TryHackMe | OpenVAS

tryhackme.com/room/openvas

7%

OpenVAS, an application used to scan endpoints and web applications to identify and detect vulnerabilities. It is commonly used by corporations as part of their mitigation solutions to quickly identify any gaps in their production or even development servers or applications. This is not an end all be all solution but can help to get rid of any common vulnerabilities that may have slipped through the cracks.

From the OpenVAS GitHub repository "This is the Open Vulnerability Assessment Scanner (OpenVAS) of the Greenbone Vulnerability Management (GVM) Solution. It is used for the Greenbone Security Manager appliances and is a full-featured scan engine that executes a continuously updated and extended feed of Network Vulnerability Tests (NVTs)."

Answer the questions below

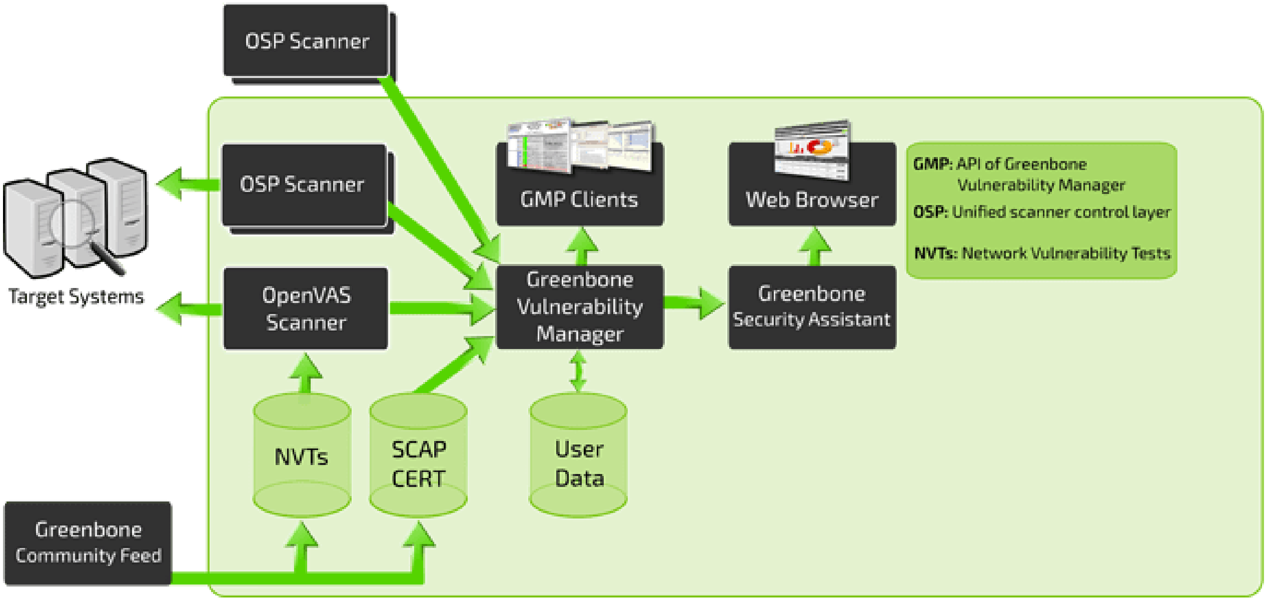
Read the introduction

As previously mentioned OpenVAS is built off the GreenBone Vulnerability Management (GVM) solution and is only one of the appliances that is released from GreenBone.

Greenbone

Sustainable Resilience

OpenVAS is a service within a larger framework of services known as Greenbone Vulnerability Management (GVM). In this task we will break down the services that make up the framework and their roles.


OSP Scanner
OSP Scanner
GMP Clients
Web Browser
GMP: API of Greenbone Vulnerability Manager
OSP: Unified scanner control layer
NVTs: Network Vulnerability Tests
Target Systems
OpenVAS Scanner
Greenbone Vulnerability Manager
Greenbone Security Assistant
NVTs
SCAP CERT
User Data
Greenbone Community Feed

Above is a brief visual breakdown of what the GVM framework looks like. There are many components that are apart of the architecture for the GVM framework, but we can break it down into three distinct sections: Front-End, Back-End, and Vulnerability/Information feed. These sections are further explained below.

Vulnerability/Information Feed (NVT, SCAP CERT, User Data, Community Feed)

This section will contain all information and vulnerability tests that come from the Greenbone Community Feed that will be the main baseline for testing against systems. This can also include User Data provided by the user in place of Greenbone NVTs and SCAP CERTs.

Back-End (OSP, OpenVAS, Targets)

The back-end infrastructure is what will be actually conducting all of the vulnerability scanning and processing data and NVTS through OpenVAS and GVM. Greenbone Vulnerability Manager will be the middle man between the scanners and the front-end user interfaces.

Front-End (GSA, Web Interfaces)

This is what you interact with when you navigate to OpenVAS in your browser. The web interfaces are built off of the Greenbone Security Assistant and make life easier for an analyst or operator when working with OpenVAS or other forms of scanners through the GVM.

For more information about the GVM framework architecture check out this forum post https://community.greenbone.net/t/about-gvm-10-architecture/1231.

Answer the questions below

Read about GVM architecture and move on to setting up OpenVAS

Note: OpenVAS is not meant to be installed on the AttackBox.

The installation procedure for OpenVAS can vary based on how you decide to install. You can install from Kali/OpenVAS repos, install from source, or run from a docker container. For our purposes, the preferred method is to run it inside a docker container as we don't have to worry about a lot of the setup or errors that we may run into with other installation methods.

Option 1: Install from Kali/OpenVAS repositories

Installing from repositories can sometimes be very simple or it can be a very painful process. For OpenVAS, the installation ranges in difficulty and can require many configurations ran. For more information about this option check out the guides below.

https://websiteforstudents.com/how-to-install-and-configure-openvas-on-ubuntu-18-04-16-04/

https://www.agix.com.au/installing-openvas-on-kali-in-2020/

Option 2: Install from Source

Installing from source is the least preferred option for beginners and the least optimized way of installing OpenVAS due to prerequisites and make errors. For more information about installing from source look at the INSTALL.MD.

