



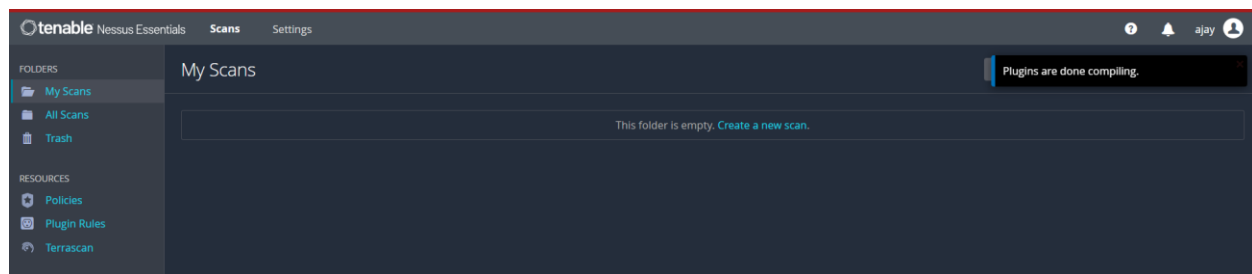
BTA 2023 ©

Vulnerability Scanning and Management

EXERCISE 3 – Vulnerability Scanning and Management

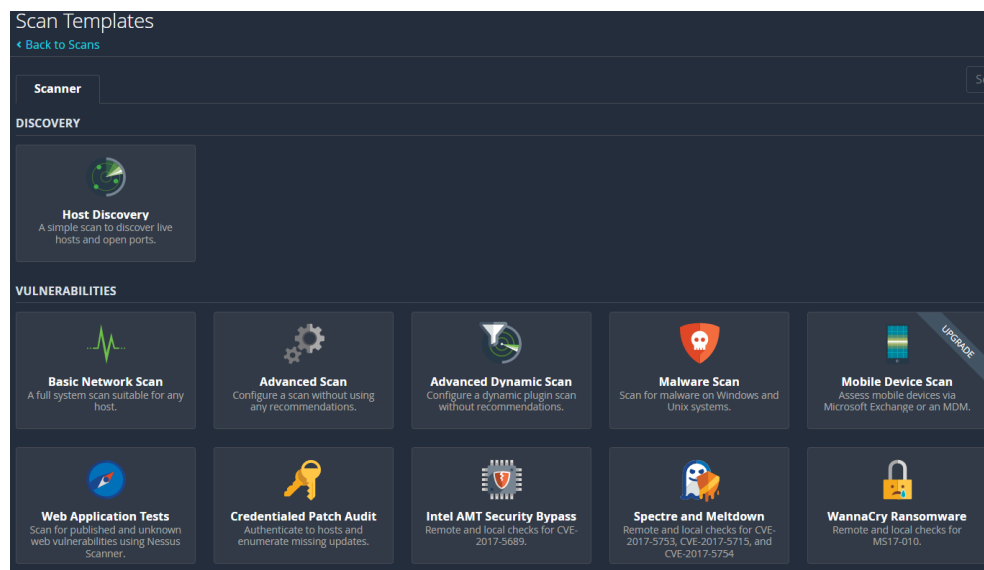
Task 1 – Conduct your first Vulnerability Scan – Home Network

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**.



BTA 2023 ©

Name: Something logical, so you can understand it.

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

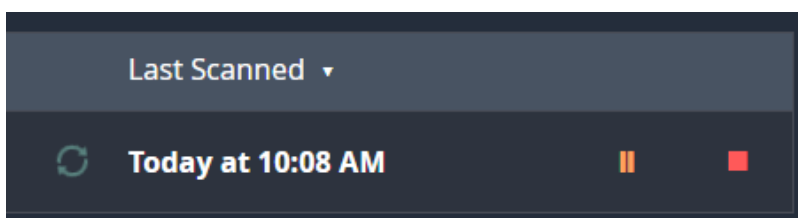
Targets, will be your Network Scope, which will likely be different from mine. (See all that Networking and Subnetting and CIDR is... relevant.)

