

**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,


Subekti Ningsih, 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 Atthariq

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'idi, S.Kom, M.Eng
NIK. 190302459

Subekhtiningsih, M.Kom
NIK. 190302413

Skrripsi 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 kehadiran Allah SWT yang telah memberikan rahmat dan Karunia-Nya. Sholawat dan salam semoga selalu tercurahkan 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 kehadiran 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

HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Studi Literatur	5
2.2 Dasar Teori	12
2.2.1 Virtual Private Server.....	12
2.2.2 Intrusion Detection Service.....	12
2.2.3 Snort.....	12
2.2.4 Honeypot.....	13
2.2.5 Cowrie.....	13
2.2.6 Alert_Json	14
2.2.7 Pulled Pork.....	14
2.2.8 Splunk	14
2.2.9 Distributed Denial of Service (DDoS).....	14
2.2.10 Bruteforce	14

2.2.11	Secure Socket Shell (SSH).....	15
2.2.12	Web Server.....	15
2.2.13	AbuseIPDB.....	15
BAB III METODE PENELITIAN		16
3.1	Alur Penelitian	16
1.	Prepare	16
2.	Plan	17
3.	Design	17
4.	Implement	17
5.	Operate	17
6.	Optimize	18
3.2	Alat dan Bahan.....	18
3.2.1	Alat/Instrumen	18
1)	Kebutuhan Hardware	18
2)	Kebutuhan Software	18
BAB IV HASIL DAN PEMBAHASAN		20
4.1	Prepare (Persiapan)	20
4.2	Plan	21
4.2.1	IDS Snort	21
4.2.2	Honeypot Cowrie	22
4.3	Design	23
4.3.1	Topologi dan Skema Sistem Keamanan.....	23
4.3.2	Topologi dan Skema Pengujian Serangan.....	25
4.4	Implement	27
4.4.1	Virtual Private Server.....	27
4.4.2	Snort.....	28
4.4.3	Cowrie.....	35
1.	Instal Depedenci.....	35
2.	Instal Cowrie	36
4.4.4	Splunk	39
1.	Instal Splunk	39
2.	Konfigurasi	41

4.5	Operate.....	44
4.5.1	Port scanning.....	44
1.	Snort.....	45
2.	Cowrie.....	51
4.5.2	Brute Force.....	52
1.	Snort.....	52
2.	Cowrie.....	53
4.5.3	DDoS.....	56
1.	Snort.....	56
2.	Cowrie.....	57
4.6	Optimize.....	58
1.	Confidentiality (Kerahasiaan).....	58
2.	Integrity (Integritas).....	60
3.	Availability (Ketersediaan).....	62
5.1.	Kesimpulan	69
5.2.	Saran	70
REFERENSI		71

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	9
Tabel 3. 1 Spesifikasi Hardware Laptop	18
Tabel 3. 3 Spesifikasi Virtual Private Server	19
Tabel 3. 4 Spesifikasi Virtual environment Kali Linux	19
Tabel 3. 5 Kebutuhan Perangkat Lunak	19
Tabel 4. 1 Ruleset pada Pulledpork	20
Tabel 4. 2 Alat dan Library untuk Snort	21
Tabel 4. 3 tabel lanjutan dari 4.2	22
Tabel 4. 4 Alat dan Library untuk Cowrie	23
Tabel 4. 5 Tabel IP dan port	24
Tabel 4. 6 Spesifikasi VPS server	27
Tabel 4. 7 Penjelasan library pada dependensi	28
Tabel 4. 8 Source Software snort	29
Tabel 4. 9 penjelasan fields alert_json	34
Tabel 4. 10 Penjelasan dependensi cowrie	35
Tabel 4. 11 Source aplikasi	37
Tabel 4. 12 Tabel data static serangan port scanning	46
Tabel 4. 13 Hasil port scanning	48
Tabel 4. 14 Data static serangan port scanning	49
Tabel 4. 15 Hasil pengujian dan mitigasi	58
Tabel 4. 16 Penilaian aspek Confidentiality snort, cowrie, dan splunk	59
Tabel 4. 17 Aspek integrasi Snort dan Cowrie	62
Tabel 4. 18 Penggunaan Resource server	66
Tabel 4. 19 Kesimpulan CIA Triad	67

