Nessus Vulnerability Assessment Report

Cybersecurity & Ethical Hacking Internship
Company: ApexPlanet Software Pvt. Ltd.

Tool Used: Nessus Essentials
Scanner Machine: Kali Linux
Target Machine: Metasploitable2

---

1. Objective:

The objective of this assessment is to identify security vulnerabilities, misconfigurations, and potential threats present in the target system using Nessus Essentials vulnerability scanner. This helps in understanding security weaknesses that could be exploited by attackers.

2. Tool Overview:

Nessus Essentials is a professional vulnerability scanner developed by Tenable.

It is used to:

• Detect vulnerabilities.
• Identify outdated services.
• Detect backdoors and security risks.
• Assess system security posture.

Nessus provides vulnerability severity levels such as:

• Critical
• High
• Medium
• Low
• Informational

3. Target Information:

Parameter	Value
Scanner Machine	Kali Linux
Target Machine	Metasploitable2
Target IP Address	192.168.244.4
Scanner Tool	Nessus Essentials

4. Scan Configuration:

The vulnerability scan was configured using Nessus Essentials web interface.

Steps performed:

• Nessus Essentials was launched.
• Target IP address was added.

• Scan type selected: Basic Network Scan.
• Scan was started and results were analysed.

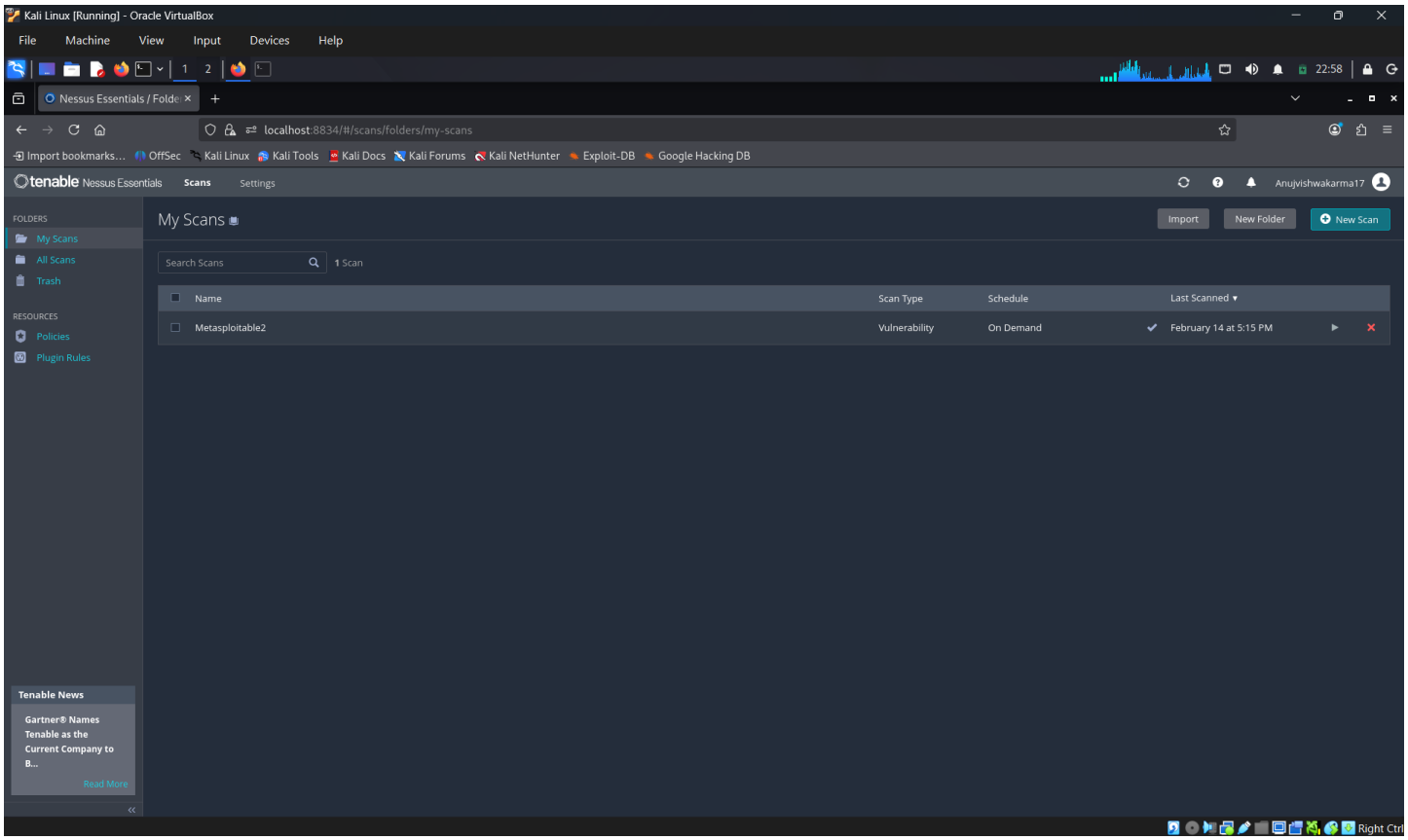

Figure 1: Nessus Essentials dashboard

5. Vulnerability Scan Results:

The Nessus scanner successfully identified multiple vulnerabilities on the target system.

