Implementasi Cowrie Honeypot Dan Snort Inline-Mode Untuk Mendeteksi Serangan Brute-Force Dan Simulasi Deteksi Serangan Dos

Rudi Ardi Hamzah[1] Agus Prihanto[2]
[1]Teknik Informatiak/Universitas Negeri Surabaya
[1]rudi.20036@mhs.unesa.ac.id
[2]agusprihanto@unesa.ac.id

***Abstrak*— Pada era digital saat ini, keamanan jaringan menjadi perhatian utama seiring meningkatnya intensitas dan kompleksitas serangan siber. Dua serangan yang sering mengancam sistem adalah brute-force dan Denial of Service (DoS). Penelitian ini bertujuan untuk mengimplementasikan Cowrie Honeypot dan Snort Inline-Mode sebagai upaya mendeteksi dan memantau serangan brute-force serta simulasi deteksi serangan DoS. Cowrie Honeypot digunakan untuk menjebak dan mencatat aktivitas serangan brute-force, sedangkan Snort Inline-Mode diimplementasikan untuk mendeteksi dan memblokir lalu lintas mencurigakan yang mengindikasikan serangan DoS. Penelitian ini dilakukan dalam lingkungan jaringan virtual menggunakan Virtual Machine. Evaluasi kinerja sistem dilakukan dengan parameter Detection Rate, Prevention Rate, Accuracy, Resource Usage, dan Availability. Hasil penelitian menunjukkan bahwa kombinasi Cowrie dan Snort dapat mendeteksi aktivitas serangan brute-force dan DoS dengan efektivitas yang cukup baik, serta mampu memberikan data yang bermanfaat untuk analisis pola serangan. Temuan ini diharapkan dapat menjadi acuan bagi praktisi keamanan jaringan dalam mengembangkan sistem pertahanan terhadap serangan siber.**

Kata Kunci - Cowrie Honeypot, Snort, keamanan jaringan

I. PENDAHULUAN

Di era digital saat ini, teknologi informasi memainkan peran yang sangat penting dalam mendukung berbagai aspek kehidupan, mulai dari bisnis, pendidikan, hingga pemerintahan. Namun, di balik manfaat besar yang ditawarkan teknologi ini, terdapat risiko keamanan yang semakin meningkat, terutama terkait ancaman serangan siber. Dua serangan yang paling sering dihadapi oleh organisasi adalah serangan *brute-force* dan serangan *Distributed Denial of Service* (DDoS). Serangan-serangan ini, meskipun berbeda dalam teknik dan tujuan, sama-sama berpotensi merusak sistem, menyebabkan gangguan operasional, kerugian finansial, hingga kerusakan reputasi bagi organisasi yang menjadi targetnya.

Serangan *brute-force* merupakan upaya penyerang untuk memperoleh akses ilegal ke dalam suatu sistem dengan mencoba kombinasi kata sandi yang berbeda hingga menemukan kombinasi yang benar. Dalam serangan ini, kredensial pengguna menjadi sasaran utama, dan sering kali pelaku menggunakan perangkat otomatis untuk melakukan ribuan bahkan jutaan percobaan kata sandi dalam waktu singkat. Serangan ini semakin mudah dilakukan dengan adanya alat bantu seperti *hydra* atau *medusa* yang memungkinkan penyerang untuk mengotomatisasi upaya brute-force. Di sisi lain, serangan DDoS memiliki tujuan yang berbeda, yaitu untuk membuat sistem atau jaringan menjadi tidak dapat diakses oleh pengguna yang sah. Dalam serangan DDoS, pelaku akan membanjiri *server* dengan permintaan palsu atau *overload* lalu lintas, sehingga layanan terganggu dan bahkan dapat mengalami *downtime* yang lama.

Untuk mengatasi ancaman tersebut, berbagai teknologi dan metode keamanan jaringan dikembangkan, salah satunya adalah penggunaan honeypot dan *sistem Intrusion Prevention System* (IPS). Honeypot merupakan alat yang dirancang untuk menarik serangan siber, dengan cara meniru sistem yang rentan atau menarik bagi pelaku serangan. Dalam konteks ini, honeypot seperti Cowrie dapat digunakan untuk mengamati dan memantau pola-pola serangan brute-force, sehingga informasi berharga tentang taktik, teknik, dan prosedur (TTP) yang digunakan penyerang dapat diperoleh. Cowrie Honeypot bahkan dapat mencatat aktivitas interaktif, termasuk upaya *login*, sehingga sangat efektif untuk mendeteksi serangan *brute-force*.

Selain honeypot, sistem IPS seperti Snort dalam mode *inline* juga merupakan alat penting dalam keamanan jaringan. Berbeda dengan honeypot yang lebih berfokus pada pendeteksian dan pengumpulan data, Snort *Inline-Mode* dapat mendeteksi dan memblokir serangan secara real-time. Snort bekerja dengan menginspeksi setiap paket yang masuk dan keluar dari jaringan, mencari pola yang mencurigakan atau mengidentifikasi ciri khas serangan tertentu. Dalam mode inline, Snort dapat digunakan untuk mencegah serangan DDoS dengan membatasi lalu lintas berlebihan yang masuk ke dalam jaringan, sehingga mencegah server dari kelebihan beban akibat lalu lintas yang tidak wajar. Kombinasi antara Cowrie dan Snort memberikan lapisan perlindungan yang komprehensif, di mana Cowrie mengumpulkan informasi penting tentang serangan sementara Snort mengambil

tindakan pencegahan.

