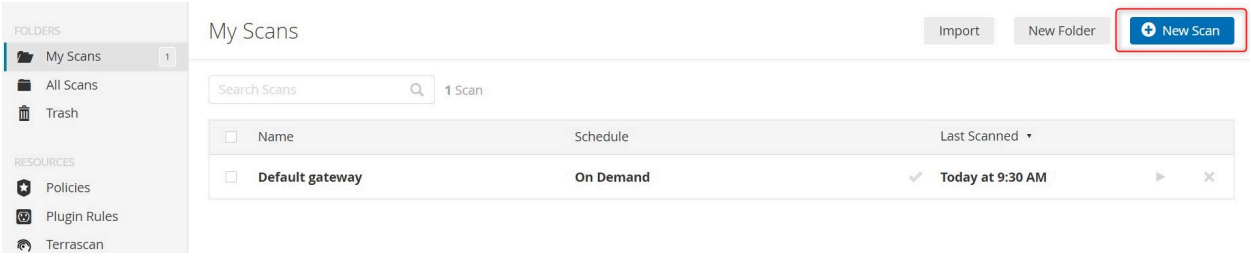
Name: Cristian Barreno

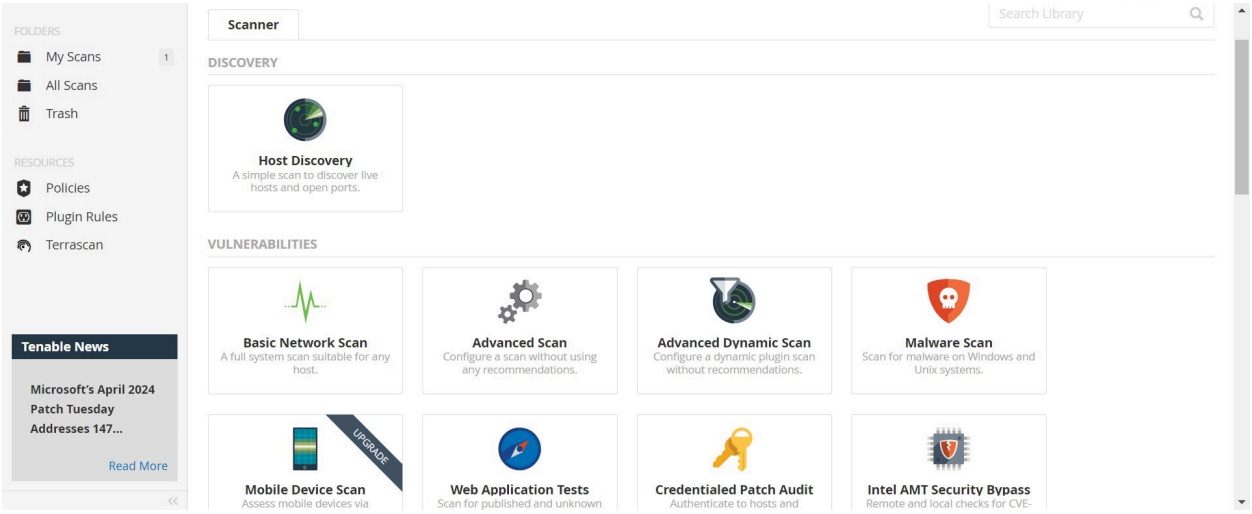
EXERCISE 3 – Vulnerability Scanning and Management