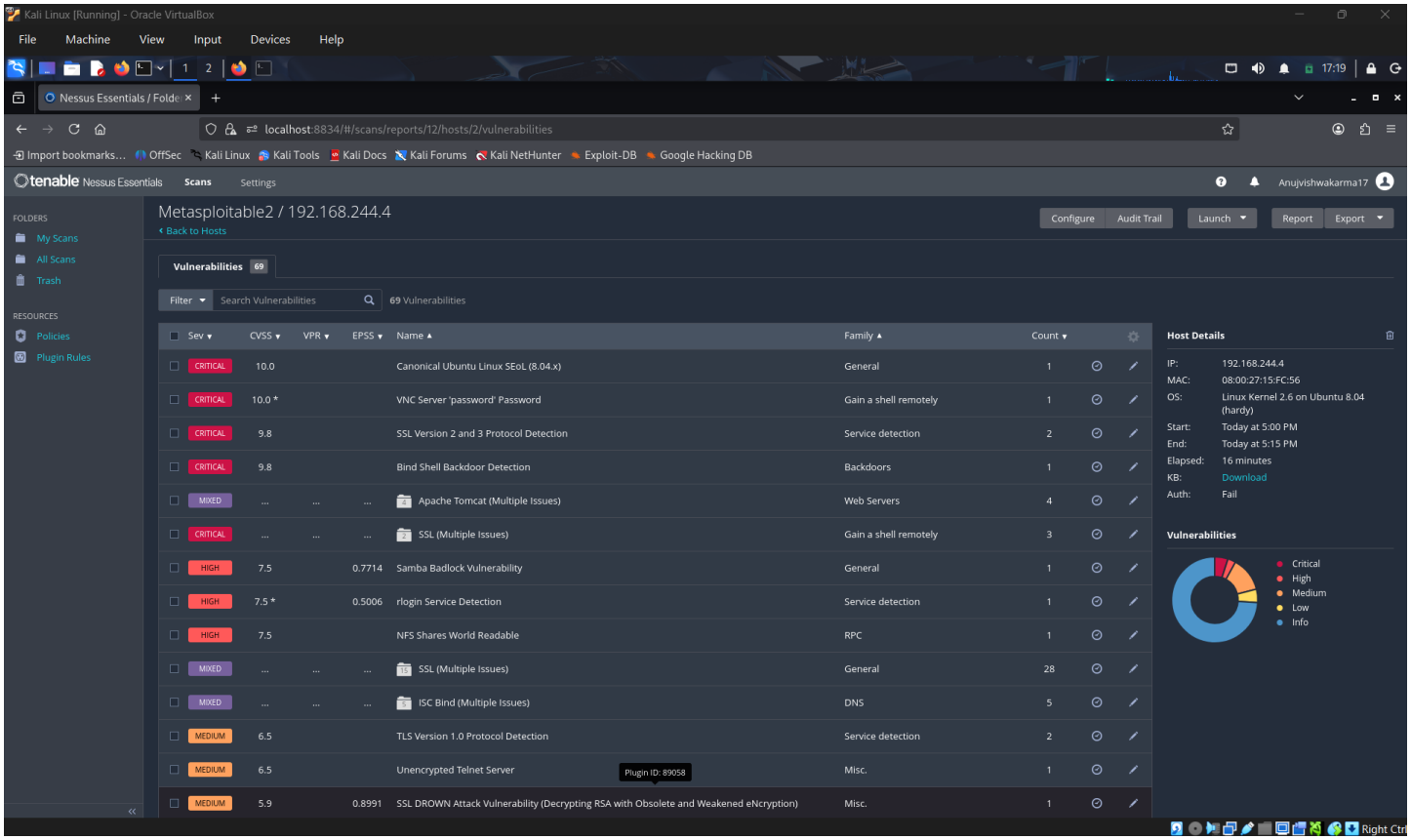

Figure 2: Vulnerability scan results

6. Critical Vulnerability Identified:

A critical vulnerability was detected indicating the presence of a backdoor service.

This vulnerability could allow unauthorized access to the system.

