

# **Institute of Information Technology (IIT)**

## **Jahangirnagar University**



### **EDGE- B11 Cyber Security.**

#### **Assignment No 4:**

Vulnerability Assessment & Port Scanning using ZenMap and Nessus

#### **Submitted By**

Name: Sidratul Afrida

ID No: 2111263

Batch No: 11

#### **Submitted To**

Moinoddeen Quader Al Arabi

Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber  
Security Consultant in Dhaka Division, Bangladesh

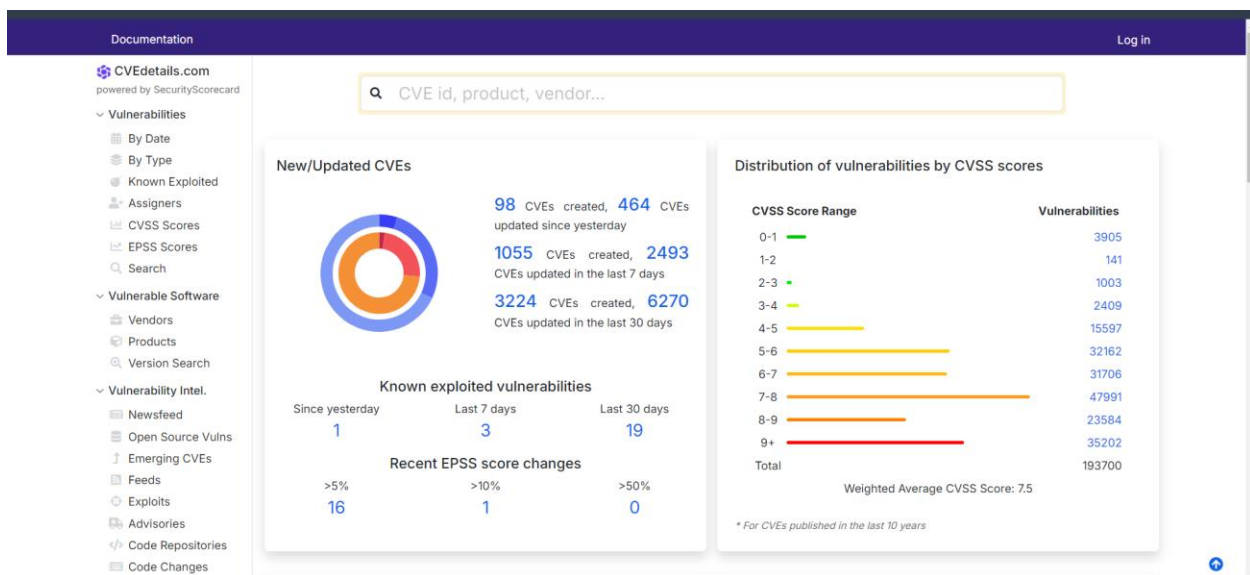
# Vulnerability Analysis and Research using Online Database:

## Understanding the Vulnerability Landscape:

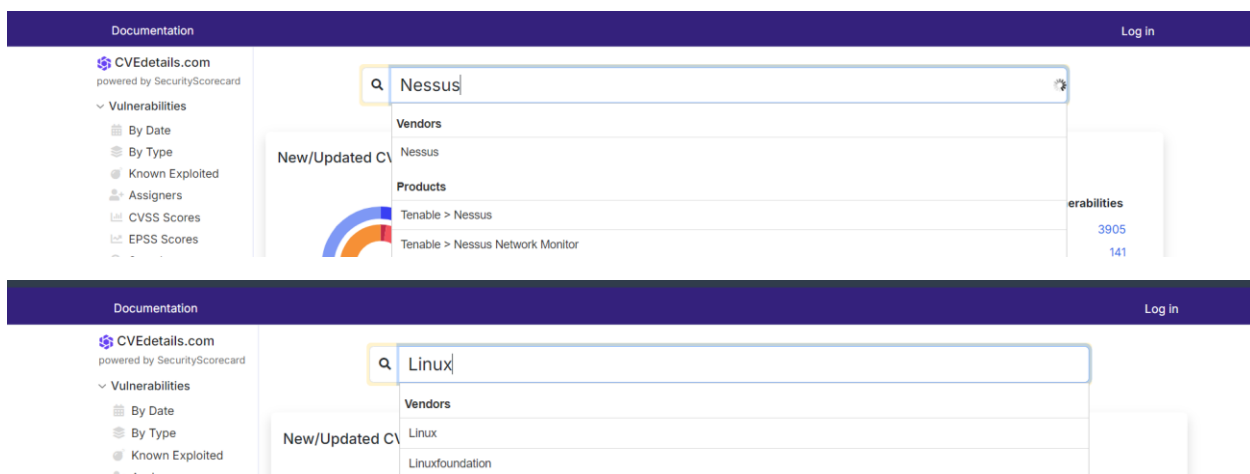
### Online Database:

**CVEdetails:** CVEDetails is a platform that provides detailed information about publicly known cybersecurity vulnerabilities, known as Common Vulnerabilities and Exposures (CVEs). It aggregates data from sources like the National Vulnerability Database (NVD) and CVE.org, offering insights into vulnerabilities, associated exploits, risk scores, and related advisories. Users can search for CVEs by products, vendors, or vulnerability types, making it easier to assess and manage potential security risks. The site also presents metrics like CVSS scores and trends over time to help organizations prioritize vulnerability management.

