

**MENINGKATKAN KEAMANAN SERVER DENGAN TEKNIK  
HARDENING SERVER MENGGUNAKAN METODE NIST  
PADA PTPN VII PAGARALAM**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**Yoga Pangestu**

**18.83.0146**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SAMIKOMYOGYAKARTA  
YOGYAKARTA  
2023**

**MENINGKATKAN KEAMANAN SERVER DENGAN TEKNIK  
HARDENING SERVER MENGGUNAKAN METODE NIST  
PADA PTPN VII PAGARALAM**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**Yoga Pangestu**

**18.83.0146**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**MENINGKATKAN KEAMANAN SERVER DENGAN TEKNIK  
HARDENING SERVER MENGGUNAKAN METODE NIST  
PADA PTPN VII PAGARALAM**

yang disusun dan diajukan oleh

**Yoga Pangestu**

**18.83.0146**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 15 Agustus 2023

**Dosen Pembimbing,**



**Joko Dwi Santoso, M.Kom**

**NIK. 190302181**

# HALAMAN PENGESAHAN

SKRIPSI

## MENINGKATKAN KEAMANAN SERVER DENGAN TEKNIK HARDENING SERVER MENGGUNAKAN METODE NIST PADA PTPN VII PAGARALAM

yang disusun dan diajukan oleh

**Yoga Pangestu**

**18.83.0146**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 15 Agustus 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Joko Dwi Santoso, M.Kom**  
NIK. 190302181

**Muhammad Kopravi, S.Kom., M.Eng**  
NIK. 190302454

**Jeki Kuswanto, M.Kom**  
NIK. 190302456



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 15 Agustus 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom.**  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Yoga Pangestu  
NIM : 18.83.0146

Menyatakan bahwa Skripsi dengan judul berikut:

### **MENINGKATKAN KEAMANAN SERVER DENGAN TEKNIK HARDENING SERVER MENGGUNAKAN METODE NIST PADA PTPN VII PAGARALAM**

Dosen Pembimbing : Joko Dwi Santoso, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 15 Agustus 2023

Yang Menyatakan,

  
  
Yoga Pangestu

## KATA PENGANTAR

Puji dan syukur peneliti panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, rahmat, nikmat, kekuatan dan kesehatan sehingga peneliti dapat menyelesaikan skripsi dengan judul “Meningkatkan Keamanan Server Dengan Teknik Hardening Server dengan Metode NIST pada PTPN VII Pagaram” sebagai diinginkan peneliti. Skripsi ini ditulis sebagai jawaban atas salah satu syarat kelulusan program sarjana Program Studi Teknologi Informasi Universitas AMIKOM Yogyakarta. Selain itu, ini juga merupakan bukti bahwa Mahasiswa telah menyelesaikan studi sarjana mereka dan memiliki gelar sarjana dalam bidang ilmu komputer.

Akhir kata peneliti tidak lupa mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta
2. Bapak Hanif Al Fatta, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Joko Dwi Santoso, M.Kom selaku Dosen pembimbing yang telah membimbing penulis dalam menyelesaikan skripsi ini.
4. Bapak Muahammad Kopravi, S.Kom, M.Eng dan Bapak Ibnu Jeki Kuswanto, M.Kom. selaku Dosen Penguji yang telah menguji skripsi peneliti dan memberikan saran-saran yang membuat skripsi ini lebih baik.
5. Seluruh Dosen dan Karyawan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta khususnya program studi Teknik komputer yang telah membimbing dan menularkan ilmu-ilmunya kepada mahasiswanya.
6. Terimakasih kepada Bapak dan Ibu saya yang telah mendoakan dan memberi semua dukungannya agar dilancarkan pembelajarannya hingga akhir.
7. Terimakasih kepada teman-teman UWAW Corporate yang banyak membantu semangat dan membantu dalam pengerjaan tugas akhir ini.

Yogyakarta, 15 Agustus 2023

Yoga Pangestu

## DAFTAR ISI

HALAMAN JUDUL .....	1
HALAMAN PERSETUJUAN.....	2
HALAMAN PENGESAHAN.....	3
HALAMAN PERNYATAAN KEASLIAN SRIPSI.....	4
KATA PENGANTAR.....	5
DAFTAR ISI.....	6
DAFTAR TABEL.....	8
DAFTAR GAMBAR.....	9
DAFTAR LAMPIRAN.....	10
INTISARI.....	11
ABSTRACT.....	12
BAB I PENDAHULUAN.....	13
1.1 Latar Belakang.....	13
1.2 Rumusan masalah.....	14
1.3 Batasan Masalah.....	14
1.4 Tujuan Penelitian.....	14
1.6 Sistematika Penulisan.....	15
BAB II TINJAUAN PUSTAKA.....	16
2.1 Studi Literatur.....	16
2.2 Dasar Teori.....	8
2.2.1 Server.....	8
2.2.2 Penetration Testing.....	8
2.2.3 NIST.....	8
2.2.4 Virtual Box.....	9
2.2.5 Webmin.....	9
2.2.6 Honeypot.....	9
2.2.7 Metasploit.....	9
2.2.8 Nmap.....	10
2.2.9 Brute Force.....	10