Namun, implementasi kedua alat ini juga menghadirkan tantangan tersendiri. Salah satu tantangan dalam penggunaan Cowrie Honeypot adalah risiko keamanan yang mungkin muncul jika konfigurasinya tidak tepat, yang bisa memberikan akses tidak sengaja ke dalam jaringan internal. Selain itu, konfigurasi Snort yang kurang optimal juga dapat menyebabkan masalah, seperti kegagalan mendeteksi serangan atau bahkan mengganggu lalu lintas jaringan yang sah. Oleh karena itu, sangat penting untuk memiliki pemahaman yang mendalam tentang pengaturan dan konfigurasi kedua alat ini agar implementasi dapat berjalan efektif. Kombinasi Cowrie dan Snort perlu dikonfigurasi sedemikian rupa untuk mencapai keseimbangan antara keamanan dan kelancaran operasional jaringan.

Penelitian ini bertujuan untuk mengeksplorasi cara dalam mengimplementasikan Cowrie *Honeypot* dan Snort *Inline-Mode* untuk mendeteksi dan mencegah serangan *brute-force* dan DDoS. Dalam penelitian ini, akan dilakukan simulasi serangan dalam lingkungan terkontrol untuk menguji bagaimana Cowrie dapat menangkap aktivitas brute-force dan bagaimana Snort mampu memblokir serangan DDoS. Dengan analisis dari *log* Cowrie dan Snort, diharapkan dapat diperoleh pemahaman yang lebih baik tentang efektivitas kedua alat ini dalam menghadapi serangan siber yang semakin kompleks dan canggih.

Melalui penelitian ini, diharapkan organisasi dapat memperoleh wawasan tentang bagaimana cara mengintegrasikan Cowrie dan Snort dalam strategi keamanan jaringan mereka. Dengan penerapan yang tepat, kombinasi kedua alat ini dapat memberikan keuntungan ganda, yaitu kemampuan untuk memonitor dan mempelajari pola serangan serta kapabilitas untuk mencegah kerusakan yang lebih luas. Hasil dari penelitian ini diharapkan dapat menjadi acuan bagi praktisi keamanan jaringan dalam membangun sistem yang lebih aman dan tangguh dalam menghadapi ancama

II. METODE PENELITIAN

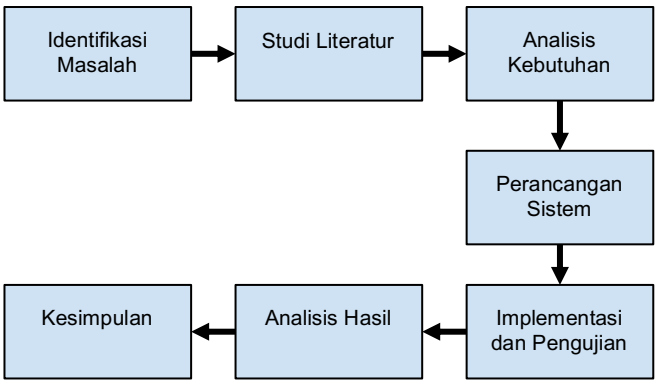
A. Model Pengembangan

Penelitian ini menggunakan metode eksperimental design untuk menguji efektivitas kombinasi dua teknologi keamanan siber, yaitu Cowrie Honeypot dan Snort Inline-Mode, dalam mendeteksi dan mencegah dua jenis serangan yang paling sering terjadi di dunia maya: brute-force dan DDoS. Dengan pendekatan ini, peneliti dapat mengevaluasi sistem secara langsung dalam kondisi yang terkontrol melalui eksperimen yang dirancang untuk meniru serangan yang terjadi di dunia nyata.

Penerapan Cowrie Honeypot bertujuan untuk mensimulasikan layanan yang sering menjadi target serangan brute-force, seperti SSH atau Telnet, di mana penyerang berusaha menebak password untuk mendapatkan akses ke server. Dengan mengkonfigurasi Cowrie untuk merekam aktivitas penyerang, peneliti dapat memperoleh wawasan mengenai pola serangan dan teknik yang digunakan oleh penyerang. Honeypot ini juga dapat menarik serangan, memberikan waktu lebih lama bagi sistem pertahanan untuk merespons dan memblokir penyerang, serta membantu mengidentifikasi potensi celah atau kerentanannya.

Di sisi lain, Snort Inline-Mode digunakan untuk memantau dan menganalisis lalu lintas jaringan secara real-time, serta mendeteksi dan memblokir serangan DDoS dan brute-force yang terjadi. Snort Inline-Mode berfungsi tidak hanya sebagai detektor serangan, tetapi juga sebagai penghalang aktif yang mencegah trafik berbahaya memasuki atau meninggalkan jaringan. Dengan menggunakan Snort untuk memonitor jaringan secara langsung, peneliti dapat menilai sejauh mana kemampuan Snort dalam mendeteksi dan menghambat serangan DDoS, yang biasanya melibatkan pengiriman trafik dalam jumlah besar untuk membanjiri dan mengganggu ketersediaan layanan, serta serangan brute-force yang mencoba masuk melalui upaya penetrasi berulang pada port layanan yang rentan.

Melalui eksperimen ini, peneliti dapat mengevaluasi secara mendalam efektivitas kedua teknologi ini dalam bekerja bersama, serta memantau interaksi antara Cowrie Honeypot yang berfungsi untuk menarik penyerang dan Snort *Inline-Mode* yang bertugas untuk menghalau serangan. Dengan memanfaatkan data yang diperoleh dari log dan monitoring yang tercatat selama eksperimen, peneliti dapat menganalisis keandalan sistem dalam menghadapi serangan secara berkelanjutan, serta mengidentifikasi kekuatan dan kelemahan dari pendekatan ini.



