Secure remote network: A comprehensive study to secure organization’s remote network and setup secure VPN

MSc Research Project
MSc in Cybersecurity

Vikas Rajak
Student ID: 23206071

School of Computing
National College of Ireland

Supervisor: Mr. Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Vikas Sunil Kumar Rajak

Student ID: 23206071

Programme: MSc in Cybersecurity **Year:** 2024- 2025

Module: Practicum 2

Supervisor: Mr. Jawad Salahuddin

Submission Due Date: 29.01.2025

Project Title: Secure Remote network: A comprehensive study to secure organization's remote network and setup secure VPN

Word Count: 9223 **Page Count:** 29

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 28.01.2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Secure Remote network: A comprehensive study to secure organization’s remote network and setup secure VPN

Vikas Rajak
23206071

Abstract

The growing reliance on remote work by numerous organizations and businesses has expanded the target landscape for cybercriminals. As a result, organizations must enhance their security measures to address challenges such as endpoint vulnerabilities, securing internet- and intranet-facing servers, and ensuring safe access to corporate resources. This paper explores the implementation of various security strategies to secure a organization’s remote networks and minimize the organization’s attack surface. Key measures include the adoption of secure authentication, robust endpoint protection, data encryption, and zero-trust security models. Emphasis is also placed on employee awareness and training to reduce human error, a significant contributor to security risks. A practical demonstration involved exploiting a vulnerable server and subsequently patching it to highlight the critical importance of maintaining updated and secure server configurations. Additionally, the research underscores the significance of Virtual Private Networks (VPNs) in securing organizational remote networks. It discusses the role of VPNs in enabling secure data transmission over public networks and evaluates various protocols, recommending L2TP/IPSec for its robust encryption and security features. The study also details the practical setup of a VPN server within a virtual environment, its connection to a host client, and subsequent hardening to ensure secure end-to-end communication. This comprehensive approach integrates theoretical insights with practical applications to strengthen organizational security in the remote work era.

1 Introduction

After the covid 19 pandemic most of the organizations has started to adopt work from home policy allowing their employee to work remotely. This provided a larger attack surface to an attacker to perform an attack on remote network of the organization. Thus, research is conducted to analyse the challenges faced by the organization in securing it’s remote network and provide relevant solutions to the challenges. To address the cybersecurity incidents related to remote working the aim of the project is to critically analyze and understand “How to secure an organization’s remote network, including a secure VPN setup?”
The research will contribute to the organization to secure their remote work policy by identifying and setting up a most secure remote network .The proposed solution will make use of most recent cybersecurity solutions and technologies. The research also looks into setting up a VPN server and securing the VPN server to ensure that the communication between the remote employee and the organization is secure. The research provide insights

on valid reasoning to keep upgrading the servers and components and not using outdated serves as they me contain potential vulnerability.

The question can be efficiently answered if the following mentioned objective are achieved at the end of the research
1. To provide recommendation to organization to secure their remote network
2. To perform an exploit mitigation process on a vulnerable server
3. To setup a VPN Server
4. To secure this VPN Server.

The structure of the report will follow the following sequence:

1. Related work:

The section will present critical analysis and discussion of research and studies conducted in the similar areas i.e. secure remote network an organization and a secure VPN setup.

2. Research Methodology:

This section will discuss a detailed methodology conducted to adopted to address the research question and complete the research including Providing solutions to secure a remote network of an enterprise organization, simulating a remote based attacks on a vulnerable system and providing mitigation process for the same, Setting up a secure VPN server.

3. Design Specification:

This section discusses the detailed process adopted to design and run the research work. The section is broadly divided into three major sections- Design description of a secure network diagram of an organization, Setup design and environment to performing remote based exploit, Designing and setting up a VPN server in virtual box

4. Implementation:

This section provides a detailed discussion on implementing the solutions and procedures those are necessary to answer the problem statement. The section provides implementation solutions for the following three aspects as per the research, securing a remote network of an enterprise organization, patching the vulnerability, implementing secure policies to harden the VPN

5. Evaluation

This section provides detailed steps to assess and evaluate the entire research, including the design specifications and implementation. The evaluation offers a clear insight into how effectively the proposed design and implementation address the research problem and how the provided recommendations can be practically applied in real-world situations.

6. Conclusion and future work

This section will conclude the research project and will highlight if the research question is been answered. The section also includes discussing the future that can be done in continuation of this research.

2 Related Work

The below literature review is carried broadly studies strategies for securing an organization's remote network and establishing a secure VPN setup. It evaluates previous research and similar work, providing the significant importance of VPNs in ensuring remote network security. The reviewed studies highlight the role of various VPN protocols, analyzing their requirements based on specific use cases. This study provides insights into selecting appropriate protocols to address distinct organizational needs, ensuring robust protection for remote connections while maintaining functionality.

The research paper titled "Ensuring Robust Security in Remote Work Environments: Addressing Challenges and Implementing Strategic Solutions" explores the increasing need of cybersecurity in remote working environment for an organization. The paper addresses the challenges a organization face while implementing a remote working policy such as management of end point devices as they can be the major obstacle for remote security if not hardened properly. Another major concern mentioned is authentication and access management for employees connecting remotely as week authentication and access management can allow malicious user to access the network. The research critically describes personal devices and unsecured home networks are increasingly targeted by ransomware, phishing, and malware attacks as these devices are vulnerable and if used for remote working can allow the attackers to access the organization's network by exploiting these vulnerabilities. The study further discusses the need of security solutions and best practices such as implementation of EDR, MFA, latest and stable encryption algorithm for data in rest as well as data in transit, role-based access control, secure VPN implementation. However, the research provides significant needs of secure processes that an organization needs to follow including frequent vulnerability assessments, audits, necessary employee trainings, implementation of proper Incident response plan and regularly updating it as the business evolves. Further, it mentions the importance of having clear business continuity plan in case of recovering from an incident (Anil, A.K., Anas, S., Parambil, I., and Santhosh, T.N., 2023).

The paper titled "Securing Remote Workforces: Challenges and Solutions" majorly address two sections i.e. Highlighting the challenges faced in securing remote workforce and providing effective solutions to mitigate security risk. In addition to the challenges and solutions mentioned in the last paper this paper critically discusses the challenges such as Network security including vulnerabilities in home network, lack of control over traffic as the employee access the corporate resources and data over various and vulnerable location may not allow organization to track and monitor the network. The analysis compliance challenges with data protection legal regulations, including GDPR and HIPAA compliance concerns, aligning with the rapidly evolving cybersecurity landscape. The research provides a descriptive discussion mitigate these challenges by implementing a secure VPN for secure remote access and enabling a zero-trust access methodology to verify and trust the user/ device. Zero trust works on never trust, always verify" approach to network access which enhances security by adapting granular level access control this methodology ensures network security. To ensure data security the paper recommends to implement end to end encryption and DLPs to prevent unauthorized data access. Similar to last research this paper too focuses on user training and awareness as it is one of the key methods that can prevent an organization from a cyberattack. The paper deeply focused on enabling real time monitoring using SIEM technology to monitor all the traffic and users interacting with organization's resources and implementation of threat hunting models to detect any kind of threat to organization and fix it before getting exploited (Saeed, S., 2023).

The research paper titled “Securing a remote workforce with zero trust strategy” explores the challenges posed by remote work, highlighting endpoint diversity, unsecured networks, and compliance as key vulnerabilities. The research emphasizes on implementation of zero trust and multi factor authentication for remote access to overcome these challenges. The implementation of Zero trust will significantly reduce the attack surface as it works on “deny all” and “trust, but verify” policy and giving minimum privilege to the user to access the resources only on need-to-know basis. The paper discusses how a zero-trust strategy be an ideal framework to secure access of an user on organization’s device from any location at any time with fine granular policies and monitoring. The research discusses the continuous steps to implement zero trust which include deliver the digital workspace, secure the device, secure the access, protect against threats and data loss, monitor user activity. Other than the mentioned zero trust strategy configuration the research focus on importance of employee training in mitigating cybersecurity risks. The research advocates a multi-layered approach addressing the unique challenges of securing remote workforces combining advanced technology and organizational policies (Cahill, D., and Grady, J., 2022).

The paper, A Survey on Designs and Implementations of Virtual Private Network (VPN), presents a comprehensive analysis of VPN technologies, emphasizing their role in modern network architectures. The research shows VPN designs, methodologies, and implementations, used in various industries, including corporate networks, military and healthcare. VPNs are mentioned as secure solutions for integrating remote and private networks, utilizing encryption to protect data across public infrastructures. The paper categorizes studies into four approaches: service, architecture, use case, and comparison, revealing trends like the shift toward hybrid and mobile broadband networks during the COVID-19 pandemic. It also evaluates the effectiveness of VPN implementations across sectors like government, power utilities, and broadcasting, underscoring challenges and innovative solutions. With the survey data from over 45 papers ranging from 1997 to 2022, The survey outlines the classification of VPN research covering designs, encryption methods, and protocols, while emphasizing on VPN’s adaptability in integrating diverse technologies and industries securely (Irsyad, I.D., and Mulyana, E., 2023).

