Module 05: Vulnerability Analysis

Scenario

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Objective

The objective of this lab is to extract information about the target system that includes, but not limited to:

- **Network vulnerabilities**
- **IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening**
- **Application and services configuration errors/vulnerabilities**
- **The OS version running on computers or devices**
- **Applications installed on computers**
- **Accounts with weak passwords**
- **Files and folders with weak permissions**
- **Default services and applications that may have to be uninstalled**
- **Mistakes in the security configuration of common applications**
- **Computers exposed to known or publicly reported vulnerabilities**

Overview of Vulnerability Assessment

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

1. **Perform vulnerability research with vulnerability scoring systems and databases**
    - **Perform vulnerability research in Common Weakness Enumeration (CWE)**
2. **Perform vulnerability assessment using various vulnerability assessment tools**
    - **Perform vulnerability analysis using OpenVAS**

Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- **Perform vulnerability research in Common Weakness Enumeration (CWE)**

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. By default, Windows 11 machine is selected, click Ctrl+Alt+Delete to activate the machine and login with Admin/Pa$$w0rd.

Networks screen appears, click Yes to allow your PC to be discoverable by other PCs and devices on the network.

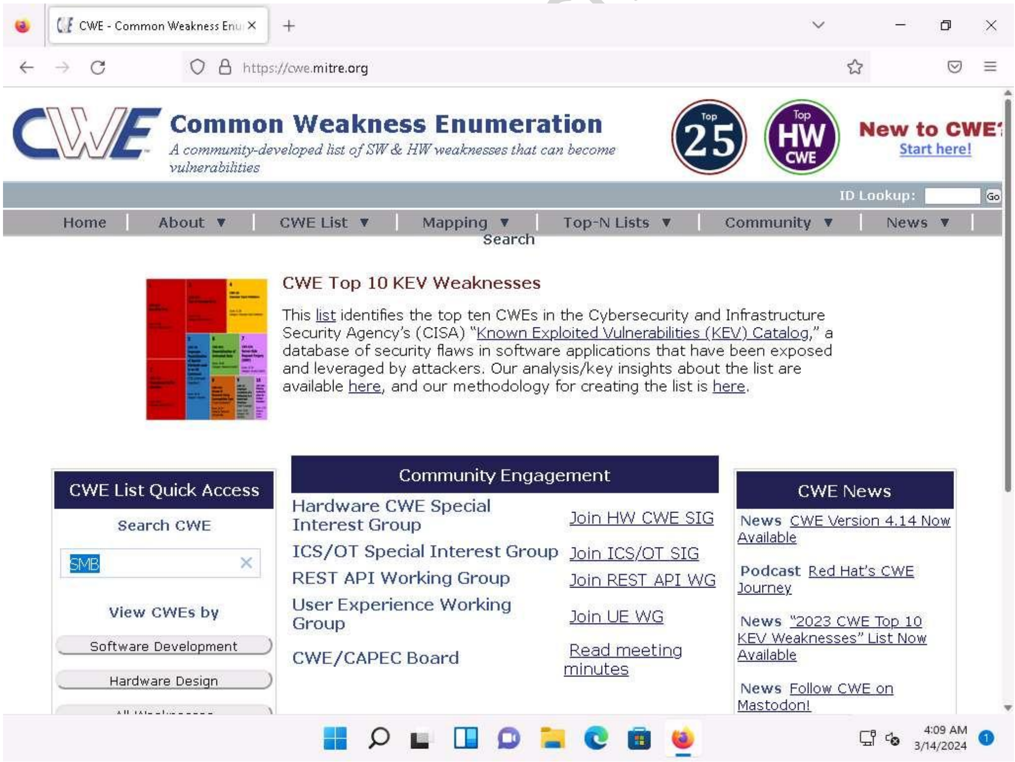
2. Launch any web browser, and go to https://cwe.mitre.org/ website (here, we are using Mozilla Firefox).

If the Default Browser pop-up window appears, uncheck the Always perform this check when starting Firefox checkbox and click the Not now button.

If a New in Firefox: Content Blocking pop-up window appears, follow the step and click start browsing to finish viewing the information.

3. CWE website appears. Navigate to Search tab, in the Google Custom Search under CWE List Quick Access section and search for SMB in the search field.

Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



CWE - Common Weakness Enu

https://cwe.mitre.org

Common Weakness Enumeration

A community-developed list of SW & HW weaknesses that can become vulnerabilities

New to CWE? Start here!

ID Lookup: Go

Home | About ▼ | CWE List ▼ | Mapping ▼ | Top-N Lists ▼ | Community ▼ | News ▼ | Search

CWE Top 10 KEV Weaknesses

This list identifies the top ten CWEs in the Cybersecurity and Infrastructure Security Agency's (CISA) "Known Exploited Vulnerabilities (KEV) Catalog," a database of security flaws in software applications that have been exposed and leveraged by attackers. Our analysis/key insights about the list are available here, and our methodology for creating the list is here.

CWE List Quick Access

Search CWE

SMB

View CWEs by

Software Development

Hardware Design

Community Engagement

Hardware CWE Special Interest Group	Join HW CWE SIG
ICS/OT Special Interest Group	Join ICS/OT SIG
REST API Working Group	Join REST API WG
User Experience Working Group	Join UE WG
CWE/CAPEC Board	Read meeting minutes