Click on SAVE

Name	Schedule	Last Scanned		
Basic Home Scan	On Demand	N/A	▶	✕

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.





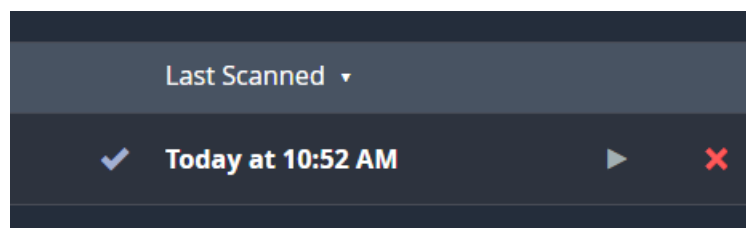
From the CLI, I can run **htop** to view how hard the server is working and this is my output.

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

```
0[|||||] 6.9% Tasks: 31, 67 thr; 1 running
1[|||||] 11.8% Load average: 1.04 1.14 0.99
2[|||||] 16.4% Uptime: 00:48:46
3[|||||] 20.4%
Mem[|||||] 520M/7.75G
Swp[ ] 0K/0K
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1157	root	20	0	1223M	250M	12816	S	59.7	3.2	46:20.42	nessusd -q
1162	root	20	0	1223M	250M	12816	S	15.1	3.2	0:08.48	nessusd -q
1213	root	20	0	1223M	250M	12816	S	12.9	3.2	0:11.48	nessusd -q
1210	root	20	0	1223M	250M	12816	S	9.1	3.2	0:13.64	nessusd -q
1211	root	20	0	1223M	250M	12816	S	6.8	3.2	0:08.68	nessusd -q
1209	root	20	0	1223M	250M	12816	S	3.0	3.2	0:15.21	nessusd -q
1212	root	20	0	1223M	250M	12816	S	2.3	3.2	0:03.82	nessusd -q
1214	root	20	0	1223M	250M	12816	D	1.5	3.2	0:03.36	nessusd -q
1219	root	20	0	1223M	250M	12816	S	1.5	3.2	0:22.13	nessusd -q
1221	root	20	0	1223M	250M	12816	S	1.5	3.2	0:00.53	nessusd -q
662	systemd-r	20	0	25536	12796	8604	S	0.8	0.2	0:00.47	/lib/systemd/systemd-resolved
1158	root	20	0	1223M	250M	12816	S	0.8	3.2	0:11.53	nessusd -q
1177	root	20	0	1223M	250M	12816	S	0.8	3.2	0:41.68	nessusd -q
1216	root	20	0	1223M	250M	12816	S	0.8	3.2	0:19.69	nessusd -q
1224	root	20	0	1223M	250M	12816	S	0.8	3.2	0:00.52	nessusd -q
1229	root	20	0	1223M	250M	12816	S	0.8	3.2	0:09.89	nessusd -q
1	root	20	0	162M	11932	8476	S	0.0	0.1	0:02.41	/sbin/init
404	root	19	-1	48136	17196	16052	S	0.0	0.2	0:00.38	/lib/systemd/systemd-journald
443	root	RT	0	282M	27176	9072	S	0.0	0.3	0:01.15	/sbin/multipathd -d -s
445	root	20	0	26044	6940	4732	S	0.0	0.1	0:00.30	/lib/systemd/systemd-udev
471	root	20	0	282M	27176	9072	S	0.0	0.3	0:00.00	/sbin/multipathd -d -s
472	root	RT	0	282M	27176	9072	S	0.0	0.3	0:00.00	/sbin/multipathd -d -s