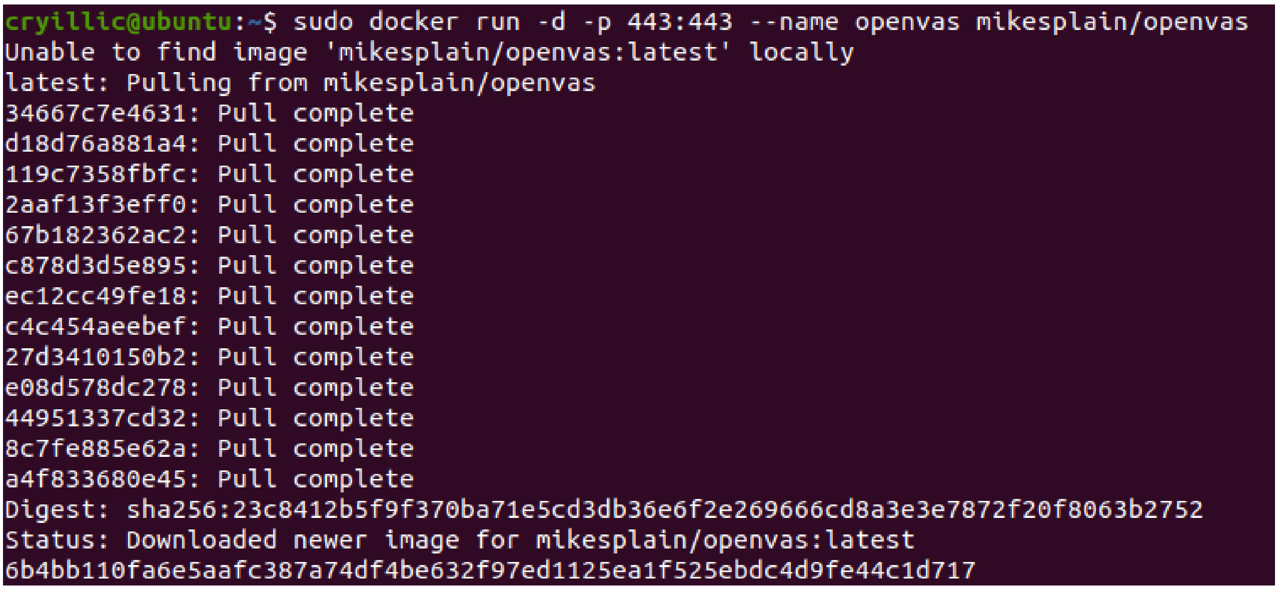
Option 3: Run from Docker (Preferred)

Docker is by far the easiest of all three installation methods and only requires one command to be run to get the client started. For this installation procedure, you will need docker installed.

For more information about this information procedure checkout the openvas-docker project on GitHub and DockerHub.

1. `apt install docker.io`

2. `docker run -d -p 443:443 --name openvas mikesplain/openvas`



```
cryillic@ubuntu:~$ sudo docker run -d -p 443:443 --name openvas mikesplain/openvas
Unable to find image 'mikesplain/openvas:latest' locally
latest: Pulling from mikesplain/openvas
34667c7e4631: Pull complete
d18d76a881a4: Pull complete
119c7358fbfc: Pull complete
2aaf13f3eff0: Pull complete
67b182362ac2: Pull complete
c878d3d5e895: Pull complete
ec12cc49fe18: Pull complete
c4c454aeebef: Pull complete
27d3410150b2: Pull complete
e08d578dc278: Pull complete
44951337cd32: Pull complete
8c7fe885e62a: Pull complete
a4f833680e45: Pull complete
Digest: sha256:23c8412b5f9f370ba71e5cd3db36e6f2e269666cd8a3e3e7872f20f8063b2752
Status: Downloaded newer image for mikesplain/openvas:latest
6b4bb110fa6e5aafc387a74df4be632f97ed1125ea1f525ebdc4d9fe44c1d717
```

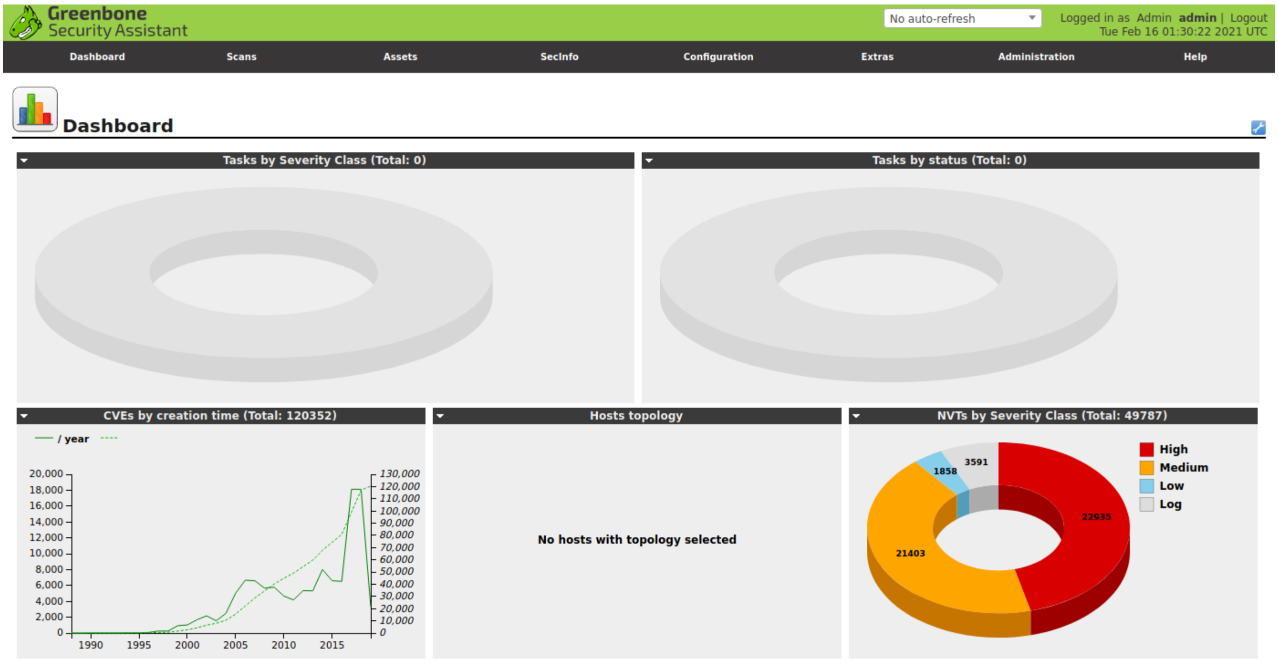
This command will both pull the docker container and then run the container. It may take a few minutes for the container to fully set up and begin running. Once it is complete you can then navigate to https://127.0.0.1 in your preferred browser and OpenVAS will be setup and ready to go!

Below are the default credentials to access OpenVAS/GVM:

Username: `admin`

Password: `admin`

If you successfully logged into OpenVAS you should see a dashboard that looks similar to the one below.