CWE News

News CWE Version 4.14 Now Available

Podcast Red Hat's CWE Journey

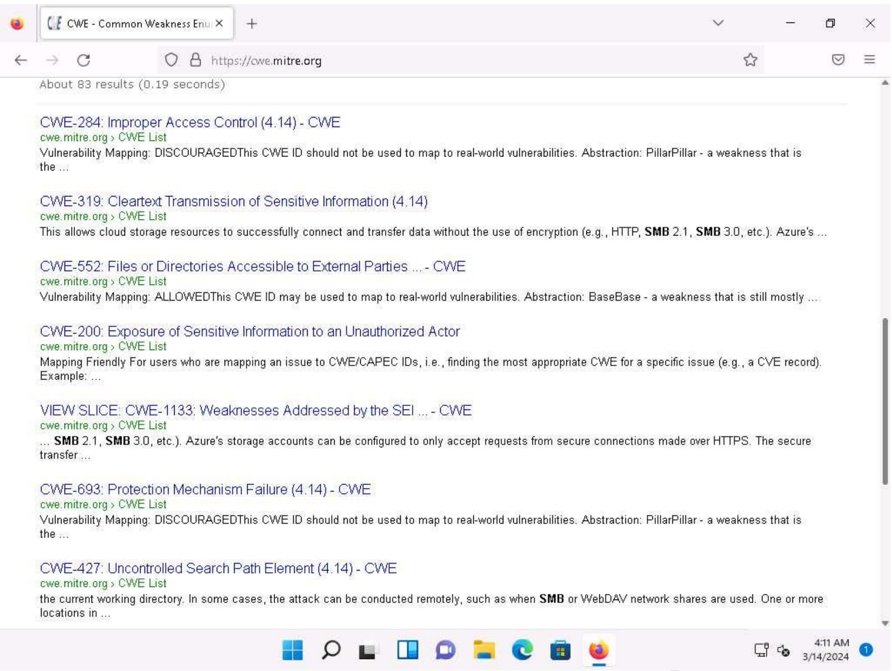
News "2023 CWE Top 10 KEV Weaknesses" List Now Available

News Follow CWE on Mastodon!

4:09 AM 3/14/2024

4. The search results appear, scroll-down to view the underlying vulnerabilities in the target service (here, SMB). You can click any link to view detailed information on the vulnerability.

The search results might differ when you perform this task



About 83 results (0.19 seconds)

CWE-284: Improper Access Control (4.14) - CWE
cwe.mitre.org › CWE List
Vulnerability Mapping: DISCOURAGEDThis CWE ID should not be used to map to real-world vulnerabilities. Abstraction: PillarPillar - a weakness that is the ...

CWE-319: Cleartext Transmission of Sensitive Information (4.14)
cwe.mitre.org › CWE List
This allows cloud storage resources to successfully connect and transfer data without the use of encryption (e.g., HTTP, **SMB** 2.1, **SMB** 3.0, etc.). Azure's ...

CWE-552: Files or Directories Accessible to External Parties ... - CWE
cwe.mitre.org › CWE List
Vulnerability Mapping: ALLOWEDThis CWE ID may be used to map to real-world vulnerabilities. Abstraction: BaseBase - a weakness that is still mostly ...

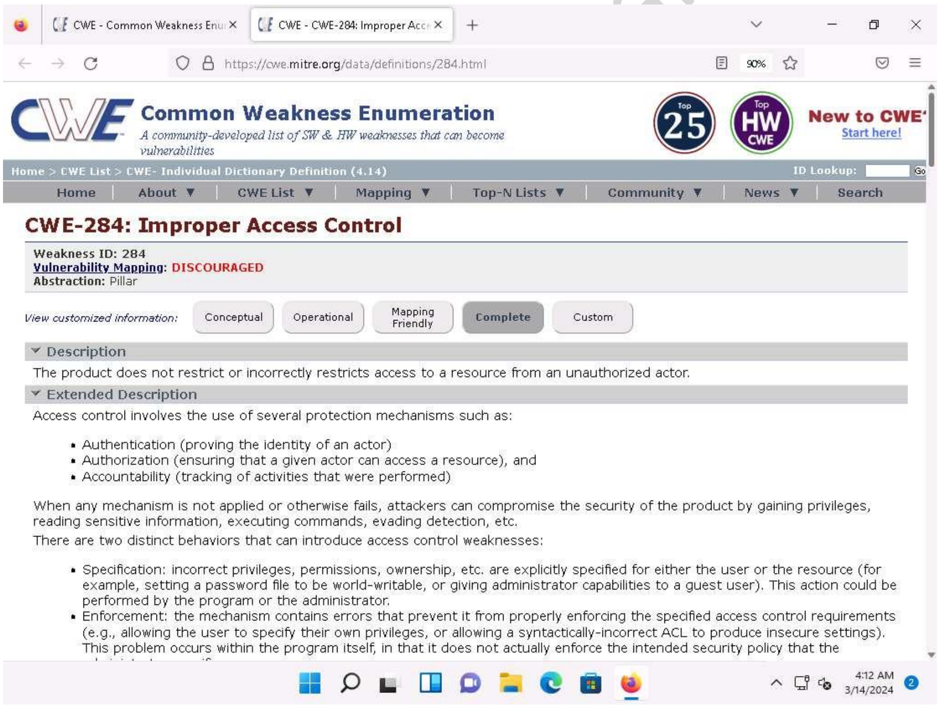
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...

VIEW SLICE: CWE-1133: Weaknesses Addressed by the SEI ... - CWE
cwe.mitre.org › CWE List
... **SMB** 2.1, **SMB** 3.0, etc.). Azure's storage accounts can be configured to only accept requests from secure connections made over HTTPS. The secure transfer ...

CWE-693: Protection Mechanism Failure (4.14) - CWE
cwe.mitre.org › CWE List
Vulnerability Mapping: DISCOURAGEDThis CWE ID should not be used to map to real-world vulnerabilities. Abstraction: PillarPillar - a weakness that is the ...

CWE-427: Uncontrolled Search Path Element (4.14) - CWE
cwe.mitre.org › CWE List
the current working directory. In some cases, the attack can be conducted remotely, such as when **SMB** or WebDAV network shares are used. One or more locations in ...