The research paper “Comparing VPN Security Technologies” analysis the differences between various VPN protocols such as PPTP, L2TP, IPSec, and SSL including their advantages and disadvantages. The paper further focuses on the growing preference for SSL VPNs due to their ease of use and robust security features. As per the research the PPTP protocol is simple and transparent for users but it lacks strong encryption and are limited in scalability supporting only up to 255 connections. On the other hand, IPSec protocol offers strong encryption and end-to-end security. It is recommended to be an ideal protocol for site-to-site connections. However, it has basic dependencies such as requiring client software and exposing networks to security risks. The next protocol discussed is SSL VPNs, it operates at the application layer, providing granular access control, user-level authentication, and compatibility with modern browsers, making them suitable for remote access. SSL VPNs also include advanced features like host integrity checks and detailed activity logs, enhancing security. While IPSec is preferred for tightly controlled environments, SSL VPNs are increasingly favored for broader remote access needs due to their cost efficiency and simplified administration. The paper further mentions evolution of SSL VPN technology and its potential use cases, particularly with the adoption of IPv6, which may allow extensive using of IPSec is unlikely to reduce the increasing dependence on SSL VPNs (Lanos,E., and Costinela,D., 2012).

The paper “Analysis of the Importance of VPN for Creating a Safe Connection Over the World of Internet” focuses the critical role of Virtual Private Networks (VPNs) in ensuring secure communication in the digital age. It addresses the growing need for data protection across sectors like healthcare, e-commerce, and emergency services. It provides insights on VPNs capabilities including creating secure private networks over public infrastructures, offering features like encryption, authentication, and tunnelling to safeguard information from hackers. The paper further discusses various VPN protocols such as PPTP, L2TP/IPSec, and OpenVPN, critically describing their capabilities which includes encrypting data and enabling secure connections for remote and site-to-site communications. Further the research discusses the real time scenario which includes the affordability and accessibility of VPNs compared to traditional private networks, by mentioning how they lower operational costs while maintaining robust security. The paper further describes challenges like potential logging by VPN providers and solutions like employing advanced encryption algorithms and firewalls. The paper shows how VPNs enhance data confidentiality and network scalability, making them indispensable for secure online interactions. Thus, the paper critically describes how VPNs are not just tools for privacy but essential components of modern IT infrastructure, addressing cyber threats and ensuring the integrity of global communication networks (Islam, M.Z., Rahman Khan, M. A., Hossain, M. I. and Hossain, R., 2021).

3 Research Methodology

This section outlines the methodology adopted to address the research question: “How to secure an organization’s remote network, including a secure VPN setup?”

To gain a comprehensive understanding of secure remote configurations and VPN implementation, an extensive literature review was conducted. This review for securing remote network provided critical insights into the growing importance of cybersecurity in remote work environments, the challenges organizations face in maintaining secure remote operations, the necessity of robust security measures, and best practices to address these challenges and mitigate potential vulnerabilities. Additionally, the literature review for setting up a VPN setup focused on key aspects, such as understanding how VPNs enable secure remote connections between servers and clients, identifying the most secure VPN protocols, and exploring the design, methodologies, and implementation strategies adopted across various industries to integrate VPN solutions into organizational networks.

To critically answer the problem statement, research is divided into three major sections i.e.

- Providing solutions to secure a remote network of an enterprise organization.
- Simulating a remote based attacks on a vulnerable system and providing mitigation process for the same
- Setting up a secure VPN server

3.1 Securing a remote network of an enterprise organization

To establish comprehensive security for an enterprise's network, it is essential to implement a foundational secure network architecture. This framework ensures the organization has core cyber defenses in place, including effective network segmentation, VLAN segregation, strategic placement of firewalls, deployment of backup servers, proper integration of MZ and DMZ zones within the network, and the use of load balancers to mitigate network overloads. A detailed network diagram of an enterprise-level organization is outlined in the design specification with necessary security measures to be adopted to enhance the security of the network from a foundational to an advanced level.

To enhance the security of the enterprise network, the NIST Cybersecurity Framework is being used due to its flexible and risk-based approach to managing cybersecurity. It plays a crucial role in effectively segregating and understanding the processes of identifying, protecting, detecting, responding to, and recovering from security threats.

Below is a detailed explanation of how the NIST framework can contribute to improving the enterprise's security.

1. Identify**:** This phase focuses on recognizing potential threats and vulnerabilities within the network. It involves secure asset management, thorough risk assessments, and the implementation of governance policies within the organization.

2. Protect: It involves preventing and shielding organization from potential threats and attacks. This phase also ensures that the organization's critical and sensitive data is being prevented from getting compromised. This can be achieved by implementing secure access control, conducting awareness trainings and implementing data security policies.

3. Detect: It involves identifying and detecting any kind of attack or cyber incident within the network. This can be achieved by implementing continuous real time monitoring solutions and establishing baselines for detecting anomalies.

4. Respond: It involves efficient respond to an attack in case of an attack already happened. This ensures a efficient recovery from an attack. This can be achieved by implementing a strong incident response plan.

5. Recover: It involves restoring the data and systems after an attack has been happened to ensure the business continuity is achieved. This can be achieved by implementing a strong, secure backup and a DR server.

A detailed security implementation policies and procedures aligned with NIST are outlined in the design specification section of the report.

3.2 Simulating a remote based attacks providing mitigation process for the same

The aim of this section is to critically describe how an outdated server and OS can have a potential and unpatched vulnerability and can be very easily exploited by the attacker.

The section provides details of one of such remote based attack i.e. MS15-034 Vulnerability in HTTP.sys that could Allow Remote Code Execution can allow an attacker to compromise the system. Specifically, this vulnerability affects IIS 7.0 running on Windows 7 systems. The vulnerability arises due to an integer overflow condition in the HTTP.sys component, which handles HTTP requests for the server. An attacker can exploit this flaw by sending a specially crafted HTTP request to the vulnerable IIS 7.0 instance. When the request is processed, it can trigger the vulnerability (Microsoft, 2015).

If the attack is successful, it can allow the attacker to critically breakdown the system and make the system unavailable to the authorized users.

To simulate this attack consider a attacking machine placed outside the organization and it tries to attack the IIS 7.0 server placed in the organization remotely. The attack was performed by using a specially crafted HTTP request and executing it on the vulnerable target. The vulnerable request was appended in a python code and the same code was executed on the target making it unavailable.

The detailed setup and attack vector performed is discussed in the design specification section of the report.

3.3 Setting up a secure VPN server

A virtual private network is a communication protocol used to establish a digital communication between a computer and a remote server over a public network. VPN creates a point-to-point secure tunnel through which the data is travels in a secure manner by getting encrypted and protecting it from unauthorized access. It also masks the user’s IP which enhances the privacy and security. VPN is the most commonly technology used by the organizations which are involved in remote working policy and organization’s those have multiple branches and have to establish a secure communication channel (Microsoft Azure, 2024).

This segment of research aims to set up a VPN server and secure the server with various security policies that can safeguard essential VPN functionality including Access management in VPN, Logging and monitoring, user segregation, implementing a “Deny by default” approach to enhance overall security of VPN

The entire setup is executed in oracle virtual box where Windows server 2022 VM is configured as VPN Server and the host computer is operated as VPN client. The configuration ensures unique IP for server and client and they connect through VPN service. To setup this VPN server L2TP/ IPSec protocol is used as it has been identified through research and literature review as one of the most secure tunneling methods. L2TP/IPsec utilizes advanced encryption standards (AES) to ensure robust data protection and secure communication channels.

To secure the VPN server NSA, CISA guidelines were referred. This guidelines clearly explains processes to secure a VPN connection.

NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs which included

1. Updating and patching regularly
2. Enforce strong authentication
3. Encryption
4. Logging and Monitoring
5. Auditing and compliance
6. Secure Backups
7. Key exchange

4 Design Specification

This section discusses the detailed process adopted to design and run the research work. The section is broadly divided into three major sections:

- Design description of a secure network diagram of an organization
- Setup design and environment to performing remote based exploit
- Designing and setting up a VPN server in virtual box

4.1 Design description a secure network diagram of an organization

Consider a mid-sized organization's network diagram this includes- The basic segregation of the entire network into Demilitarized zone (DMZ) and Militarized zone (MZ). The incoming traffic from the internet enters the DMZ and lands on the perimeter router which controls inbound and outbound traffic between the external internet and the organization's network forwarding incoming data to the Layer 3 perimeter switch. The switch plays a critical role in routing traffic within the DMZ, which houses externally accessible services like web servers, mail servers, and application servers.

The switch transfers this incoming traffic to the perimeter firewall. The perimeter firewall act as first line of defense which should be configured with strong firewall rule, IDS, IPS to ensure only legitimate traffic enters the network and any malicious traffic if present id detected and prevented from getting in the network. After getting filtered from perimeter the traffic lands on the load balancer which performs to ensure only legitimate traffic enters the network and any malicious traffic if present id detected and prevented from getting in the network and efficiently distribute the incoming load efficiently in the MZ.

After the traffic enters the MZ, it is processed by the core firewall. This traffic is further routed through the core switch, eventually reaching the server farm, which hosts servers in various VLANs supporting different applications.

After the perimeter firewall the filtered traffic enters the MZ and lands on the core firewall and after getting filtered from core firewall the traffic lands on the core switch from where the traffic lands on the server farm which are the servers in multiple segments and applications it in different VLANS. This is how a idle network is configured.

To adapt the network for a remote working policy, the initial configuration remains unchanged for external internet traffic. where the internet traffic (Remote user) enters the network through DMZ and then it lands on VPN array. Now, Large enterprise organizations often handle large number of remote working employees thus they need to implement a series of VPN server termed as VPN array. The VPN server should authenticate the user and should allow the user to access a regular system in the network (no direct access to the server). On the regular server the user can take a Remote desktop connection (RDP) to the required server and carry on the work remotely based on the access permissions defined for the remote user

Thus, given the critical nature of remote access it is essential to set up a secure and robust VPN server to prevent unauthorized access and ensure a secure remote working environment.

