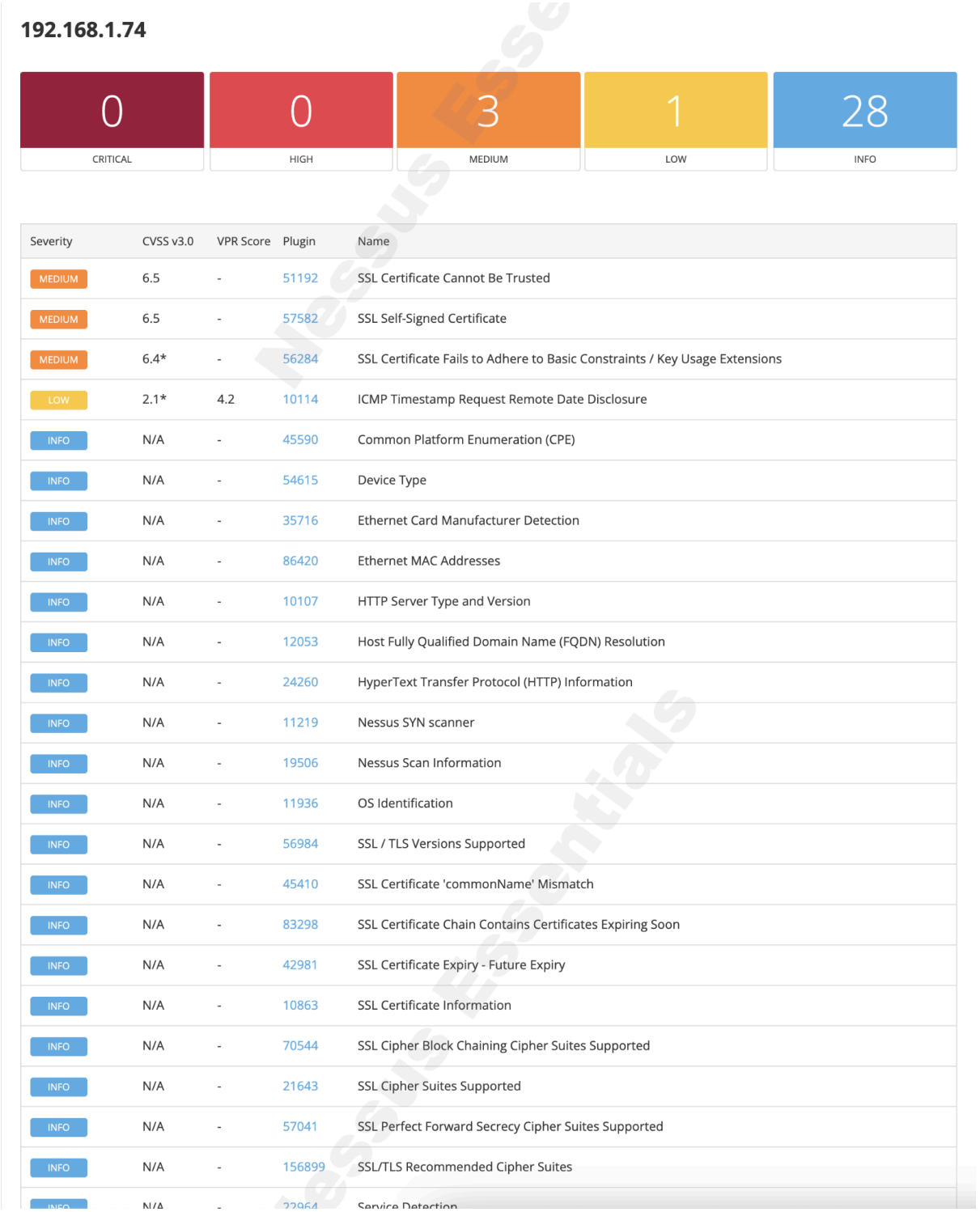
After choosing the desired file format, click on the **Generate Report** option at the bottom-left of the pop-up window. When this is done, the report is downloaded onto the host computer and saved to the **Downloads** folder. This is illustrated below:



Opening the downloaded report shows a comprehensive, and brightly-colored user-friendly report. This is illustrated below:



Clicking on the **Show** option at the bottom of each host displays a more comprehensive output of the vulnerability scan of that particular host. This is also illustrated below:

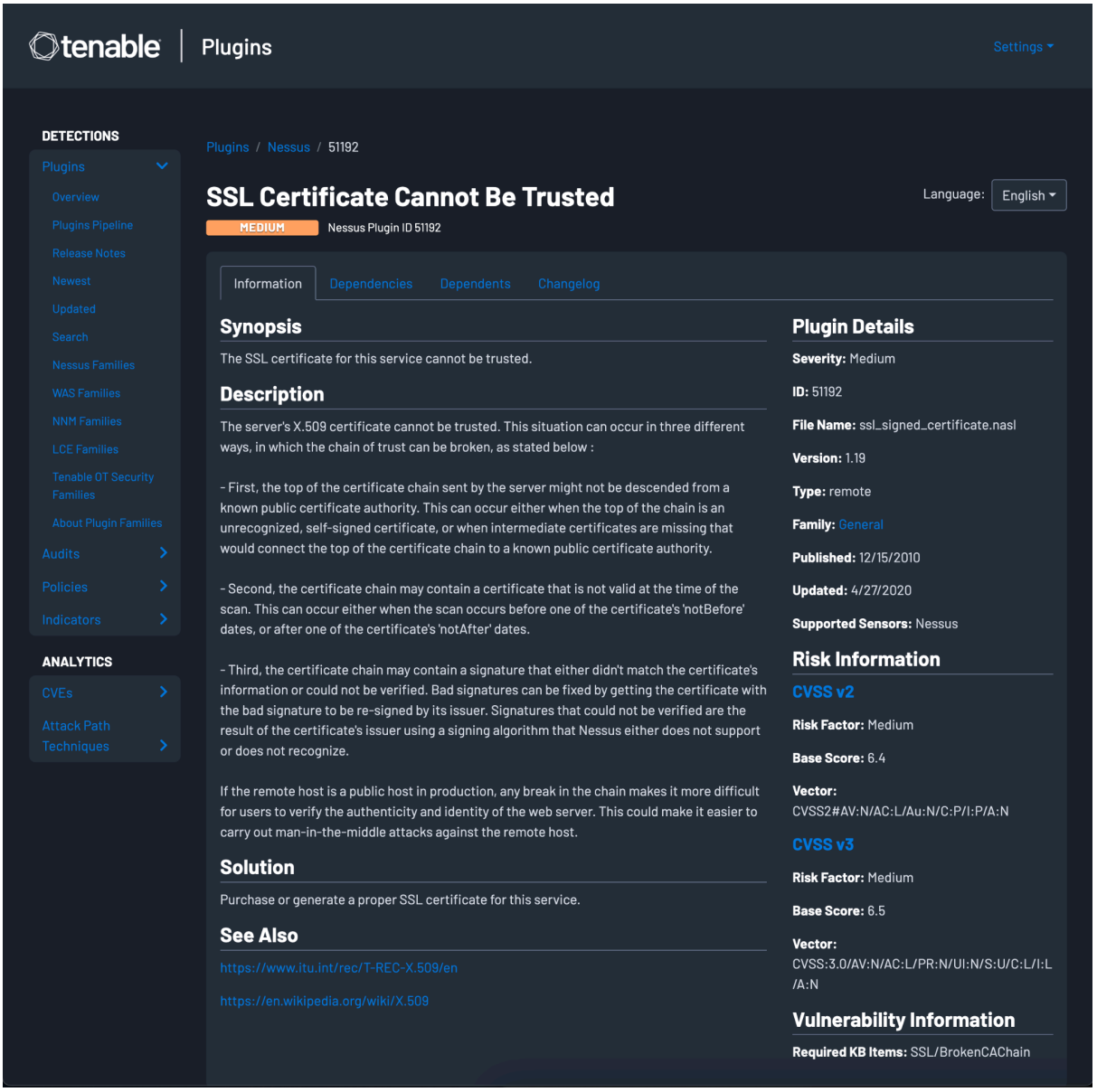


192.168.1.74

0	0	3	1	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

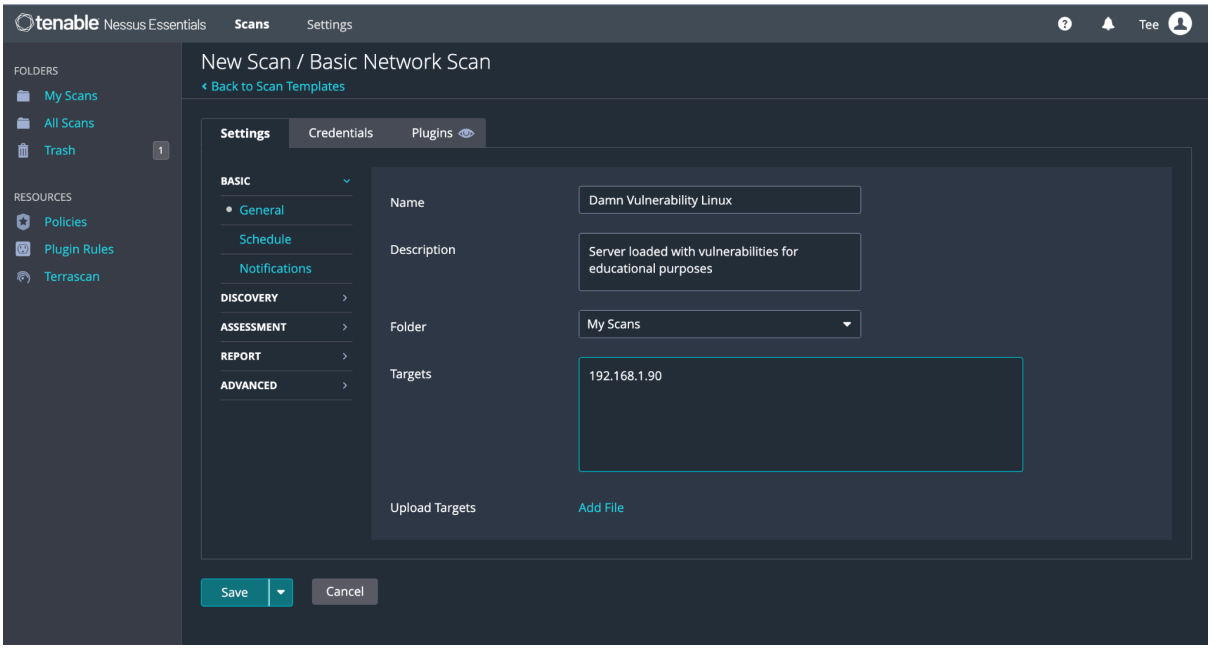
Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.4*	-	56284	SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection

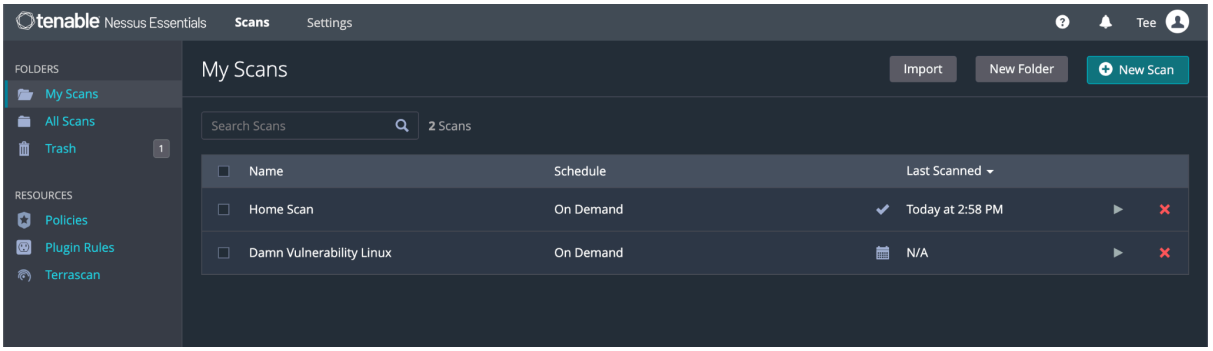
This detailed report shows the severity of the found vulnerabilities, the CVSS score, Plugins, and Name of the vulnerability. Clicking on the Plugins provides extra data relating to the vulnerability and a possible solution. An example of the extra information the Plugins provide is shown below:



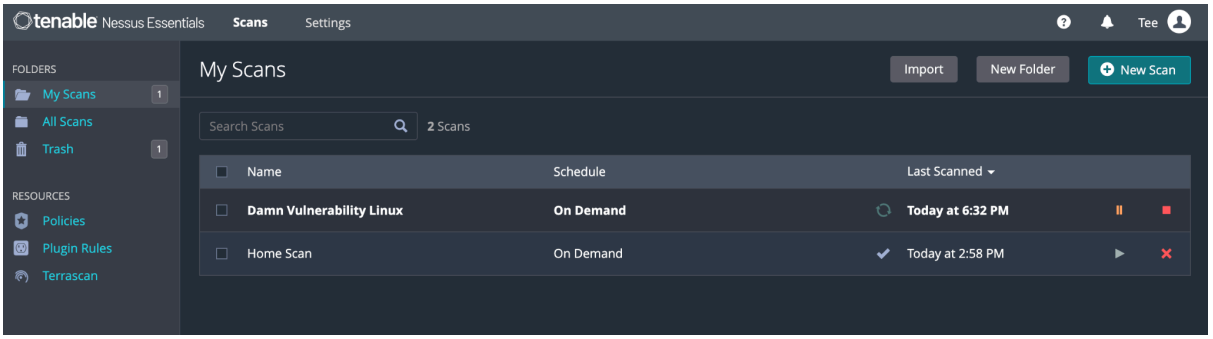
Task 2

The next step in this demo is to scan a Linux server loaded with vulnerabilities for educational purposes. The IP address to this server is 192.168.1.90. Another **Basic Network Scan** will be initiated targeting the aforementioned IP address. This is illustrated below:





Upon creation of this new scan; **Damn Vulnerability Linux** click on the play button '►' to initiate the scan. This starts the scan as illustrated below:



When the scan is complete, click on the **Damn Vulnerability Linux** scan to view the results. This is illustrated below:

A report can also be generated by clicking on the **report** option at the top-right corner of the vulnerability results page. We have successfully scanned two different servers for vulnerabilities using **Nessus.**