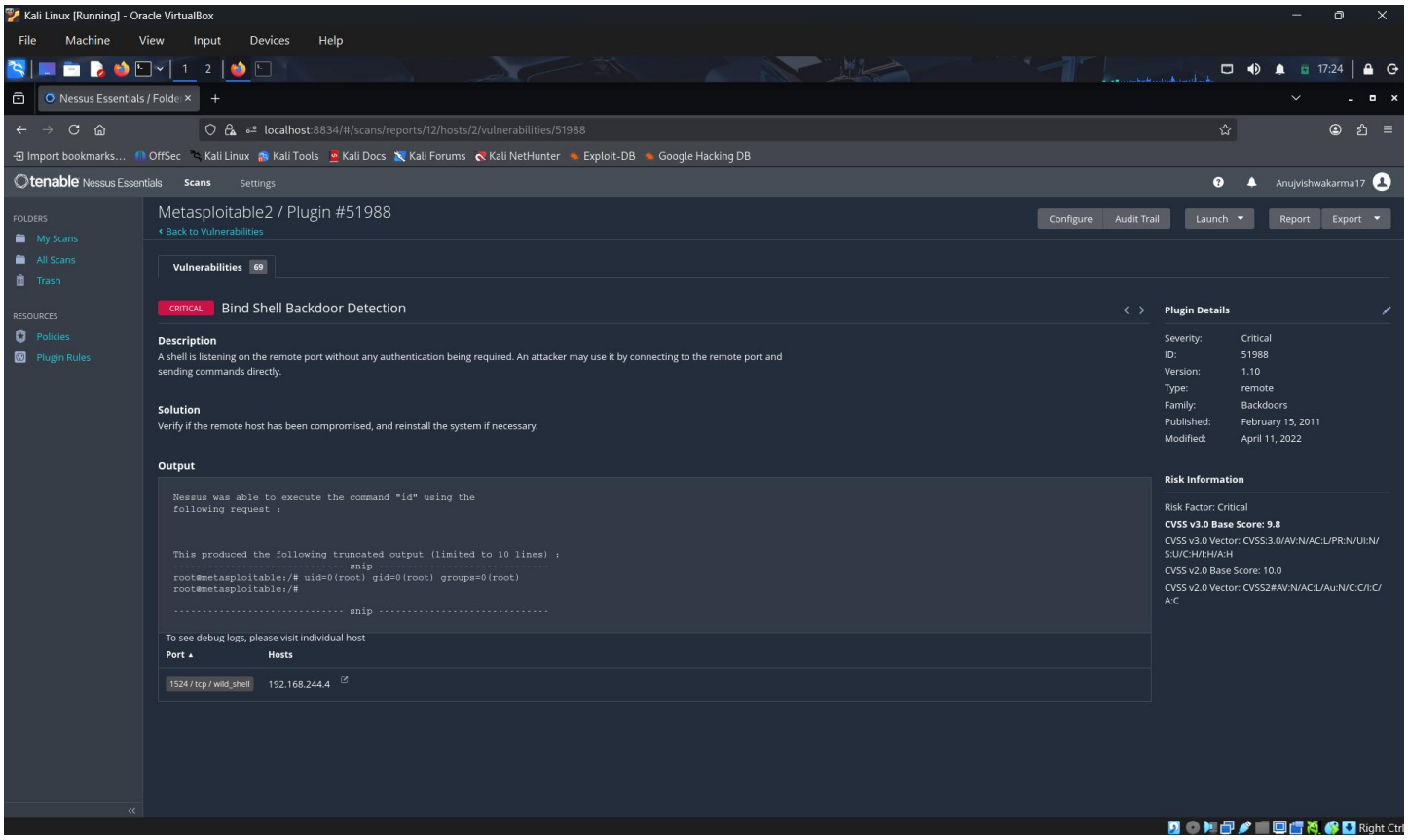

Figure 3: Critical vulnerability detected

7. Vulnerability Summary:

Example vulnerability findings:

Severity	Description
Critical	Backdoor service detected
High	Outdated service version
Medium	Security misconfiguration
Low	Information disclosure

These vulnerabilities indicate potential security risks in the system.

8. Analysis:

The vulnerability scan revealed that the target system contains multiple security weaknesses. The presence of outdated services and backdoor vulnerabilities significantly increases the risk of system compromise.

Attackers could exploit these vulnerabilities to gain unauthorized access, execute malicious code, or compromise system integrity.

This highlights the importance of regular vulnerability scanning and security patching.

9. Security Recommendations:

To improve system security, the following measures are recommended:

• Remove unnecessary services.
• Update outdated software.
• Apply security patches.
• Configure firewall rules.
• Regularly perform vulnerability scans.

10. Conclusion:

The Nessus vulnerability assessment successfully identified critical vulnerabilities and security weaknesses in the target system.

The scan provided valuable insights into potential threats and exposed services. Nessus Essentials proved to be an effective tool for vulnerability assessment and security analysis.

This activity enhanced practical knowledge of vulnerability detection and security assessment methodologies used in cybersecurity.

------X------X------X------