473	root	RT	0	282M	27176	9072	S	0.0	0.3	0:00.00	/sbin/multipathd -d -s
474	root	RT	0	282M	27176	9072	S	0.0	0.3	0:00.02	/sbin/multipathd -d -s
475	root	RT	0	282M	27176	9072	S	0.0	0.3	0:00.67	/sbin/multipathd -d -s
476	root	RT	0	282M	27176	9072	S	0.0	0.3	0:00.00	/sbin/multipathd -d -s
614	systemd-t	20	0	89360	6536	5736	S	0.0	0.1	0:00.13	/lib/systemd/systemd-timesyncd

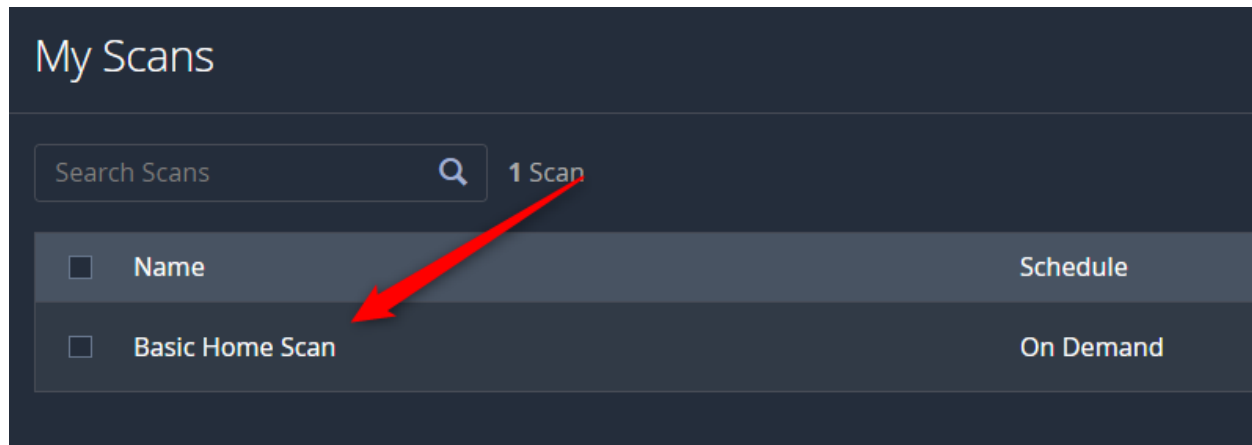
This is what it looks like when the scan is finished;





BTA 2023 ©

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.



BTA 2023 ©

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

Basic Home Scan / 10.0.0.124

Configure Audit Trail Launch Report Export

Vulnerabilities 21

Filter Search Vulnerabilities 21 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		Redis Server Unprotected by Password A...	Misc.	1
MIXED	SSL (Multiple Issues)	General	8
MEDIUM	6.5	4.9	IP Forwarding Enabled	Firewalls	1
MIXED	TLS (Multiple Issues)	Service detection	4
INFO	HTTP (Multiple Issues)	Web Servers	6
INFO	TLS (Multiple Issues)	General	2
INFO	Nessus SYN scanner	Port scanners	5
INFO	Service Detection	Service detection	4
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1

Host: 10.0.0.124

Host Details

IP: 10.0.0.124
MAC:
OS: FreeBSD 6.0
FreeBSD 6.1
FreeBSD 6.2
Mac OS X 10.4
Start: Today at 3:09 PM
End: Today at 3:28 PM
Elapsed: 19 minutes
KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (blue).

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

CRITICAL Redis Server Unprotected by Password Authentication

Description
The Redis server running on the remote host is not protected by password authentication. A remote attacker can exploit this to gain unauthorized access to the server.

Solution
Enable the 'requirepass' directive in the redis.conf configuration file.

See Also
<https://redis.io/commands/auth>

Output
An unauthenticated INFO request to the Redis Server returned the following:

```
# Server
redis_version:4.0.14
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:7c61ee3c1f3ffc88
redis_mode:standalone
more...
```


To see debug logs, please visit individual host

Port **Hosts**
6379 / tcp / redis_ser... 10.0.0.124

Plugin Details

Severity: Critical
ID: 100634
Version: 1.2
Type: remote
Family: Misc.
Published: June 6, 2017
Modified: April 11, 2022

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information
CPE: cpe:/a:pivotal_software:redis

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!



BTA 2023 ©

Let's go back to My Hosts:

Basic Home Scan / 10.0.0.124

[Back to Hosts](#)

Vulnerabilities 21

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		Redis Server Unprotected by Password A...	Misc.	1
MIXED	SSL (Multiple Issues)	General	8
MEDIUM	6.5	4.9	IP Forwarding Enabled	Firewalls	1
MIXED	TLS (Multiple Issues)	Service detection	4
INFO	HTTP (Multiple Issues)	Web Servers	6
INFO	TLS (Multiple Issues)	General	2

Host: 10.0.0.124

Host Details

IP: 10.0.0.124
MAC: BC:D0:74:0D:95
OS: FreeBSD 6.0
FreeBSD 6.1
FreeBSD 6.2
Mac OS X 10.4
Start: Today at 3:09 PM
End: Today at 3:28 PM
Elapsed: 19 minutes
KBs: [Download](#)

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

Basic Home Scan

[Back to My Scans](#)

