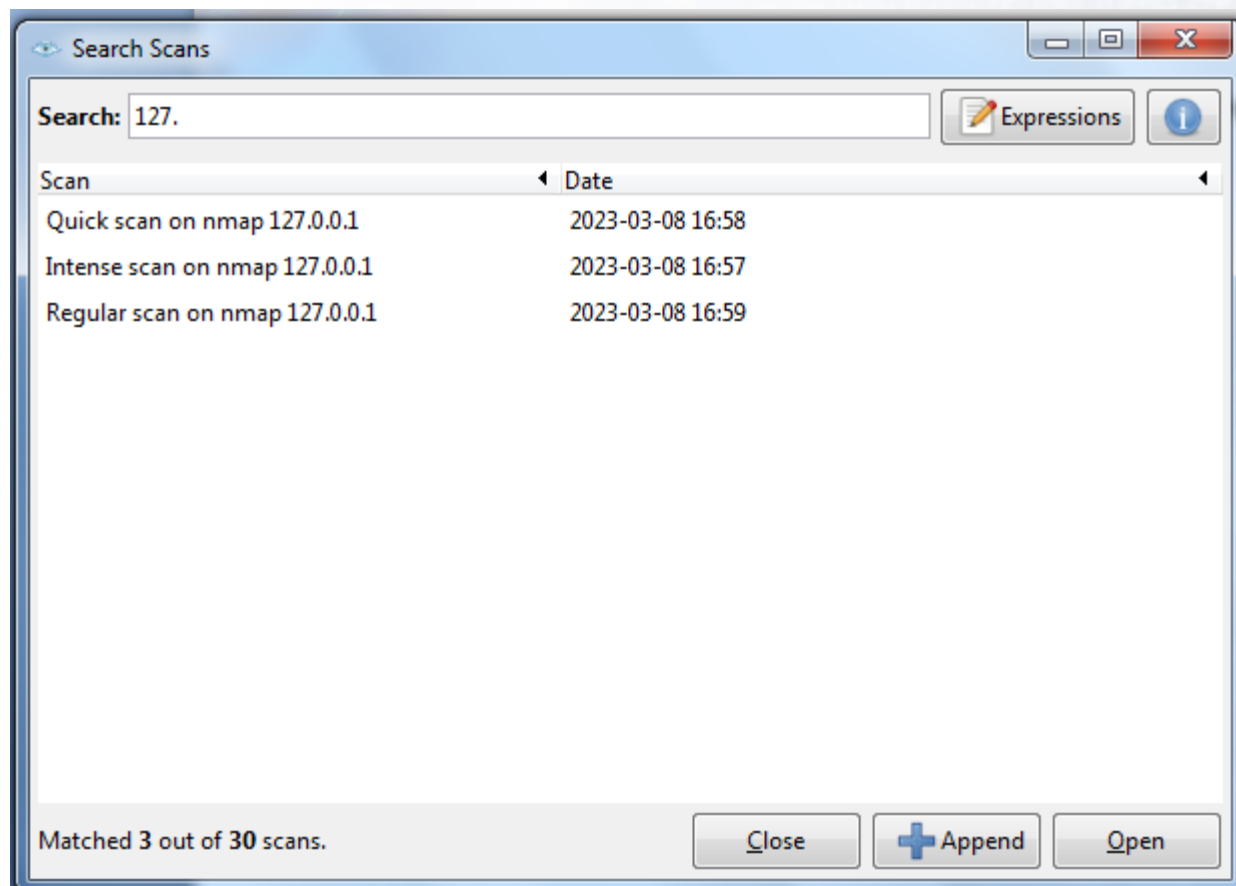




```
nmap -F nmap 127.0.0.1
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 16:58 Pakistan Standard Time
```

```
Nmap scan report for localhost
```

```
Failed to resolve "nmap"
```

```
Host is up (0.00015s latency)
```

```
Not shown: 91 closed tcp ports
```

```
PORT      STATE SERVICE
```

```
135/tcp   open  msrpc
```

```
445/tcp   open  microsoft-ds
```

```
554/tcp   open  rtsp
```

```
49152/tcp open  unknown
```

```
49153/tcp open  unknown
```

```
49154/tcp open  unknown
```

```
49155/tcp open  unknown
```

```
49156/tcp open  unknown
```

```
49157/tcp open  unknown
```

```
Nmap done: 1 IP address
```

Search Scans

Search: 127

Expressions

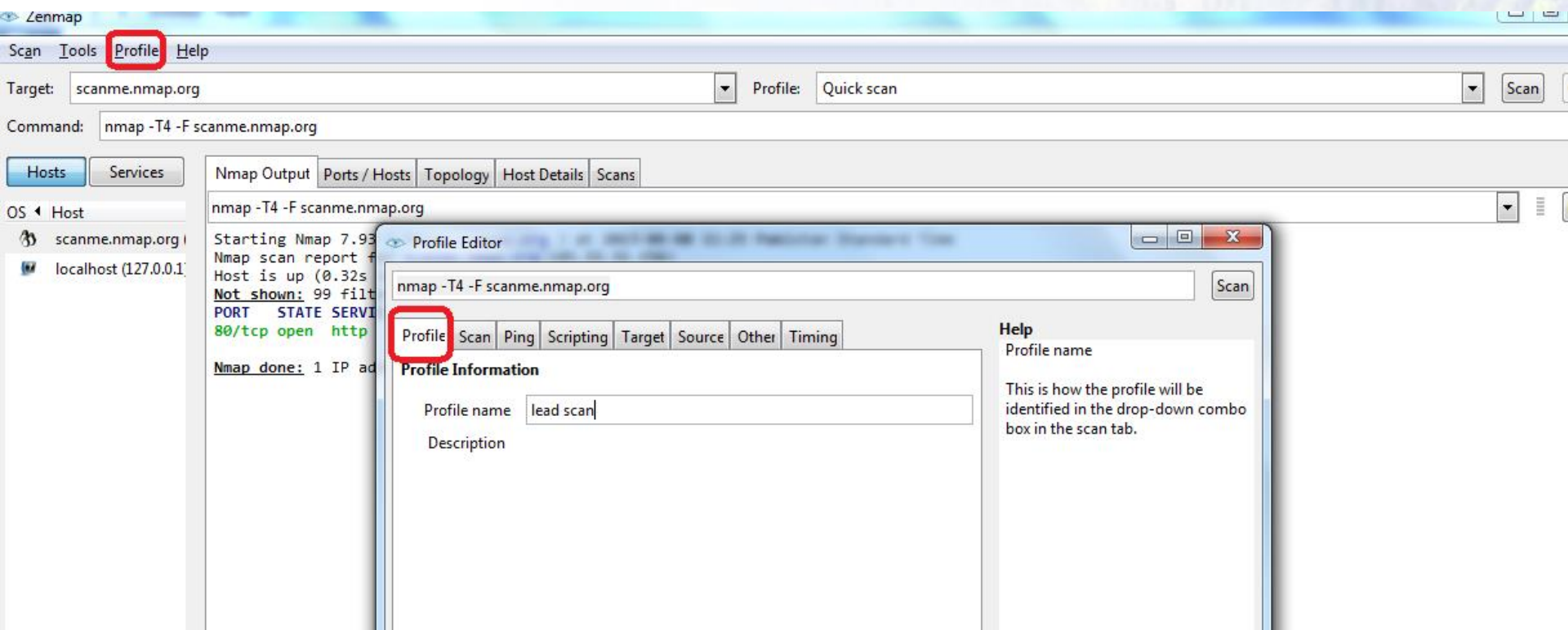
Scan	Date
Quick scan on nmap 127.0.0.1	2023-03-08 16:58
Intense scan on nmap 127.0.0.1	2023-03-08 16:57
Regular scan on nmap 127.0.0.1	2023-03-08 16:59