5. Now, click any link (here, CWE-284) to view detailed information about the vulnerability.


CWE - Common Weakness Enu
CWE - CWE-284: Improper Acc
https://cwe.mitre.org/data/definitions/284.html
90%
Common Weakness Enumeration
A community-developed list of SW & HW weaknesses that can become vulnerabilities
Top 25
Top HW CWE
New to CWE?
Start here!
Home > CWE List > CWE- Individual Dictionary Definition (4.14)
ID Lookup:
Go
Home
About ▼
CWE List ▼
Mapping ▼
Top-N Lists ▼
Community ▼
News ▼
Search

CWE-284: Improper Access Control

Weakness ID: 284
Vulnerability Mapping: DISCOURAGED
Abstraction: Pillar

View customized information:
Conceptual
Operational
Mapping Friendly
Complete
Custom

▼ Description

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

▼ Extended Description

Access control involves the use of several protection mechanisms such as:

- Authentication (proving the identity of an actor)
- Authorization (ensuring that a given actor can access a resource), and
- Accountability (tracking of activities that were performed)

When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

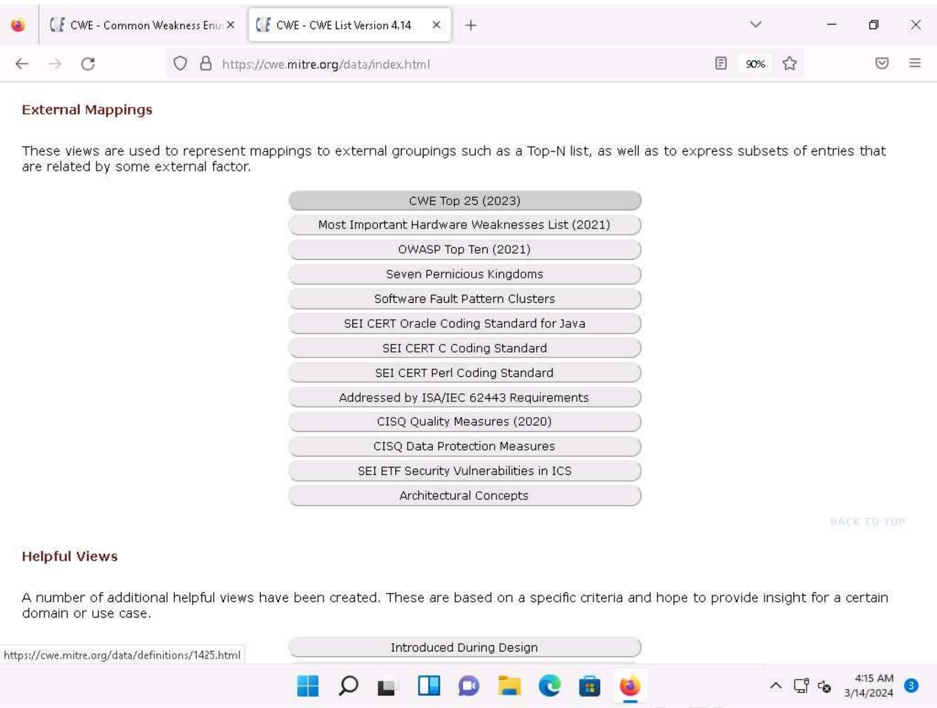
There are two distinct behaviors that can introduce access control weaknesses:

- Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.
- Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the

6. Similarly, you can click on other vulnerabilities and view detailed information.

7. Now, navigate to the CWE List tab. CWE List Version will be displayed. Scroll down, and under the External Mappings section, select CWE Top 25 (2023).

The result might differ when you perform this task.



CWE - Common Weakness Enu
CWE - CWE List Version 4.14
https://cwe.mitre.org/data/index.html
90%

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor.

- CWE Top 25 (2023)
- Most Important Hardware Weaknesses List (2021)
- OWASP Top Ten (2021)
- Seven Pernicious Kingdoms
- Software Fault Pattern Clusters
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT Perl Coding Standard
- Addressed by ISA/IEC 62443 Requirements
- CISQ Quality Measures (2020)
- CISQ Data Protection Measures
- SEI ETF Security Vulnerabilities in ICS
- Architectural Concepts

BACK TO TOP

Helpful Views

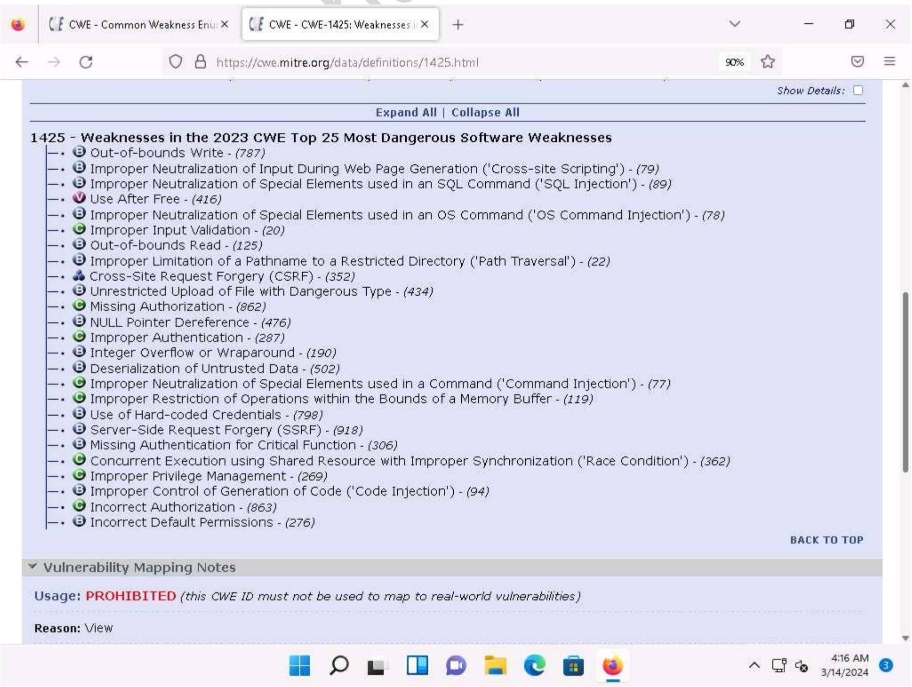
A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight for a certain domain or use case.

- Introduced During Design

8. A webpage appears, displaying CWE VIEW: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses. Scroll down and view a list of Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses under the Relationships section. You can check each weakness to view detailed information on it.

This information can be used to exploit the vulnerabilities in the software and further launch attacks.

The result showing publishing year might differ when you perform this task.