4.2 Setup design and environment to performing remote based exploit

Consider an organization has an IIS 7.0 server running on windows 7 inside the network of an organization. In a remote network setups scenario, if the remote employee of the organizations has known and unpatched vulnerabilities in their system it can be exploited by an attacker to gain access of the remote employee’s system. Once the attacker has the access to the compromised remote system they can infiltrate and access the organization’s network. By performing necessary reconnaissance steps the attacker can identify the presence of vulnerable IIS server in the network and can try to exploit the MS15-034 Vulnerability in HTTP.sys. which could allow remote code execution or denial-of-service attacks.

To set up this real time scenario the research makes use of Oracle virtual box where the kali linux VM is acting as an attacking machine the IIS 7 on windows 7 VM is the target machine. Following steps were performed to simulate the mentioned attack.

1. As described in the above case the attacking machine was able to directly connect to the target machine the Figure 1 of appendix shows ping status from kali linux to Windows 7
2. The malicious python script was prepared on the attacking device. This code was available publicly (jc-base4sec, 2020).
3. The attack was launched by using the following command (jc-base4sec, 2020):
   “python <Python file name>.ppy -t <Tagret IP adress> -p <port> --exploit”

The attack was successful and the target system successfully breakdown which is evident in figure 2 of appendix.

4.3 Designing and setting up a VPN server in virtual box

A real-time VPN server in an enterprise remote network setup enables two systems—one located within the organization’s secure internal network and another situated remotely outside the secure network (in different networks)—to communicate securely. To simulate this real-time scenario, the configuration is implemented using Oracle VirtualBox. This allows the virtual environment to mirror the similar separation and secure connectivity between the internal and external systems.

Following are the steps setup a VPN server on Oracle Virtual Box:

1. In oracle virtual box, Windows server 2022 VM was installed to setup a VPN server
2. The host computer with windows 11 OS acted as the VPN client.

This setup simulates the Windows server 2022 as a internal VPN server and Windows 11 host as a remote client.

3. The windows server 2022 VM uses bridged network to establish the connectivity.

The Bridged network allows the machines have two separate IPs in same subnet similar to the VLAN segregation of an enterprise VPN setup. This setup replicates to two systems with different Ips not present in the same network have to connect to each other through VPN.

4. After configuring network connection, install all the necessary packages and modules needed to setup a VPN server

These packages and modules include installation of Remote Access feature, Direct Access and VPN (RAS), Routing along with management tools.

5. Next step is to set up and configure Routing and Remote Access in tools section of server manager.

This step allows to select services that are to be enabled on the server in this case select “VPN access”

6. To setup a secure Routing and remote access, in server manager select the server name.

In the properties section, under security, configure following settings

   a. Authentication provider: Windows Authentication
   b. Accounting provider: Windows Accounting
   c. Enable “Allow custom IPSec policy for L2TP/IKEv2 connection” and provide a pre-shared key which will be further used by client to connect to server.

Before going to the next step of IP configuration, set the static IP for the VPN server as it will be further needed by client to connect to the same IP address. Under IP4 section select static address pool IPv4 address range of your organization’s need, ensure that the IP range should not conflict with the server’s IP and Client IP. Enter the starting address and ending address of the IP address range, you want the users to assign to. and click on “Apply”. And restart the server to save all the configuration changes.

7. Configure Firewall Rules

To allow VPN traffic it is mandatory to allow UDP Port 1701 for L2TP, UDP 500 for IPSec. This ports can be configured and allowed by creating the new rules (if not existing already already) in the inbound rules section.

8. Create a VPN user

On VPN server create a user that will be used by the client to connect to VPN server. Create a user, provide username and password which will be further used to connect to VPN server. Under the user's property allow access for network access permission in dial-in tab

9. VPN client configuration

   9.1 Configure firewall rules:

   To allow VPN traffic it is mandatory to allow UDP Port 1701 for L2TP, UDP 500 for IPSec similar to server configuration. These ports can be configured and allowed by creating the new rules (if not existing already already) in the outbound rules section.

   9.2 Adding VPN connection:

   a. VPN connection name
   b. Server name: IP address of the server
   c. Pre-shared Key: Key provided while setting up the server
   d. Type of sign-in info: Username and password
   e. Username: Username of the user created
   f. Password: Password assigned

10. Connect to VPN

Figure 3 of appendix shoes a successful connection between a VPN server and a client desktop.

Following steps will allow to setup a end to end VPN setup that will simulate a real world scenario

After a successful set up the necessary security policies and protocols are implemented on the VPN server to secure it as per the NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs which included Secure encryption, Authentication, Logging and monitoring, Patching and updates, Audit and compliance, Backup servers.

5 Implementation

This section provides a detailed discussion on implementing the solutions and procedures those are necessary to answer the problem statement. The section provides implementation solutions for the following three aspects as per the research

- Securing a remote network of an enterprise organization
- Patching the vulnerability of IIS 7.0 server on windows 7
- Implementing secure policies to harden the VPN

5.1 Securing a remote network of an enterprise organization

As understood in the literature review the organization which operates on remote working policy have to face significant cybersecurity challenges. To mitigate and overcome this challenges the enterprise organization is recommended to implement secure polices and procedures to ensure their cybersecurity posture of remote network is strong enough to prevent itself form a cyber-attack.

The report follows a NIST framework to ensure overall security of the enterprise's remote is hardened (Cisco., n.d.), (Gittlen, S., 2021) and (BrendaCarter,. n.d.).

1. **Red teaming exercise:**

   Red teaming is an ethical security assessment approach where red team professionals simulate the real time attacks on the organization's network in a way a real-world attackers would to attempt to compromise an organization's network. By emulating the actions of malicious actors, red teaming helps identify vulnerabilities and weaknesses in the organization's defenses that might otherwise go unnoticed.

   Implementing red teaming exercise will allow organization to

   - Identify realistic understanding of their security posture
   - Test and upgrade the defense mechanism and increase the cyber readiness of the organization
   - Implement actionable recommendations to patch the discovered vulnerabilities.

2. **Internal and external audits**

   Internal or external audits ensures that the organization is secured with most advanced security policy and the organization comply with various cybersecurity compliance body such as ISO 27001.

   Implementing a policy for regular audits enables an organization to systematically identify and analyze gaps in its security posture. This approach ensures alignment with compliance requirements set by regulatory bodies such as ISO 270001 helping address real-time advanced security threats. Thus, by conducting frequent audits, organizations can proactively update their defenses, improve compliance with evolving standards, and strengthen their overall cybersecurity strategy.

3. **Threat intelligence and threat hunting**

   Threat intelligence is the process of identifying potential threats to an organization by analyzing both previous and current threats the organization has faced, as well as the large global threat landscape affecting similar organizations or businesses. It involves gathering and assessing information to predict and understand the tactics, techniques, and procedures (TTPs) used by cyber adversaries. Additionally, threat hunting is a proactive approach focused on identifying and mitigating threats that are either previously known or ongoing and have not yet been remediated. Threat hunters actively search for anomalies, hidden threats, and signs of compromise within a network, often before they conduct a full fledge attack

Thus, implementing both the process of threat intelligence and threat hunting will allow the cyber professionals of the organization to identify and mitigate the potential threats to the organization.

4. **Blue teaming exercise**

Blue teaming is the process in which the blue team professionals, establishes and implements robust defense mechanisms to safeguard an organization's network and infrastructure. The of this goal is to protect the organization from cyber threats and ensure the integrity of the network. The blue team's defenses are then tested and evaluated by the red team, which simulates attacks to bypass the defenses and attempt to compromise the network, much like a real-world cyber adversary.

Implementing blue teaming exercise will allow organization to

- Implement defense mechanism for real time attacks.
- Provide solutions to the identified vulnerabilities in read teaming.
- Keep the security posture of the organization upgraded.

5. **Encryption**

Encryption is essential for safeguarding an organization's sensitive and critical data, ensuring its confidentiality. Organizations are recommended to apply robust encryption methods to protect both data at rest and data in transit.

- For data at rest, AES 256-bit encryption is highly recommended due to its strong security and widespread adoption in securing stored data.
- For data in transit, implementing TLS v1.2 or a higher version ensures secure communication channels, protecting data as it moves across networks.

6. **Strong authentication**

It is recommended for organizations to implement a secure authentication system, such as centralized authentication with two-factor authentication (2FA). This approach consolidates user access to the organization's network by providing a single platform for authentication, offering efficient and comprehensive monitoring for administrators. Additionally, centralized authentication ensures accountability by providing detailed data on user activities and tasks performed, contributing to enhanced security and auditability.

7. **Access management**

In an enterprise organization, access management plays a critical role in safeguarding data from unauthorized access. Key components of implementing robust access control include:

1. Role-Based Access Control (RBAC): This allows organizations to define specific roles and responsibilities, assigning access permissions to users based on their roles and ensuring they only have the minimum necessary privileges.
2. Authentication: This process involves verifying the identity of users through various authentication technologies, such as Multi-Factor Authentication (MFA) or password-based authentication, to ensure only authorized users gain access.
3. Authorization: After successful authentication, authorization specifies the access permissions granted to the user, defining what actions or resources they can access within the organization's network.
4. Accountability: This refers to tracking and monitoring user activity, ensuring that all actions within the organization's network can be logged.

8. Network segregation

Network segregation is the security practice where the organization is recommended to segregate their network into multiple sub network to improve the overall security of the network.

Network segregation allows following security in the network.

- Allows to segregate critical and important data on different with high and most strong security on that network.
- It improves over security performance such as separating user traffic from administrative traffic
- It allows easier and effective monitoring
- It reduce the attack surface of an attack as if the network is segregated the attacker will have minimum lateral movement

9. Antivirus

It is recommended to implement strong Antivirus, IDS and IPS tools as they provide basic and effective security to the environment by prevent the access of malicious threat in terms of malicious traffic and code to be detected and blocked at the entry level.

