Assessment 1

Network Vulnerability Assessment

EXTION INFOTECH

Growth Towards Future

Intern Name: Leburi SriRam

Date: 06/02/2024

Network Vulnerability Assessment

This assessment is to **scan vulnerabilities** in a network or website using **Nessus** tool in **Kali linux OS**

Objective:

This project is to **find vulnerabilities** of a network or websites etc and to gain knowledge about vulnerabilities, how to **mitigate** the threats due to vulnerabilities and some safety measures to **secure** our network or websites etc

Introduction:

Network Vulnerability:

Vulnerabilities are **weak points** that cybercriminals can use **togain unauthoriz ed access** to a computer. By exploiting vulnerabilities, cyber attackers can run malicious code, install malware, and even steal sensitive data. There are many ways to exploit this vulnerability, including **SQL injection**, exploits, crosssite s cripting **(XSS)**, and **open source tools** used to **detect** vulnerable vulnerabilities and **vulnerabilities** in web applications.

Network **vulnerability scanning** is the **evaluation** and **reporting** of computers, networks,web applications or other devices,including switches,routers,firewalls andwirelessaccess,points.
Cause of vulnerabilities:There are many. Vulnerabilities, including open ports, incorrect network settings, or outdated software running on the network, may or may not be known and can be easily exploited by hackers and used to insert con tent into the system.

Why is Network Vulnerability Scanning important?

Identifying vulnerabilities in the network helps mitigate many of the cybersecuri ty risks and issues that exist in an organization. If vulnerabilities in an organizati on's IT infrastructure go undetected, cybercriminals can easily exploit them. Bus inesses can experience data breaches even with proper protections in place. Ho wever, regular vulnerability checks and timely patching can help prevent cyber attacks.

Vulnerability scanning is an important part of a company's security posture beca use it provides the following benefits:

- Detects anomalies
- Provides proactive mitigation
- Inspects the entire attack surface
- Complies with cybersecurity regulations
- Offers continuous monitoring
- Safeguards reputation

Types of Network Vulnerability Scanning

- Unauthenticated scanning
- Authenticated scanning
- Host-based scanning
- Network-based scanning
- Web application scanning
- Database scanning
- Port scanning
- Cloud vulnerability scanning

Here,In this assessment I performed a **Network-Based Scanning** and **Web Application Scanning** using Nessus tool.

Network-Based Scanning: This scanning identifies vulnerabilities such as weak passwords in network devices, including routers, servers, firewalls and switches. Limited penetration testing is also conducted through network scanning without affecting the underlying system or network performance.

Web application scanning: This targeted scanning of web apps aims to identify security flaws in their code, configurations and authentication mechanisms, which helps mitigate common web-based security breaches.

CVSS: CVSS stands for the **Common Vulnerability Scoring System**. It's a way to evaluate **and rank reported vulnerabilities** in a standardized and repeatable way. The goal of CVSS is to help you compare vulnerabilities in different applications – and from different vendors - in a standardized, repeatable, vendor agnostic approach.

CVSS generates a score from 0 to 10 based on the severity of the vulnerability. A score of 0 means the vulnerability is less significant than the highest vulnerability with a score of 10,

PVR: Vulnerability priority rating (VPR), the output of Tenable Predictive Prioritization, helps organizations improve their remediation efficiency and effectiveness by rating vulnerabilities based on severity level – Critical, High, Medium and Low – determined by two components: technical impact and threat.

Network based scanning:

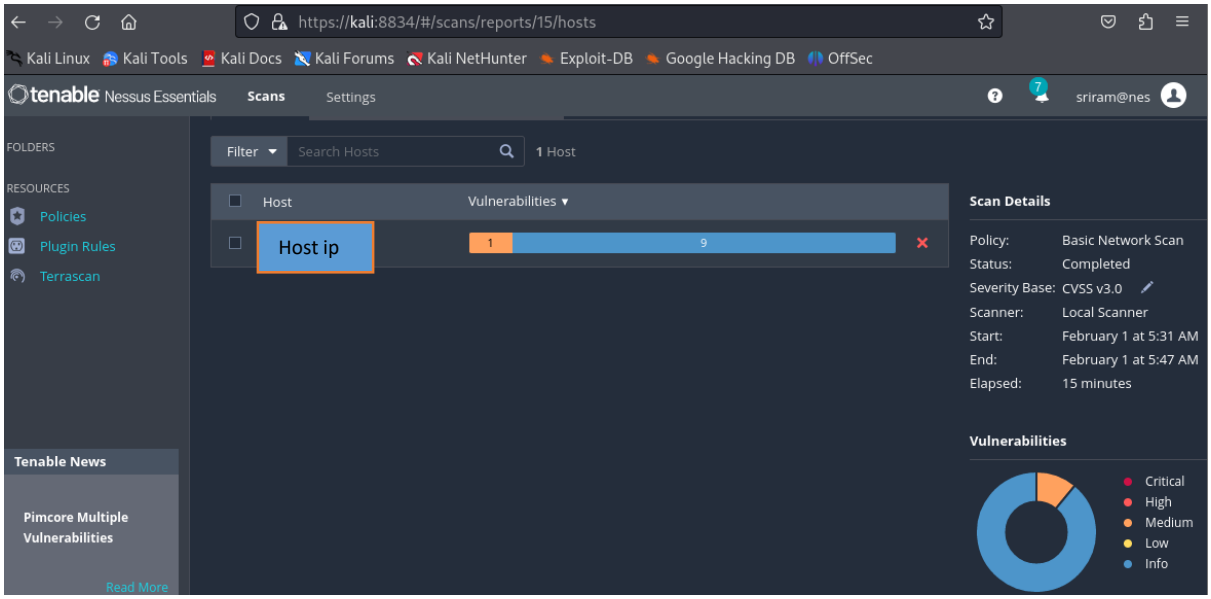

Fig1:Vulnerability severity level

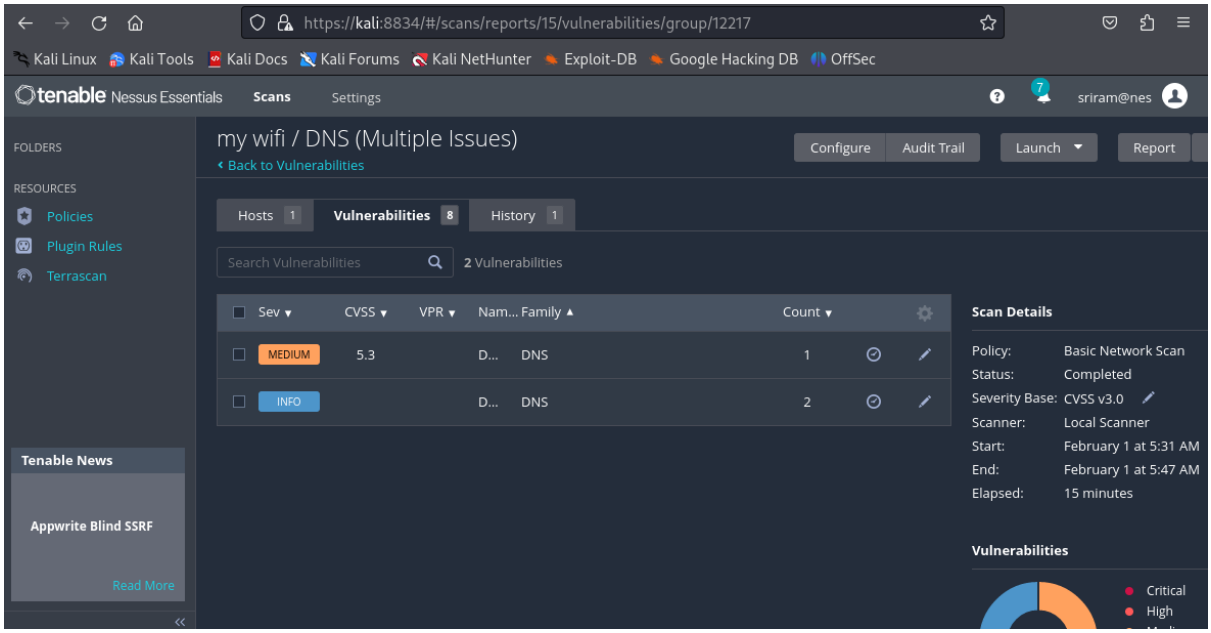

Fig2 : Vulnerabilities found

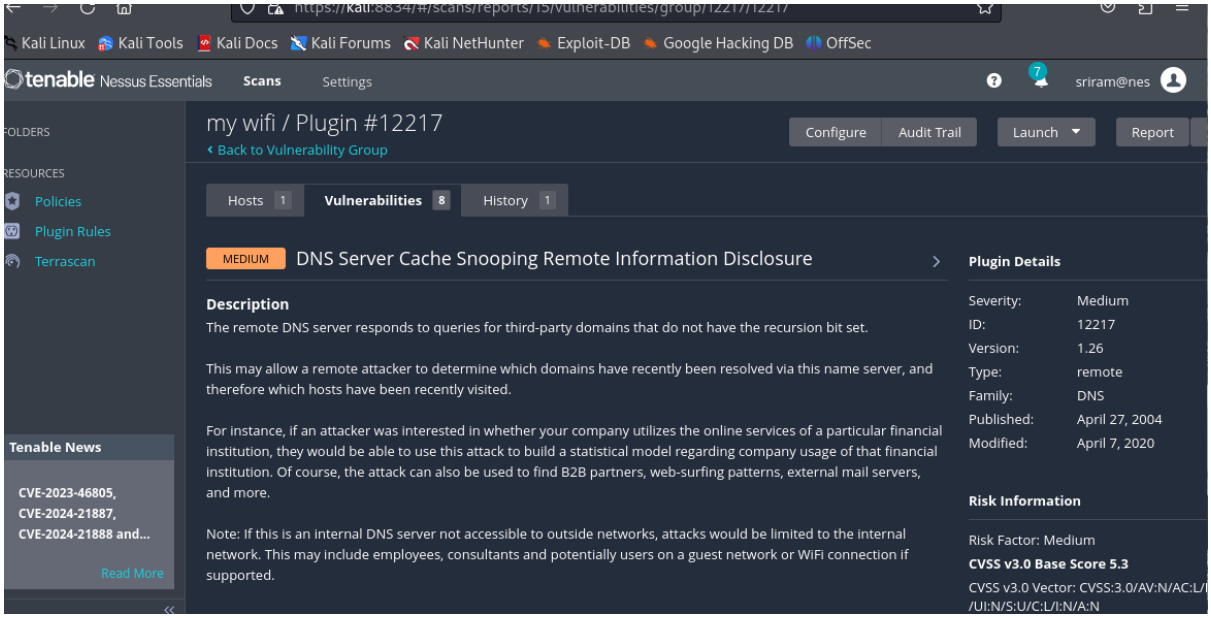

Fig3 :report

Web application scanning:

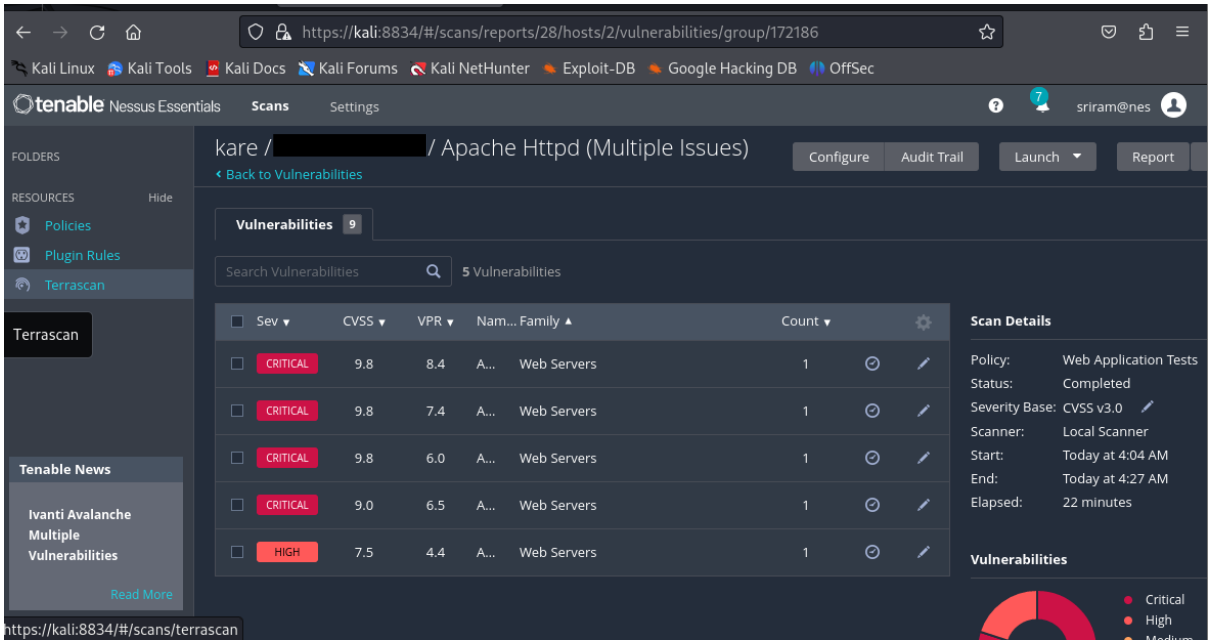

Fig 4:vulnerability severity report

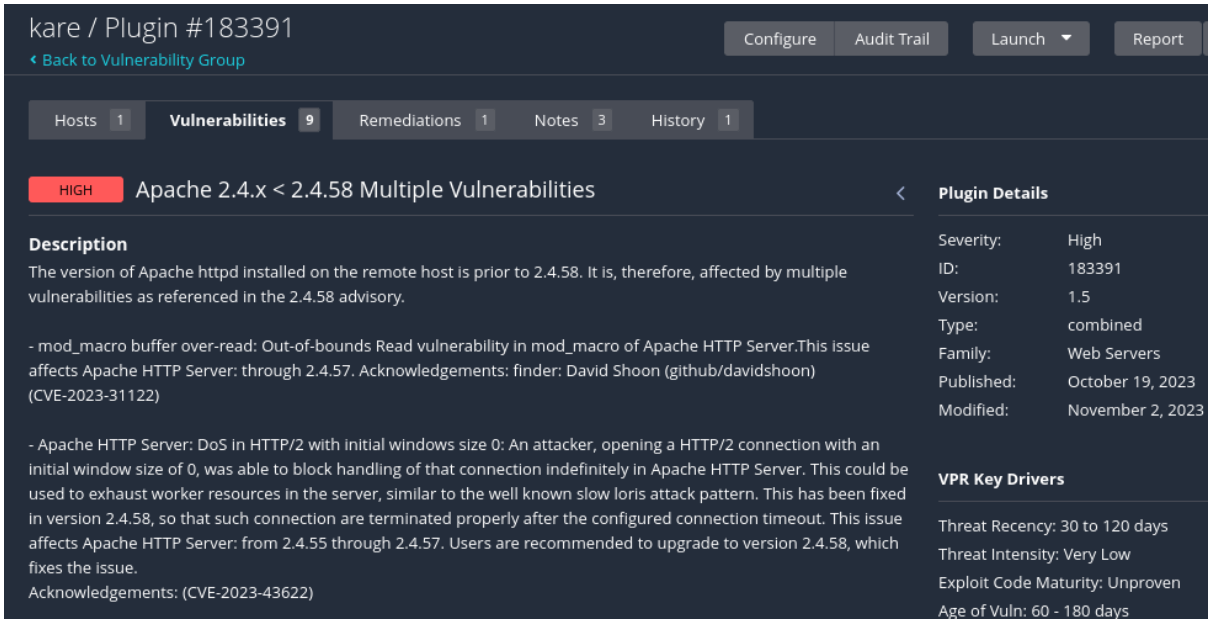

Fig5:High severe Vulnerability report

Vulnerabilities found in Both Network and web application scan:

- Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
- DNS Server Cache Snooping Remote Information Disclosure

Apache 2.4.x < 2.4.58 Multiple Vulnerabilities:

The remote web server is affected by multiple vulnerabilities. Description The version of Apache httpd **installed** on the remote host is **prior** to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

DNS Server Cache Snooping Remote Information Disclosure:

“DNS Server Cache Snooping Remote Information Disclosure” attacks lately, **mostly coming from reports** generated by one very popular security scanner: The remote DNS server **responds** to queries for **third-party domains** that do not have the recursion bit set.

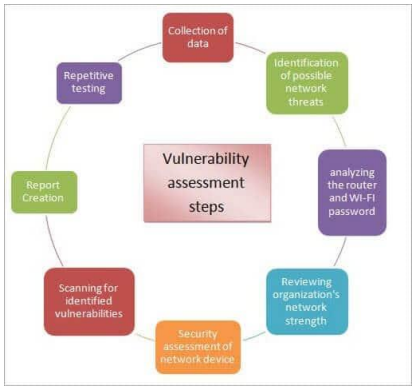

Fig 6: Vulnerability Assessment steps

Benefits of Vulnerability Scanning:

1. It provides a good way to close any security vulnerabilities in the system and helps maintain good security for the organization, data centers and th e employees themselves.
2. Network scanning helps organizations protect systems from hackers expl oiting vulnerabilities.
3. Scanning helps protect important and sensitive information in manageme nt, defense and other information in the organization from malicious attacks.

Mitigations:

Continuous monitoring risks by performing vulnerability assessment

Everything should be up to date

Fix the identified vulnerabilities in time

Implement security controls

Conclusion:

By here I am concluding this project that by performing vulnerability assessments, aware of types of vulnerabilities and their risks early fix them early and by taking some security measures everyone should secure their network. Protect your network or websites from hackers by early fixing identied vulnerabilities. I learn more about network vulnerability scanning and the severity of vulnerabilities.