Logged in as Admin admin | Logout
Tue Feb 16 01:30:22 2021 UTC

Dashboard

Tasks by Severity Class (Total: 0)

Tasks by status (Total: 0)

CVEs by creation time (Total: 120352)

Hosts topology

No hosts with topology selected

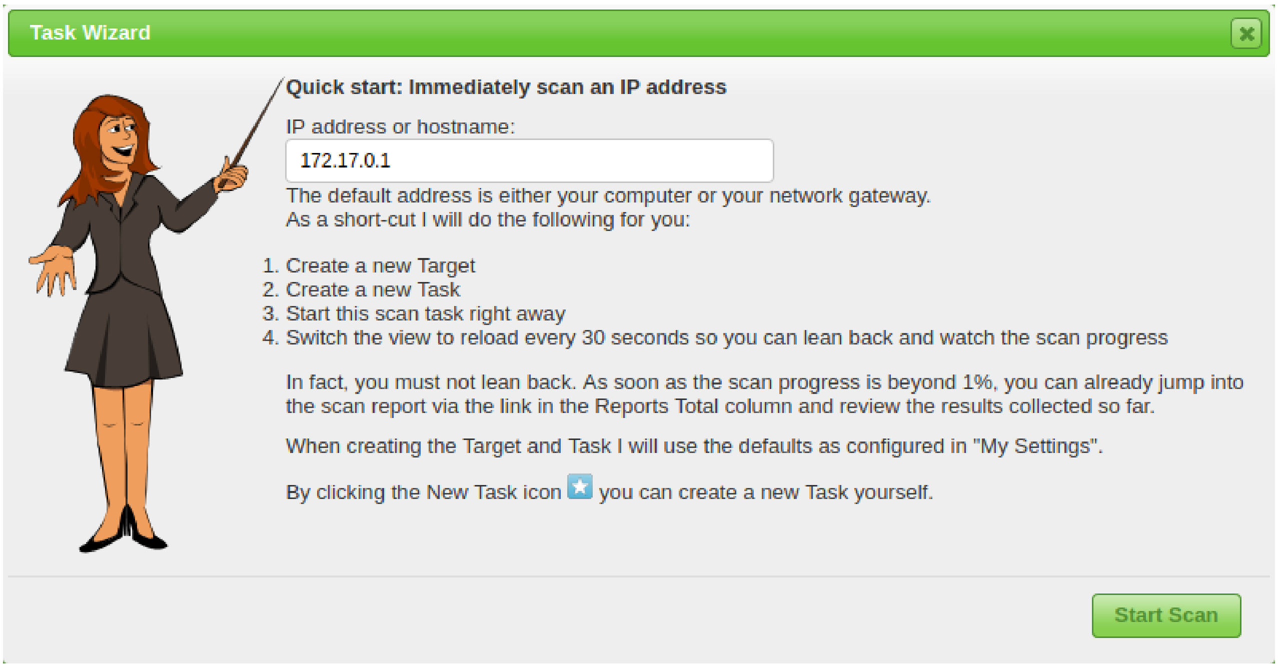
NVTs by Severity Class (Total: 49787)

Answer the questions below

Read the above and prepare your environment.

Before we can start scanning and implementing OpenVAS into our vulnerability management solution we need to do a little bit of maintenance and configuration to get OpenVAS properly working. Luckily for us, OpenVAS makes the process very easy and includes a wizard to make the process straightforward.

Begin by navigating to *Scans* > *Tasks* and clicking on the purple magic wand icon to begin the basic configuration wizard. We recommend beginning a scan on `127.0.0.1` to test out your installation and ensure it is working properly.



Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 172.17.0.1

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

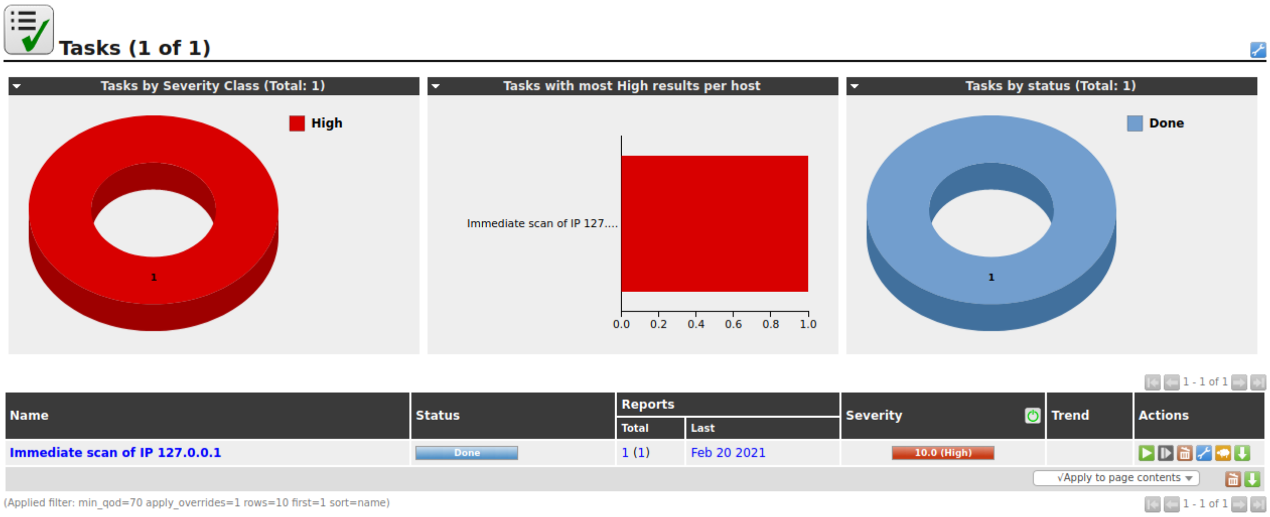
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon ✩ you can create a new Task yourself.

If you successfully navigated to the wizard you should see a pop-up similar to the one above. This is where you will set up your initial scan against your localhost to ensure everything is properly configured.

The scan may take a while to complete, allow OpenVAS enough time to finish the scan, and then you will be met with a new dashboard for monitoring and analyzing your complete and ongoing scans like the one below.


Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High results per host
Immediate scan of IP 127....
0.0
0.2
0.4
0.6
0.8
1.0
Tasks by status (Total: 1)
Done
1
1 - 1 of 1

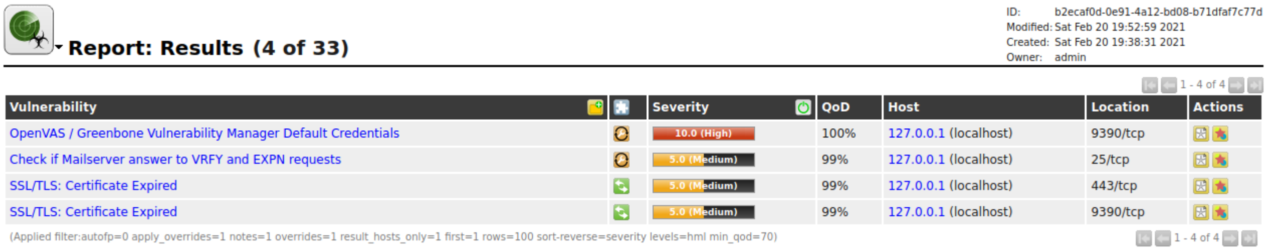
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 127.0.0.1	Done	1 (1)	Feb 20 2021	10.0 (High)		

√Apply to page contents

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

1 - 1 of 1

Once your scan has finished you can navigate to *Scans* > *Reports* and click on your newly created report from your previous task.