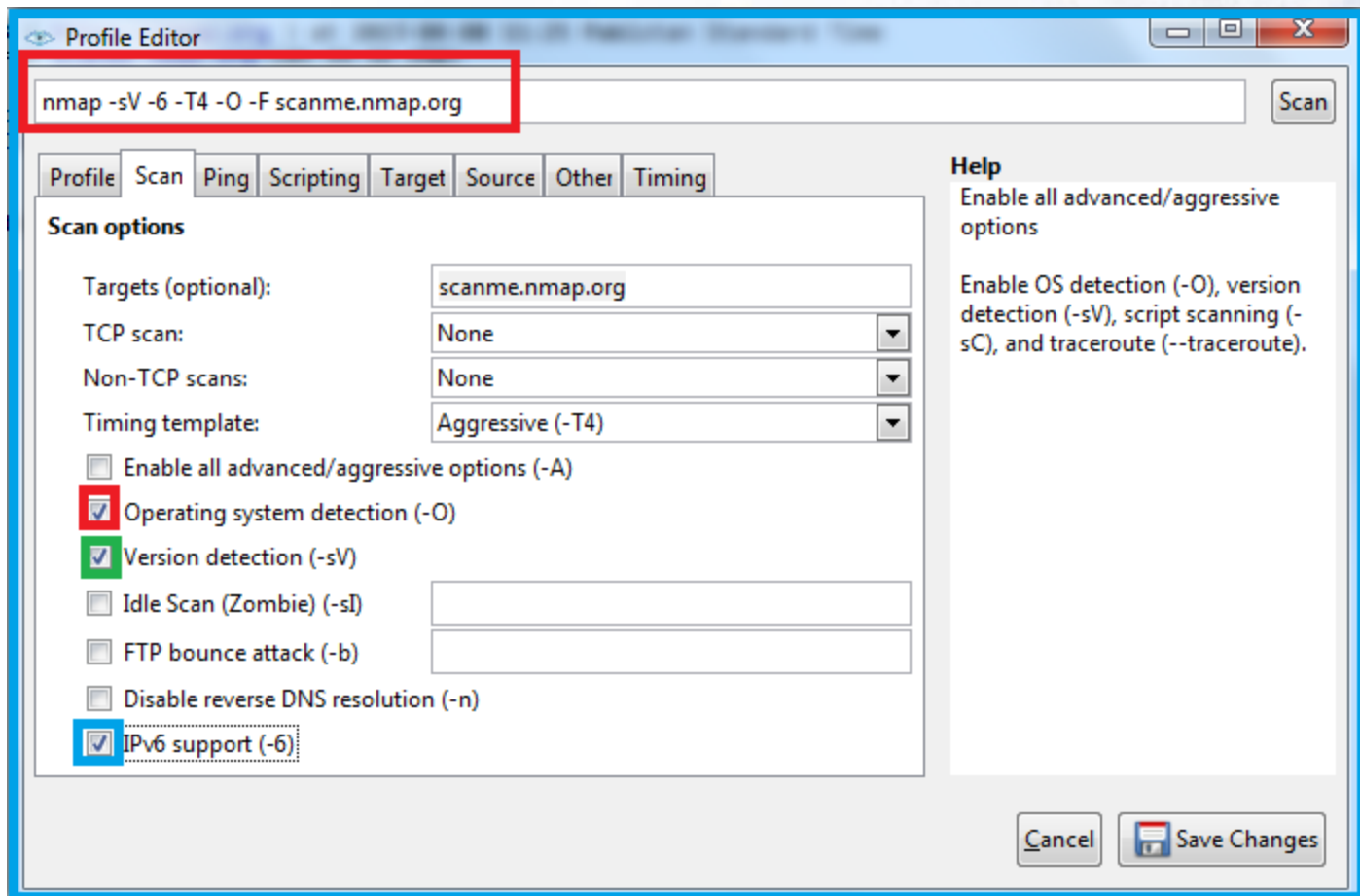
Matched 3 out of 30 scans.

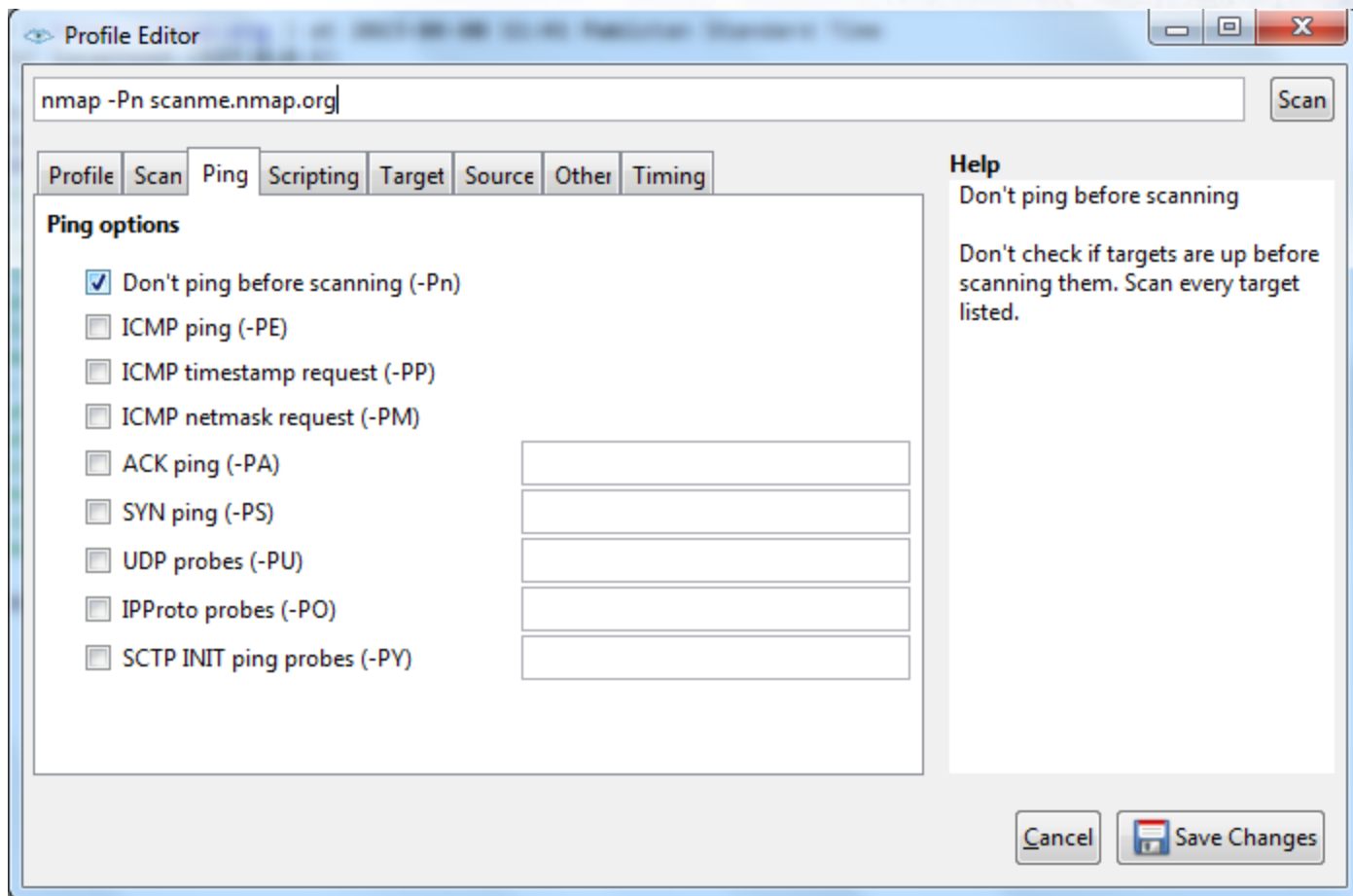
Close

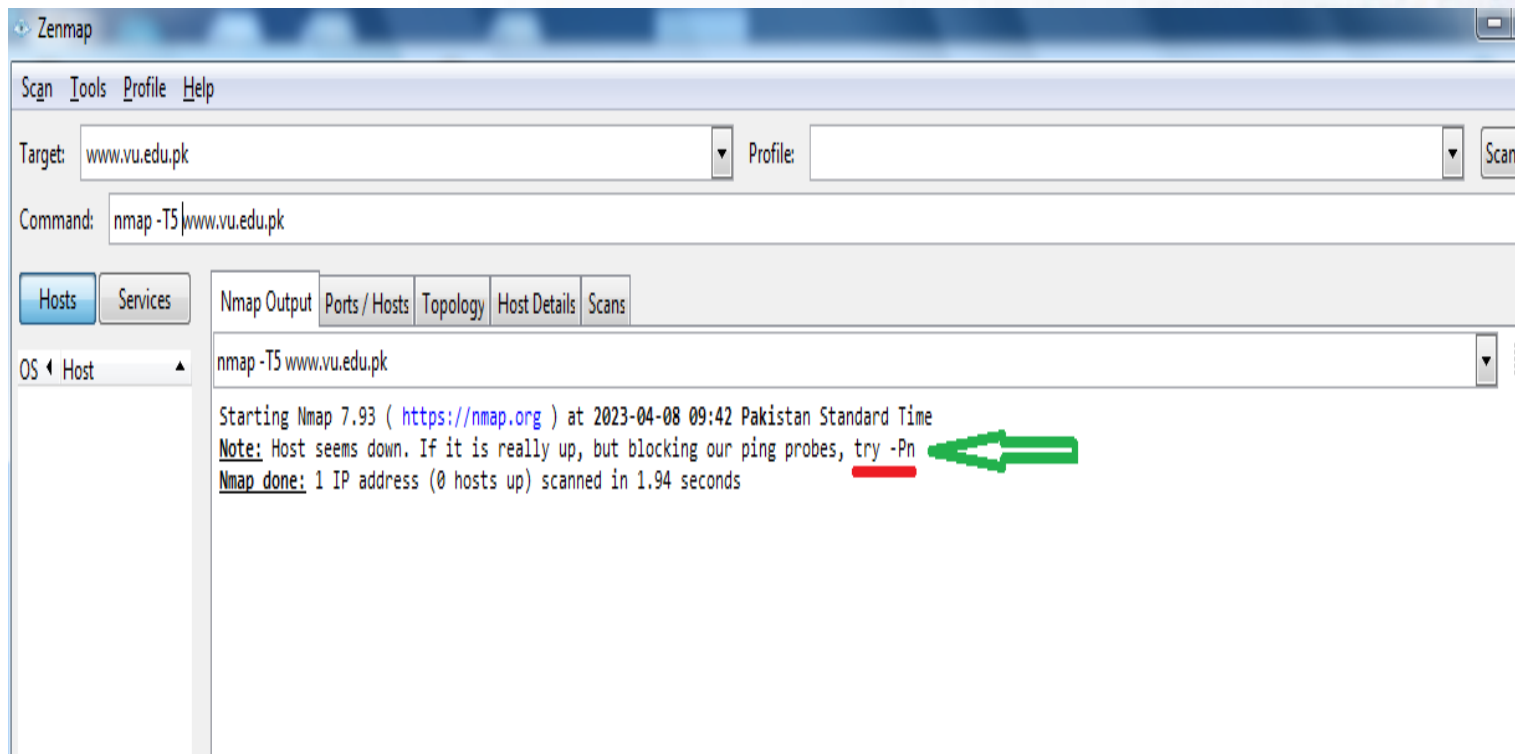
+ Append

Open









Nessus New scan

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Scan Templates

[Back to Scans](#)

