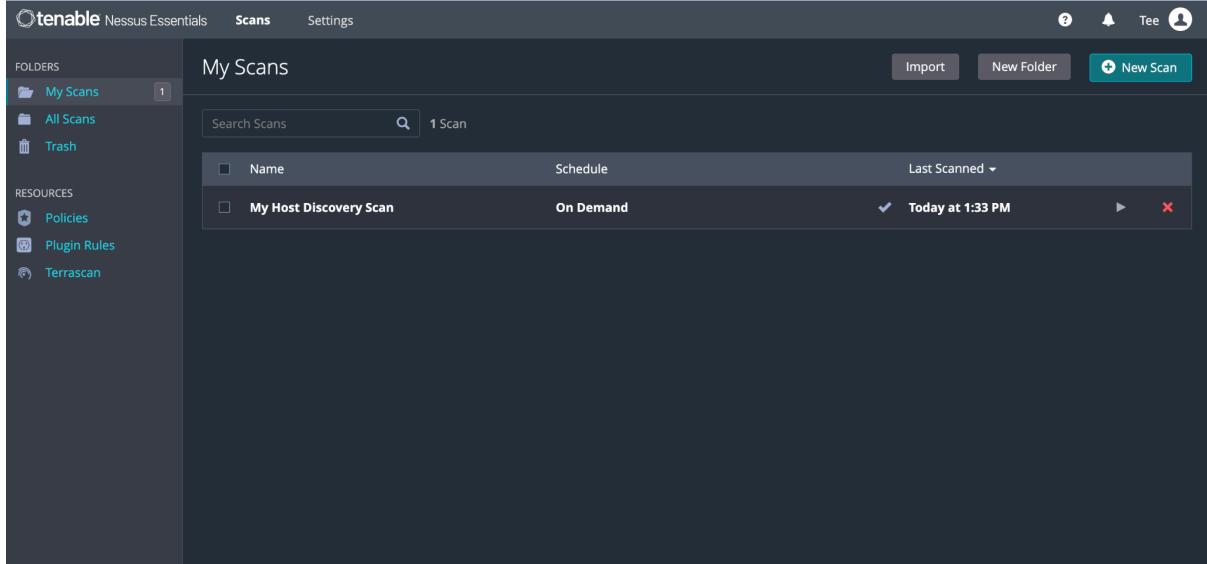


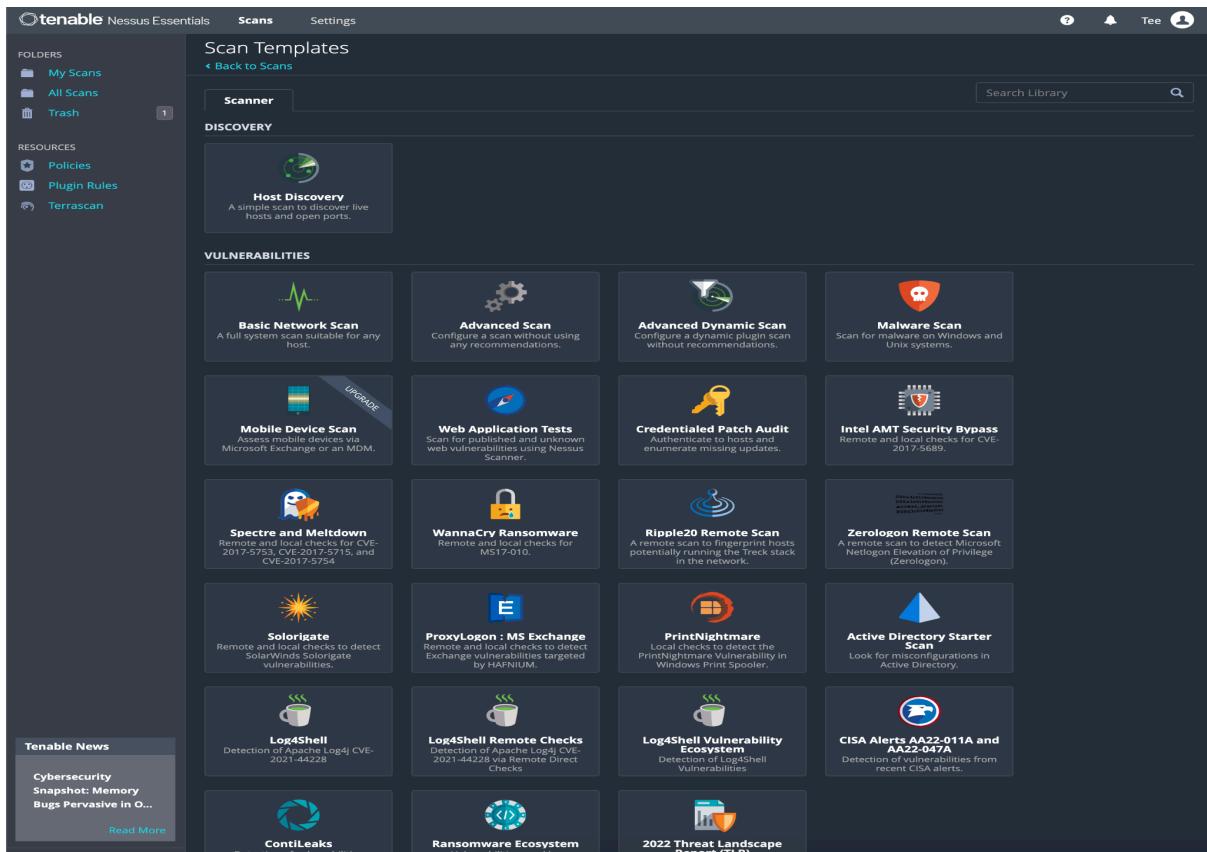
Vulnerability Scanning and Management

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:



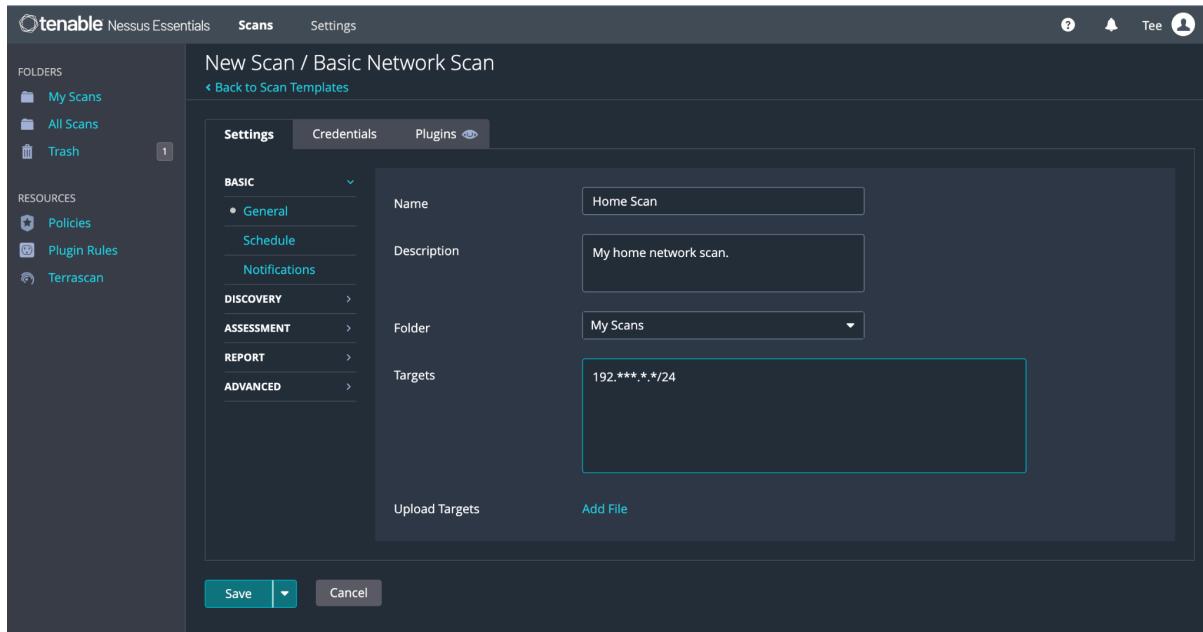
The screenshot shows the Tenable Nessus Essentials interface. The left sidebar contains 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area is titled 'My Scans' with a search bar and a table. The table has columns for 'Name', 'Schedule', and 'Last Scanned'. One entry, 'My Host Discovery Scan', is listed with 'On Demand' as the schedule and 'Today at 1:33 PM' as the last scan time.