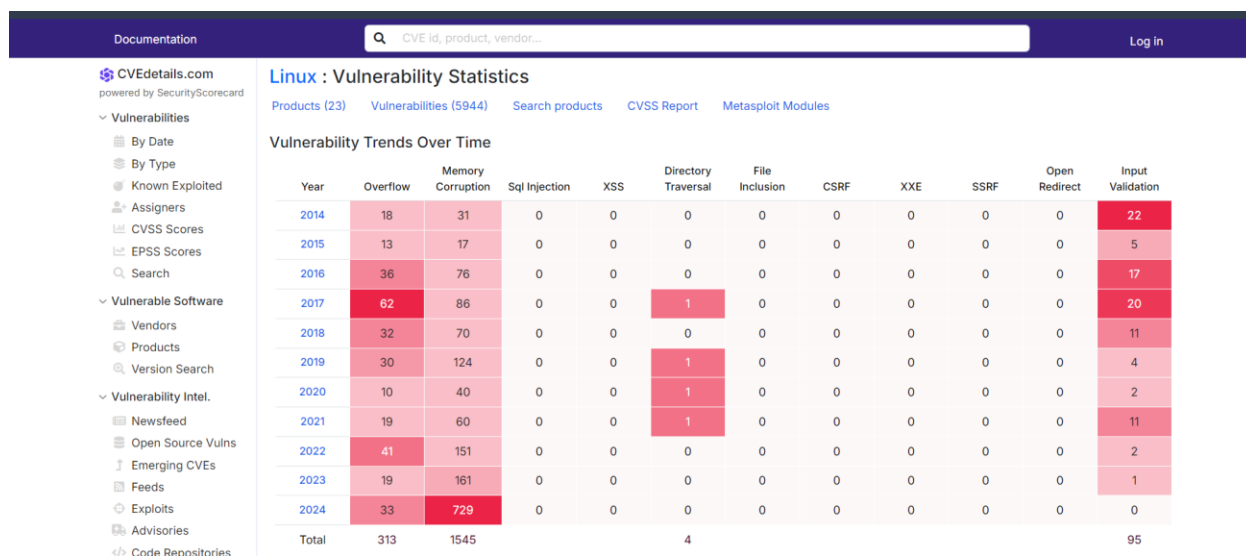
Link: <https://www.cvedetails.com/>



There has option for search any product, vendor etc.

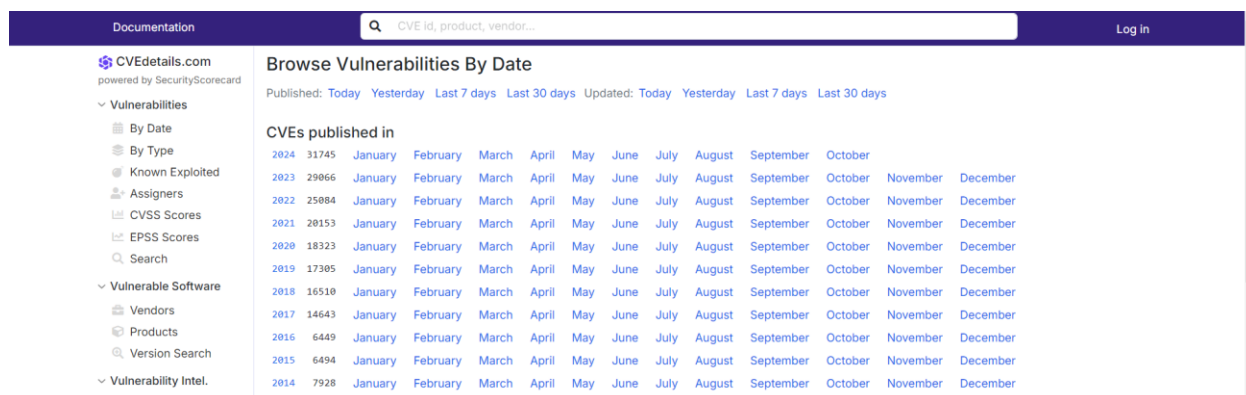


Here details of vulnerability is show until present month of the Year:



We can search by date, type.

Result of search by Date:



Today's vulnerability (Green is good condition, orange is for risk medium and red for high risk of Base Severity):

Documentation

CVEdetails.com

powered by SecurityScorecard

Vulnerabilities

By Date

By Type

Known Exploited

Assigners

CVSS Scores

EPSS Scores

Search

Vulnerable Software

Vendors

Products

Version Search

Vulnerability Intel.

Newsfeed

Open Source Vulns

Emerging CVEs

Feeds

Q

CVE id, product, vendor...

Log in

Security Vulnerabilities, CVEs Published In October 2024

Published In:

≡

2024

January

February

March

April

May

June

July

August

September

October

CVSS Scores Greater Than:

0 1 2 3 4 5 6 7 8 9

In CISA KEV Catalog

Sort Results By :

Publish Date

Update Date

CVE Number

CVE Number

CVSS Score

EPSS Score

Page: 1

>

Copy

CVE-2024-50312

A vulnerability was found in GraphQL due to improper access controls on the GraphQL introspection query. This flaw allows unauthorized users to retrieve a comprehensive list of available queries and mutations. Exposure to this flaw increases the attack surface, as it can facilitate the discovery of flaws or errors specific to the application's GraphQL implementation.

