BAB II
LANDASAN TEORI

2.1 Sistem Keamanan Jaringan

Sistem keamanan jaringan adalah teknologi yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya dalam suatu jaringan komputer. Ini melibatkan berbagai komponen dan strategi yang bekerja bersama-sama untuk mengidentifikasi, mencegah, dan merespons ancaman yang terjadi terhadap jaringan tersebut.

Beberapa komponen utama sistem keamanan jaringan adalah sebagai berikut:

2.1.1 Firewall

Firewall mengatur lalu lintas antara jaringan yang aman dan tidak aman. Mereka dapat membatasi atau mengizinkan lalu lintas dengan cara tertentu.

2.1.2 Enkripsi

Algoritme enkripsi digunakan untuk melindungi data yang dikirim melalui jaringan, sehingga hanya penerima yang sah yang dapat membacanya.

2.1.3 *Virtual Private Network* (*VPN*)

VPN memungkinkan Anda mengakses jaringan dari lokasi yang tidak aman dengan menggunakan koneksi internet. Enkripsi melindungi data yang dikirim.

2.1.4 Keamanan Nirkabel

Menggunakan protokol enkripsi seperti WPA (Wi-Fi Protected Access) dan WPA2 untuk melindungi jaringan nirkabel dari akses yang tidak sah.

2.1.5 Pemantauan Jaringan

Menggunakan alat pemantauan untuk mengidentifikasi aktivitas mencurigakan atau serangan keamanan.

Sistem keamanan jaringan memungkinkan untuk mencegah atau menghentikan tindakan buruk para penyusup yang ingin mengakses komputer melalui sistem jaringan. Sistem keamanan jaringan dibuat untuk melindungi jaringan komputer, secara langsung maupun tak langsung. Karena sistem keamanan jaringan memungkinkan komunikasi dua arah antara pengirim dan penerima, setiap pesan dan komunikasi yang dikirim melalui jaringan komputer sangat rawan disalahgunakan oleh penyusup yang tidak bertanggung jawab.

2.2 Serangan *Website*

Serangan pada situs web adalah jenis tindakan yang dilakukan oleh pihak yang tidak berwenang atau penyerang untuk mengakses, merusak, atau mengambil alih sebuah situs web. Serangan ini dapat memiliki berbagai tujuan, seperti pencurian data, kerusakan situs web, penyebaran *malware*, atau bahkan untuk menyebarkan ideologi atau pesan politik tertentu. Berikut adalah beberapa jenis serangan website yang umum:

2.2.1 SQL Injection

SQL Injection adalah kerentanan keamanan web yang memungkinkan penyerang mengganggu *query* aplikasi ke basis datanya. Kerentanan ini dapat menyerang banyak jenis *website* yang menggunakan *database* SQL, seperti MySQL, Oracle, dan SQL Server. Serangan ini biasanya terjadi pada aplikasi web yang tidak memvalidasi atau menyaring input yang diterima dari pengguna sebelum mengirimkannya ke database.

2.2.2 DoS

Denial of Service Attack dilakukan dengan mengirimkan *fake traffic* atau lalu lintas palsu secara terus menerus ke sistem atau server. DOS berfungsi untuk menghentikan atau meniadakan layanan sistem atau jaringan komputer sehingga pengguna tidak dapat menikmati fungsinya

dengan mengganggu ketersediaan komponen sumber daya yang terkait. Salah satu contohnya adalah dengan mengirimkan request pada server dengan jutaan paket, yang menyebabkan penggunaan memori yang meningkat. Akibatnya, klien yang ingin mengakses server benar-benar tidak dapat melakukannya karena server sibuk menanggapi serangan DOS[5].

2.2.3 XSS

XSS adalah singkatan dari "*Cross-Site Scripting*" (Pemrograman Lintas Situs). Ini adalah jenis kerentanan keamanan dalam aplikasi web yang memungkinkan pencuri memasukkan kode skrip berbahaya, biasanya *JavaScript* ke dalam halaman web. Serangan XSS terjadi ketika aplikasi web tidak memvalidasi atau menyaring data pengguna dengan benar sebelum menampilkannya kepada pengguna lain. Ini memungkinkan penyerang untuk memasukkan kode skrip yang akan dijalankan oleh peramban web pengguna yang rentan.

2.3 *Vulnerable Website*

"*Vulnerable website*" atau "situs web yang rentan" adalah situs web yang memiliki kelemahan keamanan yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan atau akses yang tidak sah. Kerentanan ini dapat berkisar dari kesalahan konfigurasi sederhana hingga masalah keamanan yang kompleks. Web server adalah perangkat keras atau perangkat lunak yang berfungsi untuk menyimpan, mengelola, dan mengirimkan halaman web serta sumber daya web lainnya kepada pengguna yang memintanya melalui internet atau jaringan lokal. Web server bertindak sebagai mediator antara klien dan server yang meng-host situs web atau aplikasi web.

