Network Vulnerability Assessment Report

Date: June 8, 2024

Prepared by: Dinesh Kumar P

INTERNSHIP PROJECT AT EXTION INFOTECH

TABLE OF CONTENTS

Executive Summary………………………………………………...1

Methodology……………………………………………………..1

Vulnerability Overview…………………………………………….5

Detailed Vulnerability Descriptions……………………………..5

Mitigation Plan…………………………………………………..6

Final Scan Report……………………………………………..…7

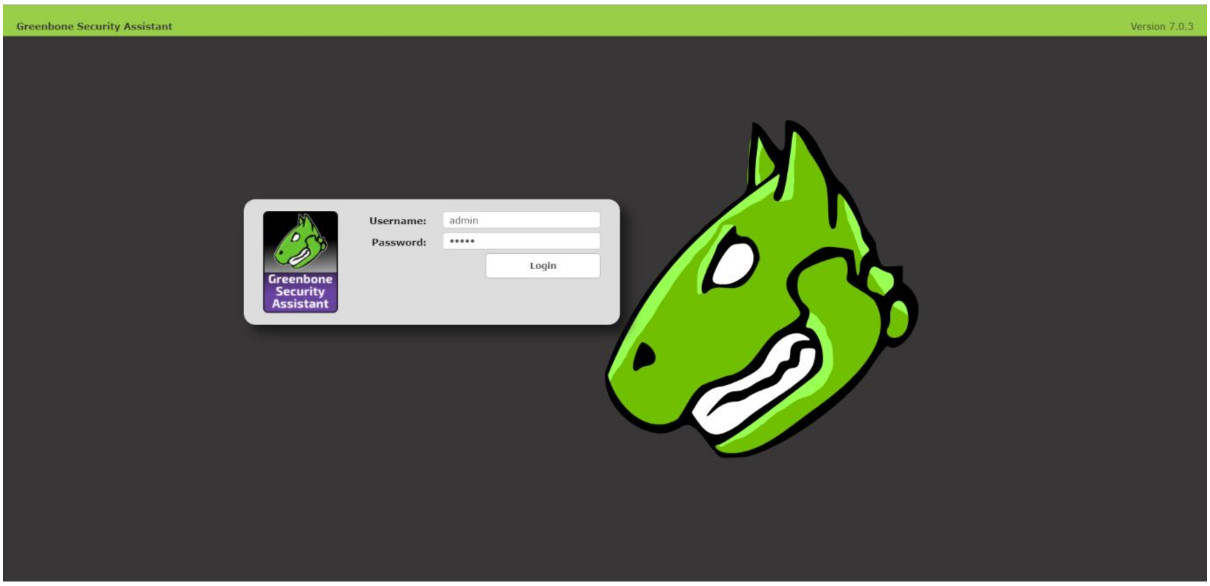
1) Executive Summary

This report documents the findings from a comprehensive network vulnerability assessment conducted on a simulated network environment using OpenVAS. The scan aimed to identify critical vulnerabilities, assess their potential impact, and recommend mitigation strategies. The assessment targeted the host 172.28.224.1 and identified several vulnerabilities categorized as medium and low threats, along with various logs. No high threat vulnerabilities were detected.

2) Methodology

The assessment was conducted using OpenVAS, a robust open-source tool for vulnerability scanning and management. The scan was executed from June 8, 2024, 13:47:40 UTC to June 8, 2024, 14:17:22 UTC. The results were analyzed, and detailed reports were generated for each identified vulnerability.

