

**PERBANDINGAN HARDENING SERVER MENGGUNAKAN
METODE NIST DAN EC COUNCIL**

SKRIPSI



Disusun oleh:

Ali Akbar Saragih

18.83.0182

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

HALAMAN PERSETUJUAN

SKRIPSI

PERBANDINGAN HARDENING SERVER MENGGUNAKAN METODE NIST DAN EC COUNCIL

yang dipersiapkan dan disusun oleh

Ali Akbar Saragih

18.83.0182

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Agustus 2022

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T

NIK. 190302452

**HALAMAN PENGESAHAN
SKRIPSI**

**PERBANDINGAN HARDENING SERVER MENGGUNAKAN METODE
NIST DAN EC COUNCIL**

yang dipersiapkan dan disusun oleh

Ali Akbar Saragih

18.83.0182

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 September 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Wahid Miftahul Ashari, S.kom., M.T

NIK. 190302452

Banu Santoso, S.T., M.Eng

NIK. 190302327

Joko Dwi Santoso, M.Kom

NIK. 190302181

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 September 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif AlFatta, S.Kom., M.Kom

NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ali Akbar Saragih

NIM : 18.83.0182

Menyatakan bahwa Skripsi dengan judul berikut:

Perbandingan Hardening Server Menggunakan Metode NIST Dan EC Council

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T

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 tidak benaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya dengan norma yang berlaku di perguruan tinggi.

