

Vulnerability Scanning with Nessus

[Nessus](#) is a vulnerability scanner from Tenable. Nessus can be deployed on most system, including Raspberry Pi for portability. Can be downloaded form here, but does require you to make an account to receive a license. On the free account you can scan up to 16 IPs.

So typically when using it for your own environment you want to use the same machines OR set different machines to same IPs you had previously scanned.

Download it from [here](#)

OR on Linux:

```
nessus_amd64_file=$(curl https://www.tenable.com/downloads/nessus\?loginAttempted\=true | grep -o -m1 -E "Nessus-[0-9]{1,2}.[0-9]{1}.[0-9]{1}-debian10_amd64.deb" | grep -m1 -i ".deb")

nessus_amd64="https://www.tenable.com/downloads/api/v2/pages/nessus/files/$nessus_amd64_file"

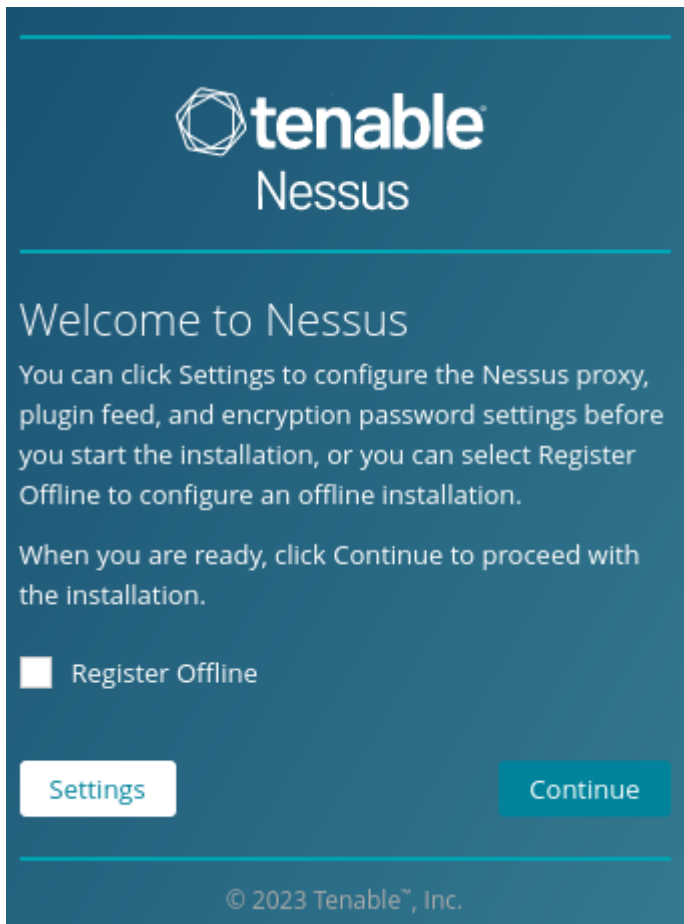
sudo wget -q $nessus_amd64 -O /tmp/nessus_amd64.deb
sudo dpkg -i /tmp/nessus_amd64.deb
sudo rm -f /tmp/nessus_amd64.deb
```

Upon first run, it will initialize and install plugins so it may take a while.

Starting / Stopping Nessus

- Start: `sudo /bin/systemctl start nessusd.service`
- Stop: `sudo /bin/systemctl stop nessusd.service`

- Go to: <https://localhost:8834/>



The image shows the Tenable Nessus Welcome screen. At the top is the Tenable Nessus logo. Below it, the text "Welcome to Nessus" is displayed. A paragraph explains that users can click "Settings" to configure the Nessus proxy, plugin feed, and encryption password settings before starting the installation, or select "Register Offline" to configure an offline installation. Another paragraph states that when ready, users should click "Continue" to proceed with the installation. At the bottom, there is a checkbox labeled "Register Offline" and two buttons: "Settings" and "Continue". The footer shows the copyright notice "© 2023 Tenable™, Inc."