Source: Red Hat, Inc.

Max CVSS

5.3

EPSS Score

0.05%

Published

2024-10-22

Updated

2024-10-22

CVE-2024-50311

A denial of service (DoS) vulnerability was found in OpenShift. This flaw allows attackers to exploit the GraphQL batching functionality. The vulnerability arises when multiple queries can be sent within a single request, enabling an attacker to submit a request containing thousands of aliases in one query. This issue causes excessive resource consumption, leading to application unavailability for legitimate users.

Source: Red Hat, Inc.

Max CVSS

6.5

EPSS Score

0.1%

Published

2024-10-22

Updated

2024-10-22

**NVD:** The National Vulnerability Database (NVD) is a U.S. government repository of standards-based vulnerability management data. Managed by the National Institute of Standards and Technology (NIST), NVD enhances CVE vulnerability data by adding details like severity scores, impact ratings, and fix information. It helps organizations prioritize vulnerabilities and guides them in applying appropriate security patches or mitigations. NVD also includes tools for searching and analyzing vulnerabilities, making it a crucial resource for cybersecurity professionals to manage threats effectively.

- |                       |   |
|-----------------------|---|
| General               | + |
| Vulnerabilities       | + |
| Vulnerability Metrics | + |
| Products              | + |
| Developers            | + |
| Contact NVD           |   |
| Other Sites           | + |
| Search                | + |



**New Communications Page**



## CVSS v4.0 Support



## 2.0 APIs

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics.

<https://nvd.nist.gov>

## VULNERABILITIES

## 🚧 CVE-2024-47675 Detail

### Description





In the Linux kernel, the following vulnerability has been resolved: bpf: Fix use-after-free in bpf\_uprobe\_multi\_link\_attach() If bpf\_link\_prime() fails, bpf\_uprobe\_multi\_link\_attach() goes to the error\_free label and frees the array of bpf\_uprobe's without calling bpf\_uprobe\_unregister(). This leaks bpf\_uprobe->uprobe and worse, this frees bpf\_uprobe->consumer without removing it from the uprobe->consumers list.

## Metrics

CVSS Version 4.0	CVSS Version 3.x	CVSS Version 2.0
------------------	------------------	------------------

CVSS Version 2.0

these sites. Please address comments about this page to [nyu@nsl.gov](mailto:nyu@nsl.gov).

Hyperlink	Resource
<a href="https://git.kernel.org/stable/c/5fe6e308abaea082c0f2ba5df8e14495622cf">https://git.kernel.org/stable/c/5fe6e308abaea082c0f2ba5df8e14495622cf</a>	 Patch
<a href="https://git.kernel.org/stable/c/790c630ab0e7d7aba6186581d4627c09cf0e6f3">https://git.kernel.org/stable/c/790c630ab0e7d7aba6186581d4627c09cf0e6f3</a>	 Patch
<a href="https://git.kernel.org/stable/c/7c1d782e5afb7f50ba74ecc4ddc18a05d63ee5e">https://git.kernel.org/stable/c/7c1d782e5afb7f50ba74ecc4ddc18a05d63ee5e</a>	 Patch
<a href="https://git.kernel.org/stable/c/cdf127834cd3dd59abf7eb8e4ee87ee9e307eb25c">https://git.kernel.org/stable/c/cdf127834cd3dd59abf7eb8e4ee87ee9e307eb25c</a>	 Patch

## Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-416	Use After Free	NIST

### Known Affected Software Configurations [Switch to CPE 2.2](#)

**Configuration 1** ([hide](#))

✖ cpe:2.3:linux:linux_kernel:*:*:*:*:*:*	From (including)	Up to (excluding)
<a href="#">Show Matching CPE(s)▼</a>	6.6	6.6.54
✖ cpe:2.3:linux:linux_kernel:*:*:*:*:*:*	From (including)	Up to (excluding)
<a href="#">Show Matching CPE(s)▼</a>	6.7	6.10.13
✖ cpe:2.3:linux:linux_kernel:*:*:*:*:*:*	From (including)	Up to (excluding)
<a href="#">Show Matching CPE(s)▼</a>	6.11	6.11.2

