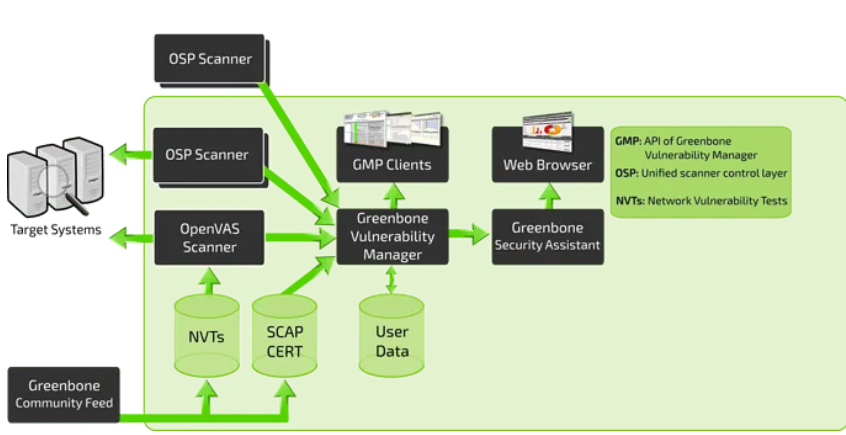
**TASK 3**



# Installing OpenVAS

# apt install docker.io

# docker run -d -p 443:443 --name openvas mikesplain/openvas

# 

# Initial Configuration

# 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.

# 

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.

# 

# Scanning Infrastructure

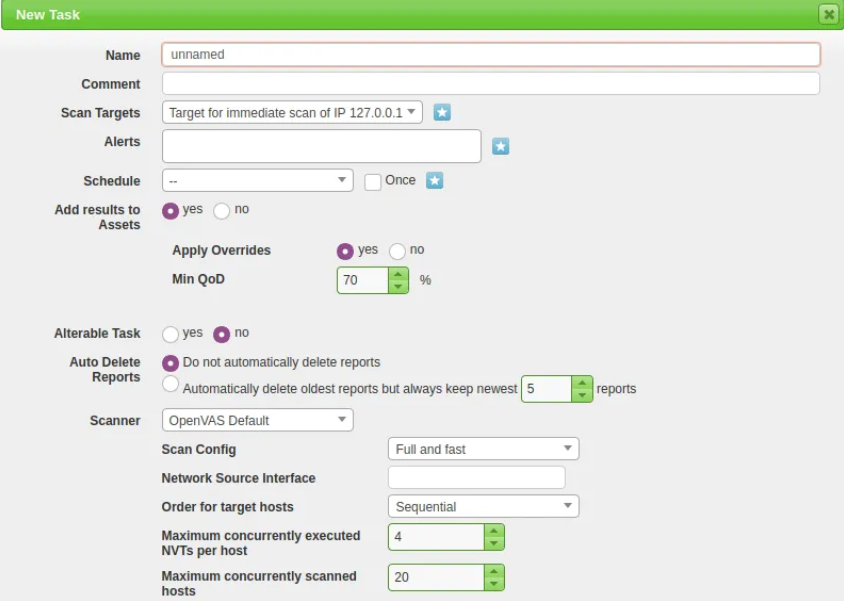
# Now that we know that everything is working we can get into the nitty-gritty of OpenVAS and how it works. Deploy the machine and navigate to *Scans > Tasks* to begin creating a task to scan the provided machine.