tenable
Nessus

Welcome to Nessus

You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

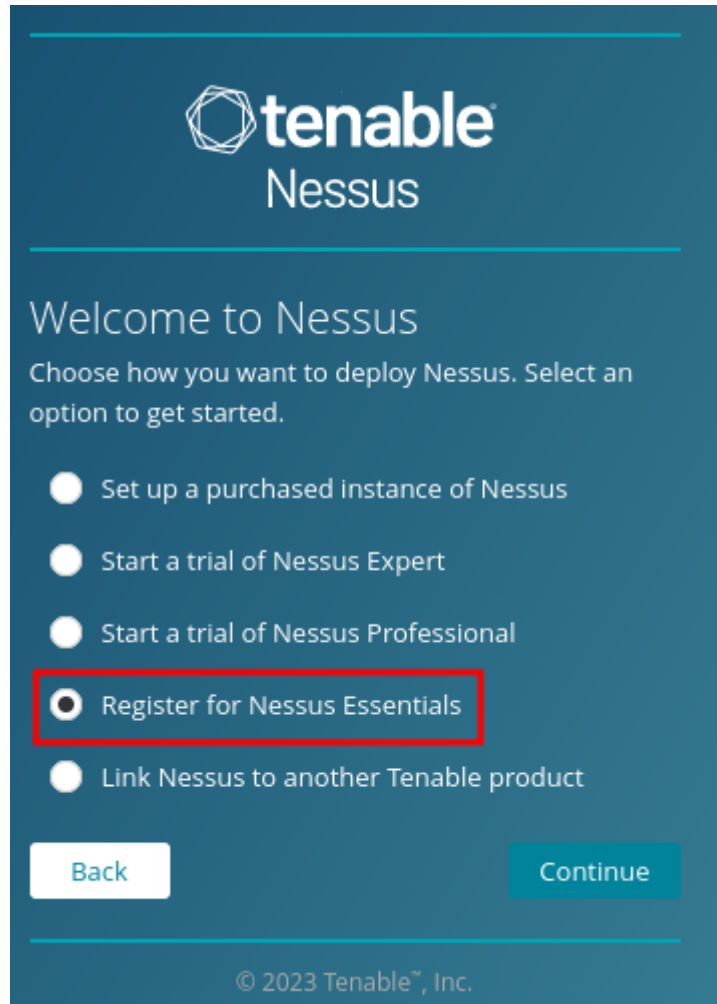
When you are ready, click Continue to proceed with the installation.

☐ Register Offline

[Settings](#) [Continue](#)

© 2023 Tenable™, Inc.

Select the "Register for Nessus Essentials"



The image shows the Tenable Nessus Welcome screen with deployment options. At the top is the Tenable Nessus logo. Below it, the text "Welcome to Nessus" is displayed. A paragraph asks the user to choose how they want to deploy Nessus and select an option to get started. There are five radio button options: "Set up a purchased instance of Nessus", "Start a trial of Nessus Expert", "Start a trial of Nessus Professional", "Register for Nessus Essentials" (which is selected and highlighted with a red box), and "Link Nessus to another Tenable product". At the bottom, there are two buttons: "Back" and "Continue". The footer shows the copyright notice "© 2023 Tenable™, Inc."