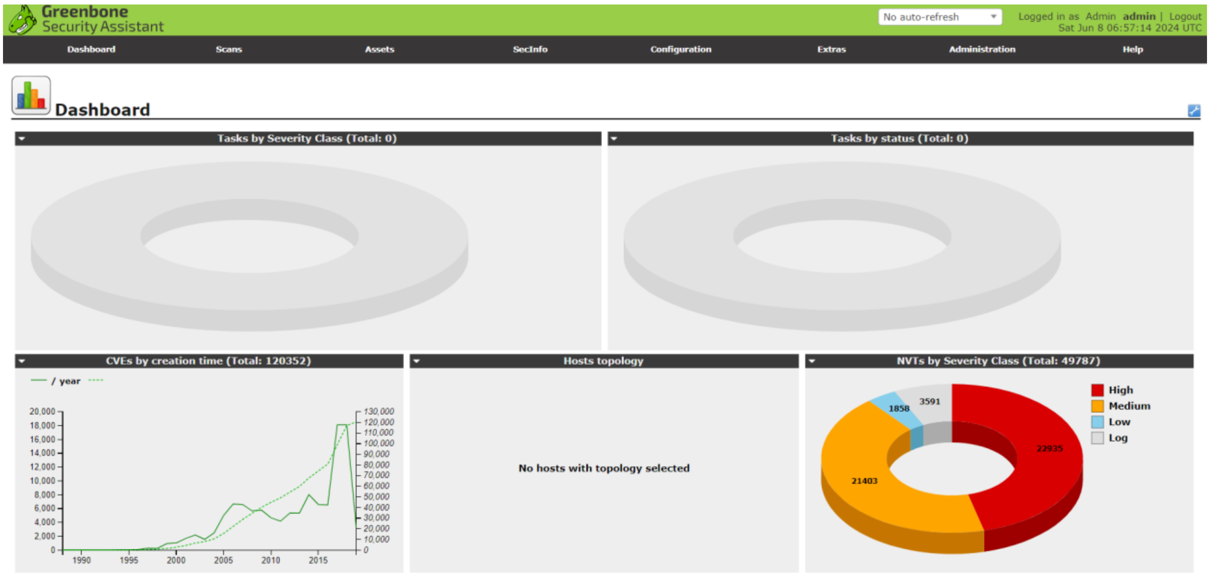
Login page of OpenVAS



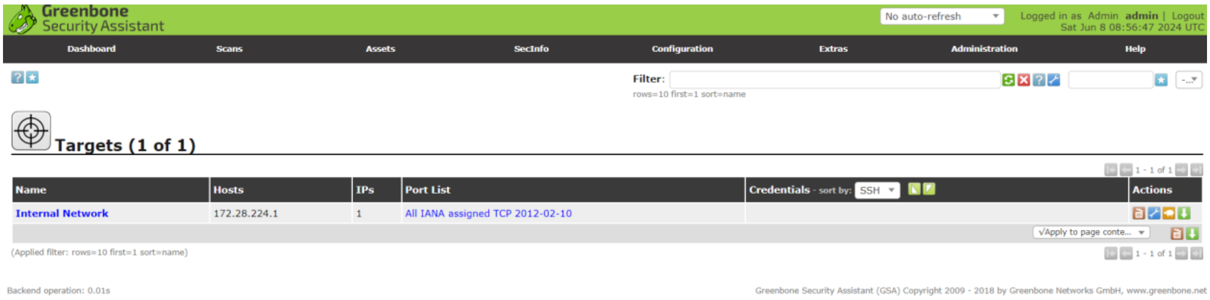
Username: admin

Password: *****

Dashboard before vulnerability scan



Creating target



rows=10 first=1 sort=name

Targets (1 of 1)

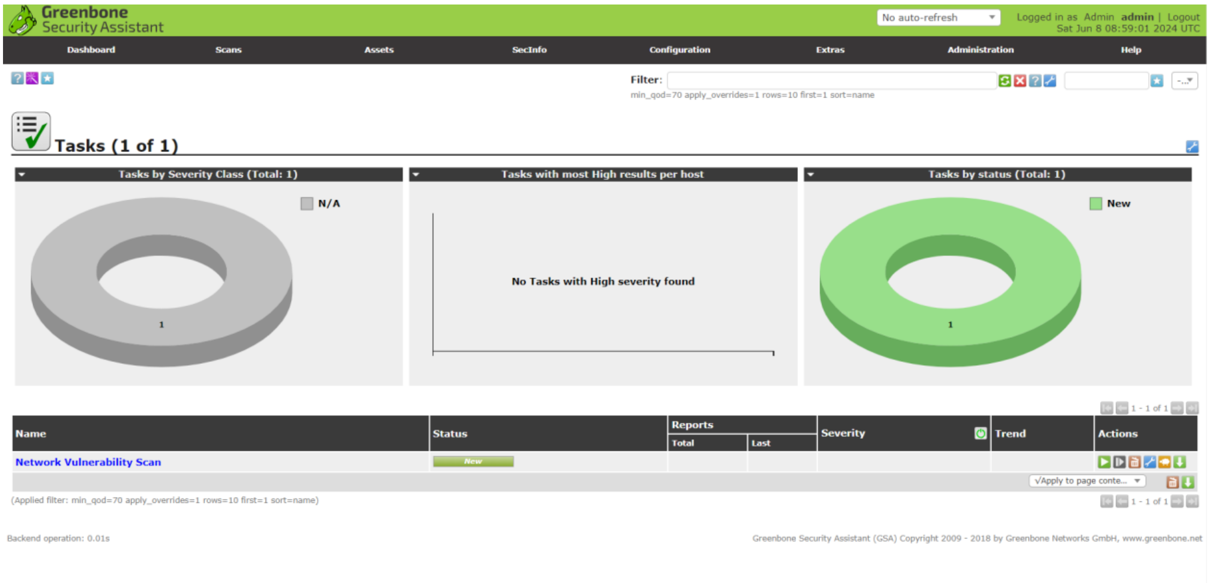
Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Internal Network	172.28.224.1	1	All IANA assigned TCP 2012-02-10		

