Project Report

Identifying and Mitigating Network Vulnerabilities using Nessus

CYBER SECURITY

INTERNSHIP

AT

EXTION INFOTECH

Submitted by :-

KARTIK MADAAN

Nessus Report Index

About Me

Enthusiastic and skilled third-year B.Tech [Computer Science And Engineering (Cyber Security)] student. I am hardworking, punctual and honest. Always keen to work in all circumstances to gain strength, confidence and always ready to learn new things to take up future endeavors under the guidance of seniors and mentors.

Contact

E-mail|LinkedIn

Introduction

- Project objective

The main goal of this project is used to Tenable Nesses to identify and address network vulnerabilities. This report covers the entire process, including setting up of the environment, conducting vulnerability scans, analyzing the result, the implementing mitigation strategies to improve the network's overall security.

- Background

Network Wellness abilities can lead to data breaches, unauthorized access and denial of service attacks. It's essential to identify these vulnerability to maintain a secure and strong network infrastructure. Tenable Nesses has established itself as a cornerstone in the field of vulnerability assessment, providing organizations with the tools they need to identify the address security weakness effectively.

- Scan objectives

a) Identify at least five vulnerabilities in the network.
b) Provide detailed report on each vulnerability.
c) Provide recommendations for mitigation identified vulnerabilities.

Overview of Nessus

1. Historical Development and Evolution.

The journey of Nessus began in the late 1990s when Renaud Deraison, motivated by the need of better vulnerability assessment tools, created the initial version of Nessus. Originally an open source project, Nessus provided a platform for security professionals to identify vulnerabilities in their systems. Its open source nature allowed for community contribution and rapid updates for string a collaborative approach to cybersecurity.

In 2005 Tenable Inc. acquired Nessus, Transitioning it from an open source project to a commercial product. This transition introduced new features, enhanced functionality and a more structured support model. Despite this shift, tenable continue to maintain a free version of Nessus, known as Nessus essential for personal and educational use.

2. What is Nessus?

Nessus is a widely used vulnerability scanning tool developed by Tenable, Inc. It is designed to identify security vulnerabilities in computer systems, networks and applications. By detecting these vulnerabilities Nessus helps organization to mitigate potential security risk before they can exploited by attackers. Originally developed by Renaud Deraison in 1998, Nessus has evolved into a robust tool used globally by security professional to enhance their cybersecurity posture.

3. Key Features of Nessus

Vulnerability Scanning

Nessus performs comprehensive scans of systems and networks to identify known vulnerabilities. It uses a continually updated database of vulnerability signatures and threat intelligence to detect security issues across various components, including operating systems, applications, and network devices.

Extensive Plugin Library

Nessus utilizes a large library of plugins that are regularly updated to address new vulnerabilities and threats. Each plugin is designed to check for specific vulnerabilities or configuration issues. This extensive library ensures that Nessus can provide thorough coverage of known security issues.

Customizable Scan Policies

Users can create and customize scan policies to tailor assessments to their specific needs. Nessus allows users to define scan parameters, select specific plugins, and configure settings to focus on particular areas of interest or compliance requirements.

Detailed Reporting

After completing a scan, Nessus generates detailed reports that provide insights into identified vulnerabilities. These reports include information on the nature and severity of each vulnerability, along with recommendations for remediation. Reports can be customized to include specific details and formats.

Integration and Automation

Nessus integrates with a variety of security tools and platforms, such as security information and event management (SIEM) systems, ticketing systems, and network management tools. It also supports automation through its API, allowing organizations to incorporate vulnerability scanning into their continuous security monitoring and incident response processes

User-Friendly Interface

Nessus features a user-friendly web-based interface that simplifies the configuration and management of scans. The interface provides easy access to scan settings, results, and reports, making it accessible for users with varying levels of expertise.

4. Advantages Of Nessus

Comprehensive Vulnerability Detection

Nessus provides a thorough assessment of systems and networks by identifying a wide range of vulnerabilities. Its extensive plugin library and regular updates ensure that it can detect both common and emerging threats.

User-Friendly Interface

The web-based interface of Nessus is intuitive and easy to navigate. It simplifies the process of configuring scans, reviewing results, and generating reports, making it accessible to users with varying levels of expertise.