Gambar 3.1 Metode Eksperimental Design

Berikut merupakan alur tahapan yang dilakukan dalam

penelitian ini. Tahapan penelitian yang dilakukan mencakup beberapa langkah penting, yang akan dijelaskan sebagai berikut:

1. Identifikasi Masalah

   Langkah pertama dalam penelitian ini adalah mengidentifikasi masalah utama terkait keamanan jaringan, khususnya ancaman serangan brute-force dan DDoS yang semakin meningkat dan berpotensi merusak sistem jaringan. Serangan brute-force berupaya menebak kredensial login untuk mendapatkan akses tidak sah, sedangkan serangan DDoS bertujuan untuk mengganggu ketersediaan layanan dengan membanjiri trafik jaringan. Identifikasi masalah ini dilakukan untuk merumuskan tujuan dari penerapan Cowrie Honeypot dan Snort Inline-Mode sebagai upaya mitigasi dan pencegahan serangan-serangan tersebut.

2. Studi Literatur

   Tahap studi literatur dilakukan untuk mendapatkan pemahaman mendalam tentang konsep-konsep utama dalam penelitian ini, yaitu honeypot, IDS/IPS (Intrusion Detection/Prevention System), serangan brute-force, dan DDoS. Melalui studi literatur, peneliti mempelajari bagaimana Cowrie Honeypot digunakan untuk menarik dan memantau aktivitas penyerang, serta bagaimana Snort Inline-Mode dapat mendeteksi dan memblokir serangan secara real-time. Selain itu, literatur tentang parameter efektivitas dalam mendeteksi dan mencegah serangan juga akan dikaji untuk merumuskan pengukuran keberhasilan sistem.

3. Analisis Kebutuhan

   Pada tahap ini, dilakukan analisis kebutuhan perangkat keras dan perangkat lunak yang diperlukan untuk implementasi Cowrie Honeypot dan Snort Inline-Mode. Analisis ini meliputi spesifikasi minimum server, jaringan, dan sistem operasi yang kompatibel untuk memastikan kedua teknologi ini dapat berjalan secara optimal. Selain itu, kebutuhan jaringan, konfigurasi firewall, serta perangkat lunak tambahan yang diperlukan untuk simulasi serangan brute-force dan DDoS juga diidentifikasi. Analisis kebutuhan ini akan menjadi dasar bagi perancangan sistem pada tahap berikutnya.

4. Perancangan Sistem

   Tahap ini berfokus pada perancangan arsitektur sistem dan skenario pengujian. Dalam perancangan sistem, dibuat arsitektur jaringan yang melibatkan Cowrie Honeypot sebagai sistem yang berfungsi untuk memonitor upaya akses brute-force, dan Snort Inline-Mode sebagai sistem yang memantau dan memblokir trafik mencurigakan, terutama dari serangan DDoS. Desain skenario pengujian dibuat untuk mensimulasikan kondisi serangan nyata dengan menempatkan honeypot dan IDS/IPS dalam satu jaringan yang rentan. Setiap tahapan perancangan akan dibuat dalam bentuk diagram dan alur sistem untuk memudahkan implementasi dan pengujian nantinya.

5. Implementasi Kebutuhan

   Pada tahap ini, perangkat keras dan perangkat lunak yang telah ditentukan pada tahap analisis kebutuhan akan diimplementasikan sesuai dengan rancangan sistem. Implementasi melibatkan pemasangan dan konfigurasi Cowrie Honeypot dan Snort Inline-Mode, serta pengaturan jaringan yang memungkinkan honeypot dan IDS/IPS berfungsi dengan optimal. Honeypot akan dikonfigurasi untuk memantau aktivitas brute-force, sementara Snort akan dikonfigurasi dalam mode inline untuk memantau, mendeteksi, dan memblokir serangan DDoS dan serangan brute-force yang terdeteksi. Implementasi ini juga melibatkan simulasi serangan brute-force menggunakan alat seperti Hydra dan simulasi serangan DDoS menggunakan hping3 atau LOIC.

6. Analisis Hasil

   Pada tahap analisis ini, log aktivitas dari Cowrie Honeypot dan Snort Inline-Mode dievaluasi berdasarkan enam parameter utama: kerahasiaan, ketersediaan, akurasi, penggunaan sumber daya, tingkat deteksi, dan tingkat pencegahan. Confidentiality (Kerahasiaan) berfokus pada kemampuan honeypot untuk mengarahkan serangan ke sistem palsu dan melindungi data sensitif, sementara Snort membantu membatasi akses ke pihak yang tidak sah. Availability (Ketersediaan) menilai seberapa baik Snort mempertahankan ketersediaan layanan selama serangan DDoS dengan membatasi lalu lintas berbahaya. Accuracy (Akurasi) dievaluasi melalui kemampuan Snort membedakan antara trafik normal dan mencurigakan, mengurangi kesalahan deteksi untuk meningkatkan efektivitas sistem. Selanjutnya, Resource Usage (Penggunaan Sumber Daya) mengamati efisiensi sistem dalam menggunakan CPU, RAM, dan bandwidth, memastikan bahwa proses deteksi dan pencegahan berjalan tanpa membebani server. Detection Rate (Tingkat Deteksi Serangan) mengevaluasi efektivitas Cowrie dan Snort dalam mengenali serangan yang terjadi, diukur sebagai persentase dari total serangan yang dikirim ke sistem. Terakhir, Prevention Rate (Tingkat Pencegahan) mengukur keberhasilan Snort dalam memblokir serangan setelah dideteksi, mencerminkan seberapa efektif sistem ini dalam mencegah dampak serangan terhadap jaringan. Analisis keseluruhan bertujuan untuk menilai keberhasilan

implementasi Cowrie Honeypot dan Snort Inline-Mode dalam mendeteksi dan mencegah serangan brute-force dan DDoS, sehingga dapat meningkatkan keamanan jaringan dari ancaman eksternal.

