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

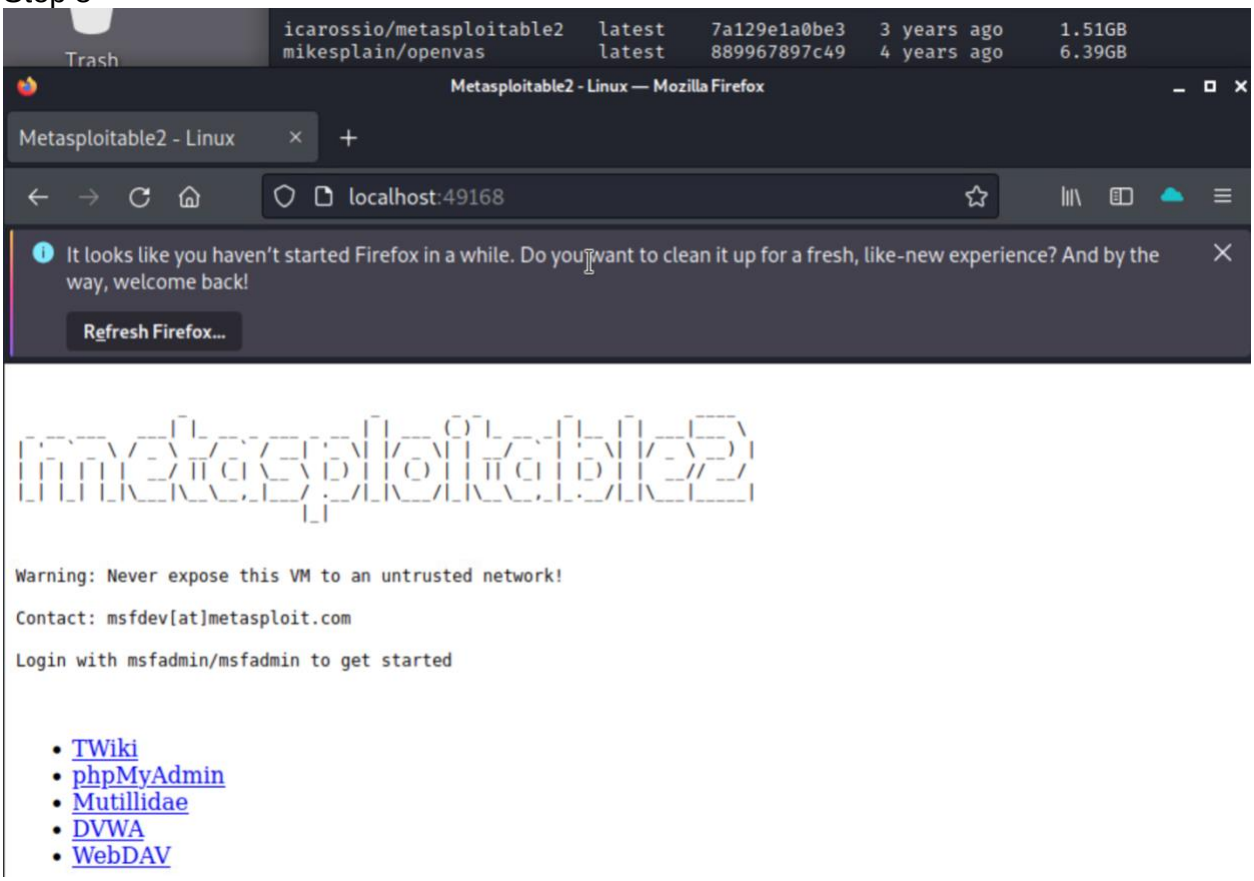
Part 1.1:

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

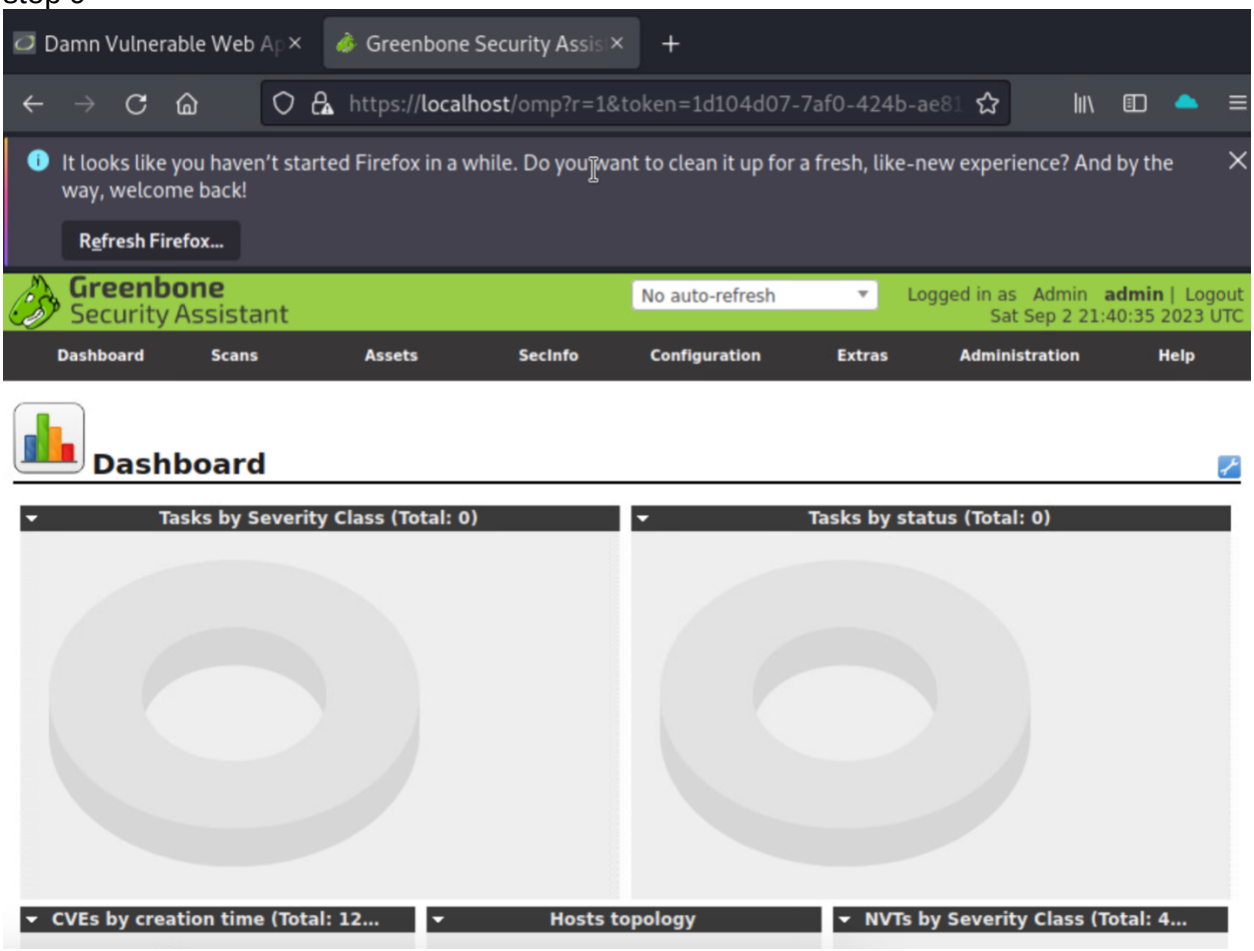


Part 1.2:

Step 2

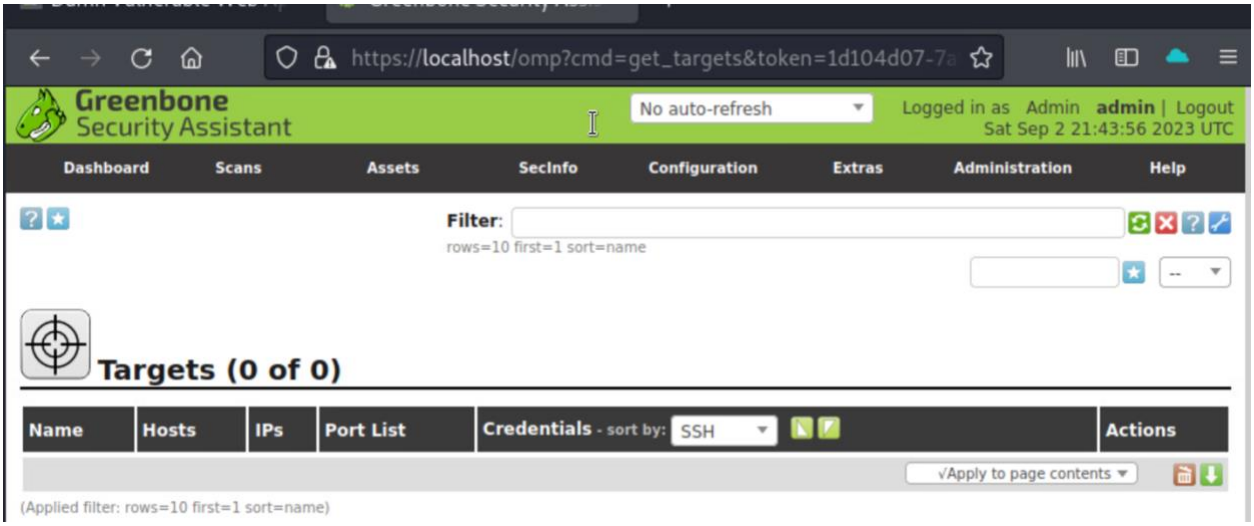
```
┌──(kali㉿kali)-[~]
└─$ sudo docker run --rm -d -p 443:443 --name openvas mikesplain/openvas
dd7796cc1fae5ebde670a437cee3a67ae8638f766f50a1f5709acb3e52f499f6
```

step 9



Part 2.1:

Step 1



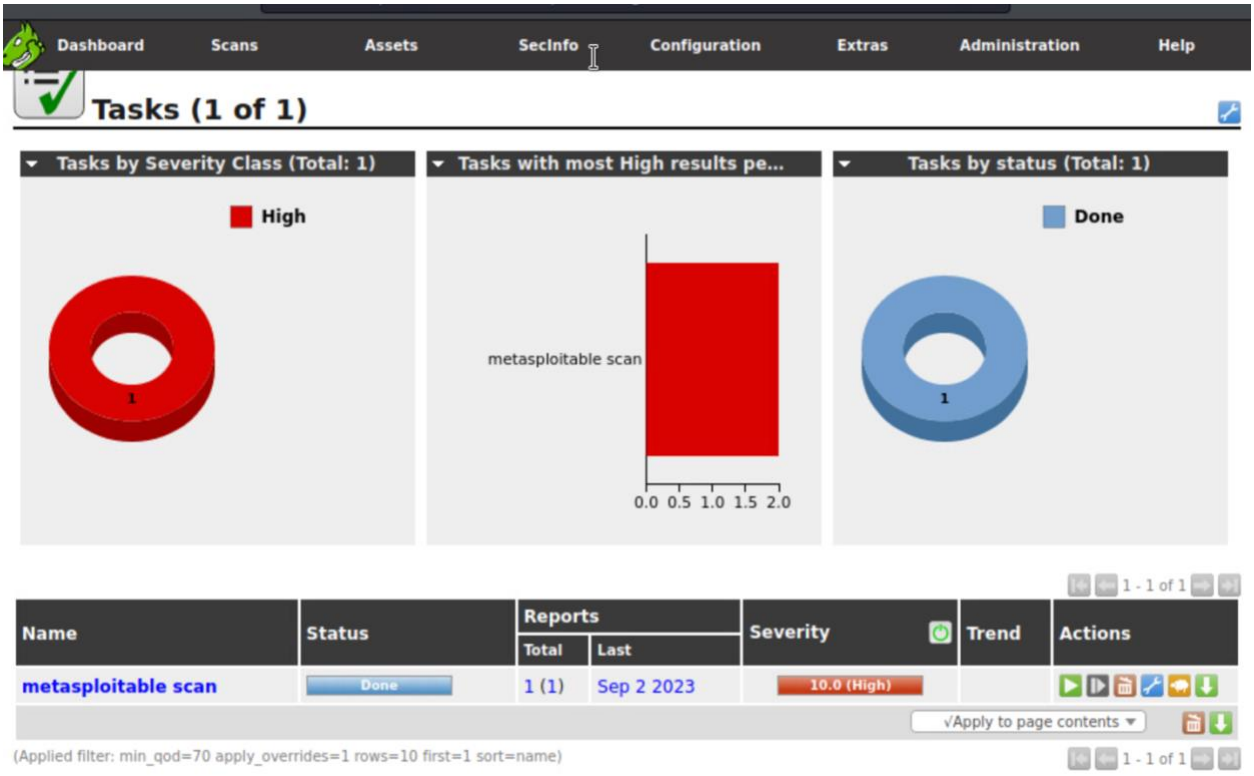
step 3

Part 2.2:

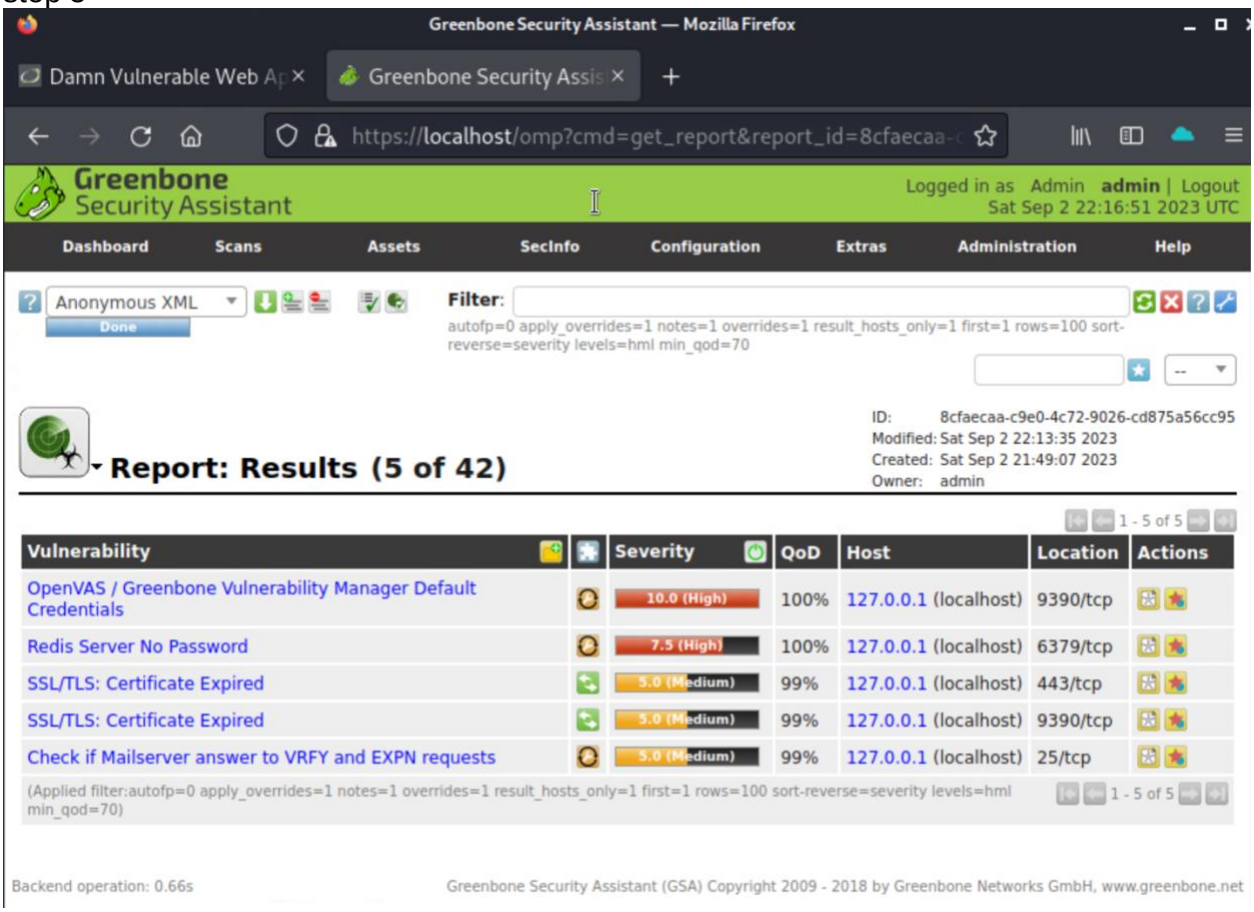
step 3

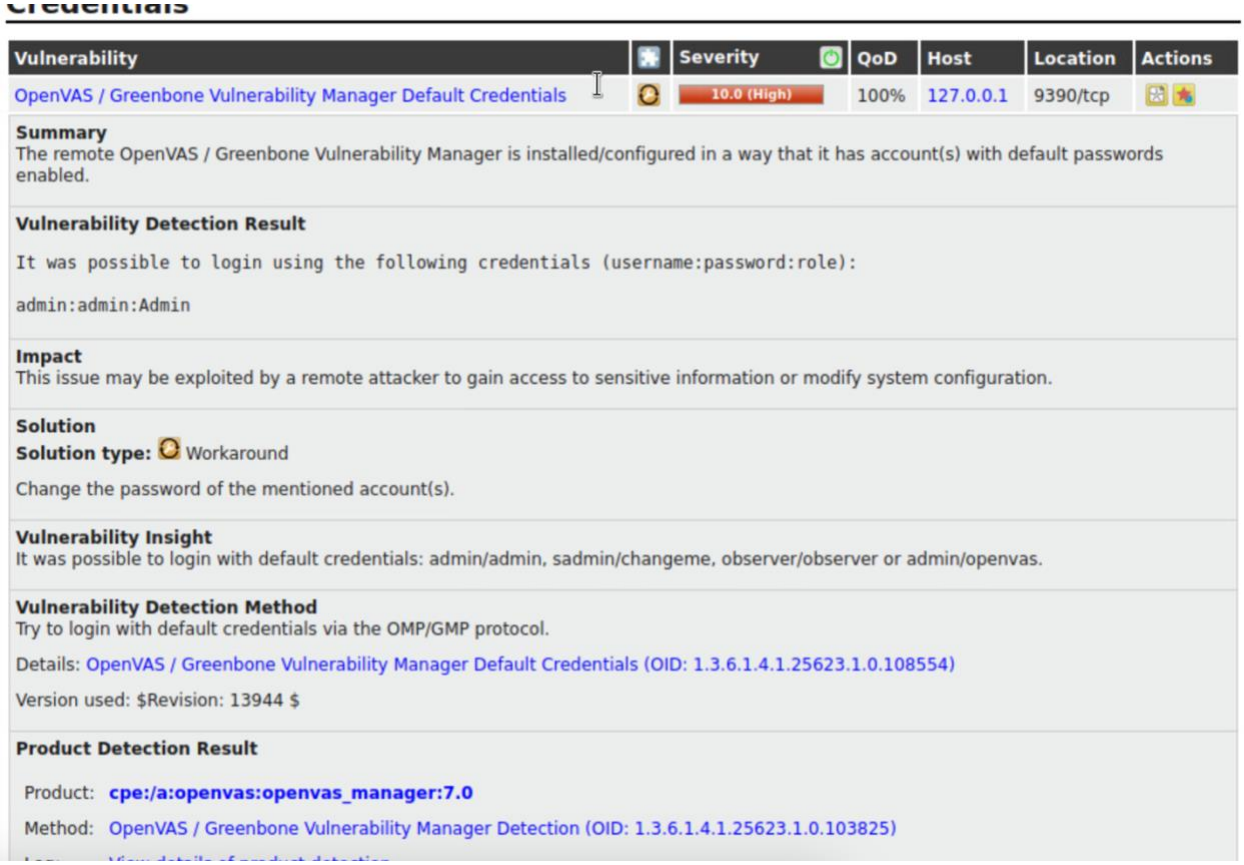
Part 2.3:

step 3


Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
High
1
Tasks with most High results pe...
metasploitable scan
0.0 0.5 1.0 1.5 2.0
Tasks by status (Total: 1)
Done
1
1 - 1 of 1
Name
Status
Reports
Total
Last
Severity
Trend
Actions
metasploitable scan
Done
1 (1)
Sep 2 2023
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

step 5


Greenbone Security Assistant — Mozilla Firefox
Damn Vulnerable Web A
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
ID: 8cfaecaa-c9e0-4c72-9026-cd875a56cc95
Modified: Sat Sep 2 22:13:35 2023
Created: Sat Sep 2 21:49:07 2023
Owner: admin
Report: Results (5 of 42)
1 - 5 of 5
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)
1 - 5 of 5
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
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	127.0.0.1	9390/tcp	

Summary
The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result

```
It was possible to login using the following credentials (username:password:role):

admin:admin:Admin
```

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Solution type: Workaround

Change the password of the mentioned account(s).

Vulnerability Insight
It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

Vulnerability Detection Method
Try to login with default credentials via the OMP/GMP protocol.

Details: OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)

Version used: $Revision: 13944 $

Product Detection Result

Product: **cpe:/a:openvas:openvas_manager:7.0**

Method: OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)

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.