CWE - Common Weakness Enu
CWE - CWE-1425: Weaknesses i
https://cwe.mitre.org/data/definitions/1425.html
90%
Show Details: □
Expand All | Collapse All

1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses
- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Input Validation - *(20)*
- Out-of-bounds Read - *(125)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Missing Authorization - *(862)*
- NULL Pointer Dereference - *(476)*
- Improper Authentication - *(287)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Use of Hard-coded Credentials - *(798)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Missing Authentication for Critical Function - *(306)*
- Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - *(362)*
- Improper Privilege Management - *(269)*
- Improper Control of Generation of Code ('Code Injection') - *(94)*
- Incorrect Authorization - *(863)*
- Incorrect Default Permissions - *(276)*

BACK TO TOP

Vulnerability Mapping Notes

Usage: PROHIBITED *(this CWE ID must not be used to map to real-world vulnerabilities)*

Reason: View

9. Similarly, you can go back to the CWE website and explore other options, as well.

10. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.

11. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).

12. Close all open windows and document all the acquired information.

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- **Perform vulnerability analysis using OpenVAS**

Overview of Vulnerability Assessment

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

There are two approaches to network vulnerability scanning:

- Active Scanning
- Passive Scanning

Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Here, we will perform a vulnerability analysis using OpenVAS.

In this task, we will use the Parrot Security (10.10.1.13) machine as a host machine and the Windows Server 2022 (10.10.1.22) machine as a target machine.

1. Click on Parrot Security to switch to the Parrot Security machine and login with attacker/toor.

If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

If a Question pop-up window appears asking you to update the machine, click No to close the window.

2. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

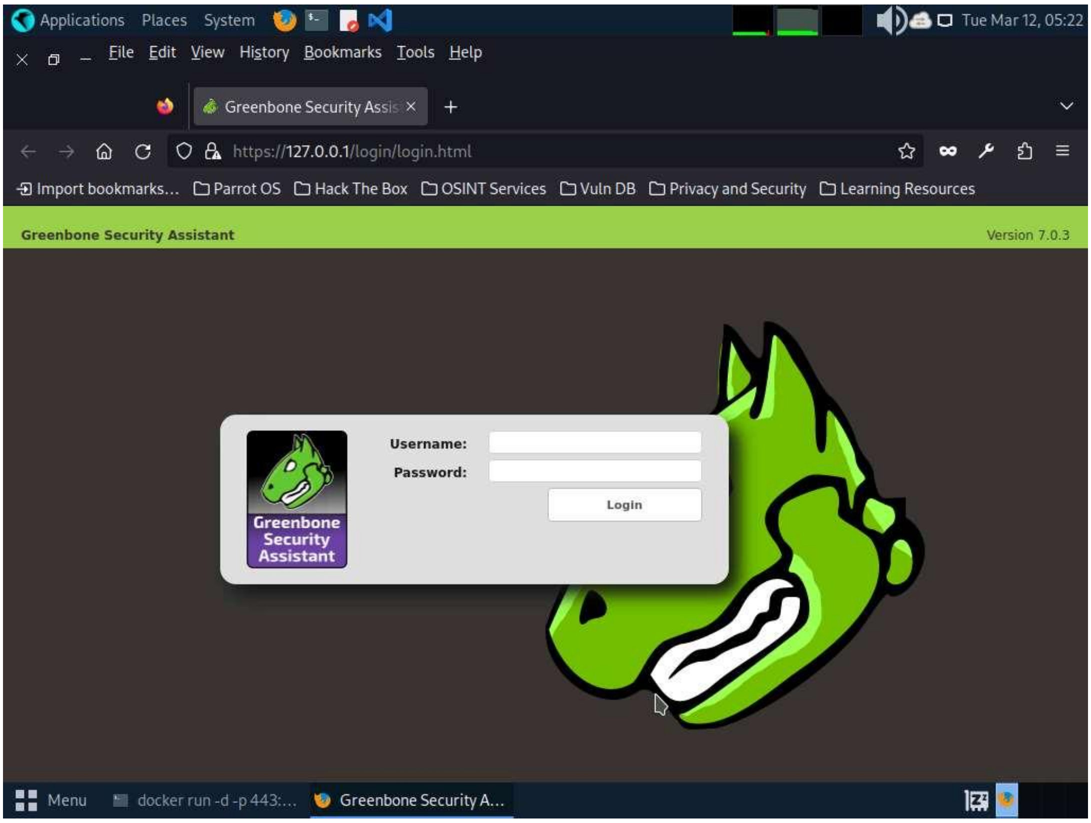
The password that you type will not be visible.

3. Run **docker run -d -p 443:443 –-name openvas mikesplain/openvas** command to launch OpenVAS.

4. After the tool initializes, click Firefox icon from the top-section of the Desktop.

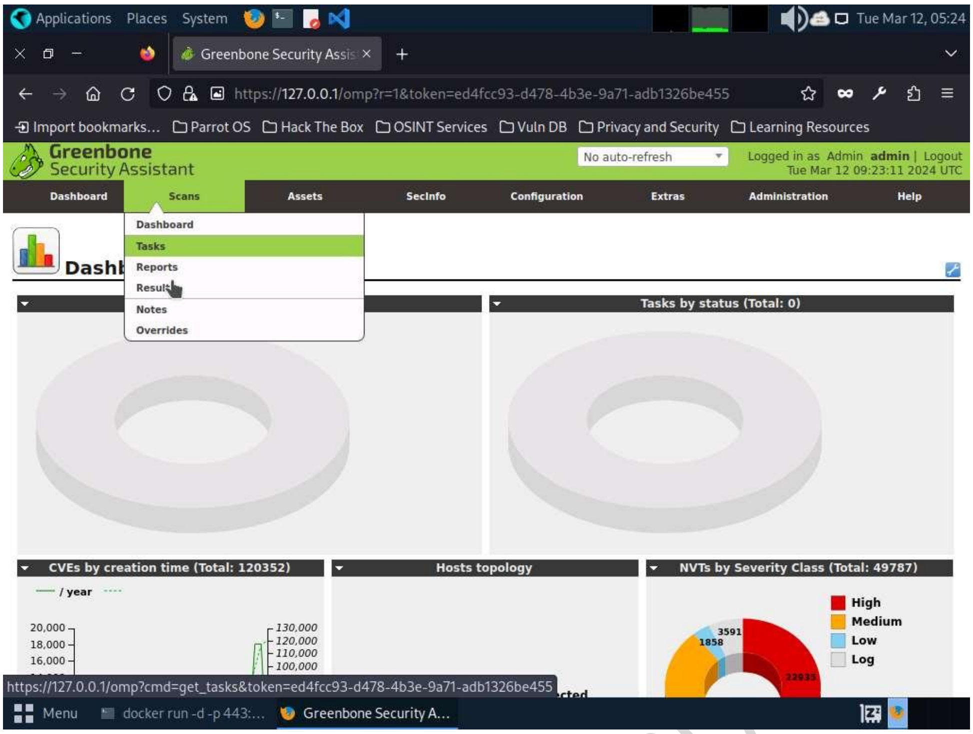
5. The Firefox browser appears, go **to https://127.0.0.1/. OpenVAS** login page appears, log in with admin/admin.

