ANALISA PENERAPAN *HONEYPOT* COWRIE DAN IPS UNTUK MENINGKATKAN KEAMANAN WEB SERVER

Ardi Rusli, Husain, Lilik Widyawati, Muhammad Awzar, Muhammad Innudin

Universitas Bumigora, Mataram, Indonesia

Correspondence : *e-mail*: Ardylonk3@gmail.com

Abstrak

Perkembangan teknologi jaringan yang pesat membawa tantangan baru dalam menjaga keamanan sistem, khususnya pada web server yang rentan terhadap berbagai serangan siber. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan Honeypot Cowrie dan Intrusion Prevention System (IPS) Suricata dalam mendeteksi serta mencegah serangan seperti brute force, port scanning, dan DDoS. Metode yang digunakan adalah Network Development Life Cycle (NDLC) yang terdiri dari tahapan identifikasi, analisis, desain, implementasi, dan evaluasi. Honeypot Cowrie berperan dalam mencatat aktivitas penyerang seperti login SSH palsu dan perintah berbahaya, sementara Suricata bertindak sebagai sistem pertahanan aktif terhadap lalu lintas mencurigakan. Hasil pengujian menunjukkan bahwa kombinasi Honeypot dan IPS mampu mendeteksi serangan secara real-time, mencatat data log secara detail, serta memberikan peringatan atau tindakan pencegahan secara otomatis. Dengan demikian, pendekatan integratif ini terbukti meningkatkan efektivitas sistem keamanan web server dari ancaman nyata yang semakin kompleks.

Kata kunci: Honeypot Cowrie, Suricata, IPS, Keamanan Jaringan, Web Server, Brute Force, DDoS.

Abstract

The rapid development of network technology brings new challenges in maintaining system security, especially on web servers which are vulnerable to various cyber attacks. This research aims to analyze the effectiveness of implementing Cowrie's Honeypot and Suricata's Intrusion Prevention System (IPS) in detecting and preventing attacks such as brute force, port scanning and DDoS. The method used is the Network Development Life Cycle (NDLC) which consists of the stages of identification, analysis, design, implementation and evaluation. Cowrie's Honeypot plays a role in logging attacker activity such as fake SSH logins and malicious commands, while Suricata acts as an active defense system against suspicious traffic. Test results show that the combination of Honeypot and IPS is able to detect attacks in real-time, record detailed log data, and provide warnings or preventative actions automatically. Thus, this integrative approach is proven to increase the effectiveness of the web server security system against increasingly complex real threats.

Keywords*: Cowrie Honeypot, Suricata, IPS, Network Security, Web Server, Brute Force, DDoS.*

1. Pendahuluan

Perkembangan Teknolologi jaringan terutama system keamanan jaringan yang semakin berkembang menuntut agar system keamanan untuk berkembang, terutama pada keamanan server yang merupakan salah satu tugas pokok dari *system* administrator.[1] Hal ini didasarkan pada karakteristik umum dari jaringan komputer yang pada dasarnya adalah tidak aman untuk diakses secara bebas. Terbukanya port untuk layanan yang bersifat *public* maupun bersifat *private*, memiliki kemungkinan resiko yang tinggi untuk diserang oleh para *hacker*.[2] Untuk mengatasi hal tersebut maka dibutuhkan sebuah keamanan yang dapat menjaga jaringan server dari *hacker*.[3] Salah satu keamanan yang digunakan adalah penerapan *Honeypot*, yaitu sistem buatan yang meniru jaringan asli dan bertujuan untuk menarik, memantau, dan mencatat aktivitas penyerang.[4]*Cowrie* adalah salah satu jenis *honeypot* berbasis *SSH* dan Telnet yang bersifat interaktif, dan mampu mencatat percobaan login serta perintah yang dijalankan oleh pelaku.[5]