10. EDR

Endpoint Detection and Response (EDR) such as Microsoft Defender for Endpoint is a cybersecurity solution designed to monitor, detect, and respond to threats on endpoint devices like laptops, desktops. EDR tools provide visibility into endpoint activity, allowing organizations to quickly identify and mitigate security incidents. Implementing EDR can allow the organization to have continuous monitoring on the device, Threat detection on the device, EDRs store log details making the forensic process efficient. Thus, it is recommended to have EDRs on the endpoint devices of the organization

11. DLP

Data loss prevention (DLP) such as McAfee Total Protection for DLP, Microsoft Purview DLP, Trend Micro Integrated DLP prevent sensitive and critical data of organization from being accessed, or leaked outside an organization. Thus it is recommended to enable

DLP in the network as it ensures that critical information, such as PII data or financial data remains protected against unauthorized access or exfiltration.

12. **User training**

Training and awareness are critical components of an organization's overall security strategy. Even with advanced security tools and technologies in place, a single error or lapse in judgment by employees can compromise the entire organization. Therefore, it is recommended to regularly provide comprehensive training programs to educate staff about the latest cyber threats, vulnerabilities, and preventive measures.

13. **Secure VPN Configuration**

As the considered organization operate on remote access, it is essential to select a secure and efficient protocol for establishing remote connections. In this research, VPN technology is utilized to connect to remote devices. To ensure maximum security, it is recommended to use the most secure VPN protocol, such as L2TP/IPsec. This protocol offers strong encryption for data transmission and secure communication with remote systems, safeguarding sensitive information during remote access.

14. **Firewall rules configuration**

It is recommended to implement multiple firewalls in the organization such as Perimeter firewall and core firewalls. Perimeter firewall will be placed at the out edge of the network to filter the incoming traffic in the network. However, a core firewall is placed incident the network of the organization to secure internal traffic.

The firewalls should be configured with strong firewall rules and Iptables to ensure only allowed traffic gets the access of network and internal segments.

15. **zero-trust network access**

The Zero Trust security model is one of the most recent and highly recommended approaches for enhancing network security. This model operates on the principle of "deny all by default" at every stage of the network. Rather than relying on a one-time authentication and authorization process at the network perimeter, Zero Trust continuously verifies identity and access throughout the network. It minimizes unnecessary lateral movement between applications, services, and systems, accounting for both insider threats and the risk of a legitimate account being compromised. By doing so, it significantly strengthens the network's security posture and reduces the overall attack surface

16. **Logging and monitoring**

Logging and monitoring is a critical practice that organizations are recommended to implement, as it enables the recording and preservation of various events and activities occurring across the network. This includes tracking user actions, system processes, application behaviors, and network activities. By enabling logging and monitoring, organizations can generate essential logs such as system logs, network logs, and audit logs, which provide valuable insights for security and operational oversight.

17. **Real time monitoring**

    Organizations are recommended to implement advanced tools capable of real-time network monitoring to proactively identify and respond to potential threats. Solutions like Security Information and Event Management (SIEM) systems are instrumental in aggregating, analyzing, and monitoring security events across the entire network. By providing centralized visibility into incidents and activities, SIEM helps detect anomalous behaviors and potential malicious activities, enabling prompt detection and response.

18. **Implement strong IRP**

    Organizations are recommended to implement a comprehensive and robust Incident Response (IR) plan to ensure an effective and organized approach to handling cyber incidents. A well-defined IR plan allows the organization to respond quickly and efficiently, minimizing the incident's impact on business operations, reputation, and financial resources.

19. **Strong backup solution:**

    Organizations are recommended to maintain backups of critical data in a secure, separate network to ensure that, in the event of an incident, the backup remains uncompromised. This strategy safeguards the integrity of the backup and ensures that data can be quickly restored for efficient recovery operations.

20. **DR servers**

    In the event of downtime caused by a cyber incident impacting an organization’s primary operations, a robust disaster recovery (DR) server ensures that essential functions can seamlessly transition to the DR environment. This minimizes disruption to critical processes, strengthens organizational resilience, and supports continuity of operations with minimal impact on productivity.

5.2 Patching the vulnerability of IIS 7.0 server on windows 7

The vulnerable IIS 7.0 server on windows 7 has a vulnerability in HTTP.sys. which was exploited leading to a denial-of-service attacks. This section provides detailed patch implementation process to ensure the vulnerability is been mitigated and the server is secure for the respective attack.

As per the guidelines released by Microsoft to prevent an enterprise organization from such attacks it is recommended them to not use outdated or an unpatched system. Thus, it is recommended to use the upgraded version of IIS to ensure all the known vulnerabilities are been patched.

Alternately, If an organization is completely dependent on the system it is recommended them to implement all the secure policies released by the OEM (Microsoft in this case) to ensure the systems are secure.

To prevent IIS 7.0 on windows 7 from MS15-034 Vulnerability it is recommended to disable kernel caching from the server. Following process can be used to disable the same

1. Open IIS manager
2. In the feature view, open output caching
3. On the output caching page, select edit feature setting in the action pane
4. In the edit output caching setting, select disable kernel cache and click OK.

Kernal caching is a vulnerable service enabled by default on the IIS 7 that needs to be disabled manually or use the upgraded versions of IIS that has kernel caching disabled by default preventing it form the mentioned attack.

A patched server is shown in the figure 4 of appendix

Note:
This simulation demonstrates how an attacker can effortlessly compromise a system by exploiting known vulnerabilities. Therefore, it is strongly advised that organizations avoid using outdated or vulnerable components within their networks, whether on the internet or intranet. While the organization asserts that a vulnerable server exists only in the intranet and relies on robust perimeter security to prevent unauthorized access, it is crucial to acknowledge that if perimeter defenses are breached, maintaining secure and updated systems within the network would serve as an additional layer of protection.

5.3 Implementing secure policies to harden the VPN

As per the design specification a VPN server is configure on Windows server 2022 in a virtual environment. To fully answer the research question hardening of this VPN server needs to be done. The VPN server is hardened on the basis of NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs.

1. Managing Authentication
   The configured VPN server uses authentication provided by windows i.e. MS-CHAP v2 and EAP (Extensible Authentication Protocol) when paired with authentication technique such as username and password base, pre shared key it make a strong authentication mechanism for the VPN server. The configured Authentication method is shown in figure 5 of appendix (Crawford, D. 2019) and (Zacheller.dev. 2020)

2. Logging and monitoring
   It is recommended to configure logging and monitoring configuration on the VPN server to ensure all events, including security and system logs related to the VPN server, are recorded. The successful logging and monitoring configuration with locating logs file is shown in figure 6 and figure 7 of appendix

3. Patching and updates
   Patching and updating the server with the lates release patch ensure that the server are secure for the know vulnerabilities. Thus it is recommended to install all the released patch and updates on the server. The the patching and updating configured to automatically download all released patches from the OEM as soon as they become available as shown in figure 8 of appendix

4. Audit and compliance
   The auditing policy is successfully configured on the VPN server, the server has been successfully set up to track and log all successful and failed events for the required audit policies specified in the implementation plan. Configured audit policy is shown in figure 9 of appendix

5. Secure encryption configuration:
   The configured VPN server utilizes the L2TP/IPSec protocol, which uses the latest encryption standards by default, i.e. AES 256-bit encryption. This ensures a highly secure mode of remote communication. Thus, it is recommended to configure AES 256 with IPSec to provides a strong layer of protection by securing data integrity and confidentiality during transmission. This setup enhances the overall security of remote access, making it suitable for safeguarding sensitive data in the organization. Figure 10 of appendix shows encryption configuration

6. Setting up a secure backup
   It is recommended to maintain backups of critical data in a secure, separate network to ensure that, in the event of a cyber-attack, the backup remains uncompromised. A backup configuration with it’s specific limitation is shown in the figure 11 and figure 12 of appendix

6 Evaluation

This section provides detailed steps to assess and evaluate the entire research, including the design specifications and implementation. The evaluation offers a clear insight into how effectively the proposed design and implementation address the research problem and how the provided recommendations can be practically applied in real-world situations.

The evaluation of the research is broadly classified in following three sections:

- Evaluating secure remote network
- Evaluating the attack simulation
- Evaluating the security of VPN Server

6.1 Evaluating secure remote network

As the research methodology mentions the organizations remote network security can be asses based on the NIST framework, the same framework is is applied to evaluate the proposed implementation for securing the organization's remote network.

According to the NIST framework, securing an organization’s end-to-end network requires the security policy to clearly implement the following phases: Identify, Protect, Detect, Respond, and Recover.

Below is a detailed explanation of how the outlined security implementation steps align with the NIST framework and contribute to enhancing the enterprise's security.

1. Identify

Security implementation including Red teaming exercise, Internal and external audits, Threat intelligence and threat hunting clearly discuss how an incident, a potential vulnerability and threat in an organization’s network can be identified.

2. Protect

The recommendations for implementing the following security measures, Blue teaming exercises, encryption, strong authentication, access management, network segregation, antivirus, EDR, DLP, user training, secure VPN configuration, firewall rules configuration, and zero-trust network access, ensure the protection of the organization’s sensitive and critical data from malicious access or attacks.

3. Detect

The implementation recommendation for implementing Logging and monitoring and Real time monitoring ensures that the organization’s entire network is continuously monitored and presence of any kind of anomaly and threat can be detect efficiently

4. Respond

The implementation of a robust Incident Response Plan ensures that the organization is well-prepared and resilient enough to detect, respond and recover from any incidents. As this plan not only helps in minimizing damage but also ensures a rapid recovery, reduces downtime, and safeguards critical assets.

