VULNERABILITY SCANNING AND MANAGEMENT

We have found three vulnerabilities in one of the systems that we've scanned. The three vulnerabilities are

- MySQL/ Maria DB Weak password
- SSH weak encryption algorithms supported
- SSH weak MAC algorithms supported

All the three vulnerabilities are found on a single system of IP 192.168.252.61.

1. MySQL/ Maria DB Weak password:

CVSS: 9.0 High
PORT: 3306/ TCP
DATE: Tue Dec 6 00:58:06 2022.
Quality of Detection: remote_active (95%)

Summary:

It was possible to login into remote MySQL using weak credentials. This vulnerability was found by logging into the said sql using an empty password.
The best possible solution was to change the password or at least to have on. The reason for its high CVSS score was that it has an impact on all three parts of the CIA triad along with access complexity. It has a low impact on access complexity and partial impact on both integrity and availability, but it has complete impact on the confidentiality piece.

2. SSH Weak encryption supported:

CVSS: 4.3 Medium
PORT: 22/ TCP
DATE: Tue Dec 6 00:57:35 2022
Quality of Detection: remote_active (95%)

Summary:

As suggested by the title, the ssh server is configured to allow weakly encrypted algorithms. Particularly in this situation, we are talking about couple of weak encryptions like Arc four, None (no encryption) and cipher block chaining (CBC) mode. This was detected by checking for above mentioned weak encryptions.
The above-mentioned ciphers are said to be weak, for example: arc four is said to have problems with weak keys. This vulnerability exists in CBC-mode, this gives the bad actor an easy way to decrypt the cipher text.

This can be solved just by disabling the weak encryption algorithms. The CVSS score is medium because it has a medium impact on access complexity and along with a partial impact in the confidentiality.

3. SSH Weak MAC algorithms supported:

CVSS: 2.6 Low
PORT: 22/ TCP
DATE: Tue Dec 6 00:57:35 2022
Quality of Detection: remote_active (95%)

Summary:

The remote ssh server is configured in a way that it allows weak message digest and/or 96 – bit MAC algorithms. Like the above solution, this can also be taken care of by disabling the weak MAC algorithms.

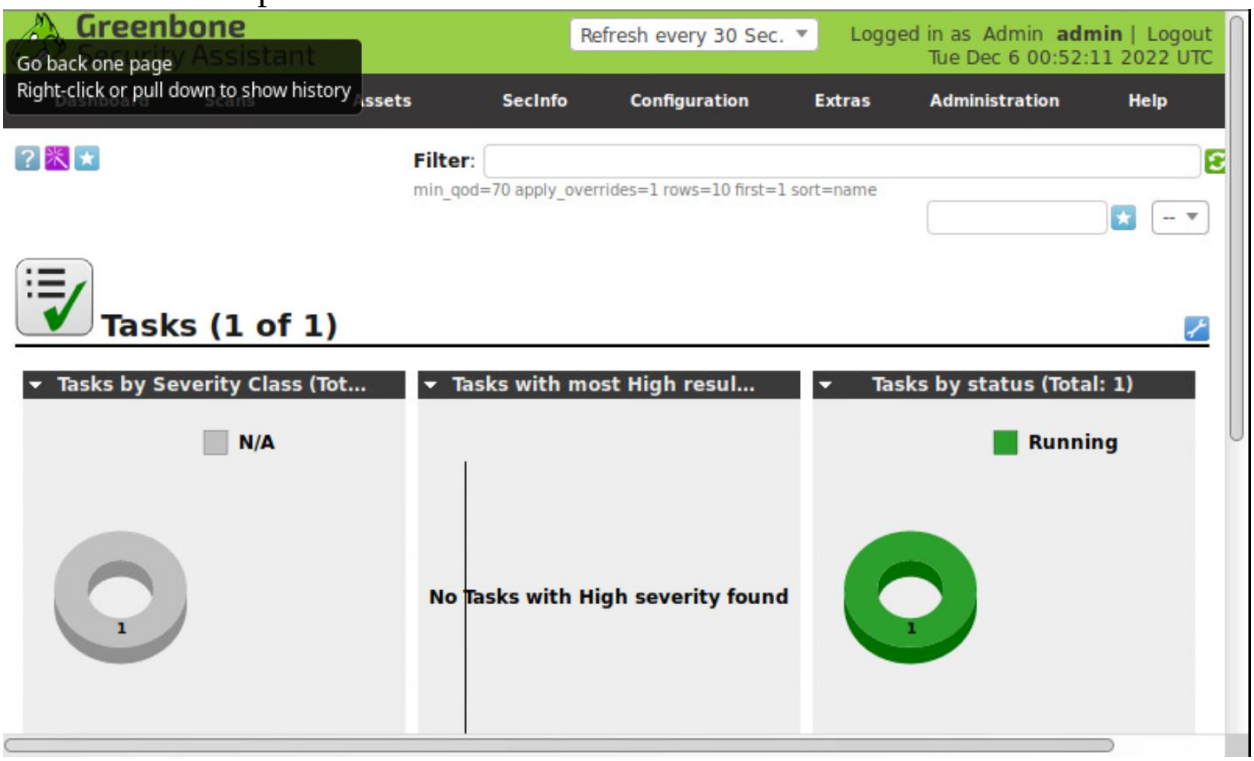
The CVSS score is based on the High impact it has on the access complexity and the partial Impact it has on confidentiality.

