BAB 1 PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, keamanan jaringan menjadi salah satu aspek krusial bagi organisasi, perusahaan, dan individu. Serangan siber seperti brute-force attack, malware injection, dan eksploitasi sistem semakin meningkat, mengancam data dan infrastruktur penting. Seiring dengan berkembangnya teknologi, serangan siber menjadi semakin canggih dan sulit dideteksi oleh sistem pertahanan tradisional. Oleh karena itu, diperlukan metode yang lebih efektif dalam mendeteksi dan memahami pola serangan yang dilakukan oleh peretas.Salah satu cara yang efektif untuk memantau dan menganalisis serangan siber adalah dengan menggunakan honeypot.

Honeypot adalah sistem yang sengaja dirancang untuk menarik perhatian peretas, agar mereka melakukan serangan yang dapat dipantau dan dianalisis. Data yang diperoleh dari honeypot ini memungkinkan kita untuk mengetahui teknik dan alat yang digunakan peretas, serta memberikan wawasan yang berharga untuk meningkatkan sistem pertahanan.Cowrie adalah salah satu jenis honeypot low-interaction yang dirancang khusus untuk mensimulasikan layanan SSH (Secure Shell) dan Telnet. Honeypot ini dapat mencatat percakapan login, perintah yang dijalankan oleh peretas, serta alamat IP penyerang.

Dengan memanfaatkan Cowrie, kita dapat lebih memahami bagaimana peretas mencoba menembus sistem, serta memperoleh informasi yang dapat digunakan untuk memperkuat keamanan jaringan yang sebenarnya.Penelitian ini bertujuan untuk mengimplementasikan honeypot Cowrie dalam lingkungan Debian dan menganalisis pola serangan yang terjadi. Dengan demikian, penelitian ini dapat memberikan wawasan tentang bagaimana peretas bekerja dan bagaimana kita dapat meningkatkan keamanan sistem berdasarkan data yang diperoleh dari honeypot.

1.2 Cara Kerja Honeypot

Honeypot bekerja dengan cara memikat peretas untuk menyerang sistem yang tampak sebagai sistem yang rentan. Setelah peretas masuk ke dalam honeypot, sistem ini akan memantau dan merekam setiap aktivitas yang dilakukan. Data yang dikumpulkan dari honeypot berupa log aktivitas dapat memberikan informasi tentang teknik yang digunakan oleh

peretas, alat yang digunakan dalam serangan, serta pola serangan yang sering dilakukan.Beberapa fungsi utama honeypot adalah

1. Deteksi Serangan Dini (Early Detection): Honeypot dapat mendeteksi serangan yang mencoba mengeksploitasi kerentanannya lebih awal, sebelum serangan tersebut mencapai sistem yang lebih penting.
2. Pengumpulan Data Serangan: Honeypot dapat mengumpulkan data mengenai teknik dan alat yang digunakan oleh peretas, yang berguna untuk meningkatkan pertahanan sistem.
3. Mengalihkan Peretas dari Sistem Asli: Dengan menarik perhatian peretas ke honeypot, kita dapat melindungi sistem yang sebenarnya dari serangan langsung.

Cowrie, sebagai honeypot low-interaction, memiliki fungsi utama untuk mensimulasikan layanan SSH dan Telnet yang umum digunakan oleh peretas untuk melakukan serangan. Dengan menggunakan Cowrie, kita dapat merekam setiap usaha login yang dilakukan oleh peretas, perintah yang dijalankan, serta alamat IP yang digunakan, yang dapat digunakan untuk menganalisis pola serangan yang sering terjadi.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka penelitian ini akan berfokus pada beberapa permasalahan seperti di bawah

1. Bagaimana cara mengimplementasikan honeypot Cowrie pada sistem berbasis Debian?
2. Bagaimana cara menguji serangan terhadap honeypot Cowrie untuk memastikan fungsionalitasnya?
3. Apa saja pola serangan yang ditemukan berdasarkan data yang dikumpulkan dari honeypot Cowrie?
4. Bagaimana hasil analisis data dari honeypot ini dapat digunakan untuk meningkatkan keamanan jaringan?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini akan dijelaskan dibawah

1. Menginstal dan Mengonfigurasi Honeypot Cowrie pada Sistem Debian:

   Melakukan instalasi dan konfigurasi honeypot Cowrie pada sistem operasi berbasis Debian, dengan penyesuaian yang diperlukan untuk menjamin fungsionalitas yang optimal

dalam mendeteksi dan mencatat serangan yang dilakukan melalui SSH dan Telnet. Hal ini meliputi konfigurasi sistem dan penyesuaian terkait log untuk analisis lebih lanjut.

2. Melakukan Simulasi Serangan terhadap Cowrie untuk Menguji Fungsionalitasnya:

   Melakukan serangkaian pengujian, baik dengan serangan yang sudah dikenal seperti brute-force attack maupun serangan baru, untuk memastikan bahwa honeypot Cowrie berfungsi dengan baik dalam menangkap percakapan peretas, perintah yang dijalankan, dan informasi lain yang relevan.

3. Menganalisis Data Serangan yang Tercatat dalam Log Cowrie:

   Menganalisis hasil log yang dihasilkan oleh Cowrie untuk menemukan pola-pola serangan yang umum atau berulang, serta teknik peretas yang sering digunakan. Analisis ini juga akan meliputi identifikasi alamat IP sumber serangan, waktu serangan, serta perintah-perintah yang paling sering dieksekusi.