7. Kesimpulan

Berdasarkan analisis hasil, peneliti akan menarik kesimpulan mengenai efektivitas penerapan Cowrie Honeypot dan Snort Inline-Mode dalam mendeteksi dan mencegah serangan brute-force dan DDoS. Kesimpulan ini mencakup rekomendasi mengenai penerapan teknologi ini dalam lingkungan jaringan yang lebih luas, potensi perbaikan, serta saran untuk penelitian lanjutan.

B. Analisis Kebutuhan

Dalam implementasi Cowrie Honeypot dan Snort Inline-Mode untuk mendeteksi dan mencegah serangan brute-force dan DDoS, analisis kebutuhan meliputi pemenuhan terhadap aspek-aspek teknis dan fungsional sebagai berikut:

1. Hardware

Tabel 3.1 Analisis Hardware

No	Komponen	Spesifikasi
1.	CPU	2.0 GHz
2.	RAM	4 GB
3.	Storage	20 GB SSD

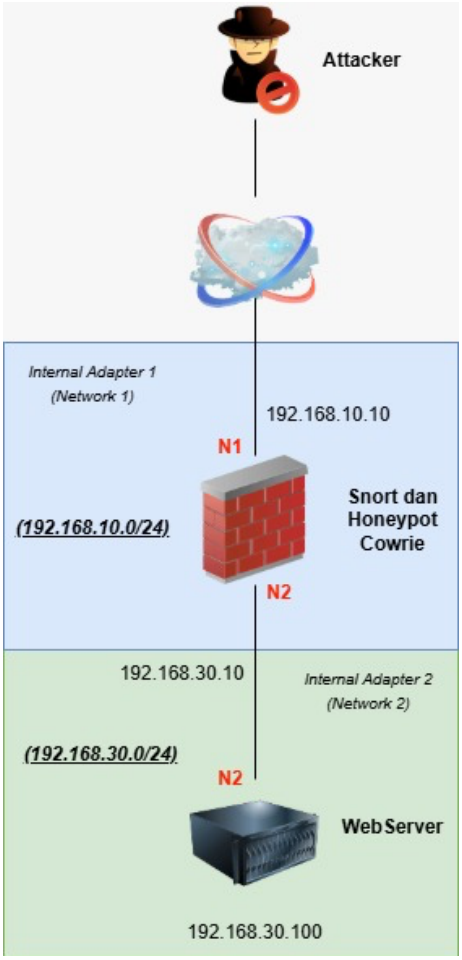
2. Software

Tabel 3.2 Analisis Software

No	Komponen	Software	Keterangan
1.	Cowrie Honeypot	The latest stable release of Cowrie.	Digunakan untuk mensimulasikan layanan SSH dan Telnet untuk menarik penyerang.
2.	Snort Inline-Mode	Versi 2.x atau 3.x.	Digunakan untuk mendeteksi dan memblokir serangan DDoS dan brute-force.
3.	OS (Server)	Debian 12/Ubuntu 24.	Sistem operasi yang mendukung instalasi Cowrie dan Snort secara stabil seperti Debian.
4.	Virtualization	Virtual Box 7.1.14.	Untuk menjalankan VM-server dan VM-attacker dalam lingkungan terisolasi.
5.	DDos/Brute-Force	Hydra, Hping3, Loic.	Digunakan untuk mensimulasikan serangan brute-force dan DDoS.

C. Perancangan Sistem

Untuk mengimplementasikan Cowrie Honeypot dan Snort Inline-Mode dalam mendeteksi dan mencegah serangan Brute-Force dan DDoS menggunakan VirtualBox, perancangan sistem ini mencakup beberapa tahapan penting, yaitu penyiapan mesin virtual (VM), konfigurasi jaringan, serta pengujian dan monitoring. Tujuan utama dari perancangan ini adalah untuk mensimulasikan kondisi serangan dalam lingkungan virtual yang terkontrol, sehingga dapat mengevaluasi efektivitas kedua teknologi tersebut dalam mendeteksi dan mengatasi serangan yang terjadi.



Gambar 3.2 Perancangan Sistem

D. Perancangan Pengujian

Tahap terakhir adalah menyimpulkan hasil penelitian

berdasarkan analisis yang telah dilakukan.

Tabel 3.3 Perancangan Pengujian

No	Parameter Uji	Keterangan
1.	Detection Rate	Mengukur persentase serangan yang berhasil dideteksi oleh sistem dari total serangan yang dilakukan. Semakin tinggi nilainya, semakin baik kemampuan deteksi sistem.
2.	Prevention Rate	Mengukur persentase serangan yang berhasil dicegah oleh sistem agar tidak mencapai target atau tidak berdampak. Menunjukkan efektivitas sistem dalam menghentikan serangan.
3.	Accuracy	Mengukur ketepatan sistem dalam membedakan antara lalu lintas normal dan serangan. Dihitung berdasarkan perbandingan True Positive, False Positive, True Negative, dan False Negative.
4.	Resource Usage	Resource Usage Mengukur penggunaan sumber daya seperti CPU, RAM, dan bandwidth selama proses deteksi dan pencegahan serangan berlangsung.
5.	Availability	Mengukur sejauh mana sistem tetap dapat memberikan layanan secara normal meskipun sedang mengalami serangan, terutama dalam konteks DDoS.