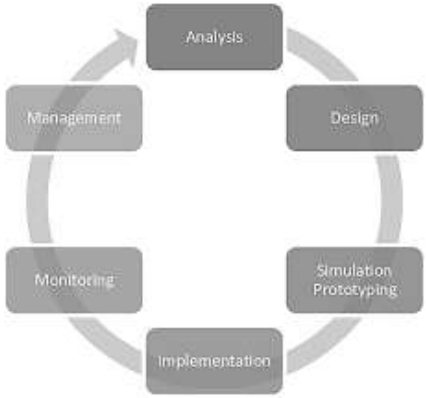
Selain mencatat data, *honeypot* juga berfungsi sebagai sistem observasi untuk memahami pola dan teknik serangan terkini.[6]

Untuk mendukung fungsi tersebut secara lebih reaktif, *Honeypot* dapat dikombinasikan dengan Intrusion Prevention System (IPS) seperti Suricata,[7] yang mampu menganalisis lalu lintas jaringan secara *real-time* dan melakukan tindakan otomatis saat mendeteksi ancaman. IPS memiliki keunggulan dibanding IDS karena tidak hanya mendeteksi, tetapi juga langsung mencegah dan memblokir serangan sebelum mencapai sistem target.[8]. Penelitian ini mengambil pendekatan integratif dengan menggabungkan *Honeypot Cowrie* dan Suricata IPS dalam sebuah lingkungan virtual web server.[5]Tujuannya adalah untuk menganalisis efektivitas sistem ini dalam mendeteksi dan mencegah serangan siber yang umum seperti *brute force, port scanning*, dan *DdoS.*[9]

Berdasarkan hasil pengujian yang dilakukan dalam penelitian ini, sistem *Honeypot Cowrie* berhasil mencatat berbagai aktivitas serangan yang nyata. Misalnya, saat dilakukan serangan *brute force* menggunakan tool *Hydra*, *honeypot* mencatat kombinasi login dan password yang dicoba oleh penyerang, termasuk perintah-perintah yang dijalankan setelah berhasil login ke *shell* palsu. Selain itu, saat dilakukan serangan port scanning menggunakan *Zenmap*, Cowrie mencatat IP penyerang, waktu kejadian, serta port mana saja yang dipindai. Serangan *DDoS* yang disimulasikan juga menyebabkan beban tinggi pada web server, dan aktivitas trafik yang tidak wajar ini berhasil dideteksi oleh sistem Suricata sebagai bagian dari IPS. Bukti-bukti ini menunjukkan pentingnya penerapan *honeypot* dan IPS dalam menjaga keamanan jaringan dari ancaman nyata. Dengan pendekatan ini, penelitian bertujuan untuk menunjukkan bahwa sistem keamanan berbasis *Honeypot Cowrie* dan IPS tidak hanya efektif untuk mendeteksi ancaman, tetapi juga dapat menjadi solusi preventif dan adaptif dalam menghadapi serangan nyata terhadap *web server.*

2. Metode Penelitian

Dalam penelitian ini, penulis menggunakan pendekatan terhadap model Network Development Life Cycle (NDLC). NDLC mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. Kata cycle merupakan kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara keseluruhan proses dan tahapan pengembangan sistem jaringan yang berkesinambungan.[10]



Gambar 1 metodologi NDLC

NDLC dijadikan metode yang digunakan sebagai acuan (secara keseluruhan atau secara garis besar) pada proses pengembangan dan perancangan sistem jaringan komputer. Metode Perancangan yang penulis gunakan *adalah Network Development Life Cycle (NDLC)* yang merupakan suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang awal dan akhirnya dalam membangun sebuah jaringan komputer.[11]

Langkah-langkah yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

1. Analisis *(Analysis)*

   Tahap ini berfokus pada pengumpulan kebutuhan dan pemahaman terhadap masalah atau kebutuhan sistem yang akan dikembangkan.

2. *Design* (Perancangan)

Berdasarkan hasil analisis, dibuat desain sistem yang mencakup arsitektur, alur kerja, dan solusi teknis.