If a Warning page appears, click Advanced and select Accept the Risk and Continue.


Applications Places System
Tue Mar 12, 05:22
File Edit View History Bookmarks Tools Help
Greenbone Security Assis
https://127.0.0.1/login/login.html
Import bookmarks… Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Greenbone Security Assistant
Version 7.0.3
Greenbone Security Assistant
Username:
Password:
Login
Menu
docker run -d -p 443:…
Greenbone Security A…

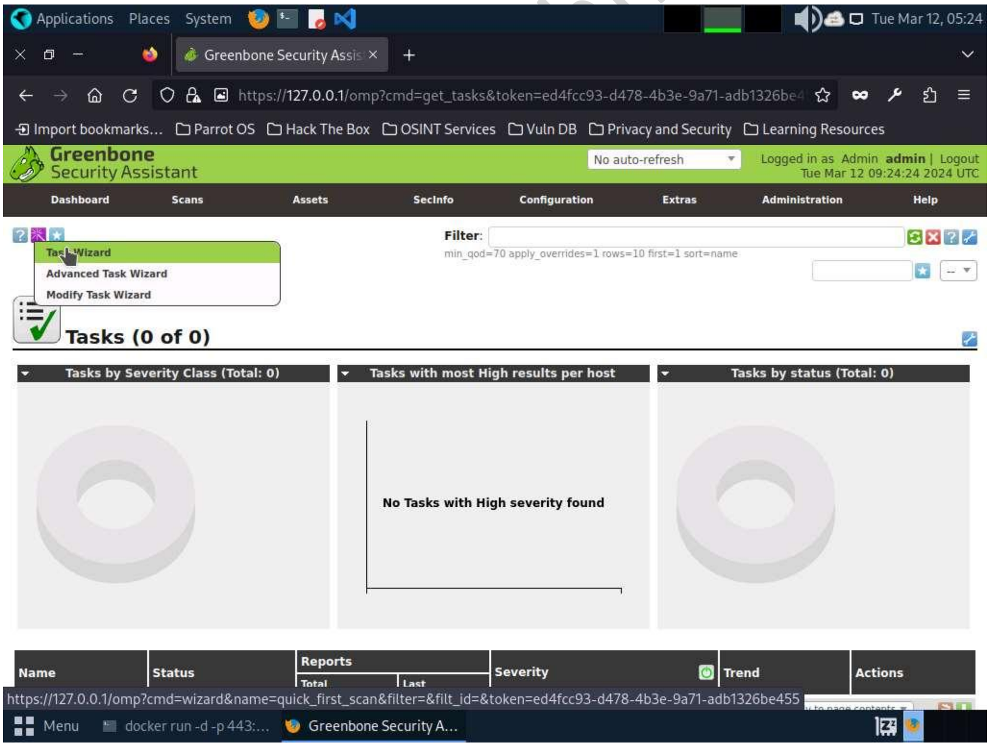
6. The OpenVAS Dashboards appears. Navigate to Scans --> Tasks from the Menu bar.

If a Welcome to the scan task management! pop-up appears, close it.



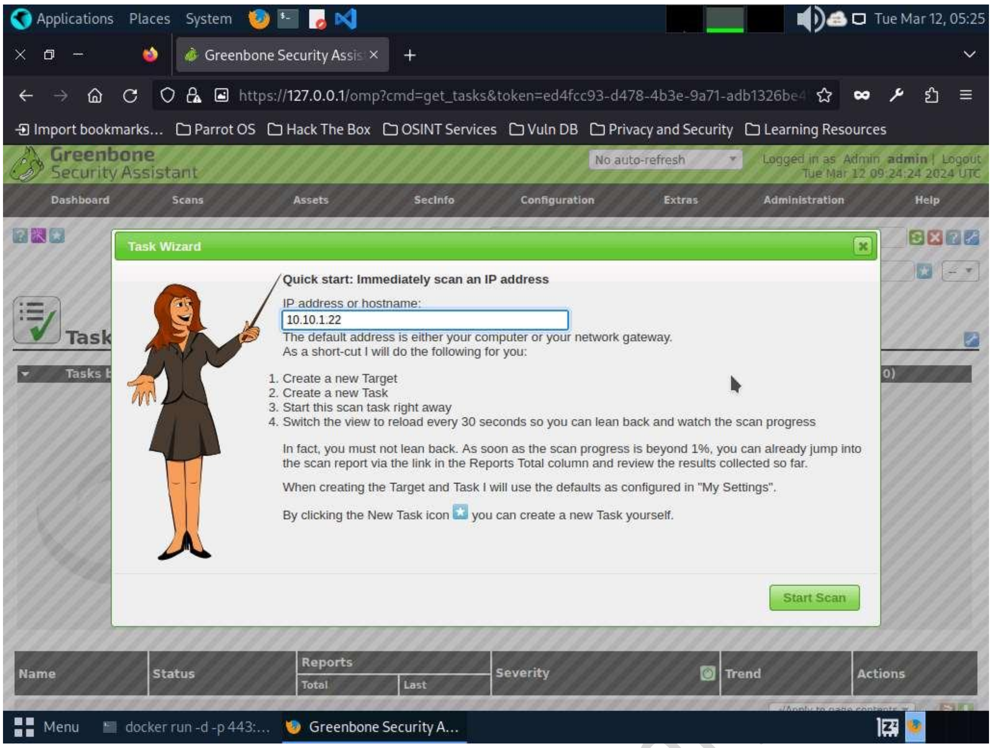
Applications Places System
Tue Mar 12, 05:24
Greenbone Security Assis
https://127.0.0.1/omp?r=1&token=ed4fcc93-d478-4b3e-9a71-adb1326be455
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Mar 12 09:23:11 2024 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Dashboard
Tasks
Reports
Results
Notes
Overrides
Dashb
Tasks by status (Total: 0)
CVEs by creation time (Total: 120352)
/ year
20,000
18,000
16,000
130,000
120,000
110,000
100,000
Hosts topology
NVTs by Severity Class (Total: 49787)
3591
1858
22033
High
Medium
Low
Log
https://127.0.0.1/omp?cmd=get_tasks&token=ed4fcc93-d478-4b3e-9a71-adb1326be455
Menu docker run -d -p 443:... Greenbone Security A...