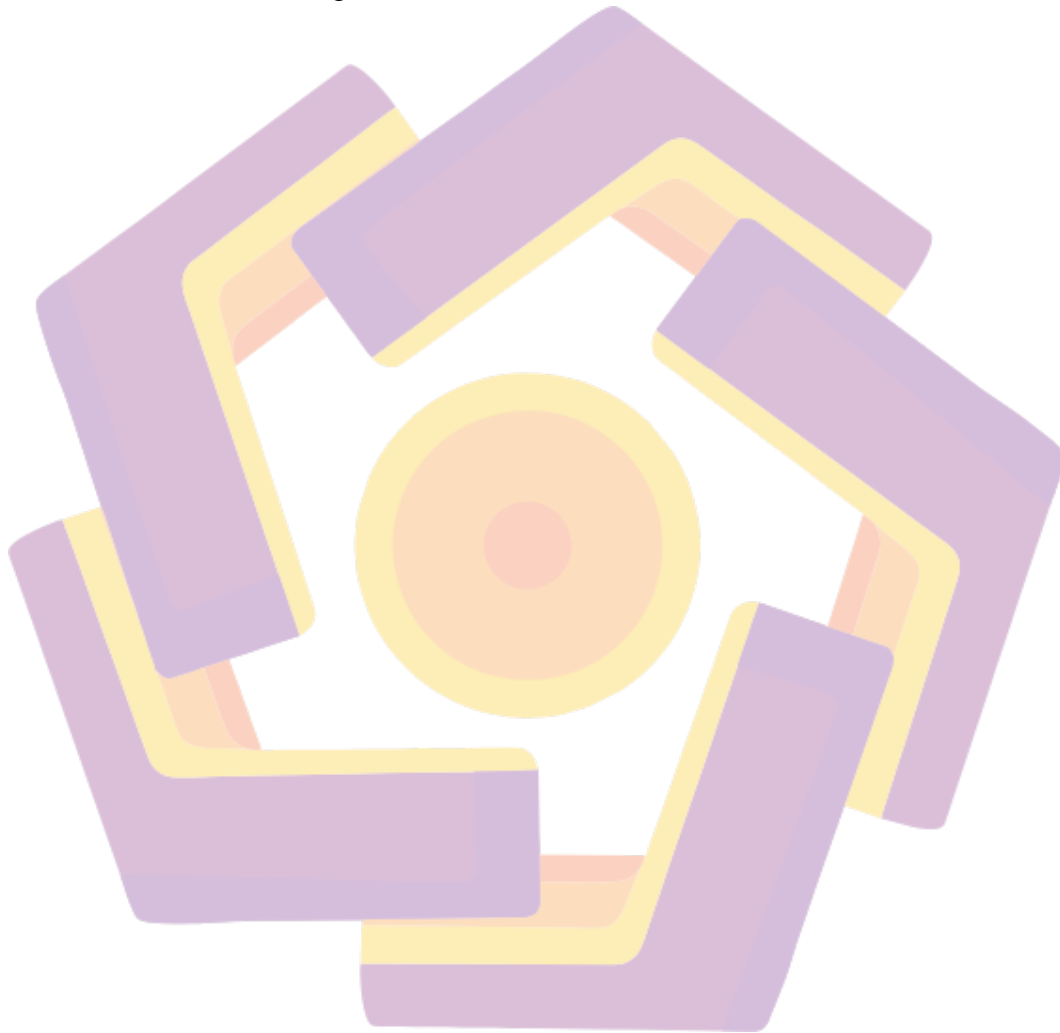


BAB III METODE PENELITIAN.....	11
3.1 Metodologi Objek Penelitian .....	11
3.2 Alur Penelitian .....	11
3.3 Pra Eksperimen.....	12
3.3.1 Alat dan Bahan Penelitian .....	12
3.3.2 Desain.....	13
3.4 Eksperimen .....	13
3.4.1 Testing .....	13
3.4.2 Skenario Testing.....	13
3.4.3 Pra Testing .....	14
3.4.4 Pentesting.....	14
3.4.5 Paska Testing .....	14
3.5 Paska Eksperimen.....	14
4.1 Desain.....	15
4.1.1 Implementasi System.....	15
4.2 Implementasi NIST.....	15
4.2.1 Update Repository .....	16
4.2.2 Install Ufw .....	17
4.2.3 Port Knocking .....	17
4.2.4 Honeypot.....	18
4.2.5 Instalasi webmin.....	21
4.3 Hasil Implementasi .....	25
4.4 Pengujian tool NIST SP 800-123.....	26
4.7 Paska Testing .....	30
4.8 Analisa data.....	30
BAB V PENUTUP.....	31
5.1 Kesimpulan .....	31
5.2 Saran.....	31
REFERENSI.....	32
DAFTAR LAMPIRAN.....	34