3. *Simulation / Prototyping* (Simulasi / Pembuatan Prototipe)

   Dilakukan simulasi atau pembuatan prototipe untuk menguji desain sebelum implementasi penuh. Tujuannya adalah untuk mengidentifikasi kesalahan lebih awal.

4. *Implementation* (Implementasi)

   Sistem yang telah dirancang dan diuji mulai diimplementasikan ke dalam lingkungan nyata.

5. *Monitoring* (Pemantauan)

   Sistem yang telah berjalan dipantau untuk memastikan bahwa kinerjanya sesuai dengan harapan dan tidak ada kesalahan.

6. Management (Manajemen / Evaluasi)

   Tahap ini mencakup pengelolaan, pemeliharaan, dan pengembangan lebih lanjut agar sistem tetap relevan dan optimal digunakan.

3. Hasil dan Pembahasan

Pada bagian ini akan dilakukan pengujian pada sistem yang telah dibuat. Pengujian sistem dilakukan dengan melakukan beberapa serangan untuk mengetahul apakah sistem dapat bekerja dengan baik.

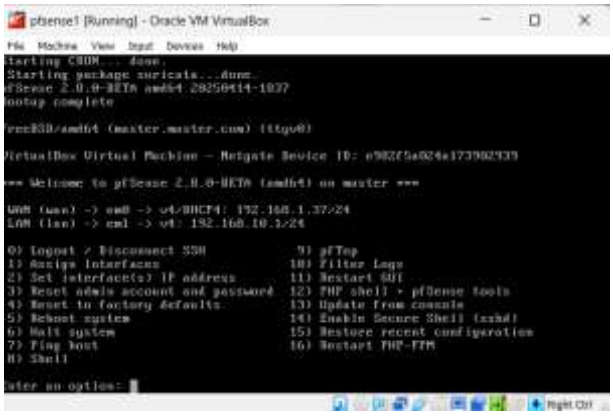
3.1. Konfigurasi

3.1.1. Konfigurasi Kali Linux

Gambar 2 konfigurasi kali linux

Gambar ini menampilkan tampilan layar login Kali Linux yang sedang berjalan di dalam Oracle VM VirtualBox. Kali Linux adalah sistem operasi berbasis Linux yang umum digunakan untuk keperluan pengujian keamanan dan penetration testing. Pada gambar terlihat antarmuka login dengan latar belakang bermotif labirin khas Kali Linux,

3.1.2. Konfigurasi Pfsense



Gambar 3 konfigurasi pfsense

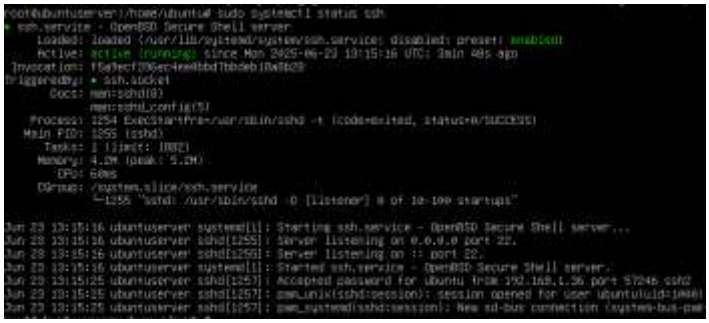
Gambar diatas tersebut menunjukkan tampilan antarmuka konsol dari sistem operasi pfSense versi 2.8.0-BETA yang sedang berjalan di dalam Oracle VM VirtualBox. pfSense adalah firewall dan router berbasis FreeBSD yang digunakan untuk mengelola jaringan dan keamanan. Pada layar ditampilkan berbagai opsi konfigurasi dasar seperti pengaturan alamat IP, reset password admin, reboot sistem, hingga akses ke shell.

3.1.3. Konfigurasi Ubuntu

Pada konfigurasi Ubuntu sebagai server keamanan jaringan, digunakan beberapa tools penting untuk mendukung proses deteksi dan analisis serangan. Salah satu tools utama yang digunakan adalah Cowrie, yaitu honeypot yang berfungsi sebagai server palsu untuk memancing dan merekam aktivitas penyerang, terutama melalui protokol SSH,Telnet dan Apache2.

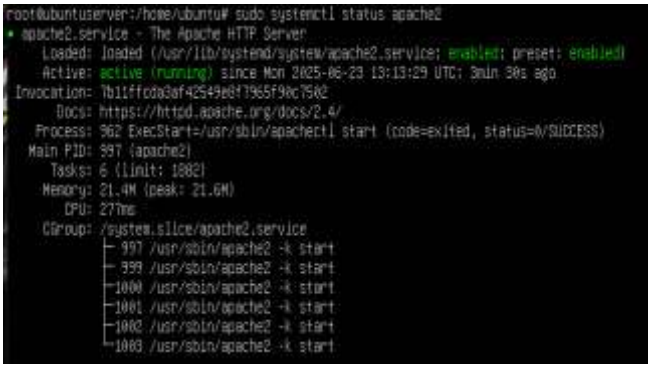
Gambar 4 honeypot cowrie

Gambar tersebut menunjukkan hasil perintah sudo systemctl status cowrie pada sistem Ubuntu, yang digunakan untuk memeriksa status layanan *Honeypot* Cowrie. Dari output terlihat bahwa layanan Cowrie sudah terinstal dan enabled.



Gambar 5 Status SSH

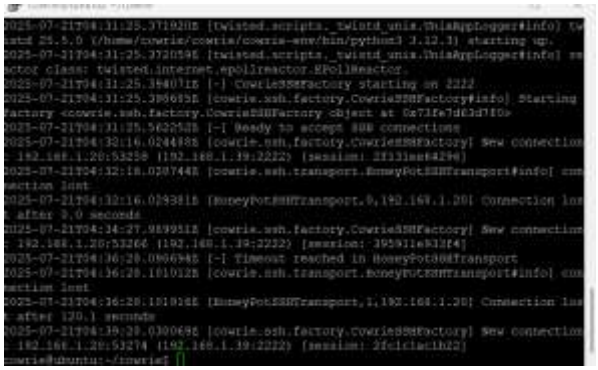
Gambar tersebut menunjukkan hasil perintah sudo systemctl status ssh pada sistem Ubuntu, yang digunakan untuk memeriksa status layanan SSH (Secure Shell). Dari output terlihat bahwa layanan SSH aktif dan berjalan dengan baik ditandai dengan status active (running).



Gambar 6 Status Apache2

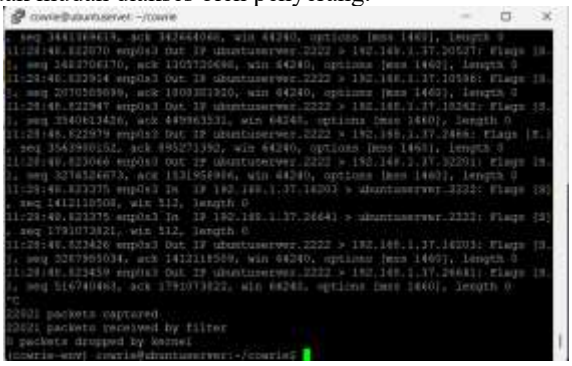
Gambar tersebut menunjukkan hasil perintah sudo systemctl status apache2 pada sistem Ubuntu, yang digunakan untuk memeriksa status layanan Apache2, yaitu web server HTTP. Dari informasi tersebut terlihat bahwa layanan Apache2 berhasil dijalankan dan aktif dengan status active (running).

