
**GROUP ASSIGNMENT**

| | | |
|---|---|---|
| **NAME (TP NUMBER)** | **:** | Suryakrishnan Balamurugan (TP080525)<br>Koo Wai Kit (TP081761)<br>Mostafa Aldabeeb (TP079442) |
| **INTAKE CODE** | **:** | APUMF2406CYS |
| **MODULE TITLE** | **:** | CT112-3-M-Advanced Ethical Hacking |
| **MODULE LECTURER** | **:** | Ts. Dr. Vinesha A/P Selvarajah |
| **PROJECT TITLE** | | Vulnerability Assessment, Risk Analysis and Policy Formulation |
| **DATE ASSIGNED** | **:** | 25 November 2024 |
| **DATE COMPLETED** | **:** | 7 February 2025 |

# Table of Contents

# List of Figures



# List of Tables

# 1.0 Introduction

Organisations now depend on online systems to reach their goals while improving performance because of the rapid technological advancements at the workplace. ShopEase Indonesia stands as an Indonesian e-commerce firm which maintains a position among major market players. The firm experienced a major growth in both customer count and operational scale while facing increasing cyber-attacks recently. A major cyber-attack on ShopEase's database led the company's CTO Maya Suhendra to issue an order for a security audit of the organization's internal IT environment.

The assessment analyses VMware snapshot risks of a Windows Server 2008 virtual machine (VM) to detect threats which could compromise confidentiality, integrity and availability of the platform. Company assets need vulnerability assessments to maintain security while such assessments serve three essential purposes: customer confidence building, regulatory compliance and legal protection against future incidents.

OpenVAS serves as the vulnerability assessment tool for this report to establish a standardized scanning protocol which meets industry recognition standards. The assessment reveals three critical results which detail ShopEase Indonesia's security risks with recommended countermeasures and policy adjustments to minimize potential threats. The primary focus aims to strengthen ShopEase's website security while building up its IT environment's overall resilience.

## 1.1 Selection of a Vulnerability Scanning Tool

OpenVAS (Open Vulnerability Assessment Scanner) serves as the selected vulnerability scanning tool for this project. The selection of OpenVAS as vulnerability scanning tool emerged from an extensive evaluation against Nessus which established its position as another popular scanning solution. OpenVAS is selected for this project due to its robust capabilities combined with cost-effectiveness and flexible features.

### 1.1.1 OpenVAS

OpenVAS stands as an open-source vulnerability scanner because it provides detailed vulnerability monitoring capabilities. OpenVAS executes authenticated alongside unauthenticated scans while operating with numerous high-level and low-level Internet protocols. The OpenVAS database includes Network Vulnerability Tests (NVTs) that receive

continuous updates to detect both established vulnerabilities alongside newly emerging threats (Greenbone Community Edition – Documentation, n.d.). The tool proves ideal for Windows Server 2008 scanning because it effectively detects many existing vulnerabilities in the platform.

OpenVAS functions as an open-source technology which provides users with substantial adaptability options. Users gain access to customization options for this tool's functionality which helps them fulfil their assessment needs beyond what proprietary systems typically provide. OpenVAS integrates with the Greenbone Security Assistant (GSA) which offers both a simple web-based scanning interface and detailed report generation. The tool generates reports which break down vulnerabilities into risk categories while delivering step-by-step security recommendations for simpler issue prioritization (Greenbone Community Edition – Documentation, n.d.).

OpenVAS operates with certain operational constraints. The tool requires significant processing power particularly for extensive network scans while its installation and customization demand higher technical skill levels than standard proprietary tools demand.

### 1.1.2 Nessus

The vulnerability scanning software Nessus which Tenable developed has gained recognition for its precision and simple interface design. The system delivers an intuitive interface alongside extensive scanning features which enable complete vulnerability discovery and comprehensive compliance verification. Nessus demonstrates exceptional speed combined with efficiency when performing scans in enterprise-sized environments that need regular assessments. Prebuilt policies in Nessus support different compliance standards helping organizations with regulatory needs to simplify their scanning operations (Tenable Nessus® Professional, n.d.).

The strengths of Nessus scanning platform are overshadowed by its major limitations. Its cost emerges as the main drawback of this system. Small organizations along with academic programs may find Nessus unaffordable because it operates under a proprietary model. Its closed-source nature prevents users from achieving the same detailed customization or transparent operation which OpenVAS offers. Enterprise environments benefit from Nessus, but its high costs and limited adaptability eliminate its effectiveness for small budget projects requiring unique functionality.

### 1.1.3 Justification for Choosing OpenVAS

1. **Cost-Effectiveness**: OpenVAS operates as an open-source platform so users can obtain its functionality without payment, which makes it suitable for organizations working with budget constraints. Nessus demands payment for its licensing model and poses substantial financial costs for projects that can afford only limited funds.
2. **Comprehensive Vulnerability Detection**: Through regular updates of its NVT database OpenVAS achieves detailed vulnerability monitoring. Windows Server 2008 system assessment benefits from this capability because it detects existing vulnerabilities in addition to future threats through its thorough detection methods.
3. **Flexibility and Customization**: Users can modify OpenVAS beyond its default capabilities to adapt it for precise assessment requirements which Nessus does not support. OpenVAS delivers excellent flexibility to academic projects and smaller organizations because it provides customizable solutions.
4. **Integration and Reporting**: OpenVAS works with the Greenbone Security Assistant (GSA) to deliver a robust web interface that both configures scans and presents assessment results. The vulnerability reports from OpenVAS classify security flaws by their risk severity while delivering specific remediation guidance for targeted fixes.

Nessus remains a strong contender because of fast scanning speed and enterprise-grade features yet its high licensing fees combined with limited customization impede its usefulness for this project. OpenVAS demonstrates superior compatibility with project needs due to its budget-friendly nature and extensive vulnerability detection abilities and adaptable framework.

## 1.2 Proposed Scanning Methodology

For the scanning, we will be using GSA to manage the scan operations performed by OpenVAS. The scanning process is divided into several phases, consisting of preparation, configuration, execution, analysis, and reporting phases. Each phase is important to ensure that the scan is thorough, accurate and effective. The order of the phases is illustrated in Figure 1.


*Figure 1: Phases in the scanning methodology*

### 1.2.1 Preparation Phase

- **Asset Inventory**: While the VM contains only the Windows Server 2008 R2, a list of all installed applications and services, as well as all established network connections should be made.
- **Credential Management**: Gather the necessary administrative permissions as authenticated scans will reveal additional details about the weaknesses in a system's security.
- **Import VM**: Import the victim's VMware file into VMware Workstation.
- **Sign In as Administrator**: On the target machine, a password is required to sign into the administrator account. Since no password was provided, test a few common passwords. The password 'P@ssw0rd' is valid and grants access to sign in as the administrator.
- **Install and Update OpenVAS**: Install and set up OpenVAS in a separate VM that functions as the scanning machine. If OpenVAS was installed previously, update the application for the latest Network Vulnerability Tests that are used in identifying the latest vulnerabilities.
- **Whitelist Traffic**: Check for firewalls or other security mechanisms on the target VM. If there are any, turn off the security features that will block OpenVAS scanning traffic.

### 1.2.2 Configuration Phase

- **Define Scan Scope**: Determine the target machine's IP address. The vulnerability scanning will be conducted based on this IP address.
- **Create New Target in GVM Web Interface**: Create a new target to scan using the target machine's IP address.
- **Create New Scan Task in GVM Web Interface**: Create a new task to start scanning the target machine. Configure the scan with specific settings that apply to the target VM.

### 1.2.3 Execution Phase

- **Perform Scan**: Start an automated scan to determine the weaknesses of the target machine.
- **Monitor Scan Progress**: Monitor the progress of the scanning process to ensure there are no disruptions or incomplete results.

### 1.2.4 Analysis Phase

- **Remediation Prioritisation**: Prioritise remediation efforts based on the assigned severity level of each vulnerability (high, medium, low).
- **Impact Assessment**: Evaluate the impact for each vulnerability if they are exploited.

### 1.2.5 Reporting Phase

- **Documentation**: Keep detailed records the scanning methods and results for any future validation or compliance purposes.
- **Develop Plan**: For the identified vulnerabilities, develop risk assessment plan and policies to address the vulnerabilities.
- **Final Report**: Develop a final report for stakeholders that combines findings, remediation, and recommended improvements.

# 2.0 Vulnerability Assessment, Risk Analysis, and Policy Formulation

The research investigates the cybersecurity threats encountered by ShopEase Indonesia. The assessment of Windows 2008 Server VM will reveal security weaknesses that need remediation. A detailed examination of each vulnerability will be provided before moving on to risk assessments which evaluate business impact scenarios from vulnerability exploitation. An overview of the studied vulnerabilities is shown in Figure 2. The final section will deliver policy recommendations that help reduce security risks.

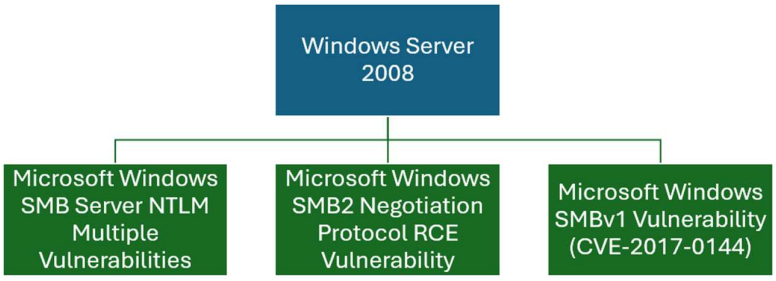


*Figure 2: Overview of identified vulnerabilities*

The tasks will produce a complete report which displays vulnerability findings alongside risk assessments and mitigation strategies and policy recommendations to enhance ShopEase Indonesia's security posture.

