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: Shariful Islam

ID No: 2111252

Batch No: 11

Submitted To

Moinoddeen Quader Al Arabi

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

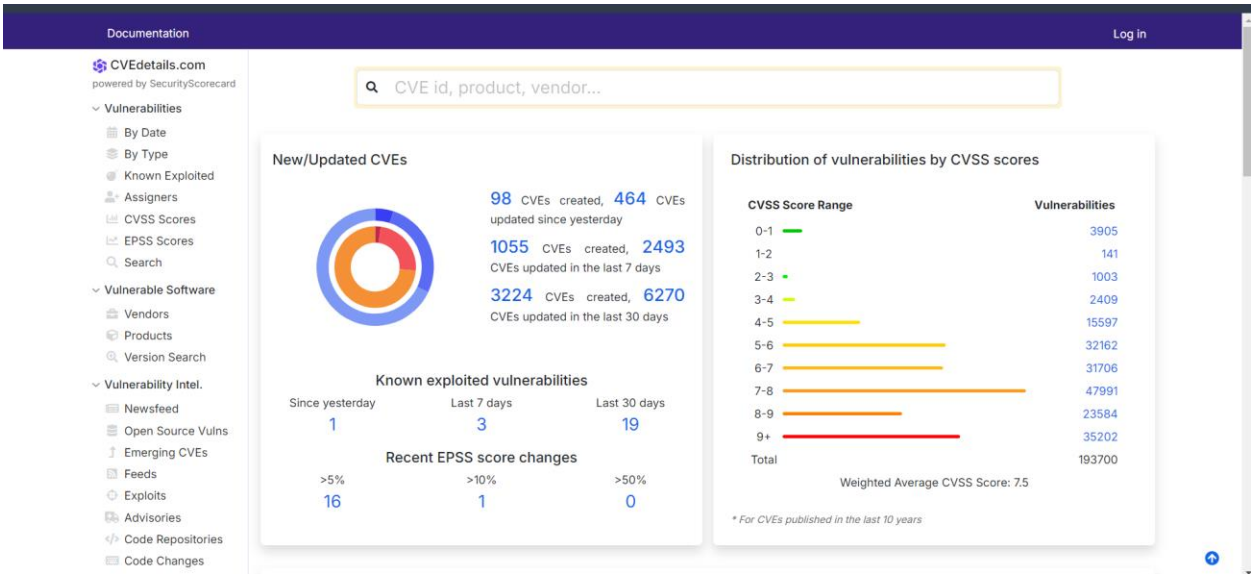
Vulnerability Analysis and Research using Online Database:

Understanding the Vulnerability Landscape:

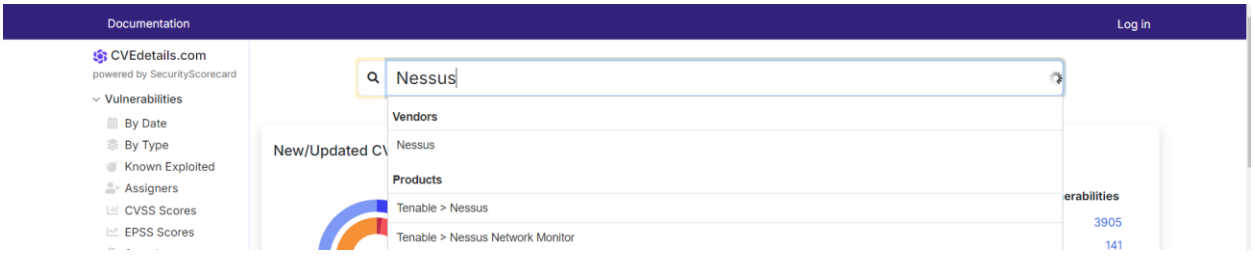
Online Database:

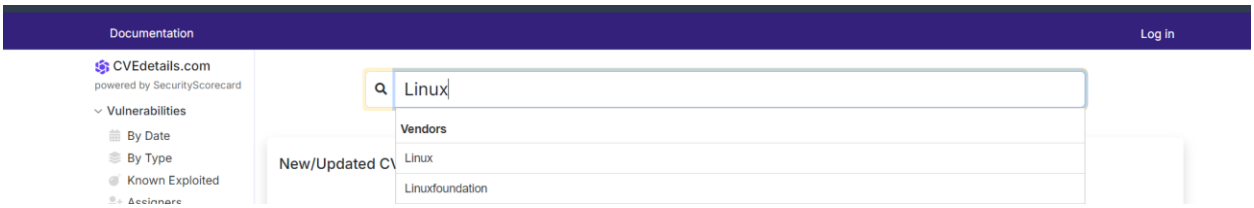
CVEdetails: CVEDetails is a platform that provides detailed information about publicly known cybersecurity vulnerabilities, known as Common Vulnerabilities and Exposures (CVEs). It aggregates data from sources like the National Vulnerability Database (NVD) and CVE.org, offering insights into vulnerabilities, 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/

