CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

SCHOOL OF ENGINEERING AND TECHNOLOGY

Name: V Ebinesh

Register Number: 2462167

Class: 3 BTCSAIML B Course

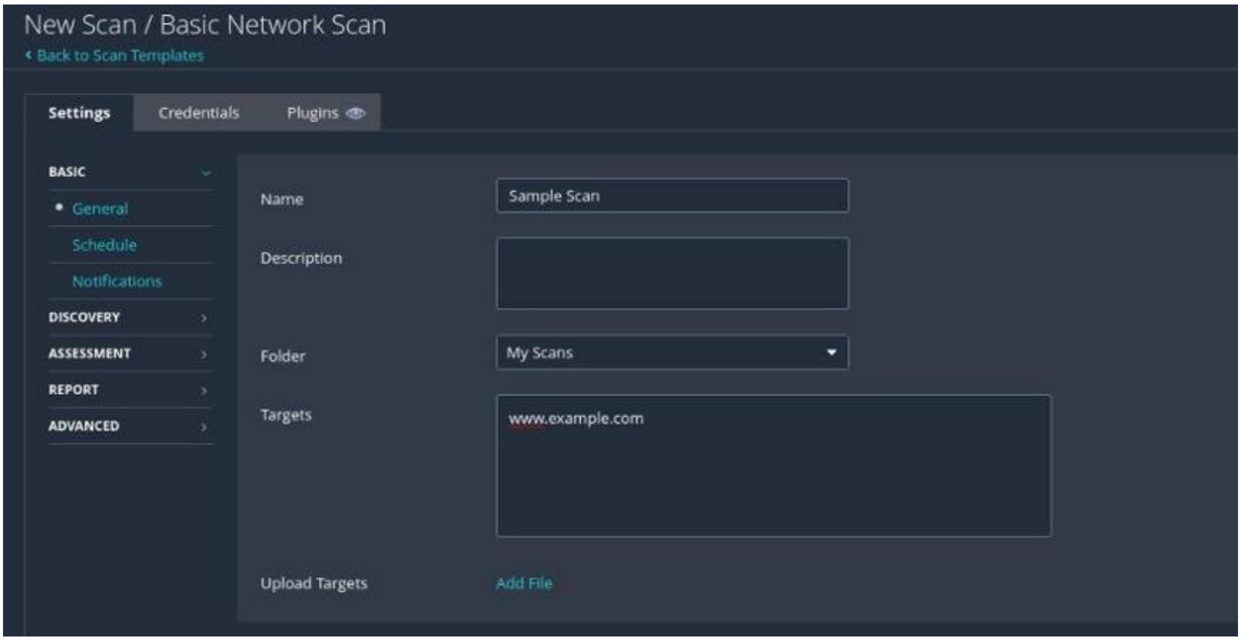
Code: CSHO331CSP

Ethical Hacking

INDEX

SCAN USING NESSUS

Start a new scan and provide the target as www.example.com. Save the scan and later in the Saved Scan, launch the scan.



New Scan / Basic Network Scan

Name: Sample Scan

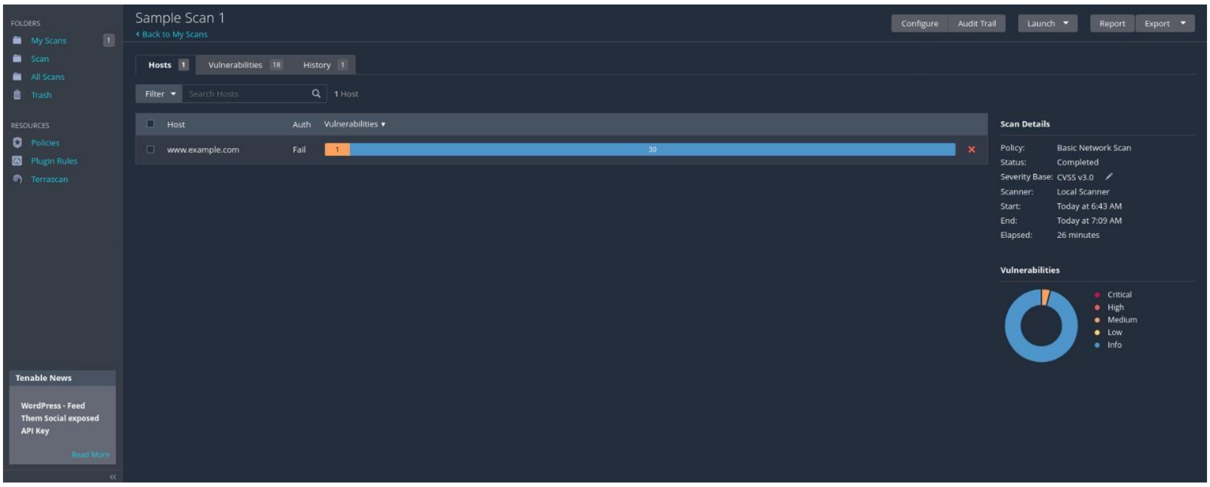
Description:

Folder: My Scans

Targets: www.example.com

Upload Targets: Add File

To view the scanned result, click on the scan. It will provide information on the Hosts, Vulnerabilities, and History.



