sudo
Jurnal Teknik Informatika
https://jurnal.ilmubersama.com/index.php/sudo

Cybersecurity

Implementasi Layanan Cloudflare sebagai Mitigasi terhadap Ancaman Pemindaian dan Eksploitasi Siber Menggunakan Nmap dan Metasploit

Rizki Ripai [1], Riki Aldi Pari [1], Fazar Sidik [1], Sony Veri Shandy [2], Fajar Mahardika [3]*

[1] *Prodi Rekayasa Keamanan Siber, Politeknik Piksi Input Serang, Banten, Indonesia*
[2] *Teknik Informatika, Universitas Utpadaka Swastika, Tangerang, Indonesia*
[3] *Teknik Informatika, Jurusan Komputer dan Bisnis, Politeknik Negeri Cilacap, Cilacap, Indonesia*

INFORMASI ARTIKEL

Diterima Redaksi: 02 Juni 2025
Revisi Akhir: 11 Juni 2025
Diterbitkan *Online*: 11 Juni 2025

KATA KUNCI

Keamanan Siber
Cloudflare
Nmap
Metasploit
Pemindaian Jaringan
Web Application Firewall

KORESPONDENSI (*)

Phone: +62 812-9491-4513
E-mail: rizky.ripai@gmail.com

A B S T R A K

Serangan siber berbasis pemindaian jaringan dan eksploitasi sistem menjadi ancaman signifikan bagi keamanan aplikasi web. Alat seperti Nmap dan Metasploit banyak digunakan oleh peretas untuk mengidentifikasi celah keamanan serta mengeksploitasi sistem target. Penelitian ini bertujuan untuk mengevaluasi efektivitas layanan Cloudflare dalam memitigasi serangan reconnaissance dan eksploitasi tersebut. Metode yang digunakan adalah pendekatan eksperimental dengan melakukan simulasi serangan terhadap dua lingkungan server: satu tanpa proteksi Cloudflare dan satu dengan konfigurasi penuh layanan Cloudflare. Serangan dilakukan menggunakan teknik pemindaian port dan service enumeration dari Nmap, serta injeksi payload eksploitasi menggunakan Metasploit Framework. Hasil pengujian menunjukkan bahwa Cloudflare mampu secara signifikan mengurangi keberhasilan pemindaian dan eksploitasi, dengan tingkat deteksi dan pemblokiran mencapai lebih dari 90% terhadap permintaan mencurigakan. Fitur seperti Web Application Firewall (WAF), rate limiting, dan penyembunyian IP server terbukti efektif dalam menghambat proses pengintaian serta serangan berbasis payload otomatis. Penelitian ini menyimpulkan bahwa Cloudflare merupakan solusi mitigasi yang efisien dalam meningkatkan ketahanan sistem web terhadap serangan berbasis Nmap dan Metasploit.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah membawa transformasi besar dalam cara berbagai institusi menjalankan aktivitas operasional, komunikasi, serta memberikan layanan publik. Sistem berbasis web menjadi tulang punggung dalam berbagai proses ini, memberikan kemudahan akses dan efisiensi yang sebelumnya sulit dicapai. Namun, peningkatan ketergantungan terhadap sistem digital tersebut menimbulkan tantangan serius terkait keamanan data dan keberlangsungan operasional organisasi. Ancaman siber menjadi semakin nyata dan kompleks, terutama dalam bentuk serangan reconnaissance dan eksploitasi yang menyasar celah keamanan pada jaringan dan aplikasi. Salah satu metode serangan yang cukup umum terjadi adalah pemindaian jaringan (network scanning) menggunakan alat seperti Nmap, yang bertujuan memetakan sistem target dan mengidentifikasi titik lemah. Setelah menemukan celah, pelaku biasanya menggunakan framework seperti Metasploit untuk melakukan eksploitasi dan memperoleh akses tidak sah, melakukan injeksi kode berbahaya, atau mencuri data sensitif. Alat-alat ini sangat populer bukan hanya di kalangan pakar keamanan dalam melakukan pengujian penetrasi secara etis, tetapi juga sering disalahgunakan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan berbahaya[1].

Menyikapi ancaman tersebut diperlukan sistem pertahanan yang dapat melakukan mitigasi secara real-time terhadap berbagai aktivitas mencurigakan. Salah satu solusi yang banyak diterapkan adalah penggunaan layanan berbasis cloud

https://doi.org/10.56211/sudo.v4i1.902

seperti Cloudflare. Platform ini menyediakan fitur-fitur keamanan seperti Web Application Firewall (WAF), Content Delivery Network (CDN), serta proteksi terhadap serangan Distributed Denial of Service (DDoS), bot, dan pemindaian jaringan. Selain mempercepat distribusi konten, Cloudflare juga berfungsi sebagai perisai keamanan dengan menyembunyikan IP asli server, memblokir permintaan yang mencurigakan, dan membatasi akses pada endpoint kritikal aplikasi.

Sejumlah penelitian terkait keamanan web telah menghasilkan temuan yang berharga. Misalnya, studi oleh Supriadi et al. (2024) yang memanfaatkan pendekatan vulnerability assessment OWASP pada website universitas menemukan beberapa kerentanan dengan tingkat risiko sedang dan rendah. Dalam pengujian tersebut, serangan Clickjacking berhasil dieksploitasi namun XSS berhasil dicegah, menandakan mekanisme pertahanan yang cukup efektif terhadap jenis serangan tertentu[2]. Meski demikian, pemanfaatan dan evaluasi efektivitas layanan Cloudflare dalam konteks mitigasi serangan Nmap dan Metasploit secara empiris masih sangat terbatas. Khususnya, masih minim kajian yang secara langsung menguji performa Cloudflare dalam menghadapi serangan yang dilakukan secara sistematis pada server target. Hal ini menimbulkan kebutuhan mendesak untuk melakukan penelitian komprehensif yang dapat mengukur sejauh mana layanan cloud tersebut mampu mencegah atau meminimalkan dampak serangan reconnaissance dan eksploitasi.

Penelitian ini bertujuan untuk mengisi celah tersebut dengan mengevaluasi efektivitas Cloudflare dalam mencegah serta memitigasi serangan yang berbasis pada Nmap dan Metasploit secara empiris serta sistematis. Hasil penelitian diharapkan memberikan kontribusi penting dalam pengembangan strategi pertahanan siber yang adaptif, efisien, dan berbasis layanan cloud, sehingga dapat memperkuat keamanan data dan keberlanjutan operasional institusi yang semakin bergantung pada teknologi digital[3].

Penelitian yang dilakukan oleh Supriadi, D., Suryadi, E., Muslim, R., & Samsumar, L. D. (2024). Implementasi Vulnerability Assessment Owasp (Open Web Application Security Project) Pada Website Universitas Teknologi Mataram. Penelitian ini menghasilkan laporan yang mengidentifikasi tiga kerentanan dengan level sedang, empat kerentanan dengan level rendah, serta tidak ada kerentanan dengan level tinggi. Setelah pemindaian, hasil pengujian menunjukkan bahwa serangan Clickjacking berhasil dieksploitasi, sementara serangan XSS tidak berhasil dilakukan, menunjukkan adanya mekanisme pertahanan yang baik terhadap XSS [4].

Meskipun Cloudflare telah digunakan secara luas, studi mengenai efektivitas layanan ini dalam konteks mitigasi serangan Nmap dan Metasploit masih terbatas, terutama dalam konteks implementasi langsung pada server target dan pengujian sistematis. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi secara empiris sejauh mana Cloudflare mampu mencegah atau meminimalkan dampak dari serangan pemindaian dan eksploitasi yang dilakukan melalui dua alat tersebut. Hasil dari penelitian ini diharapkan dapat menjadi referensi dalam membangun strategi pertahanan siber berbasis layanan cloud yang adaptif dan efisien.

TINJAUAN PUSTAKA

Penulis melampirkan penelitian terdahulu yang berkaitan dengan penelitian penulis. Penelitian terdahulu sebagai berikut: penelitian yang dilakukan oleh [5] Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi. Berdasarkan temuan ini, berbagai langkah mitigasi direkomendasikan, termasuk pembaruan sistem secara berkala, pengaturan konfigurasi keamanan yang lebih ketat, dan penggunaan plugin keamanan tambahan. Menerapkan teknik mitigasi ini diharapkan dapat meningkatkan keamanan situs WordPress Anda secara signifikan, mengurangi kemungkinan serangan, dan melindungi data pengguna Anda. Penelitian ini memberikan wawasan yang dapat ditindaklanjuti bagi administrator situs WordPress agar dapat mengidentifikasi dan memulihkan kerentanan keamanan secara lebih efektif.

Penelitian selanjutnya yang dilakukan oleh [6] Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap. Teknik SQL Injection ini tidak sulit dilakukan, sehingga pemahaman tentang cara kerjanya sangat berguna bagi para admin dan pengembang aplikasi web untuk mengamankan akses pengguna dari serangan. Pengujian ini memungkinkan kita memahami proses serangan dan dampak yang ditimbulkan oleh serangan tersebut. Penelitian selanjutnya dilakukan oleh [7] Penerapan Acunetix Vulnerability Scanner dari Serangan Siber pada Keamanan Website Kampus. Berdasarkan scanning literasi, website Fakultas Teknik UM Sumatera Barat dikategorikan pada tingkat ancaman 3 yang tinggi, terdapat 245 peringatan yang teridentifikasi, di antaranya, 8 dianggap berada pada tingkat high, 2 berada pada tingkat medium, 13 berada ditingkat Low dan selebihnya Informational Berdasarkan evaluasi yang telah

dilakukan, tingkat keamanan yang tercapai berada pada level 0. Pada level ini, tidak terdapat kerentanan yang teridentifikasi (nol kerentanan) dan dukungan keamanan juga mencapai tingkat optimal (nol dukungan).

Penelitian selanjutnya yang dilakukan oleh [8] Analisis dan Rekomendasi Keamanan Website Kampus X Menggunakan ISSAF. Pemindaian menggunakan OWASP ZAP mengidentifikasi 24 alert keamanan, dengan 12,5% di antaranya masuk kategori risiko tinggi, termasuk SQL Injection dan kurangnya Content Security Policy (CSP). Selain itu, simulasi serangan DDoS menunjukkan ketahanan server, tetapi pengujian menunjukkan perlunya peningkatan keamanan pada aspek lain. Rekomendasi utama meliputi implementasi DNSSEC, penutupan port yang tidak digunakan, penambahan CSP header, dan peningkatan perlindungan terhadap serangan berbasis aplikasi web. Penelitian ini menegaskan pentingnya pendekatan holistik dan berkelanjutan dalam pengelolaan keamanan website, termasuk audit berkala dan pemantauan real-time. Dengan strategi ini, diharapkan institusi dapat memperkuat postur keamanan, melindungi aset digital, dan meminimalkan risiko serangan siber yang terus berkembang.

Penelitian selanjutnya yang dilakukan oleh [9] Audit Keamanan Aplikasi Web Studi Kasus pada Website E-Commerce Warung Ayam Goreng Selimut Griya Cirebon. Metodologi yang digunakan dalam audit ini adalah analisis risiko, dan evaluasi terhadap standar keamanan web seperti SiteCheck by Sucuri. Hasil penelitian menunjukkan adanya beberapa kerentanan pada aplikasi web ayam goreng selimut yang perlu segera ditangani untuk menghindari potensi ancaman keamanan

METODOLOGI

Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan metode uji penetrasi (penetration testing) untuk mengevaluasi efektivitas layanan Cloudflare dalam memitigasi serangan siber berbasis Nmap dan Metasploit. Tahapan penelitian dijelaskan sebagai berikut:

Gambar 1. Tahapan-Tahapan Penelitian

1. Perancangan Infrastruktur Pengujian
   Infrastruktur pengujian terdiri atas dua lingkungan:
   a. Server Tanpa Proteksi Cloudflare (Baseline) [10]
      Digunakan untuk mengukur tingkat keberhasilan serangan ketika Cloudflare tidak diaktifkan.
   b. Server dengan Proteksi Cloudflare
      Server yang dikonfigurasi dengan berbagai fitur keamanan Cloudflare seperti Web Application Firewall (WAF), rate limiting, DNS proxy, dan bot management [11].

   Kedua server memiliki aplikasi web sederhana berbasis LAMP stack yang memiliki endpoint login dan beberapa celah keamanan XSS dan SQL Injection[12] sebagai target pengujian.

2. Simulasi Serangan
   Penyerangan dilakukan dalam dua tahap menggunakan tools open-source:

 https://doi.org/10.56211/sudo.v4i1.902

a. Nmap
   Untuk melakukan network scanning dan service enumeration. Parameter seperti -sS, -A, dan --script digunakan untuk memindai port dan mengidentifikasi service serta OS.
b. Metasploit Framework
   Digunakan untuk melakukan eksploitasi berbasis payload umum seperti remote code execution, brute force login, dan SQL injection (melalui module auxiliary dan exploit).
   Setiap serangan dilakukan terhadap kedua lingkungan (dengan dan tanpa Cloudflare) untuk membandingkan efektivitas mitigasi.

3. Konfigurasi Cloudflare
   Fitur-fitur yang dikonfigurasi di sisi Cloudflare antara lain
   a. Aktivasi Web Application Firewall (WAF)[13]
   Penerapan Firewall Rules untuk memblokir User-Agent tertentu (misalnya Nmap)
   b. Rate Limiting untuk endpoint login
   Aktivasi Bot Fight Mode dan Captcha Challenge
   c. Penggunaan proxy DNS dan penyembunyian IP asli server

Pengumpulan dan Analisis Data

Data yang dikumpulkan mencakup:
1. Waktu respon server terhadap serangan
2. Jumlah permintaan (requests) yang diblokir
3. Jenis dan jumlah payload yang berhasil atau gagal [14]
4. Log dari Cloudflare dashboard dan server lokal

Data dianalisis secara kuantitatif untuk mengetahui persentase pengurangan risiko serangan antara server yang tidak menggunakan Cloudflare dan yang menggunakan Cloudflare.

Evaluasi Keamanan

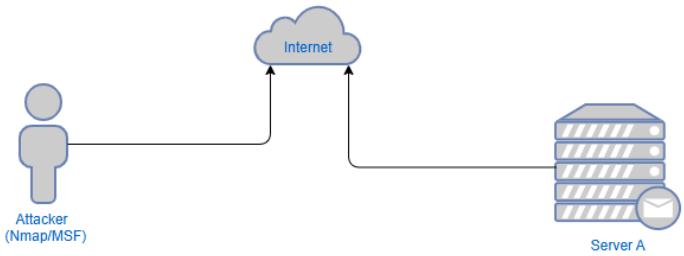
Evaluasi dilakukan dengan membandingkan:
1. Keberhasilan eksploitasi pada kedua kondisi
2. Efektivitas fitur Cloudflare dalam mendeteksi dan memblokir serangan
3. Dampak kinerja server saat menerima beban serangan.

HASIL DAN PEMBAHASAN

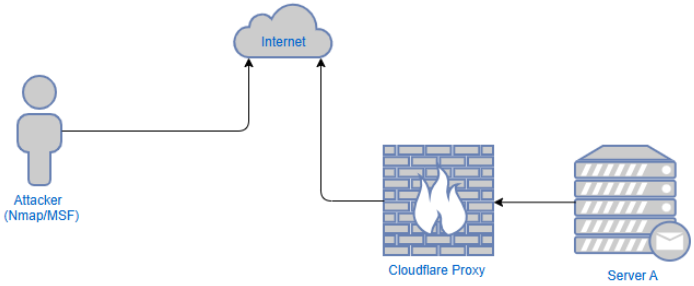
Perancangan Infrastruktur Pengujian

Struktur topologi dalam pengujian ini dibagi menjadi dua skenario utama yang bertujuan untuk mengevaluasi tingkat keamanan sistem sebelum dan sesudah penerapan layanan Cloudflare. Skenario pertama (Tanpa Cloudflare) merepresentasikan kondisi di mana server web langsung terhubung ke jaringan internet tanpa adanya lapisan perlindungan tambahan. Dalam keadaan ini, alamat IP publik serta port yang terbuka dapat dengan mudah diakses oleh pihak luar, menjadikan server lebih rentan terhadap aktivitas pemindaian dan upaya eksploitasi menggunakan tools Nmap dan Metasploit.

Sebaliknya, Skenario kedua (Dengan Cloudflare) menggambarkan situasi di mana server dilindungi oleh Cloudflare yang berperan sebagai reverse proxy. Pada skenario ini, setiap permintaan yang masuk akan terlebih dahulu melewati sistem keamanan Cloudflare sebelum mencapai server utama, sehingga IP publik dari server disamarkan. Selain itu, fitur keamanan seperti Web Application Firewall (WAF), perlindungan terhadap DDoS, dan pembatasan laju akses (rate limiting) dapat diaktifkan guna memperkuat pertahanan terhadap potensi serangan siber. Skenario tersebut digambarkan sebagai berikut:



Gambar 2. Skenario A



Gambar 3. Skenario B

Tabel 1. Komponen Infrastruktur

Komponen	Fungsi
Web Server	Target simulasi serangan. Dapat digunakan Apache/Nginx dengan CMS (WordPress) atau aplikasi dummy yang memiliki celah.
Cloudflare	Reverse proxy, DNS dan firewall untuk menyembunyikan IP asli & menyaring traffic.
Kali Linux	Digunakan sebagai mesin penyerang, berisi Nmap, Metasploit, dll.
Nmap	Untuk melakukan scanning port dan service enumeration.
Metasploit	Untuk eksploitasi celah keamanan pada server target.