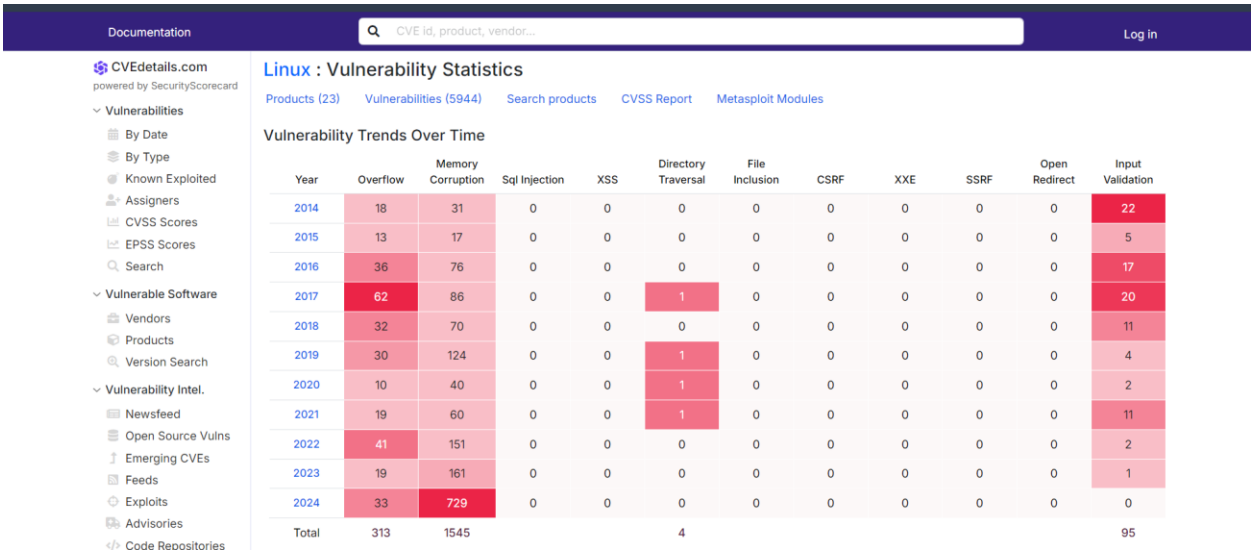


There has option for search any product, vendor etc.



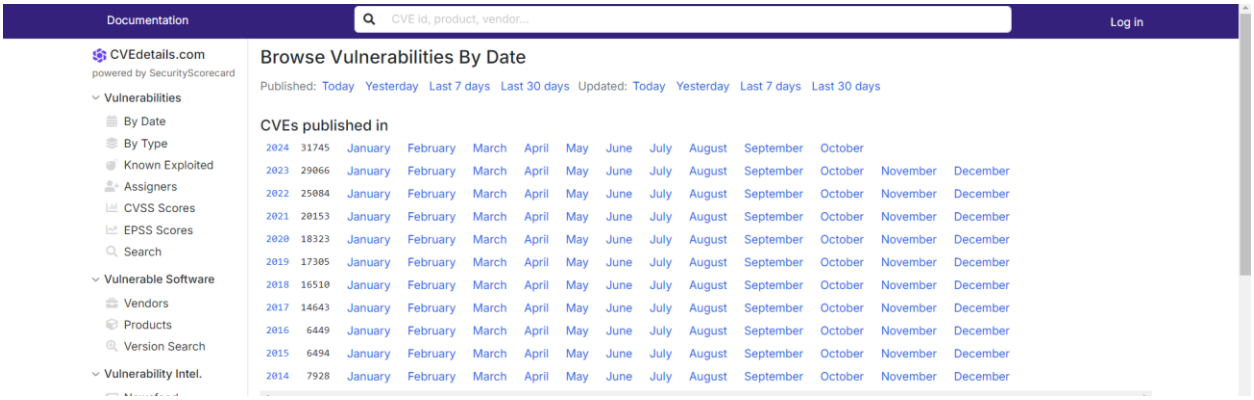


Here details of vulnerability is show until present month of the Year:

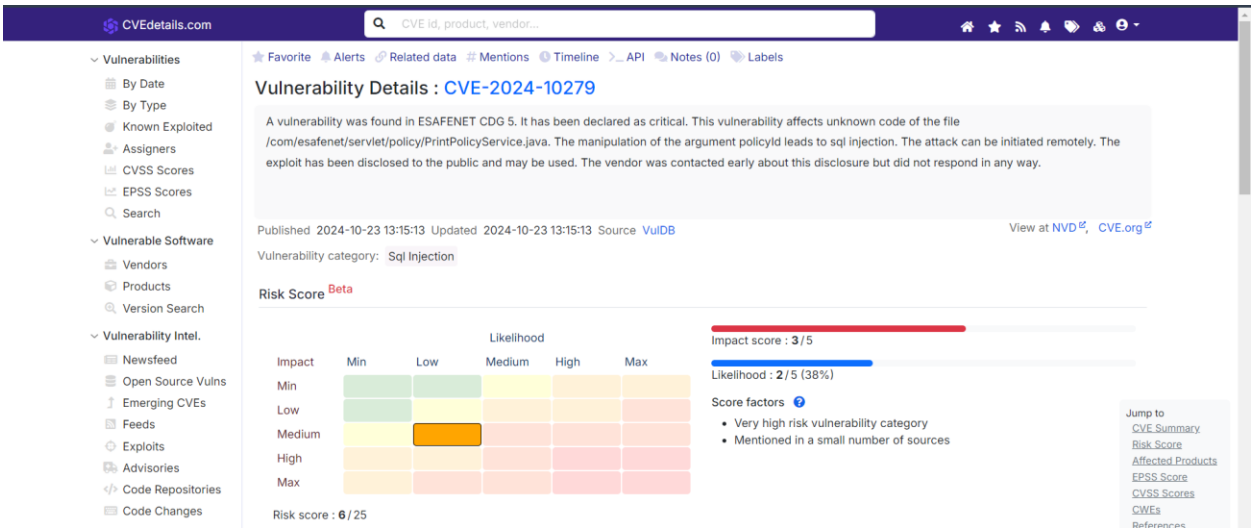


We can search by date, type.

Result of search by Date:

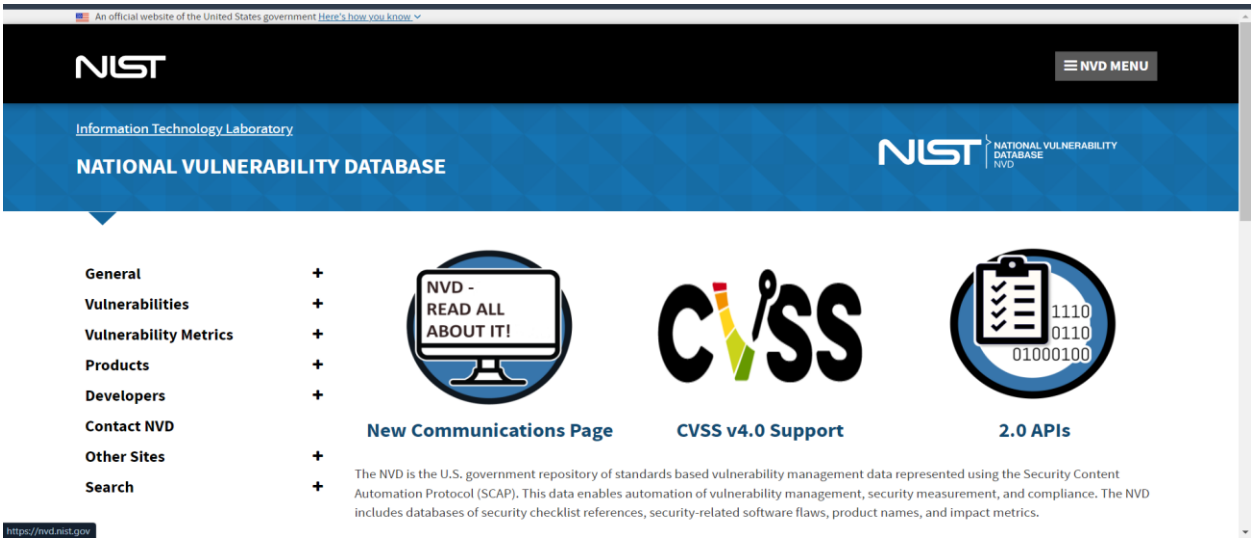


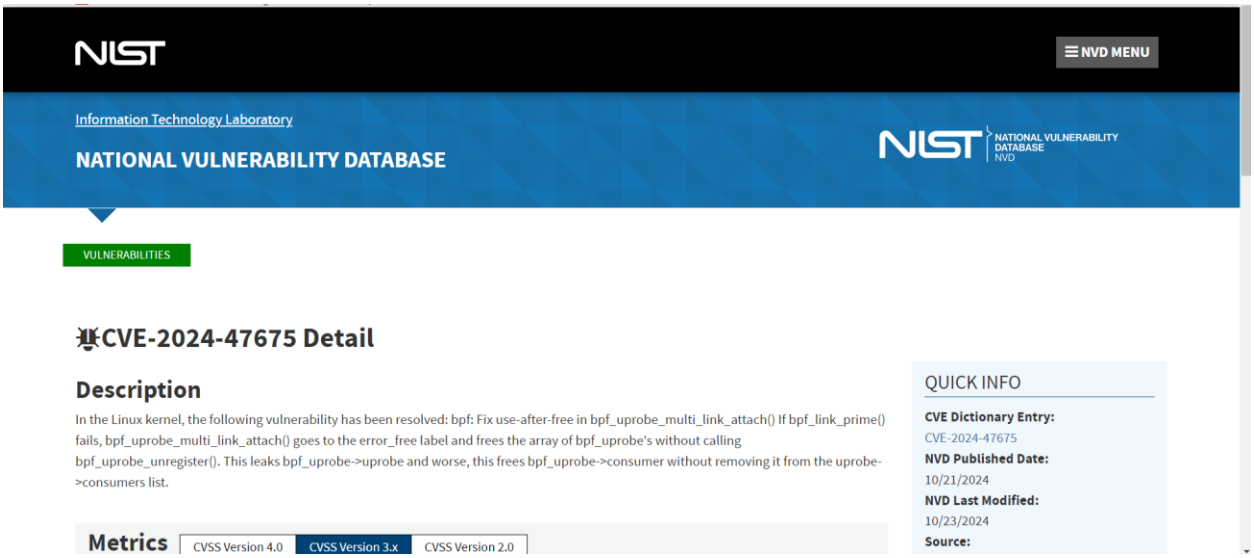
Today's vulnerability (Green is good condition, orange is for risk medium and red for high risk of Base Severity):



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.

Link: https://nvd.nist.gov/





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.

QUICK INFO

CVE Dictionary Entry:
CVE-2024-47675
NVD Published Date:
10/21/2024
NVD Last Modified:
10/23/2024
Source:

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://git.kernel.org/stable/c/5fe6e308abaea082c20fbf2aa5df8e14495622cf	Patch
https://git.kernel.org/stable/c/790c630ab0e7d7aba6d186581d4627c09fce60f3	Patch
https://git.kernel.org/stable/c/7c1d782e5afbf7c50ba74ecc4ddc18a05d63e5ee	Patch
https://git.kernel.org/stable/c/cdf27834c3dd5d9abf7eb8e4ee87ee9e307eb25c	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)

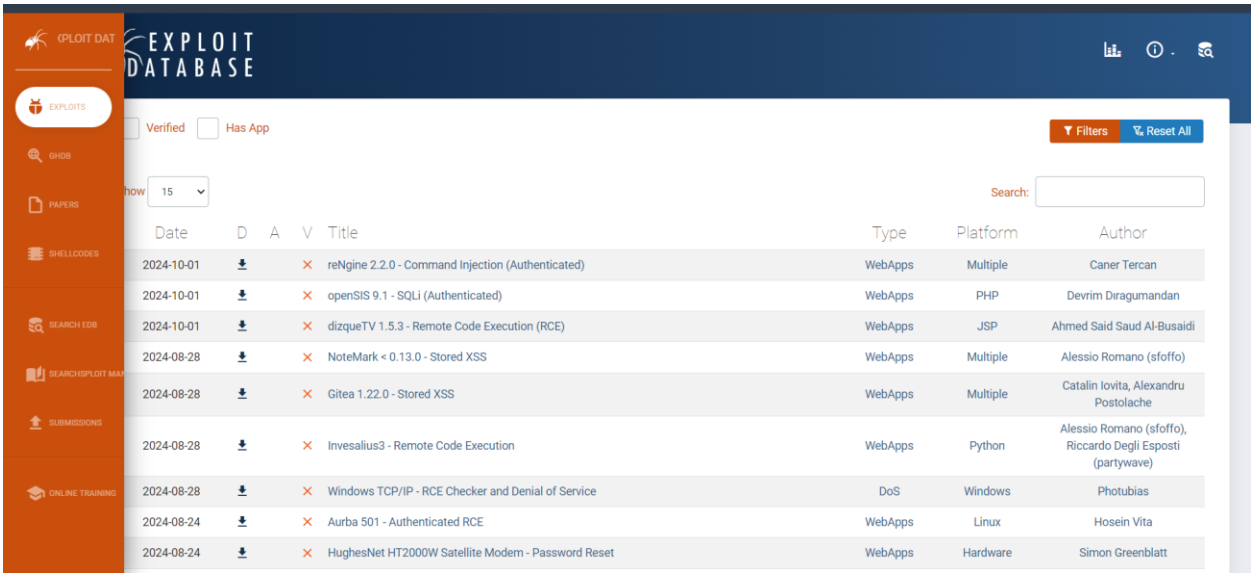
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.6	6.6.54
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.7	6.10.13
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.11	6.11.2

Denotes Vulnerable Software

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

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.

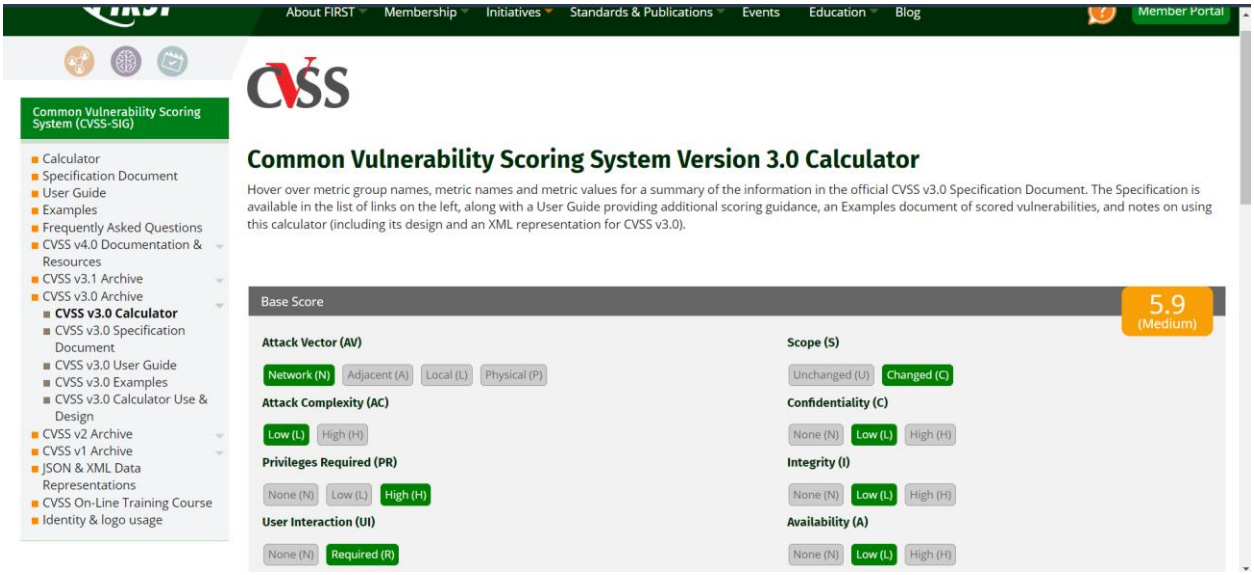
Link: https://www.exploit-db.com/



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

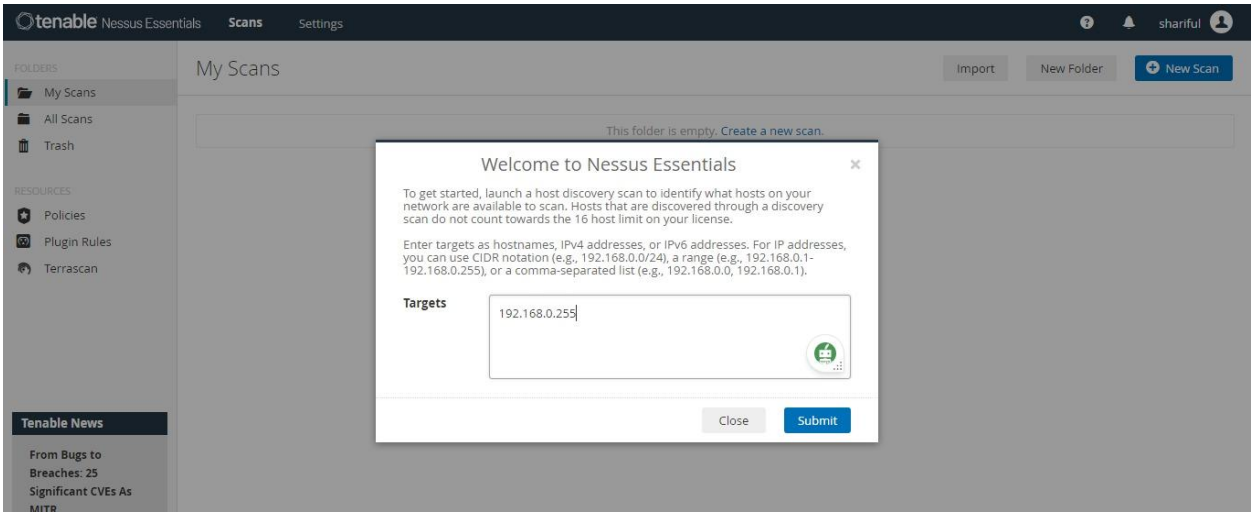


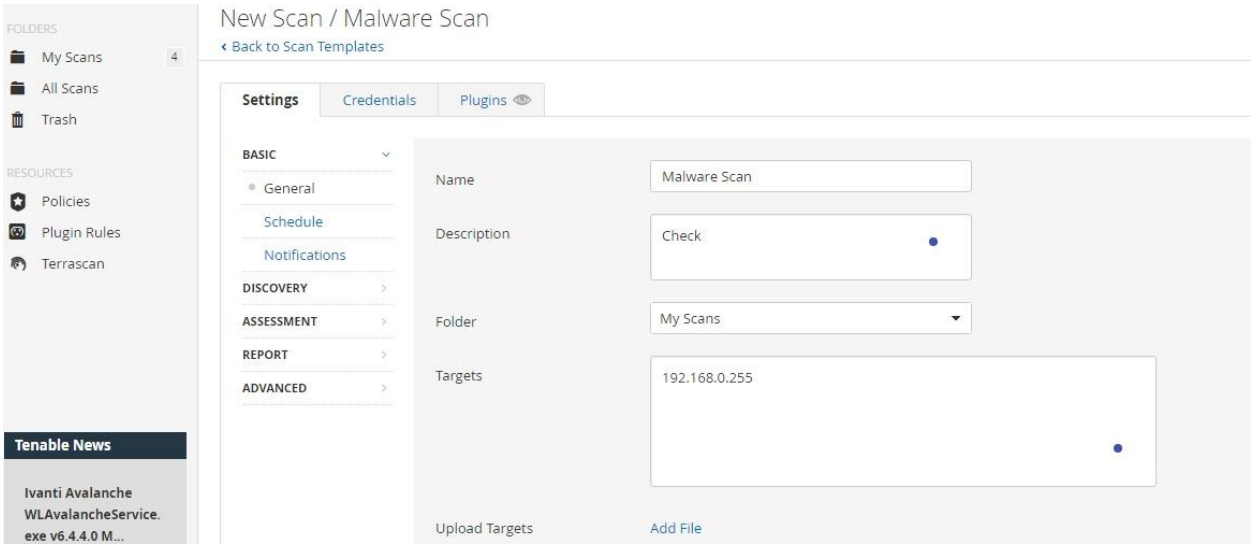
Vulnerability Scanning using Manual Tools

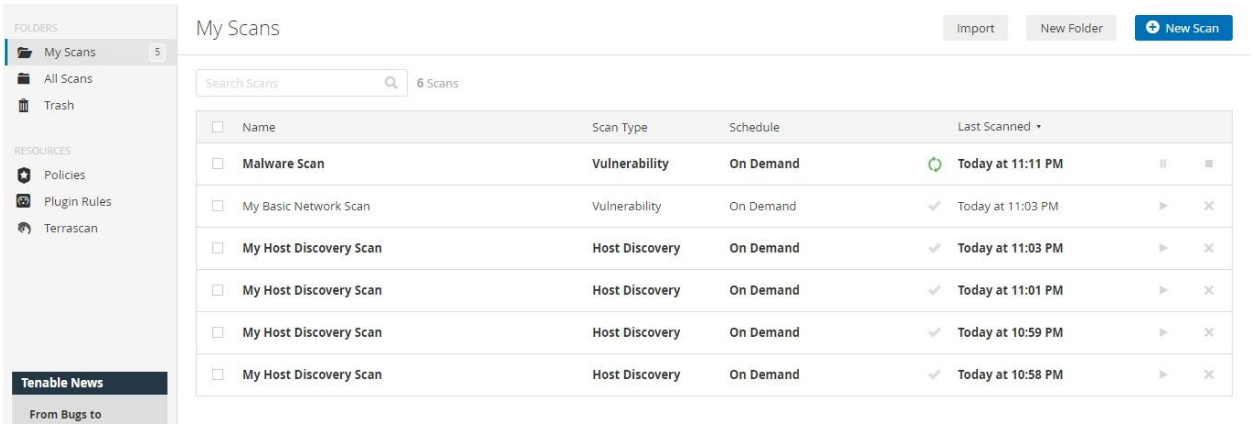
Hands-on Assessment:

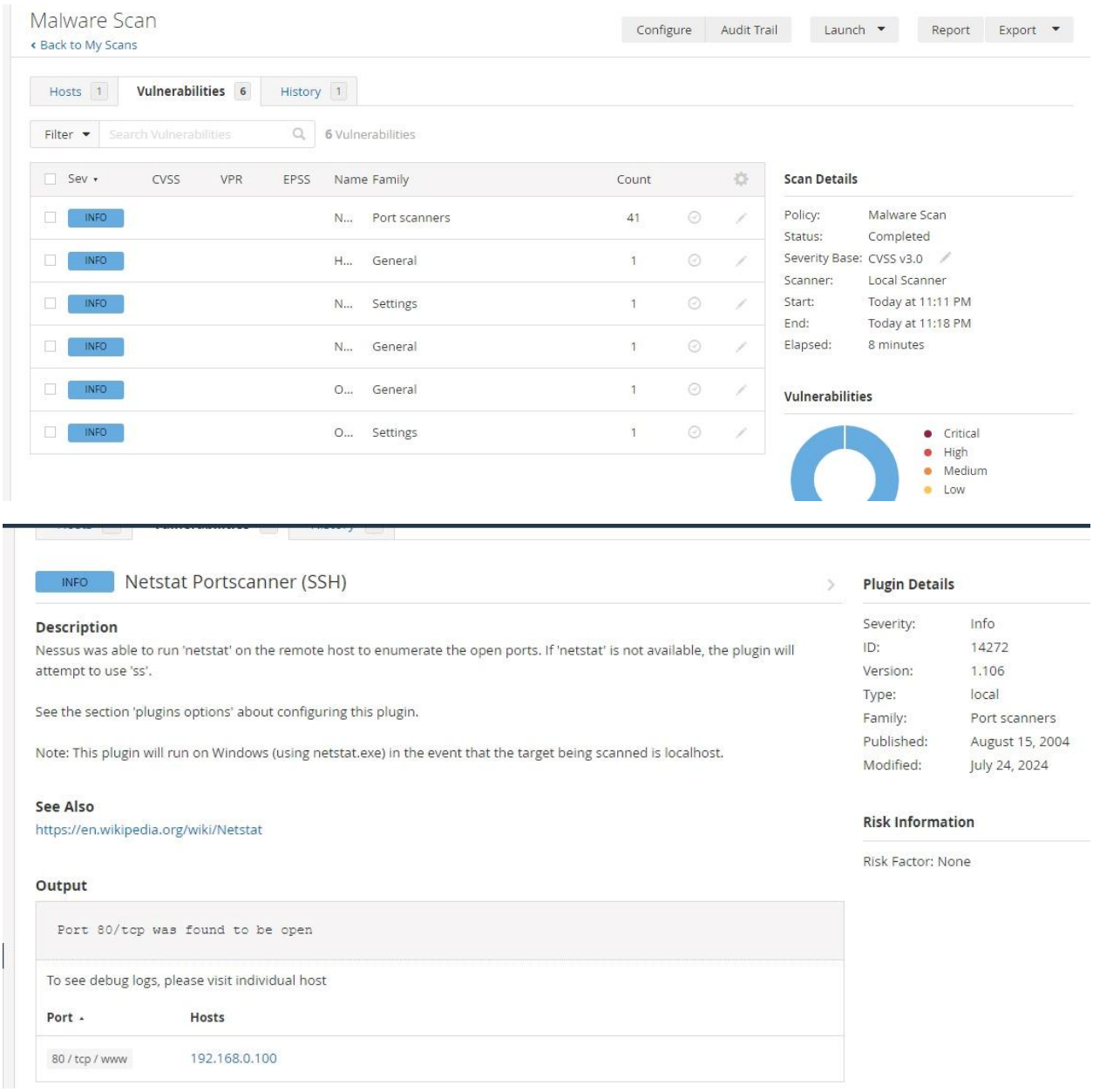
Manual Tools:

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.