Sample Scan 1

Host	Auth	Vulnerabilities
www.example.com	Fail	1 30

Scan Details

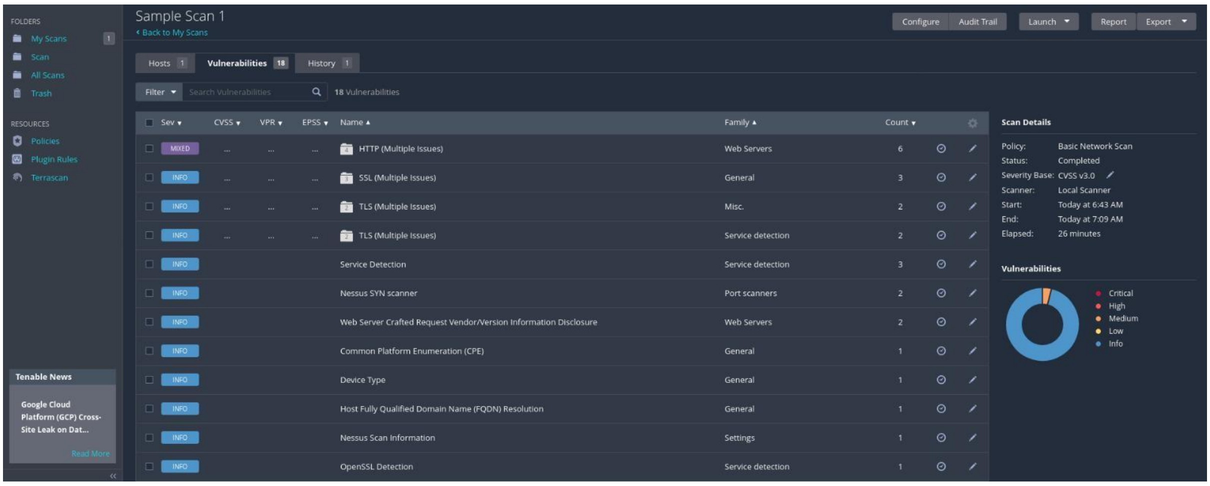
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:43 AM
End:	Today at 7:09 AM
Elapsed:	26 minutes

Vulnerabilities

Tenable News

WordPress - Feed Them Social exposed API Key

Vulnerabilities:



Sample Scan 1

‹ Back to My Scans

18 Vulnerabilities

□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
□	MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	6
□	INFO	...	...	...	SSL (Multiple Issues)	General	3
□	INFO	...	...	...	TLS (Multiple Issues)	Misc.	2
□	INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
□	INFO				Service Detection	Service detection	3
□	INFO				Nessus SYN scanner	Port scanners	2
□	INFO				Web Server Crafted Request Vendor/Version Information Disclosure	Web Servers	2
□	INFO				Common Platform Enumeration (CPE)	General	1
□	INFO				Device Type	General	1
□	INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO				Nessus Scan Information	Settings	1
□	INFO				OpenSSL Detection	Service detection	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:43 AM
End:	Today at 7:09 AM
Elapsed:	26 minutes

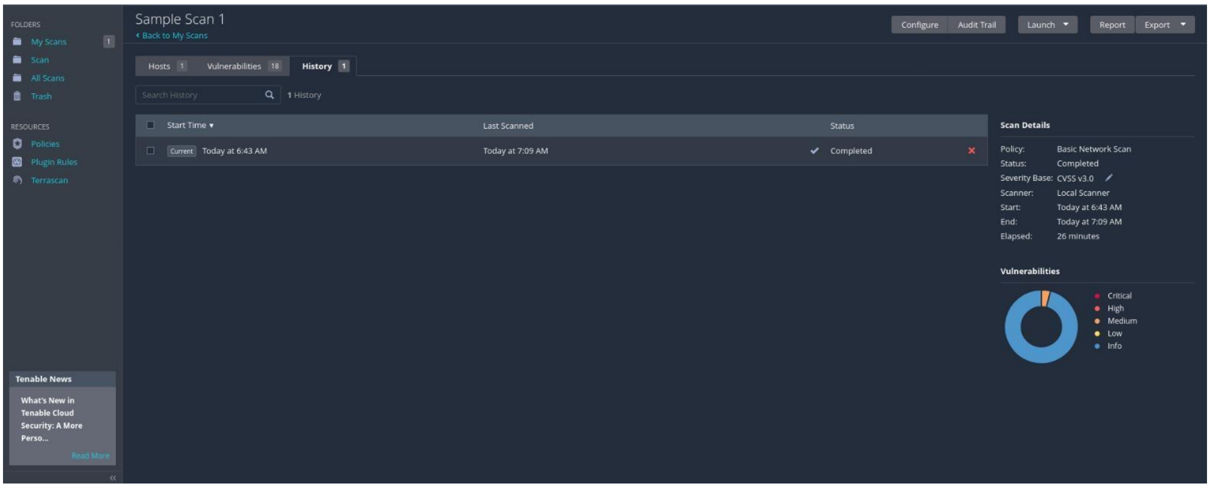
Vulnerabilities

Tenable News

Google Cloud Platform (GCP) Cross-Site Leak on Dat...

Read More

History :



Sample Scan 1

‹ Back to My Scans

1 History

□	Start Time ▾	Last Scanned	Status
□	Current Today at 6:43 AM	Today at 7:09 AM	✓ Completed

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:43 AM
End:	Today at 7:09 AM
Elapsed:	26 minutes

Vulnerabilities

Tenable News

What's New in Tenable Cloud Security: A More Perso...

