PENGEMBANGAN SISTEM KEAMANAN JARINGAN WIRELESS BERBASIS HONEY NETWORK DAN IDS DENGAN PENTBOX

Muhlis Tahir[1], Alvin Kamil[2], Aurellia Maharani Putri[3]
muhlis.tahir@trunojoyo.ac.id[1], 220631100006@student.trunojoyo.ac.id[2],
220631100108@student.trunojoyo.ac.id[3]
Universitas Trunojoyo Madura

ABSTRAK

Perkembangan jaringan wireless di lingkungan pendidikan membawa kemudahan akses namun juga meningkatkan risiko serangan siber seperti brute-force, spoofing, dan Denial of Service (DoS). SMKN 3 Bangkalan sebagai sekolah berbasis teknologi masih memiliki keterbatasan sistem keamanan sehingga rentan terhadap intrusi. Penelitian ini bertujuan mengembangkan dan menguji prototipe sistem keamanan jaringan wireless berbasis Honey Network dan Intrusion Detection System (IDS) menggunakan Pentbox untuk mendeteksi aktivitas berbahaya secara real-time. Metode yang digunakan meliputi perancangan arsitektur keamanan, implementasi honeypot dan IDS, pengujian melalui serangan brute-force pada SSH dan FTP, serta serangan DoS SYN Flood pada jaringan internal. Hasil pengujian menunjukkan bahwa honeypot berhasil menangkap seluruh percobaan brute-force dengan mencatat detail intrusi yang berulang, sementara IDS mampu mendeteksi pola serangan DoS melalui lonjakan paket SYN yang dikirim secara masif. Sistem terbukti efektif dalam memberikan deteksi dini, mencatat aktivitas serangan, dan membantu analisis pola ancaman tanpa mengganggu jaringan utama. Temuan ini menunjukkan bahwa integrasi Honey Network dan IDS menggunakan Pentbox dapat menjadi solusi keamanan yang ringan, ekonomis, dan relevan bagi institusi pendidikan dengan sumber daya terbatas.
Kata Kunci: Honeypot, IDS, Pentbox, Keamanan Jaringan, Brute-Force, Dos SYN Flood.

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi (TIK) telah mendorong institusi pendidikan untuk mengintegrasikan jaringan komputer dalam kegiatan pembelajaran maupun administrasi. SMKN 3 Bangkalan, yang berlokasi di Jl. Soekarno Hatta No. 4 Bangkalan, merupakan salah satu sekolah yang aktif memanfaatkan teknologi tersebut, khususnya melalui program keahlian Teknik Komputer dan Jaringan (TKJ). Implementasi jaringan wireless di lingkungan sekolah memberikan kemudahan akses informasi bagi siswa, guru, serta tenaga kependidikan. Jaringan nirkabel memiliki kerentanan yang lebih tinggi dibandingkan jaringan kabel, terutama terhadap serangan akses tidak sah, pencurian data, sniffing, spoofing, brute-force attack, hingga serangan Denial of Service (DoS). Ancaman ini kian meningkat seiring bertambahnya insiden keamanan siber di sektor pendidikan dan lemahnya kontrol keamanan pada titik akses jaringan.

Lingkungan sekolah dengan pengguna multiuser di SMKN 3 Bangkalan, memperbesar potensi risiko keamanan jaringan wireless. Banyaknya perangkat dan variasi aktivitas pengguna menyebabkan jaringan lebih rentan terhadap eksploitasi, baik dari internal maupun eksternal. Berdasarkan laporan BSSN menunjukkan peningkatan signifikan pada insiden siber di sektor pendidikan, terutama sejak meningkatnya penggunaan TIK selama dan setelah pandemi. Tanpa sistem keamanan yang andal, jaringan sekolah berpotensi menjadi target empuk bagi pelaku kejahatan siber. Sehingga,

diperlukan langkah pengamanan yang bersifat preventif, mendeteksi dini ancaman, serta mampu memberikan informasi akurat terkait pola serangan yang masuk ke jaringan.

