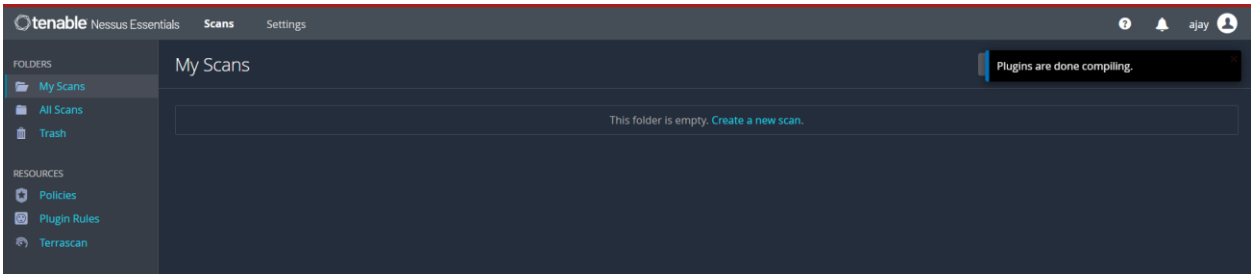
EXERCISE 3 – Vulnerability Scanning and Management

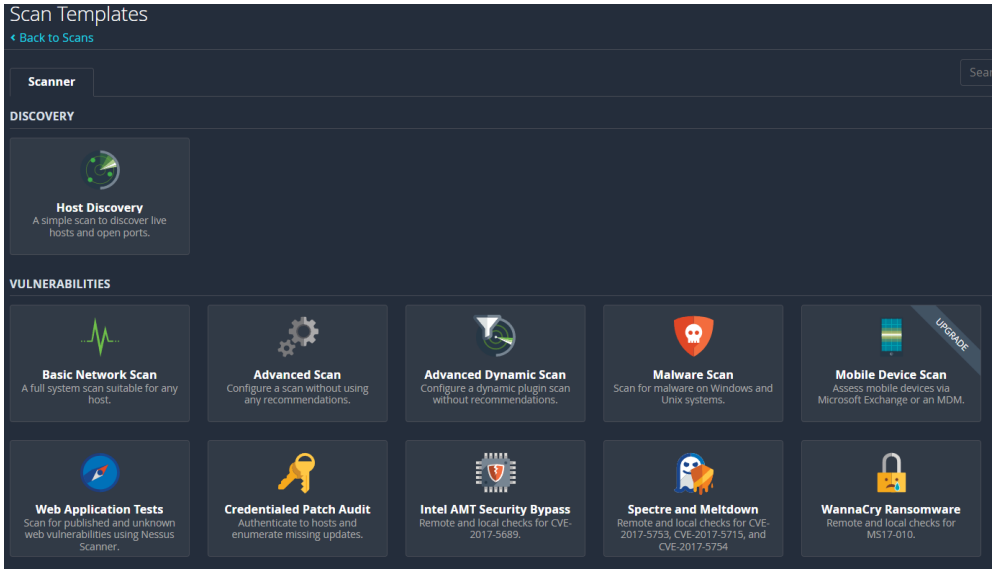
Task 1 – Conduct your first Vulnerability Scan – Home Network

Starting from the dashboard of Tenable Nessus:



Let's click on "Create a new Scan"

You will be peppered with different options, don't fret.

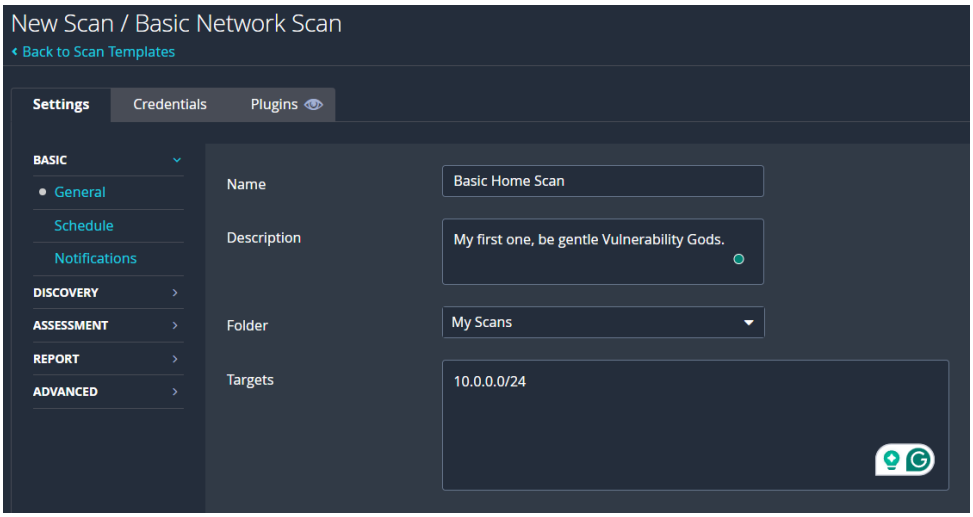


We are just going to do a **Basic Network Scan**.

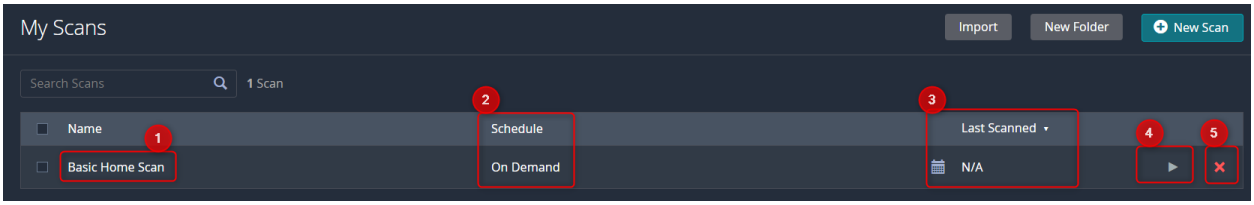
Name: Something logical, so you can understand it.