Customizability

Nessus offers flexible configuration options, allowing users to create customized scan policies and tailor assessments to their specific needs. This customization enhances the effectiveness of vulnerability management and ensures that scans align with organizational requirements.

Integration and Automation

Nessus integrates with other security tools and platforms, facilitating seamless integration into broader security operations. Its automation capabilities, through API support, enable organizations to incorporate vulnerability scanning into continuous monitoring and incident response workflows.

Cost-Effective

Nessus provides a cost-effective solution for vulnerability assessment compared to other tools in the market. Its scalability makes it suitable for organizations of all sizes, and its comprehensive features help avoid costly security breaches and incidents.

Regular Updates and Support

Tenable provides regular updates to Nessus, including new plugins and features, to address evolving threats. Additionally, users have access to support resources, including documentation, forums, and customer support, to assist with any issues or questions.

Setup Up Nessus

Download and Installation

To set up Nessus, follow these steps:

- **Download**: Visit the Tenable website to download the appropriate Nessus version for your operating system (Windows, Linux, macOS).
- **Install**: Follow the installation instructions provided for your operating system. This typically involves running an installer or package manager to complete the setup.

Initial Configuration

After installation, you need to configure Nessus:

- **Access the Web Interface**: Open a web browser and navigate to the Nessus web interface, typically accessible via https://localhost:8834 or the IP address of the server where Nessus is installed.
- **Create an Account**: The first time you access the interface, you will be prompted to create an administrator account. Provide the necessary information and create a secure password.
- **License Activation**: Enter your Nessus license key or select the free version (Nessus Essentials) if you are using it for personal or non- commercial use. Follow the prompts to activate the license.

Update Plugins

Nessus requires regular updates to its plugin database to stay current with the latest vulnerabilities. After initial setup, Nessus will automatically download and update plugins. You can also manually trigger updates from the web interface.

Configuration

Create and Configure Scan Policies

- **Scan Policy Creation**: In the Nessus web interface, navigate to the "Policies" section and create a new scan policy. Define the policy settings, including the type of scan (e.g., basic network scan, web application scan), target systems, and specific plugins to use.
- **Customize Settings**: Configure additional settings such as scan schedules, authentication credentials, and advanced options based on your requirements.

Set Up and Launch Scans

- **Define Targets**: In the "Scans" section, create a new scan by specifying the target systems or network ranges. Enter relevant information, such as IP addresses or hostnames.
- **Apply Policies**: Select the scan policy you created and apply it to the scan.
- **Run the Scan**: Start the scan by clicking the appropriate option in the interface. Monitor the progress and results through the web interface.

Review and Analyze Results

- **View Results:** Once the scan is complete, review the results in the "Reports" section. Nessus provides detailed information on identified vulnerabilities, including severity levels and potential impacts.

- **Remediation**: Use the recommendations provided in the reports to address and remediate identified vulnerabilities. Nessus may also offer guidance on best practices and mitigation strategies.

Vulnerability Identification

The results that were outputted by the vulnerability scanner:
Nessus were categorized according to the National Vulnerability Database Common Vulnerability Scoring system (CVSS) through five score metrics: Critical, High, Medium, Low or Informational.

- **Critical:** These are vulnerabilities with a CVSS score of 9.0 to 10.0, that indicate they can be easily exploited by an attacker and system can be compromised.
- **High:** Vulnerabilities with a CVSS score of 7.0 to 8.9, that indicate local users can gain privileges that can allow unauthenticated remote users to view resources or cause a denial of service.
- **Medium:** Vulnerabilities with a CVSS score of 4.0 to 6.9, that indicate flaws that may be difficult for third parties to exploit but are cause for concern as they can still lead to compromise.
- **Low:** Vulnerabilities with CVSS score of 0.1 to 3.9, that indicate vulnerabilities that if exploited may cause either no adverse effect or minimal adverse consequences.