tenable
Nessus

Welcome to Nessus

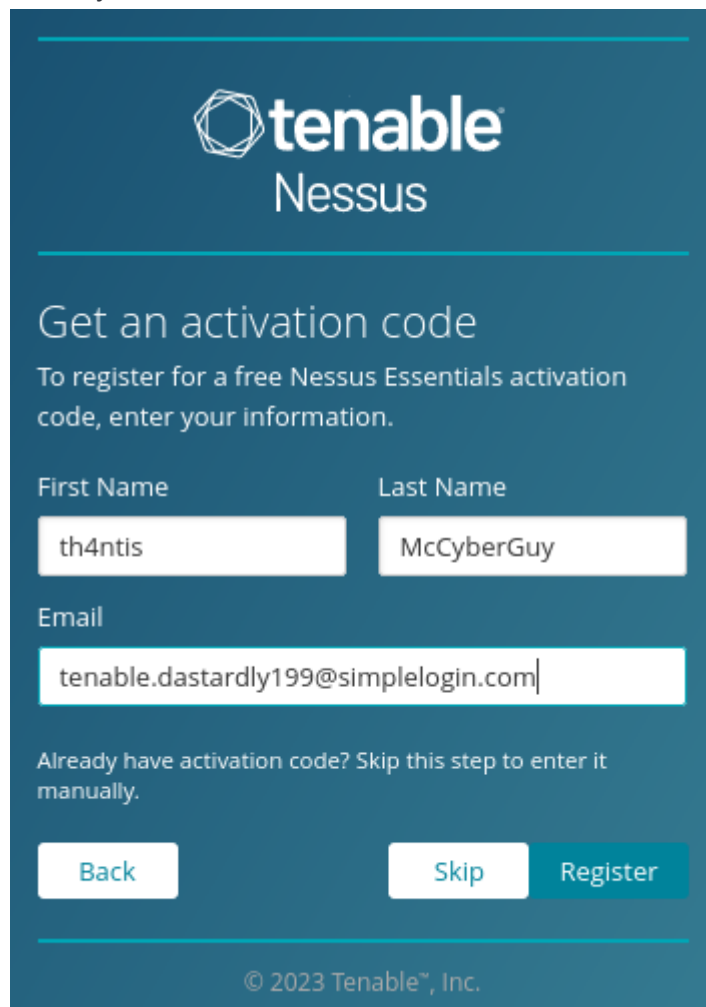
Choose how you want to deploy Nessus. Select an option to get started.

- ☐ Set up a purchased instance of Nessus
- ☐ Start a trial of Nessus Expert
- ☐ Start a trial of Nessus Professional
- ☒ Register for Nessus Essentials
- ☐ Link Nessus to another Tenable product

[Back](#) [Continue](#)

© 2023 Tenable™, Inc.

Put in your name and email for them to send the license to, OR it will show up on the next screen.



The image shows the Tenable Nessus registration form. At the top is the Tenable Nessus logo. Below it, the text "Get an activation code" is followed by "To register for a free Nessus Essentials activation code, enter your information." There are three input fields: "First Name" with the value "th4ntis", "Last Name" with the value "McCyberGuy", and "Email" with the value "tenable.dastardly199@simplelogin.com". Below these fields is a link "Already have activation code? Skip this step to enter it manually." At the bottom are three buttons: "Back", "Skip", and "Register". The footer says "© 2023 Tenable™, Inc."

tenable
Nessus

Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

First Name Last Name

th4ntis McCyberGuy

Email

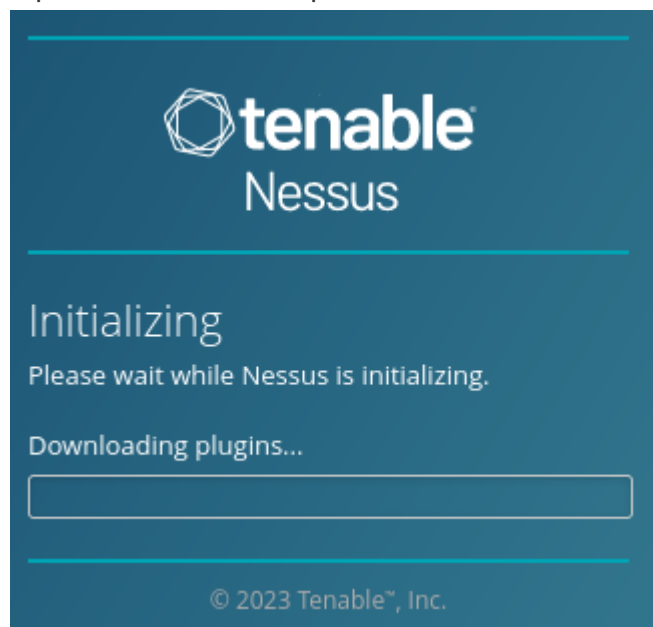
tenable.dastardly199@simplelogin.com

Already have activation code? Skip this step to enter it manually.