Configure Audit Trail Launch **Report** Export

Hosts 16 Vulnerabilities 63 Notes 2 History 1

Filter Search Hosts 16 Hosts

Host Vulnerabilities

10.0.0.91 72

Notice: Your scanning limit of 16 was reached, and 14 hosts were removed from this scan. [License more.](#)

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

Generate Report

Report Format: ☒ HTML ☐ CSV

Select a Report Template:

- SYSTEM
- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:

This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:

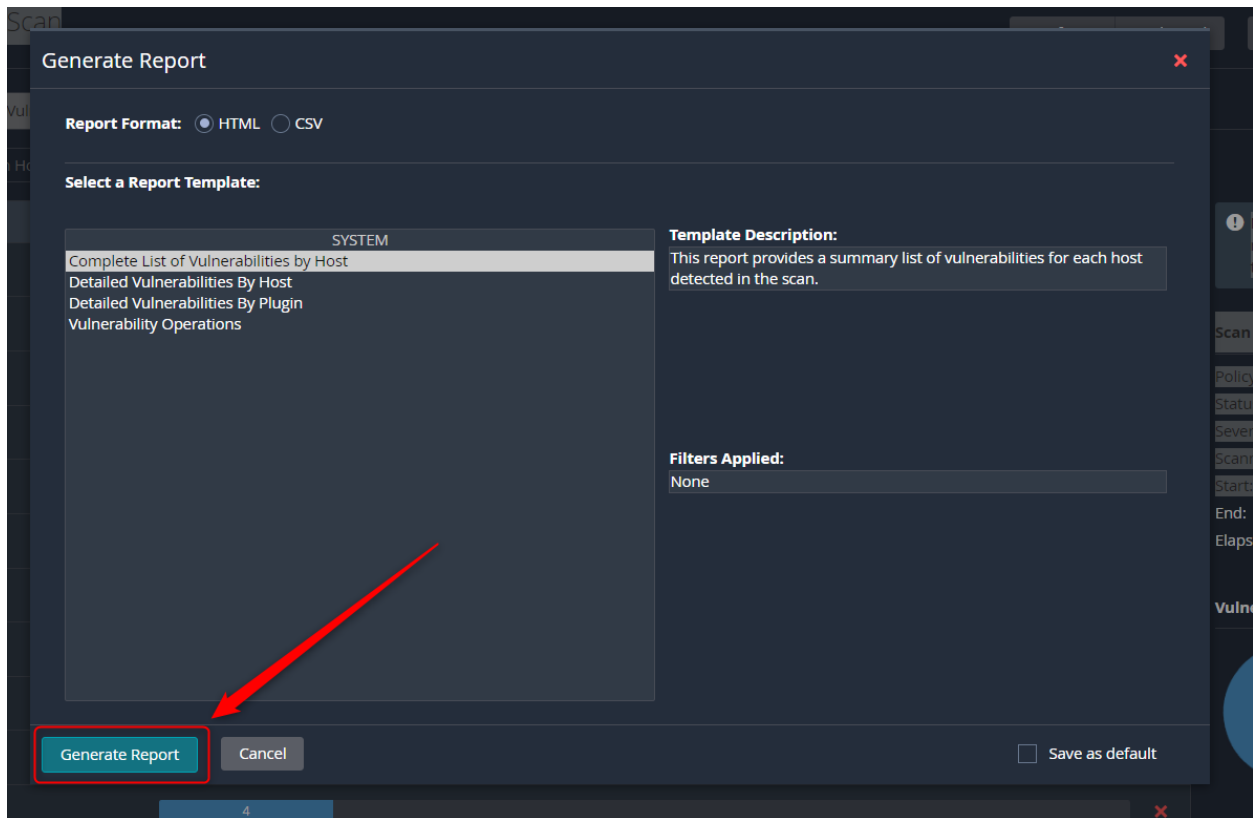
None

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

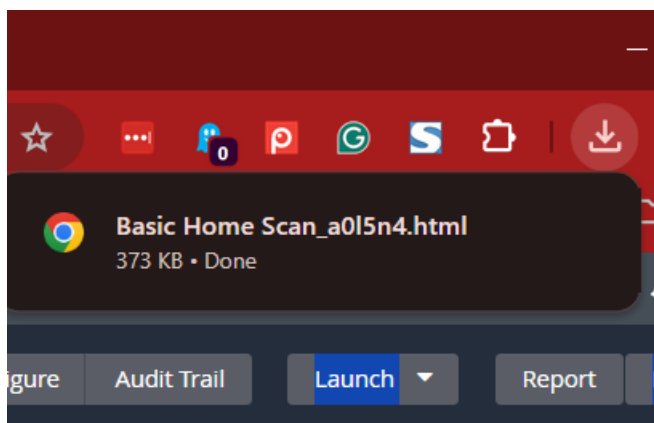


BTA 2023 ©

Click GENERATE REPORT in the lower left corner.



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



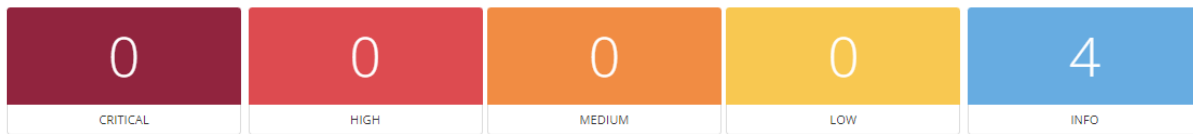
You can open it with a browser.

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



BTA 2023 ©

10.0.0.118



Show

10.0.0.124



Show

10.0.0.127



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

10.0.0.124



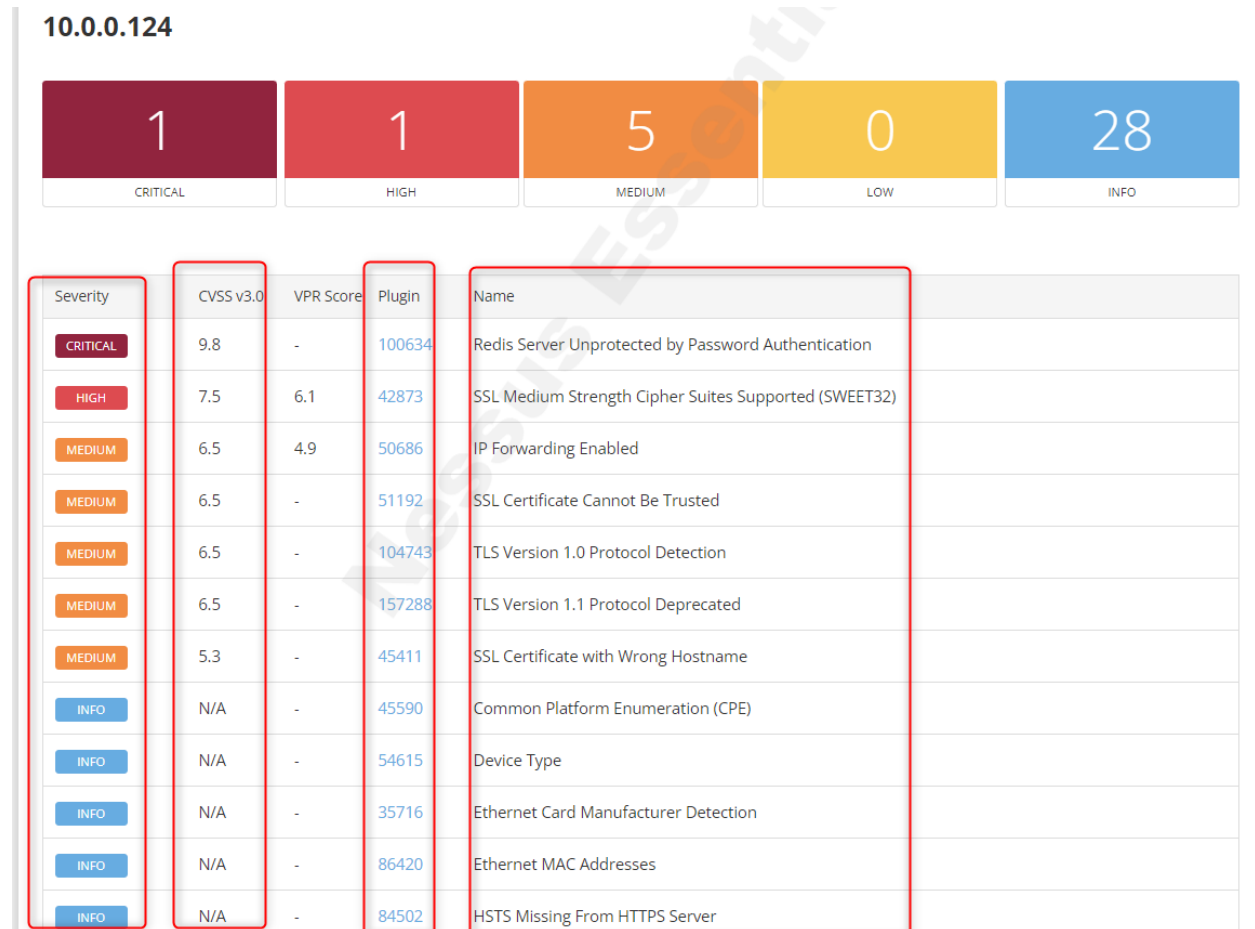
Show





BTA 2023 ©

And you will be graced with a nice graphical output:



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



BTA 2023 ©

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