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

Backend operation: 0.01s

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

Creating task


Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sat Jun 8 08:59:01 2024 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
New
1
1 - 1 of 1
√Apply to page conte...

min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

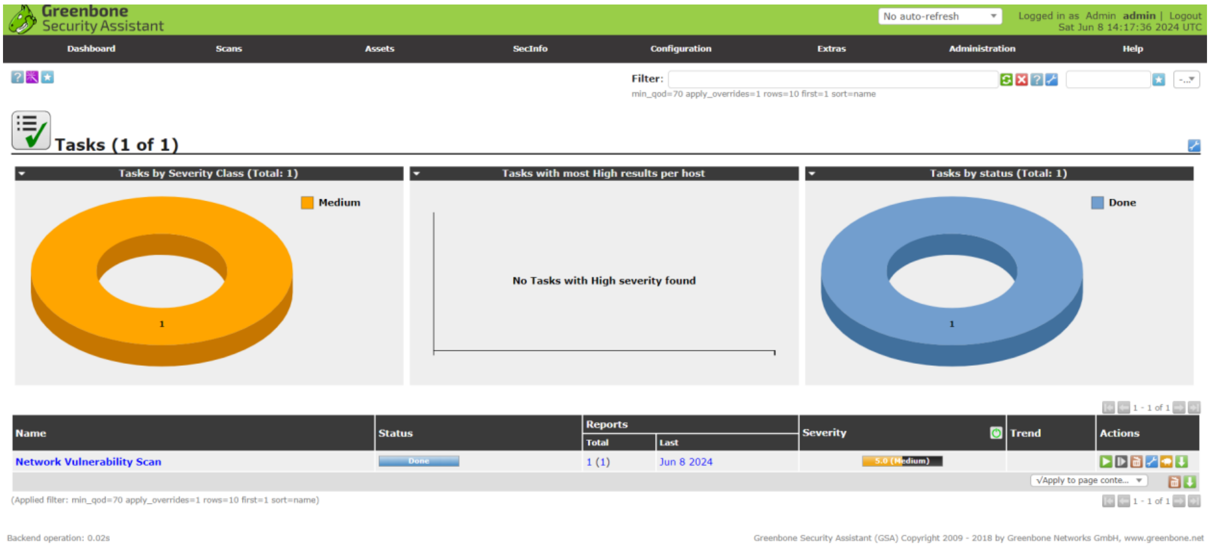
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Network Vulnerability Scan	New					

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

Backend operation: 0.01s

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

After completion of task


Greenbone
Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Sat Jun 8 14:17:36 2024 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter:
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
Medium
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
Done
1
1 - 1 of 1
√Apply to page conte...