Mengatasi kerentanan pada situs web melibatkan penerapan praktik keamanan terbaik, seperti memperbarui perangkat lunak, memeriksa dan mengamankan formulir input, mengaudit konfigurasi server, dan melakukan pengujian keamanan rutin untuk menemukan dan memperbaiki potensi kerentanan. Pemilik situs web dapat meningkatkan keamanan situs mereka dan melindungi pengalaman pengguna. eb server menyediakan halaman web yang

berisi dokumen dan informasi yang dapat dibagikan atau diperlukan oleh pengguna. Menurut survei web server Netcraft, web server Apache adalah salah satu web server yang paling populer pada bulan Agustus 2019. Berbagai jenis serangan, baik kecil maupun besar, sering menyerang Web Server, yang dapat mengakibatkan kematian. Hal ini dapat terjadi karena elemen keamanan web server kurang diperhatikan atau diterapkan secara tidak efektif, yang memungkinkan risiko yang cukup besar[4].

2.3.1 DVWA

DVWA singkatan dari "*Damn Vulnerable Web Application*", adalah aplikasi web yang dirancang khusus untuk tujuan pelatihan dan pendidikan tentang keamanan web. Tujuan DVWA adalah untuk memberikan pengalaman praktis dalam menemukan, mengeksploitasi, dan memahami kerentanan keamanan web yang umum terjadi pada aplikasi web dunia nyata.

DVWA sengaja dibuat rentan terhadap berbagai jenis serangan keamanan web, termasuk serangan SQL injection, *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), dan banyak lagi. Tujuannya adalah untuk membantu peneliti memahami bagaimana melindungi aplikasi web mereka dari serangan-serangan ini dengan mempelajari teknik-teknik penyerangan dan bagaimana melawannya.

2.3.2 WackoPicko

WackoPicko adalah sebuah lingkungan pelatihan (training environment) yang dirancang untuk membantu para profesional keamanan informasi dan peneliti keamanan dalam memahami dan mengevaluasi kelemahan serta keamanan aplikasi web. Dalam konteks pelatihan keamanan, WackoPicko memungkinkan pengguna untuk melakukan serangan yang dikendalikan pada aplikasi web yang telah disediakan, yang dapat membantu dalam memahami bagaimana kerentanan tertentu bisa dieksploitasi.

Tujuan dari WackoPicko adalah untuk memberikan pengalaman praktis kepada para profesional keamanan informasi untuk memahami dan mengidentifikasi kerentanan pada aplikasi web, sehingga mereka dapat mengembangkan kemampuan untuk melindungi sistem mereka dari serangan.

2.4 *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) adalah sebuah sistem yang bertujuan untuk mencegah masalah keamanan pada jaringan komputer dengan menggunakan perangkat lunak atau perangkat keras yang beroperasi secara otomatis. IDS memiliki fungsi utama dalam memantau kondisi jaringan komputer serta menganalisis potensi ancaman keamanan. IDS dapat dianggap sebagai alat, teknik, dan sumber daya yang membantu dalam mengidentifikasi dan memberikan laporan tentang aktivitas di jaringan komputer[1].

Ada dua kategori utama pengenalan intrusi:

2.4.1 *Host-based Intrusion Detection System* (HIDS)

HIDS ditempatkan di dalam host atau sistem operasi dan digunakan untuk memantau dan menganalisis kegiatan di tingkat host. HIDS memantau log keamanan, sistem file, dan aktivitas pengguna di dalam sistem. HIDS dapat memberikan peringatan atau mengambil tindakan pencegahan jika ada pola perilaku atau aktivitas yang mencurigakan.

2.4.2 *Network-based Intrusion Detection System* (NIDS)

NIDS beroperasi di tingkat jaringan dan menganalisis lalu lintas di seluruh jaringan. NIDS memantau paket data yang mengalir melalui jaringan dan mencoba menemukan pola atau indikasi serangan. Jika pola atau indikasi ancaman terdeteksi, NIDS dapat memberikan peringatan kepada administrator jaringan.

Salah satu kemampuan utama IDS adalah memberikan notifikasi awal kepada Administrator Jaringan ketika terdeteksi aktivitas yang tidak diinginkan dalam sistem yang mereka tangani. Selain itu, IDS juga memiliki kemampuan

untuk melacak aktivitas yang dapat merusak sistem. IDS dapat melakukan pemantauan terhadap paket data yang berlalu-lalang di jaringan dan berusaha untuk mengidentifikasi paket-paket yang mungkin berisi aktivitas yang mencurigakan[1].