## 2.1 Microsoft Windows SMB Server NTLM Multiple Vulnerabilities

As per the scan report produced by OpenVAS, The Microsoft Windows SMB Server NTLM Multiple Vulnerabilities which is identified as 971468 consists of four critical flaws which affects the Server Message Block (SMB) protocol and the NTLM authentication mechanism. These are known as CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, and CVE-2010-0231, and affect multiple versions of Windows, including the Windows Server 2008. The vulnerabilities have a CVSS score of 10.0, meaning that they are critical, they can result to remote code execution, denial of service (DoS) and authentication bypassing.

All these vulnerabilities were discovered and were covered under Microsoft Security Bulletin MS10-012 in February 2010 (Microsoft Security Bulletin MS10-012 - Important, 2010). These issues stem from Host Input Validation, Race Condition, and issues to Cryptographic Entropy during NTLM Authentication which cause the signal or components to be under the control of the remote unauthenticated attacker.

### 2.1.1 Technical Details

CVE-2010-0020 represents the SMB Pathname Overflow Vulnerability which produces a critical buffer overflow through inadequate path validation in specially created SMB packets (CVE-2010-0020 Detail, 2010). Attackers create malformed pathnames that exceed memory buffer allocation to trigger this vulnerability. Attackers gain full system control through arbitrary code execution because the buffer memory gets overwritten during this vulnerability. The SMB service terminates unexpectedly in unsuccessful attacks which results in denial-of-service conditions that block file-sharing service availability.

A race condition in the SMB server handling multiple Negotiate requests during CVE-2010-0021 creates the SMB Memory Corruption Vulnerability (CVE-2010-0021 Detail, 2010). The improper synchronization between processes that attempt to access shared data results in failed memory synchronization which causes corruption. Inducing these situations give attackers the opportunity to create SMB packets that initiate race condition errors. Successful exploitation of this vulnerability allows attackers to execute remote code or make the SMB service crash which disrupts both system operations and network services.

CVE-2010-0022 also known as the SMB NULL Pointer Dereference Vulnerability arises from an integer underflow that affects SMB path translation (CVE-2010-0022 Detail, 2010). An attacker who sends a malformed SMB packet forces the server to access non-existent memory

causing a system crash. The vulnerability stops the SMB service from operating correctly which results in major file-sharing functionality disruption. The disruption caused by this vulnerability affects networks that heavily depend on SMB for their operations because it creates massive productivity delays.

CVE-2010-0231 represents the SMB NTLM Authentication Weakness because inadequate entropy exists in cryptographic challenges created by NTLM authentication (CVE-2010-0231 Detail, 2010). The absence of randomness in generated authentication challenges enables attackers to run brute-force attacks to guess response information. Attackers exploit this weak cryptographic element to authenticate against network resources for unauthorized access to shared files and directory systems. Attackers exploit this security weakness to perform privilege elevation so they can gain wider access to network resources and escalate their permissions throughout the system. Table 1 presents a summary of the information about these vulnerabilities including descriptions and impacts and affected systems.

*Table 1: Summary of vulnerabilities affecting Microsoft Windows SMB Server NTLM*

| CVE ID | Vulnerability Name | Description | Impact | Affected Systems |
|---|---|---|---|---|
| CVE-2010-0020 | SMB Pathname Overflow | Buffer overflow caused by improper validation of pathnames in specially crafted SMB packets. | RCE, DoS | Windows 2000 SP4, XP SP3, Vista SP2, Server 2003 SP2, Server 2008 SP2 |
| CVE-2010-0021 | SMB Memory Corruption | Race condition when handling concurrent Negotiate requests, leading to memory corruption. | RCE, DoS | Windows XP SP3, Vista SP2, Server 2003 SP2, Server 2008 SP2 |
| CVE-2010-0022 | SMB NULL Pointer Dereference | Integer underflow leading to NULL pointer dereference during SMB path translation. | DoS | Windows XP SP3, Vista SP2, Server 2003 SP2, Server 2008 SP2 |

| | | | | |
|---|---|---|---|---|
| CVE-2010-0231 | NTLM Authentication Weakness | Weak entropy in NTLM cryptographic challenges allows brute-force attacks to bypass authentication. | Authentication Bypass, Privilege Escalation | Windows XP SP3, Server 2003 SP2, Server 2008 SP2 |

### 2.1.2 Risk Assessment Plan

A risk assessment plan is paramount in identifying and minimizing the risks related to the Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, and CVE-2010-0231). It has a CVSS score of 10.0, which are critical; these vulnerabilities affect several Windows systems, including Windows Server 2008. The vulnerabilities can lead to remote code execution (RCE), denial of service (DoS), and authentication bypass (Microsoft Security Bulletin MS10-012 - Important, 2010).

This risk assessment plan outlines a structured methodology for identifying, analysing, and evaluating these vulnerabilities. The key components of the plan include:

1. Identification of Assets
2. Threat Identification
3. Risk Analysis
4. Risk Evaluation
5. Access Control Assessment
6. Residual Risk Analysis


*Figure 3: Risk assessment plan for Microsoft Windows SMB Server NTLM Multiple Vulnerabilities*

**Justification for the Risk Assessment Plan:**

The established risk evaluation template implements an organizational structure derived from ISO 31000 (Risk management — Guidelines, 2018) together with NIST SP 800-30 (Guide for Conducting Risk Assessments, 2012) standards to examine threats through impact assessment and risk probability evaluation. The Microsoft Windows SMB Server NTLM vulnerabilities benefit from this structured approach which ensures all critical vulnerability aspects receive effective assessment and prioritization and mitigation.

The main motivation behind this selection is the asset identification and threat evaluation framework because it helps organizations understand their vulnerable assets and potential attackers. The risk matrix within the plan provides visual representations of vulnerability risk levels which helps decision-makers make efficient resource allocation decisions. The risk assessment model identifies residual threats to maintain proactive management of vulnerabilities that survive mitigation measures. The proposed method proves most effective for dealing with severe vulnerabilities such as CVE-2010-0020 and CVE-2010-0021 because system compromise risks remain substantial. The plan addresses vulnerabilities through complete measures which reduces exploitation chances without interrupting operational continuity.

#### *2.1.2.1 Identification of Assets*

A risk assessment begins with discovering assets which might be vulnerable to SMB Server NTLM weaknesses. A security breach affects any organizational asset that holds value and importance. The main assets under threat in this situation include Windows servers together with network infrastructure and user accounts and critical data.

The vulnerabilities affect Windows servers with Windows Server 2008 as a prime example of these critical assets (Microsoft Security Bulletin MS09-050 - Critical, 2023). Organizations rely on these systems to support core operational needs through their capabilities for file sharing and authentication functions and data storage capabilities. These vulnerabilities enable unauthorized access to servers which exposes both system infrastructure and the services they deliver to potential attack.

The organization's network infrastructure stands as a critical asset because it consists of routers switches and SMB servers to enable system communication. The components remain at high risk because SMB traffic uses TCP port 445 as its transmission channel. The exploitation of these flaws permits cyber criminals to perform damaging traffic interceptions and manipulations across the network infrastructure.

The exposure of confidential data presents a serious risk because it includes authentication credentials together with customer information and essential business files. Attackers who exploit these vulnerabilities could steal sensitive files while simultaneously corrupting or deleting them which would lead to major financial losses and severe damage to reputation. The security of user accounts using NTLM authentication faces critical risk because weak cryptographic challenges within NTLM enable brute-force attempts that lead to unauthorized system access. SMB-based services availability stands as a critical business continuity element. Service disruptions create operational downtime which prevents the organization from performing effectively.

#### *2.1.2.2 Threat Identification*

Microsoft Windows SMB Server NTLM vulnerabilities enable multiple security threats through different types of attackers who exploit various attack paths. External attackers who exploit unsecured SMB vulnerabilities become the main threat to systems because they can gain unauthorized access to systems through unpatched vulnerabilities (Microsoft Security Bulletin MS10-012 - Important, 2010). Through EternalBlue these attackers take advantage of SMB protocol weaknesses to execute harmful actions. Internal threats create substantial

security risks to organizations. Through their authorized system access disgruntled staff members and malicious insiders can exploit SMB vulnerabilities which results in major damage to both organizational systems and data.

Automated malware campaigns represent a major threat because they exploit vulnerable SMB services to spread across entire networks. The WannaCry ransomware variant used these vulnerabilities to lock down essential data which caused massive operational disruption across affected systems (CVE-2010-0022 Detail, 2010). Automated threats exploit unsecured systems at high speed because they target systems without proper updates. This makes them especially hazardous when organizations maintain older systems. The weak cryptographic challenges of NTLM authentication mechanisms remain a substantial threat because they are vulnerable to brute-force attacks. Through automated tools attackers exploit CVE-2010-0231 vulnerabilities to bypass authentication systems thereby gaining unauthorized access to sensitive systems (CVE-2010-0231 Detail, 2010).

These vulnerabilities create multiple attack scenarios which demonstrate their potential risks. External attackers use Remote Code Execution (RCE) techniques to exploit CVE-2010-0020 or CVE-2010-0021 through specially crafted SMB packets. Exploiters gain the ability to run arbitrary code either with or without SYSTEM privileges which results in complete system takeover (Microsoft Security Bulletin MS10-012 - Important, 2010). Attackers exploit CVE-2010-0022 by sending malicious SMB packets to terminate SMB service operations in denial of service (DoS) attacks (CVE-2010-0022 Detail, 2010). Such attacks make systems unable to function properly and cause severe operational disruptions. The critical attack scenario authentication bypass allows intruders to bypass NTLM authentication through CVE-2010-0231 (CVE-2010-0231 Detail, 2010). Weapons employed solely on weak cryptographic challenges through brute-force attacks permit unauthorized system entry that enables increased privileges while threatening essential resource systems.

Organizations need to handle these dangers in a complete manner so they can prioritize security measures while lowering their vulnerability exposure areas.