# 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*.

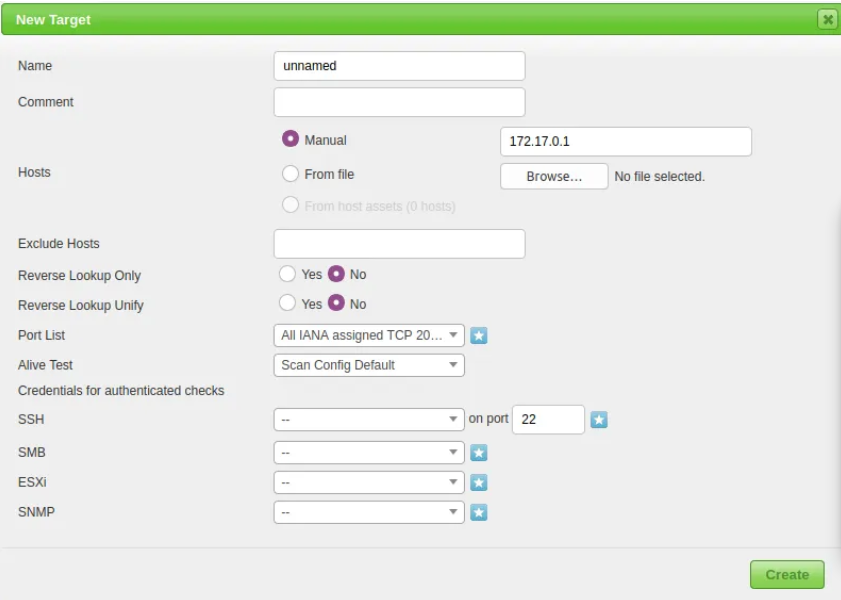
# 

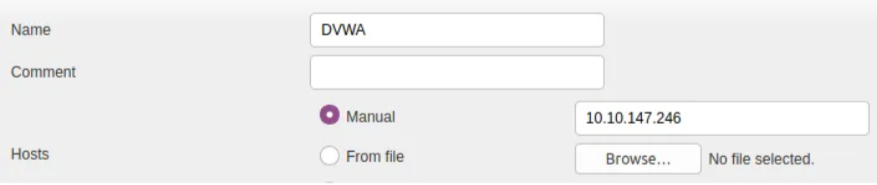
Once you select New Task from the dropdown you will be met with a large pop-up with many options. We will break down each of the options sections and what they can be used for.

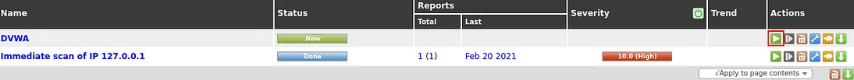


For this task, we will be focusing only on the Name, Scan Targets, and Scanner Type, and Scan Config. In later tasks, we will be focusing on the other options for more advanced configuration and implementation/automation.

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.