4. Memberikan Rekomendasi untuk Meningkatkan Keamanan Sistem Berdasarkan Hasil Analisis Honeypot:

   Menggunakan wawasan yang diperoleh dari analisis honeypot untuk memberikan rekomendasi yang dapat digunakan oleh administrator sistem dalam meningkatkan keamanan jaringan mereka, baik dengan mengoptimalkan konfigurasi yang ada maupun dengan menambahkan lapisan pertahanan baru.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat

Manfaat Akademik:

1. Menambah Wawasan tentang Penggunaan Honeypot dalam Riset Keamanan Siber:

   Penelitian ini memberikan kontribusi baru dalam memahami penerapan honeypot khususnya Cowrie dalam pengujian serangan terhadap sistem SSH dan Telnet. Hal ini dapat menjadi sumber informasi bagi akademisi dan peneliti yang ingin mengembangkan penelitian lanjutan terkait honeypot dan analisis serangan.

2. Memberikan Referensi bagi Mahasiswa atau Peneliti yang Ingin Mendalami Honeypot dan Analisis Serangan Siber:

   Hasil penelitian ini dapat digunakan sebagai referensi bagi mahasiswa atau peneliti yang tertarik untuk memahami cara kerja honeypot dalam mendeteksi dan menganalisis serangan siber, serta implementasi praktisnya dalam mengamankan sistem informasi.

Manfaat Praktis:

1. Membantu Administrator Jaringan dalam Mendeteksi dan Memahami Pola Serangan pada Layanan SSH:

   Dengan menggunakan honeypot Cowrie, penelitian ini dapat membantu administrator jaringan untuk mengidentifikasi serangan yang biasanya tidak terdeteksi oleh sistem pertahanan tradisional, memberikan wawasan yang lebih dalam mengenai teknik yang digunakan oleh peretas.
2. Memberikan Insight tentang Bagaimana Peretas Bekerja untuk Meningkatkan Keamanan Sistem yang Sebenarnya:

   Penelitian ini memberikan gambaran lebih jelas tentang metode dan alat yang digunakan peretas, yang dapat membantu organisasi atau individu dalam memperkuat perlindungan mereka dari ancaman yang mungkin belum terdeteksi oleh sistem pertahanan mereka.
3. Menjadi Referensi bagi Organisasi atau Perusahaan dalam Menggunakan Honeypot sebagai Sistem Deteksi Dini (Intrusion Detection System - IDS):

   Hasil penelitian ini dapat menjadi panduan bagi organisasi atau perusahaan dalam memanfaatkan honeypot sebagai sistem deteksi dini untuk mengidentifikasi dan menangkal serangan sebelum berdampak pada sistem yang lebih penting.

1.6 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini dibatasi pada implementasi honeypot Cowrie pada sistem operasi berbasis Debian untuk tujuan analisis serangan siber. Penelitian ini hanya akan memfokuskan pada serangan yang dilakukan melalui layanan SSH dan Telnet, dengan menggunakan Cowrie sebagai honeypot low-interaction yang bertugas untuk mensimulasikan layanan-layanan tersebut. Berikut adalah beberapa batasan ruang lingkup penelitian ini:

1. Lingkup Sistem Operasi**:** Penelitian ini akan berfokus pada implementasi dan konfigurasi honeypot Cowrie pada sistem operasi berbasis Debian. Pengujian dan analisis tidak mencakup sistem operasi lain seperti Windows atau distribusi Linux lainnya.
2. Jenis Honeypot**:** Honeypot yang digunakan dalam penelitian ini adalah Cowrie, yang merupakan honeypot tipe low-interaction yang mensimulasikan layanan SSH dan Telnet. Penelitian ini tidak mencakup jenis honeypot lain seperti honeypot high-interaction atau honeypot yang dirancang untuk layanan lainnya.

3. Jenis Serangan**:** Penelitian ini akan memfokuskan pada analisis serangan yang dilakukan melalui metode brute-force, eksploitasi login, serta percakapan-percakapan yang dilakukan dalam sistem SSH dan Telnet. Penelitian ini tidak mencakup serangan yang menggunakan metode lain di luar lingkup tersebut.
4. Data yang Diperoleh**:** Fokus penelitian ini adalah pada data yang dikumpulkan dari log aktivitas yang tercatat oleh Cowrie, termasuk percakapan login, perintah yang dijalankan oleh peretas, serta alamat IP penyerang. Penelitian ini tidak akan membahas analisis lebih lanjut terhadap data lain di luar data yang tercatat dalam log Cowrie.
5. Tujuan Penelitian**:** Penelitian ini bertujuan untuk menganalisis pola serangan yang terjadi berdasarkan data yang dikumpulkan oleh Cowrie dan memberikan rekomendasi untuk meningkatkan keamanan sistem berdasarkan analisis tersebut. Penelitian ini tidak membahas upaya mitigasi serangan atau pengembangan teknologi pertahanan lainnya.

Dengan batasan-batasan tersebut, penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai efektivitas honeypot Cowrie dalam mendeteksi dan menganalisis pola serangan yang terjadi pada layanan SSH dan Telnet dalam lingkungan Debian.