Task 1 – Conduct your first Vulnerability Scan – Home Network

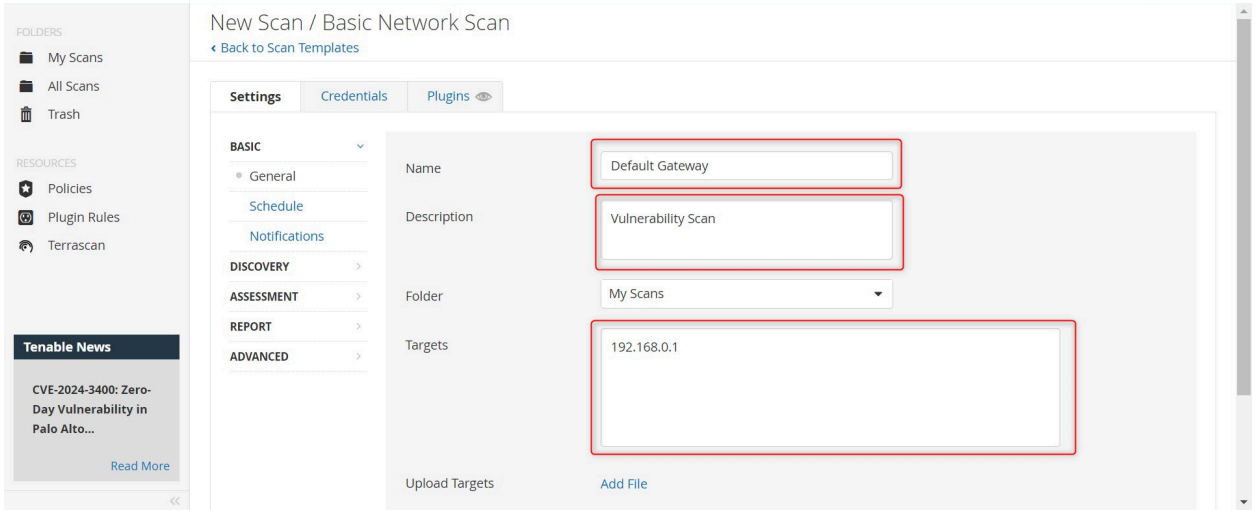
We are going to start from the dashboard of Tenable Nessus.
Next click on “New Scan”

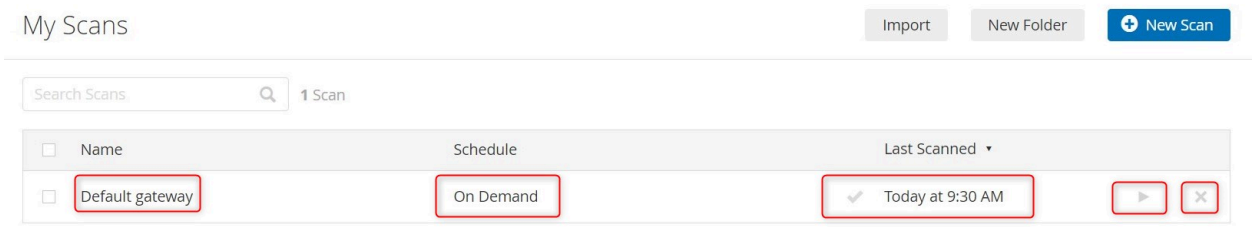


Select Basic Network Scan



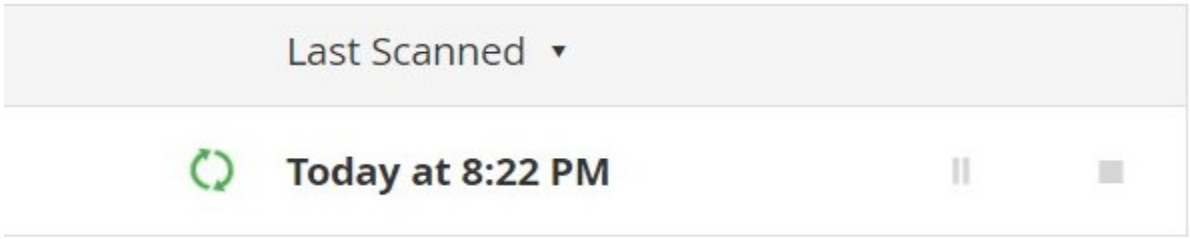
Fill out all the information required, like name, description, and target. In the Target box we are going to put the IP or IP ranges that we are going to scan.