Read More

Scan Overview :

The Nessus Essentials scan of example.com identified 25 vulnerabilities, with the following severity breakdown:

- Critical: 0
- High: 0
- Medium: 1
- Low: 0

□ Informational: 24 **Key**

Vulnerabilities Detected

- **Medium Severity**:
- HSTS Missing From HTTPS Server (RFC 6797): This indicates the web server does not have HTTP Strict Transport Security (HSTS) enabled, which can increase the risk of SSL stripping attacks.
- **Informational Findings**:
- HTTP Server Type and Version Discovery
- SSL Certificate and Cipher Suite Information
- Supported SSL/TLS Versions (including detection of TLS 1.2 and 1.3)
- QUIC Service Detection
- OS Identification and Fingerprinting
- Traceroute and Service Detection
- Device Type and FQDN Resolution
- Web Server Crafted Request Vendor/Version Information Disclosure

Observations

- No critical or high-risk vulnerabilities were detected.
- The majority of the findings were informational, which indicates good baseline security practices.
- The only medium-risk finding is related to the absence of HSTS, which is a common but important web security best practice.

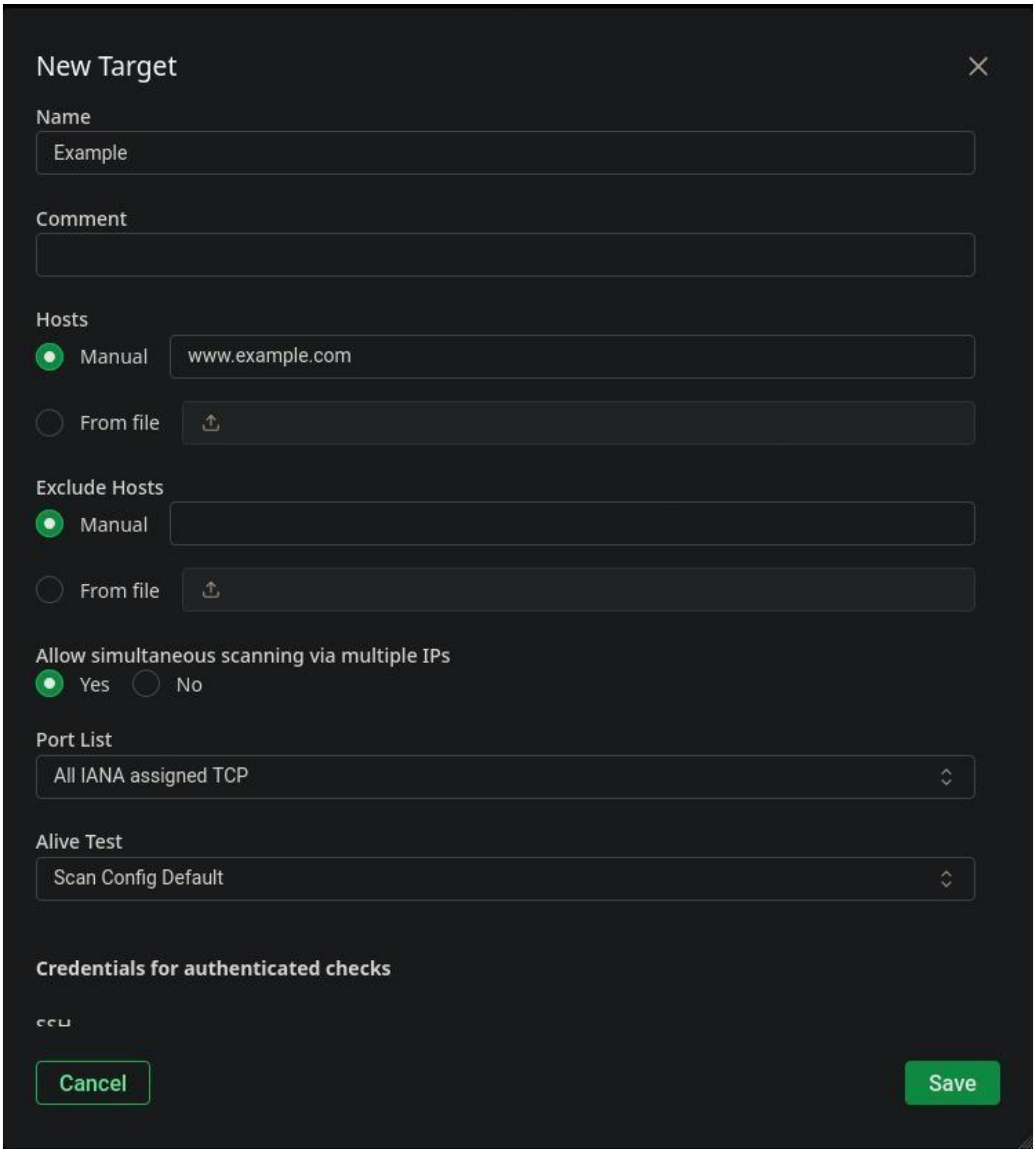
Conclusion:

This scan shows example.com is mostly secure, with informational findings and a single medium-priority improvement related to HTTP security headers.