Back Skip Register

© 2023 Tenable™, Inc.

Input a username and password and let it do it's thing.



The image shows the Tenable Nessus "Initializing" screen. It features the Tenable Nessus logo at the top. Below the logo, the text "Initializing" is followed by "Please wait while Nessus is initializing." and "Downloading plugins...". There is a progress bar below the text. The footer says "© 2023 Tenable™, Inc."

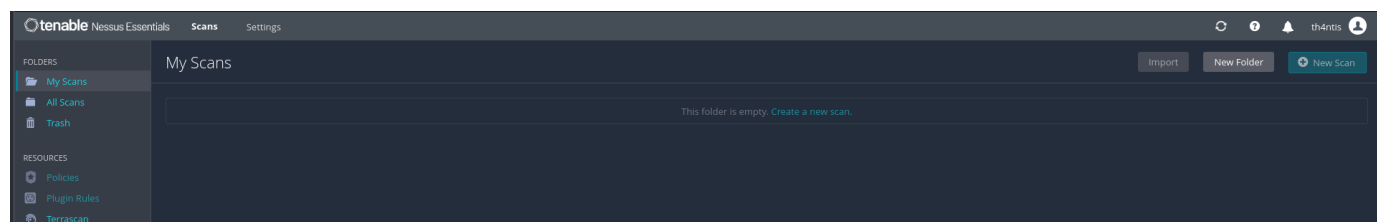
tenable
Nessus

Initializing

Please wait while Nessus is initializing.

Downloading plugins...

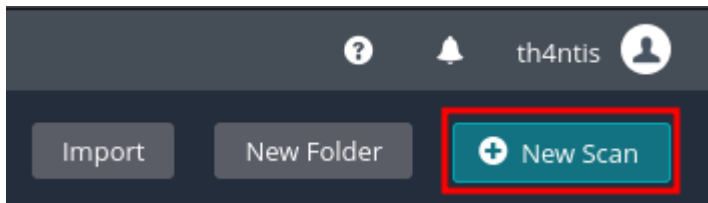
© 2023 Tenable™, Inc.