Report of Vulnerability via Nessus

VULNERABILITY SCAN WIN 7

Report generated by Tenable Nessus™ Tue, 14 Jan 2025 23:25:55 IST

TABLE OF CONTENTS

192.168.1.13

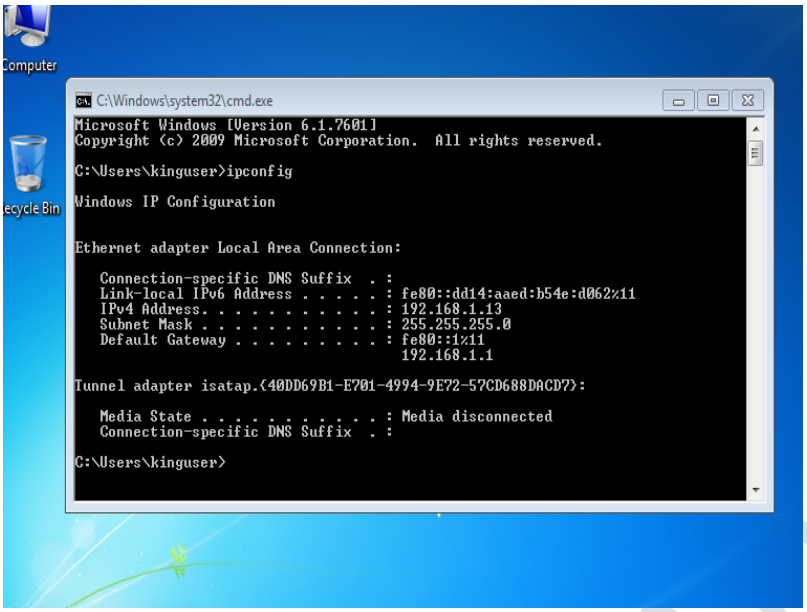
Vulnerabilities Total: 35

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.5	0.9752	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentiale check)
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.3	0.8244	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remot Code Execution (2509553) (remote check)
HIGH	8.1	9.8	0.9719	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3*	9.6	0.7951	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Rem Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	6.0	0.0224	90510	MS16-047: Security Update for SAM and LSAD Remote Protoc (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	0.0053	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	4.0	-	-	58453	Terminal Services Doesn't Use Network Level Authentication (Only
MEDIUM	4.3*	-	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration

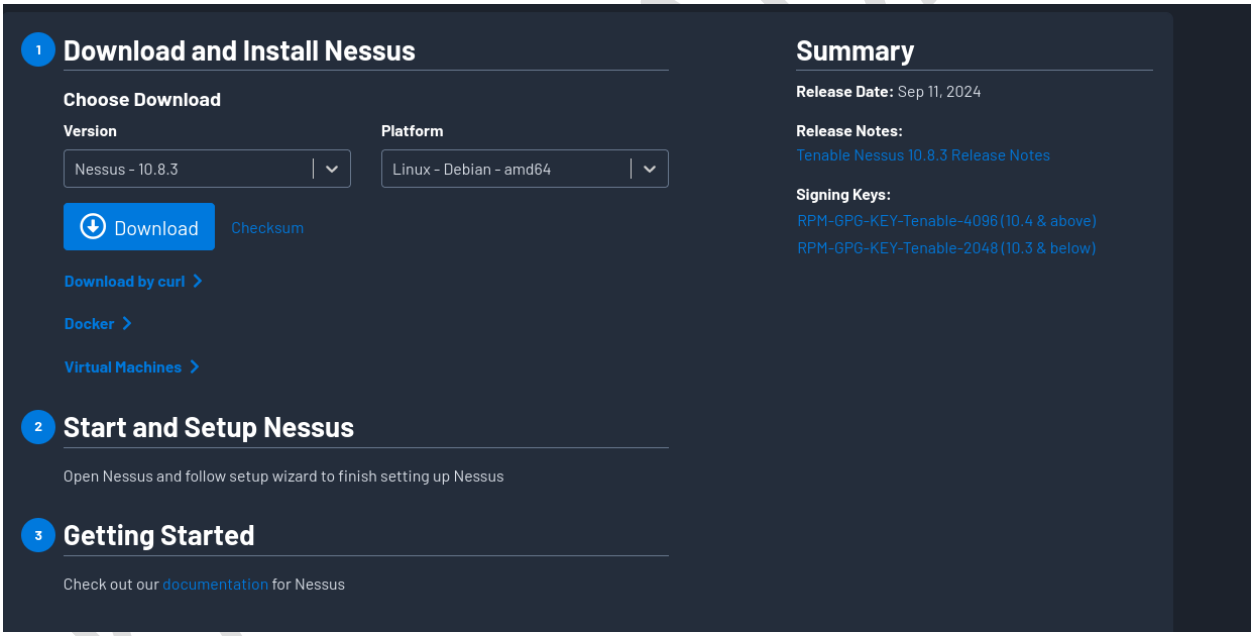
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remc check)
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

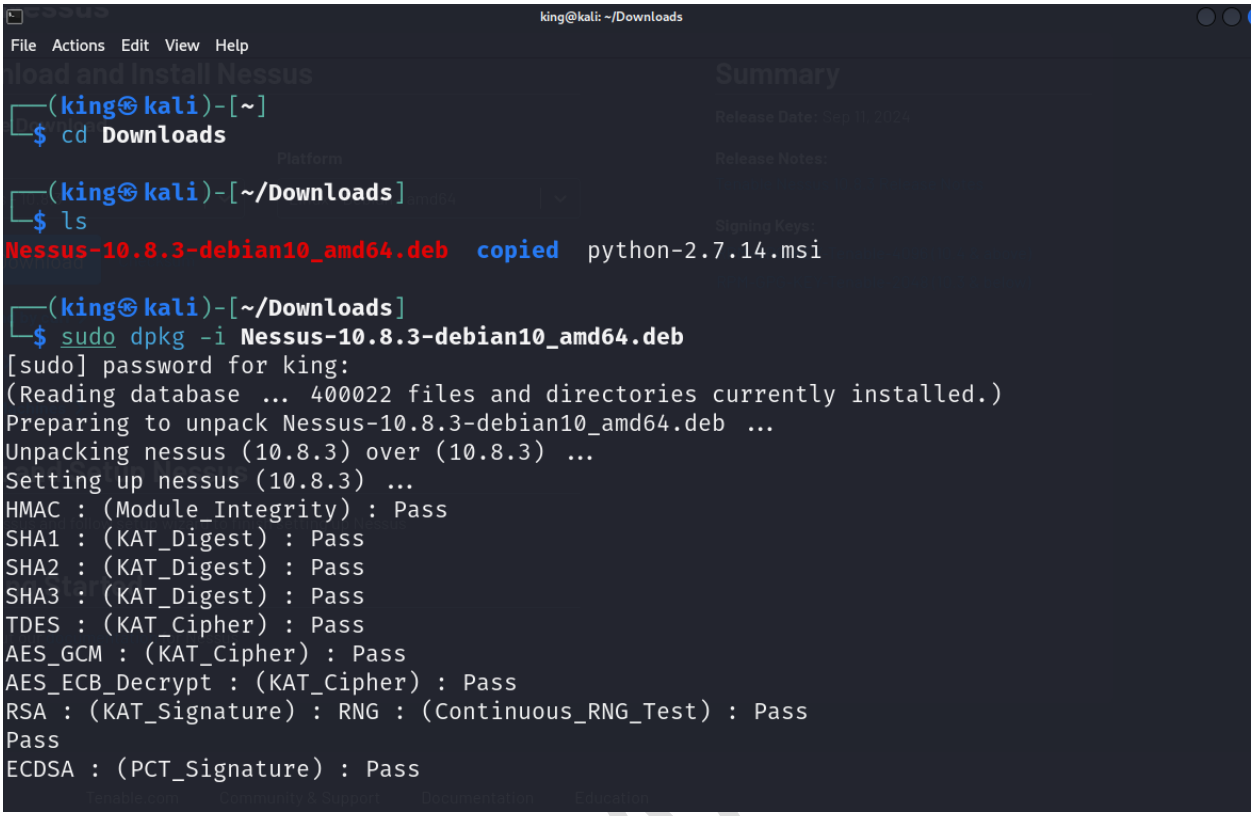
* indicates the v3.0 score was not available; the v2.0 score is shown

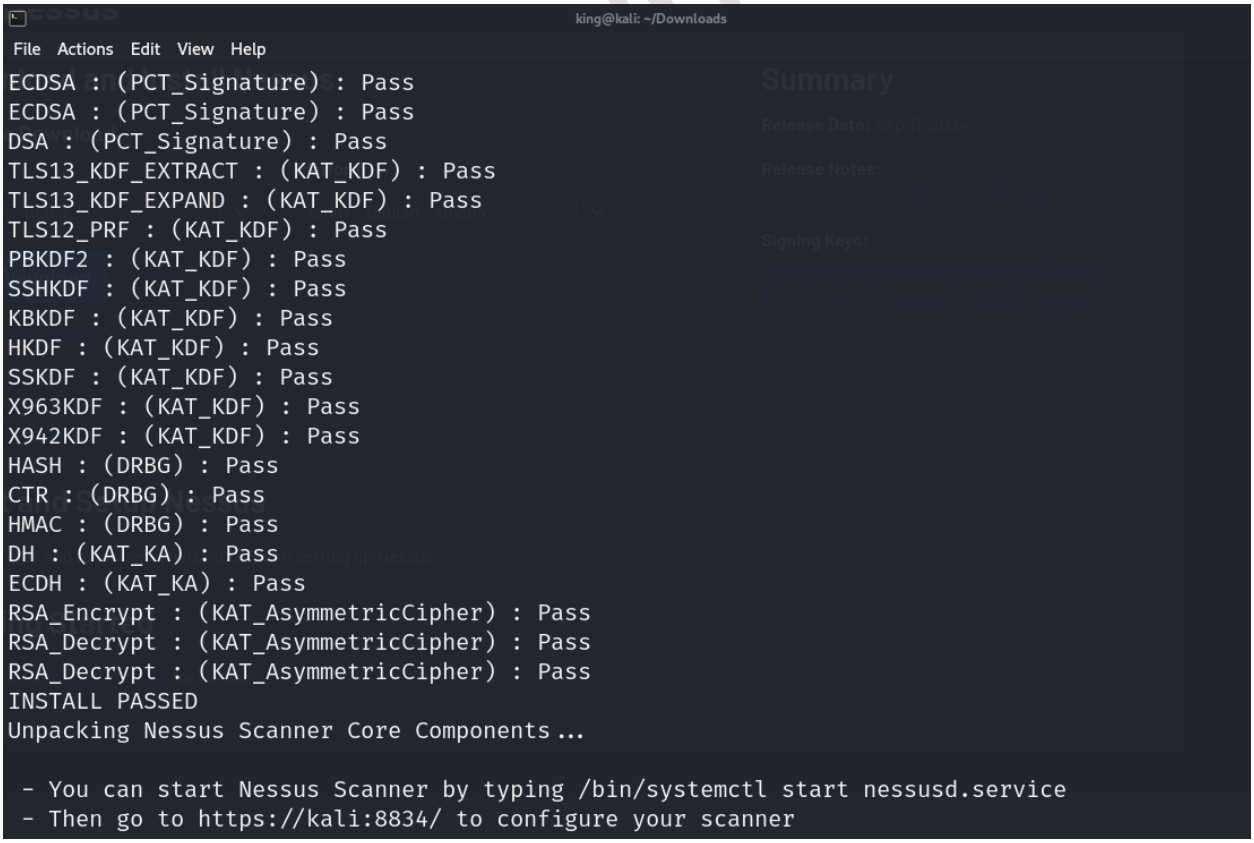
Steps to Perform the Vulnerability Assessment



MACHINE ON WHICH ASSESMENT PERFORM AND ITS IP ADDRESS




king@kali: ~/Downloads
File Actions Edit View Help
┌──(king㉿kali)-[~]
└─$ cd Downloads
┌──(king㉿kali)-[~/Downloads]
└─$ ls
Nessus-10.8.3-debian10_amd64.deb copied python-2.7.14.msi
┌──(king㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb
[sudo] password for king:
(Reading database ... 400022 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) over (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass

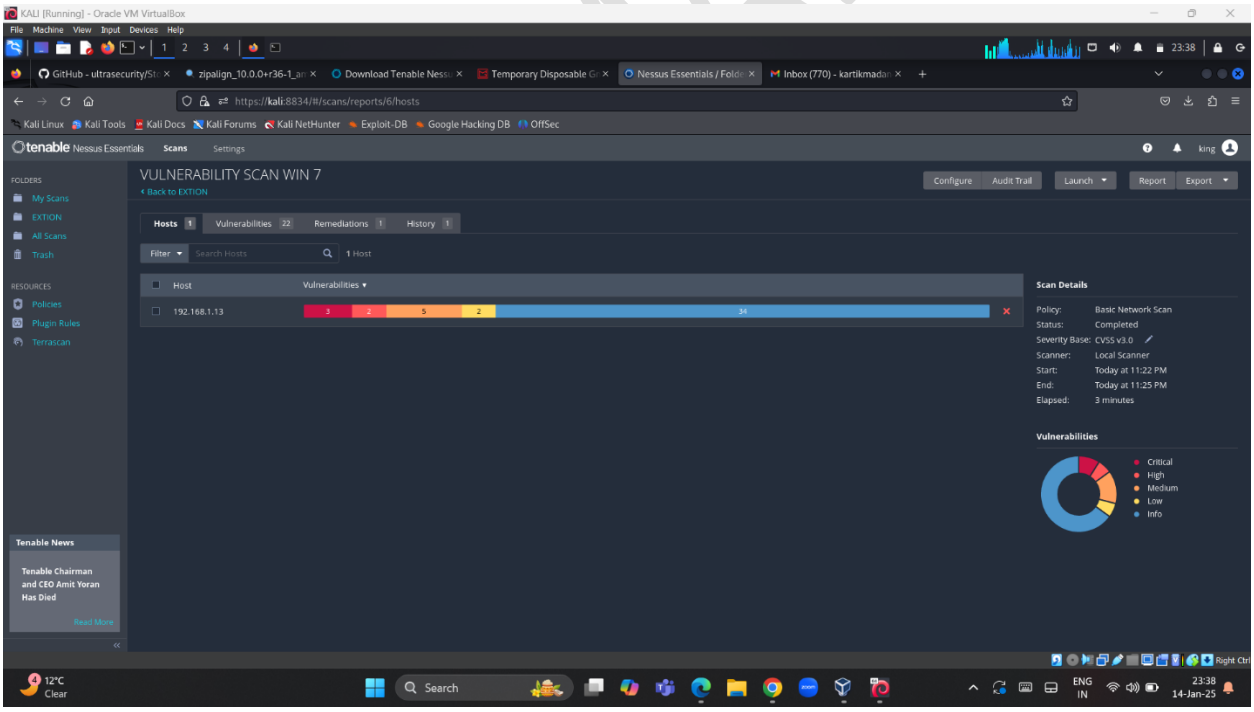

king@kali: ~/Downloads
File Actions Edit View Help
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

```
┌──(king㉿kali)-[~/Downloads]
└─$ /bin/systemctl start nessusd.service

┌──(king㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd

┌──(king㉿kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-01-14 23:35:52 IST; 56s ago
 Invocation: 2af8e69ca5f24af4b84906cf84875960
   Main PID: 57828 (nessus-service)
      Tasks: 15 (limit: 2272)
     Memory: 425.9M (peak: 471.7M)
        CPU: 46.722s
     CGroup: /system.slice/nessusd.service
             ├─57828 /opt/nessus/sbin/nessus-service -q
             └─57832 nessusd -q

Jan 14 23:35:52 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jan 14 23:36:26 kali nessus-service[57832]: Cached 303 plugin libs in 124msec
Jan 14 23:36:26 kali nessus-service[57832]: Cached 303 plugin libs in 185msec
```



Vulnerability and Mitigation of Identified Vulnerability

Vulnerability Identification

The following five critical vulnerabilities have been identified from the report:

1. Microsoft RDP Remote Code Execution (CVE-2019-0708)

- **Severity**: Critical (CVSS 9.8, VPR Score 9.5)
- **Potential Impact:**

  1. Exploitable remotely without authentication.

  2. Could allow an attacker to execute arbitrary code and take control of the system (e.g., BlueKeep exploit).

- **Recommended Mitigation:**

1. Apply the patch released by Microsoft for CVE-2019-0708.
2. Disable Remote Desktop Protocol (RDP) if not needed.
3. Restrict RDP access to internal networks using a VPN.
4. Enable Network Level Authentication (NLA) to require authentication before a session is established.

2. Unsupported Windows OS

- **Severity**: Critical (CVSS 10.0)
- **Potential Impact:**

  1. Unsupported operating systems do not receive security updates, making them highly vulnerable to attacks.
  2. Poses risks of malware, ransomware, and unauthorized access.