ID: b2ecaf0d-0e91-4a12-bd08-b71dfaf7c77d
Modified: Sat Feb 20 19:52:59 2021
Created: Sat Feb 20 19:38:31 2021
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
OpenVAS / Greenbone Vulnerability Manager Default Credentials		10.0 (High)	100%	127.0.0.1 (localhost)	9390/tcp	
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99%	127.0.0.1 (localhost)	25/tcp	
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	127.0.0.1 (localhost)	443/tcp	
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	127.0.0.1 (localhost)	9390/tcp	

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

1 - 4 of 4

If correctly configured you should see three different vulnerabilities reported all originating from OpenVAS itself. This is normal behavior and can be configured/changed to maintain your OpSec.

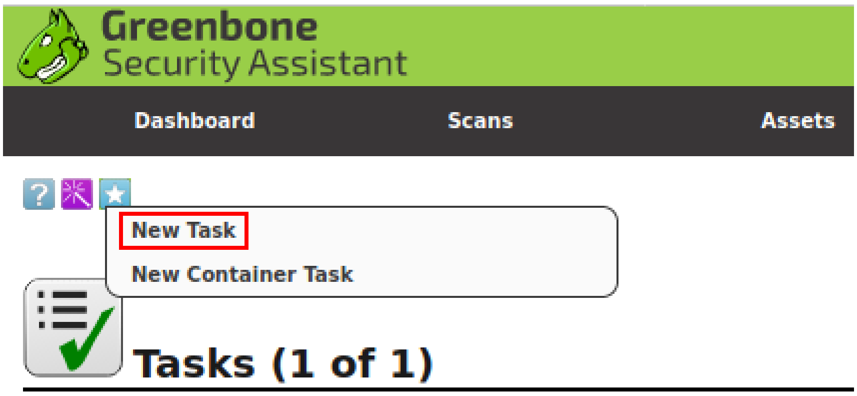
Answer the questions below

Read the above and complete your first scan!

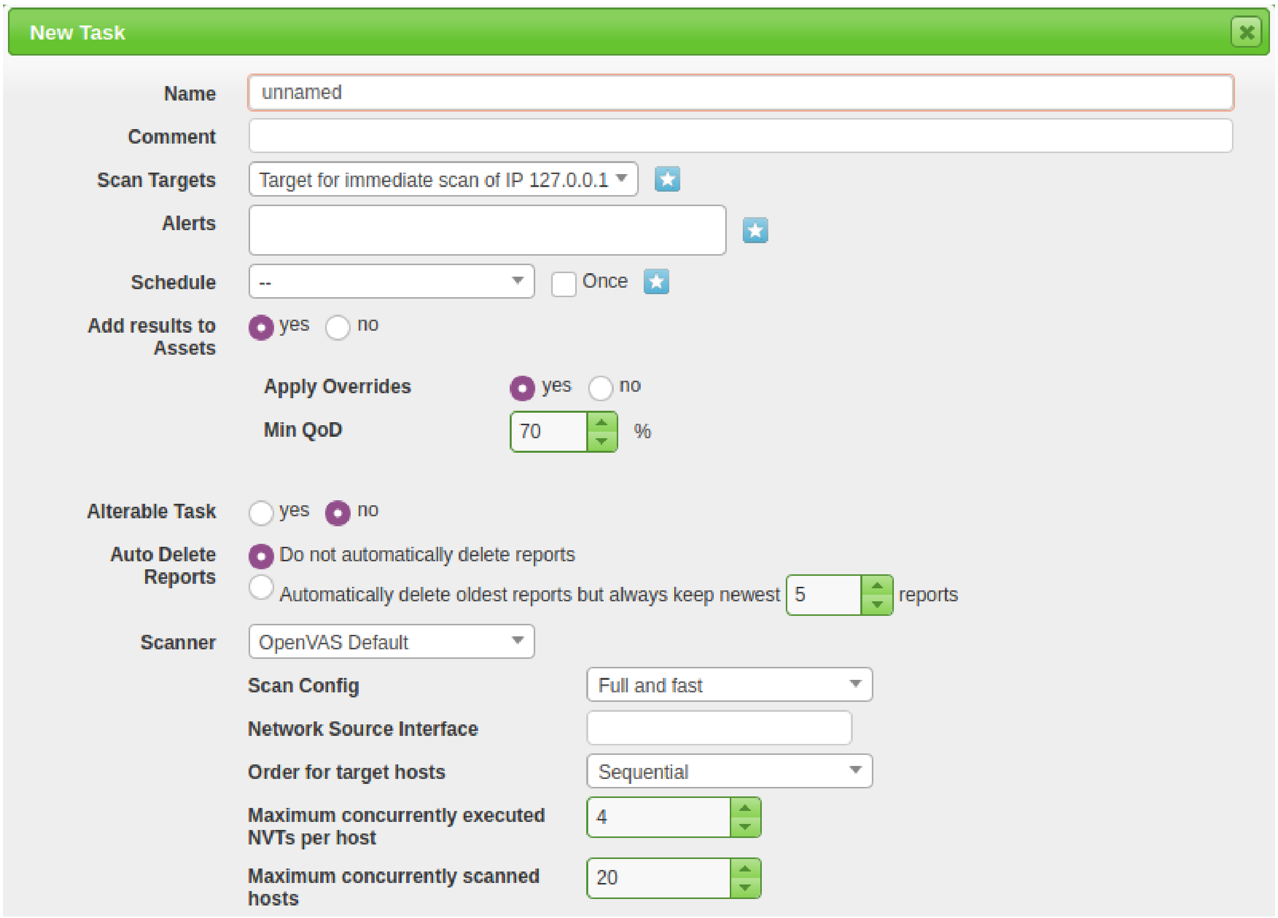
Now that we know that everything is working we can get into the nitty-gritty of OpenVAS and how it works. Deploy the machine and navigate to *Scans* > *Tasks* to begin creating a task to scan the provided machine.

Creating a Task

To create a configurable task navigate to the star icon in the upper right-hand corner of the *Tasks* dashboard and select *New Task*.



Once you select New Task from the dropdown you will be met with a large pop-up with many options. We will break down each of the options sections and what they can be used for.