Description, something more descriptive, funny is ok at home, don't play at work.

Targets, will be your Network Scope, which will likely be different from mine. (See all that Networking and Subnetting and CIDR is... relevant.)

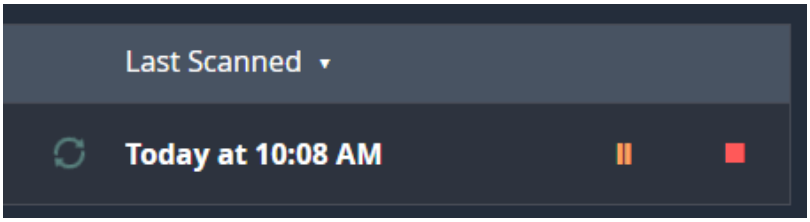


Click on SAVE



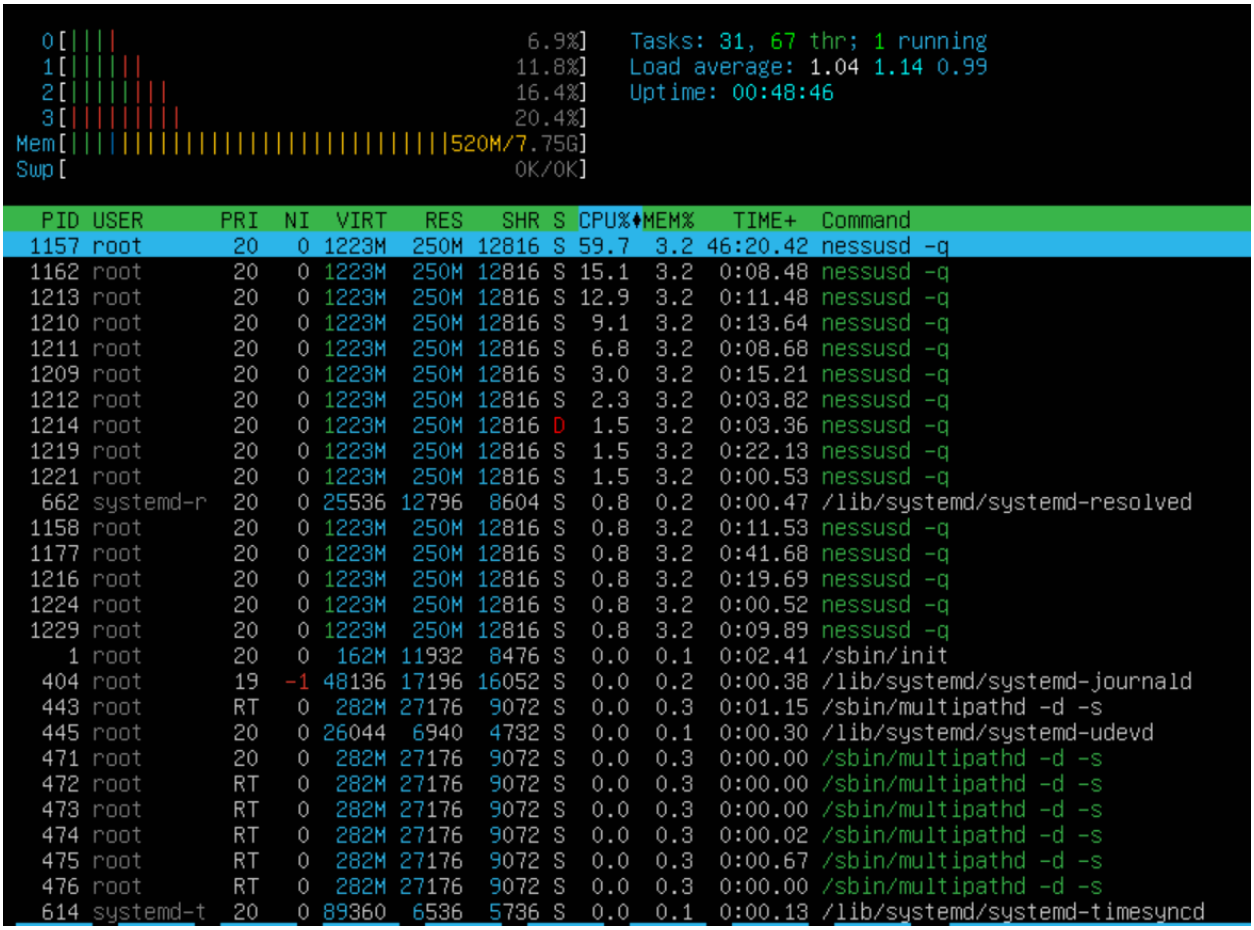
1. The name of your configured scan
2. If it is going to run on an automated schedule.
   (Would be smart, less work, more glory!) q'pla! >>:-|
3. When was the last scan run for this saved scan.
4. Start the scan ON DEMAND
5. DELETE the scan

Go ahead and start the scan ON DEMAND and it will kick off.

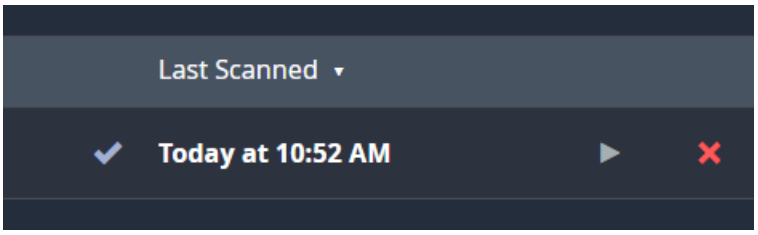


From the CLI, I can run `htop` to view how hard the server is working and this is my output.