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:

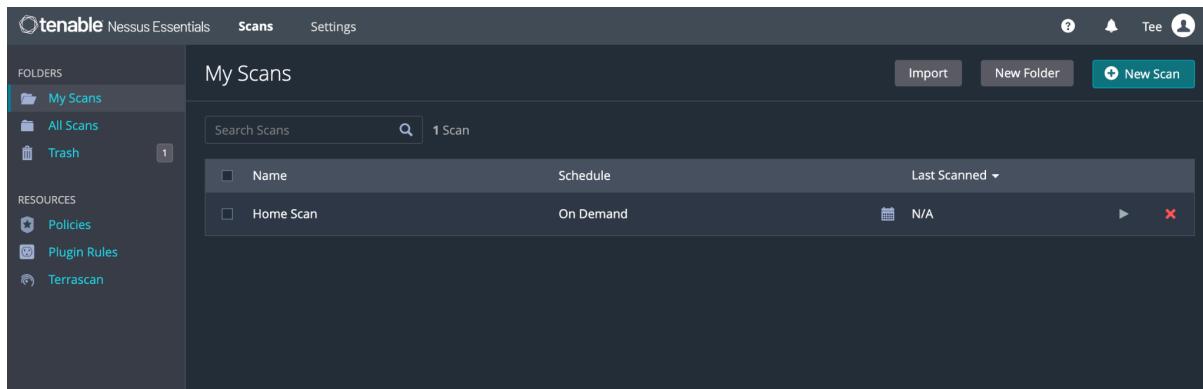


The screenshot shows the 'Scan Templates' page. The left sidebar includes 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main content area is titled 'Scan Templates' with a 'Back to Scans' link. It features a 'DISCOVERY' section with a 'Host Discovery' template. Below it is a 'VULNERABILITIES' grid containing 16 different scan templates, each with an icon and a brief description. Some templates are marked as 'UPGRADE' or have specific notes like 'Spectre and Meltdown' or 'Log4Shell'.

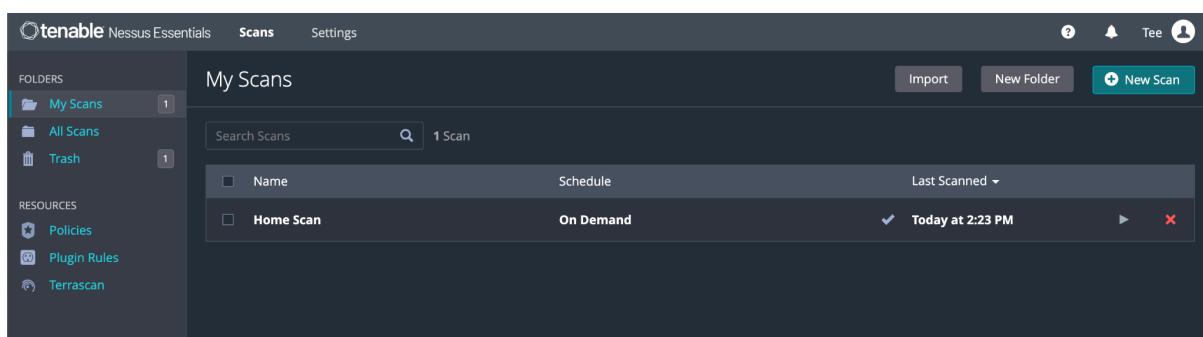
Clicking on the ‘**basic discovery scan**’ option displays a window asking for basic descriptions such as name, description, folder, and targets. When the required fields have been filled, click on the save option. This is illustrated below:



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:

```

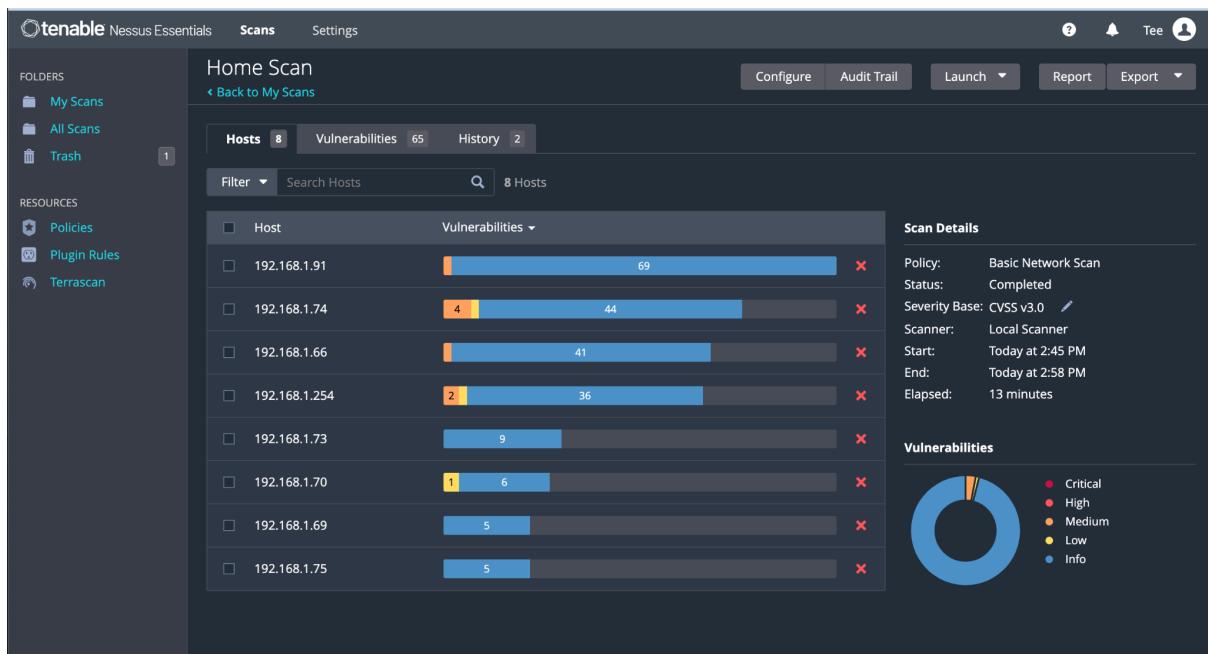
CPU[| 0.7%] Tasks: 28, 43 thr; 1 running
Mem[||||| 382M/4.67G] Load average: 0.00 0.00 0.00
Swp[| 268K/4.00G] Uptime: 00:59:33

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
665 root 20 0 428M 191M 13936 S 1.4 4.0 2:15.73 nessusd -q
763 root 20 0 428M 191M 13936 S 0.7 4.0 0:16.96 nessusd -q
835 root 20 0 428M 191M 13936 S 0.7 4.0 0:18.97 nessusd -q
1 root 20 0 98M 11564 8244 S 0.0 0.2 0:01.21 /sbin/init
379 root 19 -1 56316 23592 22496 S 0.0 0.5 0:00.24 /lib/systemd/systemd-journald
413 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.33 /sbin/multipathd -d -s
417 root 20 0 26024 6812 4628 S 0.0 0.1 0:00.13 /lib/systemd/systemd-udevd
421 root 20 0 282M 27236 9072 S 0.0 0.6 0:00.00 /sbin/multipathd -d -s
422 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.00 /sbin/multipathd -d -s
423 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.00 /sbin/multipathd -d -s
424 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.00 /sbin/multipathd -d -s
425 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.27 /sbin/multipathd -d -s
426 root RT 0 282M 27236 9072 S 0.0 0.6 0:00.00 /sbin/multipathd -d -s
571 systemd-t 20 0 89364 6588 5780 S 0.0 0.1 0:00.12 /lib/systemd/systemd-timesyncd
596 systemd-t 20 0 89364 6588 5780 S 0.0 0.1 0:00.00 /lib/systemd/systemd-timesyncd
627 systemd-n 20 0 16128 8036 7020 S 0.0 0.2 0:00.13 /lib/systemd/systemd-networkd
629 systemd-r 20 0 25540 12680 8488 S 0.0 0.3 0:00.08 /lib/systemd/systemd-resolved
640 root 20 0 6896 2872 2628 S 0.0 0.1 0:00.01 /usr/sbin/cron -f -P
642 messagebu 20 0 8772 4752 3936 S 0.0 0.1 0:00.05 @dbus-daemon --system --address=syst
648 root 20 0 2816 964 864 S 0.0 0.0 0:00.00 /opt/nessus/sbin/nessus-service -q
649 root 20 0 32736 19056 10432 S 0.0 0.4 0:00.07 /usr/bin/python3 /usr/bin/networkd-d
651 root 20 0 229M 6604 5980 S 0.0 0.1 0:00.02 /usr/libexec/polkitd --no-debug
652 syslog 20 0 217M 5084 3996 S 0.0 0.1 0:00.02 /usr/sbin/rsyslogd -n -iNONE
655 root 20 0 1216M 28300 18852 S 0.0 0.6 0:00.65 /usr/lib/snapd/snapd
657 root 20 0 23536 7456 6440 S 0.0 0.2 0:00.05 /lib/systemd/systemd-logind
659 root 20 0 383M 12792 10712 S 0.0 0.3 0:00.12 /usr/libexec/udisks2/udisksd
663 root 20 0 7816 4496 3592 S 0.0 0.1 0:00.02 /bin/login -p --
666 root 20 0 229M 6604 5980 S 0.0 0.1 0:00.00 /usr/libexec/polkitd --no-debug