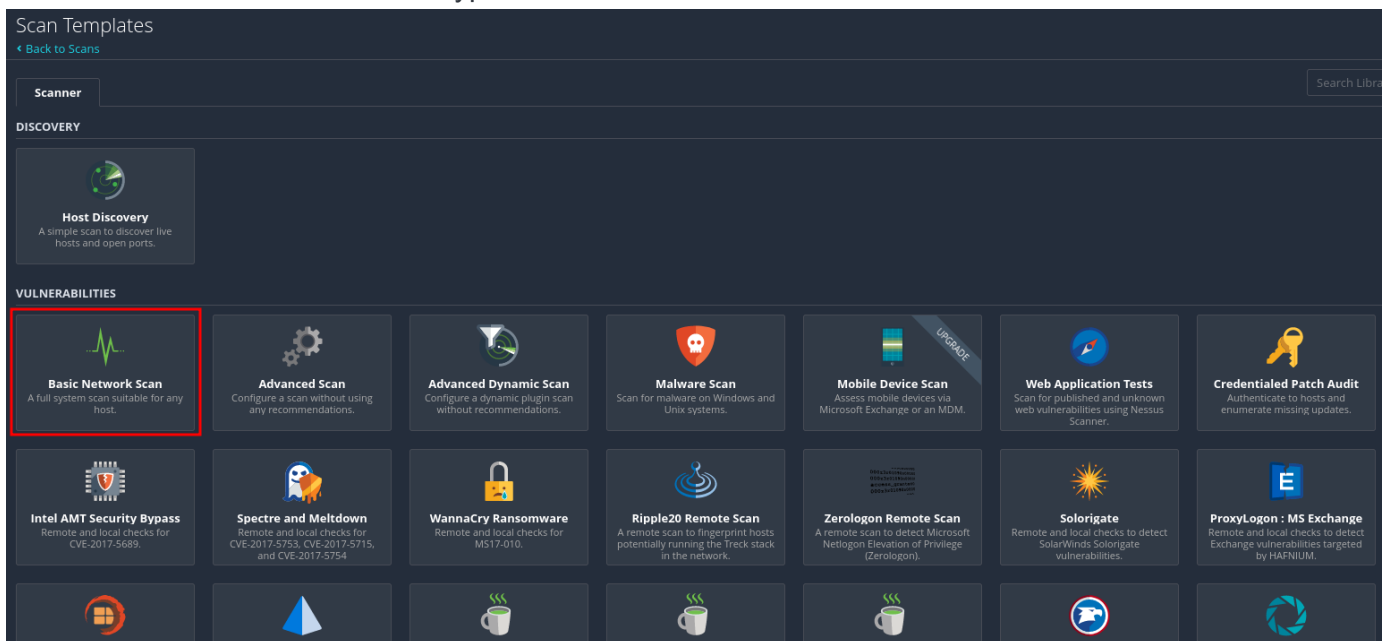
Scanning

Since this is the free edition, we can only scan 16 private IP addresses. We will scan our Kioptrix machine.

Click "New Scan" in the top right



We will see a list of various scan types we can do. We will do a Basic Network Scan