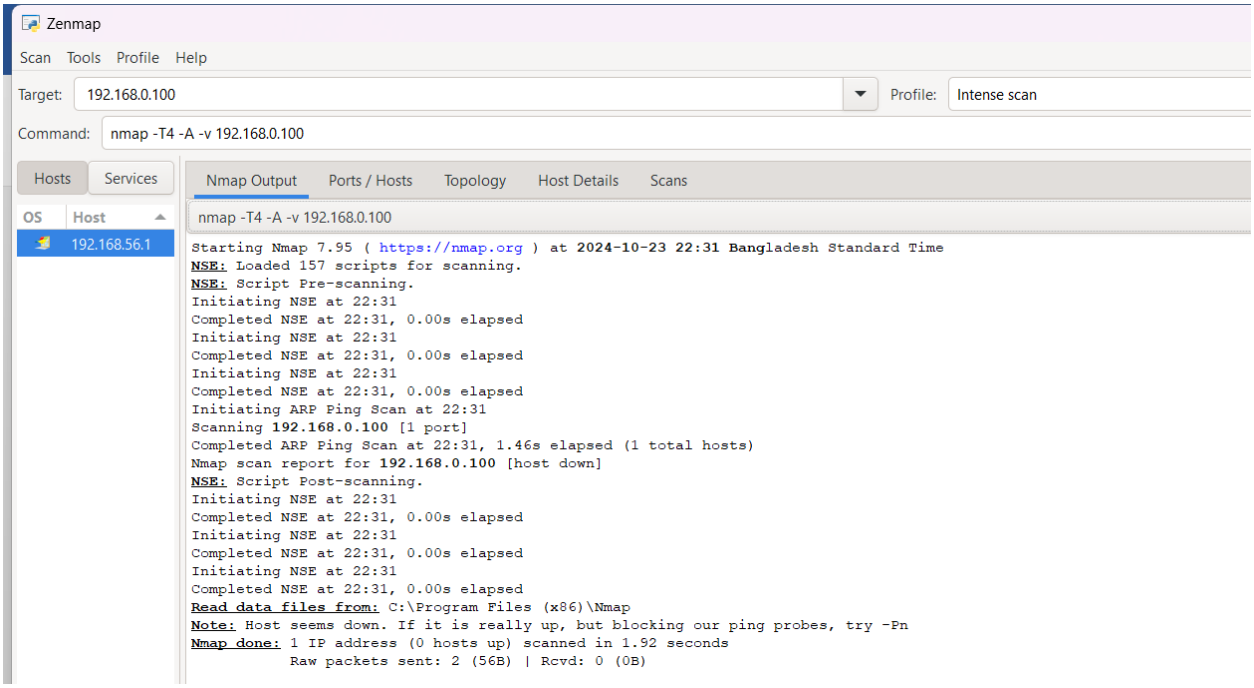

tenable Nessus Essentials
Scans
Settings
shariful
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
From Bugs to Breaches: 25 Significant CVEs As
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
Welcome to Nessus Essentials
To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).
Targets
192.168.0.255
Close
Submit

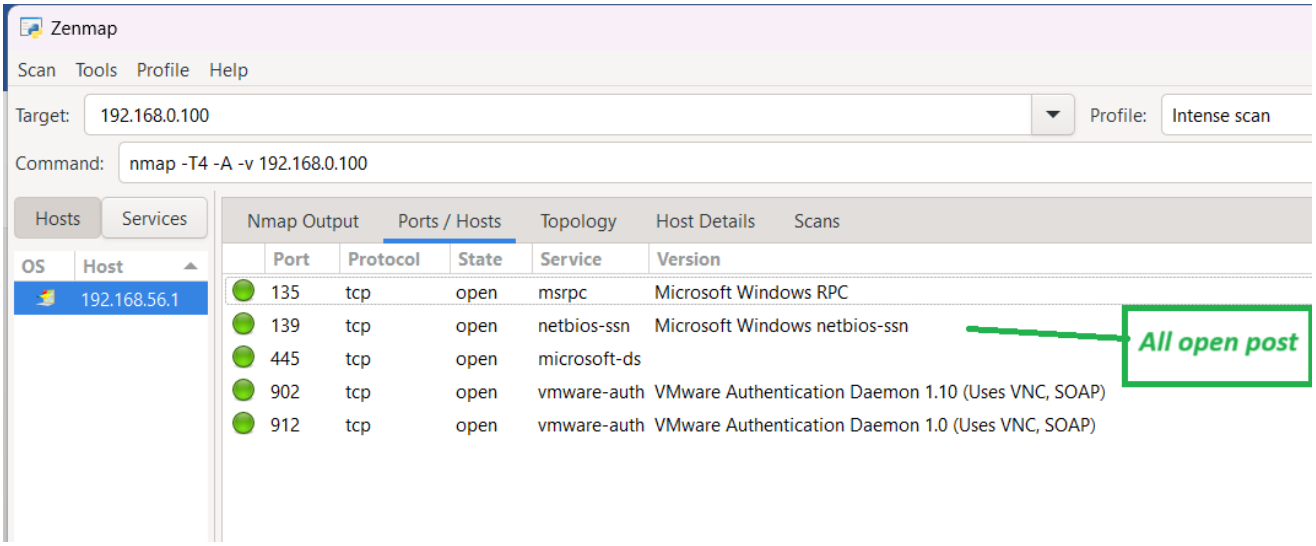

FOLDERS
My Scans 4
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Ivanti Avalanche WLAvalancheService.exe v6.4.4.0 M...
New Scan / Malware Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Malware Scan
Description
Check
Folder
My Scans
Targets
192.168.0.255
Upload Targets
Add File


FOLDERS
My Scans 5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
From Bugs to
My Scans
Import
New Folder
New Scan
Search Scans
6 Scans
Name
Scan Type
Schedule
Last Scanned
Malware Scan
Vulnerability
On Demand
Today at 11:11 PM
My Basic Network Scan
Vulnerability
On Demand
Today at 11:03 PM
My Host Discovery Scan
Host Discovery
On Demand
Today at 11:03 PM
My Host Discovery Scan
Host Discovery
On Demand
Today at 11:01 PM
My Host Discovery Scan
Host Discovery
On Demand
Today at 10:59 PM
My Host Discovery Scan
Host Discovery
On Demand
Today at 10:58 PM



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

testing. It's widely used by penetration testers, security researchers, and ethical hackers to audit web applications effectively.