III HASIL DAN PEMBAHASAN

1. Instalasi Network Adapter Virtual Box

Tabel 4.1 Network Adapter Virtual

No	VM	Net 1	Net 2	Net 3
1.	Attacker	Nat Network	Internal Network (N1)	-
2.	Snort dan Cowrie	Nat Network	Internal Network (N1)	Internal Network (N2)
3.	WebServer	Nat Network	Internal Network (N1)	-

Arsitektur jaringan dalam penelitian ini terdiri dari tiga Virtual Machine (VM) yang saling terhubung melalui beberapa jaringan virtual. VM pertama adalah Attacker, yang terhubung ke Internal Network (N1) dan berfungsi untuk melakukan simulasi serangan terhadap sistem, seperti brute-force SSH dan DDoS yang ditargetkan ke WebServer serta Cowrie Honeypot. VM kedua adalah Snort dan Cowrie, yang berperan sebagai sistem deteksi dan pencegahan serangan. VM ini memiliki dua antarmuka jaringan, yaitu Internal Network (N1) untuk memantau lalu lintas jaringan utama dan Internal Network (N2) sebagai jaringan terisolasi tempat Cowrie Honeypot dijalankan. VM ketiga adalah WebServer, yang terhubung ke Internal Network (N1) dan berfungsi sebagai target potensial dalam pengujian serangan.

Dalam arsitektur ini, Snort dikonfigurasi dalam mode inline, yang memungkinkan sistem untuk tidak hanya mendeteksi tetapi juga mencegah serangan yang terjadi di jaringan. Snort dipasang di antara N1 dan N2, sehingga semua lalu lintas yang melewati kedua jaringan ini dapat diperiksa. Jika Snort mendeteksi aktivitas mencurigakan, seperti percobaan login SSH yang berulang atau peningkatan jumlah paket SYN dalam waktu singkat sebagai indikasi serangan SYN Flood DDoS, Snort akan secara otomatis memblokir lalu lintas yang mencurigakan atau menerapkan aturan mitigasi lainnya sebelum mencapai target.

Sementara itu, Cowrie Honeypot ditempatkan di jaringan terisolasi (N2) dengan tujuan untuk menjebak penyerang yang mencoba mengeksploitasi layanan seperti SSH atau Telnet. Honeypot ini dikonfigurasi agar menyerupai sistem asli, sehingga penyerang tertarik untuk berinteraksi dengannya. Setiap aktivitas yang dilakukan oleh penyerang, seperti percobaan login dan perintah yang dijalankan, akan direkam secara detail. Data ini dapat digunakan untuk menganalisis pola serangan dan membantu meningkatkan aturan deteksi Snort, sehingga sistem keamanan dapat berkembang seiring dengan metode serangan yang semakin canggih.

Attacker dalam penelitian ini digunakan untuk melakukan serangan berbasis brute-force SSH dan DDoS. Dalam serangan brute-force, Attacker mencoba berbagai kombinasi username dan password untuk mendapatkan akses ke Cowrie Honeypot atau WebServer. Sementara dalam serangan DDoS, Attacker membanjiri jaringan dengan lalu lintas palsu untuk menguji ketahanan sistem. Snort kemudian mendeteksi pola serangan ini berdasarkan aturan yang telah dikonfigurasi. Jika Snort mendeteksi percobaan login SSH yang berulang dalam waktu singkat atau lalu lintas yang mencurigakan dalam jumlah besar, Snort akan memblokir alamat IP penyerang atau menjatuhkan paket berbahaya sebelum mencapai target.

Dengan mengintegrasikan Snort inline-mode dan Cowrie Honeypot, sistem ini memiliki keunggulan dalam mendeteksi serangan secara real-time dan mencegah dampaknya sebelum mencapai target utama. Selain itu, data yang dikumpulkan dari Cowrie Honeypot memberikan wawasan yang lebih dalam mengenai teknik yang digunakan oleh penyerang, yang kemudian dapat digunakan untuk memperbarui aturan deteksi Snort agar lebih efektif. Dengan adanya mekanisme ini, penelitian ini memberikan lingkungan pengujian yang aman dan terkendali untuk menguji efektivitas sistem deteksi dan pencegahan serangan siber.

2. Instalasi dan Konfigurasi Honeypot Cowrie

Pada implementasi Honeypot Cowrie, langkah instalasi

dan konfigurasi dilakukan secara terstruktur untuk memastikan sistem bekerja dengan baik dalam mendeteksi aktivitas mencurigakan di jaringan. Berikut adalah penjelasan untuk setiap langkah:

- Pengaturan IP

Pada implementasi Honeypot Cowrie, langkah instalasi dan konfigurasi dilakukan secara terstruktur untuk memastikan sistem bekerja secara optimal dalam mendeteksi aktivitas mencurigakan di jaringan. Salah satu aspek utama dalam konfigurasi adalah pengaturan IP pada VM yang menjalankan Snort dan Cowrie, yang memiliki dua interface jaringan. Interface pertama, enp0s3, dikonfigurasi dengan IP 192.168.10.10/24 dan terhubung ke Internal Network (N1). Interface kedua, enp0s8, memiliki IP 192.168.30.10/24 dan terhubung ke Internal Network (N2).