My Kioptrix machine was 192.168.48.129

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

Kioptrix

Description

Folder

My Scans

Targets

192.168.48.129

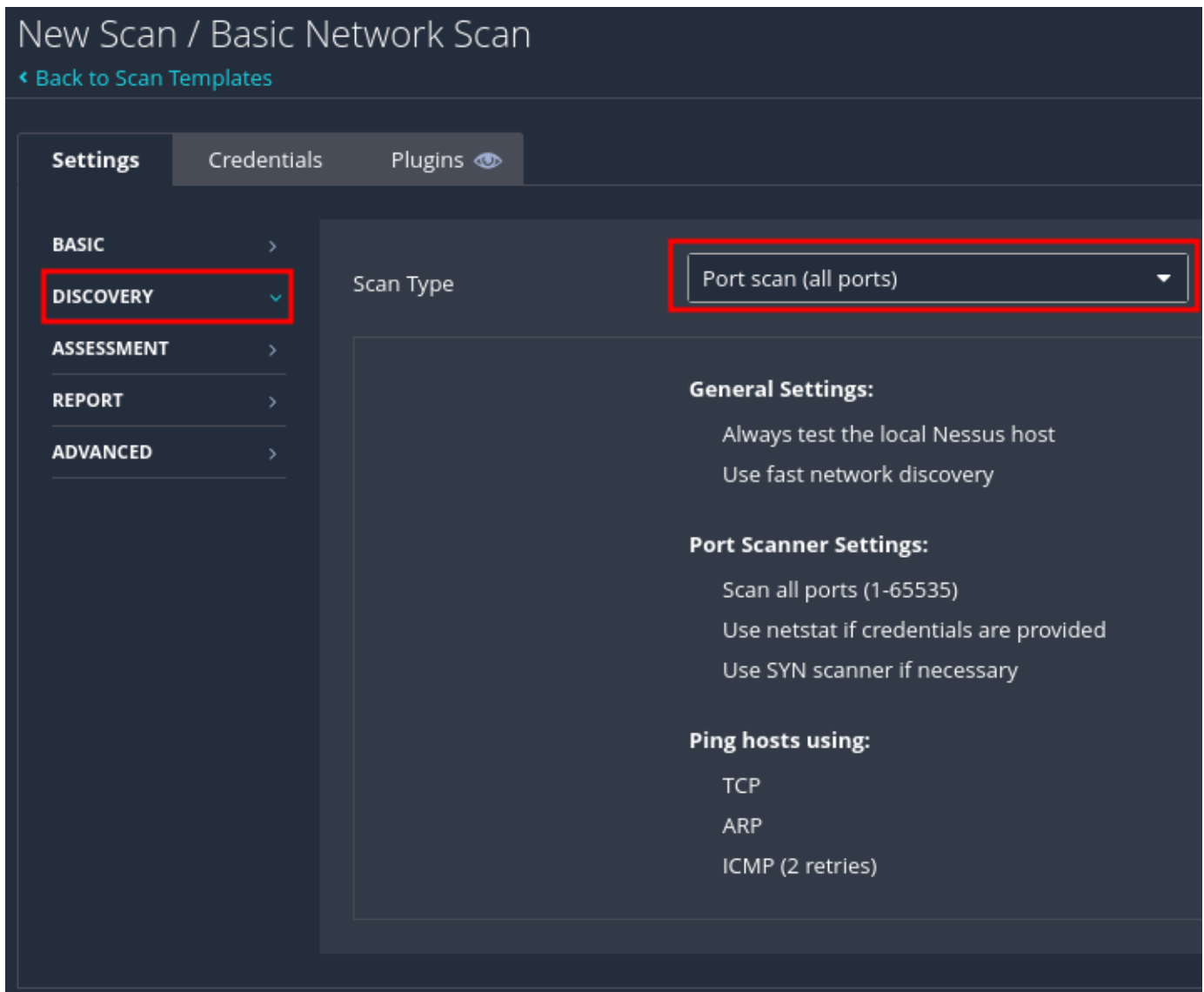
Upload Targets

[Add File](#)