7. Hover over wand icon and click the Task Wizard option.



Applications Places System
Tue Mar 12, 05:24
Greenbone Security Assis
https://127.0.0.1/omp?cmd=get_tasks&token=ed4fcc93-d478-4b3e-9a71-adb1326be4
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Mar 12 09:24:24 2024 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (0 of 0)
Tasks by Severity Class (Total: 0)
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 0)
Name Status Reports Total Last Severity Trend Actions
https://127.0.0.1/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=ed4fcc93-d478-4b3e-9a71-adb1326be455
Menu docker run -d -p 443:... Greenbone Security A...

8. The Task Wizard window appears; enter the target IP address in the IP address or hostname field (here, the target system is Windows Server 2022 [10.10.1.22]) and click the Start Scan button.



Applications Places System
Tue Mar 12, 05:25
Greenbone Security Assis
https://127.0.0.1/omp?cmd=get_tasks&token=ed4fcc93-d478-4b3e-9a71-adb1326be4
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Tue Mar 12 09:24:24 2024 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 10.10.1.22

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

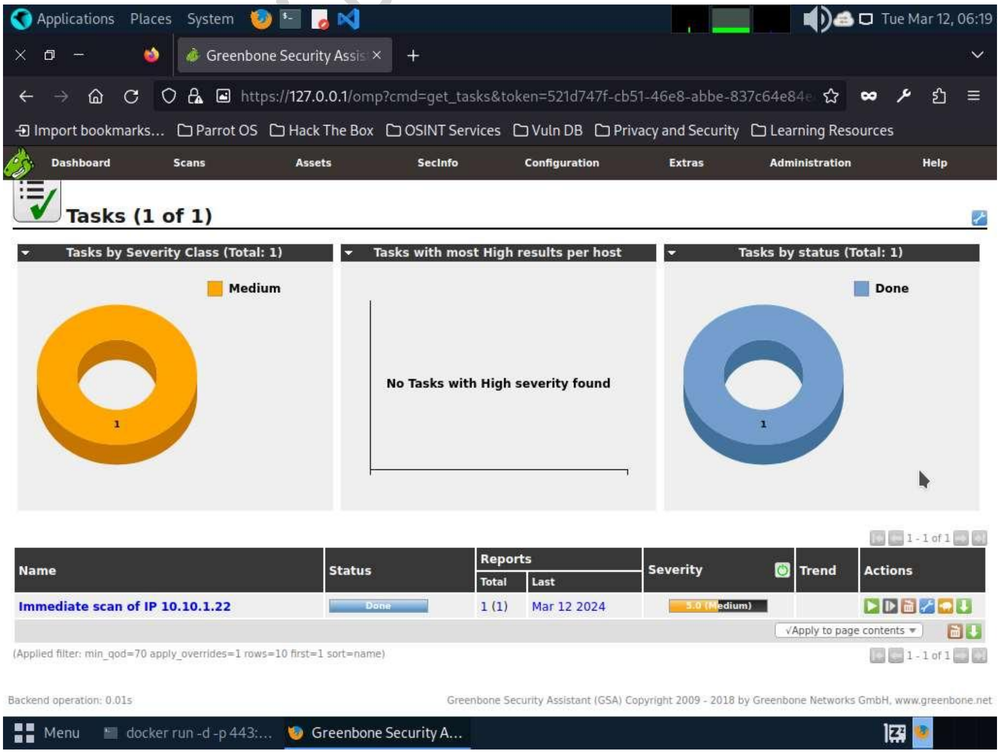
Start Scan
Name Status Reports Total Last Severity Trend Actions
Menu docker run -d -p 443:... Greenbone Security A...

9. The task appears under the Tasks section; OpenVAS starts scanning the target IP address.

10. Wait for the Status to change from Requested to Done. Once it is completed, click the Done button under the Status column to view the vulnerabilities found in the target system.

It takes approximately 20 minutes for the scan to complete.

If you are logged out of the session then login again using credentials admin/admin.



Applications Places System
Tue Mar 12, 06:19
Greenbone Security Assis
https://127.0.0.1/omp?cmd=get_tasks&token=521d747f-cb51-46e8-abbe-837c64e84
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
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