Intrusion Detection System (IDS) merupakan bagian penting dari upaya keamanan informasi karena membantu organisasi mendeteksi dan menanggapi segera ancaman keamanan pada jaringan atau sistem mereka. IDS dapat menjadi bagian penting dari kerangka keamanan yang lebih luas bersama dengan firewall, antivirus, dan alat keamanan lainnya.

2.5 Snort

Snort adalah perangkat lunak *Intrusion Detection System* (IDS) yang sangat populer di industri keamanan jaringan dan digunakan untuk mendeteksi aktivitas mencurigakan atau ancaman keamanan di jaringan. Snort, perangkat lunak sumber terbuka (open-source) yang dikembangkan oleh Martin Roesch pada tahun 1998, berjalan di berbagai platform, seperti Linux, Windows, dan macOS.

Fungsi utama Snort adalah memantau lalu lintas jaringan dan mencari sinyal serangan atau intrusi yang terjadi. Ini dicapai dengan memeriksa paket data yang melalui jaringan dan membandingkannya dengan tanda atau aturan yang telah ditetapkan sebelumnya. Jika Snort menemukan aktivitas yang bertentangan dengan aturan ini, maka akan menghasilkan peringatan atau tindakan yang sesuai dengan konfigurasi, seperti memblokir lalu lintas atau memberikan notifikasi kepada administrator jaringan.

Pada proses pengaktifan snort perlu diperhatikan rules yang akan digunakan serta seluruh perangkat berkerja dengan baik, sehingga pengujian dapat berjalan bernga lancar, pada tahap pertama pengaktifan snort IDS dengan menggunakan perintah berikut[3]:

Tabel 1 Sintaks Snort Untuk Deteksi Serangan

No	Sintaks	Keterangan
1	Sudo	Digunakan untuk menjalankan program dibawah user dengan hak akses penuh (root).
2	Snort	Merupakan sintak nama program snort.
3	-A console	Merupakan opsi yang ada pada snort yang mana seluruh allert akan dikirimkan ke layar monitor.
4	-i eth0	Digunakan untuk mendefinisikan port ethernet mana yang akan di monitoring snort.
5	-c /etc/snort/snort.conf	Digunakan untuk memberi tahu dimana tempat file konfigurasi yang akan digunakan oleh snort.
6	-l /var/log/snort	Digunakan untuk memberitahu dimana tempat menyimpan log allert yang dihasilkan.

Penjelasan berdasarkan referensi dari[3], Snort memiliki banyak aturan yang digunakan untuk mendeteksi jenis serangan, salah satu contohnya dapat dilihat pada tabel 1, merupakan fungsi atau perintah pada Snort yang terdapat pada rule dari Snort.

2.6 Penelitian Terdahulu

Tabel 2 Ringkasan Penelitian Terdahulu

No.	Judul Penelitian	Peneliti	Pembahasan Utama	Temuan/Relevansi
1	Analyzing the traffic of penetration testing tools with an IDS (2018)	F. R. Muñoz, dkk.	Penggunaan beberapa *tools* penetration testing terhadap DVWA. Pada penelitian tersebut melalui beberapa serangan dan *tools*.	SNORT tidak dapat mendeteksi semua serangan meskipun memiliki ribuan aturan
2	Perancangan dan analisis sistem keamanan	Winrou Wesley Purba,	Membahas Snort yang dapat digunakan untuk mencegah serangan pada server,	Snort bersifat open-source dan commercial, efektif

	jaringan komputer menggunakan SNORT (2020)	Rissal Efendi	fokus pada DDOS attack	dalam mencegah serangan DDOS
3	Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort (2016)	Asep Fauzi Mutaqin	Membahas tentang sistem monitoring terhadap keamanan jaringan prodi Teknik Informatika dengan menggunakan Snort.	Hasil pendeteksian Snort dilaporkan melalui SMS Alert
4	Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer (2020)	Barany Fachri, Fadli Hamdi Harahap	Membahas penggunaan SNORT sebagai keamanan jaringan dan komputer melalui beberapa uji coba serangan.	*Intrusion Detection System* (IDS) bersifat pasif. IDS hanya mendeteksi serangan, tidak mencegah
5	Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort (2020)	Benny Wijaya, Arie Pratama	Metode *Intrusion Detection System* (IDS) berbasis Snort, dapat mengetahui aliran paket-paket yang keluar masuk sistem.	IDS Snort dapat merekam semua serangan dan memberikan laporan paket mencurigakan
6	Evaluation of Web Vulnerability Scanners (2015)	Yuma Makino, Vitaly Klyuev	peneliti mengevaluasi pemindai kerentanan OWASPZAP dan Skipfish.	OWASP ZAP lebih unggul dibandingkan Skipfish, namun keduanya belum sempurna dalam mendeteksi kerentanan RFI

Penelitian-penelitian terdahulu di atas menggunakan sistem pengujian dengan metode *penetration testing*. Penelitian ini akan lebih memfokuskan pada penggunaan variasi metode dalam menguji tingkat kerentanan website, dimana yang digunakan adalah *vulnerability scanning* dan *penetration testing*.