min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

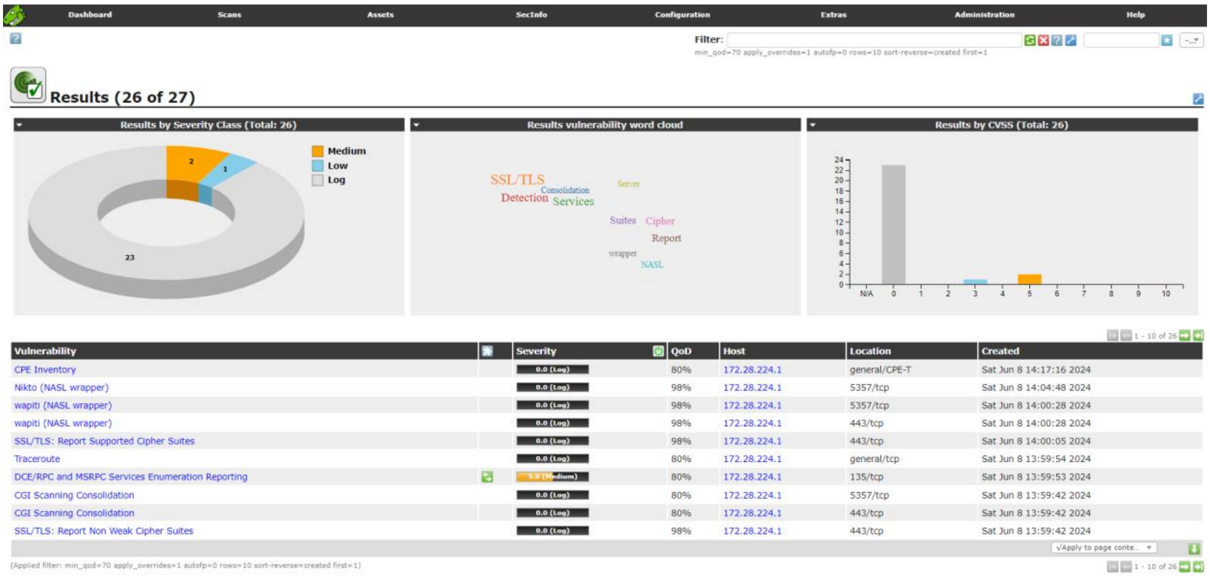
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Network Vulnerability Scan	Done	1 (1)	Jun 8 2024	5.0 (Medium)		