DAFTAR GAMBAR

Gambar 3. 1 Metode PPDIOO	16
Gambar 4. 1 Topologi jaringan sistem keamanan pada VPS	23
Gambar 4. 2 Flowchart Snort.....	24
Gambar 4. 3 Flowchart Cowrie.....	24
Gambar 4. 4 Topologi Jaringan Penyerang	25
Gambar 4. 5 Skema pengujian serangan	26
Gambar 4. 6 Dashboard Virtual Private Server.....	27
Gambar 4. 7 Instal Library dan tools	28
Gambar 4. 8 Download software Snort.....	29
Gambar 4. 9 menjalankan skrip ./configure_cmake.sh.....	29
Gambar 4. 10 build instaler snort dengan [make]	29
Gambar 4. 11 instal snort ke sistem operasi.....	30
Gambar 4. 12 Snort	30
Gambar 4. 13 Mengecek GRO dan LRO.....	30
Gambar 4. 14 Skrip ethtool.service.....	30
Gambar 4. 15 menjalankan ethtool.service.....	31
Gambar 4. 16 membuat folder dan file	31
Gambar 4. 17 Downlaod pulledpork dengan [git]	31
Gambar 4. 18 instalasi pulledpork	32
Gambar 4. 19 Konfigurasi ruleset dan oinkcode.....	32
Gambar 4. 20 menjalankan pulled pork untuk menambahkan ruleset.....	32
Gambar 4. 21 Konfigurasi pulledpork pada snort.lua.....	33
Gambar 4. 22 konfigurasi IP pada snort.lua.....	33
Gambar 4. 23 mengaktifkan fitur blocklist.....	33
Gambar 4. 24 skrip alert_json pada snort.lua	34
Gambar 4. 25 mencetak hasil log alert_json ke format txt	35
Gambar 4. 26 Hasil log alert_json	35
Gambar 4. 27 instal alat dan library	35
Gambar 4. 28 mengganti port ssh	36

Gambar 4. 29 User admin	36
Gambar 4. 30 Menyalin cowrie dari github	37
Gambar 4. 31 membuat virtual environment	37
Gambar 4. 32 update pip	38
Gambar 4. 33 instal requirement.....	38
Gambar 4. 34 Mengganti hostname cowrie	38
Gambar 4. 35 Menjalankan server dummy Cowrie	39
Gambar 4. 36 Akses download Splunk	39
Gambar 4. 37 Downlaod file instaler splunk	40
Gambar 4. 38 Unpack instaler splunk.....	40
Gambar 4. 39 Menjalankan Splunk	40
Gambar 4. 40 skrip autorun systemD	41
Gambar 4. 41 Splunk	41
Gambar 4. 42 Plugin Snort JSON Alerts	41
Gambar 4. 43 Membuat folder dan file input	42
Gambar 4. 44 akses splunk ke file log snort	42
Gambar 4. 45 cara mengakses log dari splunk	42
Gambar 4. 46 menampilkan hasil log dengan splunk [timechart]	43
Gambar 4. 47 penggunaan resource splunk	43
Gambar 4. 48 Traceroute.....	44
Gambar 4. 49 Metode port scanning Connect Scan dan SYN Scan	45
Gambar 4. 50 Pengujian dengan metode Connect Scan	45
Gambar 4. 51 Hasil deteksi snort dari serangan Connect Scan	46
Gambar 4. 52 Serangan port scanning dengan metode SYN Scan	47
Gambar 4. 53 Serangan port scanning -sS	47
Gambar 4. 54 Hasil deteksi snort dari serangan port scanning	48
Gambar 4. 55 Cek IP penyerang port scanning dengan AbuseIPdb	49
Gambar 4. 56 Hasil report dari AbuseIPdb	50
Gambar 4. 57 Serangan XMAS	50
Gambar 4. 58 hasil report penyerang dari AbuseIPdb	51
Gambar 4. 59 serangan port scanning untuk tes cowrie	51

Gambar 4. 60 Hasil deteksi cowrie untuk serangan port scanning	52
Gambar 4. 61 Hasil deteksi snort saat ada serangan ke ssh	52
Gambar 4. 62 Pengujian brute force ke layanan ssh cowrie	53
Gambar 4. 63 Hasil deteksi Cowrie dari serangan brute force	53
Gambar 4. 64 Hasil deteksi serangan brute force dari luar peneliti	54
Gambar 4. 65 Cek penyerang brute force di AbuseIPdb.....	55
Gambar 4. 66 Hasil report di AbuseIPdb	55
Gambar 4. 67 Pengujian DDoS ke port 443 dengan metode http	56
Gambar 4. 68 Hasil deteksi Snort	56
Gambar 4. 69 Pengujian DDoS ke port ssh cowrie.....	57
Gambar 4. 70 Hasil deteksi serangan DDoS ke layanan ssh cowrie	57
Gambar 4. 71 Serangan ke http	60
Gambar 4. 72 Dekrip b64_data	60
Gambar 4. 73 Cek ip penyerang di website AbuseIPDB	61
Gambar 4. 74 Idle aplikasi apache2	62
Gambar 4. 75 Idle dengan sistem keamanan snort.....	63
Gambar 4. 76 Idle Cowrie.....	63
Gambar 4. 77 Idle Splunk	63
Gambar 4. 78 Run web server Apache2.....	64
Gambar 4. 79 Run Snort	64
Gambar 4. 80 Run Cowrie	65
Gambar 4. 81 Run Splunk.....	65
Gambar 4. 82 Hasil Bloklist snort.....	68

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