```

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit

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

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

Vulnerabilities 21

Filter ▾ Search Vulnerabilities 21 Vulnerabilities

Sev	CVSS	VPR	Name	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:

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Microsoft's July 2024 Patch Tuesday). The main content area is titled "Home Scan / Plugin #10114" and "Vulnerabilities 21". A specific vulnerability is highlighted: "LOW ICMP Timestamp Request Remote Date Disclosure". The "Description" section states: "The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols." The "Solution" section suggests filtering out ICMP timestamp requests and replies. The "Output" section shows a log entry: "The difference between the local and remote clocks is 1 second." Below this is a table with columns "Port" and "Hosts", showing one entry for port 0/icmp to host 192.168.1.74. The right side of the screen contains "Plugin Details" (Severity: Low, ID: 10114, Version: 1.53, Type: remote, Family: General, Published: August 1, 1999, Modified: May 3, 2024), "VPR Key Drivers" (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Very High, CVSS3 Impact Score: 3.4, Threat Sources: No recorded events), "Risk Information" (Vulnerability Priority Rating (VPR): 4.2, Risk Factor: Low, CVSS v2.0 Base Score: 2.1, CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N), "Vulnerability Information" (Vulnerability Pub Date: January 1, 1995), and "Reference Information" (CWE: 200, CVE: CVE-1999-0524).

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:

The screenshot shows the Tenable Nessus Essentials interface with the "My Scans" folder selected in the left sidebar. The main content area is titled "My Scans" and displays a table of scans. The table has columns "Name" (Home Scan), "Schedule" (On Demand), and "Last Scanned" (Today at 2:58 PM). There are buttons for "Import", "New Folder", and "+ New Scan". The left sidebar also includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Microsoft's July 2024 Patch Tuesday).

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:

Generate CSV Report

Report Format: HTML CSV

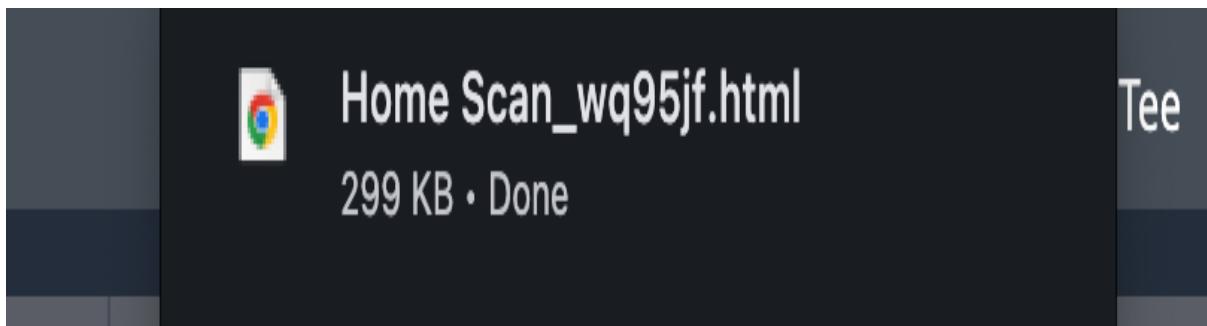
Columns

<input checked="" type="checkbox"/> Plugin ID	<input checked="" type="checkbox"/> See Also
<input checked="" type="checkbox"/> CVE	<input checked="" type="checkbox"/> Plugin Output
<input checked="" type="checkbox"/> CVSS v2.0 Base Score	<input type="checkbox"/> STIG Severity
<input checked="" type="checkbox"/> Risk	<input type="checkbox"/> CVSS v3.0 Base Score
<input checked="" type="checkbox"/> Host	<input type="checkbox"/> CVSS v2.0 Temporal Score
<input checked="" type="checkbox"/> Protocol	<input type="checkbox"/> CVSS v3.0 Temporal Score
<input checked="" type="checkbox"/> Port	<input type="checkbox"/> VPR Score
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Risk Factor
<input checked="" type="checkbox"/> Synopsis	<input type="checkbox"/> References
<input checked="" type="checkbox"/> Description	<input type="checkbox"/> Plugin Information
<input checked="" type="checkbox"/> Solution	<input type="checkbox"/> Exploitable With

[Select All](#) | [Clear](#) | [System](#)

Generate Report **Cancel** Save as default

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:

tenable Nessus

Report generated by Nessus™

Home Scan

Wed, 10 Jul 2024 18:58:19 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.1.66
- 192.168.1.69
- 192.168.1.70
- 192.168.1.73
- 192.168.1.74
- 192.168.1.75
- 192.168.1.91
- 192.168.1.254

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

192.168.1.66

0	0	1	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

192.168.1.69

0	0	0	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

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



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:

The screenshot displays the Tenable.io interface, specifically the 'Plugins' section. The main title is 'SSL Certificate Cannot Be Trusted' (Nessus Plugin ID 51192). The severity is listed as 'MEDIUM'. The page includes tabs for 'Information', 'Dependencies', 'Dependents', and 'Changelog'. The 'Information' tab is active.

Synopsis
The SSL certificate for this service cannot be trusted.

Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution
Purchase or generate a proper SSL certificate for this service.

See Also
<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Plugin Details

Severity: Medium
ID: 51192
File Name: ssl_signed_certificate.nasl
Version: 1.19
Type: remote
Family: General
Published: 12/15/2010
Updated: 4/27/2020
Supported Sensors: Nessus

Risk Information

CVSS v2
Risk Factor: Medium
Base Score: 6.4
Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSS v3
Risk Factor: Medium
Base Score: 6.5
Vector: CVSS3.0:AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Vulnerability Information
Required KB Items: SSL/BrokenCAChain

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:

The screenshot shows the 'Scans' section of the Tenable Nessus Essentials web interface. On the left sidebar, under 'FOLDERS', 'My Scans' is selected. In the main area, a 'New Scan / Basic Network Scan' dialog is open. The 'Settings' tab is selected. The 'BASIC' section contains the following fields:

Name	Damn Vulnerability Linux
Description	Server loaded with vulnerabilities for educational purposes
Folder	My Scans
Targets	192.168.1.90

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

The screenshot shows the 'My Scans' list in the Tenable Nessus Essentials interface. The 'My Scans' folder is selected in the sidebar. The main area displays a table of scans:

Name	Schedule	Last Scanned
Home Scan	On Demand	Today at 2:58 PM
Damn Vulnerability Linux	On Demand	N/A

At the top right of the list area are 'Import', 'New Folder', and a 'New Scan' button.

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:

The screenshot shows the 'My Scans' list again. The 'Damn Vulnerability Linux' scan is now listed with a green circular progress icon and the text 'Today at 6:32 PM'. The other scan, 'Home Scan', remains in the 'On Demand' state.

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

The screenshot shows the Tenable Nessus Essentials web interface. The top navigation bar includes 'Tenable' logo, 'Nessus Essentials', 'Scans' (selected), 'Settings', and user account icon. Below the navigation is a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area displays the results of a scan titled 'Damn Vulnerability Linux / 192.168.1.90'. A 'Vulnerabilities' section shows 13 findings, including 'LOW', 'INFO', and 'Critical' levels across various categories like HTWeb Servers, Port scanners, Service detection, and Web Servers. To the right, 'Host Details' provide system information: IP (192.168.1.90), MAC (08:00:27:AE:06:78), OS (Dell iDRAC Controller, KYOCERA Printer, Linux Kernel 2.6), and scan timing (Start: Today at 10:32 PM, End: Today at 10:33 PM, Elapsed: 2 minutes, KB: Download). A 'Vulnerabilities' donut chart indicates the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue).

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**.