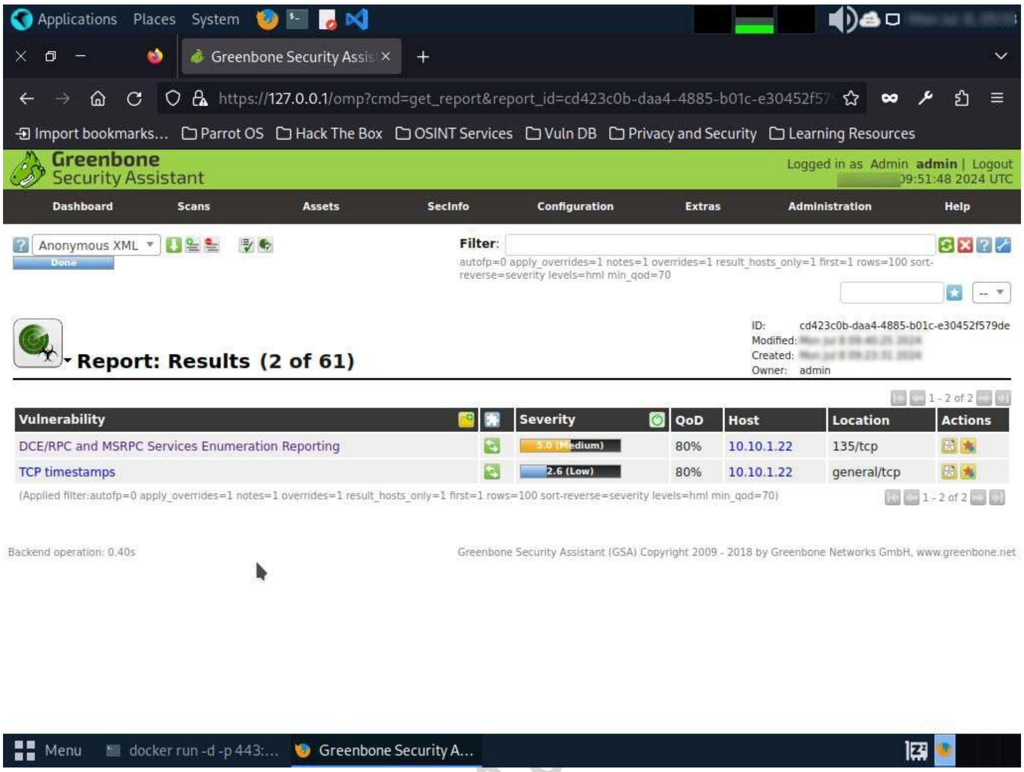
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 10.10.1.22	Done	1 (1)	Mar 12 2024	5.0 (Medium)		

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

√Apply 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
Menu docker run -d -p 443:... Greenbone Security A...

11. Report: Results appear, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

The results might differ when you perform this task.



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 (2 of 61)

ID: cd423c0b-daa4-4885-b01c-e30452f579de
Modified: [redacted]
Created: [redacted]
Owner: admin

1 - 2 of 2

Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.1.22	135/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.1.22	general/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)

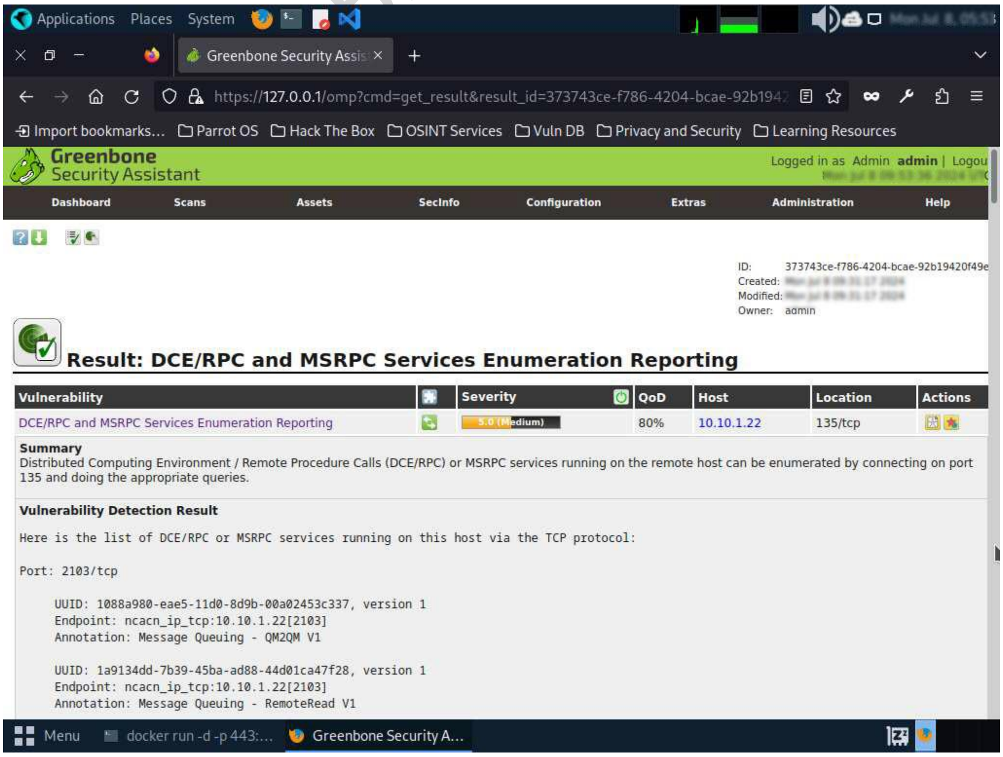
1 - 2 of 2

Backend operation: 0.40s

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

12. Click on any vulnerability under the Vulnerability column to view its detailed information.

13. Detailed information regarding selected vulnerability appears, as shown in the screenshot.



ID: 373743ce-f786-4204-bcae-92b19420f49e
Created: [redacted]
Modified: [redacted]
Owner: admin

Result: DCE/RPC and MSRPC Services Enumeration Reporting

Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.1.22	135/tcp	

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 2103/tcp

     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:10.10.1.22[2103]
     Annotation: Message Queuing - QM2QM V1