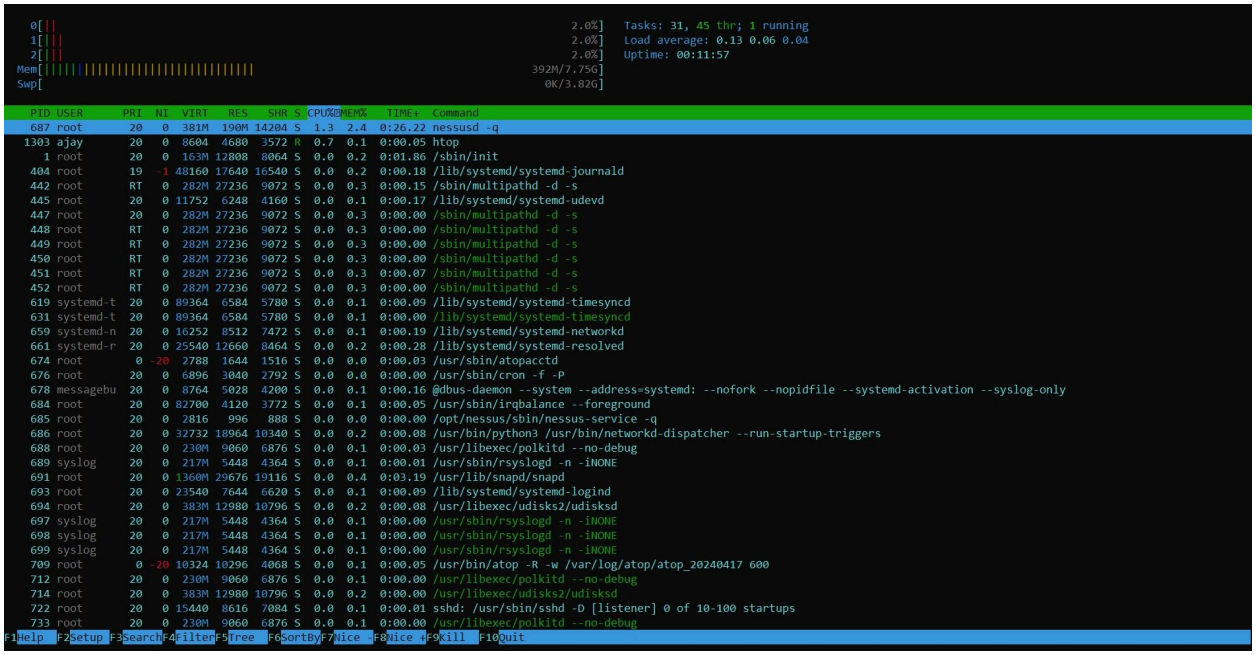


In the screenshot above we can see the name of the configured scan, if it's going to run in an automated schedule, when was the last scan run, start the scan button, and delete the scan button.

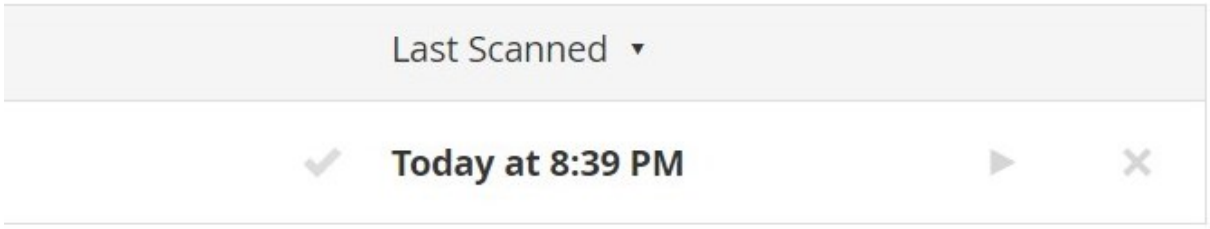
Start the scan.