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

## QUICK INFO

**CVE Dictionary Entry:**

CVE-2024-47675

## NVD Published Date:

10/21/2024

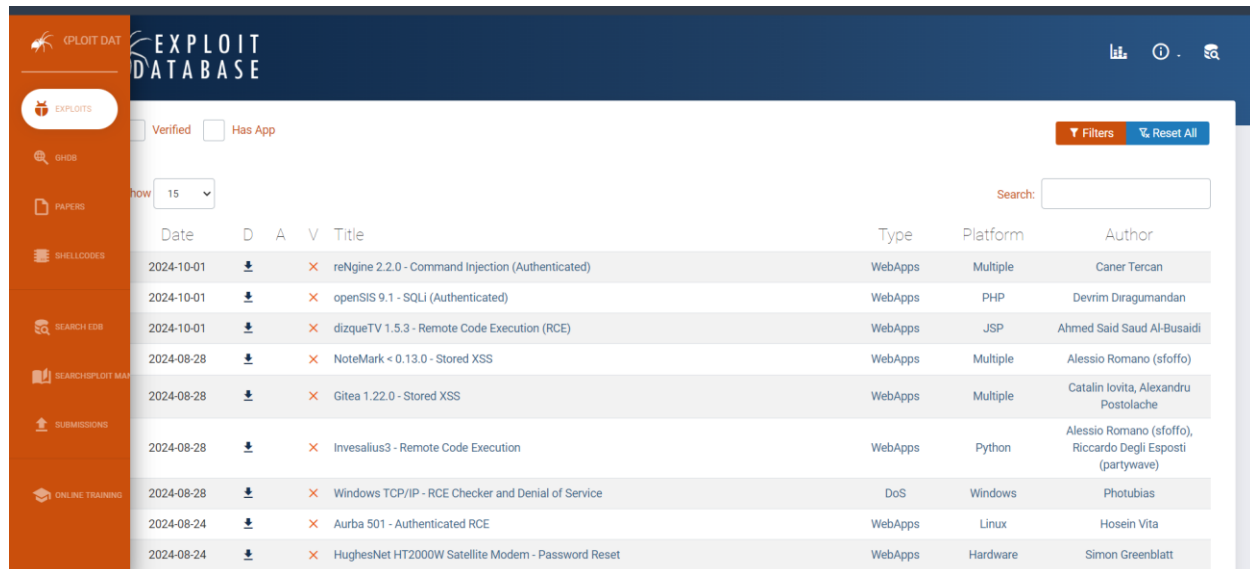
**NVD Last Modified:**

10/23/2024

**Source:**

**Exploit-DB:** Exploit-DB (Exploit Database) is an archive of public exploits and software vulnerabilities, maintained by Offensive Security. It serves as a platform for security researchers and ethical hackers to share proof-of-concept exploit code. Exploit-DB offers a searchable database of exploits for various platforms, applications, and vulnerabilities, providing detailed information such as the vulnerability description, exploitation method, and sometimes links to patches. It is a valuable resource for penetration testers and cybersecurity professionals to study real-world vulnerabilities and their potential risks.

Link: <https://www.exploit-db.com/>



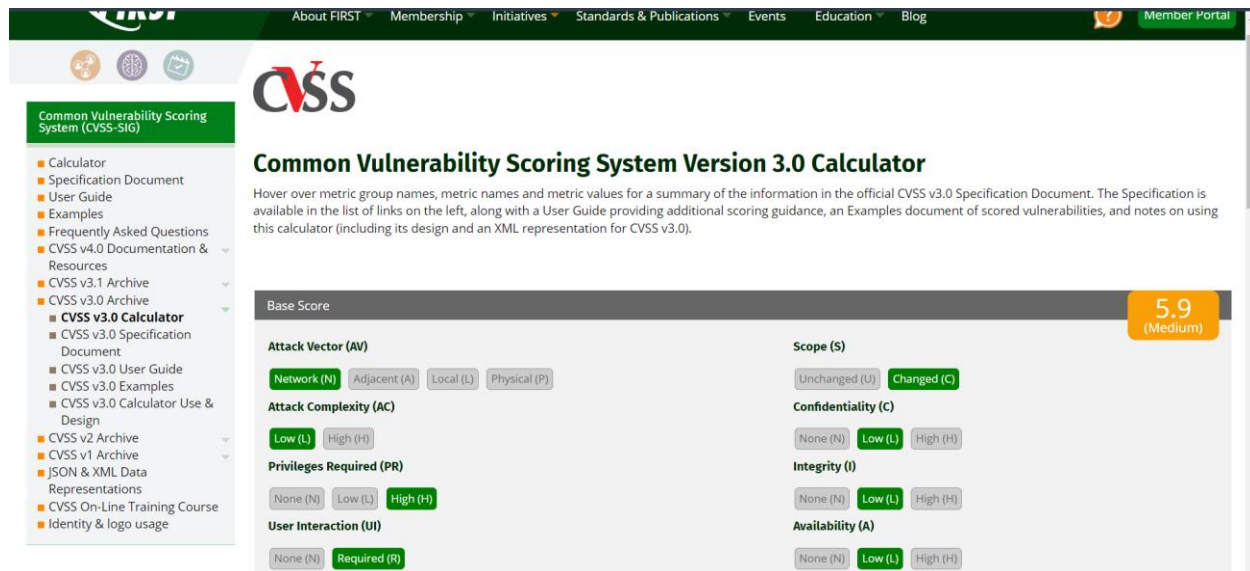
The screenshot shows the Exploit-DB website interface. On the left is a navigation sidebar with icons for EXPLOITS, GHGS, PAPERS, SHELLCODES, SEARCH EDB, SEARCH EXPLOIT MAP, SUBMISSIONS, and ONLINE TRAINING. The main content area displays a table of vulnerabilities with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. The table lists several vulnerabilities, including reNgine 2.2.0 - Command Injection (Authenticated), openSIS 9.1 - SQLi (Authenticated), dizqueTV 1.5.3 - Remote Code Execution (RCE), NoteMark < 0.13.0 - Stored XSS, Gitea 1.22.0 - Stored XSS, Invesalius3 - Remote Code Execution, Windows TCP/IP - RCE Checker and Denial of Service, Aurba 501 - Authenticated RCE, and HughesNet HT2000W Satellite Modem - Password Reset. Above the table are filters for Verified and Has App, a search bar, and buttons for Filters and Reset All.

