

**PROJECT**

**Network Firewall Simulation Using Netcat for Data Transmission Security**

Written by**:**

**Harits Rahman Hakim (2421010067)**

**Omar Justice Prasetyo (2421010180)**

Lecturer:

**Mr. Ivan Firdaus, S.T. & Tri Agus Riyadi, kom., M.T.**

Class:

**3CS1**

**CEP CCIT**

**FAKULTAS TEKNIK UNIVERSITAS INDONESIA**

**2025**

**PROJECT ON**

*Network Firewall Simulation Using Netcat for Data Transmission Security*

**DEVELOPED BY**

Harits Rahman Hakim

Omar Justice Prasetyo



**Network Firewall Simulation Using Netcat for Data Transmission Security**

Batch Code : 3CS1

Start Date : October 10, 2025

End Date : October 17, 2025

Name of Faculty : Ivan Firdaus, S.T. & Tri Agus Riyadi, kom., M.T.

Names of Developer :

1. Harits Rahman Hakim
2. Omar Justice Prasetyo

Date of Submission : 17 October, 2025



**CERTIFICATE**

This document serves as verification for the report " Network Firewall Simulation Using Netcat for Data Transmission Security" written by Harits Rahman Hakim and Omar Justice Prasetyo. The goal of this project is to complete the CCIT-FTUI course requirement.

Coordinator:

Mr. Ivan Firdaus, S.T. & Tri Agus Riyadi, kom., M.T.

**ACKNOWLEDGEMENT**

Deepest gratitude is extended to everyone who contributed to the successful completion of this project on **"Network Firewall Simulation Using Netcat for Data Transmission Security"**

Special appreciation goes to the mentors whose invaluable guidance, insightful feedback, and continuous support shaped the direction and quality of this research. Their expertise and encouragement played a crucial role in refining each aspect of the project.

Sincere thanks are also given to the dedicated group members whose collaboration, technical knowledge, and problem-solving skills greatly enhanced the development of an efficient and scalable network topology. The countless discussions, coding sessions and shared expertise made a significant impact on overcoming challenges throughout the process.

Recognition is also due to the institutions and organization that provide valuable case studies and practical insights, which enriched the real-world applicability of this systems. Their cooperation and contributions ensured that the project remained relevant, efficient, and scalable in addressing attendance tracking and shift scheduling needs.

Appreciation is extended to all individuals, peers, and institutions whose direct or indirect contributions made this research possible. Their support and encouragement created an environment that fostered innovation and excellence.

Depok, 17 September 2025

Authors

**BACKGROUND**

In today’s rapidly evolving information technology landscape, network security has become a crucial aspect to ensure the confidentiality, integrity, and availability of data within a system. Increasingly sophisticated cyber threats such as unauthorized access, brute-force attacks, and exploitation of open ports require the implementation of effective protection mechanisms. One of the key mechanisms is the firewall.

A firewall acts as a network traffic controller that determines whether a connection is allowed or denied based on predefined rules. This project simulates the implementation of a firewall using iptables in a Linux environment to demonstrate how it can prevent unauthorized access and secure local networks.

Furthermore, the project examines the behavioral differences between DROP and REJECT rules and how each affects the availability aspect of the system. By incorporating data transfer simulation using Netcat (nc), this project also links the practical implementation of a firewall with the fundamental principles of the CIA Triad Confidentiality, Integrity, and Availability in the context of network security.

**SYSTEM ANALYSIS**

**System Summary**

1. System Description

This project simulates network security using an iptables-based firewall on a Linux operating system. The main goal is to understand how a firewall prevents unauthorized access and secures network traffic between two entities: client and server.

The simulation is performed using two terminals that represent two separate computers:

* The first terminal acts as a server, listening on a specific port using nc -lvp [port].
* The second terminal acts as a client, connecting to the server using nc [IP] [port].