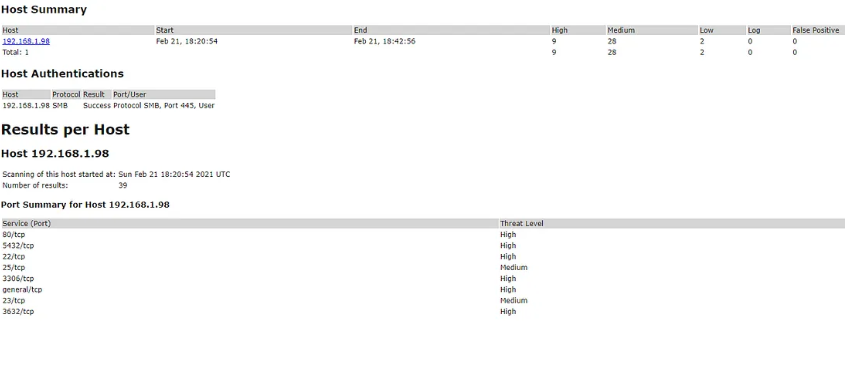


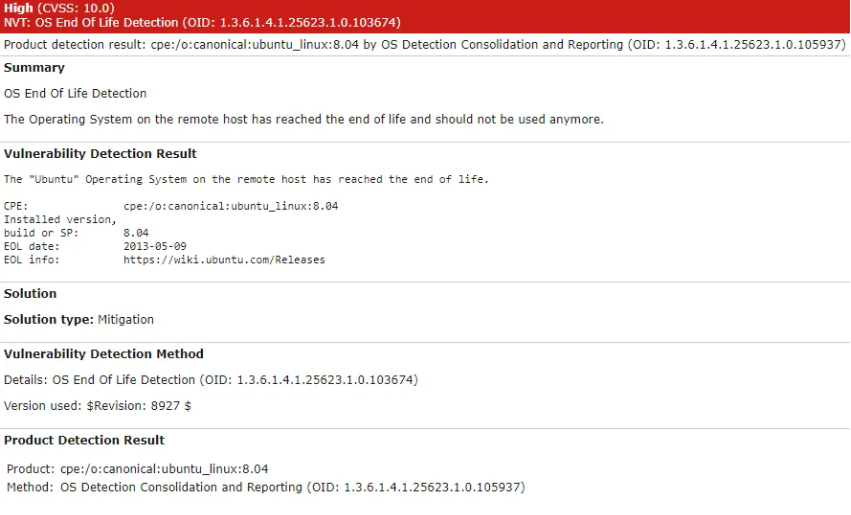
# Reporting and Continuous Monitoring

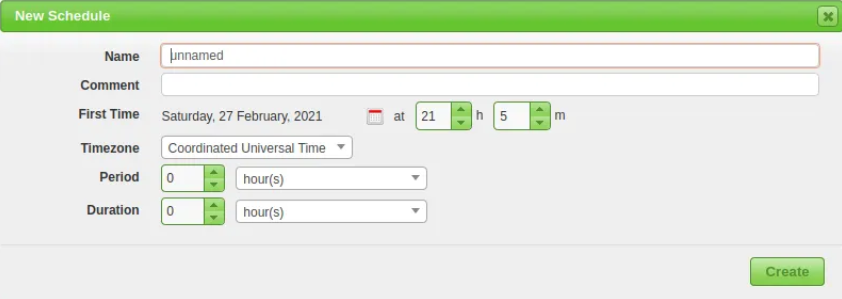
# OpenVAS has very strong reporting and monitoring capabilities that can contribute to an efficient and optimal solution in your build or vulnerability management pipeline.

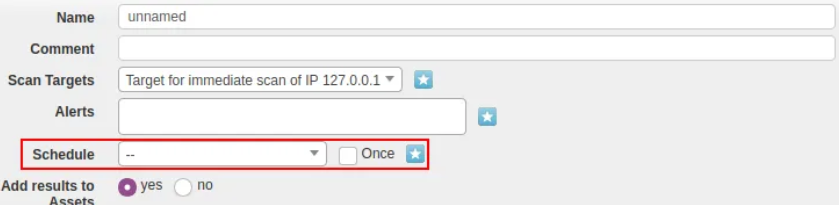
# Download the provided report from a vulnerable machine to get familiar with the automated reporting capabilities of OpenVAS.

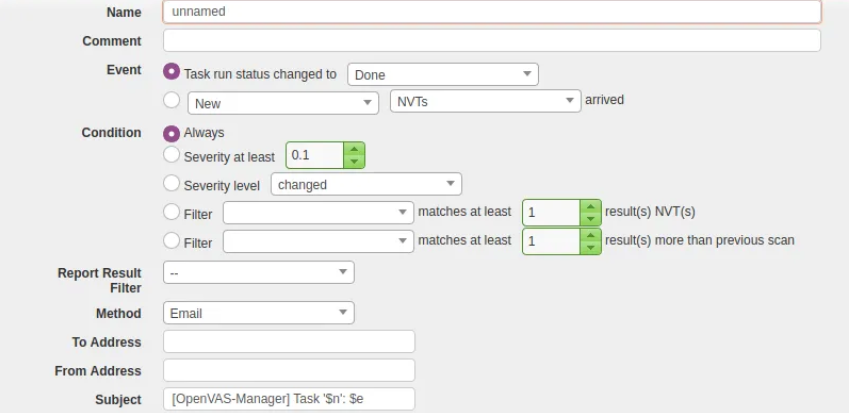
# 











# Practical Vulnerability Management

