National College of Ireland

# Configuration Manual

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 |
| **Lecturer:** | 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:** | 1140 **Page Count:** 05 |

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): | |

# Configuration Manual

Vikas Rajak
Student ID: 23206071

The configuration manual discusses the detailed implementation steps / navigations to for the procedures carried out in the research.

# 1 Configuration and detailed steps to exploit the vulnerable IIS 7.0 Server on Windows 7

Set up a attack environment in Oracle virtual box

Simulate the Attack:

1. In Oracle Virtual box install kali Linux as attacking device and install vulnerable windows 7 as target device
2. Install IIS 7.0 server on windows 7
3. Establish a connection between and attacking and target device by bridged network.
4. Check the ping status, if successful go ahead with the process
5. Download the malicious python file on kali Linux
6. Use the command mentioned in the report to initiate the attack
7. After successful attack the server should crash

Patch the Vulnerability:

1. In IIS manager, navigate to output caching
2. Uncheck the kernel caching to mitigate the vulnerability.
3. Save the configuration.

Perform the exploit again to evaluate the patch applied:

1. Using the same command initiate the attack
2. If the server did not crash the patch was applied successfully

Your first section. Change the header and label to something appropriate.

# 2 Set up a VPN Server

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.
3. The windows server 2022 VM uses bridged network to establish the connectivity.
4. After configuring network connection, install all the following packages and modules needed to setup a VPN server. (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. Under tools select Routing and Remote Access > custom configuration > 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.
   d. 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. Click on “Apply”. And restart the server to save all the configuration changes.

7. Configure Firewall Rules
   a. 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 that will be used by the client to connect to VPN server
   a. Create a user, provide username and password which will be further used to connect to VPN server.
   b. Under the user’s property allow access for network access permission in dial-in tab
9. VPN client configuration

   9.1 Configure firewall rules:
      a. 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

# 3 Secure the VPN Server

1. Authentication
   a. In server manager > Tools > Routing and remote access
   b. Right click on the server name > Properties
   c. Under security tab
   d. Open Authentication Method and select MS-CHAP v2 and EAP authentication
   e. Set a strong and complex pre shared key which will be used by the client to authenticate into the server.

2. Logging and monitoring

a. In server manager > Tools > Routing and remote access
b. Right click on the server name > Properties
c. Open logging windows > Enable log all events

3. Patching and updates
   a. Under the windows update settings enable auto download updates

4. Audit and compliance
   a. Open Local Security Policy of the server
   b. Under local policies open Audit policy
   c. Enable following policies by right clicking on it and selecting enable
      Audit account logon events, Audit logon events, Audit system events

5. Secure encryption
   It is recommended to configure and use AES 256 encryption algorithm
   a. On windows defender firewall, right click to get properties
   b. Properties > IPSec > IPSec default customize >
      Key change to advance
      Authentication to advanced
   c. Key change > Customize > Add
      Integrity algorithm- SHA 256
      Encryption algorithm- AES 256
   d. Click OK

6. Backup servers.
   a. Open Server manager
   b. Select roles and features, check windows backup service and install the backup service. This will reflect in the windows system
   c. Open windows server > Specify backup time once a day or more than once a day (as needed)
   d. Select a destination to store backed up data
   e. Idle recommendation is to select backup to hard disk that is dedicated to backup which was not possible in the research due to environment limitation