The firewall is configured using iptables to control traffic based on protocols, source IPs, and destination ports, applying actions such as DROP, ACCEPT, or REJECT.

2. System Components

1. Iptables: to create and manage firewall rules.
2. Netcat (nc): to simulate data communication between client and server.
3. Linux Terminal (CLI): serves as the main configuration and testing interface.
4. Log or Output Files: store results of the simulations for analysis.

3. System Flow

Initialization: install and prepare iptables and netcat.

Connection Phase: client attempts to connect to the server on a specific port.

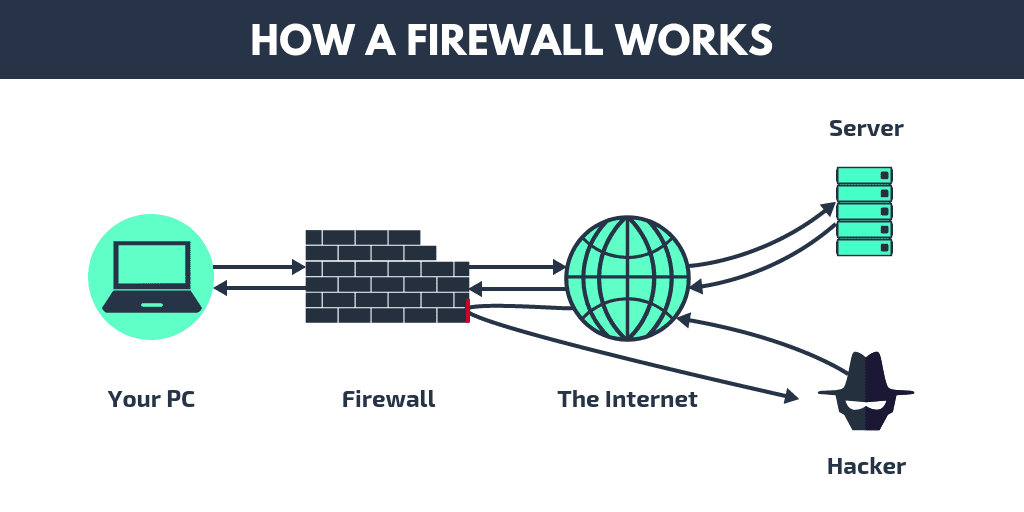
Access Restriction: firewall rules are created to block or allow connections (e.g., DROP on port 8080).

Confidentiality: prevents unauthorized access to data.

Integrity: ensures transmitted data remains unaltered during transfer.

Availability: measures the impact of firewall rules on system accessibility.

**Firewall**

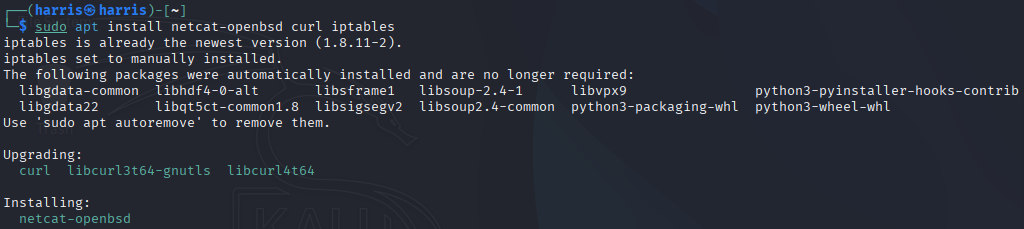


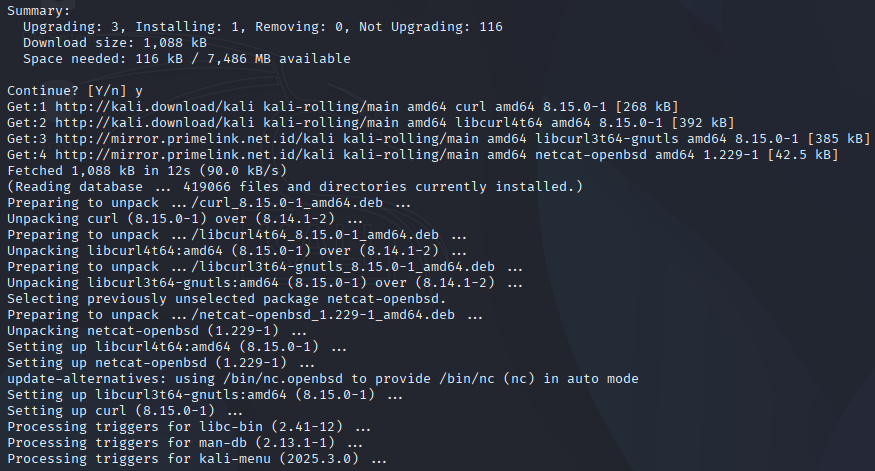
The image above illustrates how a firewall works as a network security system that protects a computer from external threats. The firewall acts as a barrier between the computer and the internet by allowing safe network traffic to reach the server and blocking harmful or unauthorized connections coming from hackers or unknown sources.

In this project, iptables is used as the firewall to manage network access based on specific ports, such as port 8080. Meanwhile, Netcat is used to simulate the connection between a client and a server. When the firewall successfully blocks unauthorized connections, it indicates that the network security system is functioning properly.

**IMPLEMENTATION**

Firewall and Supporting Tools Installation:



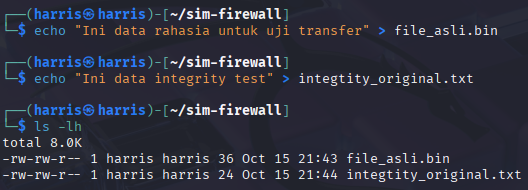


Create a working folder:



**IMPLEMENTATION**

Prepare test files:



Simple file transfer:

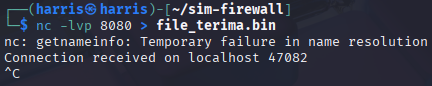
1. Terminal A (listener/receiver) run:



1. Terminal B (sender) run:

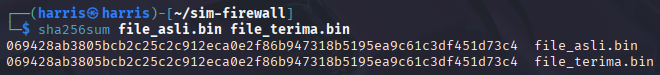


Once completed, Terminal A will appear like this



1. Verification (Integrity):

code: sha256sum file\_asli.bin file\_terima.bin



**IMPLEMENTATION**

Integrity test (tampering):

1. Repeat the transfer as above for integrity\_original.txt:

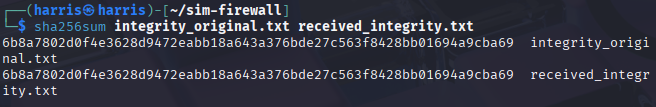
Terminal A:



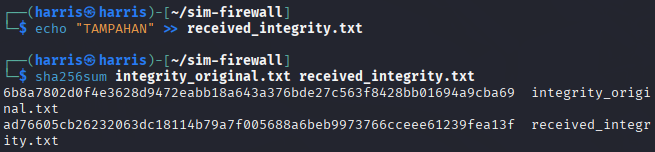
Terminal B:



1. Check checksum: (Must be the same)



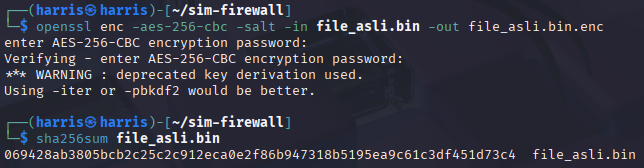
1. Tamper simulation: edit the recipient file in Terminal A before verification:



Compare with original: different, integrity detected broken.

Confidentiality (encrypt before transfer):

1. Encrypt (sender, Terminal B):



**IMPLEMENTATION**

2. Receive (receiver, Terminal A)



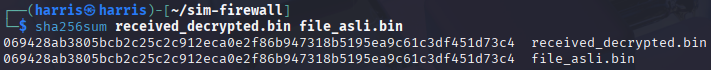
1. Send (sender Terminal B):



1. Decrypt (Terminal A receiver):



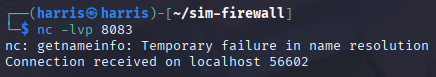
enter the same password.



Availability (firewall impact test):

1. Baseline test listener on & client connect:

Terminal A:



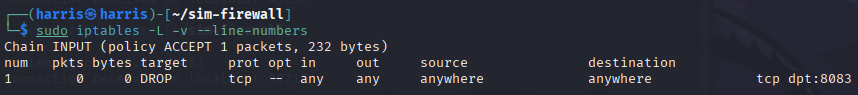
Terminal B:



1. Add a DROP (silent drop) rule:

Terminal B: block port 8083 for all interfaces



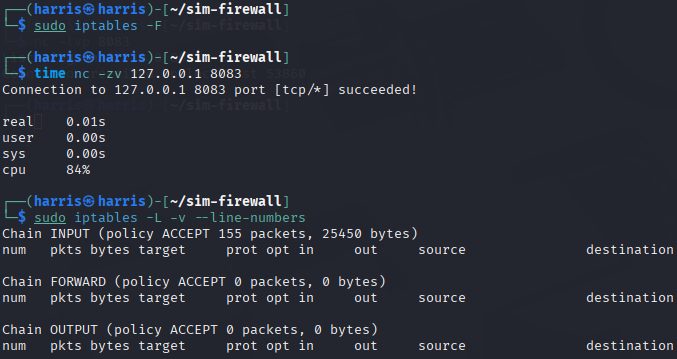


**IMPLEMENTATION**

Test (client):



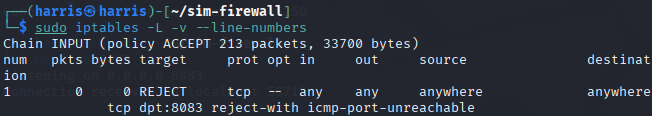
Delete all temporary rules and test again: sudo iptables -F



1. Switch to REJECT for comparison:

Add REJECT:

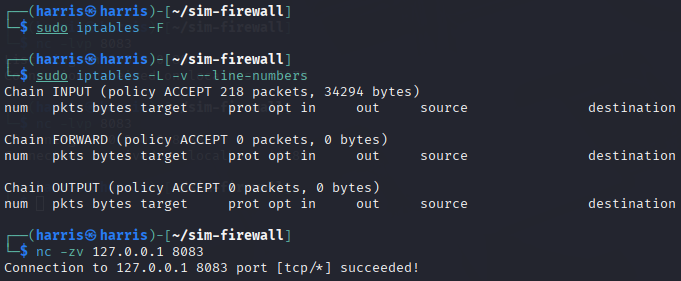




Test (client):



Delete all temporary rules and test again: sudo iptables -F



**IMPLEMENTATION**

**REQUIREMENTS**

**Hardware:**

1. Latitude 5300

**Operating System:**

1. Windows 11

**Software:**

1. VirtualBox
2. Kali Linux

**PROJECT AND FILE DETAILS**

|  |  |  |
| --- | --- | --- |
| **No.** | **Section** | **Remarks** |
| **1.** | System Analysis | Omar Justice Prasetyo |
| **5.** | Simulation | Harits Rahman Hakim |
| **6.** | Document | Harits Rahman Hakim |
| **7.** | Presentation Slide | Omar Justice Prasetyo |

|  |  |  |
| --- | --- | --- |
| **No.** | **Section** | **Remarks** |
| **1.** | Group 2 – Network Firewall Simulation Using Netcat for Data Transmission | Paper File |
| **2.** | Group 2 – Slide PPT | Presentation File |