Scan using OpenVAS

Create a New Target for Scanning

- Go to Configuration > Targets in the OpenVAS web interface.
- Click on "New Target" to define a scan target.
- Enter a name for the target
- In the "Hosts" field, enter the domain name www.example.com □ Save the target.



New Target

Name

Example

Comment

Hosts

● Manual www.example.com

○ From file

Exclude Hosts

● Manual

○ From file

Allow simultaneous scanning via multiple IPs

● Yes ○ No

Port List

All IANA assigned TCP

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

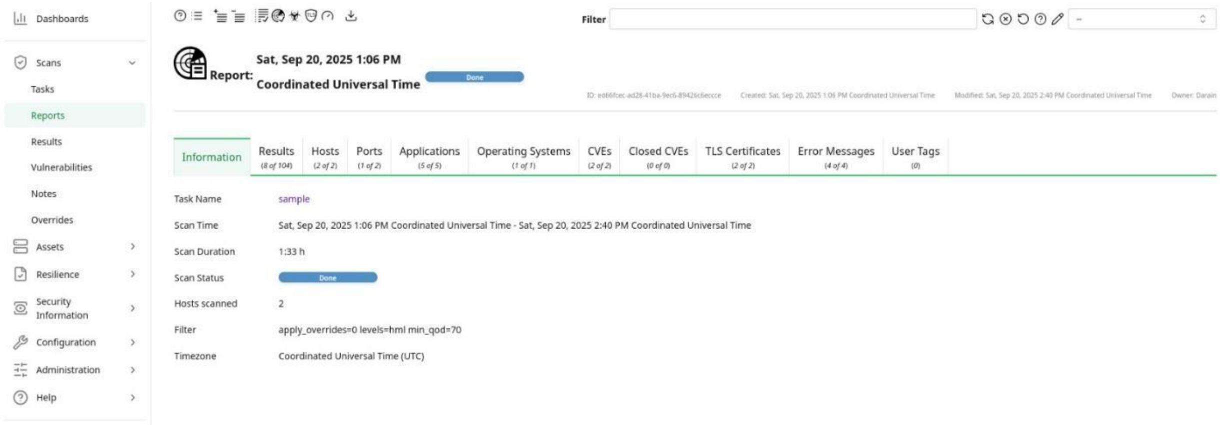
Create a New Scan Task

- Navigate to Scans > Tasks.
- Click on "New Task" to create a scanning task.
- Provide a name for the task.
- Select the scan target you created earlier from the drop-down list.
- Choose a scan configuration profile such as "Full and Fast" for comprehensive scanning or another profile depending on needs.
- Save the scan task.

Start the Scan

- In the Tasks tab, find your scan task and click the "Play" icon or "Start" button to initiate the scan.
- The scan status will change from "Requested" to "Running" and show progress.
- Scanning may take several minutes depending on the target and scan configuration.

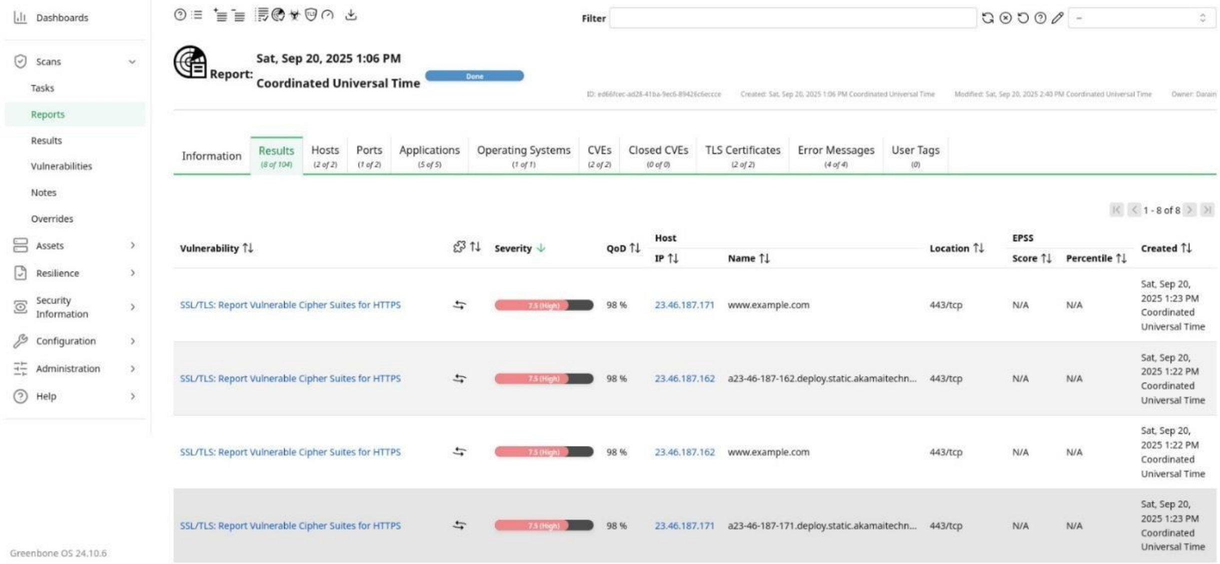
Scan Results:



Report: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

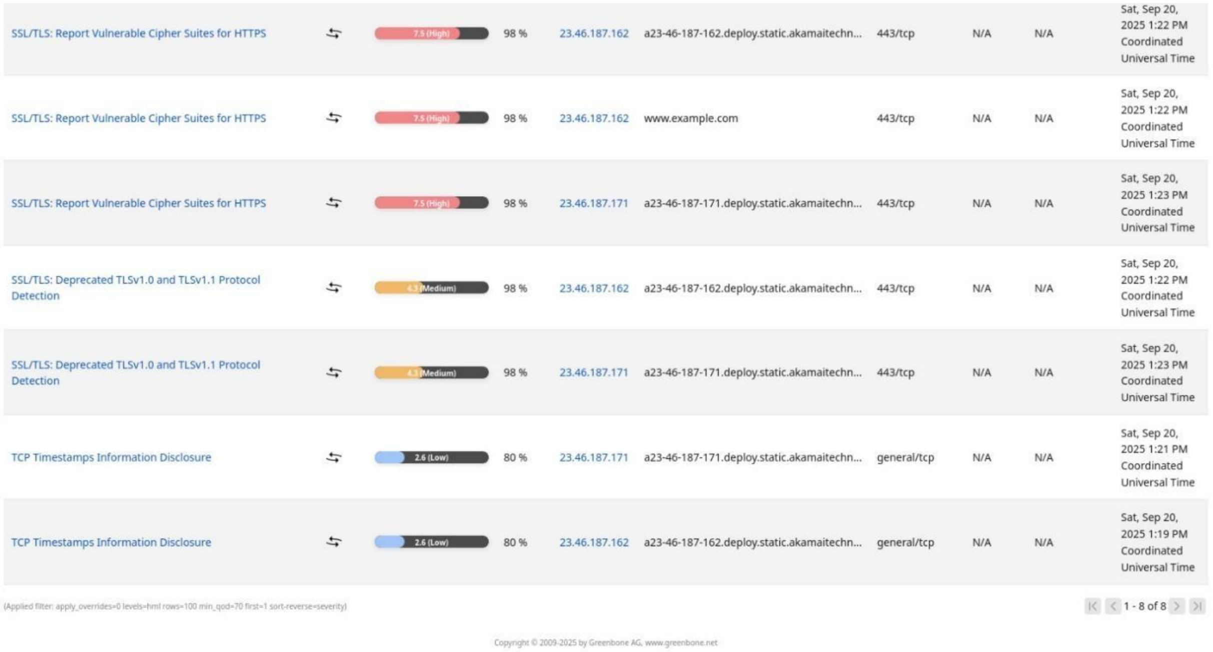
Task Name	sample
Scan Time	Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time - Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time
Scan Duration	1:33 h
Scan Status	Done
Hosts scanned	2
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)



Report: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

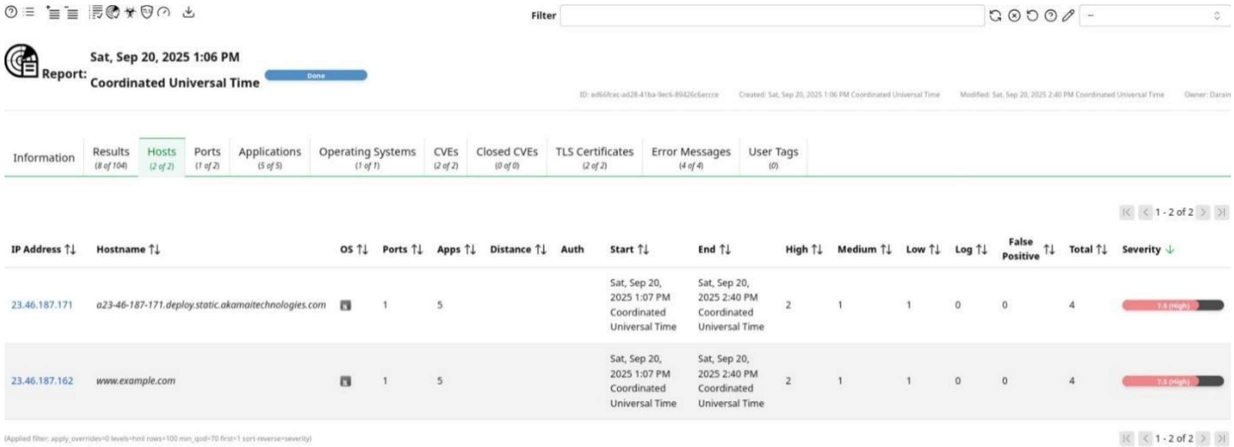
Vulnerability ⇅	⇅	Severity ↓	QoD ⇅	Host		Location ⇅	EPSS		Created ⇅
				IP ⇅	Name ⇅		Score ⇅	Percentile ⇅	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.171	www.example.com	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:23 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.162	a23-46-187-162.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:22 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.162	www.example.com	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:22 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.171	a23-46-187-171.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:23 PM Coordinated Universal Time



SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.162	a23-46-187-162.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:22 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.162	www.example.com	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:22 PM Coordinated Universal Time
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	23.46.187.171	a23-46-187-171.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:23 PM Coordinated Universal Time
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	23.46.187.162	a23-46-187-162.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:22 PM Coordinated Universal Time
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	23.46.187.171	a23-46-187-171.deploy.static.akamaitechn...	443/tcp	N/A	N/A	Sat, Sep 20, 2025 1:23 PM Coordinated Universal Time
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	23.46.187.171	a23-46-187-171.deploy.static.akamaitechn...	general/tcp	N/A	N/A	Sat, Sep 20, 2025 1:21 PM Coordinated Universal Time
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	23.46.187.162	a23-46-187-162.deploy.static.akamaitechn...	general/tcp	N/A	N/A	Sat, Sep 20, 2025 1:19 PM Coordinated Universal Time

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 8 of 8



Report: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

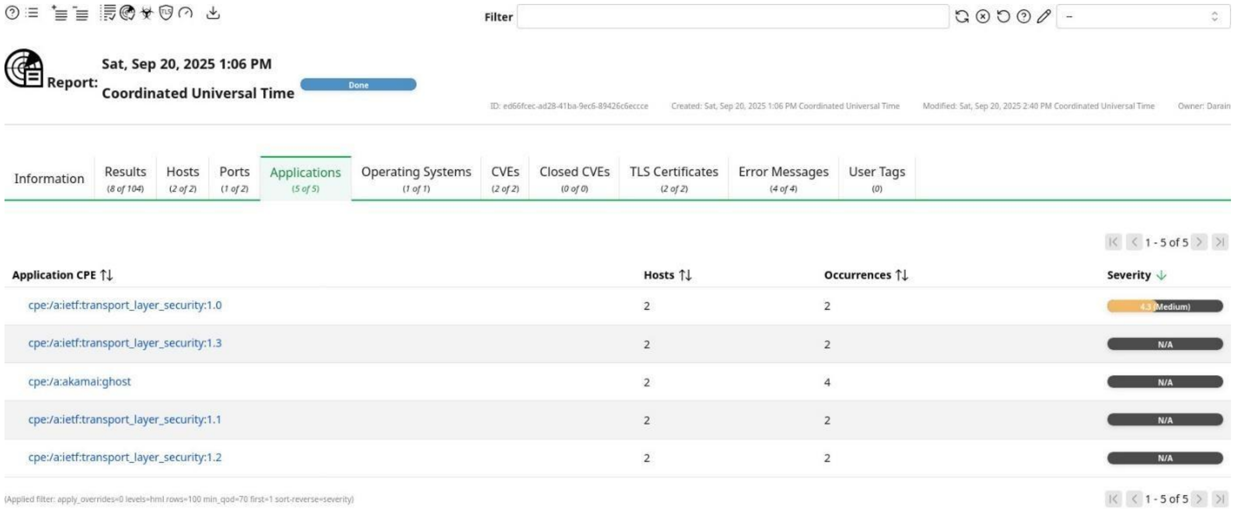
Information | Results (8 of 104) | Hosts (2 of 2) | Ports (1 of 2) | Applications (5 of 5) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (4 of 4) | User Tags (0)

1 - 2 of 2

IP Address ⇅	Hostname ⇅	OS ⇅	Ports ⇅	Apps ⇅	Distance ⇅	Auth	Start ⇅	End ⇅	High ⇅	Medium ⇅	Low ⇅	Log ⇅	False Positive ⇅	Total ⇅	Severity ↓
23.46.187.171	*a23-46-187-171.deploy.static.akamaitechnologies.com*	▪	1	5			Sat, Sep 20, 2025 1:07 PM Coordinated Universal Time	Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time	2	1	1	0	0	4	7.5 (High)
23.46.187.162	*www.example.com*	▪	1	5			Sat, Sep 20, 2025 1:07 PM Coordinated Universal Time	Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time	2	1	1	0	0	4	7.5 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2



Report: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

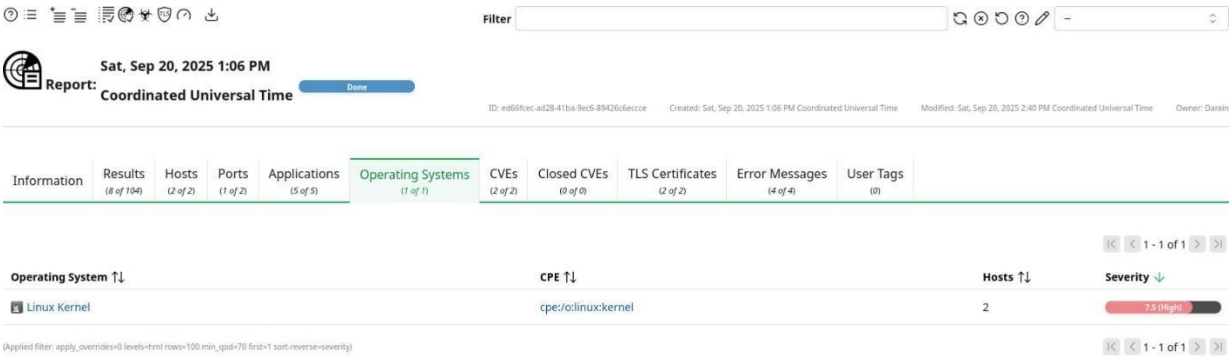
Information | Results (8 of 104) | Hosts (2 of 2) | Ports (1 of 2) | Applications (5 of 5) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (4 of 4) | User Tags (0)

1 - 5 of 5

Application CPE ⇅	Hosts ⇅	Occurrences ⇅	Severity ↓
cpe:/a:ietf:transport_layer_security:1.0	2	2	4.3 (Medium)
cpe:/a:ietf:transport_layer_security:1.3	2	2	N/A
cpe:/a:akamai:ghost	2	4	N/A
cpe:/a:ietf:transport_layer_security:1.1	2	2	N/A
cpe:/a:ietf:transport_layer_security:1.2	2	2	N/A

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5



Filter

Report: **Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time** Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

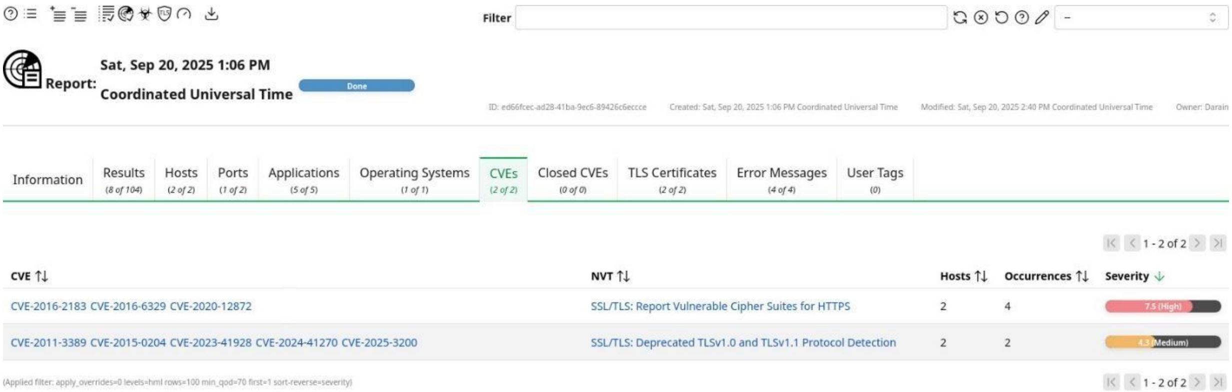
Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(8 of 104)	(2 of 2)	(1 of 2)	(5 of 5)	(1 of 1)	(2 of 2)	(0 of 0)	(2 of 2)	(4 of 4)	(0)

1 - 1 of 1

Operating System ↑↓	CPE ↑↓	Hosts ↑↓	Severity ↓
Linux Kernel	cpe:/o:linux:kernel	2	7.5 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 1 of 1



Filter

Report: **Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time** Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

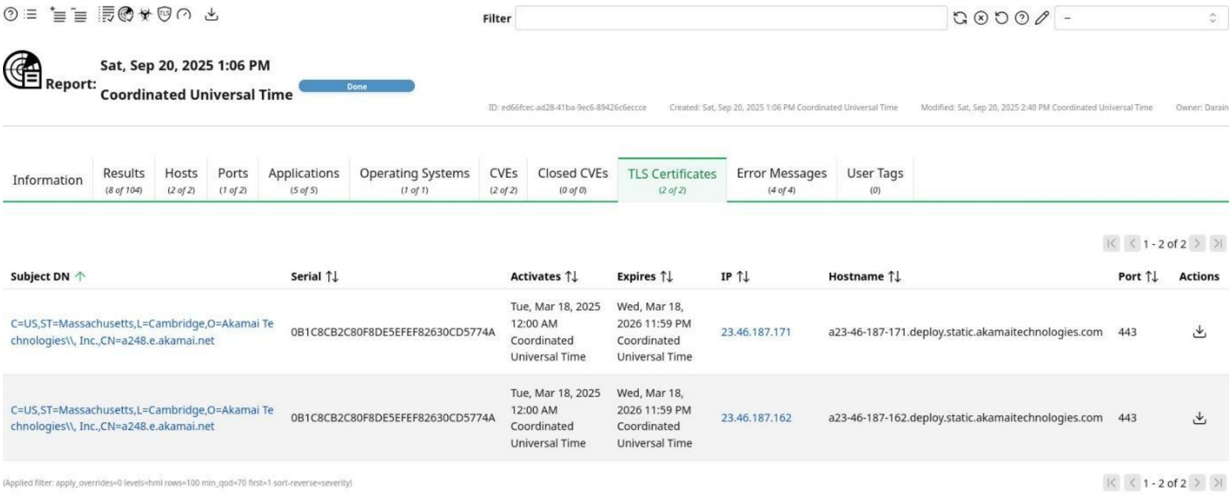
Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(8 of 104)	(2 of 2)	(1 of 2)	(5 of 5)	(1 of 1)	(2 of 2)	(0 of 0)	(2 of 2)	(4 of 4)	(0)

1 - 2 of 2

CVE ↑↓	NVT ↑↓	Hosts ↑↓	Occurrences ↑↓	Severity ↓
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	2	4	7.5 (High)
CVE-2011-3389 CVE-2015-0204 CVE-2023-41928 CVE-2024-41270 CVE-2025-3200	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2	2	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2



Filter

Report: **Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time** Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