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

Backend operation: 0.02s

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

Network vulnerability scan result

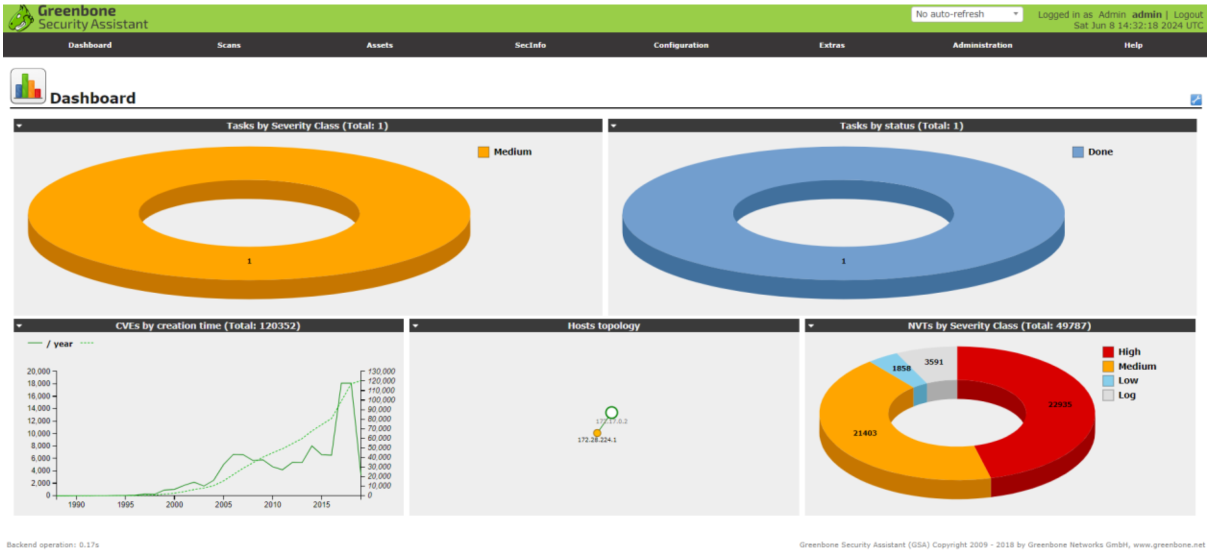


min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1

Vulnerability		Severity	QoD	Host	Location	Created
CPE Inventory		0.0 (Log)	80%	172.28.224.1	general/CPE-T	Sat Jun 8 14:17:16 2024
Nikto (NASL wrapper)		0.0 (Log)	98%	172.28.224.1	5357/tcp	Sat Jun 8 14:04:48 2024
wapiti (NASL wrapper)		0.0 (Log)	98%	172.28.224.1	5357/tcp	Sat Jun 8 14:00:28 2024
wapiti (NASL wrapper)		0.0 (Log)	98%	172.28.224.1	443/tcp	Sat Jun 8 14:00:28 2024
SSL/TLS: Report Supported Cipher Suites		0.0 (Log)	98%	172.28.224.1	443/tcp	Sat Jun 8 14:00:05 2024
Traceroute		0.0 (Log)	80%	172.28.224.1	general/tcp	Sat Jun 8 13:59:54 2024
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	172.28.224.1	135/tcp	Sat Jun 8 13:59:53 2024
CGI Scanning Consolidation		0.0 (Log)	80%	172.28.224.1	5357/tcp	Sat Jun 8 13:59:42 2024
CGI Scanning Consolidation		0.0 (Log)	80%	172.28.224.1	443/tcp	Sat Jun 8 13:59:42 2024
SSL/TLS: Report Non Weak Cipher Suites		0.0 (Log)	98%	172.28.224.1	443/tcp	Sat Jun 8 13:59:42 2024

(Applied filter: min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1)

Dashboard after vulnerability scan



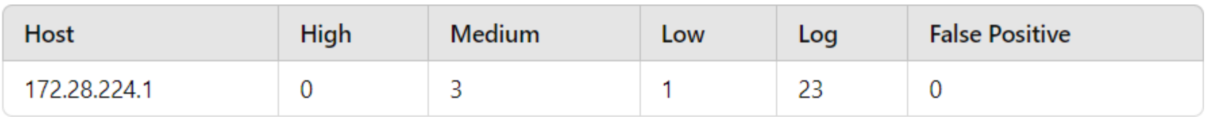
Logged in as Admin admin | Logout
Sat Jun 8 14:32:18 2024 UTC

Backend operation: 0.17s

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

3) Vulnerability Overview

3.1) Summary of Findings



Host	High	Medium	Low	Log	False Positive
172.28.224.1	0	3	1	23	0

4) Detailed Vulnerability Descriptions

4.1) DCE/RPC and MSRPC Services Enumeration

Port: 135/tcp

Description: The remote host allows enumeration of Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) and MSRPC services.

Impact: An attacker can gather information about services running on the host, which could be used to launch further attacks.

Solution: Filter incoming traffic on port 135 to block DCE/RPC and MSRPC enumeration.

4.2) TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Service: general/tcp

Description: The host is vulnerable to TCP sequence number approximation attacks, which can lead to denial of service.

Impact: Attackers can guess sequence numbers and terminate TCP connections, disrupting services.

Solution: Apply patches from the vendor and follow advisories to mitigate this vulnerability.

4.3) Expired SSL/TLS Certificate

Port: 443/tcp

Description: The SSL/TLS certificate for the remote server has expired.

Impact: An expired certificate can undermine the integrity and trust of secure communications.

Solution: Replace the expired certificate with a new, valid one.

4.4) TCP Timestamps

Service: general/tcp

Description: The remote host implements TCP timestamps, revealing the system's uptime.

Impact: The uptime information can assist attackers in crafting targeted attacks.

Solution: Disable TCP timestamps in the system configuration.

5) Mitigation Plan

5.1) DCE/RPC and MSRPC Services Enumeration

Step-by-Step Instructions:

1) Identify firewall rules allowing traffic on port 135.

2) Implement rules to block incoming traffic on this port.

3) Test to ensure services are unaffected.

Timeline: 1 week

Resources: Network administrator, firewall management tools.

5.2) TCP Sequence Number Approximation Reset DoS

Step-by-Step Instructions:

1) Review vendor advisories and apply relevant patches.
2) Monitor network traffic for signs of DoS attempts.
3) Configure TCP stack to mitigate risks.

Timeline: 2 weeks

Resources: Network security team, patch management tools.

5.3) Expired SSL/TLS Certificate

Step-by-Step Instructions:

1) Generate a new SSL/TLS certificate.
2) Install the new certificate on the server.
3) Verify the certificate installation and validity.

Timeline: Immediate

Resources: SSL certificate provider, server administrator.

5.4) TCP Timestamps

Step-by-Step Instructions:

1) Edit the system configuration file to disable TCP timestamps.
2) Apply the changes and reboot if necessary.
3) Verify that timestamps are disabled.

Timeline: 1 week

Resources: System administrator.

6) Final scan report

The final scan report generated by OpenVAS is attached below.