5. Recover

The implementation of secure backups and the deployment of a disaster recovery (DR) server ensure that, in the event of an incident, critical data can be restored, allowing the organization to continue operating smoothly using the backup data or running on the DR server.

6.2 Evaluating the attack simulation

The attack simulated on vulnerable IIS 7.0 server on windows 7 was patched by configuring necessary policy recommended by Microsoft i.e. disabling kernel caching on IIS 7.

It is necessary to evaluate the patch applied to ensure that the server is secure for the mentioned vulnerability. Thus to evaluate the server’s security against MS15-034 Vulnerability in HTTP.sys. the same attack was perform again.

As a result of this attack did not affected the system (the system was up) ensured that the patch worked properly and the system was secure.

6.3 Evaluating the security of VPN Server

As the research methodology mentions the VPN sever can be hardened based on the NSA, CISA Release Guidance on Selecting and Hardening Remote Access VPNs.
Thus, to evaluate the security of the configured framework can be made based on the mentioned framework.

NSA, CISA Release Guidance suggest a VPN server should have following security configurations- Secure encryption, Authentication, Key management, Logging and monitoring, Patching and updates, Audit and compliance, Backup servers.

Based on the security configuration made in implementation they can be evaluated as follows based on NSA, CISA Release Guidance:

1. Managing Authentication
   As per the guideline a strong authentication is configured provided by windows i.e. MS-CHAP v2 and EAP when paired with authentication technique such as username and password base, pre shared key it make a strong authentication mechanism for the VPN server.

2. Logging and monitoring
   According to the logging and monitoring configuration on the VPN server, all events, including security and system logs related to the VPN server, are recorded. These logs are stored in the log file folder located at /windows/system32/.

3. Patching and updates
   As per the configured patching and updating recommendations, the server is set up to automatically download all released patches from the OEM as soon as they become available.

4. Audit and compliance
   As per the configured auditing policy the server is successfully configured to audit all the success and failure instances of all necessary audit policies mentioned in implementation

5. Secure encryption configuration:
   As per the encryption configuration, AES 256 was configured with IPSec to enhance the security of sensitive data over the VPN.

6. Setting up a secure backup
   As per the secure backup configuration, the backup needs to be configured in a different network to ensure in case of network or server getting compromised the backup server is ready to reload the sensitive data. The VPN server has the feasibility to configure backup on remote location as mentioned in the implementation. However, in this research it was not feasible to set up a remote backup server. Thus, a secure remote backup is not configured in the research.

6.4 Discussion

The report presents a comprehensive analysis addressing the research question, “How can an organization’s remote network be secured, including the implementation of a secure VPN setup?” The research objectives are achieved through the configuration and hardening of a VPN server. It highlights the critical importance of maintaining secure and regularly updated servers by simulating a remote based attack on a vulnerable server. Additionally, the report elaborates on the process of establishing a secure remote network for an organization. However, the VPN configuration was conducted on a virtual machine, which limited the implementation to a simulated environment rather than a real-time setup.

7 Conclusion and Future Work

The primary objective of this research project was to establish a secure remote network for an organization by integrating multiple security measures to protect against potential cyber-attacks. The implementation followed the NIST Cybersecurity Framework, ensuring comprehensive hardening of the organization's network infrastructure. Another key goal was to highlight the importance of maintaining patched servers on both the organization's internet-facing and intranet networks to add an additional layer of security. This was demonstrated by successfully exploiting a remote vulnerability on the server and applying a patch to discuss the need for secure policy configurations and the risks posed by unpatched vulnerabilities. The project also involved setting up a VPN server within a virtual environment to simulate a real-world VPN server architecture. A real-time VPN setup would require a live remote network and multiple devices, which were beyond the scope of this study. Despite this limitation, the VPN server was successfully configured and connected to the VPN client (host laptop) used in this research. To further enhance security, a hardening process was implemented to ensure the VPN server provided a secure communication channel, aligning with organizational needs for remote work policies. Thus, the research meets the designed objective.

The project presents opportunities for further research, particularly in evaluating the risks associated with insider threats in organizations operating remotely. This includes exploring methods to detect and mitigate insider threats to safeguard the organization's network. Additionally, the work could involve developing strategies and implementing tools to proactively identify and address vulnerabilities that may be exploited by internal actors.

References

Anil, A.K., Anas, S., Parambil, I., & Santhosh, T.N. (2023) ‘Ensuring Robust Security in Remote Work Environments: Addressing Challenges and Implementing Strategic Solutions’ , Available at: https://www.researchgate.net/publication/376490112_Ensuring_Robust_Security_in_Remote_Work_Environments_Addressing_Challenges_and_Implementing_Strategic_Solutions [Accessed 06 October 2024]

BrendaCarter (n.d.). *Secure remote and hybrid work with Zero Trust*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/security/zero-trust/adopt/secure-remote-hybrid-work. [Accessed on: 13 November 2024].

Cahill, D., and Grady, J. (2022) ‘Securing a remote workforce with zero trust strategy’, Available at: https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/securing-a-remote-workforce.pdf [Accessed 06 October 2024]

Cisco. (n.d.). *What Is Secure Remote Access?* [online] Available at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-secure-remote-access.html. [Accessed on: 08 November 2024].

Crawford, D. (2019). *VPN Encryption Types | OpenVPN, IKEv2, PPTP, L2TP/IpSec, SSTP*. [online] ProPrivacy.com. Available at: https://proprivacy.com/vpn/guides/vpn-encryption-the-complete-guide. [Accessed on: 10 October 2024].

Gittlen, S. (2021). *Ultimate Guide to Secure Remote Access*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/Ultimate-guide-to-secure-remote-access. [Accessed on: 08 November 2024].

Irsyad, I.D., and Mulyana, E. (2023) ‘A Survey on Designs and Implementations of Virtual Private Network (VPN)’ in *2023 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 2023, pp. 1-6, doi: 10.1109/ICEEI59426.2023.10346627,* Available at: https://ieeexplore.ieee.org [Accessed 13 October 2024]

Islam, M.Z., Rahman Khan, M. A., Hossain, M. I. and Hossain, R. (2021) ‘Analysis the importance of VPN for Creating a Safe Connection Over the World of Internet’ *in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 10, Issue 10, October 2021 DOI: 10.17148/IJARCCE.2021.101017,* Available at: https://ijarcce.com/wp-content/uploads/2021/11/IJARCCE.2021.101017.pdf [Accessed on: 12 October 2024]

jc-base4sec (2020). *MS15-034/MS15-034.py at master · jc-base4sec/MS15-034*. [online] GitHub. Available at: https://github.com/jc-base4sec/MS15-034/blob/master/MS15-034.py [Accessed on: 30 September 2024].

jc-base4sec (2020). *MS15-034/usage.txt at master · jc-base4sec/MS15-034*. [online] GitHub. Available at: https://github.com/jc-base4sec/MS15-034/blob/master/usage.txt [Accessed on: 30 September 2024].

Lanos,E., and Costinela,D. (2012) ‘Comparing VPN Security Technologies’ *in 2nd World Conference on Innovation and Computer Sciences 2012,* Available at: https://www.academia.edu/ [Accessed 15 October 2024]

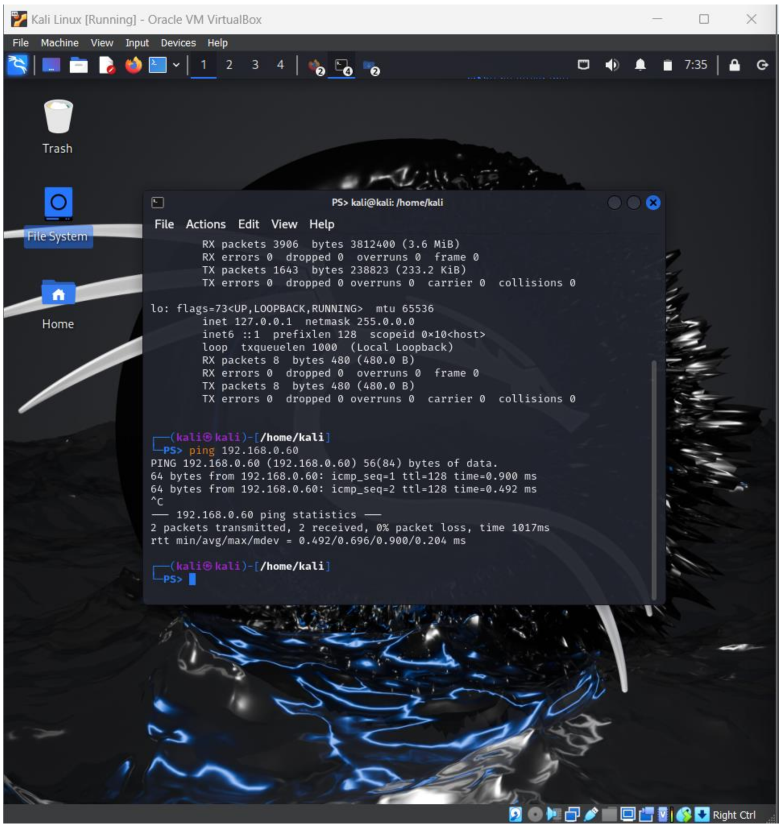
Microsoft (2015). *Microsoft Security Bulletin MS15-034 - Critical*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034 [Accessed on: 20 September 2024]

Microsoft Azure (2024). *What is a VPN? Why Should I Use a VPN? | Microsoft Azure*. [online] azure.microsoft.com. Available at: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn [Accessed on: 29 September 2024]