Scanner

User Defined

Search Library

**Advanced Scan**

Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**

Audit the configuration of third-party cloud services.

**Badlock Detection**

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**

A full system scan suitable for any host.

**Credentialed Patch Audit**

Authenticate to hosts and enumerate missing updates.

**DROWN Detection**

Remote checks for CVE-2016-0800.

**Host Discovery**

A simple scan to discover live hosts and open ports.

**Intel AMT Security Bypass**

Remote and local checks for CVE-2017-5689.

**Internal PCI Network Scan**

Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**

Scan for malware on Windows and Unix systems.

**MDM Config Audit**

Audit the configuration of mobile device managers.

**Mobile Device Scan**

Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**

Audit the configuration of network devices.

**PCI Quarterly External Scan**

Approved for quarterly external scanning as required by PCI.

**Policy Compliance Auditing**

Audit system configurations against a known baseline.

**SCAP and OVAL Auditing**

Audit systems using SCAP and OVAL definitions.

**Shadow Brokers Scan**

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

**Spectre and Meltdown**

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

**WannaCry Ransomware**

Remote and local checks for MS17-010.

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Scan Templates

[Back to Scans](#)

Scanner

User Defined

**Advanced Scan**

Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**

Audit the configuration of third-party cloud services.

**Badlock Detection**

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**

A full system scan suitable for any host.

**Credentialed Patch Audit**

Authenticate to hosts and enumerate missing updates.

**DROWN Detection**

Remote checks for CVE-2016-0800.

**Host Discovery**

A simple scan to discover live hosts and open ports.

**Intel AMT Security Bypass**

Remote and local checks for CVE-2017-5689.

**Internal PCI Network Scan**

Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**

Scan for malware on Windows and Unix systems.

**MDM Config Audit**

Audit the configuration of mobile device managers.

**Mobile Device Scan**

Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**

Audit the configuration of network devices.

**PCI Quarterly External Scan**

Approved for quarterly external scanning as required by PCI.

**Policy Compliance Auditing**

Audit system configurations against a known baseline.

**SCAP and OVAL Auditing**

Audit systems using SCAP and OVAL definitions.

**Shadow Brokers Scan**

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

**Spectre and Meltdown**

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

**WannaCry Ransomware**

Remote and local checks for MS17-010.

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC



• General

[Schedule](#)[Notifications](#)

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

REQUIRED

Description

Folder

My Scans

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Upload Targets

[Add File](#)

Save



Cancel

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

General

[Schedule](#)[Notifications](#)

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Mike's Scan

Description

Folder

My Scans

Targets

172.30.0.0/24

Upload Targets

[Add File](#)

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

- Settings
- Credentials
- Compliance
- Plugins

- BASIC
 - General
 - Schedule
 - Notifications
- DISCOVERY >
- ASSESSMENT >
- REPORT >
- ADVANCED >

Enabled ☒

Frequency

- Once
- Once
- Daily
- Weekly
- Monthly
- Yearly

Starts

15:00

Timezone

Summary

k

ay, January 31st, 2018 at 3:00 PM

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

[Credentials](#)[Compliance](#)[Plugins](#)

BASIC

[General](#)[Schedule](#)• [Notifications](#)

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Email Recipient(s)

Example: me@example.com, you@example.com

Attach Report

☐ OFF

Result Filters

[Add Filter](#)[Save](#)[Cancel](#)

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

[Credentials](#)[Compliance](#)[Plugins](#)

BASIC

[General](#)[Schedule](#)

• Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Email Recipient(s)

mike@certmike.com

Attach Report

ON

Report Type

Nessus

Max Attachment Size

25

Size is in MB and should be less than 50. If the report is larger than this size, it will not be attached.

Result Filters

[Add Filter](#)

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

Host Discovery

[Port Scanning](#)[Service Discovery](#)

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host

ON

General Settings

- ☒ Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.
- ☐ Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy network discovery bypasses those additional tests.

Ping Methods

- ☒ ARP
- ☒ TCP
Destination ports
- ☒ ICMP
☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC >

DISCOVERY ✓

[Host Discovery](#)• [Port Scanning](#)[Service Discovery](#)

ASSESSMENT >

REPORT >

ADVANCED >

Ports

☐ Consider unscanned ports as closedPort scan range:

Local Port Enumerators

- ☒ SSH (netstat)
- ☒ WMI (netstat)
- ☒ SNMP
- ☒ Only run network port scanners if local port enumeration failed
- ☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

- ☐ TCP
 - ☐ Override automatic firewall detection
 - ☒ Use soft detection

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

[Credentials](#)[Compliance](#)[Plugins](#)

BASIC

DISCOVERY

[Host Discovery](#)• [Port Scanning](#)[Service Discovery](#)

ASSESSMENT

REPORT

ADVANCED

Ports

☐ Consider unscanned ports as closedPort scan range:

Local Port Enumerators

☒ SSH (netstat)☒ WMI (netstat)☒ SNMP☒ Only run network port scanners if local port enumeration failed☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

☐ TCP☐ Override automatic firewall detection

FOLDERS

My Scans

Routine Scans5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

General

Brute Force

SCADA

Web Applications

Windows

Malware

Accuracy

Antivirus

SMTP

☐ Override normal accuracy

☒ Avoid potential false alarms

☐ Show potential false alarms

☐ Perform thorough tests (may disrupt your network or impact scan speed)

Antivirus definition grace period (in days):

0

Third party domain

example.com

This domain must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be a SMTP server.

From address

nobody@example.com

To address

postmaster@[AUTO_REPLACED_IP]

FOLDERS

My Scans

Routine Scans

5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC



DISCOVERY



ASSESSMENT



REPORT



ADVANCED



General Settings

- ☒ Enable safe checks
- ☐ Stop scanning hosts that become unresponsive during the scan
- ☐ Scan IP addresses in a random order

Performance Options

- ☐ Slow down the scan when network congestion is detected

Network timeout (in seconds)

5

Max simultaneous checks per host

5

Max simultaneous hosts per scan

30

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

Debug Settings

- ☐ Log scan details

- FOLDERS
- My Scans
 - Routine Scans 5
 - All Scans
 - Trash
- RESOURCES
- Policies
 - Plugin Rules
 - Customized Reports
 - Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

STATUS	PLUGIN FAMILY ^	TOTAL	STATUS	PLUGIN NAME
ENABLED	AIX Local Security Checks	11392	No plugin family selected.	
ENABLED	Amazon Linux Local Security Checks	953		
ENABLED	Backdoors	111		
ENABLED	CentOS Local Security Checks	2528		
ENABLED	CGI abuses	3779		
ENABLED	CGI abuses : XSS	644		
ENABLED	CISCO	889		
ENABLED	Databases	563		
ENABLED	Debian Local Security Checks	5309		
ENABLED	Default Unix Accounts	167		
ENABLED	Denial of Service	109		
ENABLED	DNS	170		
ENABLED	F5 Networks Local Security Checks	603		
ENABLED	Fedora Local Security Checks	12295		

Nessus

Scans

Settings

Filter

Search Plugin Families

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

Back to Scan Templates

Disable A

Settings

Credentials

Compliance

Plugins

Show E

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME
DISABLED	AIX Local Security Checks	11392	No plugin family selected.	
ENABLED	Amazon Linux Local Security Checks	953		
ENABLED	Backdoors	111		
ENABLED	CentOS Local Security Checks	2528		
ENABLED	CGI abuses	3779		
ENABLED	CGI abuses : XSS	644		
DISABLED	CISCO	889		
ENABLED	Databases	563		
DISABLED	Debian Local Security Checks	5309		
ENABLED	Default Unix Accounts	167		
ENABLED	Denial of Service	109		
ENABLED	DNS	170		
DISABLED	F5 Networks Local Security Checks	603		
ENABLED	Fedora Local Security Checks	12295		