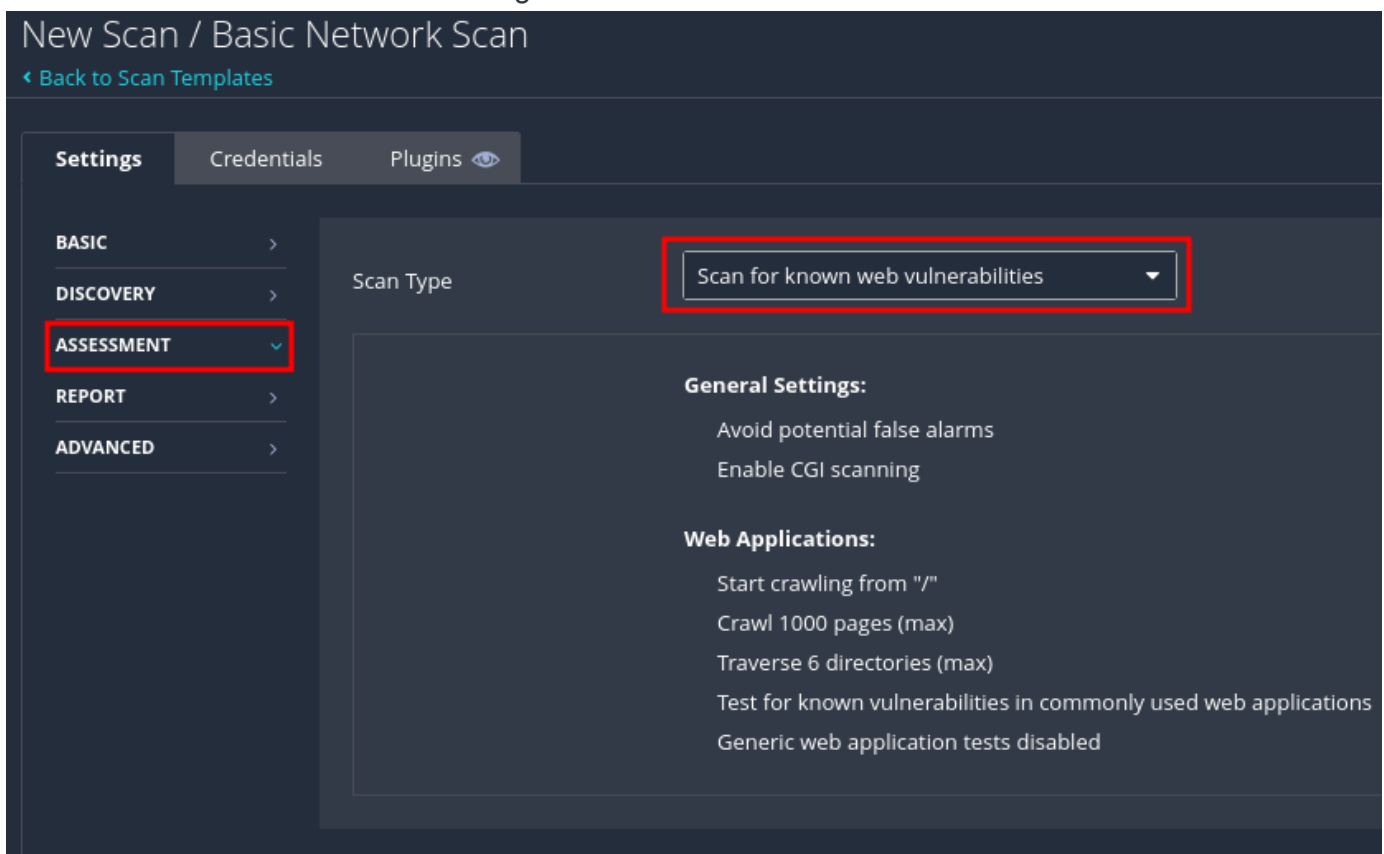
Save

Cancel

We have the ability to schedule the scan if we want for a time, occurrence, etc.. Important to note, under "Discovery", it's default to common ports, This, for this instance, will be all ports.



Under "Assessment" we will also change it to "Scan for Known Web Vulnerabilities"



Name	Schedule	Last Scanned
Kloptrix	On Demand	N/A

Kioptrix

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

[Back to Kioptrix](#)

Hosts 1

Vulnerabilities 46

Remediations 3

History 1

Filter

Search Hosts

1 Host

Host	Vulnerabilities
192.168.48.129	<div> <div>24</div> <div>33</div> <div>59</div> <div>14</div> <div>74</div> </div>

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:04 AM

End: Today at 5:21 AM

Elapsed: 18 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Kioptrix

[Back to Kioptrix](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1Vulnerabilities46Remediations3History1

FilterSearch Vulnerabilities46 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	1	
MIXED	OpenSSL (Multiple Issues)	Web Servers	50	
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	20	
CRITICAL	Apache Httpd (Multiple Issues)	Web Servers	12	
MIXED	Openbsd Openssh (Multiple Issues)	Gain a shell remotely	5	
HIGH	7.5 *	5.5	mod_ssl_ssl_util_uencode_binary Remote Overflow	Web Servers	2	
MIXED	Openbsd Openssh (Multiple Issues)	Misc.	15	
MIXED	SSL (Multiple Issues)	General	14	
MIXED	IETF Md5 (Multiple Issues)	General	2	
MIXED	Openbsd Openssh (Multiple Issues)	Denial of Service	2	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:04 AM
End: Today at 5:21 AM
Elapsed: 18 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Kioptrix / Plugin #12255

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities46

Remediations3

History1

HIGH

mod_ssl_ssl_util_uuencode_binary Remote Overflow

<>

Plugin Details

Description

The remote host is using a version of mod_ssl that is older than 2.8.18.

This version is vulnerable to a flaw that could allow an attacker to disable the remote website remotely, or to execute arbitrary code on the remote host.

Note that several Linux distributions patched the old version of this module. Therefore, this alert might be a false-positive. Please check with your vendor to determine if you really are vulnerable to this flaw.

Solution

Upgrade to version 2.8.18 (Apache 1.3) or to Apache 2.0.50.

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	192.168.48.129
80 / tcp / www	192.168.48.129

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 730 days +

Product Coverage: Medium

CVSSv3 Impact Score: 5.5

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.5

Risk Factor: High

CWE: v3.0 Base Score: 7.5