     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:10.10.1.22[2103]
     Annotation: Message Queuing - RemoteRead V1
```

14. Similarly, you can check other Reports by hovering over the Report: Results section to view other Reports regarding the vulnerabilities in the target system.

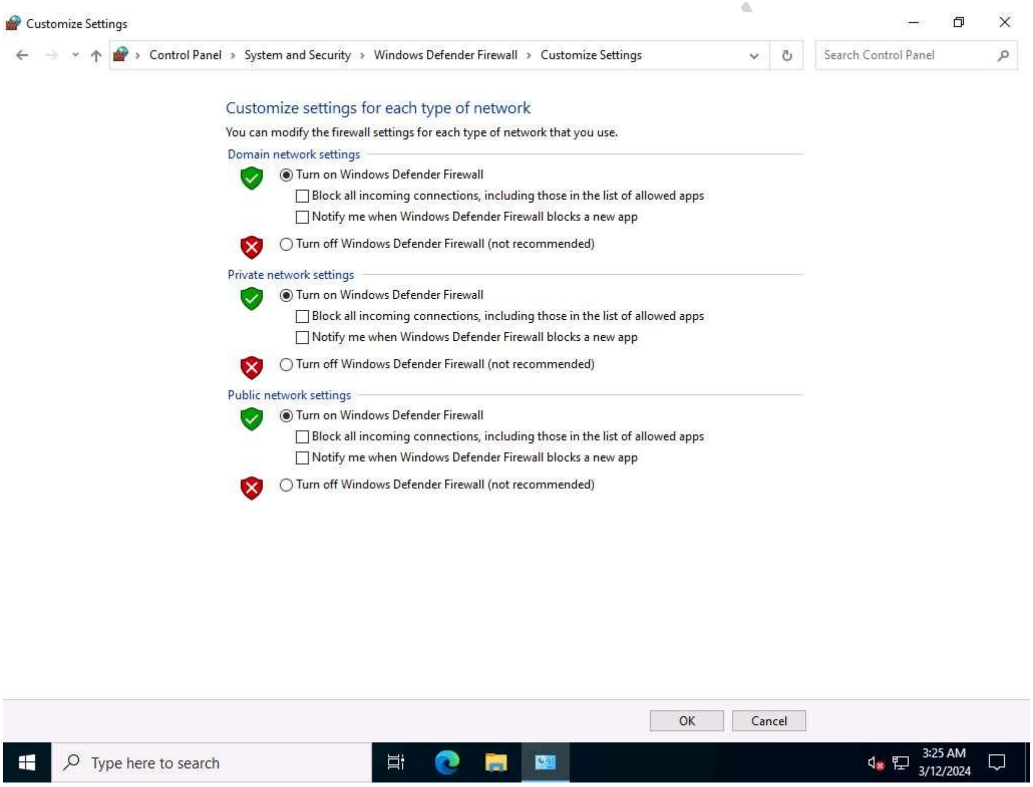
15. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your firewall ON in the Windows Server 2022 machine.

16. Now, we will enable Windows Firewall in the target system and scan it for vulnerabilities.

17. Click on Windows Server 2022 to switch to the Windows Server 2022 machine and click Ctrl+Alt+Delete and login with CEH\Administrator / Pa$$w0rd.

18. Navigate to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, enable Windows Firewall, and click OK.

By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.



Customize Settings

Control Panel › System and Security › Windows Defender Firewall › Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

19. Click on [Parrot Security]() to switch to Parrot Security machine and perform Steps# 7-9 to create another task for scanning the target system.

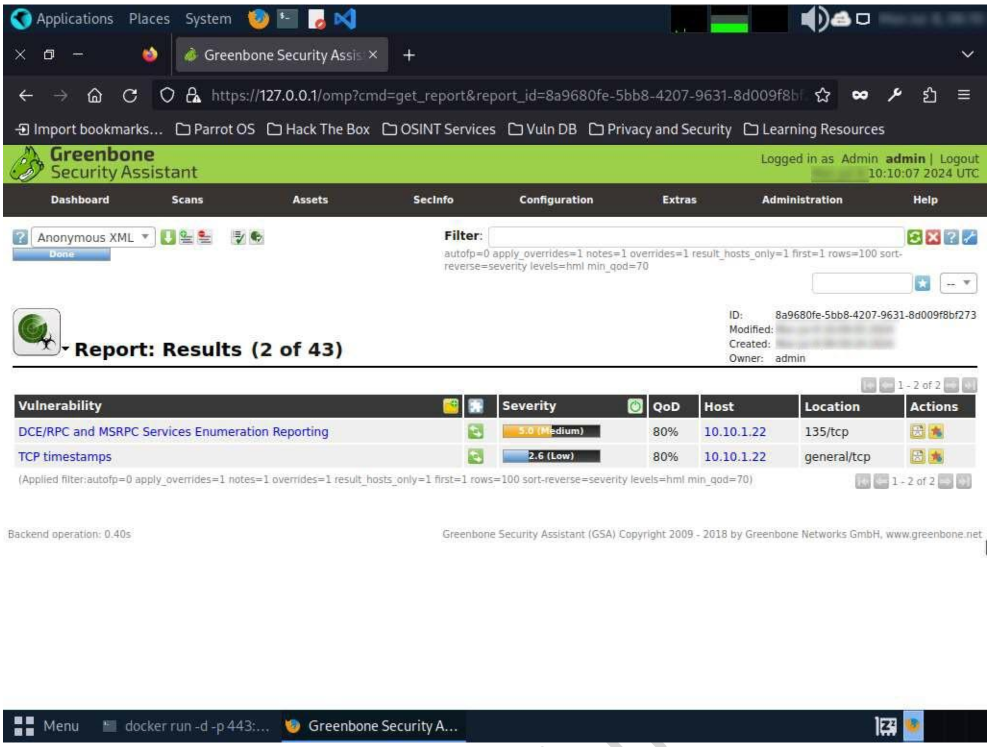
20. A newly created task appears under the Tasks section and starts scanning the target system for vulnerabilities.

21. After the completion of the scan, click the Done button under the Status column.

It takes approximately 15-20 minutes for the scan to complete.

22. Report: Results appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

The results might differ when you perform this task.



Logged in as Admin **admin** | Logout
[redacted] 10:10:07 2024 UTC

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 (2 of 43)

ID: 8a9680fe-5bb8-4207-9631-8d009f8bf273
Modified: [redacted]
Created: [redacted]
Owner: admin

1 - 2 of 2

Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.1.22	135/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.1.22	general/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 - 2 of 2

Backend operation: 0.40s

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

23. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.

24. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.

25. Close all open windows and document all the acquired information.

26. Click on Windows Server 2022 to switch to the Windows Server 2022 machine and click Ctrl+Alt+Delete login with Administrator/Pa$$w0rd.

27. Navigate to Control Panel --> System and Security --> Windows Defender Firewall --> Turn Windows Defender Firewall on or off, disable Windows Firewall, and click OK.