Yogyakarta, 21 September 2022

Yang Menyatakan,



Ali Akbar Saragih

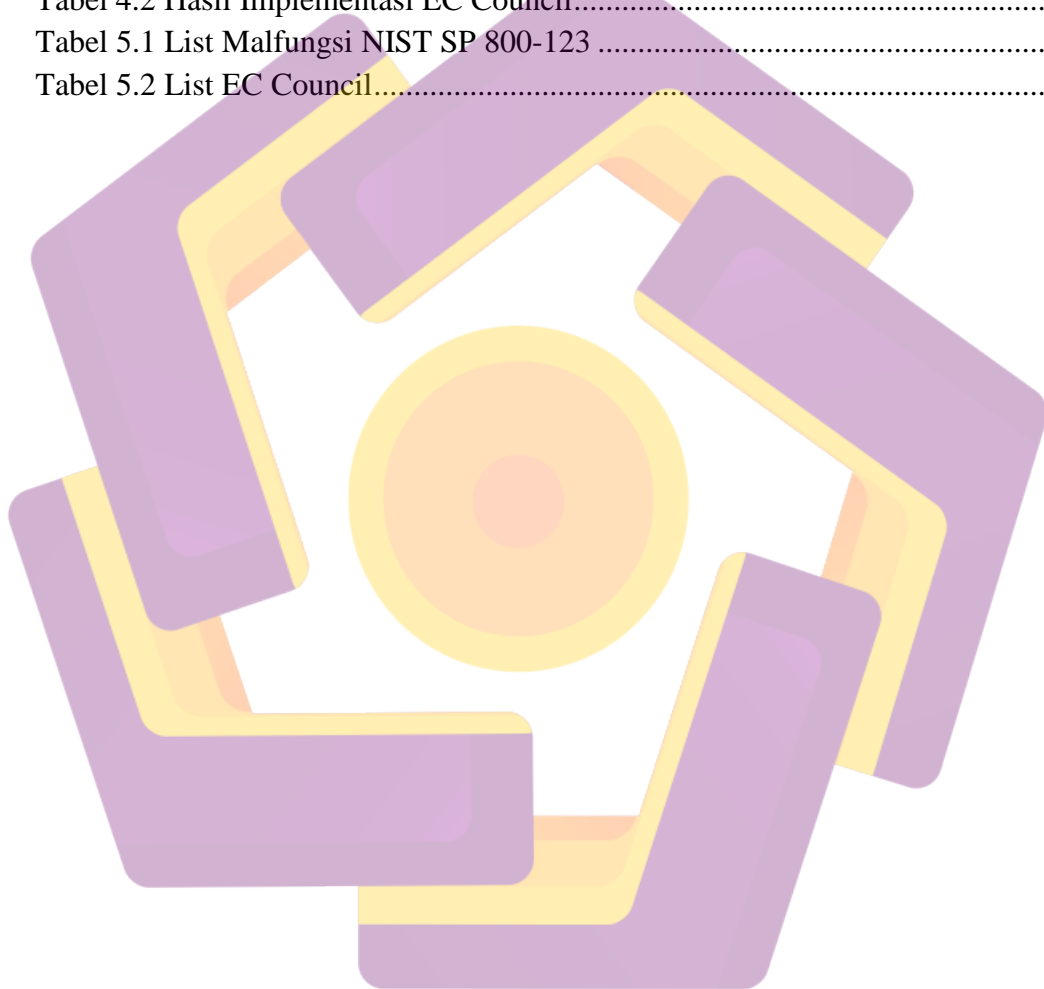
DAFTAR ISI

HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
INTISARI.....	x
<i>ABSTRACT</i>	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
BAB II LANDASAN TEORI	3
2.1 Tinjauan Pustaka.....	3
2.2 Dasar Teori.....	7
2.2.1 Database Server	7
2.2.2 Penetration Testing	7
2.2.3 NIST.....	8
2.2.4 EC Council.....	8
2.2.5 Virtual Box	9
2.2.6 Putty.....	9
2.2.7 Webmin.....	9
2.2.8 Honeypot.....	9
2.2.9 Metasploit	10
2.2.10 Nmap	10
2.2.11 Brute Force	10
BAB III METODOLOGI PENELITIAN	11
3.1 Metodologi Penelitian.....	11
3.2 Alur Penelitian	11
3.3 Pra Eksperimen	11
3.3.1 Alat dan Bahan Penelitian.....	12
3.3.2 Desain	13
3.2.1 Eksperimen	13
3.2.2 Testing	14
3.2.2.1 Skenario Testing.....	14
3.2.2.2 Pra Testing	14
3.2.2.3 Pentesting	14

3.2.2.4 Paska Testing	15
3.3 Paska Eksperimen	15
BAB IV PEMBAHASAN	16
4.1 Desain	16
4.1.1 Implementasi System.....	16
4.2 Implementasi NIST.....	16
4.2.1 Update Repository	17
4.2.2 Putty.....	18
4.2.3 Management User.....	18
4.2.4 Disable Login Root.....	20
4.2.5 Install Ufw	20
4.2.6 Port Knocking.....	21
4.2.7 Honeypot.....	21
4.2.8 Install Webmin.....	24
4.3.1 Implementasi EC Council.....	27
4.3.2 Update Repository	27
4.3.3 Install Ufw	28
4.3.4 Installasi webmin.....	29
4.3.5 Mematikan Akses Root.....	31
4.4 Hasil Implementasi	33
4.5 Pengujian Tool NIST SP 800-123	35
4.6 Pengujian Tool EC Council	40
4.7 Paska Testing	46
4.8 Analisa Data.....	47
BAB V PENUTUP	48
5.1 Kesimpulan	48
5.2 Saran	48
REFERENCES	49

DAFTAR TABEL

Tabel 2.1 Perbandingan Kajian	4
Tabel 2.2 Lanjutan	5
Tabel 2.3 Lanjutan	6
Tabel 2.4 Lanjutan	7
Tabel 3.1 Alat dan Bahan Penelitian.....	12
Tabel 4.1 Hasil Implementasi NIST SP 800-123.....	33
Tabel 4.2 Hasil Implementasi EC Council.....	34
Tabel 5.1 List Malfungsi NIST SP 800-123	47
Tabel 5.2 List EC Council.....	47



DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian.....	11
Gambar 3.2 Design.....	13
Gambar 4.1 Source Code Update Repository	17
Gambar 4.2 Update Semua Package Ke Versi Terbaru	17
Gambar 4.3 Setting SSH Melalui Putty	18
Gambar 4.4 Management User Melalui Putty.....	18
Gambar 4.5 Konfigurasi Management User Melalui Putty	19
Gambar 4.6 User Akbar Login.....	19
Gambar 4.7 User Akbar Sudah Tidak Bisa Login	19
Gambar 4.8 Masuk Ke File Root	20
Gambar 4.9 Disable Login Root	20
Gambar 4.10 Konfigurasi Install ufw.....	20
Gambar 4.11 Menutup Port 21	21
Gambar 4.12 Mengupdate Sistem.....	21
Gambar 4.13 Instalasi Pentbox Honeypot.....	22
Gambar 4.14 Ekstrak file <i>pentbox honeypot</i>	22
Gambar 4.15 Menjalankan <i>Pentbox Honeypot</i>	22
Gambar 4.16 Mengaktifkan <i>Honeypot</i>	23
Gambar 4.17 Konfigurasi <i>Honeypot</i>	23
Gambar 4.18 Mengakses <i>Port</i> Tipuan	24
Gambar 4.19 <i>Report</i> Sistem Honeypot	24
Gambar 4.20 Menginstall Kebutuhan Paket Webmin.....	25
Gambar 4.21 Mendownload Aplikasi Webmin	25
Gambar 4.22 Menginstall Webmin	25
Gambar 4.23 Menjalankan Aplikasi Webmin.....	26
Gambar 4.24 Tampilan Login Webmin	26
Gambar 4.25 Tampilan Dashboard Webmin	27
Gambar 4.26 Melihat Paket Pembaharuan.....	27
Gambar 4.27 Melakukan Pembaharuan	28
Gambar 4.28 Install Ufw.....	28
Gambar 4.29 Mengaktifkan Ufw	29
Gambar 4.30 Menambah Link Download Di Repository	29
Gambar 4.31 Menambah Webmin PGP Key	29
Gambar 4.32 Menambahkan Webmin PGP Key	30
Gambar 4.33 Mengupdate Server	30
Gambar 4.34 Install Webmin	30
Gambar 4.35 Mengubah File Miniserv	31
Gambar 4.36 Tampilan Login Webmin	31
Gambar 4.37 Masuk Ke File Root	32
Gambar 4.38 Mematikan Akses Root	32

Gambar 4.39 Akses Root Sudah Dimatikan	32
Gambar 4.40 Melihat IP Server	35
Gambar 4.41 Melihat Port yang Terbuka.....	35
Gambar 4.42 Menjalankan Console Metasploit.....	36
Gambar 4.43 Mencari Koneksi Ftp.....	36
Gambar 4.44 Masuk Ke Modul Ftp	37
Gambar 4.45 File Untuk Di Transfer	37
Gambar 4.46 Pengaturan User Login.....	37
Gambar 4.47 Pengaturan Pass Login	37
Gambar 4.48 Pengaturan Percobaan Login.....	38
Gambar 4.49 Pengaturan RHOST.....	38
Gambar 4.50 Melakukan Exploit Untuk Mendapatkan User Dan Password.....	38
Gambar 4.51 Login Ke Ftp	39
Gambar 4.52 Mengirimkan File Ke Server Yang Berhasil Di Exploit.....	39
Gambar 4.53 File Yang Berhasil Di Kirim	40
Gambar 4.54 Melihat Log Aktivitas Server Melalui Webmin.....	40
Gambar 4.55 Melihat IP Server	41
Gambar 4.56 Melihat Port Yang Terbuka Di Server	41
Gambar 4.57 Menjalankan Console Metasploit.....	42
Gambar 4.58 Mencari Koneksi Ftp.....	42
Gambar 4.59 Masuk Ke Module Ftp.....	42
Gambar 4.60 File Yang Akan Di Transfer.....	43
Gambar 4.61 Pengaturan User Login.....	43
Gambar 4.62 Pengaturan Password Login	43
Gambar 4.63 Pengaturan Percobaan Login.....	43
Gambar 4.64 Pengaturan RHOST.....	44
Gambar 4.65 Melakukan Exploit	44
Gambar 4.66 Mencoba Login Ke Ftp	44
Gambar 4.67 Masuk Ke Ftp.....	45
Gambar 4.68 Mengirimkan File Ke Server Yang Sudah Di Exploit	45
Gambar 4.69 Melihat Log Aktifitas Server Melalui Webmin	45