Saeed,S. (2020) ‘Securing Remote Workforces: Challenges and Solutions’, in Journal of Immigrant & Refugee Studies, Available at: https://www.researchgate.net/publication/380787944_Securing_Remote_Workforces_Challenges_and_Solutions [Accessed on: 04 October 2024]

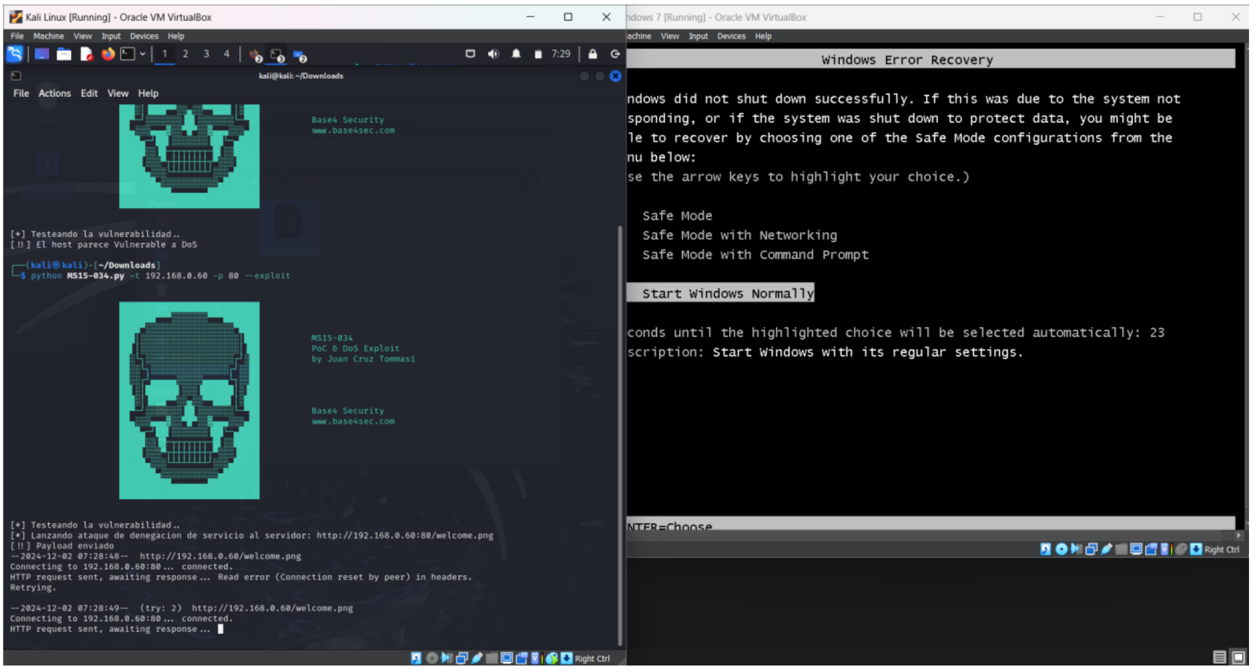
Zacheller.dev. (2020). *VPN Protocols | SecWiki*. [online] Available at: https://wiki.zacheller.dev/network-security/courses/isci-cnss-course/virtual-private-networks-vpn/vpn-protocols [Accessed on: 10 October 2024].

Appendix


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:35
Trash
File System
Home
PS> kali@kali: /home/kali
File Actions Edit View Help
Right Ctrl

```
        RX packets 3906  bytes 3812400 (3.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1643  bytes 238823 (233.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[/home/kali]
└─PS> ping 192.168.0.60
PING 192.168.0.60 (192.168.0.60) 56(84) bytes of data.
64 bytes from 192.168.0.60: icmp_seq=1 ttl=128 time=0.900 ms
64 bytes from 192.168.0.60: icmp_seq=2 ttl=128 time=0.492 ms
^C
── 192.168.0.60 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1017ms
rtt min/avg/max/mdev = 0.492/0.696/0.900/0.204 ms

┌──(kali㉿kali)-[/home/kali]
└─PS> 
```

Figure 1: Ping status of target (Windows 7) from attacking machine (kali Linux)

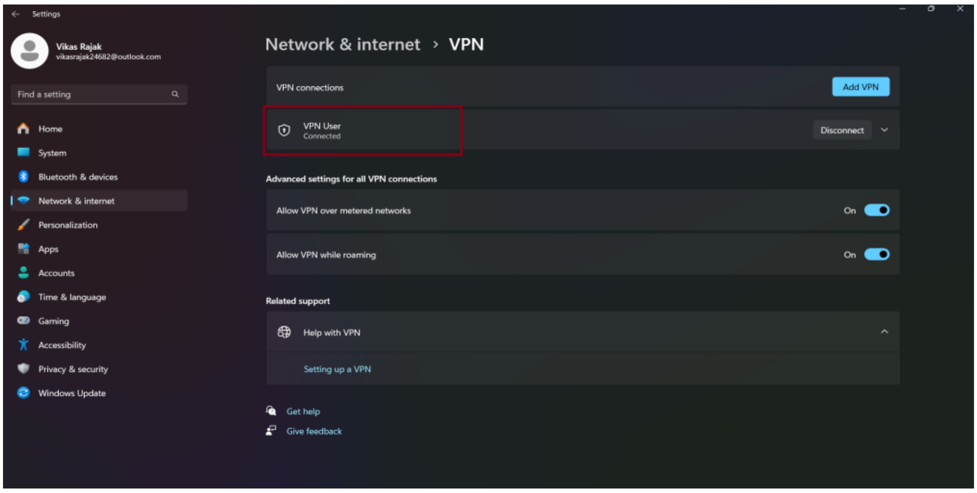


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help
ndows 7 [Running] - Oracle VM VirtualBox

```
Base4 Security
www.base4sec.com

[*] Testeando la vulnerabilidad..
[!!] El host parece Vulnerable a DoS

┌──(kali㉿kali)-[~/Downloads]
└─$ python MS15-034.py -t 192.168.0.60 -p 80 --exploit

MS15-034
PoC & DoS Exploit
by Juan Cruz Tommasi

Base4 Security
www.base4sec.com

[*] Testeando la vulnerabilidad..
[*] Lanzando ataque de denegacion de servicio al servidor: http://192.168.0.60:80/welcome.png
[!!] Payload enviado
--2024-12-02 07:28:48--  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response... Read error (Connection reset by peer) in headers.
Retrying.

--2024-12-02 07:28:49--  (try: 2)  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response...
```

```
                                Windows Error Recovery

ndows did not shut down successfully. If this was due to the system not
sponding, or if the system was shut down to protect data, you might be
le to recover by choosing one of the Safe Mode configurations from the
nu below:
se the arrow keys to highlight your choice.)

  Safe Mode
  Safe Mode with Networking
  Safe Mode with Command Prompt

  Start Windows Normally

conds until the highlighted choice will be selected automatically: 23
scription: Start Windows with its regular settings.

NTER=Choose
```

Figure 2: The Target crashed and the attack was successful



Network & internet › VPN

VPN connections — Add VPN

VPN User
Connected — Disconnect

Advanced settings for all VPN connections

Allow VPN over metered networks — On

Allow VPN while roaming — On

Related support

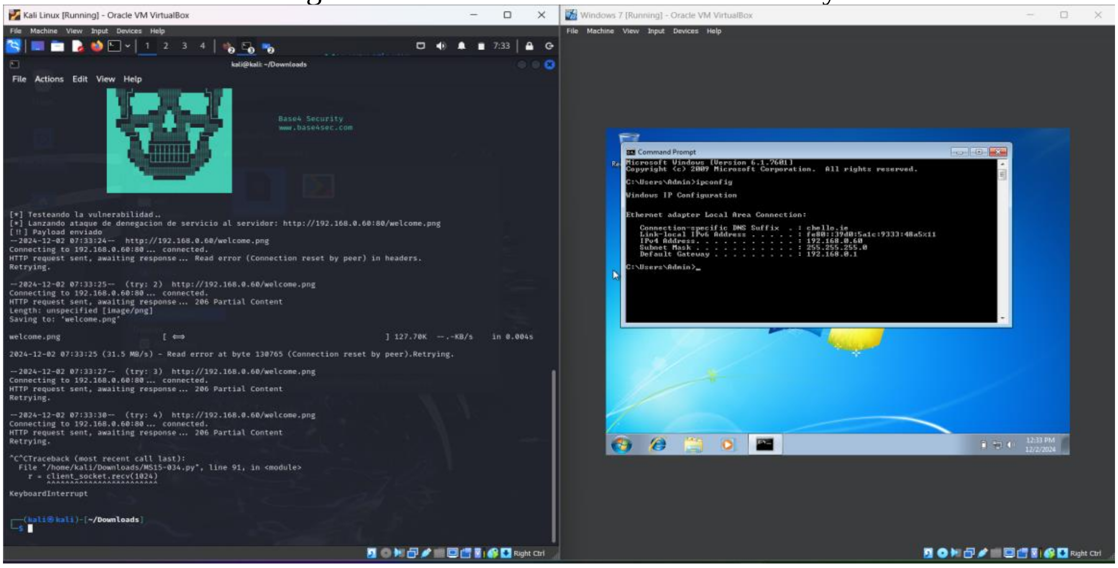
Help with VPN

Setting up a VPN

Get help

Give feedback

Figure 3: VPN User connected successfully

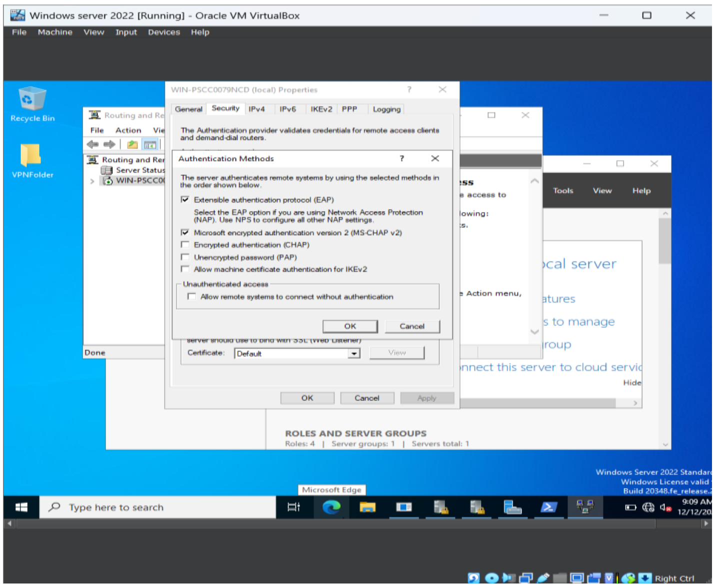


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help
Windows 7 [Running] - Oracle VM VirtualBox
Command Prompt

```
Base4 Security
www.base4sec.com

[*] Testeando la vulnerabilidad..
[*] Lanzando ataque de denegacion de servicio al servidor: http://192.168.0.60:80/welcome.png
[!!] Payload enviado
--2024-12-02 07:33:24--  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response... Read error (Connection reset by peer) in headers.
Retrying.

--2024-12-02 07:33:25--  (try: 2)  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: unspecified [image/png]
Saving to: 'welcome.png'

welcome.png                 [ <=>                                   ] 127.70K  --.-KB/s    in 0.004s

2024-12-02 07:33:25 (31.5 MB/s) - Read error at byte 130765 (Connection reset by peer).Retrying.

--2024-12-02 07:33:27--  (try: 3)  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Retrying.

--2024-12-02 07:33:30--  (try: 4)  http://192.168.0.60/welcome.png
Connecting to 192.168.0.60:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Retrying.

^C^CTraceback (most recent call last):
  File "/home/kali/Downloads/MS15-034.py", line 91, in <module>
    r = client_socket.recv(1024)
        ^^^^^^^^^^^^^^^^^^^^^^^^
KeyboardInterrupt

┌──(kali㉿kali)-[~/Downloads]
└─$
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : chello.ie
   Link-local IPv6 Address . . . . . : fe80::39d0:5a1c:9333:48a5%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.60
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\Admin>_
```

Figure 4: The patch was successful and the system did not crash after the exploit



WIN-PSCC0079NCD (local) Properties

General | Security | IPv4 | IPv6 | IKEv2 | PPP | Logging

The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication Methods

The server authenticates remote systems by using the selected methods in the order shown below.

☑ Extensible authentication protocol (EAP)

Select the EAP option if you are using Network Access Protection (NAP). Use NPS to configure all other NAP settings.

☑ Microsoft encrypted authentication version 2 (MS-CHAP v2)

□ Encrypted authentication (CHAP)

□ Unencrypted password (PAP)

□ Allow machine certificate authentication for IKEv2

Unauthenticated access

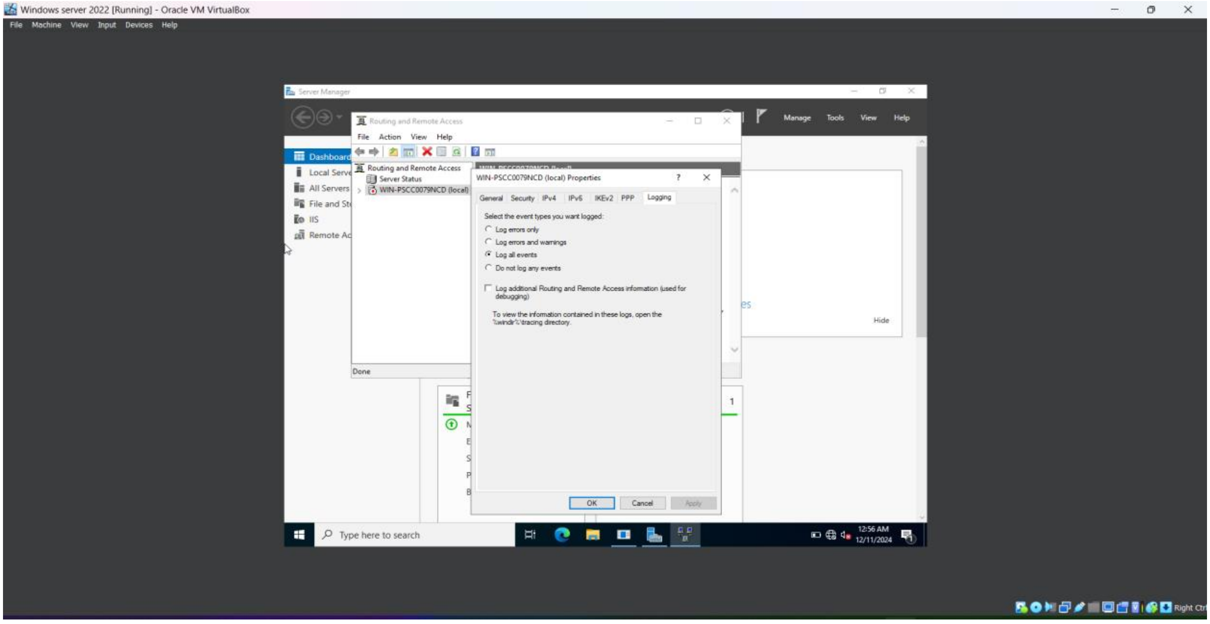
□ Allow remote systems to connect without authentication

OK | Cancel

Certificate: Default

View | OK | Cancel | Apply

Figure 5: Authentication configuration



WIN-PSCC0079NCD (local) Properties

General | Security | IPv4 | IPv6 | IKEv2 | PPP | Logging

Select the event types you want logged:

○ Log errors only

○ Log errors and warnings

● Log all events

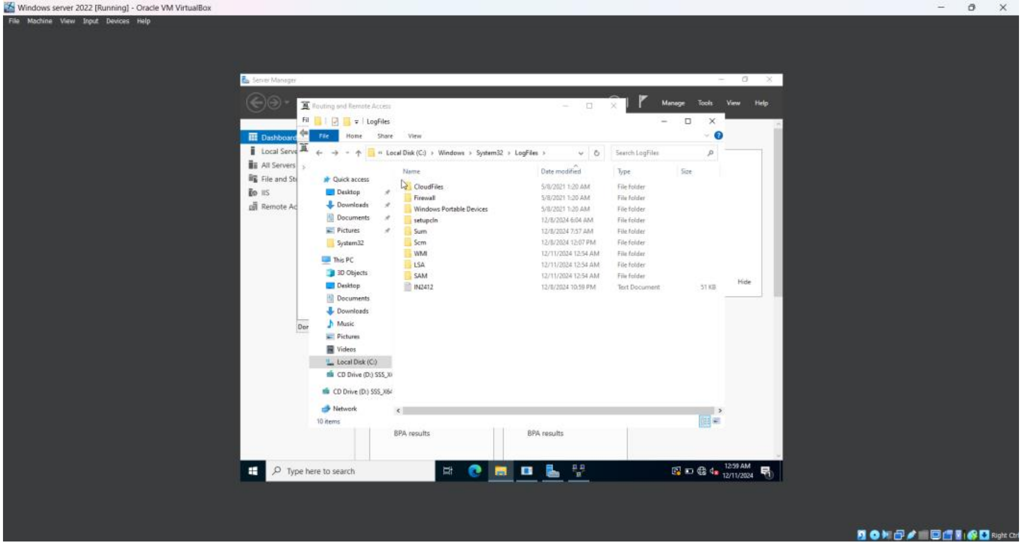
○ Do not log any events

□ Log additional Routing and Remote Access information (used for debugging)

To view the information contained in these logs, open the %windir%\tracing directory.

OK | Cancel | Apply

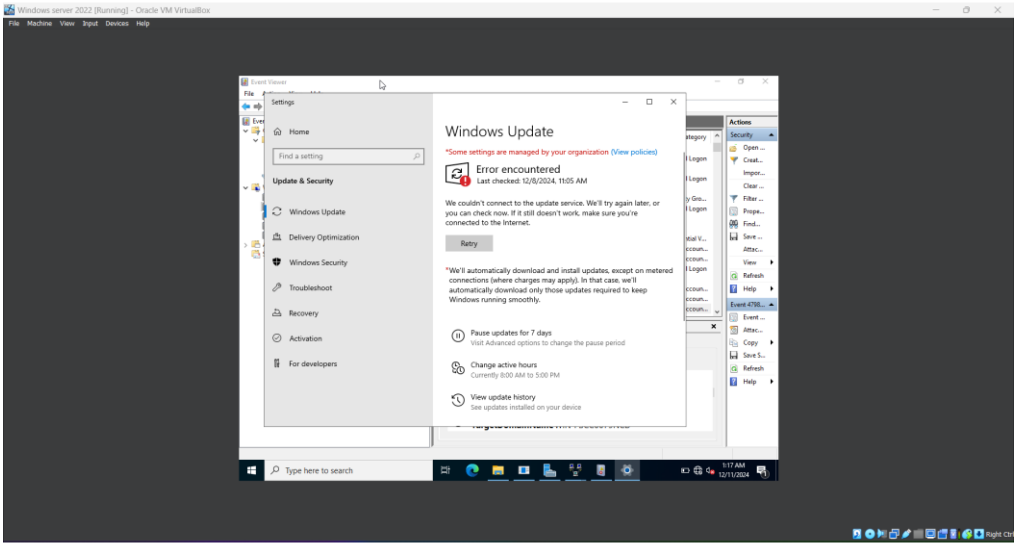
Figure 6: Logging configured on VPN server



Local Disk (C:) › Windows › System32 › LogFiles ›

Name	Date modified	Type	Size
CloudFiles	5/8/2021 1:20 AM	File folder	
Firewall	5/8/2021 1:20 AM	File folder	
Windows Portable Devices	5/8/2021 1:20 AM	File folder	
setupcln	12/8/2024 6:04 AM	File folder	
Sum	12/8/2024 7:57 AM	File folder	
Scm	12/8/2024 12:07 PM	File folder	
WMI	12/11/2024 12:54 AM	File folder	
LSA	12/11/2024 12:54 AM	File folder	
SAM	12/11/2024 12:54 AM	File folder	
IN2412	12/8/2024 10:59 PM	Text Document	51 KB

Figure 7: Locating logfile on the server



Windows Update

*Some settings are managed by your organization (View policies)

Error encountered
Last checked: 12/8/2024, 11:05 AM

We couldn't connect to the update service. We'll try again later, or you can check now. If it still doesn't work, make sure you're connected to the Internet.