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.10.10/24
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.30.10/24
```

Gambar 4.1 IP Honeypot Cowrie

- Instal Dependensi Sistem

Sebelum instalasi Cowrie, dependensi sistem yang dibutuhkan seperti git, python3-venv, libssl-dev, libffi-dev, dan authbind diinstal menggunakan package manager.

```
sudo apt-get install git python3-venv libssl-
dev libffi-dev build-essential libpython3-dev
python3-minimal authbind
```

Gambar 4.2 Depedensi Cowrie

- Buat Akun Pengguna

Untuk meningkatkan keamanan, Cowrie dijalankan menggunakan akun pengguna non-root. Akun "cowrie" dibuat dengan hak akses terbatas menggunakan perintah adduser untuk mencegah eskalasi hak akses jika Honeypot dikompromikan.

```
sudo adduser --disabled-password cowrie
```

Gambar 4.3 Depedensi Cowrie

- Unduh Cowrie

Repositori Cowrie diunduh menggunakan git ke direktori pengguna "cowrie". Berkas-berkas ini berisi kode sumber Cowrie dan konfigurasi default yang akan dikustomisasi sesuai kebutuhan.

```
git clone http://github.com/cowrie/cowrie
```

Gambar 4.4 Unduh Cowrie

- Siapkan Lingkungan Virtual

Lingkungan Python virtual dibuat menggunakan venv untuk mengisolasi dependensi Cowrie dari sistem utama. Setelah lingkungan aktif, semua pustaka Python yang dibutuhkan diinstal melalui berkas requirements.txt untuk memastikan kompatibilitas dan stabilitas system.

```
$ source cowrie-env/bin/activate
(cowrie-env) $ python -m pip install --upgrade pip
(cowrie-env) $ python -m pip install --upgrade -r requirements.txt
```

Gambar 4.5 Lingkungan Virtual

- Instal Berkas Konfigurasi

Berkas konfigurasi cowrie.cfg disiapkan berdasarkan template cowrie.cfg.dist. Pengaturan ini mencakup konfigurasi port, protokol (SSH dan telnet), serta pengaturan lainnya untuk menciptakan ilusi server yang menarik bagi penyerang.

```
[telnet]
enabled = true

[ssh]
listen_port = 22

[telnet]
enabled = true
listen_port = 23
```

Gambar 4.6 Konfigurasi cowrie

- Monitoring pada Port 22

Agar Cowrie dapat memantau koneksi SSH pada port 22, dilakukan pengalihan port menggunakan iptables atau authbind. Langkah ini memastikan Cowrie dapat menerima koneksi yang biasanya ditujukan ke layanan SSH asli tanpa menjalankan Cowrie sebagai pengguna root.

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 222
sudo iptables -t nat -A PREROUTING -p tcp --dport 23 -j REDIRECT --to-port 2223
```

Gambar 4.7 Monitoring port cowrie

- Mulai Cowrie

Cowrie dijalankan menggunakan perintah bin/cowrie start, yang mengaktifkan lingkungan virtual dan memulai layanan Honeypot. Honeypot ini mulai mencatat semua aktivitas masuk, termasuk serangan brute-force atau aktivitas mencurigakan lainnya, ke dalam log untuk analisis lebih lanjut.

```
bin/cowrie start
```

Gambar 4.8 Mulai cowrie

3. Instalasi dan Konfigurasi Snort *Inline-Mode*

Pengaturan IP pada mesin virtual yang menjalankan Snort dilakukan untuk menghubungkannya dengan komponen lain di jaringan (seperti Honeypot, Web Server, dan Attacker).

- Pengaturan IP

IP untuk setiap adapter diatur secara manual dalam file konfigurasi jaringan sistem operasi.

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.10.10/24
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.30.10/24
```

Gambar 4.9 IP snort

- Pengaturan Nginx

Nginx digunakan sebagai web server untuk memberikan layanan HTTP yang menjadi target serangan simulasi. Konfigurasi ini memungkinkan Snort untuk menganalisis lalu lintas HTTP dan mendeteksi ancaman pada level aplikasi.

```
sudo apt update && apt upgrade -y
sudo apt install -y nginx
```

Gambar 4.10 Pengaturan nginx

File konfigurasi default Nginx diubah untuk memastikan layanan dapat diakses melalui jaringan internal network untuk ip 192.168.10.10 (N1).

```
server {
    listen 80;
    server_name 192.168.10.10;

    location / {
        proxy_pass http://192.168.30.100;
        proxy_set_header Host \$host;
        proxy_set_header X-Real-IP \$remote_addr;
    }
}
```

Gambar 4.11 Konfigurasi nginx

Dengan pengaturan ini, Snort dan Cowrie dapat beroperasi secara bersamaan melalui web server Nginx, memungkinkan pemantauan dan respons terhadap aktivitas jaringan berbahaya secara lebih terorganisir dan terpusat.

```
ln -sf $NGINX_CONF_SNORT /etc/nginx/sites-enabled/snort
```

Gambar 4.12 Aktifkan Konfigurasi

Jalankan dan uji layanan Nginx.

```
sudo rm -f /etc/nginx/sites-enabled/default

sudo systemctl restart nginx
```

Gambar 4.13 Menjalankan nginx

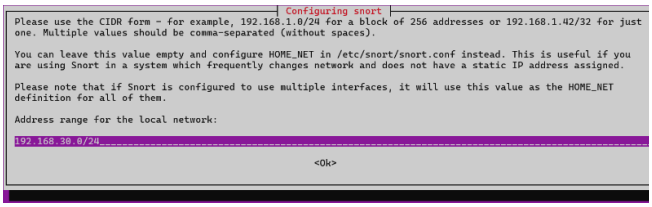
- Pengaturan Snort

Snort dikonfigurasi dalam mode inline untuk memonitor dan memblokir lalu lintas mencurigakan secara real-time. Update dan instalasi snort.

