

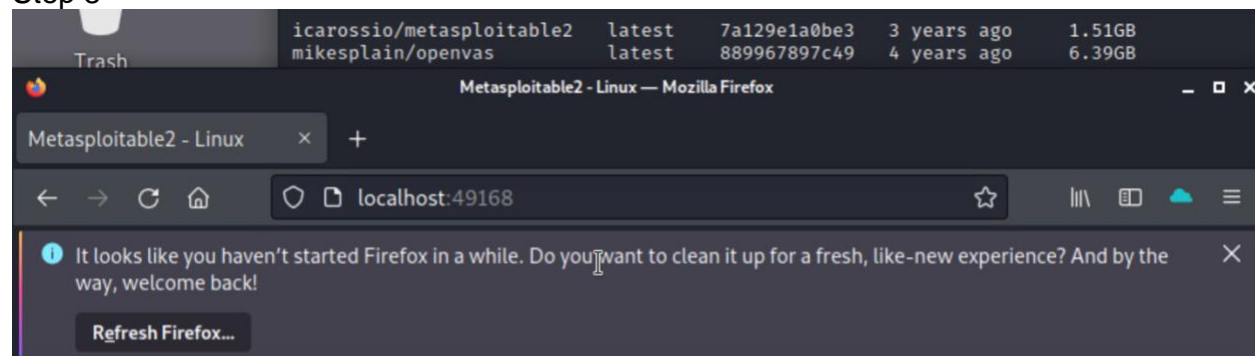
Peter Sanford  
IT 2700  
NetLab Lab 1  
9/2/2023

Part 1.1:

Step 5

```
(kali㉿kali)-[~]  
$ sudo docker run -rm -ditP icarossio/metasploitable2  
unknown shorthand flag: 'r' in -rm  
See 'docker run --help'.  
  
(kali㉿kali)-[~]  
$ sudo docker run --rm -ditP icarossio/metasploitable2  
ddde57d4c492830cd5de8bacc8bbc0d31cddf5131c0ed35bdc32afadd9826cd6
```

Step 8



Part 1.2:

Step 2

```
(kali@kali)-[~]  
$ sudo docker run --rm -d -p 443:443 --name openvas mikesplain/openvas  
dd7796cc1fae5ebde670a437cee3a67ae8638f766f50a1f5709acb3e52f499f6
```

step 9

The screenshot shows a web browser window with two tabs: 'Damn Vulnerable Web Ap...' and 'Greenbone Security Assis...'. The address bar shows the URL 'https://localhost/omp?r=1&token=1d104d07-7af0-424b-ae81'. A notification bar at the top states: 'It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!' with a 'Refresh Firefox...' button. The main header is green and contains the 'Greenbone Security Assistant' logo, a 'No auto-refresh' dropdown, and user information: 'Logged in as Admin admin | Logout Sat Sep 2 21:40:35 2023 UTC'. Below the header is a navigation menu with links: Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area is titled 'Dashboard' and features several widgets. The first two widgets are 'Tasks by Severity Class (Total: 0)' and 'Tasks by status (Total: 0)', both displaying a large 3D donut chart. Below these are three more widgets: 'CVEs by creation time (Total: 12...', 'Hosts topology', and 'NVTs by Severity Class (Total: 4...'. Each widget has a dropdown arrow on its left side.

Part 2.1:

Step 1

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout  
Sat Sep 2 21:43:56 2023 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter:  rows=10 first=1 sort=name

**Targets (0 of 0)**

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
(Applied filter: rows=10 first=1 sort=name)					

vApply to page contents

step 3

**Targets (1 of 1)**

1 - 1 of 1

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
<b>metasploitable</b>	127.0.0.1	1	All TCP		

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

vApply to page contents

1 - 1 of 1

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Part 2.2:

step 3

1 - 1 of 1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
<b>metasploitable scan</b>	New					