NOTE:

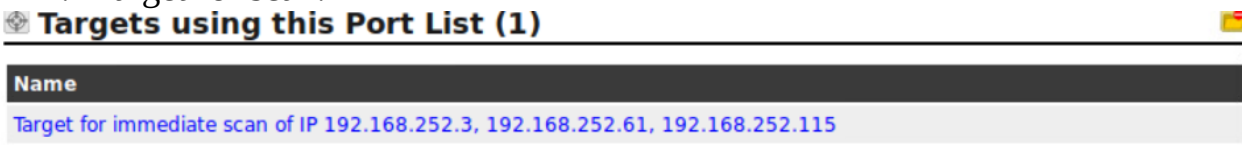
1. Quality of Detection (QoD): remote_active means that the results of remote active check, like sql injection, code execution etc, are positive implying the vulnerability exists. It is very rare that these checks would show up negative if the QoD is remote_active.
2. For all the above-mentioned vulnerabilities, the mentioned solutions fall under solution type *Mitigation.*

SCREENSHOTS:

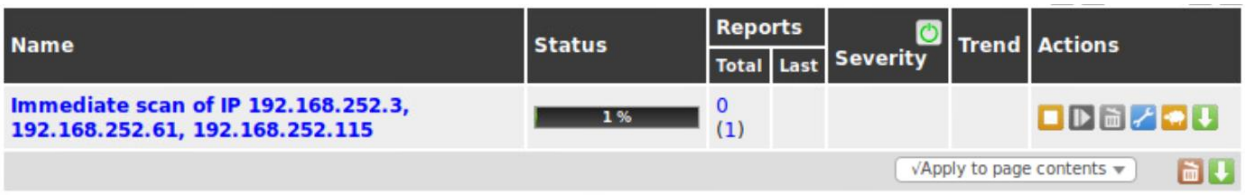
1. Initial setup



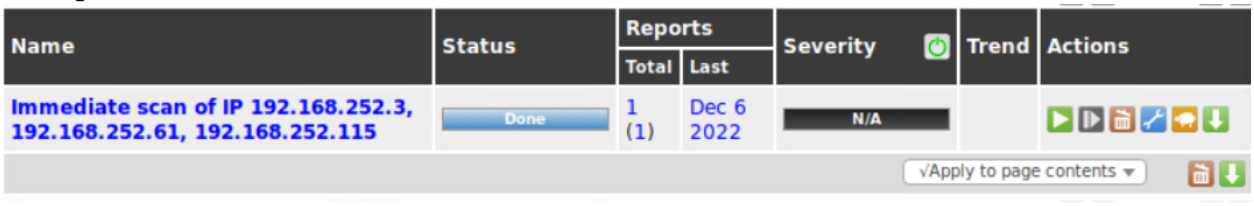
2. Target for scan:



3. Scan Status:



Completed scan



4. Port list

Name	Port Counts			Actions
	Total	TCP	UDP	
All IANA assigned TCP 2012-02-10	5625	5625	0	
All IANA assigned TCP and UDP 2012-02-10	10988	5625	5363	
All privileged TCP	1023	1023	0	
All privileged TCP and UDP	2046	1023	1023	
All TCP	65535	65535	0	
All TCP and Nmap 5.51 top 100 UDP	65634	65535	99	
All TCP and Nmap 5.51 top 1000 UDP	66534	65535	999	
Nmap 5.51 top 2000 TCP and top 100 UDP	2098	1999	99	
OpenVAS Default	4481	4481	0	

√Apply to page contents

5. Default OpenVAS

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Start	End	Protocol
1	5	tcp
7	7	tcp
9	9	tcp
11	11	tcp
13	13	tcp
15	15	tcp
17	25	tcp
27	27	tcp
29	29	tcp
31	31	tcp
33	33	tcp
35	35	tcp
37	39	tcp
41	59	tcp
61	224	tcp
242	248	tcp
256	268	tcp

6. Alerts

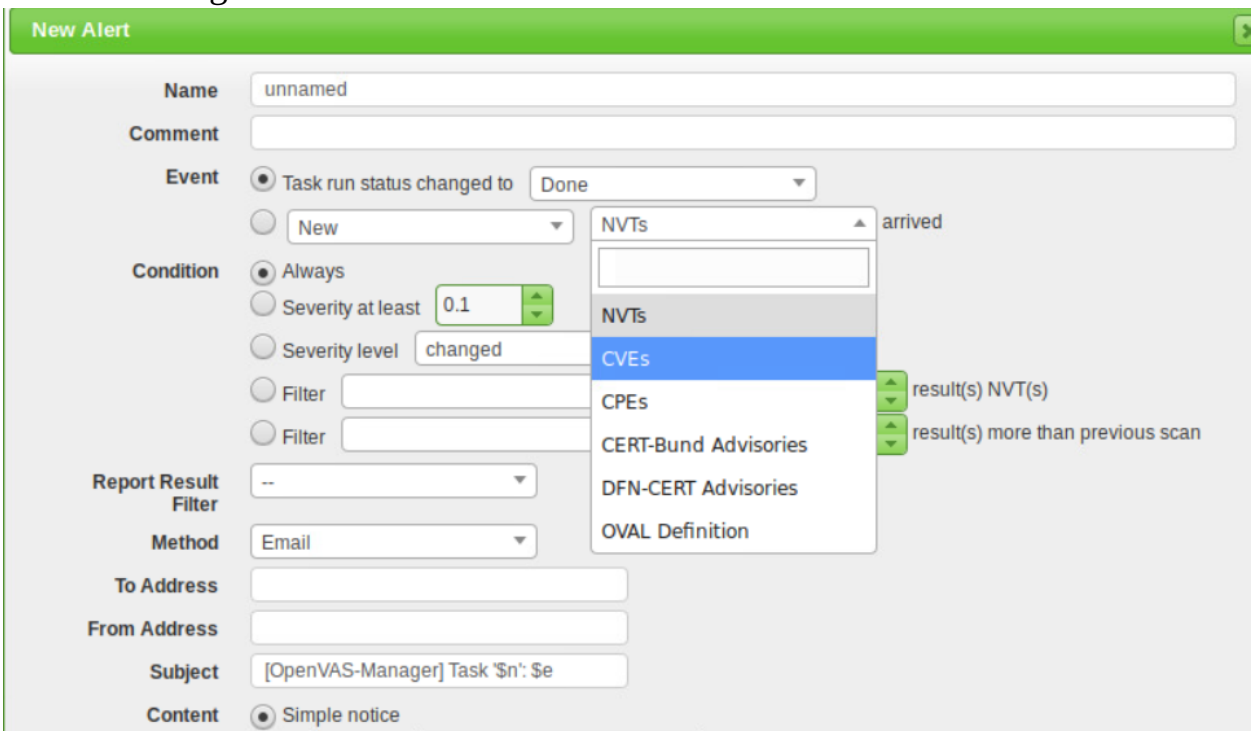
Alerts (0 of 0)