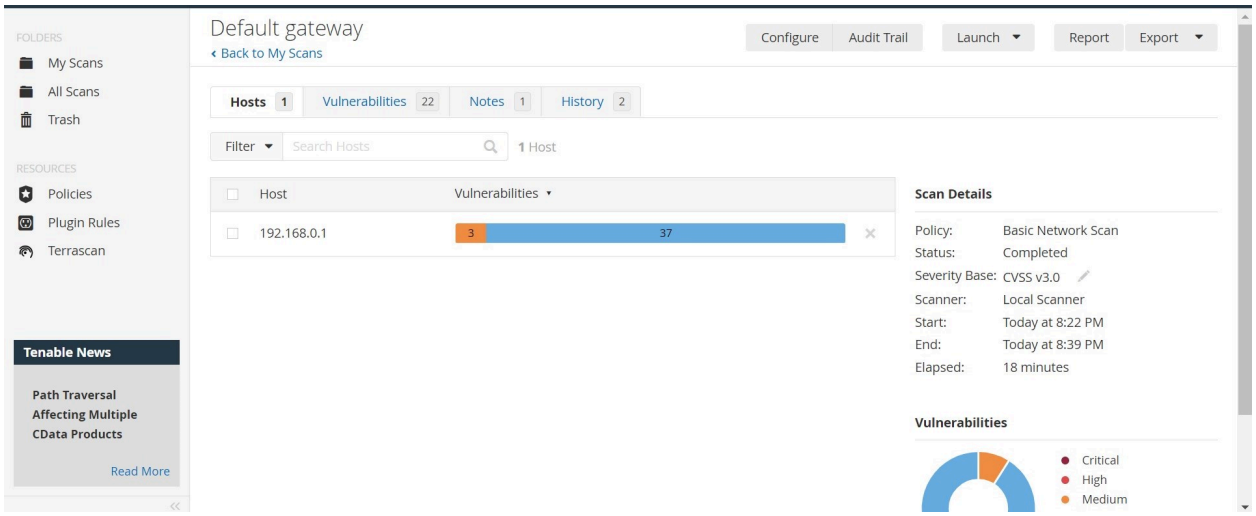


Run htop from the CLI, you will get a view of all the cores, and memory used for Nessus.



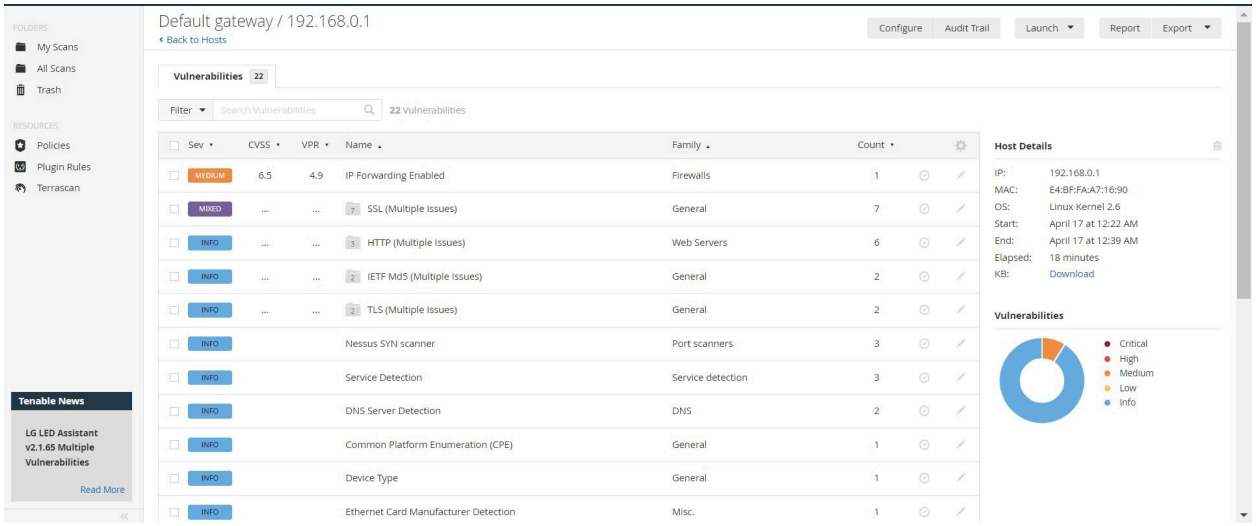
We can see a date stamp telling us when it finished scanning