New Task

Name	unnamed
Comment	
Scan Targets	Target for immediate scan of IP 127.0.0.1
Alerts	
Schedule	-- □ Once
Add results to Assets	● yes ○ no
Apply Overrides	● yes ○ no
Min QoD	70 %
Alterable Task	○ yes ● no
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default
Scan Config	Full and fast
Network Source Interface	
Order for target hosts	Sequential
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

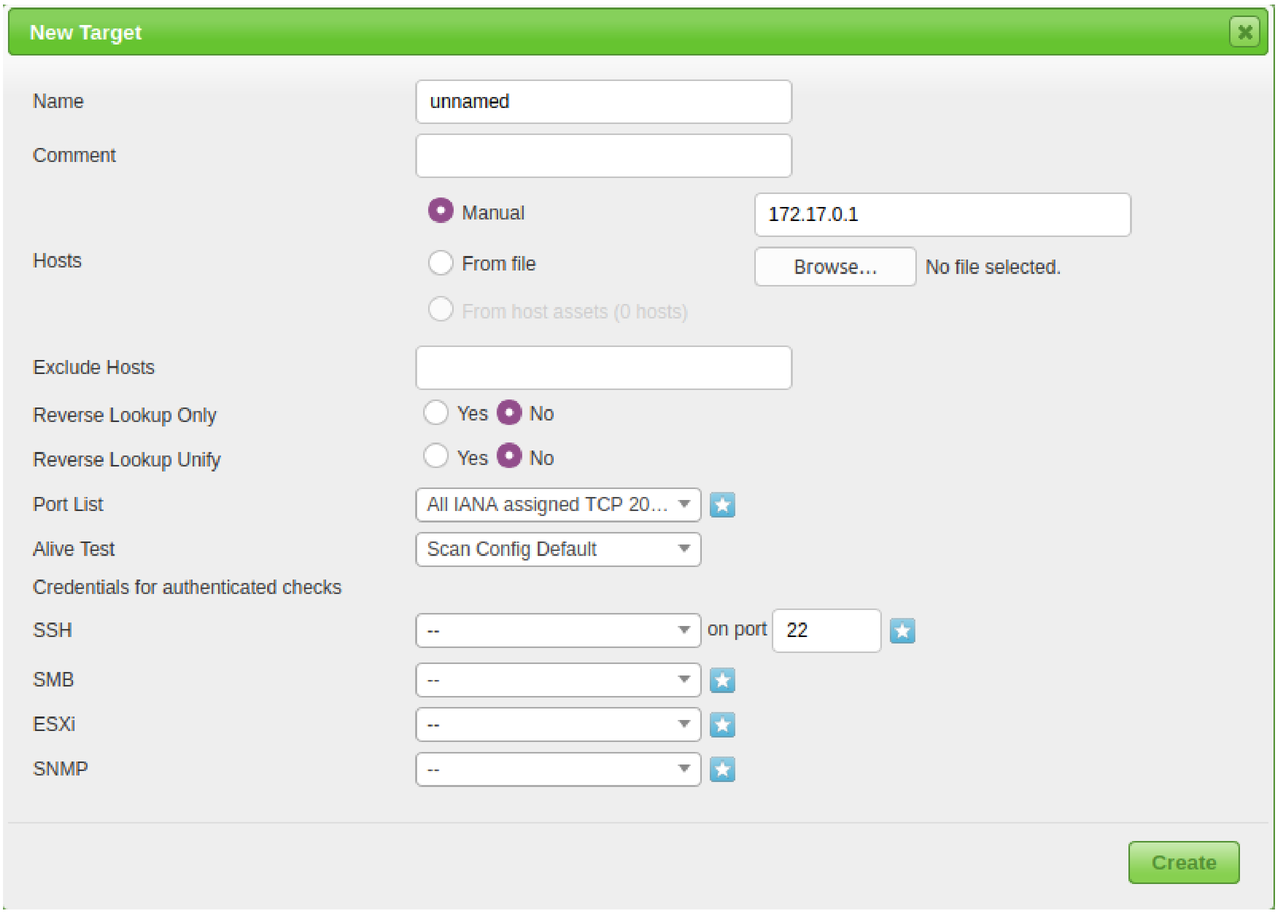
For this task, we will be focusing only on the Name, Scan Targets, and Scanner Type, and Scan Config. In later tasks, we will be focusing on the other options for more advanced configuration and implementation/automation.

1. Name: Allows us to set the name the scan will be known as inside of OpenVAS
2. Scan Targets: The targets to scan, can include Hosts, Ports, and Credentials. To create a new target you will need to follow another pop-up, this will be covered later in this task.

3. Scanner: The scanner to use by default will use the OpenVAS architecture however you can set this to any scanner of your choosing in the settings menu.
4. Scan Config: OpenVAS has seven different scan types you can select from and will be used based on how you aggressive or what information you want to collect from your scan.

Scoping a New Target

To scope a new target, navigate to the star icon next to *Scan Targets*.



New Target

Name: unnamed

Comment:

Hosts: ● Manual 172.17.0.1
○ From file Browse... No file selected.
○ From host assets (0 hosts)

Exclude Hosts:

Reverse Lookup Only: ○ Yes ● No

Reverse Lookup Unify: ○ Yes ● No

Port List: All IANA assigned TCP 20...

Alive Test: Scan Config Default

Credentials for authenticated checks

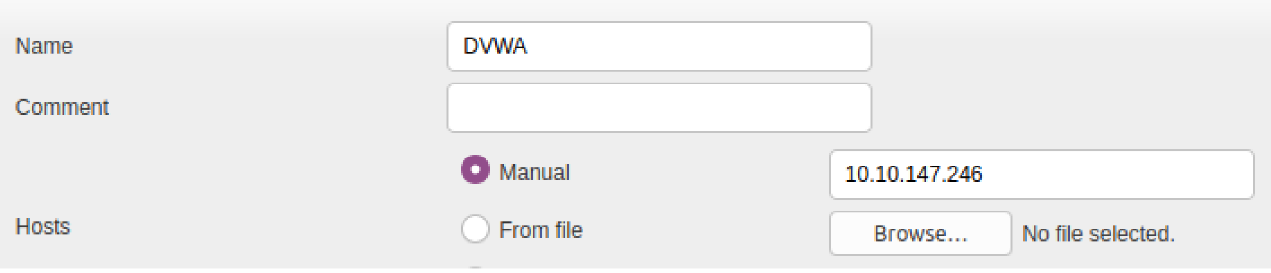
SSH: -- on port 22

SMB: --

ESXi: --

SNMP: --

Above is the menu for configuring a new target. The two main options you will need to configure are the Name and the Hosts. This procedure is fairly straight forward and other options will only be used in advanced vulnerability management solutions. These will be covered in later tasks.



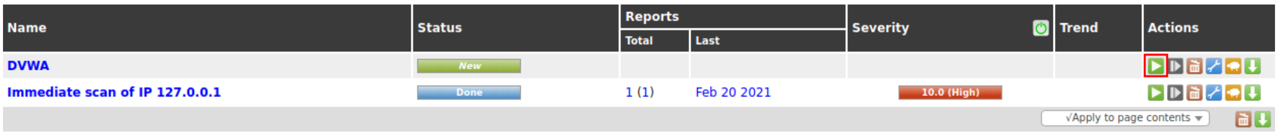
Name: DVWA

Comment:

Hosts: ● Manual 10.10.147.246
○ From file Browse... No file selected.