```
sudo apt update && apt upgrade -y
sudo apt install -y snort iptables-persistent
```

Gambar 4.14 Install snort

Masukkan ip internal dari webserver yaitu 192.168.30.0/24.



Gambar 4.15 Konfigurasi ip $Home snort

Menambahkan rules untuk deteksi Brute-Force dan Ddos.

```
drop tcp any any -> \$HOME_NET 22 (msg:"SSH Brute-Force Blocked";
flow:to_server,established; detection_filter:track by_src, count 5, seconds 60;
sid:1000001; rev:2;)
```

Gambar 4.16 Brute force rules

```
drop tcp any any -> \$HOME_NET 80 (msg:"HTTP Flood Detected and Blocked"; flags:S;
threshold:type both, track by_dst, count 20, seconds 5; sid:1000002; rev:2
```

Gambar 4.17 DDoS rules

Lalu aktifkan inline-mode

```
sudo snort -Q --daq afpacket -i enp0s3:enp0s8 -c /etc/snort/snort.conf
```

Gambar 4.18 Inline mode

Start snort

```
sudo systemctl start snort
```

Gambar 4.19 Menyalakan snort

4. Instalasi dan Konfigurasi WebServer
   - Pengaturan IP

Pengaturan IP dilakukan untuk memastikan bahwa server web dapat diakses melalui jaringan yang ditentukan. Pada sistem dengan antarmuka jaringan tertentu, alamat IP diberikan secara manual atau melalui DHCP sesuai topologi jaringan.

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.30.100/24
```

Gambar 4.20 IP webserver

- Update Sistem dan Instalasi Apache

Apache digunakan sebagai server web untuk melayani permintaan HTTP. Langkah pertama adalah memperbarui paket sistem agar sistem memiliki versi perangkat lunak terbaru, kemudian instal apache.

```
apt update && apt upgrade -y
apt install -y apache2
```

Gambar 4.21 Instalasi apache

- Pembuatan Direktori Root Web Server

Direktori root adalah tempat penyimpanan file-file yang akan disajikan oleh server web.

```
sudo mkdir -p /var/www/ecommerce
```

Gambar 4.22 Direktori webserver

- Pengaturan Hak Akses Direktori

Agar server Apache dapat membaca dan menulis file di direktori root web, hak akses harus dikonfigurasi.

```
chown -R www-data:www-data /var/www/ecommerce
chmod -R 755 /var/www/ecommerce /var/www/ecommerce
```

Gambar 4.23 Pengaturan hak akses

- Pembuatan File Konfigurasi Apache

File konfigurasi Apache dibuat untuk mendefinisikan virtual host, yang memungkinkan server melayani beberapa domain atau aplikasi dari satu server. Buat file konfigurasi baru seperti pada gambar .

```
<VirtualHost *:80>
    ServerName $SERVER_NAME
    DocumentRoot $WEB_ROOT

    <Directory $WEB_ROOT>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog \${APACHE_LOG_DIR}/ecommerce_error.log
    CustomLog \${APACHE_LOG_DIR}/ecommerce_access.log combined
</VirtualHost>
EOL
```

Gambar 4.24 Konfigurasi apache

- Aktivasi Konfigurasi Apache

Aktivasi konfigurasi dilakukan dengan menjalankan perintah berikut.

```
a2ensite ecommerce.conf
a2enmod rewrite
```

Gambar 4.25 Konfigurasi apache

- Restart Layanan Apache

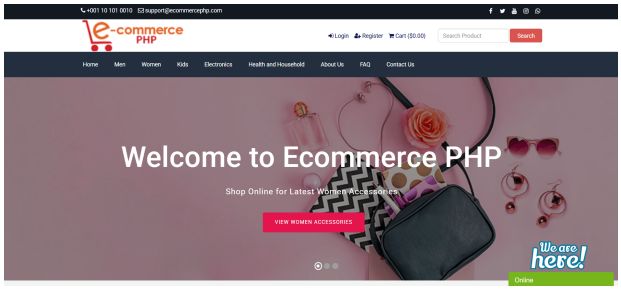
Setelah semua konfigurasi selesai, layanan Apache perlu dimulai ulang agar perubahan diterapkan.

```
sudo systemctl restart apache2
```

Gambar 4.26 Restart apache

- Output Final

Setelah semua langkah selesai, akses server web melalui browser dengan mengetikkan alamat IP atau nama domain.