Date	D	A	V	Title	Type	Platform	Author
2024-10-01				reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01				openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Diragumandan
2024-10-01				dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28				Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28				Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)
2024-08-28				Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Photubias
2024-08-24				Aurba 501 - Authenticated RCE	WebApps	Linux	Hosein Vita
2024-08-24				HughesNet HT2000W Satellite Modem - Password Reset	WebApps	Hardware	Simon Greenblatt

### Research Methodology:

**CVSS scores:** CVSS (Common Vulnerability Scoring System) scores are a standardized way of assessing the severity of security vulnerabilities. They range from 0 to 10, with higher scores indicating more critical vulnerabilities. The CVSS score is based on several factors, including the ease of exploitation, the impact on system integrity, confidentiality, and availability. The score helps organizations prioritize patching and mitigating vulnerabilities by assigning a numerical value to the risk. CVSS is widely used in tools like NVD and CVEDetails to guide security efforts.

Link: <https://www.first.org/cvss/calculator/3.0>



**Common Vulnerability Scoring System (CVSS-SIG)**

- Calculator
- Specification Document
- User Guide
- Examples
- Frequently Asked Questions
- CVSS v4.0 Documentation & Resources
- CVSS v3.1 Archive
- CVSS v3.0 Archive
  - CVSS v3.0 Calculator**
    - CVSS v3.0 Specification Document
    - CVSS v3.0 User Guide
    - CVSS v3.0 Examples
    - CVSS v3.0 Calculator Use & Design
  - CVSS v2 Archive
  - CVSS v1 Archive
  - JSON & XML Data
  - Representations
  - CVSS On-Line Training Course
  - Identity & logo usage