Redis Server Unprotected by Password Authentication

CRITICALNessus Plugin ID 100634

Language:

InformationDependenciesDependentsChangelog

Synopsis

A Redis server is not protected by password authentication.

Description

The Redis server running on the remote host is not protected by password authentication. A remote attacker can exploit this to gain unauthorized access to the server.

Solution

Enable the 'requirepass' directive in the redis.conf configuration file.

See Also

<https://redis.io/commands/auth>

Plugin Details

Severity: Critical

ID: 100634

File Name:
redis_password_protection_disabled.nasl

Version: 1.2

Type: remote

Family: Misc.

Published: 6/6/2017

Updated: 4/11/2022

Configuration: Enable thorough checks

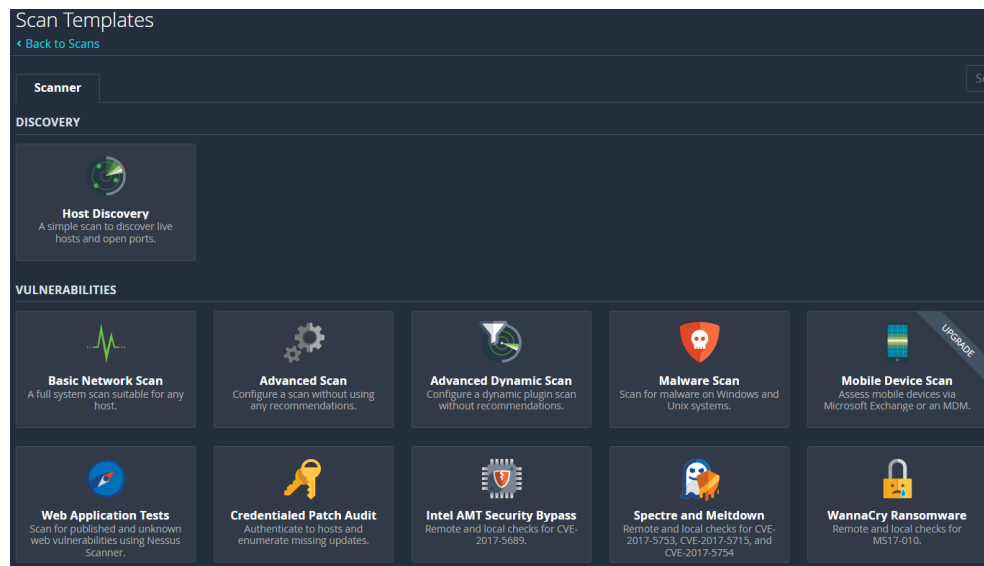
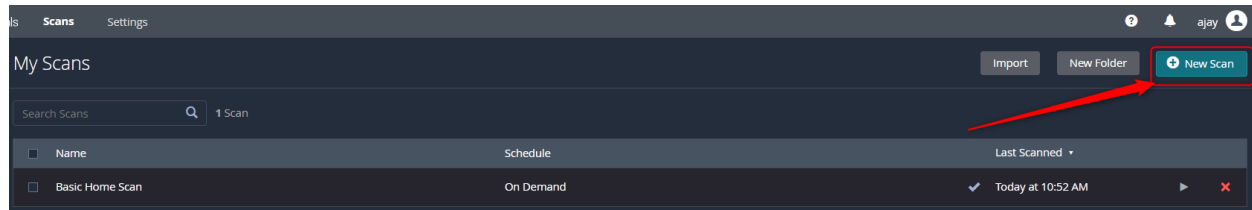
Supported Sensors: Nessus



BTA 2023 ©

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**.



BTA 2023 ©

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

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: DVL

Description: Ewww, I touched it.

Folder: My Scans

Targets: 10.0.0.52

Upload Targets | Add File

Launch the scan against the DVL:

My Scans

Import | New Folder | New Scan

Search Scans 2 Scans

Name	Schedule	Last Scan	
Basic Home Scan	On Demand	Today at 10:52 AM	
DVL	On Demand	N/A	

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

DVL

[Back to My Scans](#) | Configure | Audit Trail | Launch | Report

Hosts 1 | Vulnerabilities 13 | Notes 1 | History 1

Filter Search Vulnerabilities 13 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
INFO	HTTP (Multiple Issues)	Web Servers	2	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Service Detection	Service detection	2	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Embedded Web Server Detection	Web Servers	1	
INFO	Ethernet Card Manufacturer Detection	Misc.	1	
INFO	Ethernet MAC Addresses	General	1	
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO	MySQL Server Detection	Databases	1	
INFO	Nessus Scan Information	Settings	1	
INFO	OS Identification	General	1	

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: 2025-09-30 at 6:06 AM

End: 2025-09-30 at 6:08 AM

Elapsed: 2 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Not too bad



BTA 2023 ©

APPENDIX

Neo resources



```
sudo timedatectl set-ntp off
```

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

```
sudo timedatectl set-ntp on
```

Licensed Hosts

17 of 16 used



BTA 2023 ©

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=fIXoXyl3ImY>