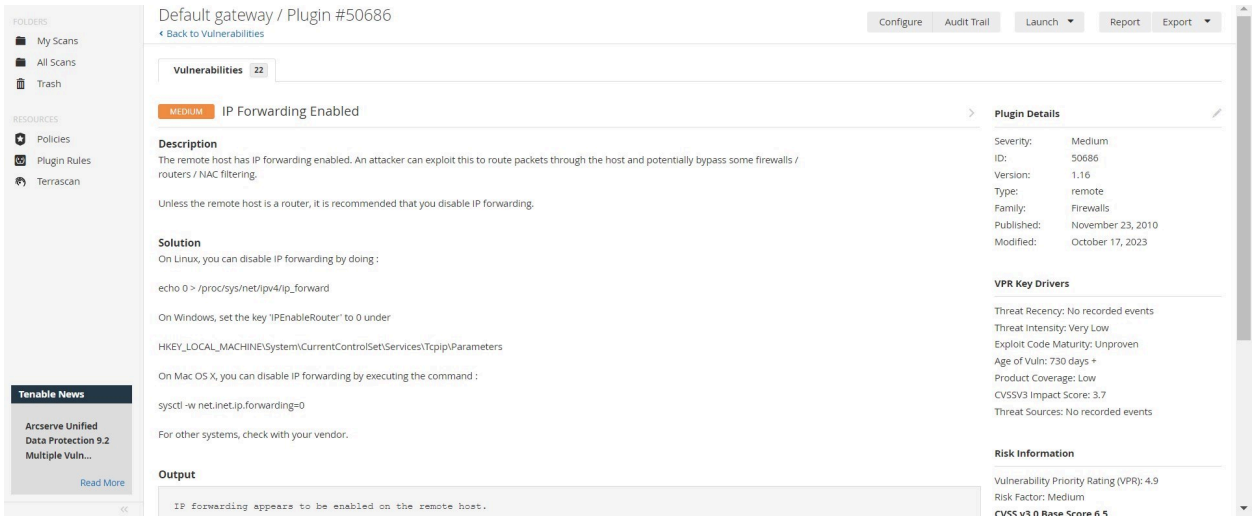


In the screenshot above we can see the vulnerabilities from the IP address that we selected.

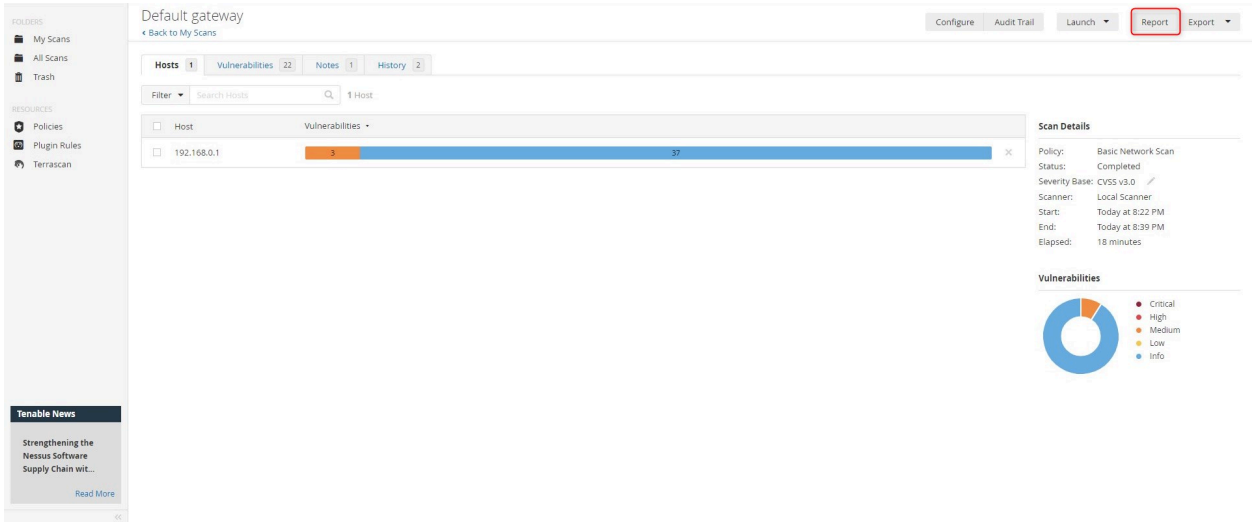
Click on the IP to see more details.



Explore more of a vulnerability by clicking on it.