#### *2.1.2.3 Risk Analysis*

The evaluation of vulnerability exploitation potential and impact levels occurs through an extensive risk analysis process. The evaluation process allows organizations to establish their risk response sequence according to threat severity levels.

*Table 2: Risk matrix for Microsoft Windows SMB Server NTLM Multiple Vulnerabilities*

| Vulnerability | Impact | Likelihood | Risk Level | Risk Category |
|---|---|---|---|---|
| CVE-2010-0020 | Remote Code Execution | High | Critical | 9 |
| CVE-2010-0021 | Remote Code Execution, DoS | High | Critical | 9 |
| CVE-2010-0022 | Denial of Service | Medium | High | 4 |
| CVE-2010-0231 | Authentication Bypass, Privilege Escalation | High | Critical | 9 |

Remote code execution vulnerabilities CVE-2010-0020 and CVE-2010-0021 hold critical status because they enable attackers to take full control of entire systems. The CVE-2010-0231 authentication bypass vulnerability creates a critical situation because it allows attackers to rise in privileges and reach sensitive resources. The denial-of-service vulnerability CVE-2010-0022 represents high-risk because it disrupts essential services which adversely affects business continuity.

#### *2.1.2.4 Risk Evaluation*

The evaluation procedure demonstrates that CVE-2010-0020 and CVE-2010-0021 present the greatest danger because they enable remote code execution. CVE-2010-0231 represents a critical vulnerability because it allows attackers to both bypass authentication systems and gain elevated privileges. CVE-2010-0022 presents a major operational disruption risk because it leads to service denial even though it lacks code execution capabilities. The evaluation process helps organizations determine which vulnerabilities need immediate attention because they represent the highest risks to their systems.

#### *2.1.2.5 Access Control Assessment*

The evaluation of access control systems reveals multiple critical weaknesses within existing frameworks. A critical security weakness exists in the way NTLM authentication functions since it allows attackers to perform brute-force attacks. A lack of robust cryptographic challenges leads to this weakness since it allows attackers to discover NTLM protocol vulnerabilities and breach authorized access. The permission vulnerability of the SMB service stands out because attackers leverage port 445 for system interactions with external networks. Organizations that expose their SMB services face increased vulnerability which produces a

bigger attack surface that attackers can easily approach through SMB protocol abuse. The problem becomes worse due to the absence of network segmentation. Attackers can navigate between different network segments because of SMB service exposure which expands the damage potential during cyber-attacks.

The presented weaknesses require interventions to rectify them. The first essential improvement involves disabling NTLM authentication followed by the implementation of Kerberos authentication. The implementation of Kerberos authentication creates a strong encryption system which establishes mutual identity verification thus making brute-force attacks much less probable (Microsoft Security Bulletin MS10-012 - Important, 2010). Organizations should limit SMB traffic to operate only between designated IP addresses on their network. By restricting SMB traffic to trusted systems organizations achieve reduced exposure to unauthorized access and exploitation of SMB vulnerabilities. Network segmentation stands as an essential implementation requirement. Organizations can protect SMB services from attackers by creating dedicated server compartments which remain separate from the rest of their network. Segmenting the network helps organizations stop attackers from spreading between different parts of their system following successful breaches.

The access control assessment demonstrates why organizations must address existing weaknesses before they can reduce exposure to Microsoft Windows SMB Server NTLM Multiple Vulnerabilities. Organizations which deploy these improvements minimize their attack exposure and increase security effectiveness for protecting their critical assets from potential attacks.

#### *2.1.2.6 Residual Risk*

Although organizations follow recommended security measures and apply required patches multiple residual security threats persist because of different contributing factors. Legacy systems act as the primary source that generates residual risk. Organizations maintain operational dependence on outdated Windows Server 2008 systems that do not receive modern security protocol upgrades or updates. Old systems that organizations continue to use heighten the risk that security weaknesses will remain active throughout the infrastructure despite all preventive measures. The continued use of essential legacy systems presents a major challenge to organizations that want to eliminate all risks from their operations.

The most important threat to SMEs comes from insider breaches as employees together with contractors use their organizational access to find and use internal system weaknesses. The

exploitation of SMB protocol weaknesses by legitimate organizational system users remains a significant security challenge because they typically bypass security measures or access vulnerabilities through existing privileges. Organizations face major challenges in managing insider threats because these threats exploit internal trust relationships while circumventing outside security measures to create sustained challenges that are hard to detect.

Zero-day exploits continue as an unsettled security threat. Attackers exploit unknown vulnerabilities to target systems because vendors remain unaware of these threats when the vulnerabilities are discovered. Due to its broad implementation and intricate protocol structure the SMB protocol attracts malicious actors who look for unknown vulnerabilities to exploit. Despite robust patch management and monitoring systems organizations face continuous challenges from unpredictable zero-day exploit risks.

The implementation of mitigation measures helps lower attack probabilities and decrease damage effects yet leaves behind unavoidable remaining security risks. The protection of critical systems depends on continuous monitoring together with regular security audits and immediate software security updates. Organizations achieve enhanced security resilience through their dedication to understanding and preparing for residual risk factors which protects them from evolving threats.

### 2.1.3 Policy for Preventing and Mitigating the Vulnerability

This policy establishes a detailed strategy to handle CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 and CVE-2010-0231 Microsoft Windows SMB Server NTLM Multiple Vulnerabilities. The exploitation of these vulnerabilities produces dangerous results including RCE attacks alongside DoS attacks and authentication bypass through weak NTLM authentication mechanisms. The policy has been designed to safeguard essential organizational assets including physical infrastructure and sensitive information and network facilities because of their critical importance. This policy prioritizes two main goals: stopping SMB Server NTLM vulnerability exploits while managing unpatched SMB service and NTLM authentication risks to allow prompt incident response and uninterrupted business operations through vital service and data protection.

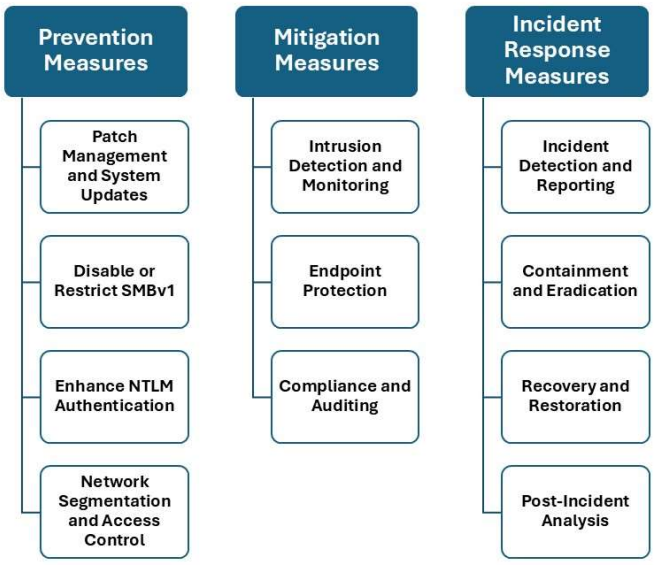


*Figure 4: Overview of policy for preventing and mitigating Microsoft Windows SMB Server NTLM Multiple Vulnerabilities*

### *2.1.3.1 Prevention Measures*

The process to reduce these vulnerabilities starts with proactive prevention initiatives. Security updates represent an essential part that needs immediate execution. The mitigation of known vulnerabilities requires consistent patch management especially for vulnerabilities included in Microsoft Security Bulletin MS10-012 (Microsoft Security Bulletin MS10-012 - Important, 2010). Organizations must create an official patch management policy which requires immediate system updates for all devices. The deployment of multiple system patches becomes easier with Windows Server Update Services (WSUS) which reduces the chance of exploitation. Organizations must use OpenVAS or Nessus tools to perform regular vulnerability scans which help both identify unknown vulnerabilities and verify security policy compliance. Organizations need to actively manage risks that emerge from their outdated system infrastructure. Organizations need to replace outdated operating systems like Windows Server 2008 and Windows XP with newer updated ones because these versions no longer obtain security updates thus creating unnecessary security risks (Microsoft Lifecycle Policy, n.d.).

To prevent security risks organizations must disable the SMBv1 protocol. The outdated SMBv1 protocol remains insecure by design which attackers use to launch high-profile ransomware attacks including WannaCry and NotPetya (CIS Releases 2017 Year in Review, 2017).

Organizations that disable the SMBv1 protocol across their entire system infrastructure protect themselves from attackers who would exploit this protocol to spread malware and execute commands. Security administrators can achieve this goal through PowerShell commands which include "Set-SmbServerConfiguration -EnableSMB1Protocol $false" and "Get-SmbServerConfiguration" for status verification. Organizations that adopt the secure protocols SMBv2 and SMBv3 will drastically decrease their exposure to cyber-attacks.

The prevention of exploitation relies heavily on NTLM authentication enhancement. When possible, organizations need to swap NTLM for Kerberos authentication because Kerberos provides superior encryption and mutual authentication features (Pamnani, Network security: LAN Manager authentication level, 2017). Policies restricting NTLM usage can be enforced through group policy settings, such as Network Security: Restrict NTLM. The security posture benefits from multi-factor authentication (MFA) because it adds multiple verification steps to access critical systems which makes exploitation of authentication weaknesses increasingly difficult for attackers (Grassi, Garcia, & Fenton, 2017).

A comprehensive enforcement of network access controls guarantees authorized system devices the sole ability for SMB communication. Firewall administration tools should manage SMB connections between specific established network addresses while shutting out external systems from using TCP port 445. Network segmentation functions as a security measure to protect critical systems by separating them from other network areas thus minimizing attacker lateral movement possibilities. The availability of SMB services for remote access should be limited to VPN connections which protect business-critical systems securely.