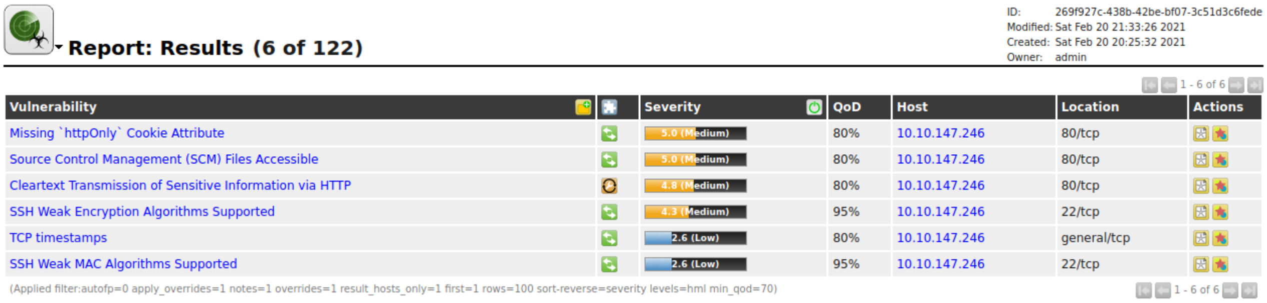
Now that we have our target scoped we can continue to create our task and begin the scan.

Once you create the task you will be brought back to the scan dashboard where you can monitor and start your task. To start the task navigate to the start icon under *Actions*.



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
DVWA	New					
Immediate scan of IP 127.0.0.1	Done	1 (1)	Feb 20 2021	10.0 (High)		

√Apply to page contents



Report: Results (6 of 122)

ID: 269f927c-438b-42be-bf07-3c51d3c6fede
Modified: Sat Feb 20 21:33:26 2021
Created: Sat Feb 20 20:25:32 2021
Owner: admin

1 - 6 of 6

Vulnerability		Severity	QoD	Host	Location	Actions
Missing `httpOnly` Cookie Attribute		5.0 (Medium)	80%	10.10.147.246	80/tcp	
Source Control Management (SCM) Files Accessible		5.0 (Medium)	80%	10.10.147.246	80/tcp	
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80%	10.10.147.246	80/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	10.10.147.246	22/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.147.246	general/tcp	
SSH Weak MAC Algorithms Supported		2.6 (Low)	95%	10.10.147.246	22/tcp	

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

1 - 6 of 6

Answer the questions below

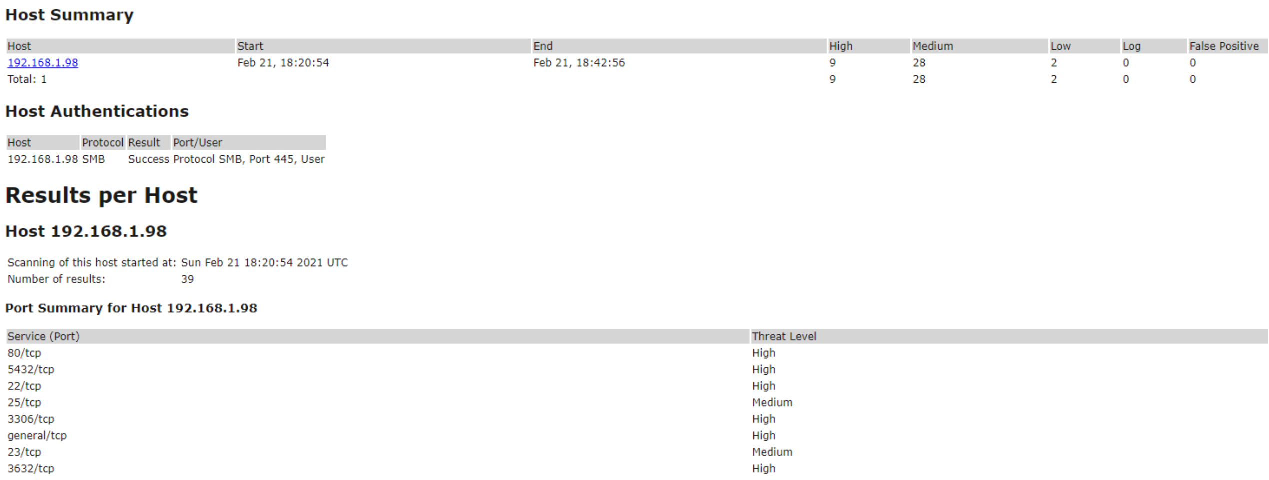
Read the above and complete your scan on DVWA to test scanning remote infrastructure.

OpenVAS has very strong reporting and monitoring capabilities that can contribute to an efficient and optimal solution in your build or vulnerability management pipeline.

Download the provided report from a vulnerable machine to get familiar with the automated reporting capabilities of OpenVAS.

Breaking Down the Report

The automated report from OpenVAS begins with some basic host and task information including Host, Start, End, and Vulnerability categories. It will also check for host authentications and an overall summary of open ports on the host.



Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
192.168.1.98	Feb 21, 18:20:54	Feb 21, 18:42:56	9	28	2	0	0
Total: 1			9	28	2	0	0

Host Authentications

Host	Protocol	Result	Port/User
192.168.1.98	SMB	Success	Protocol SMB, Port 445, User