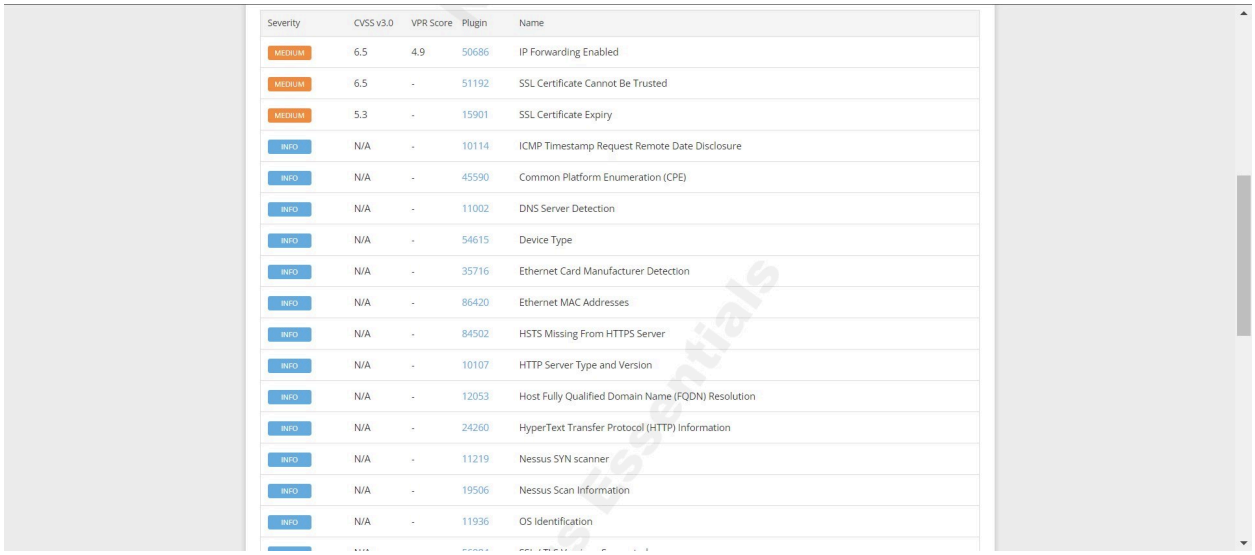


To generate a report click on the report button on the top right corner. It will download to your downloads folder.



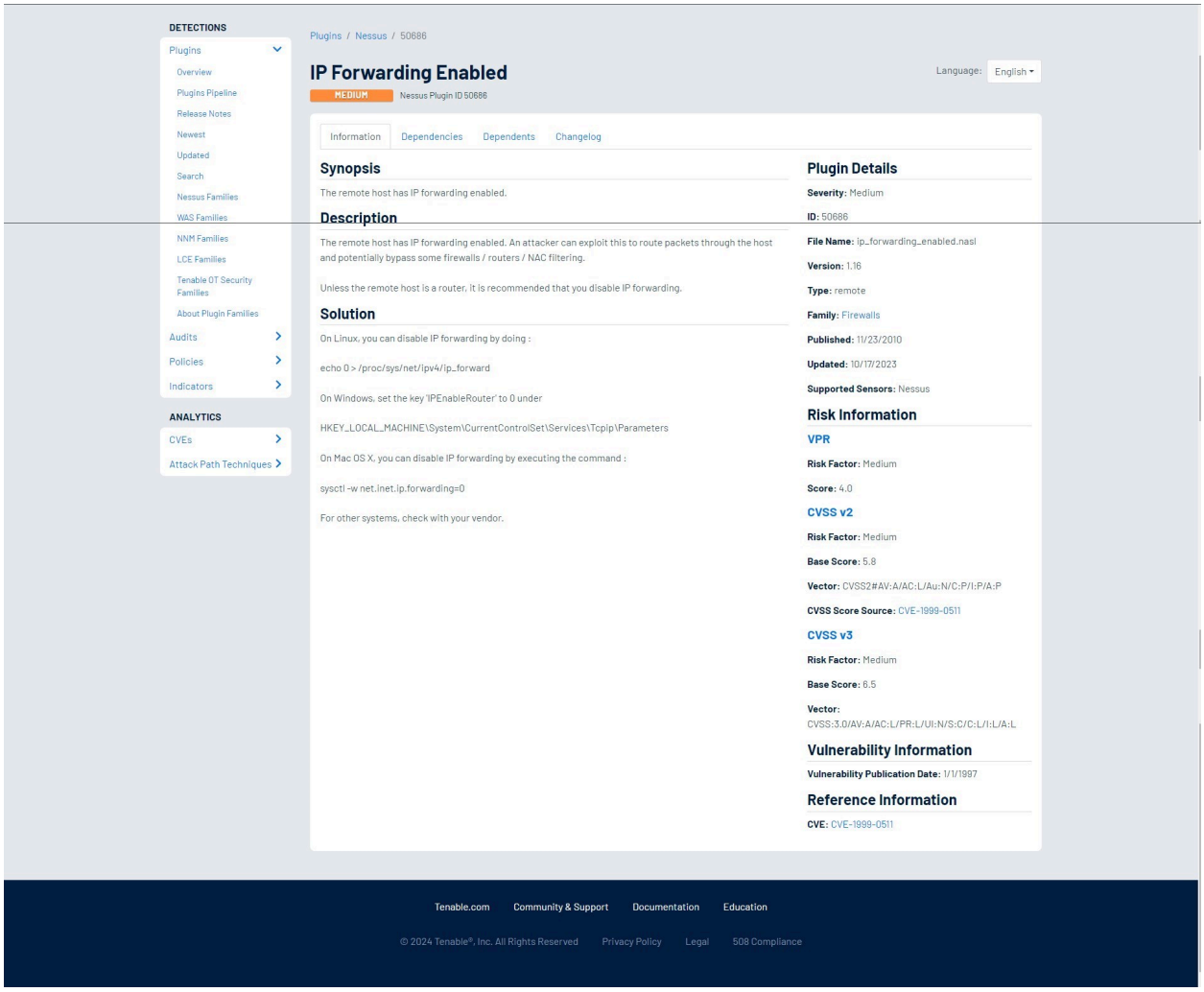
The screenshot above shows an easy to read report of the vulnerabilities scanned.