Salah satu pendekatan strategis dalam meningkatkan keamanan jaringan adalah integrasi Honey Network dan Intrusion Detection System (IDS). Honey Network berperan sebagai sistem umpan yang meniru jaringan asli untuk menarik serangan, sedangkan IDS memantau lalu lintas jaringan dan mendeteksi aktivitas berbahaya secara real-time. Penggunaan alat open-source seperti Pentbox menjadi solusi ideal bagi institusi pendidikan karena bersifat ringan, mudah dikonfigurasi, dan tidak memerlukan perangkat keras tambahan. Integrasi kedua teknologi ini memungkinkan pendekatan keamanan yang bersifat proaktif dan prediktif dapat mendeteksi serangan serta memahami karakteristik ancaman untuk meningkatkan perlindungan jaringan.

Penelitian ini dilakukan untuk merancang dan mengembangkan prototipe sistem keamanan jaringan wireless berbasis Honey Network dan IDS menggunakan Pentbox, yang kemudian diuji pada lingkungan laboratorium TKJ dan jaringan internal SMKN 3 Bangkalan. Tujuan utama penelitian ini adalah menguji efektivitas sistem dalam mendeteksi, mencatat, serta merespons berbagai bentuk serangan seperti spoofing, scanning, brute-force pada FTP dan SSH, serta DoS dan SYN Flood. Penelitian ini bertujuan mengevaluasi stabilitas, akurasi deteksi, efisiensi sumber daya, serta kompatibilitas sistem dengan infrastruktur TIK sekolah. Implementasi prototipe ini juga diharapkan dapat menjadi media pembelajaran berbasis proyek (PBL) bagi siswa TKJ dalam bidang keamanan jaringan.

Berdasarkan tujuan tersebut, penelitian ini dirancang dengan hipotesis bahwa integrasi Honey Network dan IDS menggunakan Pentbox mampu meningkatkan efektivitas sistem keamanan jaringan wireless di SMKN 3 Bangkalan. Prototipe yang dikembangkan diperkirakan dapat mendeteksi serangan brute-force pada FTP dan SSH, serangan DoS seperti SYN Flood, serta mampu bekerja secara stabil tanpa mengganggu jaringan produksi. Sistem ini diharapkan mencapai Tingkat Kesiapan Teknologi (TKT) level 4–6, sehingga layak diuji pada lingkungan nyata dan memberi manfaat edukatif sesuai kebutuhan sekolah menengah kejuruan.

METODE PENELITIAN

Dalam penelitian ini, pendekatan kualitatif-historis diterapkan untuk mengeksplorasi evolusi sistem ekonomi Islam dari zaman Nabi Muhammad hingga Dinasti Abbasiyah. Fokus utama dari studi ini adalah menganalisis perkembangan ekonomi Islam dalam konteks sejarah dan sosial dengan memanfaatkan metode library research. Melalui analisis dokumen dan literatur, baik sumber primer seperti kitab-kitab klasik ekonomi Islam maupun karya para pemikir terkenal, penelitian ini bertujuan untuk mengidentifikasi prinsip, praktik, serta kebijakan yang berlaku di masing-masing periode. Selama proses analisis, dilakukan beberapa langkah termasuk penyaringan data yang relevan, penyajian hasil yang sistematis, triangulasi untuk memastikan validitas informasi, dan interpretasi untuk mendapatkan pemahaman mendalam mengenai peran sistem ekonomi Islam dalam perkembangan peradaban.

HASIL DAN PEMBAHSAN

Bruteforce SSH

Gambar 1. Serangan pada Port 22

Berdasarkan Gambar 1, proses serangan brute-force SSH yang dijalankan menggunakan Hydra menunjukkan bahwa upaya koneksi ke layanan SSH pada alamat 192.168.1.2 port 22 gagal dilakukan. Pada tampilan tersebut terlihat bahwa Hydra telah memulai proses serangan dengan memanfaatkan daftar username dan password yang disediakan, namun sistem menampilkan peringatan bahwa banyak konfigurasi SSH membatasi jumlah tugas paralel sehingga disarankan menggunakan jumlah thread yang lebih rendah. Meskipun demikian, serangan tetap dijalankan dengan total 16 task dan 100 percobaan login. Informasi ini menunjukkan bahwa penyerangan telah dimulai dan diarahkan pada layanan SSH dengan tujuan melakukan percobaan kredensial menggunakan metode brute-force.

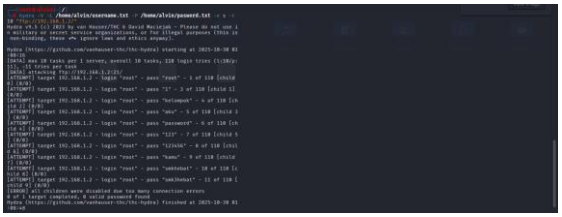
Hasil serangan pada Gambar 1 juga menunjukkan pesan “ERROR: could not connect to ssh://192.168.1.2:22 – Socket error: disconnected”, yang menandakan bahwa layanan SSH pada target menolak atau memutus koneksi sebelum Hydra dapat melakukan proses login. Kondisi ini dapat mengindikasikan beberapa hal: layanan SSH sedang tidak aktif, adanya firewall atau IDS/Honeypot yang memblokir upaya koneksi mencurigakan, atau sistem keamanan secara otomatis mendeteksi serangan dan memutuskan sambungan untuk mencegah brute-force berlanjut. Sehingga, berdasarkan hasil tampilan tersebut, dapat disimpulkan bahwa serangan brute-force pada port 22 tidak berhasil dilakukan karena koneksi ke layanan SSH gagal sejak tahap awal percobaan.

Gambar 2. Log Brute force SSH

Pada gambar 2., bahwa honeypot yang diaktifkan pada port 22 secara konsisten mendeteksi percobaan intrusi yang datang dari alamat 192.168.1.100 dengan berbagai nomor port sumber (misalnya 57834, 38800, 52416, 33512, 56070). Pola ini menunjukkan adanya upaya brute force atau pemindaian otomatis yang mencoba melakukan koneksi berulang ke layanan SSH. Honeypot mencatat detail setiap percobaan koneksi, termasuk waktu kejadian dan versi protokol SSH yang digunakan, yaitu SSH-2.0-libssh_0.11.1, yang mengindikasikan penggunaan library otomatis, bukan klien SSH biasa.

Frekuensi percobaan koneksi yang muncul dalam selang waktu sangat singkat memperlihatkan bahwa serangan dilakukan secara terotomatisasi, kemungkinan menggunakan alat seperti Hydra atau skrip bot yang berjalan terus-menerus. Sistem honeypot berhasil menangkap seluruh aktivitas ini tanpa memberikan akses ke server sebenarnya, sehingga berfungsi sebagai mekanisme monitoring dan pelindung yang efektif. Data ini menunjukkan bahwa port 22 merupakan target utama infiltrasi, dan pentingnya penerapan mitigasi seperti rate limiting, port knocking, atau penggunaan kunci SSH untuk memperkuat keamanan.

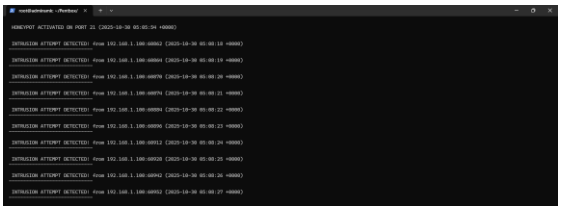
Bruteforce FTP



Gambar 3. Serangan pada Port 21

Pada Gambar 3 terlihat proses serangan bruteforce yang dilakukan terhadap layanan FTP pada port 21. Penyerang menggunakan sebuah tools otomatis yang mencoba login berulang-ulang dengan berbagai kombinasi username dan password. Setiap baris pada terminal menunjukkan upaya login yang dikirim ke server FTP target (misalnya admin : 1234, test : password, dan kombinasi lain). Tools tersebut secara sistematis mencoba seluruh pasangan kredensial dari sebuah wordlist untuk menemukan kombinasi yang valid. Aktivitas seperti ini adalah ciri khas serangan brute force: mencoba sebanyak mungkin kemungkinan hingga menemukan kecocokan.

Di bagian akhir tampilan terlihat adanya pesan "authentication errors" yang menunjukkan bahwa sebagian besar percobaan login gagal, namun serangan tetap berlanjut hingga tools selesai memproses seluruh daftar password yang tersedia. Log juga memperlihatkan IP target, port yang diserang, serta jumlah percobaan yang telah dijalankan. Dari hasil ini dapat disimpulkan bahwa sistem FTP sedang menjadi sasaran eksploitasi dengan metode brute force dan sangat rentan jika tidak memiliki proteksi seperti batas percobaan login, penggunaan password kuat, atau mekanisme blocking otomatis.



Gambar 4. Log Brute force FTP

Gambar 4 menunjukkan log aktivitas dari sebuah honeypot yang diaktifkan pada port 21 untuk memantau serangan terhadap layanan FTP. Setelah honeypot berjalan, sistem langsung merekam sejumlah aktivitas mencurigakan yang ditandai dengan pesan “INTRUSION ATTEMPT DETECTED!”. Setiap entri log menampilkan alamat IP sumber beserta port asal (source port) dan waktu terjadinya percobaan intrusi. Pola serangan tampak jelas karena percobaan koneksi dilakukan berulang-ulang hanya dalam hitungan detik, yang menunjukkan adanya upaya sistematis dari penyerang—umumnya merupakan karakteristik dari serangan brute force atau scanning otomatis.

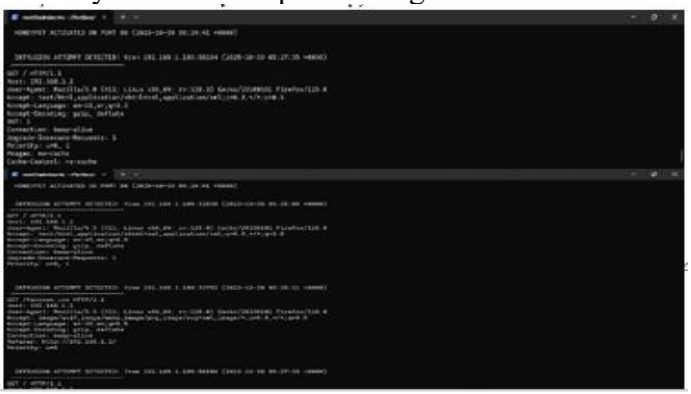
Log ini juga memperlihatkan bahwa serangan datang dari IP yang sama, menunjukkan bahwa penyerang menggunakan metode agresif untuk mencoba mengakses FTP dengan banyak permintaan secara cepat. Honeypot mencatat setiap upaya koneksi sebagai intrusi, meskipun tidak semua mencoba kredensial secara langsung, namun intensitas dan frekuensi tinggi sudah cukup untuk mengindikasikan aktivitas brute force. Data log ini sangat penting bagi administrator karena memberikan gambaran tentang pola serangan, frekuensi percobaan, dan potensi ancaman yang sedang berlangsung. Melalui catatan ini, sistem keamanan dapat dianalisis lebih lanjut untuk menentukan mitigasi seperti rate limiting, blocking IP, atau peningkatan proteksi pada layanan FTP.

Dos Sync Flood

Gambar 5. Serangan Dos Sync Flood

Gambar 5 menampilkan proses serangan DoS (Denial of Service) jenis SYN Flood yang dilakukan terhadap host dengan alamat IP 192.168.1.2. Pada bagian pertama gambar terlihat penggunaan perintah hping3 -S --flood, yang menunjukkan bahwa penyerang mengirimkan paket SYN dalam jumlah sangat besar secara terus-menerus. Setiap paket dikirim tanpa menunggu respons, sehingga target menerima banjir permintaan koneksi palsu. Hal ini bertujuan memenuhi connection queue pada sisi target sehingga host menjadi lambat merespons atau bahkan tidak dapat diakses. Log terminal juga menunjukkan respon tidak normal, RTT (round-trip time) 0.0 ms, dan output sangat cepat, menandakan lalu lintas yang membanjiri jaringan.

Pada bagian kedua gambar tampak hasil ping ke target yang menunjukkan gejala gangguan akibat serangan tersebut. Beberapa percobaan ping menghasilkan packet loss tinggi, misalnya 90%, 100%, bahkan ada respons yang sangat lambat seperti 200ms hingga 300ms. Gejala ini merupakan indikator khas serangan SYN Flood: target mengalami overload sehingga tidak mampu menanggapi permintaan ICMP sederhana. Penurunan kualitas koneksi, keterlambatan respons, hingga ketidakstabilan jaringan menunjukkan bahwa serangan DoS berhasil mengganggu ketersediaan layanan. Kondisi ini menggambarkan dampak nyata dari serangan SYN Flood, yaitu konsumsi sumber daya server hingga membuat layanan tidak dapat berfungsi secara normal.



Gambar 6. Log Dos Sync Flood

Log pada Gambar 6 menunjukkan aktivitas serangan DoS SYN Flood yang terdeteksi oleh sistem, ditandai dengan pesan “INTRUSION ATTEMPT DETECTED” yang muncul berulang dari alamat IP sumber tertentu. Pola serangan ini terlihat dari banyaknya permintaan SYN yang dikirim ke port yang sama dalam waktu sangat singkat tanpa pernah dilanjutkan ke proses three-way handshake berikutnya. Hal ini menyebabkan sumber daya server—seperti buffer koneksi—menjadi penuh oleh koneksi setengah terbuka, sehingga server tidak mampu merespon permintaan koneksi yang sah dari pengguna normal. Informasi detail HTTP header seperti User-Agent, Accept, dan Connection: keep-alive tampak disisipkan untuk membuat permintaan terlihat seperti lalu lintas normal, padahal dikirim secara masif dan terus-menerus.

Selain itu, pola waktu pada log menunjukkan bahwa serangan dilakukan secara cepat dan beruntun, yang merupakan ciri khas dari SYN Flood berbasis DoS. Sistem keamanan yang digunakan berhasil mendeteksi aktivitas abnormal tersebut dan memblokir atau memberi peringatan pada setiap koneksi mencurigakan. Pesan seperti “Priority: warn” serta rincian header paket memperlihatkan bahwa IDS/IPS mampu mencatat setiap percobaan intrusi untuk analisis lebih lanjut. Dengan adanya deteksi ini, administrator dapat mengidentifikasi sumber serangan, memahami pola trafik berbahaya, dan menerapkan langkah mitigasi seperti rate limiting, firewall filtering, atau syn cookies untuk menjaga stabilitas layanan jaringan.

Pembahasan

Hasil penelitian menunjukkan bahwa integrasi Honey Network dan Intrusion Detection System (IDS) menggunakan Pentbox mampu memberikan deteksi dini yang efektif terhadap berbagai bentuk serangan yang umum terjadi pada jaringan wireless sekolah. Pada pengujian brute-force terhadap layanan SSH dan FTP, honeypot berhasil menangkap seluruh percobaan login ilegal yang dikirim secara berulang dan otomatis oleh tools penyerang seperti Hydra. Hal ini terlihat dari log yang menunjukkan koneksi berulang dari alamat IP yang sama dengan interval waktu sangat cepat. Rekaman ini menunjukkan bahwa honeypot berfungsi optimal dalam memancing dan mencatat aktivitas penyerang tanpa memberikan akses ke server sebenarnya. Respon sistem yang memutus koneksi sebelum proses autentikasi juga menegaskan bahwa mekanisme proteksi berjalan sebagaimana mestinya meskipun diserang dengan intensitas tinggi.

Pada pengujian terhadap serangan DoS SYN Flood, sistem menunjukkan kemampuan deteksi yang kuat dengan menangkap setiap paket permintaan koneksi yang dikirim secara masif dalam waktu singkat. Log yang ditampilkan memperlihatkan pola trafik abnormal berupa banjir paket SYN yang tidak pernah dilanjutkan ke proses handshake. Kondisi ini sesuai dengan karakteristik serangan DoS yang bertujuan menghabiskan sumber daya server hingga tidak dapat memberikan layanan normal kepada pengguna. Gangguan koneksi yang terlihat dari hasil ping selama serangan berlangsung—seperti latensi tinggi dan packet loss ekstrem—menegaskan bahwa serangan SYN Flood berdampak signifikan terhadap performa jaringan. Meski demikian, pencatatan yang akurat oleh honeypot dan IDS membuktikan bahwa sistem mampu mengidentifikasi sumber serangan dan memberikan peringatan dini kepada administrator.

Data keseluruhan dari pengujian menunjukkan bahwa implementasi Honey Network dan IDS menggunakan Pentbox memberikan nilai strategis dalam meningkatkan keamanan jaringan wireless di lingkungan SMKN 3 Bangkalan. Sistem tidak hanya berperan sebagai media deteksi, tetapi juga sebagai sarana pembelajaran yang menggambarkan pola serangan nyata secara langsung kepada siswa TKJ. Informasi detail yang diperoleh dari setiap serangan dapat digunakan untuk analisis lanjutan, penyusunan kebijakan keamanan, serta penguatan konfigurasi jaringan. Dengan demikian, integrasi kedua teknologi ini terbukti mampu memberikan proteksi preventif dan responsif, sekaligus mendukung pengembangan infrastruktur keamanan jaringan sekolah secara lebih komprehensif.

KESIMPULAN

Penelitian ini menyimpulkan bahwa integrasi Honey Network dan Intrusion Detection System (IDS) menggunakan Pentbox terbukti efektif dalam mendeteksi berbagai bentuk serangan jaringan seperti brute-force pada SSH dan FTP serta serangan DoS SYN Flood pada jaringan wireless SMKN 3 Bangkalan. Sistem mampu mencatat aktivitas intrusi secara real-time, mengidentifikasi pola serangan, serta menunjukkan respons jaringan ketika berada di bawah tekanan serangan. Hasil ini menegaskan bahwa penggunaan honeypot dan IDS dapat menjadi solusi keamanan yang ekonomis, ringan, dan sesuai untuk lingkungan pendidikan dengan sumber daya terbatas. Saran untuk penelitian selanjutnya adalah mengembangkan sistem ini ke tingkat implementasi yang lebih luas, seperti integrasi dengan dashboard visual berbasis web, pengujian dengan variasi serangan lain seperti MITM atau ARP spoofing, serta penerapan otomatisasi mitigasi agar sistem tidak hanya mendeteksi tetapi juga mampu merespons serangan secara mandiri dan adaptif.

DAFTAR PUSTAKA

Alqahtani, A., and Bourouis, S., "A hybrid honeypot–IDS framework for real-time cyberattack detection in educational networks," International Journal of Network Security, vol. 22, no. 6, pp. 1094–1108, 2020.

Chen, W., Li, Z., and Zhang, H., "Improving SYN flood mitigation using adaptive queue management on wireless networks," IEEE Access, vol. 9, pp. 104233–104244, 2021.

European Commission, Technology Readiness Level (TRL) Guidelines. TRL Assessment Tool, 2019. [Online]. Available: https://www.era-learn.eu

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E., "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, no. 1–2, pp. 18–28, 2009, doi: 10.1016/j.cose.2008.08.003.

Karim, M., Hasan, M., and Rahman, A., "Lightweight intrusion monitoring using virtual honeypots for resource-limited environments," Journal of Information Security and Applications, vol. 58, pp. 1–11, 2021.

Kementerian Keuangan Republik Indonesia, Peraturan Menteri Keuangan Republik Indonesia Nomor 39 Tahun 2024 tentang Standar Biaya Masukan Tahun Anggaran 2025, 2024.

National Institute of Standards and Technology, National Vulnerability Database (NVD), U.S. Department of Commerce, 2024. [Online]. Available: https://nvd.nist.gov/

Park, J., and Lee, S., "Enhancing SSH brute-force detection through behavioral traffic profiling," International Journal of Information Security Science, vol. 10, no. 2, pp. 45–56, 2021.

Riadi, I., Luthfi, A., and Ashari, A., "Analisis serangan jaringan menggunakan kombinasi honeypot dan intrusion detection system," Jurnal Ilmiah Informatika, vol. 7, no. 2, pp. 155–166, 2017.

Scarfone, K. and Mell, P., Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, 2007.

Sharma, D., and Upadhyay, N., "A comparative analysis of DoS detection techniques on wireless infrastructures," International Journal of Computer Networks & Communications, vol. 12, no. 4, pp. 67–82, 2020.

Spitzner, L., Honeypots: Tracking Hackers. Addison-Wesley, 2003.

technicaldada, "Pentbox," GitHub Repository, 2022. [Online]. Available: https://github.com/technicaldada/pentbox

Yasin, A., Mustapha, A., and Ahmad, R., "Intrusion detection and prevention system: Using Snort and Python-based machine learning," Journal of Theoretical and Applied Information Technology, vol. 98, no. 14, pp. 2832–2843, 2020.