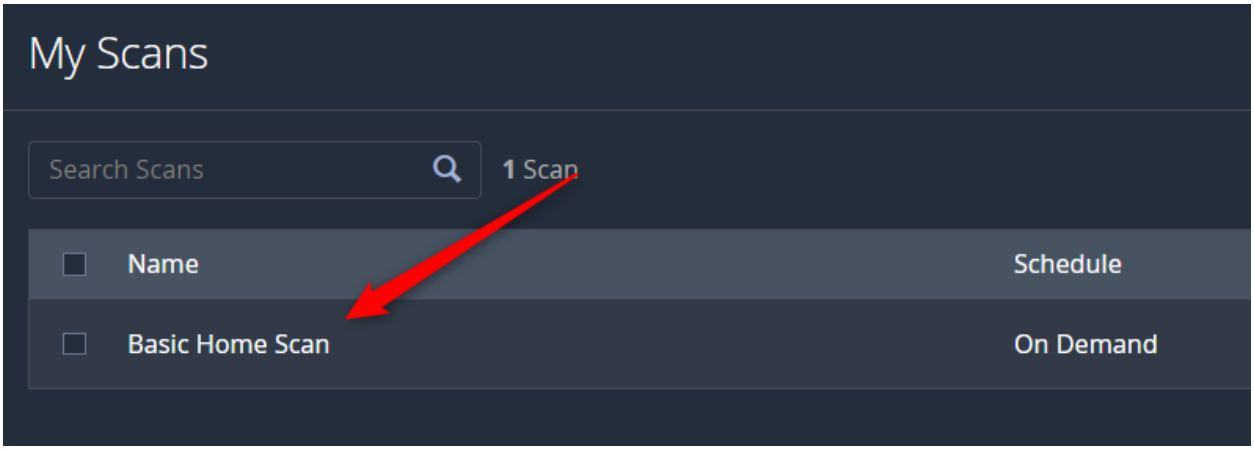
You can see all the cores working, the memory being used and a whole bunch of processor threads working `nessusd`.



This is what it looks like when the scan is finished;



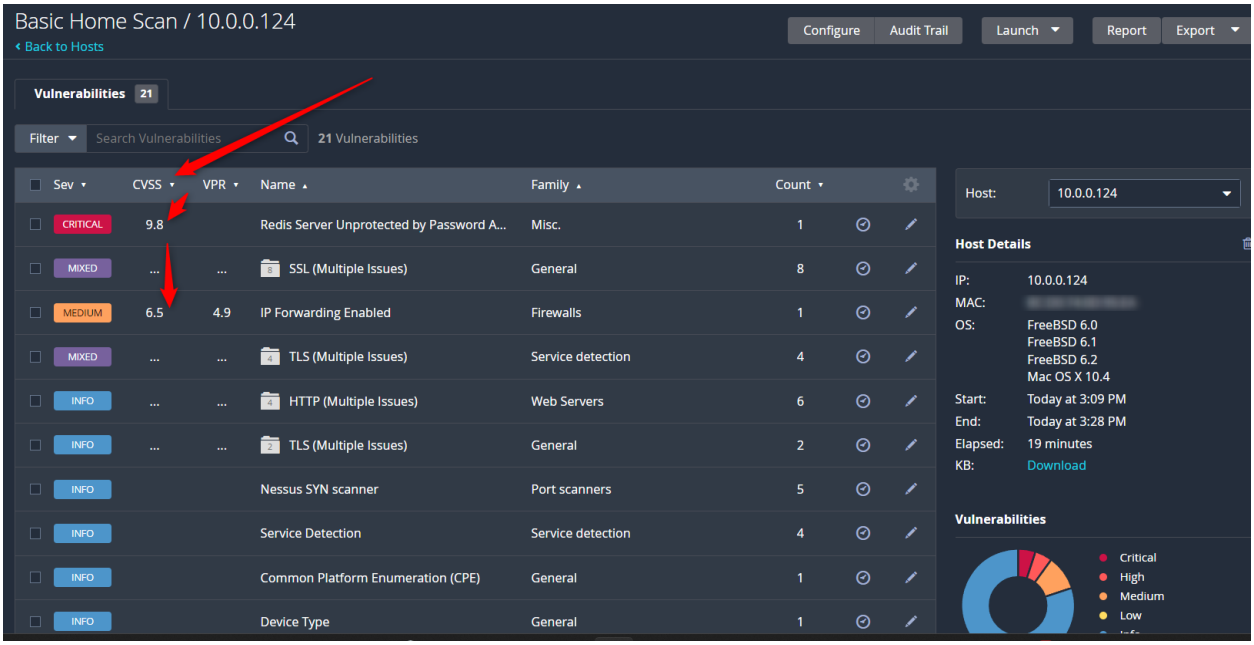
Click on the scan to see the output: (REMEMBER, your results will be different, it's your network)