If you pick a host you can see different columns for the severity, CVSS, Plugin, and name.



Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	6.5	4.9	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	15901	SSL Certificate Expiry
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
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

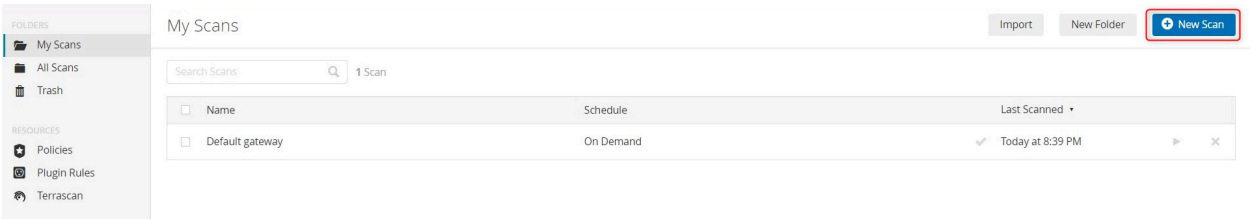
Screenshot of detailed information about a vulnerability.



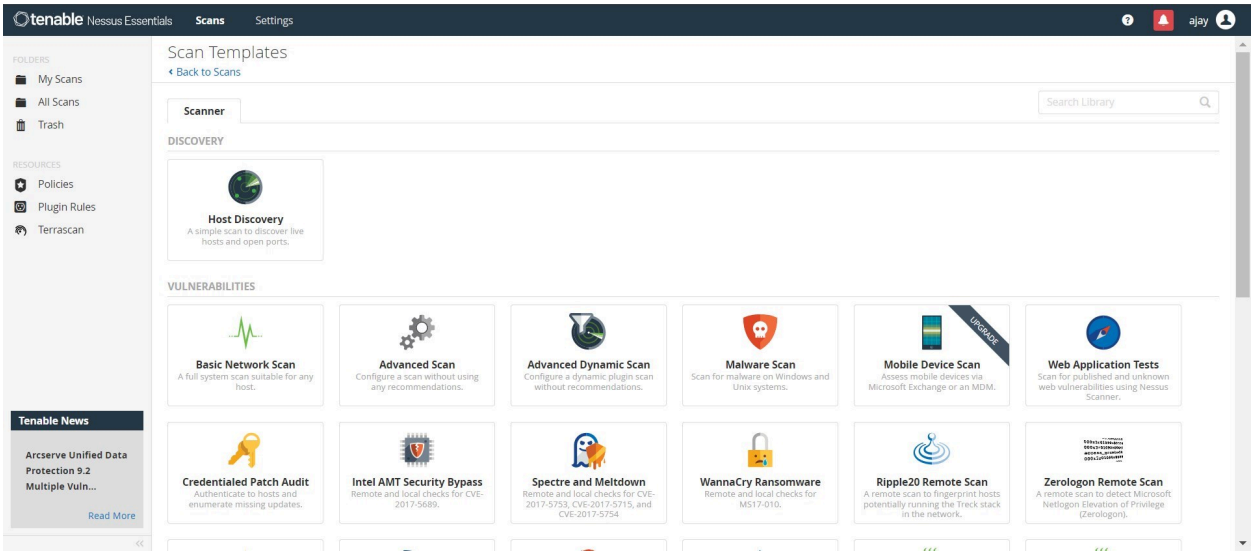
Task 2 – Conduct your first Vulnerability Scan – DVL

The first step is to have Damn Vulnerable Linux (DVL) powered on. DVL is a Linux VM that contains vulnerabilities for training purposes.

Click new scan.



Click on Basic Network Scan.



Configure a new basic network scan with the DVL IP address.
Next, launch the scan against the DVL.
The screenshot below shows the vulnerabilities scanned.