Results per Host

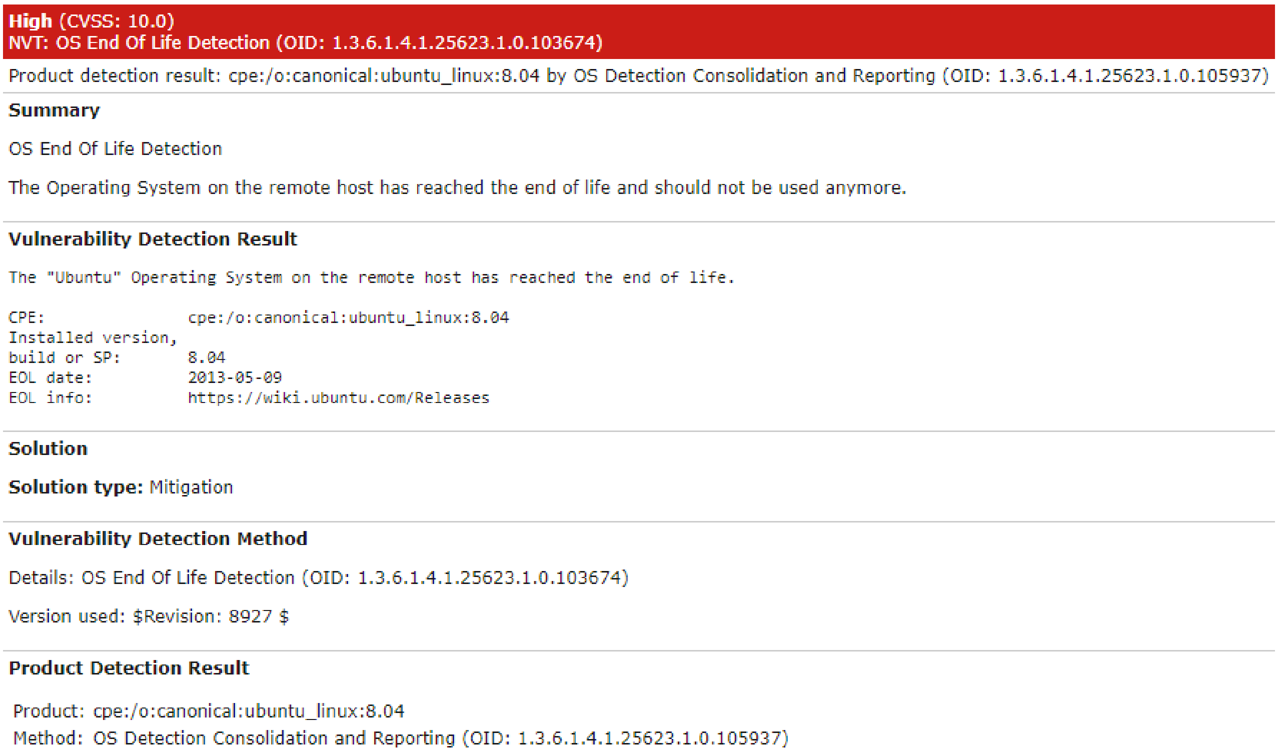
Host 192.168.1.98

Scanning of this host started at: Sun Feb 21 18:20:54 2021 UTC
Number of results: 39

Port Summary for Host 192.168.1.98

Service (Port)	Threat Level
80/tcp	High
5432/tcp	High
22/tcp	High
25/tcp	Medium
3306/tcp	High
general/tcp	High
23/tcp	Medium
3632/tcp	High

After the basic host and task information OpenVAS will report on each of the vulnerabilities found.



High (CVSS: 10.0)
NVT: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Product detection result: cpe:/o:canonical:ubuntu_linux:8.04 by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Summary

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

```
The "Ubuntu" Operating System on the remote host has reached the end of life.

CPE:               cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:       8.04
EOL date:          2013-05-09
EOL info:          https://wiki.ubuntu.com/Releases
```

Solution

Solution type: Mitigation

Vulnerability Detection Method

Details: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Version used: $Revision: 8927 $

Product Detection Result

Product: cpe:/o:canonical:ubuntu_linux:8.04
Method: OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

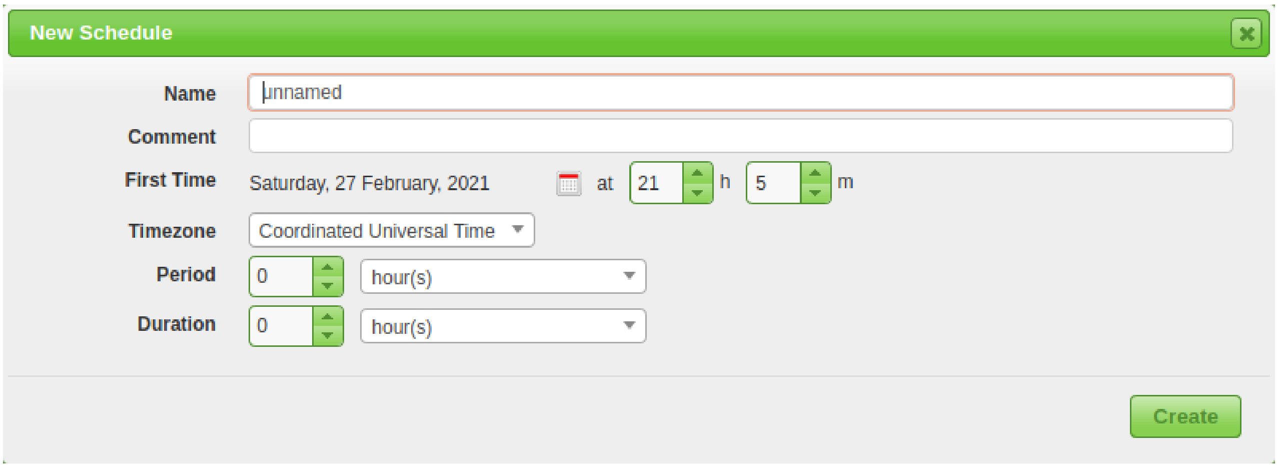
In the above image, the vulnerability breakdown can give a lot of information. We can gather a summary of the vulnerability, detection details, mitigation details, and method of detection.

Continuous Monitoring Overview

OpenVAS offers many options for continuous and scheduled monitoring/vulnerability management. If you work in a team or a pipeline this can allow you to efficiently and quickly optimize your current solutions. Examples of continuous vulnerability scanning utilities are Alerts, Schedules, and Agents. Agents are out of scope for this room but we will be covering the configuration of schedules and alerts below.

Creating Schedules

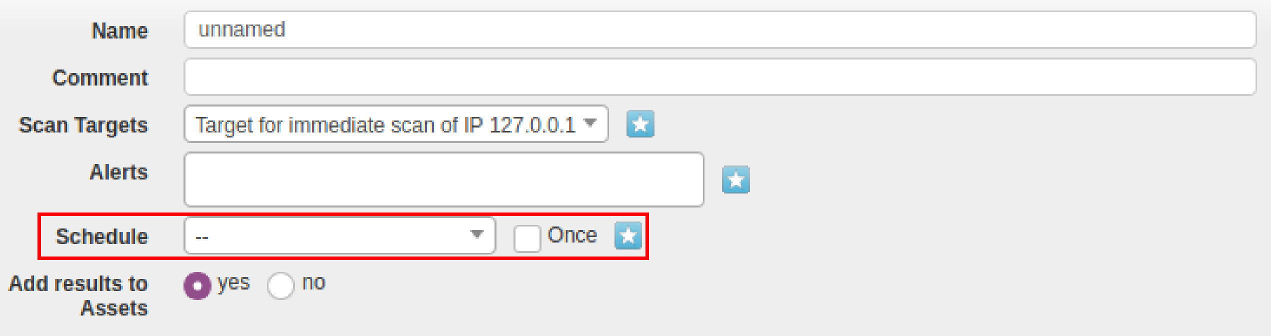
To begin creating a schedule navigate to *Configuration* > *Schedules* and as always click on the blue star icon in the upper left-hand corner. You should see a pop-up similar to the one below.



New Schedule

Name: unnamed
Comment:
First Time: Saturday, 27 February, 2021 at 21 h 5 m
Timezone: Coordinated Universal Time
Period: 0 hour(s)
Duration: 0 hour(s)

Fill out the basic information like Name, First Start Time, Period, etc. Once you have the schedule created you can now create a new Task/Scan with this created schedule attached. You can see this option below.