Save

Cancel

Linked Active

SETTINGS

About

Advanced

Proxy Server

Remote Link

SMTP Server

Custom CA

ACCOUNTS

My Account

About

Overview

Revert from Pro 7

Software Update

Master Password

Automatic Updates

☒ Update all components☐ Update plugins☐ Disabled

Update Frequency

Daily

Daily

Weekly

Monthly

Update Server

pst.mydomain.com

Save

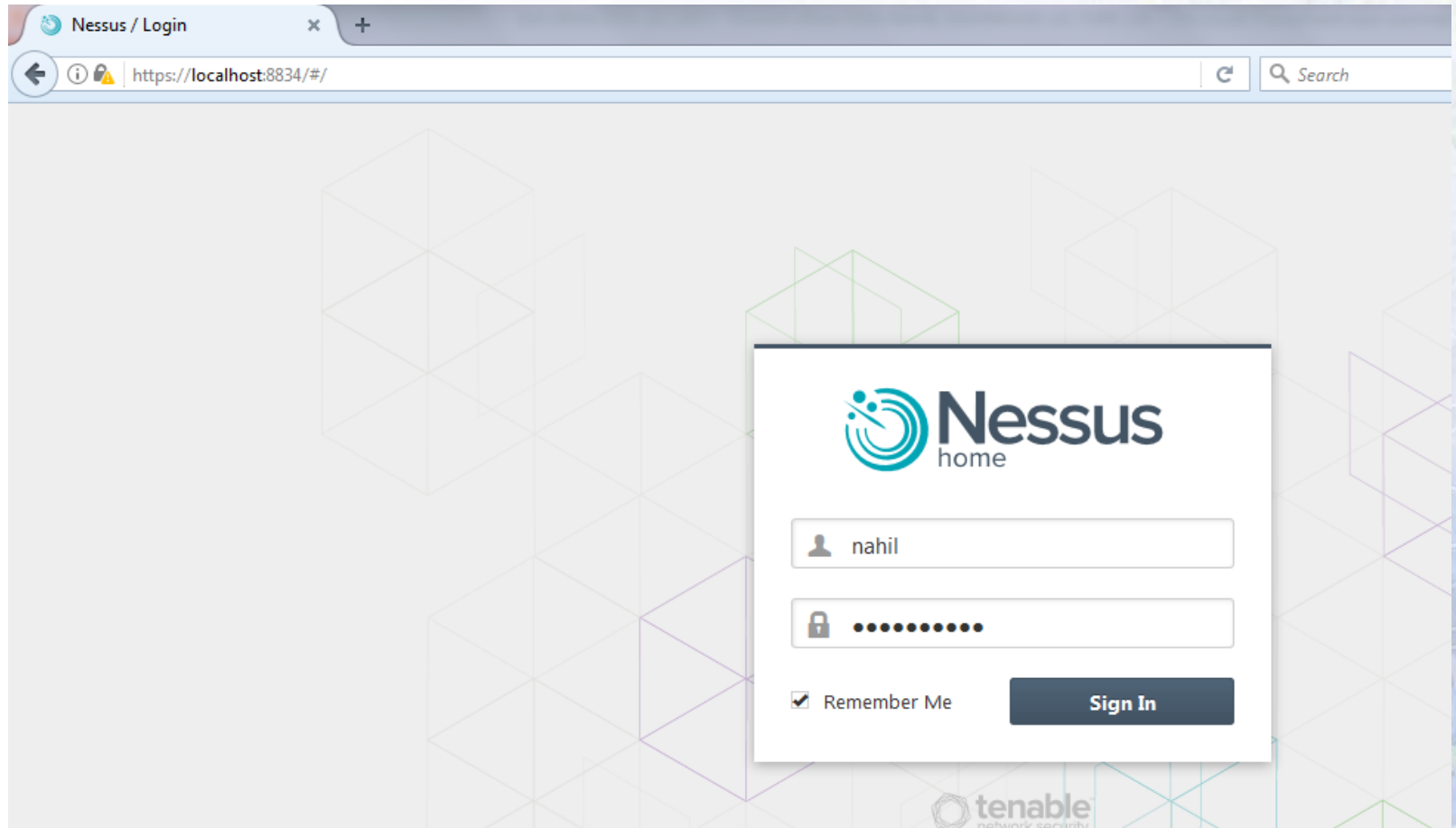
Cancel

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 1

LOGIN SCREEN



The screenshot shows a web browser window with the title "Nessus / Login". The address bar displays "https://localhost:8834/#/". The main content area features a large, faint geometric pattern. Overlaid on this is a white login form with the Nessus logo at the top. The form includes a username field with the text "nahil", a password field with masked characters, a "Remember Me" checkbox, and a "Sign In" button. The Tenable logo is visible in the bottom right corner of the page.

Nessus / Login

https://localhost:8834/#/

Nessus
home

nahil

.....

☒ Remember Me

Sign In

tenable
network security

Nessus Demo - 1

DASHBOARD

The screenshot displays the Nessus web interface for the 'Scans' section. The browser's address bar shows the URL 'https://localhost:8834/#/scans'. The interface features a dark header with the 'Nessus' logo and navigation links for 'Scans' and 'Policies'. Below the header, the main content area is titled 'Scans'. On the left, there is a sidebar with a 'New Scan' button and a list of options: 'My Scans', 'Trash', 'All Scans', and 'New Folder'. The main area is titled 'Scans / My Scans' and contains a message stating 'This folder is empty.'.

Nessus Home / Scans x +

https://localhost:8834/#/scans

Nessus Scans Policies

Scans

+ New Scan

My Scans

Trash

All Scans

New Folder

Scans / My Scans

This folder is empty.

Nessus Demo - 1

NEW SCAN

Scanner Templates

 Advanced Scan Configure a scan without using any recommendations.	 Audit Cloud Infrastructure Audit the configuration of third-party cloud services. UPGRADE	 Badlock Detection Remote and local checks for CVE-2016-2118 and	 Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and	 Basic Network Scan A full system scan suitable for any host.
 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 DROWN Detection Remote checks for CVE-2016-0800.	 Host Discovery A simple scan to discover live hosts and open ports.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	 Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan. UPGRADE
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers. UPGRADE	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. UPGRADE	 Offline Config Audit Audit the configuration of network devices. UPGRADE	 PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI. UPGRADE
 Policy Compliance Auditing Audit system configurations against a known baseline. UPGRADE	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions. UPGRADE	 Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.	 WannaCry Ransomware Remote and local checks for MS17-010.	 Web Application Tests Scan for published and unknown web vulnerabilities.

Nessus Demo - 1

WANNACRY RANSOMWARE SCAN



WannaCry Ransomware

Remote and local checks for
MS17-010.

Nessus Demo - 1

NEW SCAN WINDOW

New Scan / WannaCry Ransomware

Scan Library > Settings Credentials

BASIC 

General

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Settings / Basic / General

This policy is used to perform remote and local checks for vulnerabilities exploited by WannaCry Ransomware (MS17-010 / CVE-2017-0144). It requires the user to be provided to test via WMI and enumerate missing software updates.

Name

REQUIRED

Description

Folder

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Nessus Demo - 1

DASHBOARD VIEW WITH SCANS

Scans

+

New Scan

My Scans

Trash

All Scans

New Folder

Scans / My Scans

☐ Name	Schedule	Last Modified ▲
☐ LOCAL PC WANNACRY	On Demand	✓ 12:53 AM ▶ ✕
☐ NAHIL PC	On Demand	📅 N/A ▶ ✕

Nessus Demo - 1

NEW SCAN...

Scanner Templates



Advanced Scan

Configure a scan without using any recommendations.



UPGRADE

Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



DROWN Detection

Remote checks for CVE-2016-0800.

Nessus Demo - 1

ENTER SCAN DETAILS

New Scan / Advanced Scan

Scan Library > Settings Credentials Compliance Plugins

BASIC 

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name

LOCALHOST ADVANCED SCAN

Description

ADVANCED SCAN

Folder

My Scans

Targets

LOCALHOST

Nessus Demo - 1

CREDENTIAL SCAN

LOCALHOST ADVANCED SCAN / Confi...
POLICY: ADVANCED SCAN

Scan > Settings **Credentials** Compliance Plugins

CREDENTIALS

▶ Cloud Services

▶ Database

▼ Host

SNMPv3 1 +

SSH ∞ +

Windows ∞ +

▶ Miscellaneous

▶ Plaintext Authentication

ACTIVE CREDENTIALS

Save

Cancel

Nessus Demo - 1

COMPLIANCE SCAN

LOCALHOST ADVANCED SCAN / Confi...