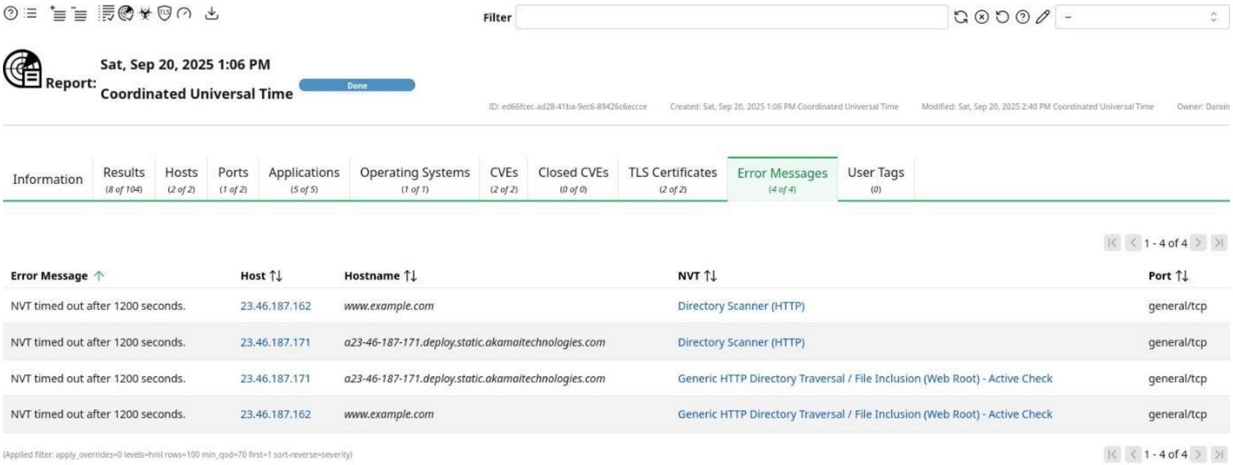
Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(8 of 104)	(2 of 2)	(1 of 2)	(5 of 5)	(1 of 1)	(2 of 2)	(0 of 0)	(2 of 2)	(4 of 4)	(0)

1 - 2 of 2

Subject DN ↑	Serial ↑↓	Activates ↑↓	Expires ↑↓	IP ↑↓	Hostname ↑↓	Port ↑↓	Actions
C=US,ST=Massachusetts,L=Cambridge,O=Akamai Technologies\\, Inc.,CN=a248.e.akamai.net	0B1C8CB2C80F8DE5EFEF82630CD5774A	Tue, Mar 18, 2025 12:00 AM Coordinated Universal Time	Wed, Mar 18, 2026 11:59 PM Coordinated Universal Time	23.46.187.171	a23-46-187-171.deploy.static.akamaitechnologies.com	443	
C=US,ST=Massachusetts,L=Cambridge,O=Akamai Technologies\\, Inc.,CN=a248.e.akamai.net	0B1C8CB2C80F8DE5EFEF82630CD5774A	Tue, Mar 18, 2025 12:00 AM Coordinated Universal Time	Wed, Mar 18, 2026 11:59 PM Coordinated Universal Time	23.46.187.162	a23-46-187-162.deploy.static.akamaitechnologies.com	443	

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2



Filter

Report: **Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time** Done

ID: ed66fcec-ad28-41ba-9ec6-89426c6eccce Created: Sat, Sep 20, 2025 1:06 PM Coordinated Universal Time Modified: Sat, Sep 20, 2025 2:40 PM Coordinated Universal Time Owner: Darain

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(8 of 104)	(2 of 2)	(1 of 2)	(5 of 5)	(1 of 1)	(2 of 2)	(0 of 0)	(2 of 2)	(4 of 4)	(0)

1 - 4 of 4

Error Message ↑	Host ↑↓	Hostname ↑↓	NVT ↑↓	Port ↑↓
NVT timed out after 1200 seconds.	23.46.187.162	*www.example.com*	Directory Scanner (HTTP)	general/tcp
NVT timed out after 1200 seconds.	23.46.187.171	*a23-46-187-171.deploy.static.akamaitechnologies.com*	Directory Scanner (HTTP)	general/tcp
NVT timed out after 1200 seconds.	23.46.187.171	*a23-46-187-171.deploy.static.akamaitechnologies.com*	Generic HTTP Directory Traversal / File Inclusion (Web Root) - Active Check	general/tcp
NVT timed out after 1200 seconds.	23.46.187.162	*www.example.com*	Generic HTTP Directory Traversal / File Inclusion (Web Root) - Active Check	general/tcp

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 4 of 4

Scan Overview :

- Hosts scanned: 23.46.187.171 and 23.46.187.162 (both mapping to www.example.com) □ Total findings (after filtering): 8 significant vulnerabilities □ Severity Breakdown: □ High: 2
- Medium: 2
- Low: 2

Major Vulnerabilities

High Severity (CVSS 7.5)

- Use of vulnerable cipher suites for HTTPS, specifically the presence of TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32 attack, CVE-2016-2183, CVE2016-6329, CVE-2020-12872).
- Impact: Attackers may be able to obtain sensitive information or exploit unspecified impacts due to the use of a weak 64-bit block cipher 3DES.

Medium Severity (CVSS 4.3)

- Deprecated protocol support—TLSv1.0 and TLSv1.1 are enabled along with newer TLSv1.2.
- Impact: Exposes the service to risks of eavesdropping, legacy cryptographic flaws (e.g., BEAST, FREAK attacks), and a lack of security patches for deprecated protocols.

Observations

- No critical (CVSS ≥ 9.0) vulnerabilities were identified.
- All findings are addressable via configuration and software patching.
- Regular vulnerability scans and monitoring are advised to promptly detect emerging threats in SSL/TLS protocols and other network layers.

Conclusion:

This provides an actionable overview of the security posture of www.example.com as evaluated by the OpenVAS scan, with a clear roadmap for remediating the discovered weaknesses.