Name	Event	Condition	Method	Filter	Actions

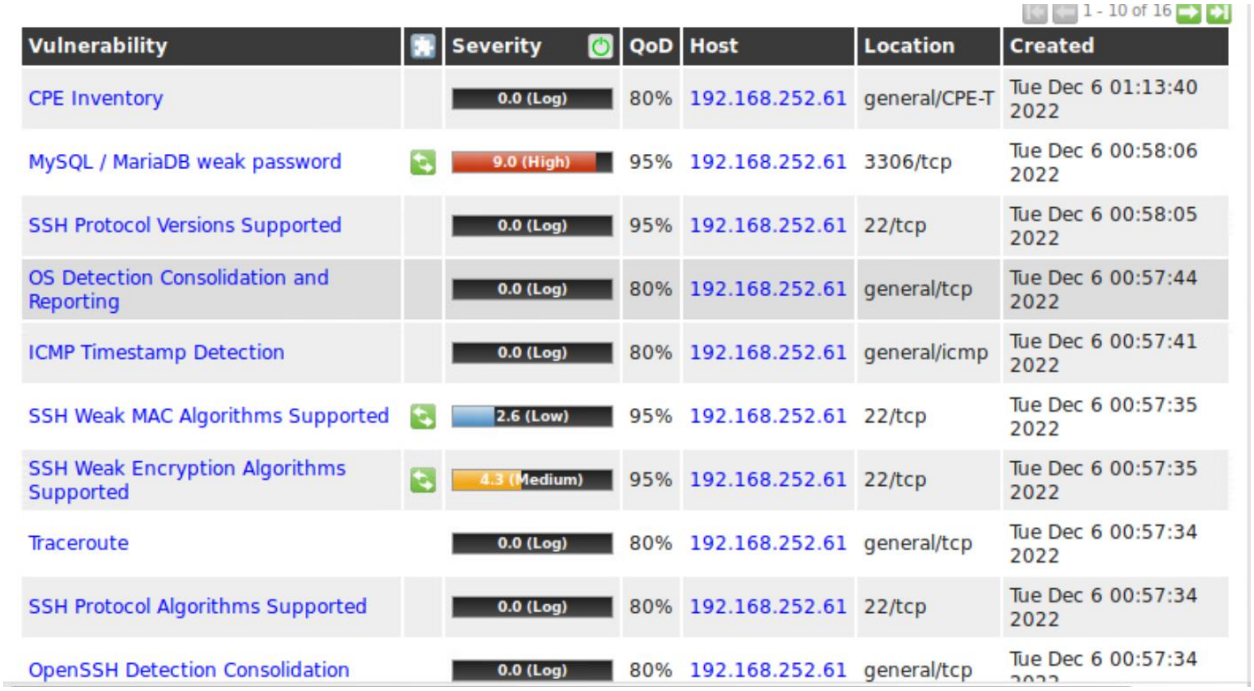
√Apply to page contents

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

7. Creating Alerts



8. Vulnerabilities List



1 - 10 of 16

Vulnerability	Severity	QoD	Host	Location	Created
CPE Inventory	0.0 (Log)	80%	192.168.252.61	general/CPE-T	Tue Dec 6 01:13:40 2022
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.252.61	3306/tcp	Tue Dec 6 00:58:06 2022
SSH Protocol Versions Supported	0.0 (Log)	95%	192.168.252.61	22/tcp	Tue Dec 6 00:58:05 2022
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.168.252.61	general/tcp	Tue Dec 6 00:57:44 2022
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.252.61	general/icmp	Tue Dec 6 00:57:41 2022
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.252.61	22/tcp	Tue Dec 6 00:57:35 2022
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.252.61	22/tcp	Tue Dec 6 00:57:35 2022
Traceroute	0.0 (Log)	80%	192.168.252.61	general/tcp	Tue Dec 6 00:57:34 2022
SSH Protocol Algorithms Supported	0.0 (Log)	80%	192.168.252.61	22/tcp	Tue Dec 6 00:57:34 2022
OpenSSH Detection Consolidation	0.0 (Log)	80%	192.168.252.61	general/tcp	Tue Dec 6 00:57:34 2022