#### *2.1.3.2 Mitigation Measures*

The reduction of potential exploitation damage requires both preventive measures and mitigation strategies. Environmental protection against SMB attacks requires using IDS solutions such as Snort and Suricata to track worrisome network activity for exploitative behaviour detection (Documents, n.d.). Organizations must implement superior system analysis and logging techniques to track both SMB authentication events while identifying authentication failures and out-of-the-ordinary SMB network patterns. Such security tools as Splunk and IBM QRadar function as Security Information and Event Management (SIEM) systems to generate one centralized threat detection and response platform from network-wide security log consolidation.

Among essential security controls endpoint protection functions as a central requirement. A network defence includes implementing trustworthy antivirus and anti-malware applications which offer defence against malicious software such as Microsoft Defender along with Symantec Endpoint Protection. The security tool known as Windows AppLocker functions as a whitelist application to stop unauthorized programs from launching thereby minimizing malware distribution between computers.

#### *2.1.3.3 Incident Response Measures*

A built-in incident response plan stands as an essential requirement for organizations to eliminate damage while recovering operations following exploitation attempts or attacks. The initial sequence of incident management begins with detection followed by reporting incidents. Organizations need to examine network traffic for indicators of compromise (IoCs) which include port 445 anomalies and unexpected process execution. The IT Security Team depends on staff training regarding incident reporting with specific use of JIRA or ServiceNow tools to enhance incident response efficiency.

Once incident response reaches the containment stage it becomes essential to its progress. Systems under attack should receive immediate network disconnection to block malware spread and devastating lateral expansion. Entry points through Firewall rules must be modified by implementing blocks that isolate IP addresses that correspond with attack actors so communication chains can be disrupted. The next phase of response work requires vulnerability elimination and system restoration after containment measures. The recovery process requires administrators to deploy updates then validate complete system upgrades while using protected backups to restore compromised systems (Bartock, et al., 2016). Security tests need to run after restoration to confirm there is no malicious code on the systems thus ensuring safe restored environments.

Every organization needs to perform a post-incident analysis to discover the original attack source and strengthen their security operations. Through root cause analysis organizations discover the incident's origin while receiving practical recommendations to enhance their policy framework and procedural framework. The organization must organize training exercises to build employee understanding of SMB weaknesses and educate staff members about appropriate protective behaviours.

The Microsoft Windows SMB Server NTLM Multiple Vulnerabilities prevention policy combines technical solutions with procedural security management strategies. Regular updates

combined with outdated protocol disabling and enhanced authentication and network control enforcement help organizations stop exploitation. In addition to preventing attacks end-point protection and intrusion detection serve as preventive measures against successful cyberattacks. An incident response structure enables immediate control and removal operations to reduce operational disruption following a crisis. Organizations achieve superior security resilience through the adoption of this policy allowing them to preserve a robust security posture despite SMB vulnerabilities.

## 2.2 Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability

According to OpenVAS scan report the Microsoft Windows SMBv2 Negotiation Protocol Remote Code Execution (RCE) is a critical vulnerability found in many Windows operating systems like Windows 7, Windows Vista and Windows Server 2008. The SMB protocol mishandles specially formatted SMBv2 packets to create this vulnerability, which maintains a CVSS score of 10.0. System hacking becomes possible through this vulnerability because an attacker could run any administrative command on the machine as if they were a genuine system administrator. When an attack fails to execute, it can result in a denial-of-service (DoS) situation.

This vulnerability was first reported in Microsoft Security Bulletin MS09-050, which provides important details about the danger and available fixes (Microsoft Security Bulletin MS09-050 - Critical, 2023). Microsoft released security updates to fix the problem, and for organisations like ShopEase Indonesia, it is really important to install these patches to prevent potential attacks.

### 2.2.1 Technical Details

The Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability is a collection of problems with how SMBv2 protocol packets are handled. These problems can let attackers take remote control, cause DoS or disrupt normal operation. Identified under different CVEs, these vulnerabilities affect different parts of SMBv2 packet handling:

- SMBv2 Infinite Loop Vulnerability (CVE-2009-2526)
- SMBv2 Command Value Vulnerability (CVE-2009-2532)
- SMBv2 Negotiation Vulnerability (CVE-2009-3103)

These issues bring unique technical challenges and different ways to attack, which together probably pose a very big risk to systems. The next subsections further describe these vulnerabilities and their contribution to the total threat.

#### *2.2.1.1 SMBv2 Infinite Loop Vulnerability (CVE-2009-2526)*

The SMBV2 Infinite Loop Vulnerability (CVE-2009-2526) is a critical denial of service (DoS) bug in the SMBv2 protocol running in Microsoft's service which affects Windows Vista and Server 2008. The vulnerability triggers an infinite loop through specially crafted SMBv2 packets which forces users to manually restart their systems. Attackers who exploit this vulnerability does not require authentication to disrupt SMB-dependent services including file sharing and network browsing. Downtime can occur for an extended period while business operations stop completely and shared resource access becomes blocked, especially for domain controllers and file servers. The vulnerability leads to severe system availability and reliability problems even though attackers are not able to execute code or gain administrative privileges (Microsoft Security Bulletin MS09-050 - Critical, 2023).

#### *2.2.1.2 SMBv2 Command Value Vulnerability (CVE-2009-2532)*

The SMBv2 Command Value Vulnerability (CVE-2009-2532) is a critical RCE flaw in Microsoft's SMBv2 protocol that affects Windows Vista, Server 2008, and Windows 7 Release Candidate. This happens because SMB implementation fails to properly check incoming command values in specially crafted SMB packets, allowing unauthorised attackers to send malicious packets in order to gain system control. Attackers who successfully exploit this vulnerability gain access to install programmes, modify or delete data, and create new accounts with all system privileges. Domain controllers and other systems with SMB Server service exposure face the highest vulnerability risks because their network shares remain accessible. Microsoft implemented a change in how SMB handled command values in packets to resolve the vulnerability (Microsoft Security Bulletin MS09-050 - Critical, 2023).

#### *2.2.1.3 SMBv2 Negotiation Vulnerability (CVE-2009-3103)*

The SMBv2 Negotiation Vulnerability (CVE-2009-3103) is a critical RCE flaw in Microsoft's SMBv2 protocol that affects Windows Vista, Server 2008, and Windows 7 Release Candidate. The problem is because SMB packets are not parsed properly, which allows any attacker that is unauthenticated to send malicious packets and gain full system control. Attackers who successfully exploit this vulnerability gain access to install programs and modify or delete data while also creating new administrator accounts. Domain controllers and other systems with the

SMB Server service running face the highest exposure risk because they have open network shares. Microsoft fixed the issue by modifying the SMB packet parsing but the vulnerability was already public before Microsoft released the fixes (Microsoft Security Bulletin MS09-050 - Critical, 2023).

Table 3 below is a summary of the vulnerabilities.

*Table 3: Summary of vulnerabilities affecting Microsoft Windows SMBv2 Negotiation Protocol*

| **CVE ID** | **Vulnerability Name** | **CVSS Score and Severity** | **Description** | **Impact** | **Affected Systems** |
|---|---|---|---|---|---|
| CVE-2009-2526 | SMBv2 Infinite Loop Vulnerability | 7.8 High | A flaw in Microsoft's SMBv2 protocol where specially crafted packets cause an infinite loop due to improper validation. | Leads to denial-of-service, causing the affected system to become completely unresponsive until manually restarted. | Windows Vista<br><br>Windows Server 2008 |
| CVE-2009-2532 | SMBv2 Command Value Vulnerability | 10.0 High | A RCE vulnerability in Microsoft's SMBv2 protocol caused by improper handling of command values in specially crafted SMB packets. | Unauthenticated attackers gain full control of systems through this vulnerability which lets them install programs, modify data and create new administrator accounts. | Windows Vista<br><br>Windows Server 2008<br><br>Windows 7 Release Candidate |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2009-3103 | SMBv2 Negotiation Vulnerability | 10.0 High | A RCE vulnerability in Microsoft's SMBv2 protocol caused by improper parsing of specially crafted SMB packets. | Unauthenticated attackers gain full control of systems through this vulnerability which lets them install programs, modify data and create new administrator accounts. | Windows Vista<br><br>Windows Server 2008<br><br>Windows 7 Release Candidate |

### 2.2.2 Risk Assessment Plan

This plan addresses the risks associated with Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability. Through a systematic methodology, the risk assessment process will identify vulnerabilities while conducting analysis and evaluation before implementing mitigation measures. The key components of the plan will consist of eight sequential steps, as illustrated in Figure 5:

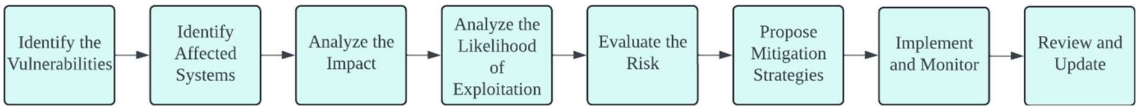


*Figure 5: Risk assessment methodology for Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability*

**Justification for this methodology:**

This risk assessment follows industry criteria based on NIST SP 800-30 that uses a standardized procedure to discover vulnerabilities and analyze potential impacts for risk reduction (Blank & Gallagher, 2012). The plan targets the SMBv2 vulnerabilities (CVE-2009-2526, CVE-2009-2532, and CVE-2009-3103) that exist within ShopEase Indonesia's Windows Server 2008 environment. This methodology delivers a complete assessment of vulnerabilities together with their potential impacts and specific measures to improve the company's cybersecurity defences. The established methodology enables ShopEase Indonesia to identify and minimise potential risks while stopping future security breaches.

#### *2.2.2.1 Step 1: Identify the Vulnerabilities*

The first vital step focuses on identifying all existing system vulnerabilities which affect ShopEase Indonesia's information technology infrastructure.

The SMBv2 Infinite Loop Vulnerability (CVE-2009-2526) causes systems to enter endless loops through specially crafted SMBv2 packets which make the system unresponsive until manual restarts (Microsoft Security Bulletin MS09-050 - Critical, 2023).

The SMBv2 Command Value Vulnerability (CVE-2009-2532) and SMBv2 Negotiation Vulnerability (CVE-2009-3103) function as RCE vulnerabilities. The SMBv2 Command Value Vulnerability occurs due to invalid command value validation in SMB packets but the SMBv2 Negotiation Vulnerability emerges from incorrect SMB packet analysis during negotiation phase. Attackers can gain full control of the affected system through these RCE vulnerabilities because they enable unauthorised access to install programs while permitting data modification and account creation with complete administrative privileges (Microsoft Security Bulletin MS09-050 - Critical, 2023).

#### *2.2.2.2 Step 2: Identify Affected Systems*

All instances of ShopEase's Windows Server 2008 systems operating with the SMBv2 protocol remain vulnerable. The SMBv2 protocol functions as a fundamental network infrastructure component for file and printer sharing operations. The vulnerability scan revealed that the Windows Server 2008.vm operates with an outdated unpatched SMBv2 version which creates an exposure to attacks. Any systems which communicate with this server through SMBv2 including domain controllers and file-sharing clients will face indirect security risks. Understanding and identifying every vulnerable system plays an essential role because it enables a clear determination of how big the exposure area is and how complete the protective measures must be.

#### *2.2.2.3 Step 3: Analyse the Impact*

These vulnerabilities produce serious consequences. Malicious exploitation of CVE-2009-2526 produces a DoS condition which makes essential services unresponsive and interrupts e-commerce processes. The vulnerabilities CVE-2009-2532 and CVE-2009-3103 enable attackers to run arbitrary code which results in unauthorised access to sensitive customer information such as usernames and encrypted passwords and transaction histories (Microsoft Security Bulletin MS09-050 - Critical, 2023).

The successful exploitation of these vulnerabilities would cause reputational damage which would diminish customer trust because ShopEase Indonesia has previously experienced data breaches. Several financial challenges await ShopEase Indonesia from regulatory fines and legal obligations together with reduced revenue and diminished customer retention because of operational disruptions. To effectively prioritise risk reduction strategies and resource distribution, it is vital to understand all potential consequences.

#### *2.2.2.4 Step 4: Analyse the Likelihood of Exploitation*

Multiple elements create a high risk for exploitation. Attackers can initiate attacks more easily because of publicly available exploit tools including Metasploit. The server operates Windows Server 2008 which Microsoft no longer provides support for, thus increasing its exposure to exploitation. The exposure of SMB ports TCP 139 and 445 to the internet creates a substantial risk of exploitation. The vulnerabilities remain exposed to attack because multiple conditions create a high probability that attackers will succeed in exploiting them unless the issues get resolved immediately (Microsoft Security Bulletin MS09-050 - Critical, 2023).

#### *2.2.2.5 Step 5: Evaluate the Risk*

The risk evaluation focuses on the potential consequences of the identified SMBv2 vulnerabilities for ShopEase Indonesia. The risk matrix under Table 4 provides a detailed breakdown of the likelihood, impact, and risk level for each vulnerability discovered.

*Table 4: Risk matrix for Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability*

| **Vulnerability** | **Likelihood** | **Impact** | **Risk Level** |
|---|---|---|---|
| CVE-2009-2526 | Moderate to high | Moderate to High (DoS) | High |
| CVE-2009-2532 | High | Critical (RCE, Data Breach) | Critical |
| CVE-2009-3103 | High | Critical (RCE, System Compromise) | Critical |

The risk matrix establishes a method to assess identified SMBv2 vulnerabilities through their exploitation potential and their corresponding impact levels. The risk levels for vulnerabilities are defined as Low, Moderate, High and Critical to establish proper mitigation priorities.

CVE-2009-2526 (SMBv2 Infinite Loop) represents a High risk rating because it shows both moderate to high exploitation potential and the ability to create operational disruptions through denial-of-service. The vulnerability poses a major issue for business continuity even though it does not enable data theft or system control.

In addition, CVE-2009-2532 (SMBv2 Command Value) alongside CVE-2009-3103 (SMBv2 Negotiation) have received Critical ratings because they present both high risk of exploitation and severe consequences. RCE vulnerabilities through these weaknesses enable attackers to breach data, compromise systems and inflict severe financial losses and reputation damage. The matrix shows that ShopEase Indonesia must prioritise fixing these vulnerabilities first because they represent the most significant cybersecurity and business operation threats.

Through this matrix the company can deploy resources strategically and design specific risk reduction strategies to minimise vulnerabilities.

#### *2.2.2.6 Step 6: Propose Mitigation Strategies*

Multiple mitigation strategies exist to address these security risks. First, security patches should be implemented since Microsoft delivered them through MS09-050 despite Windows Server 2008 is no longer supported. Securing the system by applying patches should be prioritized whenever possible. Second, the use of SMBv2 should be disabled unless necessary because SMBv1 provides better protection against these particular vulnerabilities. The registry contains a setting to enable this modification (Microsoft Security Bulletin MS09-050 - Critical, 2023).

Third, network segmentation should be used as a preventive measure because it separates compromised servers so they remain outside internet connectivity and critical system reach. Fourth, to stop external access to the SMB service, organizations must install firewall rules which block both TCP ports 139 and 445. Finally, upgrading to Windows Server 2019 or 2022 functions as the last protective measure because it provides continuous access to security updates (Microsoft Security Bulletin MS09-050 - Critical, 2023).

The combined implementation of these security strategies minimizes exposure to exploitation risks and creates an improved framework for system defense.

#### *2.2.2.7 Step 7: Implement and Monitor*

Implementation involves applying patches and disabling SMBv2 on the affected server, configuring firewall rules and network segmentation, deploying intrusion detection systems

(IDS) to monitor for suspicious SMB traffic, and conducting regular vulnerability scans to ensure no new vulnerabilities are introduced.

A comprehensive monitoring process includes tracking SMB traffic through logs and analysis for evidence of attack attempts while reviewing firewall and IDS events for unusual behavior and conducting periodic penetration tests to assess vulnerability mitigation effectiveness. A system of continuous monitoring helps identify potential exploitation efforts which can be quickly corrected.

#### *2.2.2.8 Step 8: Review and Update*

A continuous review process serves as the last step in the risk assessment. ShopEase Indonesia needs to revise its cybersecurity policies after learning from this incident. Organisational staff members need training to detect and respond to threats through the SMB protocol. The company needs to create and validate incident response protocols for SMB vulnerabilities. Security audits should be performed yearly to verify that the organisation follows industry standards like PCI DSS and ISO 27001.

By following this risk assessment plan, ShopEase Indonesia can effectively mitigate the SMBv2 vulnerabilities and strengthen its overall cybersecurity posture. Scheduled system reviews with updates help the organization defend itself safely against developing cyber threats.

### 2.2.3 Policy for Preventing and Mitigating the Vulnerability

To address the identified SMBv2 vulnerabilities and strengthen ShopEase Indonesia's cybersecurity posture, formulating a policy is necessary. This policy is divided into three key sections - Prevention, Mitigation, and Incident Response. It includes detailed steps to prevent exploitation alongside strategies for minimising incident impact and rapid response protocols. An overview of the policy is illustrated in Figure 6.

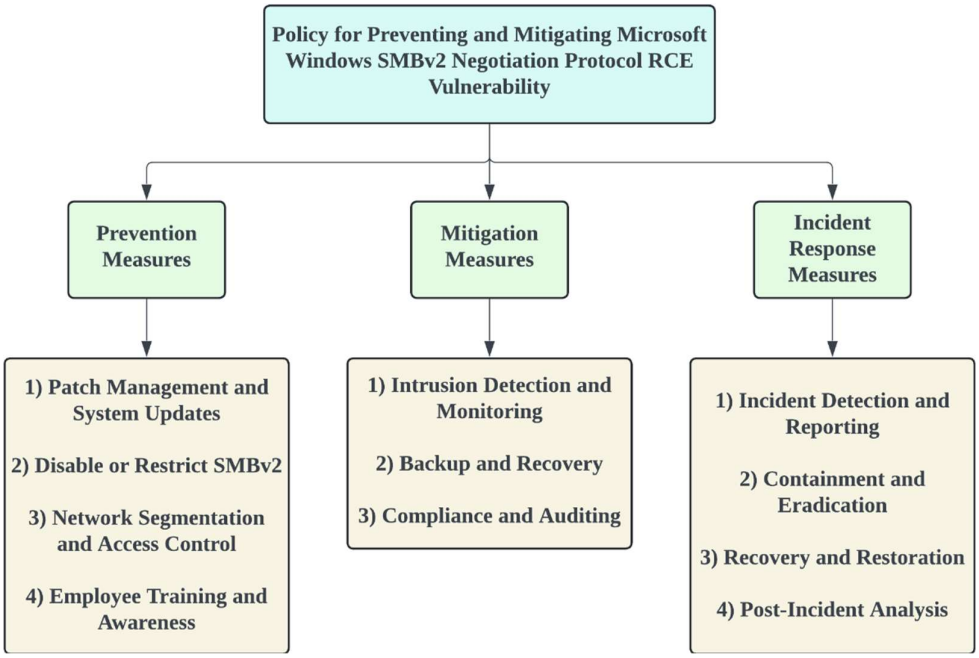


*Figure 6: Overview of the policy for preventing and mitigating Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability*

### *2.2.3.1 Prevention Measures*

Security controls together with best practices serve to minimize SMBv2 vulnerability exploitation chances when organizations apply them for proactive prevention measures.

**a) Patch management and system updates:**

ShopEase Indonesia must urgently deploy all available security patches for the SMBv2 protocol including the Microsoft Security Bulletin MS09-050. Any remaining support for Windows Server 2008 has ended but installing available security patches will help address known vulnerabilities. The organisation needs to move away from outdated systems Windows Server 2008 by adopting Windows Server 2019 or 2022 to gain access to ongoing security updates. In addition, the organisation needs to deploy automated systems for patch management to deliver timely updates for every software and system throughout its network (Microsoft Security Bulletin MS09-050 - Critical, 2023).

**b) Disable or restrict SMBv2:**

Business operations that do not require SMBv2 should disable it and use SMBv1 as the fallback option because SMBv1 remains less prone to these specific exploits. System administrators can implement this change using registry modifications or Group Policy settings. SMBv2 usage

should stay enabled only within secure internal networks while remaining inaccessible from internet connections (Microsoft Security Bulletin MS09-050 - Critical, 2023).

**c) Network segmentation and access control:**

Network segmentation stands as a fundamental preventive strategy. ShopEase Indonesia should separate SMBv2 systems from important infrastructure including payment gateways and customer databases because this segmentation minimises potential attack areas while stopping attackers from moving between systems. Firewall administrators should disable access to ports 139 and 445 because these ports enable SMB protocol operations. Only approved users and systems should access SMB shares while strict least privilege system remain in effect (Microsoft Security Bulletin MS09-050 - Critical, 2023).

**d) Employee training and awareness:**

The prevention of security incidents needs both trained employees and awareness programmes. The company must offer ongoing cybersecurity training to employees so they learn to identify and handle threats such as phishing attacks attacking compromised account credentials during a breach incident. Moreover, the employees need to participate in simulated security incidents to demonstrate their ability to manage breaches that target SMB vulnerabilities.

#### *2.2.3.2 Mitigation Measures*

The mitigation measures aim to reduce potential SMBv2 vulnerability impacts when they are exploited while protecting operational processes and data integrity.

**a) Intrusion detection and monitoring:**

Intrusion detection system (IDS) must monitor SMB traffic to detect both exploitation attempts and unusual behavioural patterns. Alert systems must activate when attackers try to exploit recognised SMB vulnerabilities. The implementation of real-time threat detection requires continuous monitoring of system logs together with network traffic analysis. In addition, network vulnerability scans should run routinely in order to detect and resolve newly discovered network vulnerabilities or misconfigurations.

**b) Backup and recovery:**

A successful attack can be mitigated through the implementation of backup and recovery procedures. The maintenance of regular backups along with secure storage and tested reliability

of critical systems and data remains essential for protection. Moreover, a disaster recovery plan must exist to maintain business operations after a successful attack occurs.

**c) Compliance and auditing:**

ShopEase Indonesia need to adhere to industry standards including PCI DSS, ISO 27001 and NIST guidelines to develop a strong security framework that remains robust. Security audits should be conducted yearly to evaluate protection measures and pinpoint areas that need enhancement. Additionally, the company should collaborate with independent cybersecurity firms for penetration testing and vulnerability assessments to gain outsider perspective about their security needs.

#### *2.2.3.3 Incident Response Measures*

The incident response measures establish systematic steps to support security incident management recovery following attacks targeting SMBv2 vulnerabilities.

**a) Incident detection and reporting:**

To respond to security events, ShopEase Indonesia should create clear processes that identify potential threats, which include detecting unusual SMB network activities or system conduct. Employees need to understand reporting processes so they can quickly refer incidents to the cybersecurity workforce.

**b) Containment and eradication:**

When incidents occur, ShopEase Indonesia should separate compromised systems to stop attack propagation while minimising harm to their network. The security team must identify and eliminate the root cause that includes vulnerabilities or malicious software.

**c) Recovery and restoration:**

Secure backups must be used for system restoration through recovery and restoration procedures. Any system restoration process requires verification of system integrity as a precondition for activating post-restoration connectivity. The correct operation and secure functioning of restored systems must be tested after recovery has occurred.

**d) Post-incident analysis:**

Each security incident requires a complete analysis to determine exactly what caused the incident then assess how the response functioned. ShopEase Indonesia should revise their

security controls through policy and procedural updates after conducting analysis of incident-related lessons. The team must share findings and improvements with stakeholders who include both management and employees.

## 2.3 Microsoft Windows SMBv1 Vulnerability (CVE-2017-0144)

### 2.3.1 Technical Details

Server Message Block Version 1 (SMBv1) is a crucial vulnerability, in which one can communicate over a networked device with one another with the exposure of Microsoft Windows SMBv1 vulnerability (or EternalBlue − CVE-2017-0144) (Gupta, 2023). WannaCry, NotPetya was used to spread a huge systemic penetration and financial damage and to leak data, but this vulnerability was used in the global ransomware attack. EternalBlue is at its simplest, an exploit that will allow an attacker to run code on the victim server, when packets specifically crafted to it are sent (Cloudflare Inc., n.d.). It is an actual threat of to the systems of Techforte Incorporation in the cases of remote code execution, malware distribution, etc.

Below are the steps of Risk Assessment Process that can be done to solve and eradicate the SMBv1 vulnerability.

### 2.3.2 Risk Assessment Plan

#### *2.3.2.1 Step 1: Identify*

Risk assessment begins with identification of the vulnerability, describing its characteristics and identifying potential systems the vulnerability affects to determine the cost associated with the vulnerability.

Also, all windows operating systems including Microsoft Windows 2008 (Microsoft Inc., 2017) have SMBv1 vulnerability (CVE-2017-0144). This vulnerability gives the attackers the complete control over the server as they can run the server's entire system. It is a vulnerability due to not validating SMBv1 requests on the network and when these packets are crafted specially.

Systems of Affected Systems: Such systems on which SMBv1 was used for file sharing and networking before include Windows Server 2008 (Microsoft Inc., 2017).

**Potential Attack Scenarios:**

a) **Server Compromise**, unauthorised access and data theft is possible since as an attacker you can run evil code on the server.
b) **SMBv1 vulnerability** – Malware such as ransomware is propagated across the network.
c) Once the hacker gets into one machine, lateral movement is used - to move from a machine to the other machines in the network.
d) **Cybercriminals** or state attackers, or any other uneighty parties that can achieve remote control of compromised systems by means of SMBv1. (Sentinel One, 2019).

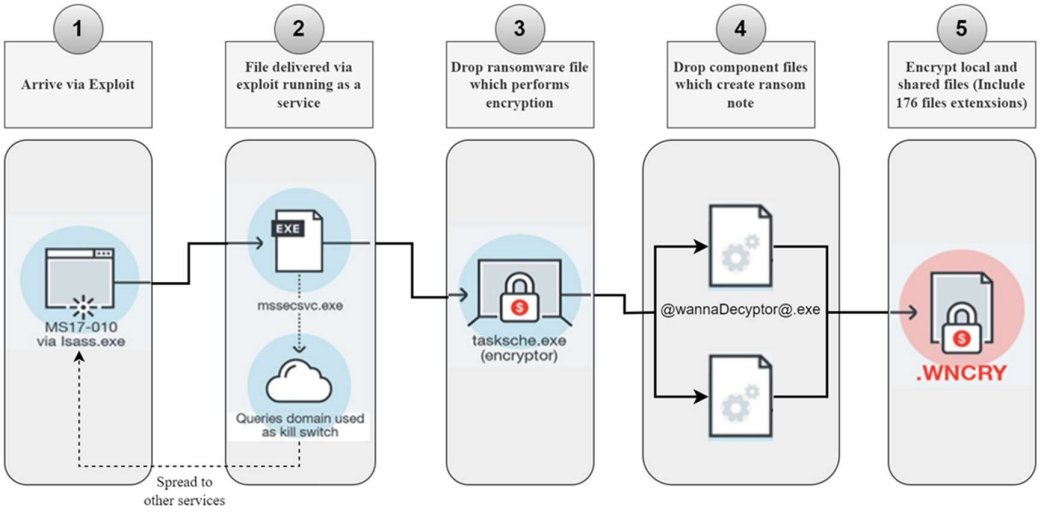


*Figure 7: Attack flow for WannaCry Ransomware that exploits SMBv1*

*Table 5: Risk matrix for Microsoft Windows SMBv1 Vulnerability (CVE-2017-0144)*

| Risk Factor | Description | Likelihood | Impact | Risk Level | Mitigation Measures |
|---|---|---|---|---|---|
| Vulnerability | Windows Server 2008 and other systems that have SMBv1 installed are vulnerable to SMBv1 | High | High | Critical | SMBv1 should be disabled, security patches should be applied, and operating systems should |

| | | | | | |
|---|---|---|---|---|---|
| | vulnerability (CVE-2017-0144). | | | | be updated to newer versions. |
| Remote Code Execution (RCE) | The code can be executed remotely, which gives the attackers the ability to compromise the system's sensitive data and take control. | High | High | Critical | Use available patches, watch the network traffic and only grant access to systems known to be patched. |
| Ransomware Transmission | Ransomware can be spread across the network and encrypts data, and it may be possible to exploit vulnerability to do both. | Medium to High | Very High | High | Install anti virus, data should be regularly backed up and the network should be divided so that the ransomware does not spread. |
| Lateral Movement | Should attackers compromise one machine, they eventually have the ability to move laterally into other machines | High | High | Critical | Network segmentation, disabling SMBv1, and detecting lateral movement across systems should be used. |

| | | | | | |
|---|---|---|---|---|---|
| | on the network, which technically allows the whole system to be compromised. | | | | |
| Data Theft | Sensitive data can be stolen from compromised systems that result in loss of personal, financial or confidential information. | High | High | Critical | Encrypt, set up data access controls and monitor unusual data transfer activities. |
| Service Disruption | SMBv1 exploitation can disrupt the key business services resulting in downtime and loss of business operations. | Medium | High | High | The redundancy and backups should ensure that it runs always, patching to not be disrupted for service. |
| Threat Actors (Cybercriminals) | It is vulnerable to cybercriminals, state sponsored attackers and | High | Very High | Critical | While it will enhance security monitoring, requesting |

| | | | | | |
|---|---|---|---|---|---|
| | other malicious actors, who can target the organization using it. | | | | application of threat intelligence, as well as additional robust incident response procedures. |
| Compliance Risk | Failure to resolve the SMBv1 vulnerability can earn an organization a noncompliance with the industry regulations and standards, thereby bringing the organization legal or financial penalties. | Medium | High | High | Keep systems up to date and patched, maintain audit trails, and have normal compliance with security standards (such as ISO 27001). |

**Impact on Organization:**

If they were in the organization such as Techforte, this weakness would cause disaster. The attackers can also control the targets, steal or modify information, spread viruses or ransomware, including in case of exploitation. This would not be smooth on operations, it will cost the company almost lots of loses and damage the company's reputation.

The foundation of this story would be set by clearly identifying the vulnerability, the potential impact and the systems which they could affect.

#### *2.3.2.2 Step 2: Assess*

In this, we will evaluate the risk of the identified vulnerability being exploited, if the vulnerability is exploited and the risk implication thus. It is useful to prioritize the vulnerability in light of risk in this step.

**This vulnerability has a high risk implication.**

Previous EternalBlue exploit has been reported and a lot of tools are using this exploit.The system is vulnerable to this and some of the most damaging ransomware attacks of the past year used this vulnerability, including WannaCry. However, so long as the system isn't patched and SMBv1 is enabled, there's a good chance it will be. Attacks are carried out in how these attackers are scanning the entire Internet to find systems using SMBv1 and attempt to exploit this vulnerability.

**Impact:**

- Critical: The SMBv1 can also be exploited even over total compromise of target system, such as machine can be infected with ransomware or other malwares and extract data from it or completely disable services that are rendered by the system. Nevertheless, business can be irreparable, with overwhelming operational shut down, financial costs, brand image and even through the legal cost via hacking events.

**Asset Value:**

- High: The customer data, and the organization data, and many other important data are stored in windows server 2008 systems. Potential sources of breach include these systems, which may allow very severe business disruption, loss of important information.

**Risk Rating:**

- **Overall Risk: High.**

As this is a simple vulnerability to exploit, a tool exists to exploit this, and the consequences on the business are so serious that this is treated as a high risk issue which should be addressed without delay.

By ranking this vulnerability according to likelihood of attack and its impact, we can focus on remediation on this vulnerability immediately.

### *2.3.2.3 Step 3: Control*

The approach of the control step is to detect and implement measures to reduce or eliminate the presence of vulnerability. The intent is to lower this risk and improve the probability that the intrusion has been thwarted if it has occurred.

**Mitigation Measures:**

1. Disable SMBv1:

- **Action**: The risk here can be best counter to this risk by turning off the SMBv1 protocol on all the relevant systems. It can be done either in windows settings or via group policies in a network of multiple machines.
- **Rationale**: This is an outdated protocol and the only proper way to prevent attacks using it, is to disable SMBv1. As better security features, SMBv2 and SMBv3 should be preferably used.

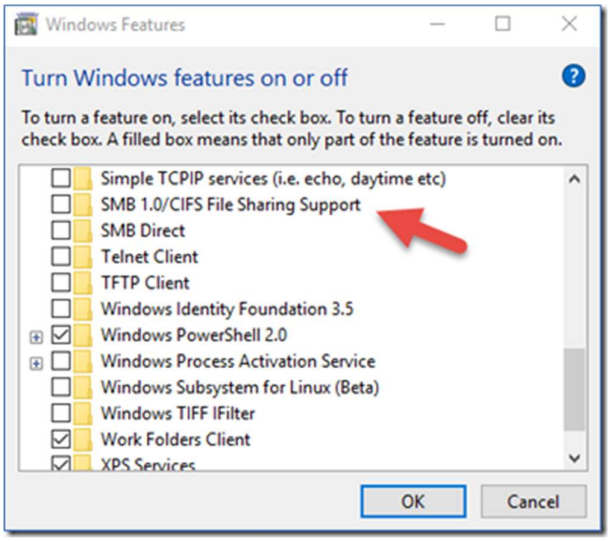


*Figure 8: Disabling SMBv1 on Windows*

2. Apply Security Patches:

- **Action**: So in all cases for Windows Server 2008, it is advised updating all the systems involved with the latest windows patches as well as those involved. In particular, it applies the update specified in the MS17-010 security bulleting that eliminates the EternalBlue exploit.

- **Rationale**: This SMBv1 patch addresses the remote code execution weakness and makes it so that outside code cannot execute on the server using this weakness.

3. Network Segmentation:

- **Action**: The organization segments the network in order to isolate the critical systems from the rest of the network that depends on SMB services to communicate. Traffic on SMB should be limited to just internal, and trusted network only.
- **Rationale**: However, if the attacker can't reach the system that is vulnerable on the network, the likelihood of that attack is basically cancelled out. Also, it can not be shifted from one part of the network to another part of the network..

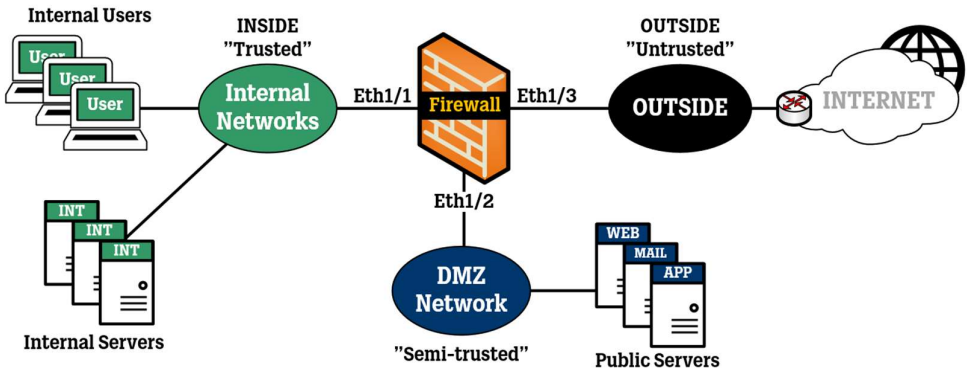


*Figure 9: Network Segmentation*

4. Intrusion Detection and Monitoring:

- **Action**: Therefore, we can use network Intrusion Detection Systems (IDS) to watch for any suspicious SMB traffic. Configuration for the alerts for ALL the suspicious, potentially exploitable, usage of SMBv1 traffic should also be alarmed unauthorised usage of SMBv1.
- **Rationale**: If suspicious activities are alerted in time, the damage can be avoided by quick response and such threats are really reduced.

5. Regular Backups:

- **Action**: Then you need first to backup all important data and constantly do that and those must be in different locations from that main network in case that main network was in destroyed/disabled.

- **Rationale**: Ransomware will represent an organization; thus, an organization can recover information without paying ransom or long outages owing to offsite backups.

6. User Access Controls:

- **Action**: All systems running or using SMB should have strict access control policies implemented so only users authorized to do administrative tasks on those systems will actually be allowed to. So ensure always that you always check on users and User Privilege Levels to be sure that there are no unauthorized users.
- **Rationale**: When the attacker gets into the system, limiting the number of administrative rights will reduce the chances the system is exploited.

#### *2.3.2.4 Step 4: Review Control*

This step helps to prevent a functionality of the control that has been implemented from becoming dysfunctioned over progress of time. To that effect, assessment of the counter measures should constantly be done to check whether they provide adequate protection to deal with the identified weakness.

1. Regular Audits:

- **Action**: Periodically review systems to ensure that SMBv1 has been disabled on all the systems. All the security patches mentioned in the MS17-010 bulletin should be installed and applied.
- **Rationale**: If the configuration of systems is not configured properly, some of these weaknesses may resurface. Also, in case patch management is not stable. Regular audits will give us a brief to check on the vulnerability & make continuous mitigation of it so to avoid falling short from the security policies.

2. Continuous Monitoring:

- **Action**: Keep an eye for indications of malicious traffic on the network, and in particular for SMB related traffic. In motion, IDS and SIEM, to be alerted when there is an attempt to exploit the vulnerability just identified on the network.
- **Rationale**: As it stands, monitoring can be helpful to ensure that later attempts to exploit the SMBv1 will be caught and remedied as they're occurring, rather than causing too much damage before they're caught.

3. Incident Response Drills:

- **Action**: Periodically perform exercise of incident response to simulate an attack with SMBv1. These drills should demonstrate the containment of inflicted systems, restore from backups and stop malware or ransomware from spreading around the organization.
- **Rationale**: The essence of incident response plan testing is the ability to motivate the organization to act quickly when attacked, so to limit downtime and loss of service or data.

4. Policy Review and Updates:

- **Action**: Keep organizations security policies regarding the use of the SMB protocol under review and updated, at least every six months. Disable the SMBv1, make sure all the new equipment using the network has the same level of which it uses.
- **Rationale**: Therefore, any changes that occur in the IT infrastructure require policies to be updated to follow it so that a clear and consistent security standard cannot be set up and maintained in the IT environment.

### 2.3.3. Policy for Preventing and Mitigating the Vulnerability

By developing a strict policy of providing the preventive measures, the mitigation measures and responsive measures to the risks as such as SMBv1 exploit (CVE-2017-0144), the organization will be protected from such vulnerabilities. This policy will force having the organization take actions in response to attacks based on SMBv1 and the ones listed below. Thus we are to make a special policy containing the measures by means of which such risks should not arise, or diminish This policy is to ensure the plan to be followed out by the company to either stop or minimize SMBv1 based risks.

**Policy Name: SMBv1 Deactivation and Secure File Sharing Protocol Policy**

**Objective:**

The policy is that the SMBv1 issue **(CVE-2017-0144)** should be neutralized, and that most of organization's systems should not use the protocol. This policy is further intended to facilitate a transition away from less secure data sharing protocols, namely **SMBv2 and SMBv3**, and to implement a series of specific actions aimed at thwarting any attempted, containment of any possible, or subsequent abatement of any potential adverse consequences resulting from such an incident, or any incident of a similar nature.

The intended objective of this policy is to protect the Organization's information system from external and internal attackers on the organization's systems and information that can gain control and execute remote code, ransomware attack permitting and unauthorized access to the organization information system in order to ensure confidentiality, purity, and availability of the organization information system.

#### *2.3.3.1 Prevention*

**a) SMBv1 Deactivation:**

Every system within the organisation needs to shut down SMBv1 right now on all its systems. It is the responsibility of the IT department to ensure that none of the machines using this protocol are of latest technology.

The system administrators will perform a scan in order to make sure SMBv1 is indeed disabled on all the connecting sever, work stations and other related devices. Machines that are utilizing this outdated protocol.

**b) Secure Protocol Usage:**

The only two standard protocols that are accepted for the file sharing services are SMBv2 and SMBv3. However, security is added to these protocols with security features such as encryption and digital signing to enhanced some levels of attacks to the file sharing systems.

**c) Patch Management:**

Every system has to be patched to latest security patch level. Specifically, any device that used SMBv1 before the MS17:010 patch should also be patched with it. In the case of defined patches, there must exist a patch management process that defines patching cycles in order to be sure that all of the defined patches are actually being deployed at the proper time.

**d) Access Control:**

Persons without authorization to the systems should not have accesses to systems that are running SMB services.

Such implementation of the role based access control (RBAC) principle will be exercised whereby access to change of SMB related settings will be provided only to those personnel having specific responsibilities.

**e) Network Segmentation:**

Only company internal networks should have SMB traffic. Firewalls and networks need to be cutback, limiting of SMB connections, need to be segmented to prevent any transfers from external sources or any untrusted network.

#### *2.3.3.2 Mitigation*

a) **Backup Strategy:**

They also require that the system provides a backup schedule under which important data are to be backed up along with the configuration of the system.. To avoid the ransomware affecting these backups it must be stored somewhere inaccessible to the primary network area, these backups have to be located.

Make sure you do regular backups so you can test their efficacy and efficiency of recovering from the attack.

b) **Monitoring and Alerts:**

It has to be continuously monitored in a network and focused more on the SMB traffic which should be tracked using intrusions detection systems (IDS) and security information and event management tools (SIEM).

Unauthorized or suspicious SMB activity that is raised should cause the cybersecurity team to intervene quickly.

c) **Regular Security Audits:**

At least once per quarter a security audit to make sure the SMBv1 is disabled on all systems and that SMBv2/SMBv3 was configured securely. For such audits it should be obligatory to include vulnerability scans to identify either new or repeating security weaknesses.

#### *2.3.3.3 Response Measures*

a) **Incident Response Plan:**

If for example there is an attempt to attack an SMBv1 vulnerability or other such matters on the security level, the incident response team has to take down its affected systems instantly to prevent further propagation of that threat. After the attack is done, the team has to follow the organization set incident response process, namely, the assessment of the incident, and after that, further know about the attack and how it has been done through the forensic investigation.

b) **Recovery Protocol:**

If the successful attack results in a penetration of the system or loss of vital information, organization will revert back to its secure backups. In doing this, because the process of recovery strictly follows the disaster recovery and business continuity plan set, it reduces the duration of the time taken in the recovery process hence reduces the time it takes to get services up and running.

c) **Post-Incident Review:**

But in any event, there will be a security issues analysis that will be carried out any security breach connected with SMBv1 or similar problems. It will analyze how the adequacy of the response all the areas that were missed in the implementation of the mitigation measures and how occurrence can be prevented in the future. If the organization's organization structure goes down such as system penetration, loss of important information then it will revert back to its secured copies. In the recovery process, the disaster recovery and business continuity plan shall be followed from the later of and so that the time can be reduced to recover up the services as much as possible.

### *2.3.3.4 Policy Enforcement*

a) **Accountability**:

Responsibilities of implementation of this policy are the IT department and together with cybersecurity. Our system checks, system audit and system monitoring will ensure compliance. They will immediately fix any system that will be found running on the SMBv1 protocol or that hasn't followed up with the security standards laid down and they will report it to the relevant stakeholders.

b) **Compliance Audits:**

The policy can be seen to be enforced if all systems are followed in regular compliance audits.. The audits will consist of checking that fields don't travel through SMBv1, that security updates have been installed, and that network segmentation has been set up correctly and that access control is used.

c) **Consequences**:

This policy will be violated by any employee for this policy and will result in disciplinary process (such as termination of the employee's privileges on the system according to any

blame). Out of compliance, may result in security consequences, and liability will be assessed out of any such occurrence occurring out of non-compliance.

d) **Continuous Review and Updates:**

Annual review of this policy or more frequently as new threats or change of the organization's system environment warrant. Likewise, all affected departments will also be notified about the changes or updates of policy so that in case of modification of the policy, they are notified about it so that modification made in the policy can be used in combating security issues.

# 3.0 Conclusion

The vulnerability assessment of ShopEase Indonesia's systems, particularly the Windows Server 2008.vm, revealed essential security flaws which demand urgent remediation. Multiple critical vulnerabilities including Microsoft Windows SMB Server NTLM Multiple Vulnerabilities, Microsoft Windows SMBv2 Negotiation Protocol RCE Vulnerability and Microsoft Windows SMBv1 Vulnerability demonstrate the requirement for immediate implementation of strong cybersecurity practises. The identified security flaws present serious risks that could result in multiple damaging outcomes including unauthorised access to confidential customer information, compromised systems and disrupted operations.

The proposed scanning methodology with OpenVAS as the vulnerability scanning tool delivered an organised method to discover and evaluate security weaknesses. The methodology, which included preparation, configuration, execution, analysis, and reporting phases, ensured a thorough assessment of the system’s security posture. The risk assessment plans and mitigation policies offer practical solutions to handle identified vulnerabilities through strategies such as patch management, network segmentation, intrusion detection and employee training.

In conclusion, ShopEase Indonesia must implement long-term cybersecurity measures through continual vulnerability assessments while following industry standards and maintaining continuous system monitoring. By implementing the recommended policies and measures, the company can reduce future cyber breaches while protecting customer data and sustaining operational continuity. This report demonstrates that e-commerce platforms like ShopEase Indonesia need strong cybersecurity measures to defend against advancing threats which exist throughout today's digital environment.

# References


Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (December, 2016). *Guide for Cybersecurity Event Recovery.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

Blank, R., & Gallagher, P. (September, 2012). *Guide for conducting risk assessments.* Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

*CIS Releases 2017 Year in Review*. (2017). Retrieved from CISA: https://www.cisa.gov/news-events/alerts/2018/07/06/cis-releases-2017-year-review

*CVE-2010-0020 Detail*. (2 October, 2010). Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2010-0020

*CVE-2010-0021 Detail*. (2 October, 2010). Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2010-0021

*CVE-2010-0022 Detail*. (2 October, 2010). Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2010-0022

*CVE-2010-0231 Detail*. (2 October, 2010). Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2010-0231

*Documents*. (n.d.). Retrieved from Snort: https://www.snort.org/documents

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (June, 2017). *Digital Identity Guidelines.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

*Greenbone Community Edition – Documentation*. (n.d.). Retrieved from Greenbone: https://greenbone.github.io/docs/latest/

*Guide for Conducting Risk Assessments.* (September, 2012). Retrieved from NIST: https://csrc.nist.gov/pubs/sp/800/30/r1/final

*Microsoft Defender for Endpoint*. (25 September, 2024). Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint

*Microsoft Lifecycle Policy*. (n.d.). Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/lifecycle/

*Microsoft Security Bulletin MS09-050 - Critical*. (8 August, 2023). Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-050

*Microsoft Security Bulletin MS10-012 - Important*. (10 February, 2010). Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-012

Pamnani, V. (19 April, 2017). *Network security: LAN Manager authentication level*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level

Pamnani, V. (7 July, 2024). *What is Microsoft Baseline Security Analyzer and its uses?* Retrieved from Microsoft Learn Challenge: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/mbsa-removal-and-guidance

*Risk management — Guidelines.* (2018). Retrieved from ISO 31000:2018: https://www.iso.org/standard/65694.html

*Tenable Nessus® Professional*. (n.d.). Retrieved from Tenable: https://www.tenable.com/products/nessus/nessus-professional

*Vulnerability & Exploit Database*. (n.d.). Retrieved from RAPID7: https://www.rapid7.com/db/

# Appendix A. Workload matrix

| **Tasks Breakdown** | Suryakrishnan Balamurugan | Koo Wai Kit | Mostafa Aldabeeb |
|---|---|---|---|
| 1.0 Introduction | ☐ | ☒ | ☒ |
| 1.1 - Selection of a Vulnerability Scanning Tool | ☒ | ☒ | ☒ |
| 1.2 - Proposed Scanning Methodology | ☒ | ☒ | ☒ |
| 1.3 - Alternative Tools | ☒ | ☐ | ☐ |
| 2.0 Vulnerability Assessment, Risk Analysis, and Policy Formulation | ☐ | ☒ | ☐ |
| 2.1 - Microsoft Windows SMB Server NTLM Multiple Vulnerabilities | ☒ | ☐ | ☐ |
| 2.2 - Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability | ☐ | ☒ | ☐ |
| 2.3 - Microsoft Windows SMBv1 Vulnerability (CVE-2017-0144) | ☐ | ☐ | ☒ |
| 3.0 Conclusion | ☐ | ☒ | ☐ |
| References | ☒ | ☒ | ☒ |

Word count: 11179