- **Recommended Mitigation:**

1. Upgrade the system to a supported Windows OS (e.g., Windows 10 or 11).
2. For legacy systems, use network isolation or air-gapped environments.
3. Implement endpoint protection solutions and monitor for anomalous activity.

3. MS11-030: Vulnerability in DNS Resolution

- **Severity**: Critical (CVSS 10.0)
- **Potential Impact:**
  1. Allows remote attackers to execute arbitrary code by sending malicious DNS responses.
  2. Could lead to denial of service or system compromise.
- **Recommended Mitigation:**

1. Apply the Microsoft security update MS11-030.
2. Restrict DNS responses to trusted sources and limit DNS recursion.
3. Monitor DNS traffic for unusual activity.

4. MS17-010: Windows SMB Vulnerabilities

- **Severity**: High (CVSS 8.1, VPR Score 9.8)
- **Potential Impact:**
  1. Exploited by EternalBlue and related threats like WannaCry.
  2. Could allow remote code execution and lateral movement within the network.
- **Recommended Mitigation:**

1. Apply patches from Microsoft's security update MS17-010.
2. Disable SMBv1 if not required.
3. Implement firewall rules to block SMB traffic from untrusted networks.

5. MS12-020: RDP Vulnerabilities

- **Severity**: High (CVSS 9.3, VPR Score 9.6)
- **Potential Impact:**
  1. Remote attackers can exploit these vulnerabilities to execute code on affected systems.
  2. Could lead to data theft, lateral movement, or complete system compromise.
- **Recommended Mitigation:**

1. Apply the MS12-020 patch from Microsoft.

2. Restrict access to RDP ports using firewalls or VPNs.
3. Enable multi-factor authentication for remote access.

Mitigation Plan

The following step-by-step mitigation plan addresses the identified vulnerabilities:

1. Microsoft RDP RCE (BlueKeep - CVE-2019-0708)

- **Steps:**

1. Download and install the latest patch for CVE-2019-0708 from Microsoft's official website.
2. Disable RDP temporarily during patch deployment to avoid exposure.
3. Implement Network Level Authentication (NLA) via group policy.
4. Use a VPN for accessing RDP services remotely.

- Timeline: 1–2 days.
- Resources: IT admin expertise, access to Microsoft patches.

2. Unsupported Windows OS

- **Steps:**

1. Identify systems running unsupported versions (e.g., Windows 7).
2. Plan for OS upgrades to Windows 10 or 11, including compatibility checks.
3. For systems that cannot be upgraded, isolate them in a VLAN and restrict internet access.

- Timeline: 1–2 weeks.
- Resources: IT admin for upgrades, budget for software licenses.

3. MS11-030 (DNS Resolution Vulnerability)

- **Steps:**

1. Apply the MS11-030 patch across all affected machines.
2. Configure DNS servers to only accept responses from trusted sources.
3. Enable DNSSEC to validate DNS responses.

- Timeline: 1–3 days.
- Resources: Microsoft patch repository, network admin for DNS configuration.

4. MS17-010 (SMB Vulnerabilities)

- **Steps:**

1. Install the MS17-010 patch on all affected systems.
2. Disable SMBv1 via group policy or manually.
3. Set up firewall rules to block incoming SMB traffic from external networks.

- Timeline: 1–2 days.
- Resources: IT admin expertise, access to firewall management tools.

5. MS12-020 (RDP Vulnerabilities)

- **Steps:**

1. Apply the MS12-020 security update.
2. Configure RDP to only allow secure connections (TLS 1.2 or higher).
3. Regularly monitor RDP logs for unauthorized attempts.

- Timeline: 1–2 days.
- Resources: Microsoft patch repository, IT security tools.

Conclusion

1. Project Outcomes

This project successfully identified and mitigated numerous network vulnerabilities using Nessus. The comprehensive scanning and analysis provided valuable insights into the security posture of the network, enabling targeted and effective remediation efforts.

2. Future Work

Future work includes establishing a regular vulnerability assessment schedule, continuous monitoring for new threats, and ongoing improvements to the network security infrastructure. Adopting a proactive approach to network security will help maintain a robust and resilient network environment.