## DAFTAR TABEL

Tabel 2. 1 Daftar Kajian Pustaka .....	6
Tabel 3. 1 Alat dan Bahan Penelitian .....	12
Tabel 4. 1 Hasil Implementasi NIST.....	25
Tabel 4. 2 List Malfungsi.....	30

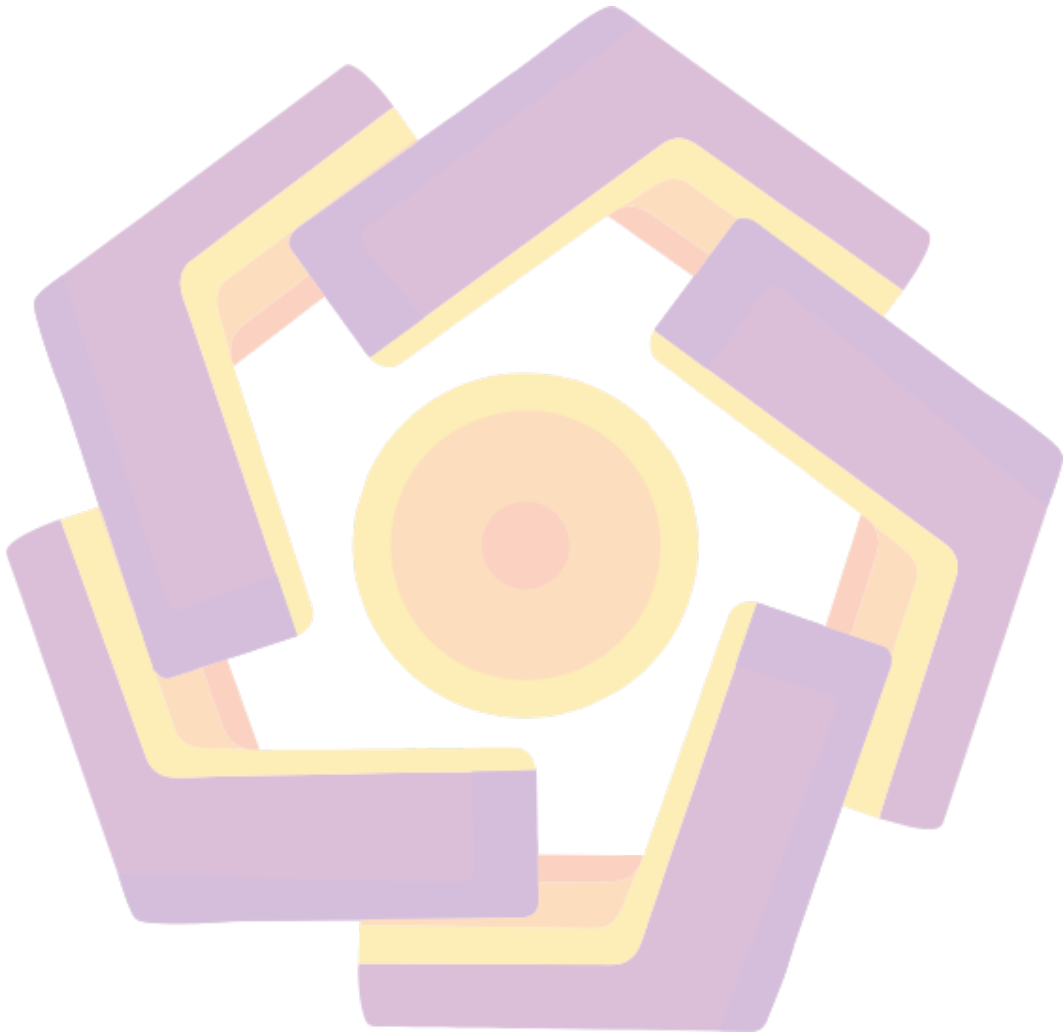


## DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian .....	11
Gambar 4. 1 Source Code Update Repository .....	16
Gambar 4. 2 Upgrade Semua Package Ke Versi Terbaru.....	16
Gambar 4. 3 konfigurasi penginstallan UFW .....	17
Gambar 4. 4 Menutup Port 21 .....	17
Gambar 4. 5 Mengupdate system .....	18
Gambar 4. 6 Install pentbox .....	18
Gambar 4. 7 Ekstrak file Pentbox Honeypot.....	19
Gambar 4. 8 Menjalankan Pentbox Honeypot.....	19
Gambar 4. 9 Tampilan awal dari honeypot .....	19
Gambar 4. 10 Tampilan pada pilihan Fast Auto Configuration .....	20
Gambar 4. 11 Tampilan pada Manual Configuration.....	20
Gambar 4. 12 Menambahkan Link Download Di Repository.....	21
Gambar 4. 13 Menambahkan Webmin PGP key .....	21
Gambar 4. 14 Menambahkan Webmin PGP key .....	22
Gambar 4. 15 Mengupdate Server .....	22
Gambar 4. 16 Install webmin .....	23
Gambar 4. 17 Tampilan Login Webmi .....	23
Gambar 4. 18 Tampilan home webmin.....	24
Gambar 4. 19 Melihat IP Server.....	26
Gambar 4. 20 Melihat Port yang terbuka .....	26
Gambar 4. 21 Mencari Koneksi Ftp.....	27
Gambar 4. 22 Masuk ke modul Ftp .....	27
Gambar 4. 23 File yang akan di transfer .....	27
Gambar 4. 24 Pengaturan User dan Password Login.....	28
Gambar 4. 25 Menghentikan Percobaan Login Jika Sudah Cocok .....	28
Gambar 4. 26 Pengaturan RHOST .....	28
Gambar 4. 27 exploit untuk mendapatkan user dan password.....	29
Gambar 4. 28 Report sistem Honeypot.....	29

## **DAFTAR LAMPIRAN**

Lampiran 1. Dokumentasi Penelitian  
Lampiran 2. Surat Balasan Penelitian



## INTISARI

Sistem keamanan jaringan menjadi hal yang sangat penting dalam menjaga sebuah jaringan, serangan yang bisa mengganggu bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat merugikan. Untuk mengatasi hal tersebut perlu dibangun sistem keamanan server untuk mencegah serangan yang dapat menyebabkan kerugian, seperti kehilangan data. Dalam proses peningkatan keamanan di suatu server tentunya banyak metode metode yang dapat diikuti, dengan tingkat keamanan yang lebih terjamin. Sehingga pada kesempatan ini penulis ingin menulis penelitian “Meningkatkan Keamanan server dengan menggunakan metode NIST” yang bertujuan untuk meningkatkan keamanan pada suatu server dengan menggunakan metode dari modul agar mengurangi tingkat kerawanan di dalamnya dari serangan-serangan peretas atau yang biasa disebut hacker yang tentunya dapat merusak server, database, aplikasi, jaringan, dan bahkan dapat merusak OS (*operating system*). Adapun penerapan ini dilakukan dengan konfigurasi sistem operasi kali linux dengan tool bawaan atau built in dari sistem. Tujuan dari penelitian ini di harapkannya dapat meningkatkan aspek keamanan pada server dengan menggunakan metode NIST. Pengujian ini dilakukan dengan uji coba via virtual serangan, dengan metode brute force untuk proses uji coba dari server yang sudah di buat untuk mencoba masuk ke dalam server, dan menambah aplikasi webmin untuk membantu monitoring server, adapun metode yang penulis gunakan adalah dengan metode black box. Dengan berjalannya hal tersebut maka akan di dapat hasil uji coba dari server.

**Kata kunci:** Keamanan Server, Linux, Brute Force, Webmin

## ABSTRACT

*Network security systems are very important in protecting a network, attacks that can interfere with and even damage the connection system between connected devices will be very detrimental. To overcome this, it is necessary to build a server security system to prevent attacks which can cause losses, such as data loss. In the process of increasing security on a server, there are of course many methods that can be followed, with a more guaranteed level of security. So that on this occasion the author would like to write a research "Improving server security using the NIST method" which aims to increase security on a server using the module method in order to reduce the level of vulnerability in it from hacker attacks or what is commonly called hackers which of course can damage servers, databases, applications, networks, and can even damage the OS (operating system). This application is carried out by configuring the Kali Linux operating system with the default tools or built in from the system. The purpose of this research is expected to be able to improve security aspects on servers using the NIST method. This test is carried out by testing via virtual attacks, with the brute force method for the trial process from the server that has been created to try to enter the server, and adding the webmin application to help monitor servers, while the method the author uses is the black box method. With this running, the test results will be obtained from the server.*

**Keyword:** Scurity Server, Linux, Brute Force, Webmin