POLICY: ADVANCED SCAN

Scan > Settings Credentials **Compliance** Plugins

COMPLIANCE CHECKS

▶ Adtran AOS

▶ Amazon AWS

▶ Arista EOS

▶ BlueCoat ProxySG

▶ Brocade FabricOS

▶ Check Point GAiA

▶ Cisco IOS

▶ Citrix XenServer

▶ Database

▶ Dell Force10 FTOS

ACTIVE COMPLIAN

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)

▸ Unix File Contents	
▸ VMware vCenter/vSphere	
▸ WatchGuard	
▼ Windows	
(Upload a custom Windows audit file)	∞ +
CIS Exchange 2007 Enterprise Edge Transport 1...	1 +
CIS Google Chrome L1 v1.1.0	1 +
CIS Google Chrome L2 v1.1.0	1 +
CIS IE 10 v1.1.0	1 +
CIS IE 11 v1.0.0	1 +
CIS IE 9 v1.0.0	1 +
CIS IIS 10 v1.0.0 Level 1	1 +
CIS IIS 10 v1.0.0 Level 2	1 +
CIS IIS 6.0 v1.0.0	1 +
CIS IIS 7 L2 v1.8.0	1 +
CIS IIS 8.0 v1.5.0 Level 1	1 +
CIS IIS 8.0 v1.5.0 Level 2	1 +

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)...

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0	×
CIS Microsoft Office Outlook 2013 v1.1.0 Level 1	×
CIS Microsoft Office 2013 v1.1.0	×
CIS Microsoft Office Word 2013 v1.1.0	×
CIS IE 10 v1.1.0	×
▶ CIS Google Chrome L1 v1.1.0	×
CIS Microsoft Office PowerPoint 2013 v1.0.1	×
CIS Windows 7 Level 2 v3.0.1	×
▼ DISA STIG Google Chrome V1R8	×

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

ADVANCED SCAN / COMPLIANCE

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0



CIS Microsoft Office Outlook 2013 v1.1.0 Level 1



CIS Microsoft Office 2013 v1.1.0



CIS Microsoft Office Word 2013 v1.1.0



CIS IE 10 v1.1.0



▶ CIS Google Chrome L1 v1.1.0



CIS Microsoft Office PowerPoint 2013 v1.0.1



CIS Windows 7 Level 2 v3.0.1



▼ **DISA STIG Google Chrome V1R8**



Nessus Demo - 2

ADVANCED SCAN / PLUG-INS

LOCALHOST ADVANCED SCAN / Confi...

POLICY: ADVANCED SCAN

Disable All Enable All

Filter Plugin Families

Scan > Settings Credentials Compliance Plugins

Show Enabled | Show All

DISABLED	SuSE Local Security Checks	10107
DISABLED	Ubuntu Local Security Checks	3763
DISABLED	Virtuozzo Local Security Checks	130
DISABLED	VMware ESX Local Security Checks	114
DISABLED	Web Servers	1018
DISABLED	Windows	3772
ENABLED	Windows : Microsoft Bulletins	1323
DISABLED	Windows : User management	28

Status	Plugin Name	Plugin ID
ENABLED	2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Ar...	58484
ENABLED	2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary M...	58321
ENABLED	3CTftpSvc Long Transport Mode Remote Overflow	23735
ENABLED	3D-FTP Multiple Directory Traversal Vulnerabilities	33218
ENABLED	3DGreetings Player ActiveX Multiple Buffer Overflows	26020
ENABLED	3ivx MPEG-4 < 5.0.2 Buffer Overflow	29749
ENABLED	7-Zip < 16.00 Multiple Vulnerabilities	91230

Save

Cancel

Nessus Demo - 2

SCAN...IN PROGRESS

Scans

+ New Scan

My Scans 1

Trash 1

All Scans

New Folder

Scans / My Scans

☐

Name

☐

LOCALHOST ADVANCED SCAN

Schedule

On Demand

Last Modified ▲

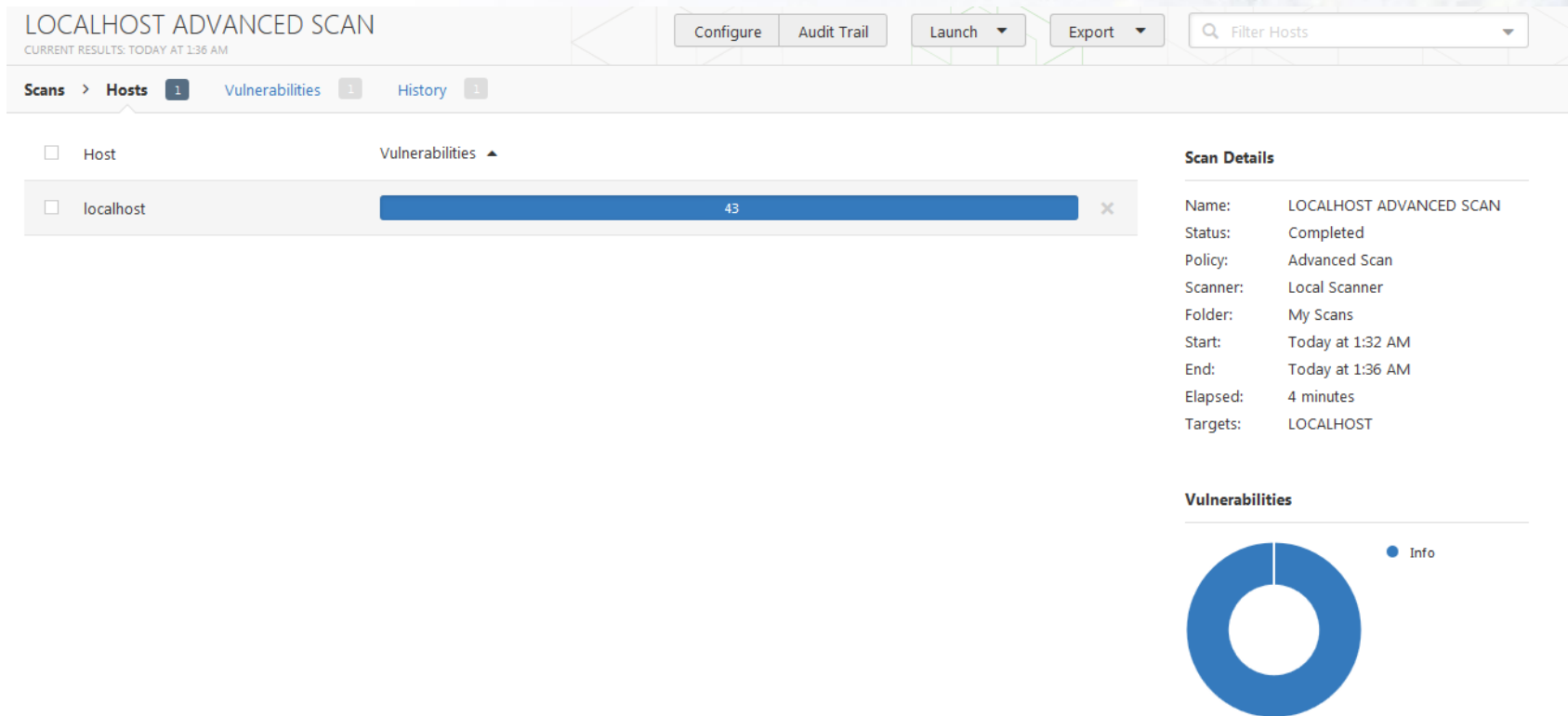
01:32 AM

||

■

Nessus Demo - 2

SCAN REPORT [43 INFO]



Nessus Demo - 2

SCAN REPORT [DETAILS]

LOCALHOST ADVANCED SCAN
CURRENT RESULTS: TODAY AT 1:36 AM

Configure

Audit Trail

Launch ▼

Export ▼

Hosts > localhost > Vulnerabilities 1

☐ Severity ▲	Plugin Name	Plugin Family	Count
☐ INFO	Netstat Portscanner (SSH)	Port scanners	43

Host Details

IP: 127.0.0.1
DNS: localhost
OS: Microsoft Windows 7 Home
Start: Today at 1:32 AM
End: Today at 1:36 AM
Elapsed: 4 minutes
KB: [Download](#)

Vulnerabilities

Info



6

Nessus Demo - 2

SCAN REPORT [DETAILS...]

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost 

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost 

Port 135/tcp was found to be open

Port ▼	Hosts
135 / tcp / epmap	localhost 

Port 137/udp was found to be open

Port ▼	Hosts
137 / udp	localhost 

Nessus Demo - 2

WEB APPLICATION TEST

Audit

ration of
ices.

PCI Quarterly External Scan

Approved for quarterly external
scanning as required by PCI.

Software

checks for
l,



Web Application Tests

Scan for published and unknown
web vulnerabilities.

Nessus Demo - 2

WEB APPLICATION TEST - CREDENTIALS

New Scan / Web Application Tests

Scan Library > Settings Credentials

CREDENTIALS

All credentials in use

ACTIVE CREDENTIALS

▼ HTTP

Authentication method	HTTP login form
Username	admin REQUIRED
Password	REQUIRED
Login page	/login.php REQUIRED
Login submission page	/process_login.php REQUIRED
Login parameters	user=%USER%&pass=%PASS% REQUIRED

If the keywords %USER% and %PASS% are used, they will be substituted with the values above.

Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT



Advanced Scan

Configure a scan without using any recommendations.



Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



DROWN Detection

Remote checks for CVE-2016-0800.



Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT

New Scan / Credentialed Patch Audit

Scan Library > Settings Credentials

CREDENTIALS

- Database
- Host
 - SSH
 - Windows
- Miscellaneous
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Authentication method: Password

Username: administrator

Password:

Domain:

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication

Nessus Demo - 2

SCANS DASHBOARD

Scans

New Scan

My Scans1

Trash1

All Scans

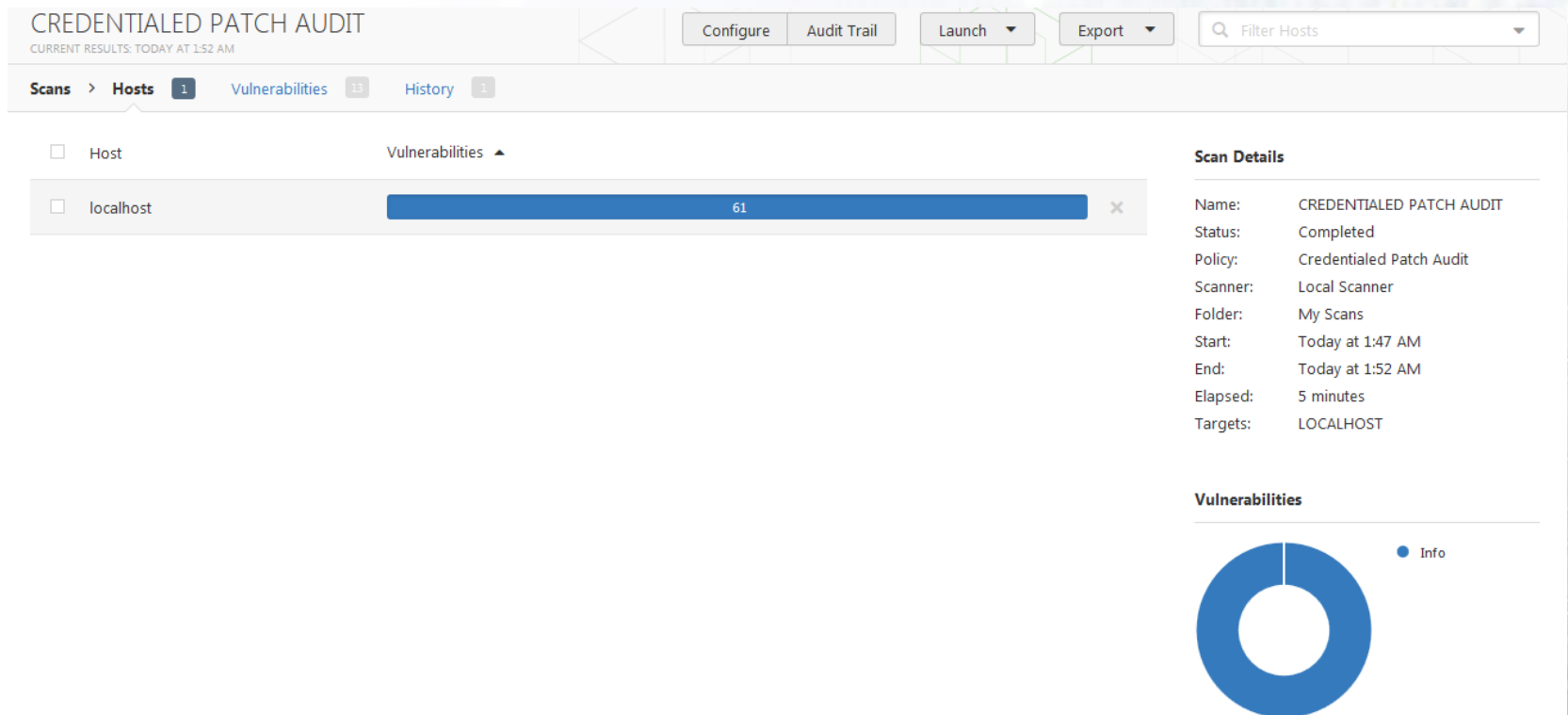
New Folder

Scans / My Scans

☐ Name	Schedule	Last Modified ▲		
☐ CREDENTIALLED PATCH AUDIT	On Demand	01:47 AM		■
☐ LOCALHOST ADVANCED SCAN	On Demand	01:36 AM	▶	✕

Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [61 INFO]



Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [61 INFO]

CREDENTIALIALED PATCH AUDIT
CURRENT RESULTS: TODAY AT 1:52 AM

Configure

Audit Trail

Launch

Export

Hosts > localhost > Vulnerabilities 13

☐ Severity ▲	Plugin Name	Plugin Family	Count
☐ INFO	Netstat Portscanner (SSH)	Port scanners	43
☐ INFO	DCE Services Enumeration	Windows	7
☐ INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1
☐ INFO	Authentication Failure - Local Checks Not Run	Settings	1
☐ INFO	Microsoft Windows NTLMSSP Authentication Request Remote Network Nam...	Windows	1
☐ INFO	Microsoft Windows SMB Log In Possible	Windows	1
☐ INFO	Microsoft Windows SMB NativeLanManager Remote System Information Dis...	Windows	1
☐ INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Regi...	Windows	1
☐ INFO	Microsoft Windows SMB Service Detection	Windows	1

Host Details

IP: 127.0.0.1
DNS: localhost
OS: Microsoft Windows 7 Home
Start: Today at 1:47 AM
End: Today at 1:52 AM
Elapsed: 5 minutes
KB: [Download](#)

Vulnerabilities

Info

Nessus Demo - 2

CREDENTIALIAED AUDIT SCAN RESULTS [DETAILS]

INFO Netstat Portscanner (SSH) >

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost 

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost 

Port 135/tcp was found to be open

Plugin Details

Severity:	Info
ID:	14272
Version:	1.68
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2017/06/16

Risk Information

Risk Factor: None

Nessus Demo - 2

SYSTEM MALWARE SCAN

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	DROWN Detection Remote checks for CVE-2016-0800.
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers.
 Policy Compliance Auditing Audit system configurations against a known baseline.	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

Nessus Demo - 2

SYSTEM MALWARE SCAN

New Scan / Malware Scan

Scan Library > Settings Credentials

CREDENTIALS

Host
SSH ∞ +
Windows ∞ +

ACTIVE CREDENTIALS

▼ Windows

Authentication method Password ▼

Username administrator

Password •••••

Domain

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication
- ☐ Start the Remote Registry service during the scan

Nessus Demo - 2

SCAN DASHBOARD

Scans

+ New Scan

My Scans1

Trash1

All Scans

New Folder

Scans / My Scans

☐	Name	Schedule	Last Modified ▲		
☐	WEBSITE	On Demand	02:16 AM		■
☐	SYSTEM MALWARE SCAN	On Demand	✓ 02:10 AM	▶	✕
☐	CREDENTIALLED PATCH AUDIT	On Demand	✓ 01:52 AM	▶	✕
☐	LOCALHOST ADVANCED SCAN	On Demand	✓ 01:36 AM	▶	✕

© 1998 - 2017 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.10.9

Nessus Demo - 2

SYSTEM MALWARE SCAN [2 INFO]

SYSTEM MALWARE SCAN

CURRENT RESULTS: TODAY AT 2:10 AM

[Configure](#) [Audit Trail](#) [Launch](#) [Export](#)

Scans > Hosts 1 Vulnerabilities 2 History 2

☐ Host Vulnerabilities ▲

☐ localhost 2

Scan Details

Name:	SYSTEM MALWARE SCAN
Status:	Completed
Policy:	Malware Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 2:10 AM
End:	Today at 2:10 AM
Elapsed:	a few seconds
Targets:	LOCALHOST

Vulnerabilities

Info

Nessus Demo - 2

SYSTEM MALWARE SCAN

SYSTEM MALWARE SCAN

CURRENT RESULTS: TODAY AT 2:10 AM

Configure

Audit Trail

Launch

Export

Filter Vulnerabilities

Hosts

localhost

Vulnerabilities

2

☐	Severity	Plugin Name	Plugin Family	Count
☐	INFO	Authentication Failure - Local Checks Not Run	Settings	1
☐	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1

Host Details

IP:

127.0.0.1

DNS:

localhost

Start:

Today at 2:10 AM

End:

Today at 2:10 AM

Elapsed:

a few seconds

KB:

[Download](#)

Vulnerabilities

Info



Nessus Demo - 2

- Nessus is an easy to use and powerful scanner
- Dozens of scans on dashboard
- Setup a new scan
- Setup a profile as scan template
- Credentialed scan
- Thousands of plugins from CIS/DISA etc

END



Nessus scan Types



Nessus Credentialed scan



Credentialed Scanning

Uses passwords to log into systems

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

My Scans

Import

New Folder

Search Scans



2 Scans

☐	Name	Schedule	Last Modified ▾
☐	Basic Discovery Scan	Weekly on Tue at 3:00 PM	✓ Today at 2:43 PM
☐	Mike's Scan	Daily at 3:00 PM	📅 N/A

Nessus

Scans

Settings

FOLDERS

My Scans

Routine Scans5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Mike's Scan

Back to My Scans

Configure

Hosts0History0

No hosts are available.

