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 Al Fatta, 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

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Sejak adanya pengembangan era industri 4.0, kemajuan di bidang IT menuntut semuanya harus bisa dilakukan dengan serba praktis. Dan seiring dengan ke praktisan 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 mengurangai 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 memonitoring 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.*