Retry

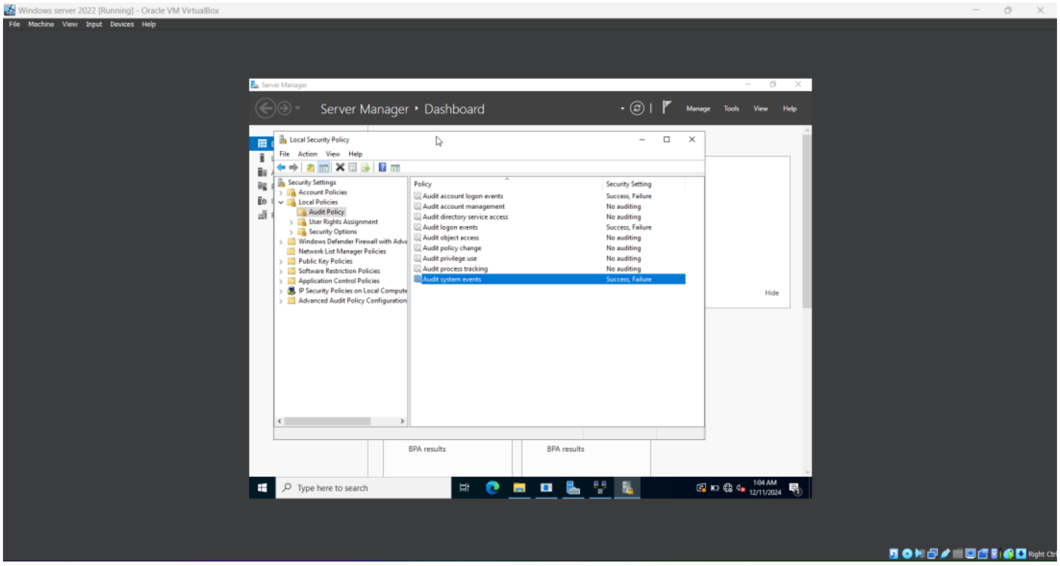
*We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

View update history
See updates installed on your device

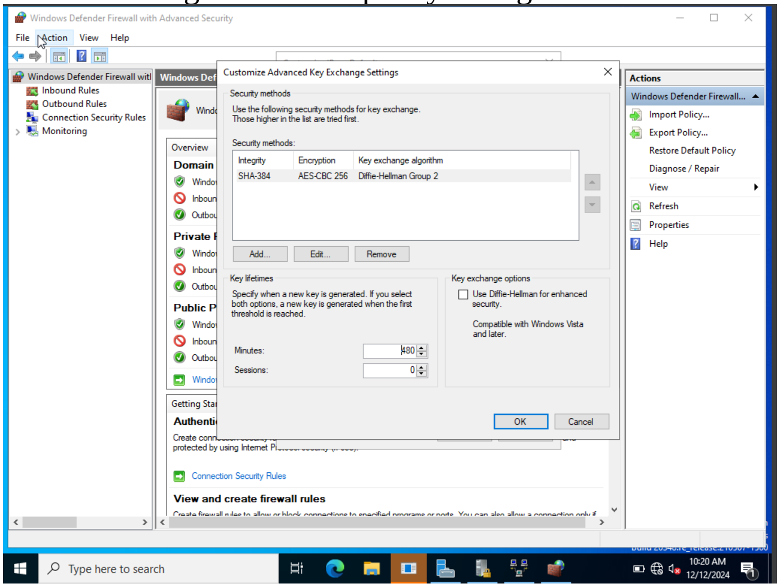
Figure 8: Configured server for auto download of the updates



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

Windows server 2022 [Running] - Oracle VM VirtualBox
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Local Security Policy
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
BPA results
Type here to search

Figure 9: Audit policy configuration



Customize Advanced Key Exchange Settings

Security methods

Use the following security methods for key exchange.
Those higher in the list are tried first.

Security methods:

Integrity	Encryption	Key exchange algorithm
SHA-384	AES-CBC 256	Diffie-Hellman Group 2

Add... Edit... Remove

Key lifetimes

Specify when a new key is generated. If you select both options, a new key is generated when the first threshold is reached.

Minutes: 480

Sessions: 0

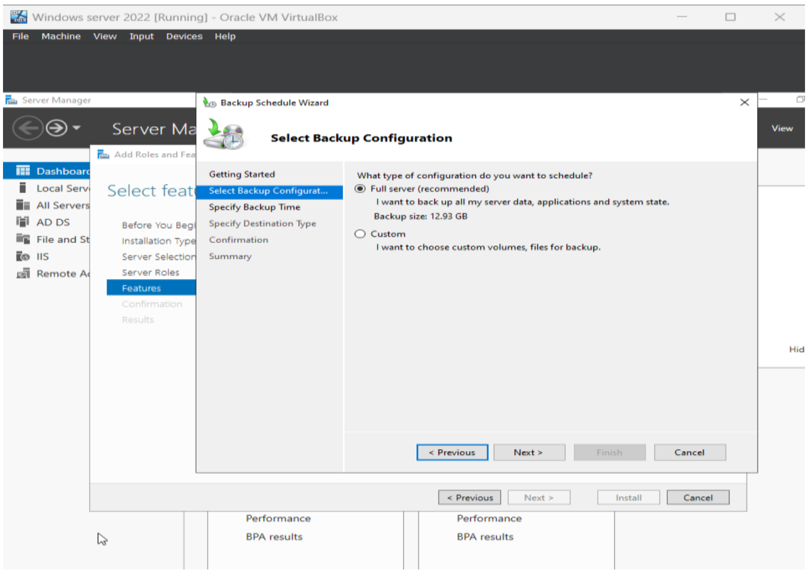
Key exchange options

□ Use Diffie-Hellman for enhanced security.

Compatible with Windows Vista and later.

OK Cancel

Figure 10: Configured AES 256



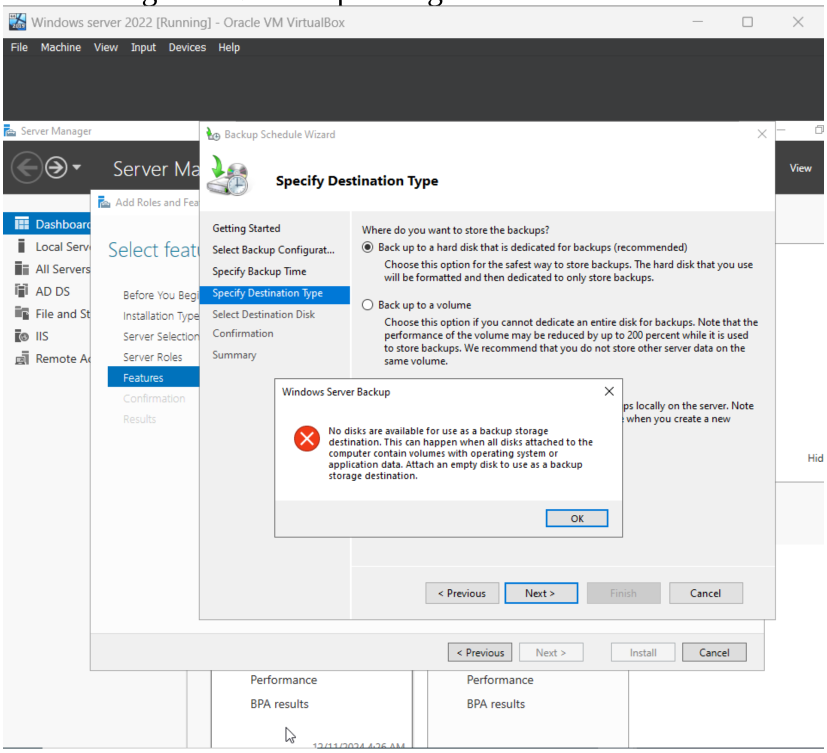
Select Backup Configuration

What type of configuration do you want to schedule?

● Full server (recommended)
I want to back up all my server data, applications and system state.
Backup size: 12.93 GB

○ Custom
I want to choose custom volumes, files for backup.

Figure 11: Backup configuration on full server



Specify Destination Type

Where do you want to store the backups?

● Back up to a hard disk that is dedicated for backups (recommended)
Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

○ Back up to a volume
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

Windows Server Backup

No disks are available for use as a backup storage destination. This can happen when all disks attached to the computer contain volumes with operating system or application data. Attach an empty disk to use as a backup storage destination.

Figure 12: Non availability of remote location