INTISARI

Sejak adanya pengembangan era industri 4.0, kemajuan di bidang IT menuntut semuanya harus bisa dilakukan dengan serba praktis. Dan seiring dengan kepraktisan dalam mengakses suatu konten pada server, diharapkan semua kegiatan bisnis maupun transaksi yang terdapat di dalam dunia industri tidak terganggu oleh apapun. Salah satu contoh gangguannya adalah dengan adanya ancaman dari peretas (*hacker*). Permasalahan berikut ini tentunya sangat merepotkan bagi instansi-instansi yang sedang dalam masa proses bangkit dan melakukan sistem *new normal* setelah adanya wabah pandemik ini, yang tentunya dapat menurunkan performa dari instansi tersebut. Dalam proses peningkatan keamanan di suatu server tentunya banyak metode metode yang dapat di ikuti, dengan tingkat keamanan yang lebih terjamin. Sehingga pada kesempatan ini penulis ingin melakukan penelitian “Perbandingan Hardening Server Dengan Metode NIST dan EC Council” yang bertujuan untuk melihat tingkat keamanan pada server dengan menggunakan metode dari masing masing modul, agar mendapatkan hasil perbandingan dan melihat mana yang lebih aman, dari mengurangi tingkat kerawanan di dalamnya dari serangan-serangan peretas (*hacker*) yang tentunya dapat merusak server, database, aplikasi, jaringan, dan bahkan OS (*Operating System*). Adapun penerapan ini dilakukan dengan konfigurasi sistem operasi kali linux dengan tool bawaan atau built in dari sistem. Tujuan utaman penulis dari penelitian ini di harapkannya dapat membandingkan aspek keamanan terhadap server dari metode NIST dan EC Council. Adapun metode yang penulis gunakan di dalam penelitian ini adalah dengan metode black box. Pengujian ini dilakukan dengan uji coba via virtual serangan, dengan metode brute force untuk proses uji coba dari ke dua server yang sudah di buat untuk mencoba masuk ke dalam server, dan juga menambahkan sebuah aplikasi webmin untuk membantu monitoring server, membatasi client yang ingin mengakses masuk, membatasi koneksi, dan dapat memantau aktifitas lainnya. Dengan berjalannya hal tersebut, maka akan di dapatkan hasil uji coba dari kedua server.

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

ABSTRACT

Since the development of the industrial era 4.0, progress in the IT field requires everything to be done practically. And along with the practicality of accessing content on the server, it is hoped that all business activities and transactions in the industrial world will not be disturbed by anything. One example of interference is the threat from hackers (hackers). The following problems are certainly very inconvenient for agencies that are in the process of awakening and carrying out a new normal system after this pandemic, which of course can reduce the performance of these agencies. In the process of increasing security on a server, of course, there are many methods that can be followed, with a more guaranteed level of security. So on this occasion the author wants to do a research "Comparison of Server Hardening With the NIST and EC Council Methods" which aims to see the level of server security using the method of each module, in order to get the results of the comparison and see which one is safer, from reducing the level of vulnerability. in it from hacker attacks (hackers) which of course can damage servers, databases, applications, networks, and even OS (Operating System). The implementation is done by configuring the Kali Linux operating system with the built-in tools from the system. The main goal of the author of this study is to compare server security with the NIST and EC Council methods. The method that the author uses in this study is the black box method. This test is carried out by testing through virtual attacks, with the brute force method for the trial process from the two servers that have been created to try to enter the server and also adding a webmin application to help monitor the server, limiting clients who want to access login, limit connections, and can unify other activities. With this running, it will get test results from both servers.

Keyword: *Linux, security, server, Webmin, Brute Force.*