IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT DAN HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA VIRTUAL PRIVATE SERVER (VPS)

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

disusun oleh
MUHAMMAD RIZALDI ATTHARIQ
20.11.3734

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT DAN HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA VIRTUAL PRIVATE SERVER (VPS)

SKRIPSI

Untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

disusun oleh

MUHAMMAD RIZALDI ATTHARIQ

20.11.3734

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT DAN HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA VIRTUAL PRIVATE SERVER (VPS)

yang disusun dan diajukan oleh

MUHAMMAD RIZALDI ATTHARIQ
20.11.3734

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 17 Oktober 2024

Dosen Pembimbing,

Subektiningsih, S.Kom, M.Kom
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT DAN HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA VIRTUAL PRIVATE SERVER (VPS)

yang disusun dan diajukan oleh

Muhammad Rizaldi Attharig
20.11.3734

Telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Oktober 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ali Mustopa, M.Kom **NIK. 190302192**	
Ahmad Sa'dii, S.Kom, M.Eng **NIK. 190302459**	
Subektiningsih, M.Kom **NIK. 190302413**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Oktober 2024

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Rizaldi Atthariq
NIM : 20.11.3734

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT DAN HONEYPOT SEBAGAI PENDETEKSI SERANGAN PADA VIRTUAL PRIVATE SERVER (VPS)

Dosen Pembimbing : Subektiningsih, S.Kom, 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, <17 Oktober 2024>

Yang Menyatakan,

Muhammad Rizaldi Atthariq

HALAMAN PERSEMBAHAN

Puji Syukur, Alhamdulillah atas kehadirat Allah SWT yang telah memberikan rahmat dan Karunia-Nya. Sholawat dan salam semoga selalu tercurahkah kepada Nabi Muhammad SAW. Pada halaman persembahan ini penulis ingin mempersembahkan skripsi yang telah penulis susun ini kepada:

1. Orang tua saya, Bapak Nana Oktafiana Wirachmana dan Ibu Rosidawati yang telah memberikan do'a, dukungan dan motivasi yang begitu tulus.
2. Ibu Subektiningsih, S.kom, M.Kom, selaku dosen pembimbing yang telah memberikan banyak saran bimbingan dan masukan sehingga saya dapat menyelesaikan skripsi ini.
3. Teman-teman yang selalu memberikan semangat dan dukungan yang telah kalian berikan.
4. Terima kasih semua pihak yang belum bisa disebutkan, akhir kata saya persembahkan skripsi ini untuk kalian semua. Dan semoga skripsi ini dapat bermanfaat dan berguna untuk pembaca

KATA PENGANTAR

Puji Syukur, Alhamdulillah atas kehadirat Allah SWT yang telah memberikan rahmat dan Karunia-Nya kepada kita semua sehingga penulis dapat menyelesaikan tugas akhir dengan judul "Implementasi *Intrusion Detection System (IDS) Snort* Dan *Honeypot* Sebagai Pendeteksi Serangan Pada *Virtual Private Server (VPS)*". Penulisan skripsi ini ditunjukkan untuk memenuhi salah satu syarat kelulusan di Universitas Amikom Yogyakarta.

Penulis menyadari bahwa penyusunan laporan akhir skripsi ini tidak akan terwujud tanpa adanya bantuan dan dorongan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Ibu Subektiningsih, S.Kom, M.Kom. Selaku dosen pembimbing yang telah membimbing, mengarahkan, serta mendukung dalam penyusunan laporan ini.
2. Kedua Orang Tua dan Kakak, yang memberikan dukungan, semangat, dan motivasi.
3. Seluruh Bapak dan Ibu dosen program studi Informatika yang telah memberikan ilmu dan bimbingan selama menjalani perkuliahan
4. Teman-teman yang telah membantu mengingatkan dan memotivasi

Penulis sangat menyadari bahwa laporan akhir skripsi ini masih jauh dari kata sempurna, baik dalam penyajian, penulisan, dan tata bahasa. Oleh karena itu, kritik dan saran sangat diharapkan guna menyempurnakan laporan ini. Akhir kata penulis berharap skripsi ini dapat bermanfaat bagi pembaca.

Yogyakarta, <17 Oktober 2024>
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Internet telah membantu setiap orang untuk mendapatkan informasi secara luas, salah satu informasi didapatkan dari *website*. Sebuah *website* berjalan pada sebuah server, salah satu server yang paling sering digunakan adalah VPS server. Akan tetapi, VPS server memiliki kekurangan apabila adanya serangan kepada server terjadi, maka server membutuhkan sistem keamanan yang dapat menjaga server dan dapat memonitoring server secara *real-time* oleh pengguna.

Sistem keamanan *IDS Snort* dan *Honeypot Cowrie* menjadi salah satu solusi sebagai *firewall*, dengan *snort* yang dapat mendeteksi serangan yang terjadi pada jaringan server dan *Cowrie* dapat menjadi server palsu untuk mengalihkan penyerang dari server asli. Hasil deteksi yang dihasilkan oleh *snort* dan *cowrie* yang tersimpan pada log, akan diintegrasikan ke *splunk* untuk membantu pengguna dalam memonitoring server secara *real-time*.

Hasil pengujian dengan serangan *port scanning*, *brute force* dan *DDoS*, *snort* dan *cowrie* dapat mendeteksi beserta mencatat semua serangan. Log yang dihasilkan oleh sistem keamanan dapat diolah pada *splunk*, sehingga pengguna mendapatkan informasi secara akurat apa yang sedang terjadi pada server. Data hasil pengujian serangan dievaluasi dengan *CIA Triad* untuk mengetahui dari keberhasilan dan kelemahan sistem dalam melindungi server dari serangan.

Kata Kunci: firewall, snort, cowrie, VPS, splunk

ABSTRACT

Everyone may now access information more extensively thanks to the internet, including information from websites. A VPS server is one of the most widely utilized types of servers that power websites. Nevertheless, the VPS server has drawbacks. Should an assault occur, the server needs a security system that can maintain it and allow users to monitor it in real time.

One option for a firewall is an IDS Snort and Honeypot Cowrie security system. Snort can identify assaults on server networks, and Cowrie can act as a fictitious server to reroute attackers away from the real server. To help users monitor the server in real-time, splunk will incorporate the detection findings produced by snort and cowrie, which are saved in logs.

Results of tests showing that cowrie and snort can detect and record all assaults, including DDoS, brute force, and port scanning. The security system's logs can be handled in Splunk to provide users with precise information about server activity. The efficacy and vulnerabilities of the system in safeguarding the server from intrusions are assessed by comparing the attack test results with the CIA Triad.

Keyword: firewall, snort, cowrie, VPS, splunk