Dengan beberapa penelitian di atas dapat disimpulkan bahwa metode yang menggunakan tools untuk menguji kerentanan khususnya pada website, dapat menghasilkan data beberapa kerentanan terhadap website, dan dalam penggunaan tools IDS, SNORT tidak dapat mendeteksi semua tipe serangan, meskipun SNORT memiliki ribuan aturan untuk berbagai macam serangan yang berbeda, SNORT tidak dapat mencakup serangan yang terperinci.

2.7 *Vulnerability Scanning*

Vulnerability scanning adalah proses pemeriksaan sistem, jaringan, atau aplikasi perangkat lunak untuk menemukan dan menganalisis kerentanan keamanan yang dapat dimanfaatkan oleh pihak yang tidak sah. Tujuan utama dari pemeriksaan kerentanan adalah untuk menemukan kelemahan potensial dalam sistem dan memberikan informasi yang diperlukan untuk mengambil tindakan yang diperlukan sebelum kelemahan tersebut dapat dimanfaatkan.

Berikut adalah beberapa poin penting mengenai scanning kelemahan:

2.7.1 Identifikasi Kelemahan

Proses ini mencakup penggunaan alat khusus untuk secara otomatis memeriksa konfigurasi sistem, kebijakan keamanan, dan kode perangkat lunak untuk menemukan kelemahan yang ada. Kelemahan ini dapat mencakup berbagai aspek, seperti konfigurasi yang salah, kerentanan perangkat lunak yang belum diperbarui, atau kebijakan keamanan yang tidak memadai.

2.7.2 Skanning Otomatis

Pemindaian kerentanan biasanya dilakukan dengan menggunakan alat otomatis atau perangkat lunak khusus yang dapat memindai secara

menyeluruh jaringan, sistem operasi, aplikasi web, atau perangkat lunak lainnya dalam waktu yang singkat.

2.7.3 Analisis Hasil

Setelah pemindaian selesai, hasilnya dianalisis untuk menilai tingkat risiko dan memperoleh pemahaman yang lebih baik tentang cara mengatasi kerentanan tersebut. Hasil ini biasanya disajikan dalam laporan yang mencakup kelemahan, tingkat urgensi, dan saran untuk penyelesaian.

Salah satu langkah proaktif penting dalam manajemen keamanan informasi adalah pemeriksaan ketahanan. Organisasi dapat meningkatkan ketahanan sistem mereka dan mengurangi risiko keamanan secara keseluruhan dengan menemukan dan mengatasi kelemahan sebelum dimanfaatkan oleh penyerang.

2.8 *Penetration Testing*

Penetration testing adalah metode pengujian keamanan di mana seorang profesional keamanan komputer yang disebut penetration tester atau ethical hacker secara aktif mengeksplorasi dan mengevaluasi kelemahan dalam sistem, aplikasi, atau jaringan. Ini juga dikenal sebagai "*pen testing*" dan "*ethical hacking*." Penetration testing memiliki dua tujuan utama: menemukan potensi celah keamanan yang dapat dimanfaatkan oleh penyerang sebelum mereka melakukannya, dan memberikan saran untuk mengamankan sistem.

Berikut adalah beberapa poin penting yang berkaitan dengan pengujian penetrasi:

2.8.1 Tujuan Pengujian

Pengujian penetrasi dilakukan untuk menemukan dan mengeksploitasi kelemahan keamanan dalam sistem atau aplikasi. Ini membantu organisasi memahami seberapa tahan sistem mereka terhadap serangan dan memberikan pemahaman tentang risiko yang akan dihadapi.

2.8.2 Skenario Serangan Nyata

Untuk mengetahui bagaimana penyerang memanfaatkan kelemahan yang ditemukan, penilaian penetrasi biasanya melibatkan simulasi serangan nyata. Injection attacks, social engineering, dan phishing adalah contohnya.

2.8.3 Rekomendasi Perbaikan

Setelah pengujian selesai, penguji penetrasi memberikan laporan yang menguraikan kelemahan, risiko, dan saran untuk perbaikan. Ini memungkinkan perusahaan untuk melakukan perbaikan yang diperlukan.

Penetration testing adalah cara yang efektif untuk meningkatkan keamanan sistem dan memastikan bahwa kemungkinan masalah keamanan dapat diperbaiki sebelum pihak yang tidak berwenang dapat memanfaatkannya. Tindakan ini membantu menjaga data, menjaga reputasi perusahaan, dan mematuhi peraturan keamanan dalam hal keamanan informasi.