## Common Vulnerability Scoring System Version 3.0 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.0).

**Base Score** 5.9 (Medium)

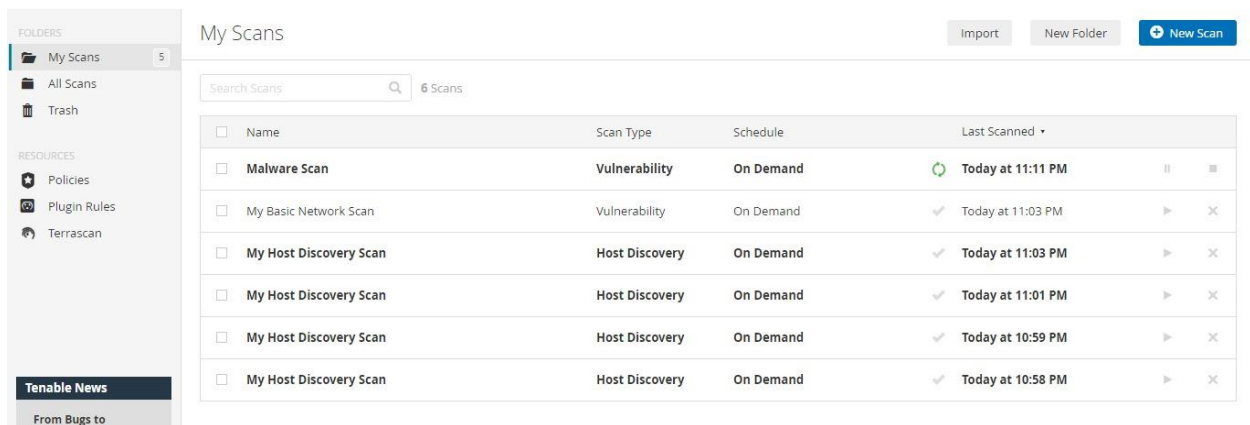
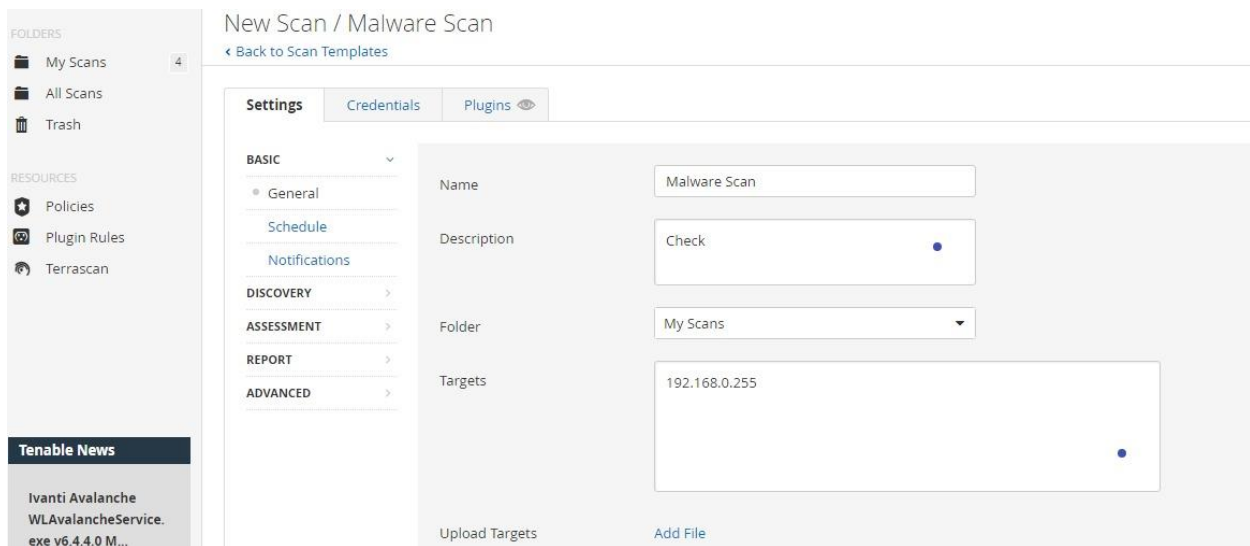
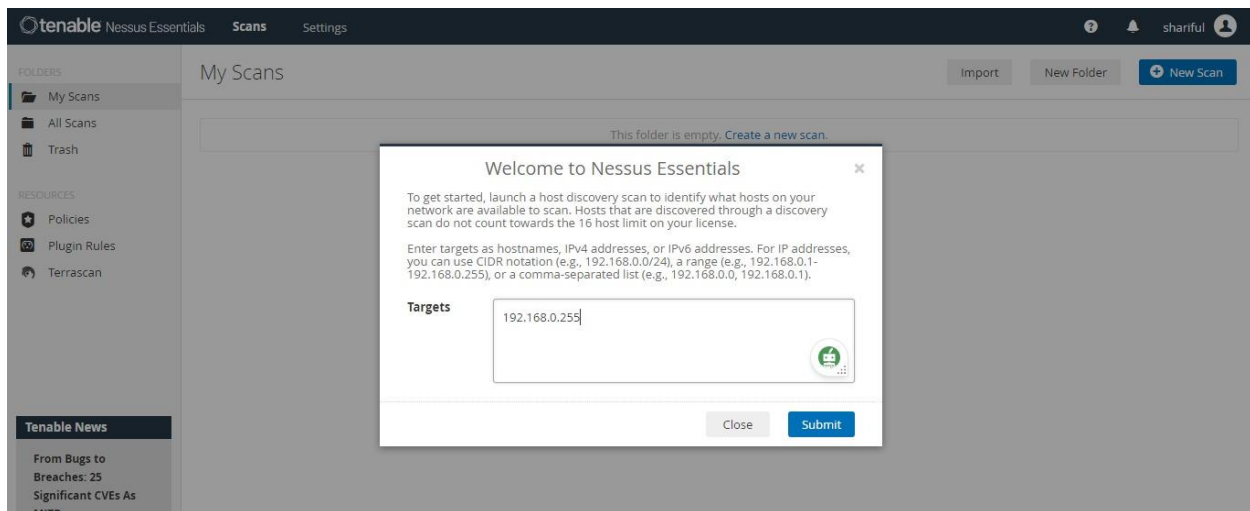
<b>Attack Vector (AV)</b> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Network (N)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">Adjacent (A)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">Local (L)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">Physical (P)</span>	<b>Scope (S)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">Unchanged (U)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Changed (C)</span>
<b>Attack Complexity (AC)</b> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Low (L)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">High (H)</span>	<b>Confidentiality (C)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">None (N)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Low (L)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">High (H)</span>
<b>Privileges Required (PR)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">None (N)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">Low (L)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">High (H)</span>	<b>Integrity (I)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">None (N)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Low (L)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">High (H)</span>
<b>User Interaction (UI)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">None (N)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Required (R)</span>	<b>Availability (A)</b> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">None (N)</span> <span style="background-color: green; color: white; padding: 2px 5px; border-radius: 3px;">Low (L)</span> <span style="background-color: #ccc; padding: 2px 5px; border-radius: 3px;">High (H)</span>