Name: unnamed

Comment:

Scan Targets: Target for immediate scan of IP 127.0.0.1

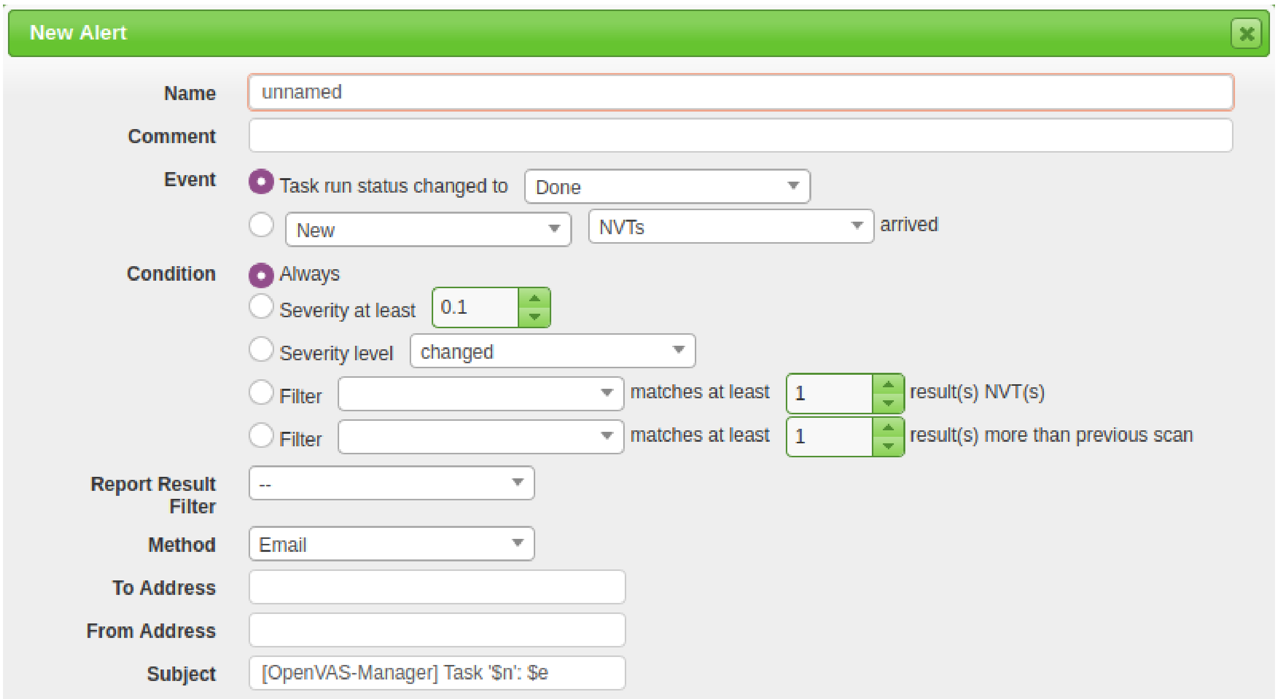
Alerts:

Schedule: -- □ Once

Add results to Assets: ● yes ○ no

Crafting Alerts

The process for creating alerts is very similar to creating a schedule, navigate to *Configuration* > *Alerts* and click on the blue star icon in the upper left-hand corner. You should see a pop-up similar to the one below.



New Alert

Name: unnamed

Comment:

Event: ● Task run status changed to Done
○ New NVTs arrived

Condition: ● Always
○ Severity at least 0.1
○ Severity level changed
○ Filter matches at least 1 result(s) NVT(s)
○ Filter matches at least 1 result(s) more than previous scan

Report Result Filter: --

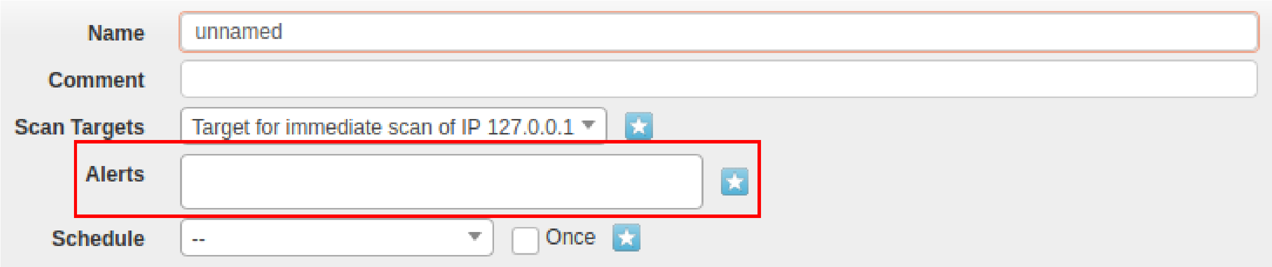
Method: Email

To Address:

From Address:

Subject: [OpenVAS-Manager] Task '$n': $e

You will notice that there are a lot more options than the schedule menu, don't let this intimidate you, the process is very similar and straightforward. The main options you will need to worry about are Name, Event, Condition, and To Address. The event can be configured to alert based on the status of the scan or when a new NVT/vulnerability is detected. The condition option will make sure that your inbox isn't flooded with alerts, this can be changed based on severity or filters. The To Address is fairly self-explanatory and will send an email of the alert to the specified mail address. Once created you will again need to connect the alert to a new Task/Scan. You can see the specific option below.



Name: unnamed

Comment:

Scan Targets: Target for immediate scan of IP 127.0.0.1

Alerts:

Schedule: -- □ Once

Answer the questions below

Read the above and practice reporting and monitoring.

The OpenVAS reports used are created from rooms on TryHackMe, machines used are credited to their respective owners.

Case 001: MS00-What?

In this scenario, you are assigned to a routine vulnerability management pipeline as a SOC analyst. Your automated pipeline has already pulled a scan on the server, it is up to you to analyze and identify risk in this report.

Answer the questions below

When did the scan start in Case 001?

When did the scan end in Case 001?

How many ports are open in Case 001?

How many total vulnerabilities were found in Case 001?

What is the highest severity vulnerability found? (MSxx-xxx)

What is the first affected OS to this vulnerability?

What is the recommended vulnerability detection method?

Want to learn more? There are many guides and blogs out on OpenVAS and GVM highlighting various advanced topics and features of the platforms. You can get a lot of information and technical understanding from the Greenbone technologies manual portal and forums.

You can find the Greenbone Technology Documentation, here.

OpenVAS

Open Vulnerability Assessment Scanner

If you want to continue working on your vulnerability management knowledge, check out the rest of the vulnerability management section of the Cyber Defense path on TryHackMe.

Answer the questions below

Check out the provided links and keep learning!

Created by Cryillic

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 32316 users are in here and this room is 852 days old.