Scan Details

Name:

Mike's Scan

Status:

Empty

Scanner:

Local Scanner

Nessus

ScansSettings

FOLDERS

My Scans

Routine Scans5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Mike's Scan / Configuration

[Back to Scan Report](#)

SettingsCredentialedCompliancePlugins

BASIC

GeneralScheduleNotifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

NameMike's Scan

Description

FolderMy Scans

Targets172.30.0.0/24

Upload Targets

Add File

Save

Cancel

5

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Mike's Scan / Configuration

[Back to Scan Report](#)

Settings

Credentials

Compliance

Plugins

CATEGORIES

Host

Filter Credentials



SNMPv3

1

SSH

∞

Windows

∞

Save

Cancel

Nessus

Scans

Settings

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Mike's Scan / Configuration

[Back to Scan Report](#)

Settings

Credentials

Compliance

Plugins

CATEGORIES

Host

Filter Credentials

SNMPv3 1

SSH ∞

Windows ∞

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Mike's Scan / Configuration

[Back to Scan Report](#)

Settings

Credentials

Compliance

Plugins

CATEGORIES

Host

Filter Credentials



SNMPv3

1

SSH

∞

Windows

∞

Windows

Authentication method

Password

Username

vulnerabilityscan

Password

Domain

Global Credential Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication
- ☐ Start the Remote Registry service during the scan
- ☐ Enable administrative shares during the scan

Save

Cancel

Qualys Demo - 1

- Lets take a look at Qualys Demo
- Free Qualys tools:
 - BrowserCheck
 - SSL
- Qualys FreeScan
 - Vulnerability
 - OWASP
 - Patch Tuesday
 - SCAP

Qualys Demo - 1

The screenshot shows the Qualys BrowserCheck website. At the top, the Qualys logo is on the left, and navigation links for 'About', 'FAQ', 'Feedback', 'Qualys.com', and 'Try Coinblocker' are on the right. The main heading is 'Check your browser.' followed by a subtext: 'Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.' Below this, there are two buttons: a green 'Install Plugin' button and a yellow 'Scan without installing plugin' button. A green arrow points from the yellow button to the right. Below the buttons are three columns of information. The first column shows a USB drive icon with the Qualys logo and text: 'Check your browser and system security' and 'Click the "Install Plugin" button to enable fast, safe scanning.' The second column shows icons for various browsers (Safari, Firefox, Chrome) with checkmarks and text: 'Find vulnerabilities at the click of a button' and 'Scan and view all security issues in an easy-to-understand detailed list.' The third column shows a blue 'Fix It' button and text: 'Take charge of any issues found' and 'Follow recommended steps to resolve each vulnerability found.' At the bottom, there is a link: 'Learn more about Qualys BrowserCheck'.

Qualys. BrowserCheck

About FAQ Feedback Qualys.com Try Coinblocker

Check your browser.

Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.

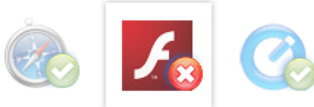
Install Plugin

Scan without installing plugin



Check your browser and system security

Click the "Install Plugin" button to enable fast, safe scanning.



Find vulnerabilities at the click of a button

Scan and view all security issues in an easy-to-understand detailed list.



Take charge of any issues found

Follow recommended steps to resolve each vulnerability found.

[Learn more about Qualys BrowserCheck](#)

<https://www.qualys.com/free-services/>

Qualys® BrowserCheck Summary

Scan start time: **Tue Apr 04 2023, 9:18 AM**

Scan duration: **00:01** (mm:ss)

Congratulations! You passed Qualys BrowserCheck.

We recommend you scan your browser regularly to stay up to date with the latest versions and plugins.

[Re-Scan](#)

INFO: For more comprehensive and automated scans [install Qualys BrowserCheck Plugin](#).



Google Chrome
111.0.0.0

Up To Date

 **Qualys. BrowserCheck**
BUSINESS EDITION


Monitor all your computers and check whether they're staying up-to-date.

Easy, Accurate & FREE!

[Try It Now >](#)



HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.



Test your server »

Test your site's certificate and configuration



Test your browser »

Test your browser's SSL implementation



SSL Pulse »

See how other web sites are doing



Documentation »

Learn how to deploy SSL/TLS correctly

Books



[*Bulletproof SSL and TLS*](#) is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system

administrators, and developers, with the main focus on getting things done. [MORE »](#)

News

[LinkedIn Faux Pas Shines Light on Certificate Management](#)

May 24, 2019

[Zombie POODLE and GOLDENDOODLE Vulnerabilities](#)

April 22, 2019

[PCI & SSL/Early TLS QIDs 38601, 42366](#)

March 14, 2019

About SSL Labs

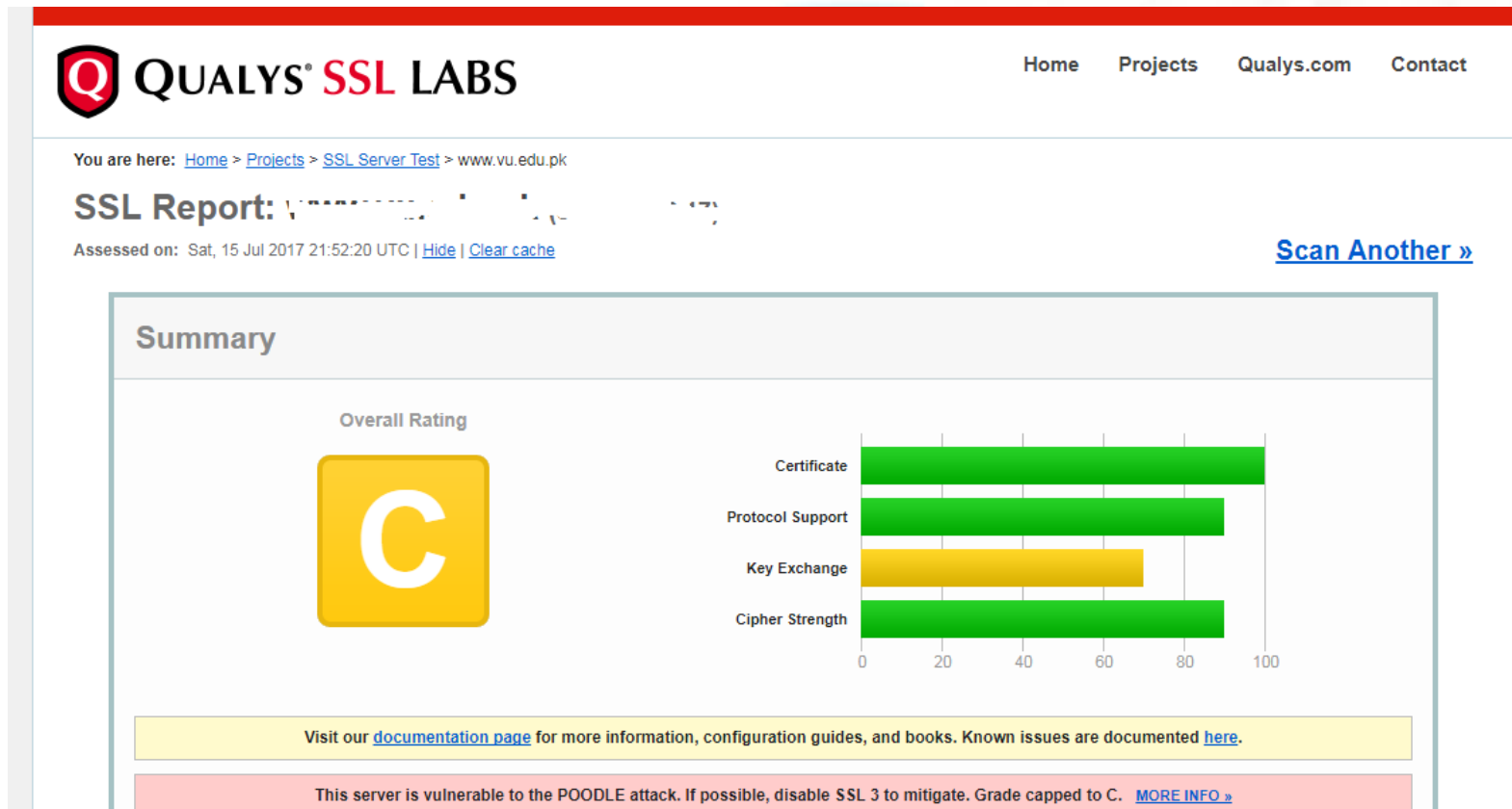
SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristić, Qualys