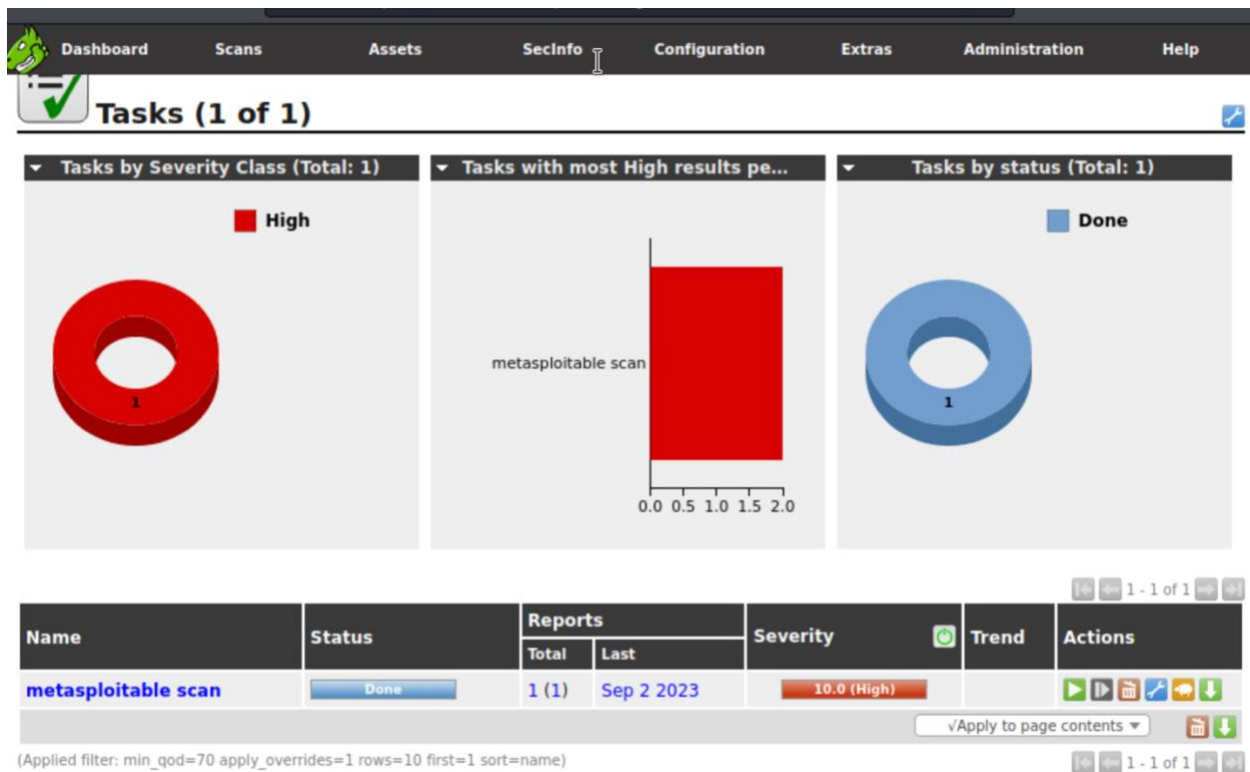
(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

vApply to page contents

1 - 1 of 1

Part 2.3:

step 3



step 5

Greenbone Security Assistant — Mozilla Firefox

Damn Vulnerable Web Ap × Greenbone Security Assis ×

https://localhost/omp?cmd=get\_report&report\_id=8cfaecaa-...

Greenbone Security Assistant Logged in as Admin admin | Logout Sat Sep 2 22:16:51 2023 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done 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

**Report: Results (5 of 42)** ID: 8cfaecaa-c9e0-4c72-9026-cd875a56cc95 Modified: Sat Sep 2 22:13:35 2023 Created: Sat Sep 2 21:49:07 2023 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	
Redis Server No Password	7.5 (High)	100%	127.0.0.1 (localhost)	6379/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	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	127.0.0.1 (localhost)	25/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)

Backend operation: 0.66s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

## Credentials

Vulnerability	Severity	QoD	Host	Location	Actions
<a href="#">OpenVAS / Greenbone Vulnerability Manager Default Credentials</a>	10.0 (High)	100%	127.0.0.1	9390/tcp	
<b>Summary</b> The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.					
<b>Vulnerability Detection Result</b> It was possible to login using the following credentials (username:password:role): admin:admin:Admin					
<b>Impact</b> This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.					
<b>Solution</b> <b>Solution type:</b> Workaround Change the password of the mentioned account(s).					
<b>Vulnerability Insight</b> It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.					
<b>Vulnerability Detection Method</b> Try to login with default credentials via the OMP/GMP protocol. Details: <a href="#">OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)</a> Version used: \$Revision: 13944 \$					
<b>Product Detection Result</b> Product: <a href="#">cpe:/a:openvas:openvas_manager:7.0</a> Method: <a href="#">OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)</a>					

### Commentary:

In this lab I ran a vulnerability scan on the test machine using the loopback address 127.0.0.1. The scan showed the vulnerabilities that it found, and it was cool to look at each one and what the description was for each. I learned how important running these scans are since they can catch things that you might not have thought about beforehand. I think it would be really cool to run a similar scan on my home machine to see what it finds. This would be useful to automate and improve vulnerability finding within you company's network, and also can help you secure your network to be in compliance with security standards.