Gambar 4.27 Output webserver

III. KESIMPULAN

A. *Kesimpulan*

Berdasarkan hasil pengujian yang dilakukan, sistem keamanan jaringan yang menggunakan kombinasi Cowrie Honeypot dan Snort Inline-Mode menunjukkan kinerja yang sangat baik dalam mendeteksi dan mencegah berbagai jenis serangan seperti Brute Force SSH dan DDoS. Pengujian detection rate membuktikan bahwa sistem mampu mendeteksi 100% dari seluruh jumlah serangan yang diluncurkan, baik pada skenario 50, 100, maupun 150 percobaan. Prevention rate juga mencapai 100% untuk serangan Brute Force dan sebagian besar serangan DoS, meskipun pada interval serangan DoS sebesar 60 detik sistem tidak mampu mencegah serangan karena frekuensinya yang rendah. Hasil pengujian accuracy menunjukkan bahwa sistem memiliki tingkat akurasi 100%, tanpa adanya false positive maupun false negative, artinya semua aktivitas normal dikenali sebagai aman dan semua serangan berhasil terdeteksi. Selain itu, penggunaan sumber daya (resource usage) tetap efisien, di mana dengan implementasi Snort dan Cowrie, beban CPU pada server utama turun drastis dari 60,68% menjadi hanya 1,09% saat serangan terjadi. Terakhir, pengujian availability membuktikan bahwa sistem dengan Snort dan Cowrie mampu menjaga ketersediaan layanan hingga 99,36%, meningkat sebesar 4,22% dibandingkan tanpa sistem keamanan. Secara keseluruhan, integrasi Cowrie Honeypot dan Snort Inline-Mode sangat efektif dalam meningkatkan keamanan jaringan serta menjaga stabilitas dan ketersediaan layanan.

B. *Saran*

Berdasarkan temuan dan kesimpulan penelitian, berikut adalah beberapa saran untuk pengembangan dan peningkatan sistem keamanan jaringan di masa depan. Meskipun Snort telah menunjukkan efektivitas yang tinggi, aturan deteksi dapat terus diperbarui dan disesuaikan dengan pola serangan terbaru. Penambahan aturan khusus untuk serangan zero-day atau teknik serangan yang lebih canggih dapat meningkatkan kemampuan sistem. Selain itu, optimasi penggunaan sumber daya dapat dilakukan dengan memanfaatkan teknologi seperti load balancing atau clustering untuk mendistribusikan beban kerja Snort dan Cowrie ke beberapa node.

Sistem juga dapat diintegrasikan dengan teknologi keamanan lain seperti Firewall, SIEM (Security Information and Event Management), atau Machine Learning-based IDS untuk meningkatkan kemampuan analisis dan respons terhadap ancaman yang lebih kompleks. Pengujian lebih lanjut dapat dilakukan pada jaringan yang lebih besar dan kompleks untuk mengevaluasi skalabilitas sistem, mengingat penelitian ini dilakukan dalam lingkungan virtual yang terbatas.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan nikmat iman, kesehatan, serta kekuatan yang diberikan sehingga penelitian ini dapat terselesaikan dengan baik. Shalawat dan salam semoga senantiasa tercurah kepada junjungan kita Nabi Muhammad SAW.

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada dosen pembimbing atas segala bimbingan dan arahan yang telah diberikan selama proses penelitian berlangsung. Ucapan terima kasih juga penulis sampaikan kepada kedua orang tua, serta seluruh keluarga atas doa, dukungan, dan semangat yang tiada henti hingga penelitian ini dapat diselesaikan dengan baik. Terimakasih juga pada seluruh tim pengelola jurnal JIEET.

REFERENSI

[1] [1] M. AbdulRaheem, I. D. Oladipo, A. L. Imoize, J. B. Awotunde, C. C. Lee, G. B. Balogun, dan J. O. Adeoti, "Machine learning assisted Snort and Zeek in detecting DDoS attacks in software-defined networking," *Int. J. Inf. Technol. (Singapore)*, vol. 16, no. 3, hal. 1627–1643, 2024. [Online]. Tersedia: https://doi.org/10.1007/s41870-023-01469-3

[2] [2] T. E. Ali, Y. W. Chong, dan S. Manickam, "Machine learning techniques to detect a DDoS attack in SDN: A systematic review," *Appl. Sci. (Switzerland)*, vol. 13, no. 5, 2023. [Online]. Tersedia: https://doi.org/10.3390/app13053183

[3] [3] A. Alnajim, F. Alotaibi, dan S. Khan, "Mitigating distributed denial of service attacks in software-defined networking," *Preprints*, 2024. [Online]. Tersedia: https://doi.org/10.20944/preprints202409.0641.v1

[4] [4] N. Alotibi dan M. Alshammari, "Deep learning-based intrusion detection: A novel approach for identifying brute-force attacks on FTP and SSH protocol," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 14, no. 6, 2023. [Online]. Tersedia: www.ijacsa.thesai.org

[5] [5] B. Arifwidodo, Y. Syuhada, dan S. Ikhwan, "Analisis kinerja Mikrotik terhadap serangan brute force dan DDoS," *Agustus*, vol. 20, no. 3, 2021.

[6] [6] T. Ernawati dan F. F. F. Rachmat, "Keamanan jaringan dengan Cowrie honeypot dan Snort inline-mode sebagai intrusion prevention system," *J. RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, hal. 180–186, 2021. [Online]. Tersedia: https://doi.org/10.29207/resti.v5i1.2825

[7] [7] A. I. Haq dan B. Santoso, "Analisis perbandingan performa metode ELK Stack dan Grafana Loki pada honeypot server," *J. Sisfokom (Sistem Informasi dan Komputer)*, vol. 10, no. 3, hal. 376–385, 2021. [Online]. Tersedia: https://doi.org/10.32736/sisfokom.v10i3.1177

[8] [8] M. W. Marzuqon dan A. Prihanto, "Analisis perbandingan behavior user menggunakan low interaction honeypot dan IDS pada sistem edge computing," 2022.

[9] [9] T. Natanegara, Y. Muhyidin, dan D. Singasatia, "Implementasi honeypot Cowrie dan Snort sebagai alat deteksi serangan pada server," 2023.

[10] [10] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, dan J. Zhao, "A highly interactive honeypot-based approach to network threat management," *Future Internet*, vol. 15, no. 4, 2023. [Online]. Tersedia: https://doi.org/10.3390/fi15040127