Qualys Demo - 1

SSL LABS REPORT

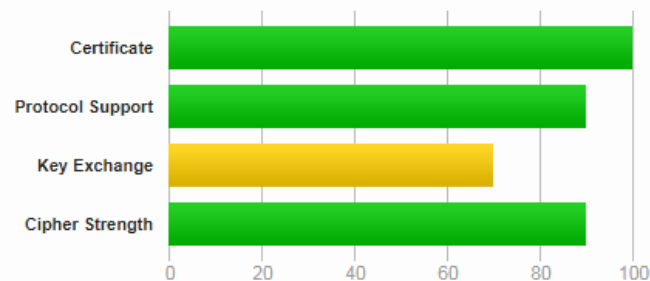


Qualys Demo - 1

SSL LABS REPORT

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)

<https://www.qualys.com/free-services/>
<https://www.ssllabs.com/>

Qualys Demo - 1

PROTOCOL DETAILS

BEAST attack	Not mitigated server-side (more info)	SSL 3: 0xa, TLS 1.0: 0xc014
POODLE (SSLv3)	Vulnerable INSECURE (more info)	SSL 3: 0xa
POODLE (TLS)	No (more info)	
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)	
SSL/TLS compression	No	
RC4	Yes INSECURE (more info)	
Heartbeat (extension)	No	
Heartbleed (vulnerability)	No (more info)	
Ticketbleed (vulnerability)	No (more info)	
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)	
Forward Secrecy	Weak key exchange WEAK	
ALPN	No	

Qualys Demo - 1

QUALYS FREESCAN

New Scan

Scan a URL and receive results on Web Application and Network Vulnerabilities, OWASP Security Risks, and Malware audits. Or, enter an IP address to scan external or internal hosts for Vulnerabilities, authenticated Patch Tuesday audits, or run a SCAP compliance scan.

Choose Scan Type



VULNERABILITY

Network | WAS | MDS Scans



OWASP

Risk Scan



PATCH TUESDAY

Authenticated Scan



SCAP

Compliance Scan

Last Scan Result

OWASP Scan

<http://www.delt...>

Summary: No OWASP Categorie...

16 Jul 2017



Vulnerability Summary

VM(33) WAS(0) MDS(0)



Patch Audit Summary

4 Patches | 4 Vulns Addressed

Last 5 Scan Results

16 Jul 2017 <http://www.deltatechglobal.com>



16 Jul 2017 <http://www.deltatechglobal.com>

[View](#) | [Rescan](#)

16 Jul 2017 <http://www.vu.edu.pk>



Qualys Demo - 1



Welcome Nahil

Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

[Back to Home](#)

[Quick Tour](#) | [Upgrade Now](#) | [Nahil Mahmood](#) | [2 Scans](#)

Scan in Progress

[Cancel scan](#)

<http://www.dalatech.com>

	Vulnerability Scan	
	Web Application Scan	
	Malware Detection	

In progress
In progress
Scan complete

Scan in Progress

[Cancel scan](#)

<http://www.dalatech.com>

	Vulnerability Scan		3 threats
	Web Application Scan		
	Malware Detection		

Scan complete
In progress
Scan complete

OWASP Scan [rename](#)

Summary: No OWASP Categories Found.

Threat Summary: 33 Vulnerabilities Found

Patch Report Summary: 4 Patches Available

<http://www.dalatech.com>
16 July 2017 at 1:25AM (GMT+0500)



[View Report](#)

Qualys Demo - 1

OWASP Scan PATCH REPORT



OWASP Scan [rename](#)
No Authentication Used

16 JULY 2017 at 11:25AM (GMT+0500)

4

Patches
Required

4

Vulnerabilities
Addressed

<http://www.deltatools.com>

www.deltatools.com
Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (4) Microsoft (0) Oracle (0) Adobe (0) Others (4)

Patches

1 - 4 of 4 < >

OpenSSH LoginGraceTime Denial of Service Vulnerability	1
OpenSSH Commands Information Disclosure Vulnerability	1
OpenSSH J-PAKE Session Key Retrieval Vulnerability	1
OpenSSH "X SECURITY" Bypass Vulnerability	1

OpenSSH LoginGraceTime Denial of Service Vulnerability

QID: 42413 Published: 09 February 2013

Vendor ID: [OpenSSH](#)

CVE: [CVE-2010-5107](#)

Solution:

Customers are advised to upgrade to [OpenSSH 6.2](#) and apply the associated server configuration settings to remediate this vulnerability.

1 Vulnerabilities Addressed

QID: 42413 Published: 09 February 2013

OpenSSH LoginGraceTime Denial of Service Vulnerability



Qualys Demo - 1

THREAT REPORT

View by:

OWASP Report

Patch Report

Threat Report

Print Report ▼



OWASP Scan [rename](#)

External Host Vulnerability Report

16 July 2017 at 1:25AM (GMT+0500)

33

Vulnerabilities
Detected

0

HIGH
Risk

10

MED
Risk

23

LOW
Risk

78

INFO
Gathered

<http://www.deltatechglobal.com>

www.deltatechglobal.com

Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID

All Scan Results

1 - 25 of 111

Mail Server Accepts Plaintext Credentials	
Discovery of Unix Account Names Vulnerability	
Web Server Stopped Responding	
Discovery of Unix Account Names Vulnerability	
POP3 Server Allows Plain Text Authentication Vulnerability	

Mail Server Accepts Plaintext Credentials

QID: 74147

CVE Base: 5.3

Port: 587

CVSS Temporal: 4.8

Category: Mail
services

CVE ID: -

Threat:

Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to

Qualys Demo - 1

THREAT REPORT

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID



All Scan Results

1 - 10 of 10

Mail Server Accepts Plaintext Credentials	
Discovery of Unix Account Names Vulnerability	
Web Server Stopped Responding	
Discovery of Unix Account Names Vulnerability	
POP3 Server Allows Plain Text Authentication Vulnerability	
OpenSSH J-PAKE Session Key Retrieval Vulnerability	
OpenSSH LoginGraceTime Denial of Service Vulnerability	
OpenSSH Commands Information Disclosure Vulnerability	
OpenSSH "X SECURITY" Bypass Vulnerability	
Apache Partial HTTP Request Denial of Service Vulnerability	

Discovery of Unix Account Names Vulnerability

QID: 5001

CVE Base: 3.3

Port: 80



CVSS Temporal: 3

Category: Brute Force Attack

CVE ID: [CVE-2001-1013](#)

Threat:

When a request for a user is made (<http://your.host/~user>), certain servers (such as Apache Versions 1.3.12 and 1.3.9) return a different reply depending on whether the account user exists on the host or not.

If a request is made for an account that exists on the host, a 403 error is returned. If a request is made for a non-existent account, then a 404 error is returned.

Impact:

Unauthorized remote users can implement brute force attacks on the Web server to guess a valid account name on the server. Even though they may be successful in obtaining a valid account, they will still have to guess the password. However, if user passwords are weak, some services may also be brute forced.

Solution:

Disable the default-enabled "UserDir" directive. To do so, add the following line to the httpd.conf file:

UserDir Disabled

Qualys Demo - 1

- Qualys is a powerful cloud-based vulnerability management tool
- Several online free tools
- Advanced web application security testing

END

QUALYS DEMO - PART 3

- Lets have a look at some further features of Qualys:
- Qualys Continuous Monitoring

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3

Ruleset BuilderLaunch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

WEBSITE CHANGES

Description

DETECT CHANGES TO WEBSITE

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types


Host


Vulnerability


Certificate


Port / Service


Software


Ticket

Drag rules here to add them to the ruleset



RULESET BUILDER

QUALYS DEMO - PART 3

Ruleset BuilderLaunch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

Description

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types


Host


Vulnerability


Certificate


Port / Service


Software


Ticket

Rule 1: New or Fixed or Active or Reopened VulnerabilityRemove

Your selection may result in excessive alerts. Select more filters to get fewer alerts.

When a vulnerability is* ☒ New ☒ Fixed ☒ Active ☒ Reopened

 Add Criteria

Rule 2: New or Expired or Expiring CertificateRemove

When a certificate is* ☒ New ☒ Expired ☐ Expiring in 10 days ☒ Expiring in 30 days ☒ Expiring in 90 days

 Add Criteria

Rule 3: Opened or Changed or Closed Port / ServiceRemove

When a port/service is* ☒ Opened ☒ Changed ☒ Closed

 Add Criteria

RULETYPES & CONFIGURATION

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Help ▾ Nahil Mahmood ▾ Log out

Alerts Configuration

74 days remaining in trial. [Upgrade Now](#)

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ [New Ruleset](#)

2 rulesets ⚙ ▾

☐	Title	# Profiles	Created by	Created on
☐	WEBSITE CHANGES DETECT CHANGES TO WEBSITE	0	detat-nm1	20 Sep 2018 10:56PM GMT+0500
☐	Initial Ruleset (System) With the Initial Ruleset you will receive alerts when a new host is found, a port is open, or an SSL certificate is expired or is about to expire. Use this ruleset as is or save a copy of it to make changes.	0	System	19 May 2018 7:38PM GMT+0500

RULESETS INTERFACE

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE