Pragadeesh V S

Vulnerability Assessment Report using Nessus Essentials

1. Introduction

This report documents an introductory vulnerability assessment performed using Nessus Essentials. The assessment aims to identify vulnerabilities present in a local machine, understand the associated risks, and explore basic mitigation strategies. Additionally, common phishing techniques are analyzed to build awareness.

2. Tools Used

Nessus Essentials was used for this vulnerability assessment. Nessus is a well-known and widely-used vulnerability scanner that provides comprehensive and detailed vulnerability information. The Essentials version is free but requires registration.

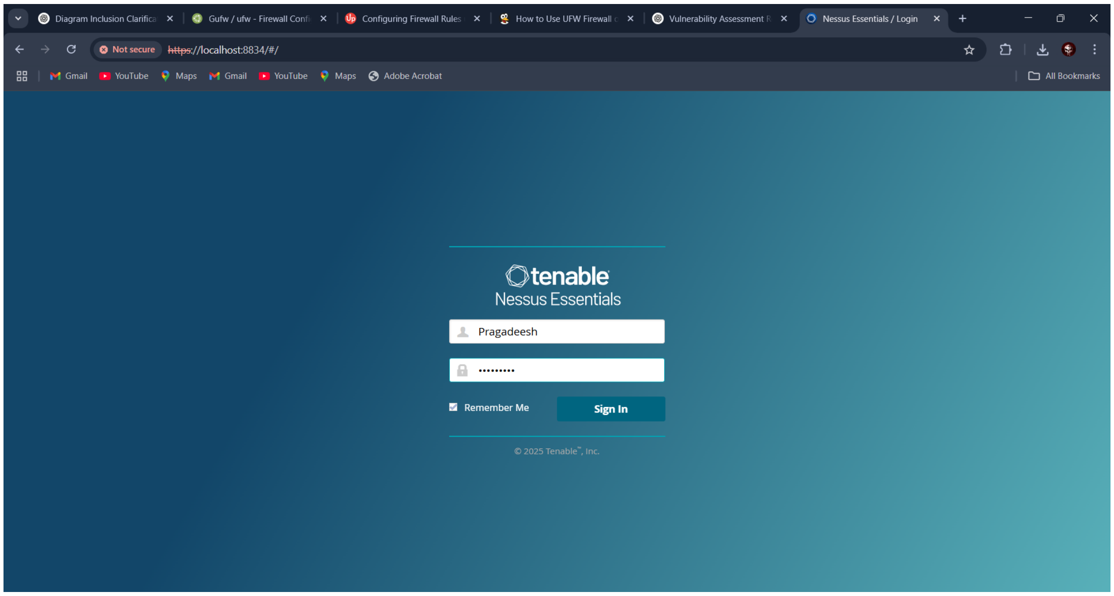
Diagram Inclusion Clarifica
Gufw / ufw - Firewall Confi
Configuring Firewall Rules
How to Use UFW Firewall c
Vulnerability Assessment R
Nessus Essentials / Login
Not secure
Gmail
YouTube
Maps
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
tenable
Nessus Essentials
Remember Me
Sign In
© 2025 Tenable™, Inc.

~~https~~://localhost:8834/#/

Pragadeesh

•••••••••

☑ Remember Me

3. Scan Setup and Execution

The scan was targeted at the local machine IP (localhost). A full vulnerability scan was initiated and allowed to complete (approximately 30–60 minutes). The scan results were reviewed to identify critical issues.

4. Critical Vulnerabilities Identified

The following are examples of critical vulnerabilities that may be identified during a scan:

- CVE-2021-34527 (PrintNightmare): Allows remote code execution via Print Spooler service.

- CVE-2020-0601 (Windows CryptoAPI Spoofing): Could allow attackers to spoof certificates.

- CVE-2017-0144 (EternalBlue): Exploited by WannaCry ransomware.

5. Suggested Fixes and Mitigations

Recommended mitigations include:

- Applying security updates and patches from the operating system vendor
- Disabling unnecessary or vulnerable services
- Using endpoint protection and host-based firewalls
- Conducting regular vulnerability scans and audits

6. Phishing Email Examples and Analysis

Below are real-world inspired phishing emails and the flaws that indicate they are phishing attempts.

Example 1: Bank Account Alert

Subject: Urgent: Unusual Activity Detected on Your Bank Account

Body:
Dear Customer,

We have detected unusual activity on your bank account. Please log in immediately to verify your transactions: http://secure-update-login.com.

Thank you,
Bank Security Team

Flaws Identified:

- Fake URL that mimics bank login page but is a malicious domain

- Urgency to provoke immediate action

- Generic greeting without user's name

7. Conclusion

This vulnerability assessment using Nessus Essentials has provided practical experience in identifying system vulnerabilities and understanding their risks. Additionally, recognizing phishing emails based on common red flags helps in developing essential cyber hygiene practices.