## Vulnerability Scanning using Manual Tools

### Hands-on Assessment:

#### Automated Tools:

**Nessus:** Nessus is a popular vulnerability scanner developed by Tenable, used to detect security flaws in systems and networks. It performs thorough scans to identify vulnerabilities such as misconfigurations, weak passwords, missing patches, and more. Nessus provides detailed reports on identified issues, including severity ratings, and often suggests remediation steps. It is widely used by IT security professionals for network auditing and vulnerability assessment due to its robust scanning capabilities and ease of use.





Malware Scan

Configure

Audit Trail

Launch

Report

Export

Back to My Scans

Hosts1

Vulnerabilities6

History1

Filter

Search Vulnerabilities

6 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
INFO				N...	Port scanners	41	
INFO				H...	General	1	
INFO				N...	Settings	1	
INFO				N...	General	1	
INFO				O...	General	1	
INFO				O...	Settings	1	

Scan Details

Policy: Malware Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 11:11 PM

End: Today at 11:18 PM

Elapsed: 8 minutes

Vulnerabilities

Critical

High

Medium

Low

INFO

Netstat Portscanner (SSH)

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 80/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	192.168.0.100

Plugin Details

Severity: Info

ID: 14272

Version: 1.106

Type: local

Family: Port scanners

Published: August 15, 2004

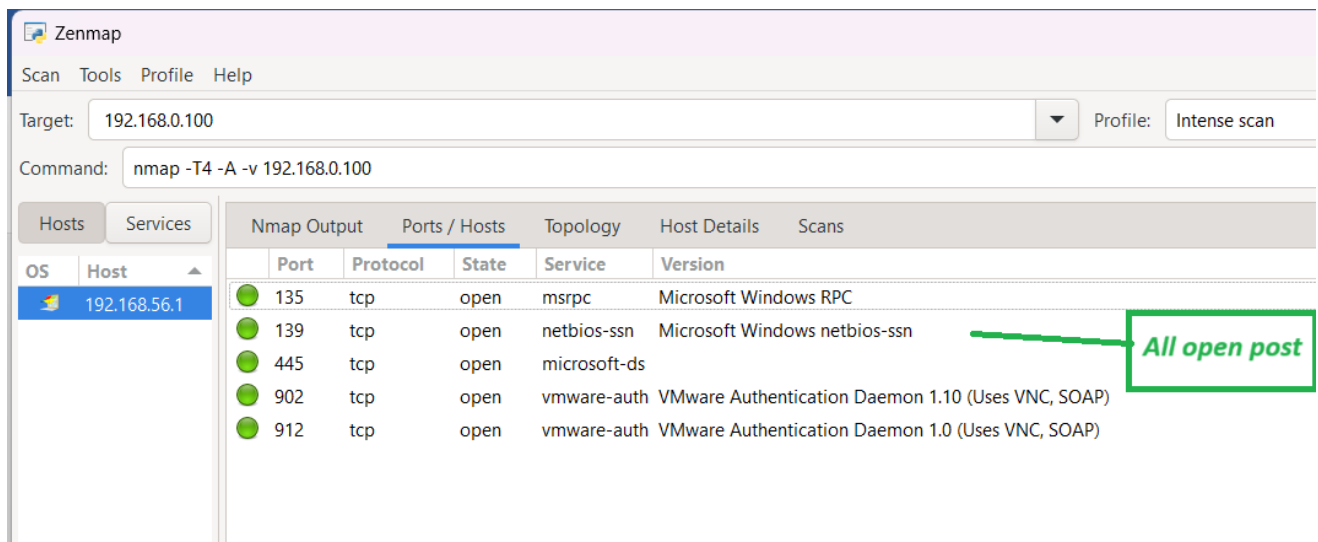
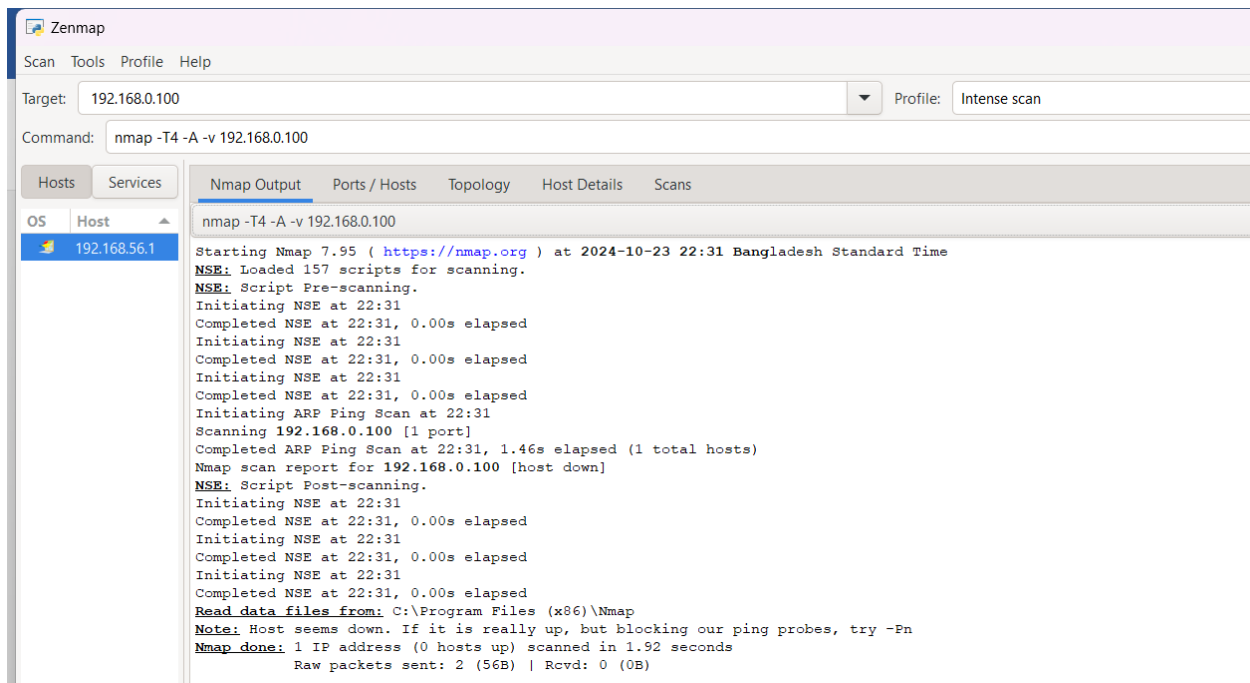
Modified: July 24, 2024

Risk Information

Risk Factor: None

## Manual Tools:

**Nmap:** Nmap (Network Mapper) is a widely used open-source tool for network discovery and security auditing. It is primarily used to scan and map networks, identify open ports, services running on hosts, and detect potential vulnerabilities. Nmap can also help with tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It supports various types of scanning techniques, such as TCP, SYN, and UDP scans, and is highly regarded by both network administrators and security professionals for its versatility and power.