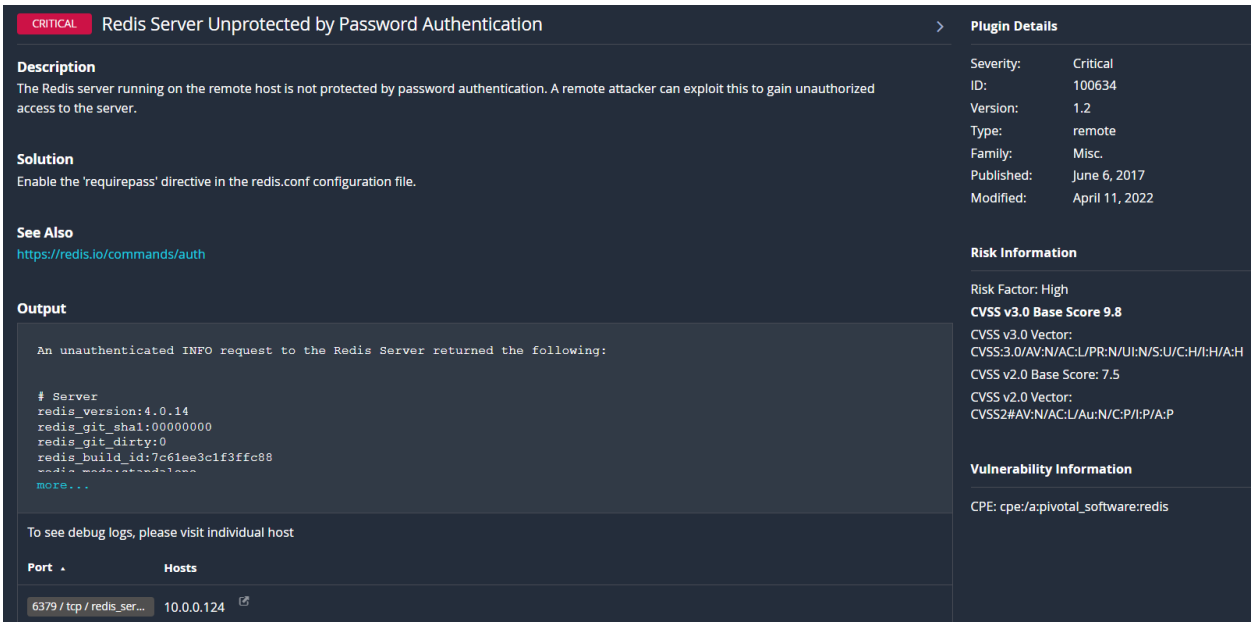
So, there are some hard limitations with the Tenable Nessus "Essentials" it limits you to 16 max hosts per scan. Which is completely ok for our purposes. You'll notice that 5 hosts popped up with vulnerabilities, and in the bar graph it shows informational, low, medium, high and CRITICAL.

I notice that 10.0.0.124 has the most critical vulnerabilities.

I'm going to click on that IP and it shows me more detail:



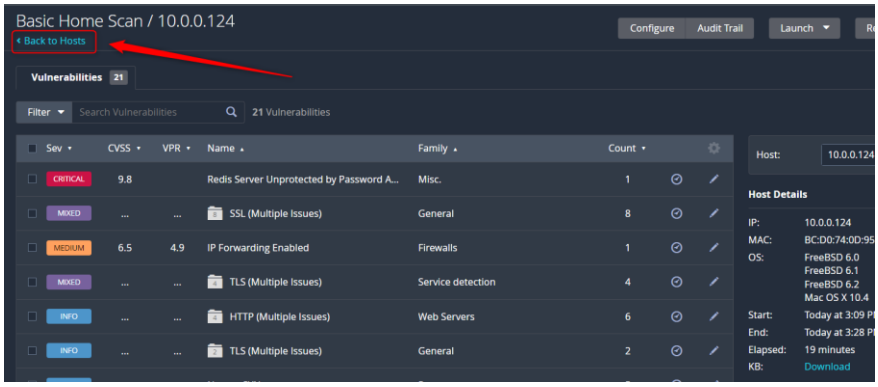
I'm going to dive down on that CRITICAL vulnerability by clicking on it:



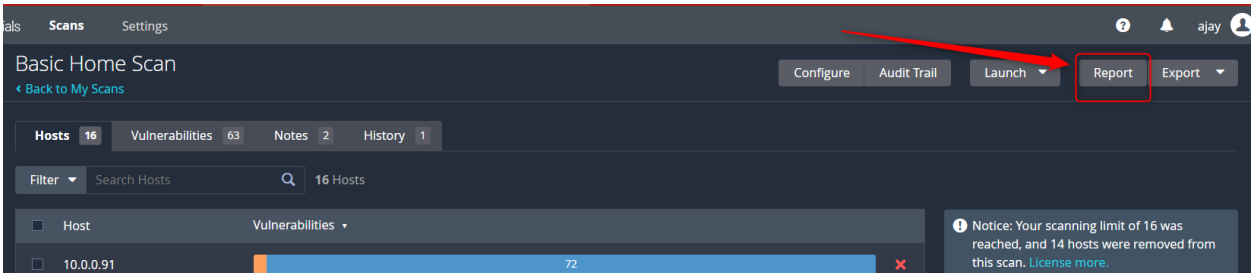
Can we agree this is a MUCH NICER interface than just CLI?

Lots of interactivity, very handsome presentation, and the ability to interact by clicking. GUI does have some advantages!

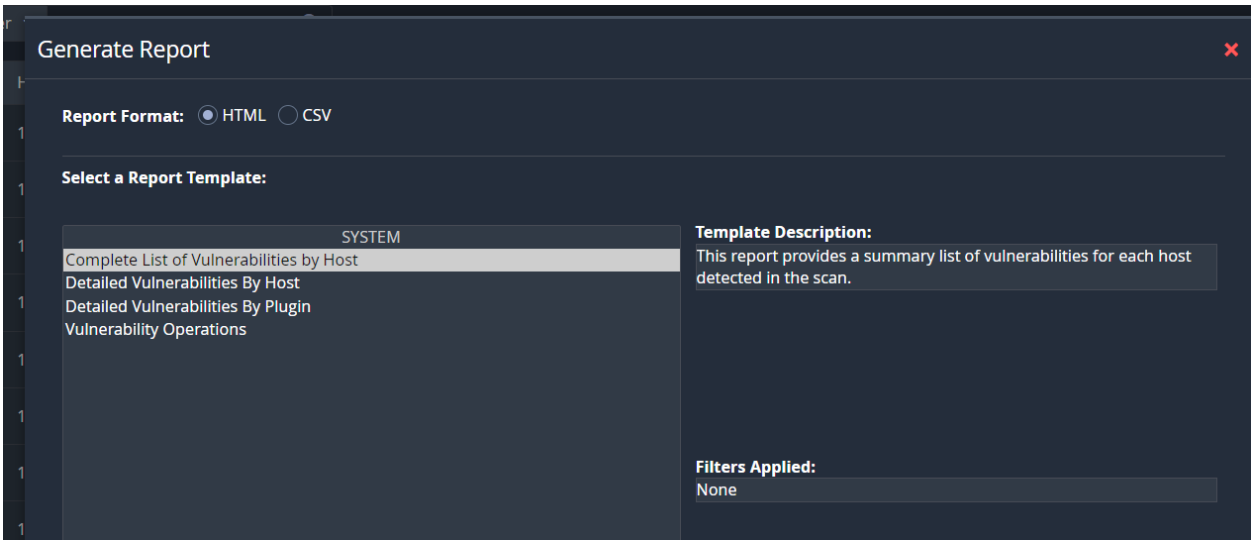
Let's go back to My Hosts:



Let's generate a report, most consumers of Vulnerability Scans, will receive it in report format:

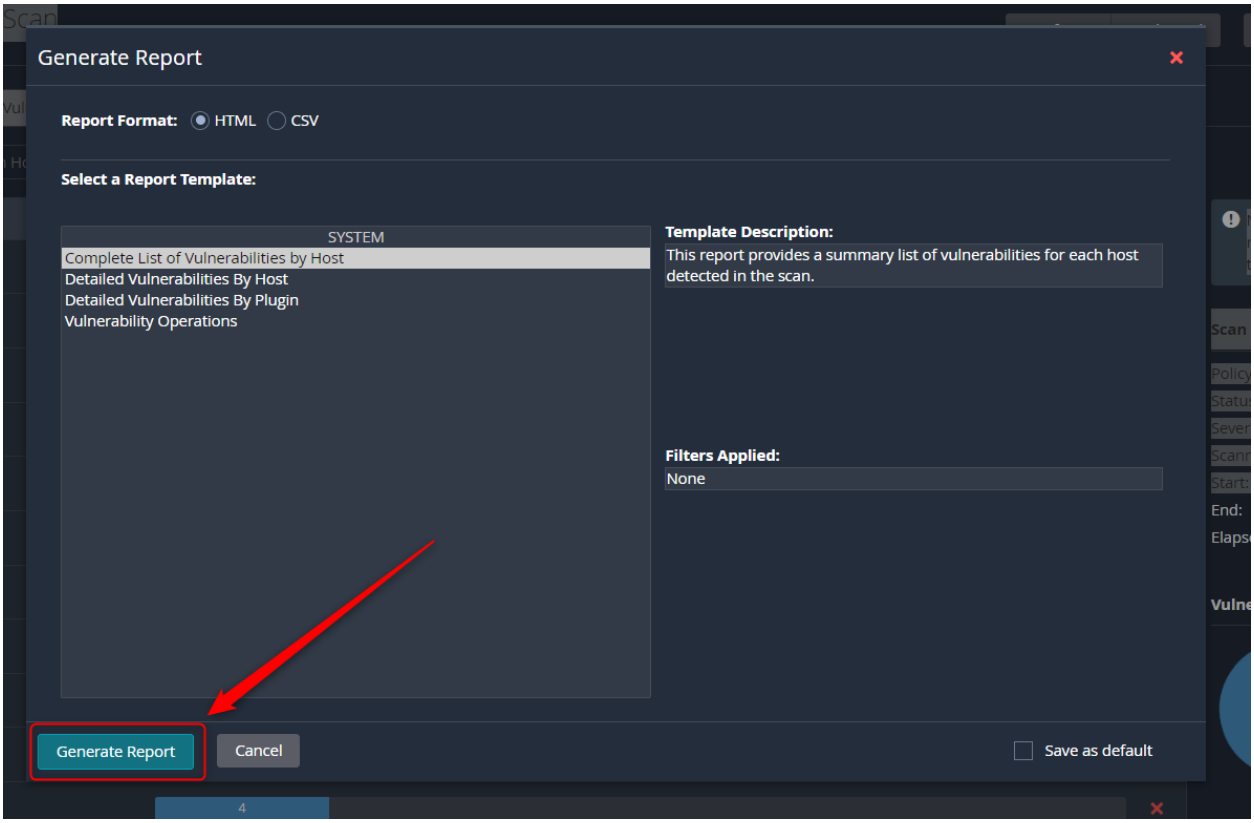


We're just going to use the default report and see what that looks like:

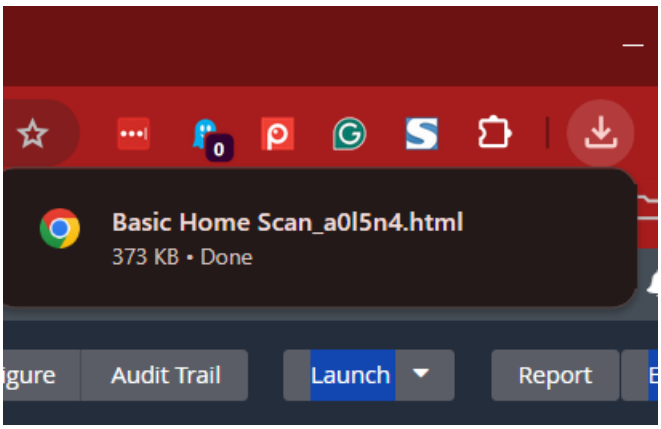


You have the choice of HTML for human beings to read, and CSV for computers to read.

Click GENERATE REPORT in the lower left corner.

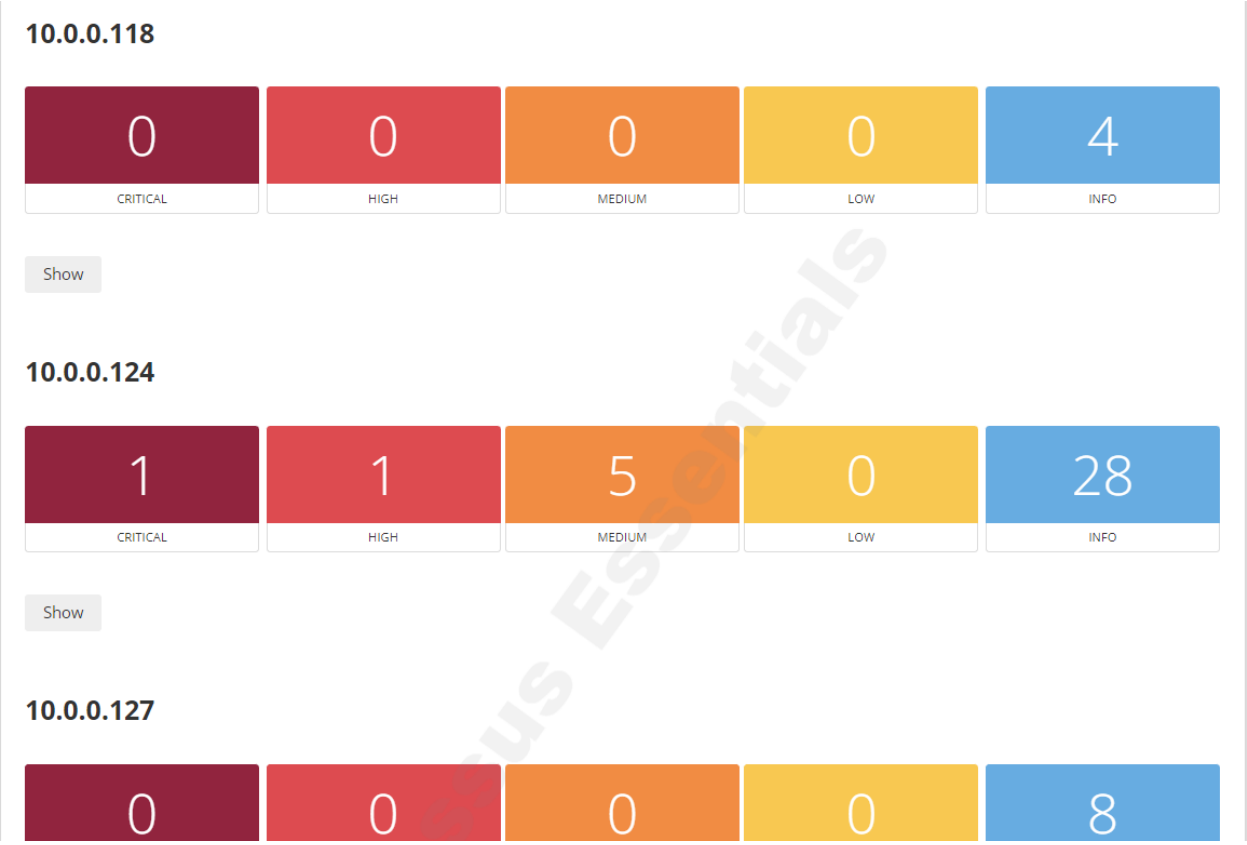


When it finishes, it will drop it into your DOWNLOADS folder:

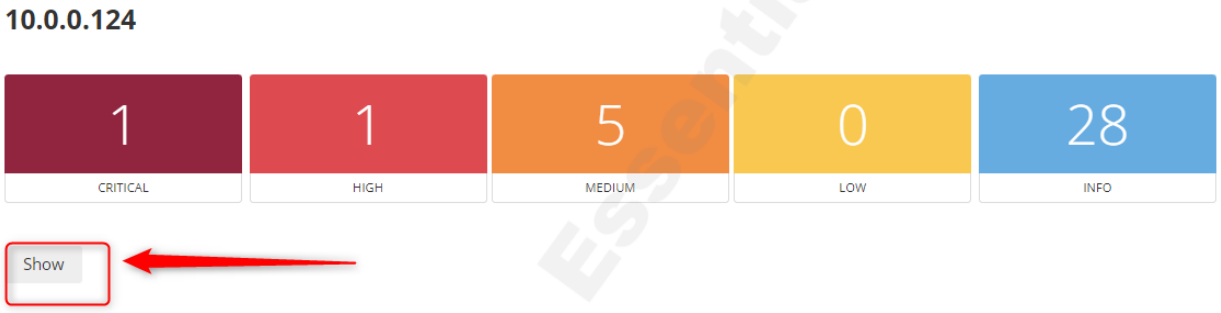


You can open it with a browser.

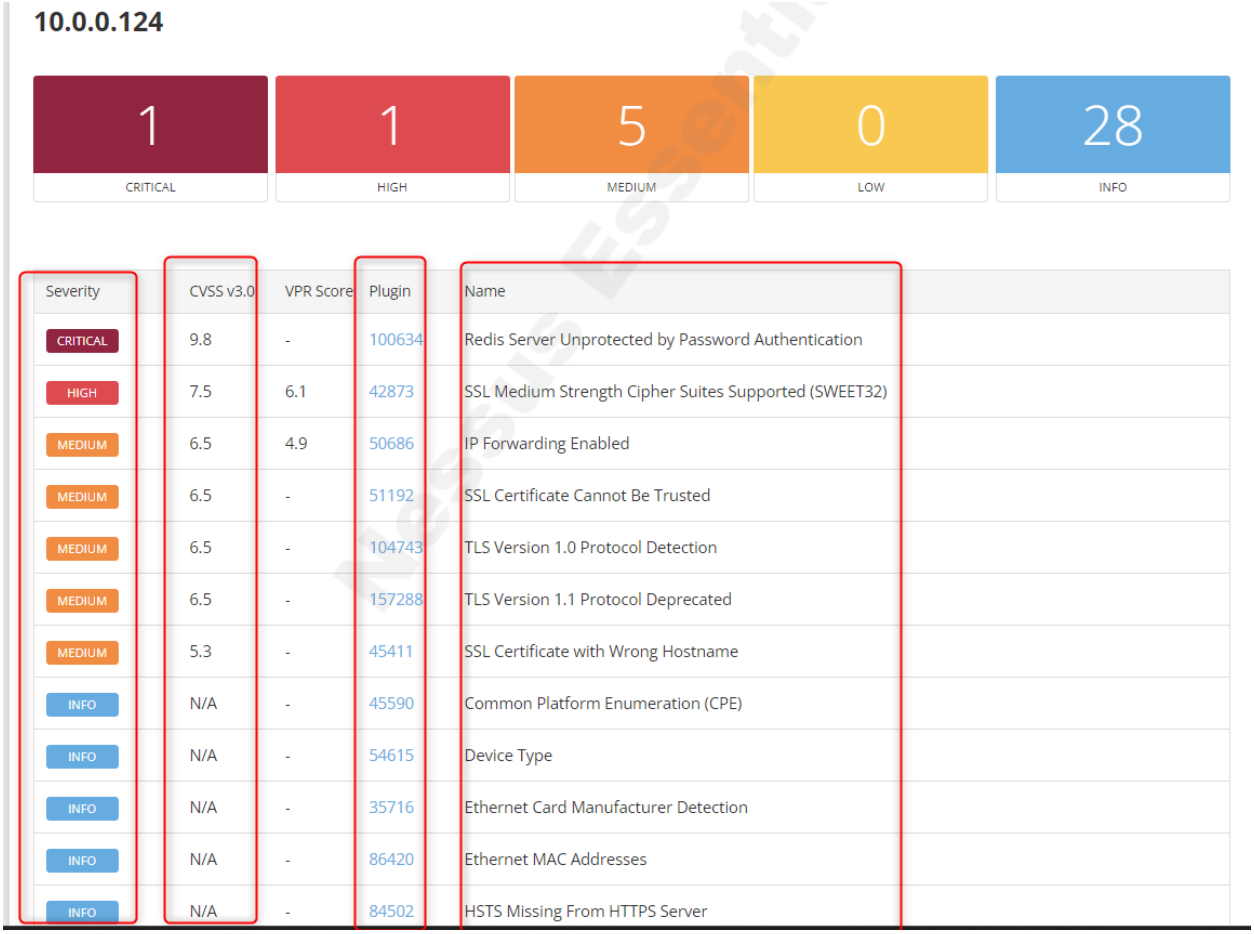
It will show you a pretty (who doesn't like colors) report:



Pick a host with some juicy vulnerabilities and click on the show button or link:



And you will be graced with a nice graphical output:



10.0.0.124

1	1	5	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	-	100634	Redis Server Unprotected by Password Authentication
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	4.9	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
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	-	84502	HSTS Missing From HTTPS Server

Its sorted via Criticality, CVSS score, the tenable plug in (clickable) and a Title to what Vuln it is.

Short, sweet, pretty, and easily digestible by End Users, Directors, Managers….

If you click on the plug in to learn more about the vulnerability, it provide you some data:

https://www.tenable.com/plugins/nessus/100634

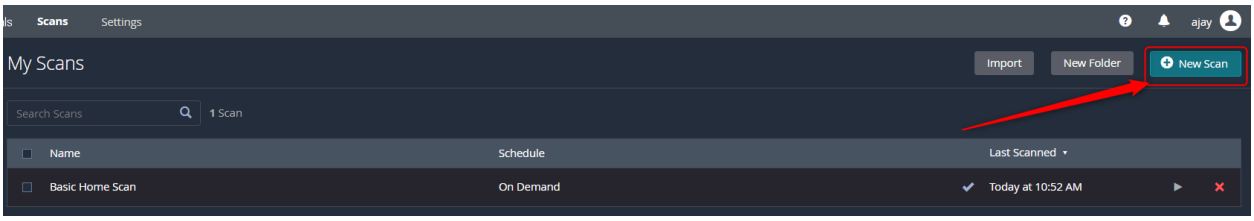
Please note that it provides:

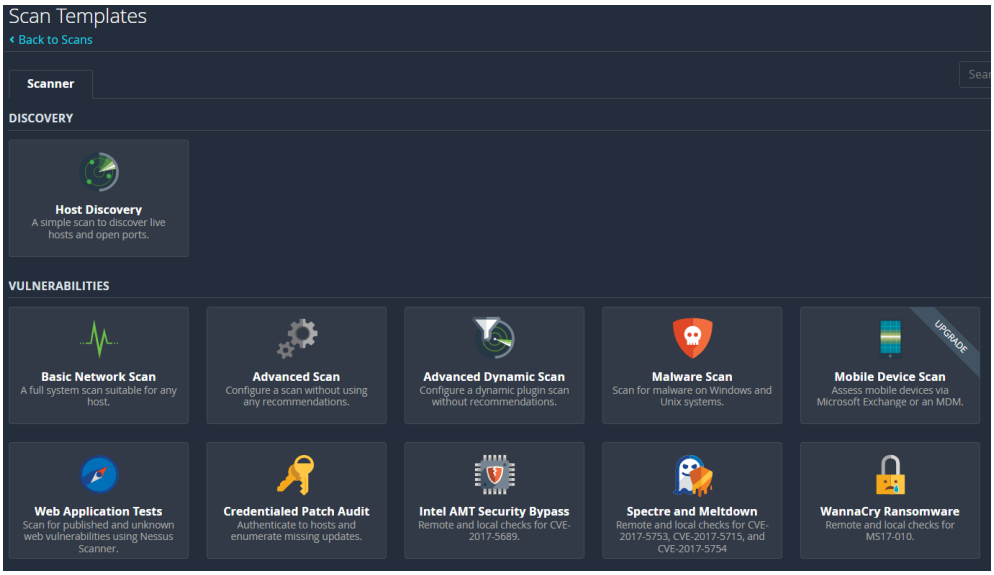
- Description
- Solution
- More information

Super handy, to hand off to an IT team Server Admin, or Network Engineer for them to do the work.