3.2. Hasil/evaluasi



Gambar 7 Hasil port scaning

Pada gambar di atas peneliti menggunakan port 2222 karena saat ini sistem masih berbentuk simulasi, dan dikhawatirkan jika menggunakan port 22 akan berbenturan dengan port default SSH. Jika diimplementasikan untuk port cowrie bisa menggunakan port 22 karena akan berbeda device dengan server. Sehingga tidak ada tumpang tindih. Dan untuk keamanan, bagi pengguna internal disarankan menggunakan SSH yang berbeda agar tidak mudah diakses oleh penyerang.



Gambar 8 Hasil DDOS

Gambar ini menunjukkan peneliti ingin menyerang cowrie dilakukan dengan mengirimkan banyak paket TCP SYN ke target, maka IP nya sesuai dengan IP COWRIE.

Gambar 9 Hasil serangan Brute force

Pada gambar di atas menggunakan hydra, peneliti bisa mencari kombinasi user dan password yang digunakan pada server. Dalam pencariannya peneliti bisa melakukan secara satu persatu atau langsung membuat list berbentuk file .txt yang berisi rangkaian kata untuk user dan password.

Gambar 10 Log Cowrie

Gmabar di atas peneliti berhasil masuk ke dalam server tiruan cowrie. Sebenarnya server ini merupakan server jebakan dan segala aktivitas akan tercatat, seperti apa saja yang diketik atau dimasukan saat di dalam server tiruan cowne ini.

4. Kesimpulan

1. Penerapan Honeypot Cowrie dan IPS terbukti mampu mendeteksi serta merespons berbagai jenis serangan seperti port scanning, brute force, dan DDoS pada web server.
2. Honeypot Cowrie berhasil mencatat aktivitas penyerang, termasuk kombinasi login yang digunakan serta perintah yang dijalankan, sementara IPS (Suricata) memberikan perlindungan tambahan dengan memblokir lalu lintas yang mencurigakan secara real-time.
3. Integrasi kedua sistem ini meningkatkan efektivitas sistem keamanan web server secara signifikan, memungkinkan administrator mendeteksi dini ancaman serta merespons secara proaktif terhadap aktivitas berbahaya di jaringan.

Daftar Pustaka

[1] D. Yadewani and R. Wijaya, “Jurnal Resti,” *Resti*, vol. 1, no. 1, pp. 19–25, 2017.

[2] F. Faldi, D. Romadoni, and M. T. Sumadi, “the Implementation of Network Server Security System Using Honeypot,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, pp. 122–130, 2023, doi: 10.33387/jiko.v6i2.6385.

[3] T. Natanegara, Y. Muhyidin, and D. Singasatia, “6989-Article Text-27420-1-10-20231124,” *(Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 1871–1877, 2023.

[4] M. Iqbal, A.- Arini, and H. B. Suseno, “Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking, Honeypot, Iptables, Icmp,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 27–32, 2020, doi: 10.14421/csecurity.2020.3.1.1933.

[5] M. H. Siregar and R. Dermawati, “Implementasi Honeypot Pada Jaringan Internet Labor Fakultas

Teknik Uniks Menggunakan Dionaea Sebagai Keamanan Jaringan," *Edutic - Sci. J. Informatics Educ.*, vol. 7, no. 1, pp. 20–30, 2020, doi: 10.21107/edutic.v7i1.8660.

[6] Z. Fuada, "Penerapan Keamanan Jaringan Menggunakan Sistem Snort Dan Honeypot Sebagai Pendeteksi Dan Pencegah Malware Skripsi," pp. 1–55, 2023.

[7] M. Arman and N. Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020, doi: 10.32767/jusikom.v5i1.752.

[8] R. E. Susanti, A. W. Muhammad, and W. A. Prabowo, "Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 1, pp. 73–78, 2022, doi: 10.32736/sisfokom.v11i1.1246.

[9] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.

[10] R. Yulianto and F. Aprilyani, "Sistem Keamanan Jaringan Komputer Menggunakan Metode NDLC Dengan Linux Zentyal Pada Instansi KEMENKO Maritim," *J. Tek. Inform. Stmik Antar Bangsa*, vol. VI, no. 2, pp. 79–86, 2020.

[11] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.