### Manual Analysis:

**Burp Suite:** Burp Suite is a powerful cybersecurity tool used for web application security testing. Developed by PortSwigger, it provides a comprehensive platform for identifying vulnerabilities like SQL injection, XSS (cross-site scripting), and others in web applications. Burp Suite includes features such as a proxy server for intercepting HTTP/S traffic, a scanner for automated vulnerability discovery, an intruder tool for automated custom attacks, and repeater for manual

[Dashboard](#)
[Target](#)
[Proxy](#)
[Intruder](#)
[Repeater](#)
[Collaborator](#)
[Sequencer](#)
[Decoder](#)
[Comparer](#)
[Logger](#)
[Organizer](#)
[Extensions](#)
[Learn](#)

[Settings](#)

---

[Intercept](#)
[HTTP history](#)
[WebSockets history](#)
[Match and replace](#)
[Proxy settings](#)

---

**Filter settings:** Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	https://d8c14d4960ca.eed67...	POST	/d8c14d4960ca/a18a4859af9c/telem...		✓							✓	18.67.233.123		22:17:23 ...	8080	
2	https://www.google-analytics...	POST	/g/_collect?v=1&tid=G-W62N0F3JM...									✓	142.250.193.142		22:17:46 ...	8080	
3	https://www.google-analytics...	POST	/g/_collect?v=1&t=J101Ba=1028012...									✓	142.250.193.142		22:17:46 ...	8080	
4	https://analytics.google.com	POST	/g/_collect?v=1&tid=G-K4557SPWBB...									✓	216.239.32.181		22:17:46 ...	8080	
5	https://www.google.com/bd	GET	/ads/ga-audiences/v=1&t=sr&sf_...									✓	142.250.182.3		22:17:46 ...	8080	
6	https://www.hacker101.com	GET	/videos									✓	185.199.111.153		22:17:52 ...	8080	
7	https://tf.hacker101.com	GET	/									✓	104.18.102.237		22:17:57 ...	8080	
8	https://d8c14d4960ca.eed67...	GET	/d8c14d4960ca/a18a4859af9c/inpu...		✓							✓	18.67.233.123		22:18:00 ...	8080	
9	https://safebrowsing.google...	GET	/v4/fullHashes/find?Id=applicatio...		✓							✓	142.250.182.10		22:18:00 ...	8080	

### Request

Pretty Raw Hex

```

POST /d8c14d4960ca/a18a4859af9c/telemetry HTTP/1.1
Host: d8c14d4960ca.eed67d5.ap-south-2.token.aswfwf.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain;charset=UTF-8
Content-Length: 3046
Origin: https://www.booking.com
Referer: https://www.booking.com/
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: document
Priority: u=4
Te: trailers
Connection: keep-alive

{
  "existing_token": "fa3abe55-e818-47de-ascl-1b5eb97580eaf:HgoAZKZyP2YTBAAAAY:y5SQLPgPNTI4DpoerrSUznbfxXjWyP7TWTWUaThBwoI/iA9SIQCLIBvIR4BIIGQAMNgOj5EYTS1508rlgs/7ixu13dJYvswBUtKoRTEBzgHpeQXYTZFN2FBFBy7YEUSqIV3hn7kTeUuaBYgvexUetgnlvURl01TY3BozaATPVetUehb547Re4EHYChRTmG6CUIhiFFdUBar7VCMTzLsvhwxygEGQITVWohBYecrlPaRHP1TJKa/PBML7tjMA",
  "aswaf_session_storage": "fa3abe55-e818-47de-ascl-1b5eb97580eaf:HgoAZKZyP2YTBAAAAY:usInUpNeFWotUDIA+IS6qrSHIEUVll0(SBK+24IXGB/Rof1izMVOQC2nHgP2C3oRk3XNCWC7Gtnsk/38ma8RctcdFTB1vTFWTVoguoDIhN0j4gf4of1ohm+CDSgetwFr/fldy8lp83Pc773+2C0UYflapagUPzo9yxcofUaFo/cChdp4tcddmgQOL4sl3YUgMBicUUYXDBHEHDynlnKAPAFAP7OSHIL/ElalacIDuq5VCDOugep7YubhoCawd4icFlabBndBWA465PC3BrWpKaBNWBA7Tl2t4AgueG7e6Pdxcs37PBEMTPl3EDDAALITVBH700ldPRVGYICD0B3808ABDEpWp91lyMac4WOCu089gd40Y3ibSBxciyeTefGQU1151ldnpv85umTr12Q4TUreMNLayqIgClANdShMy(YaB84VLHRe/CeSL19ep215bBDUdl17uCbCofoSSLLIMAnrnad1eq4P7rhGL04BvuyWch3ysBamdn0cXs48+pBg/x3juaaCfl1500Bq7yod26
        
```

### Inspector

Selection 310 (x136)

Selected text

```

fa3abe55-e818-47de-ascl-1b5eb97580eaf:HgoAZKZyP2YTBAAAAY:y5SQLPgPNTI4DpoerrSUznbfxXjWyP7TWTWUaThBwoI/iA9SIQCLIBvIR4BIIGQAMNgOj5EYTS1508rlgs/7ixu13dJYvswBUtKoRTEBzgHpeQXYTZFN2FBFBy7YEUSqIV3hn7kTeUuaBYgvexUetgnlvURl01TY3BozaATPVetUehb547Re4EHYChRTmG6CUIhiFFdUBar7VCMTzLsvhwxygEGQITVWohBYecrlPaRHP1TJKa/PBML7tjMA
        
```

See less

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	POST
Path	/d8c14d4960ca/a18a4...

Event log All issues
Memory: 124.3MB