Task 2 – Conduct your first Vulnerability Scan – DVL

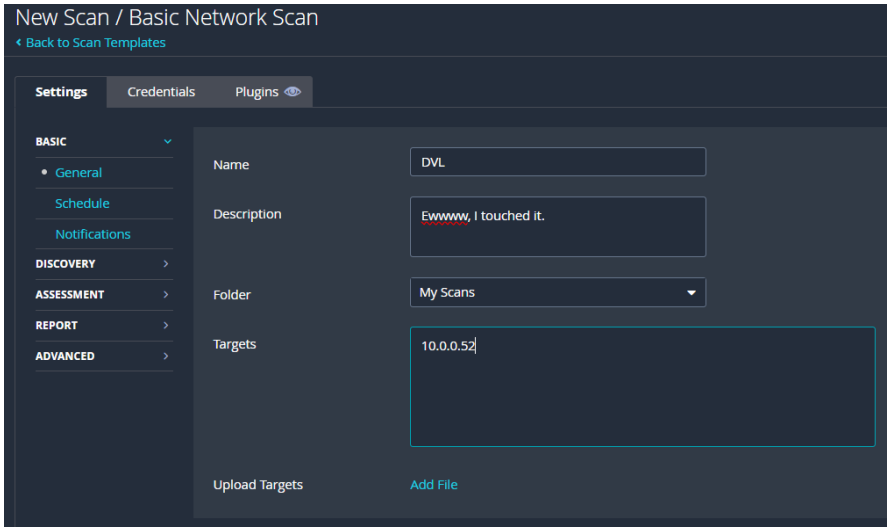
Make sure DVL is powered up and CREATE A NEW SCAN:



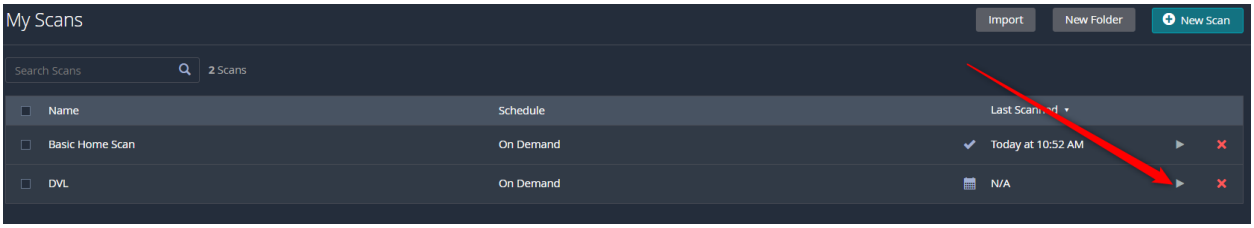


We are just going to do a **Basic Network Scan**.

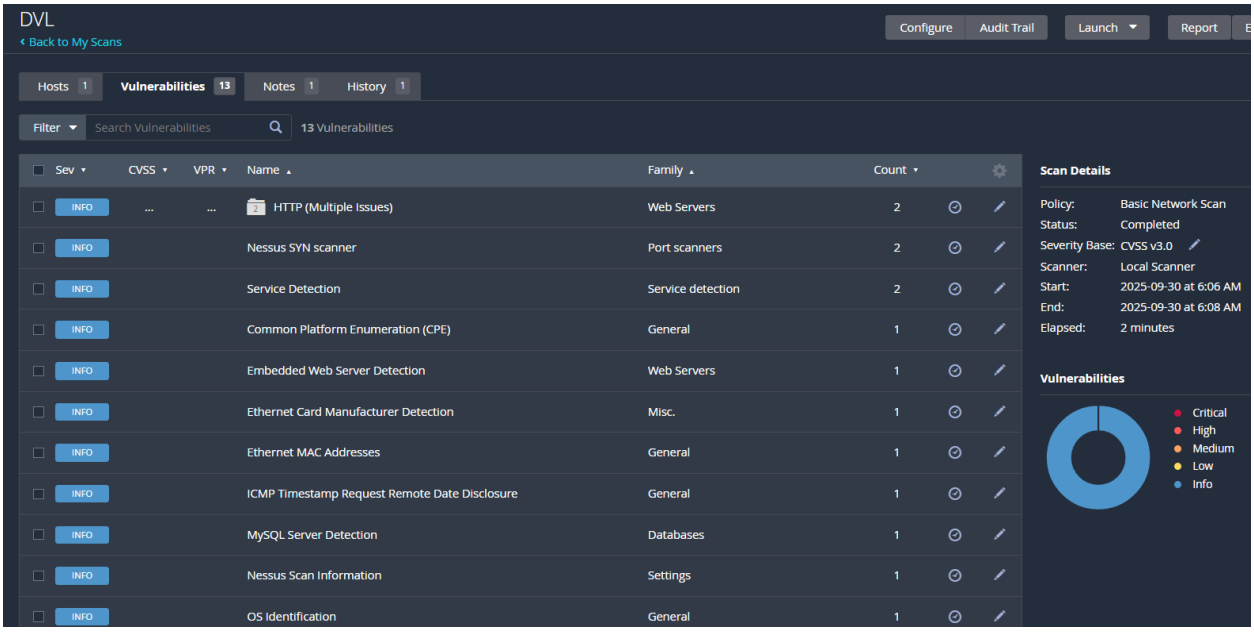
Configure the new Basic Network Scan with the ip address of your DVL:



Launch the scan against the DVL:



It's going to take some time to enumerate all of its vulnerabilities. <insert Matix Glitch>



Not too bad

APPENDIX

Neo resources

sudo timedatectl set-ntp off

sudo date --set="2025-09-30 10:05:59.990"

sudo timedatectl set-ntp on

Additional Context Videos

How to create Scans

https://www.youtube.com/watch?v=W9n-vwWm8KM

Discovery Scans

https://www.youtube.com/watch?v=0uzBMKOoEtA

Passive Network Discovery

https://www.youtube.com/watch?v=cDAfyLniwXI

What is VPR? Or Vulnerability Priority Rating

https://www.youtube.com/watch?v=XYIsBeRV1YQ

Asset Tagging? But why?

https://www.youtube.com/watch?v=xj_lYfmmQaI

Tuning for sensitive applications. (Don't hurt their feelings)

https://www.youtube.com/watch?v=vo89x18JrzE

Credentialed Scans

https://www.youtube.com/watch?v=cEMKm-k-Drs

How to read reports

https://www.youtube.com/watch?v=flXoXyl3ImY