Simulasi Serangan

Melakukan ping target

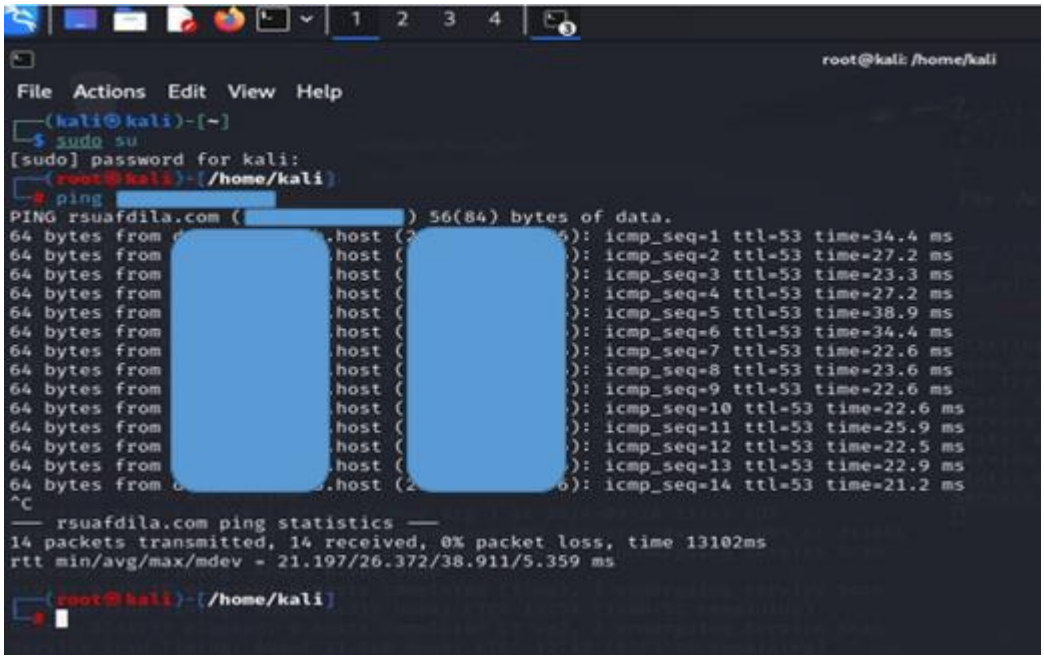
Keterangan

Target: xxxxxx.com

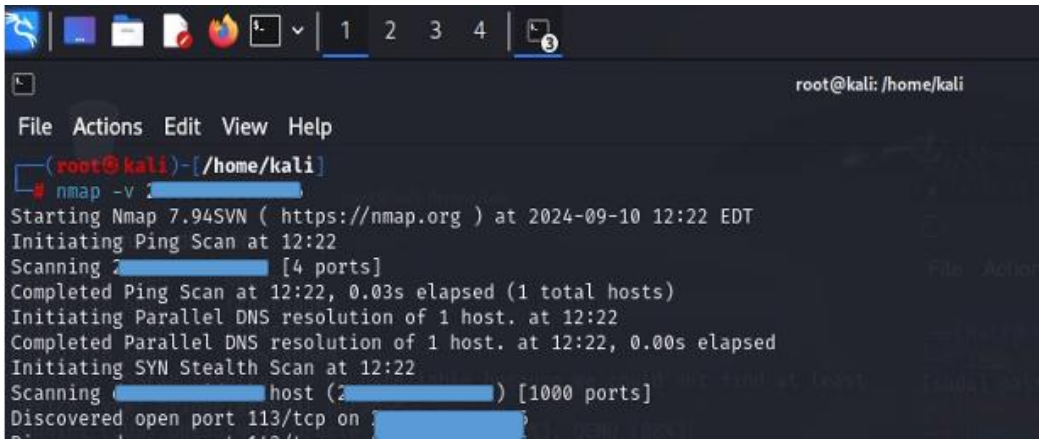
Ip <xx.161.xx.76>: Mengirimkan paket ping ke situs xxxxxx.com untuk mendeteksi Ip host < xx.161.xx.76> tersebut aktif atau responsif.

Hasil: Memberikan informasi tentang waktu respon dari host.

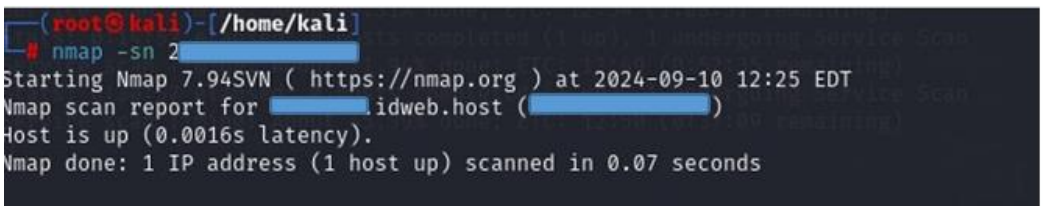
 https://doi.org/10.56211/sudo.v4i1.902



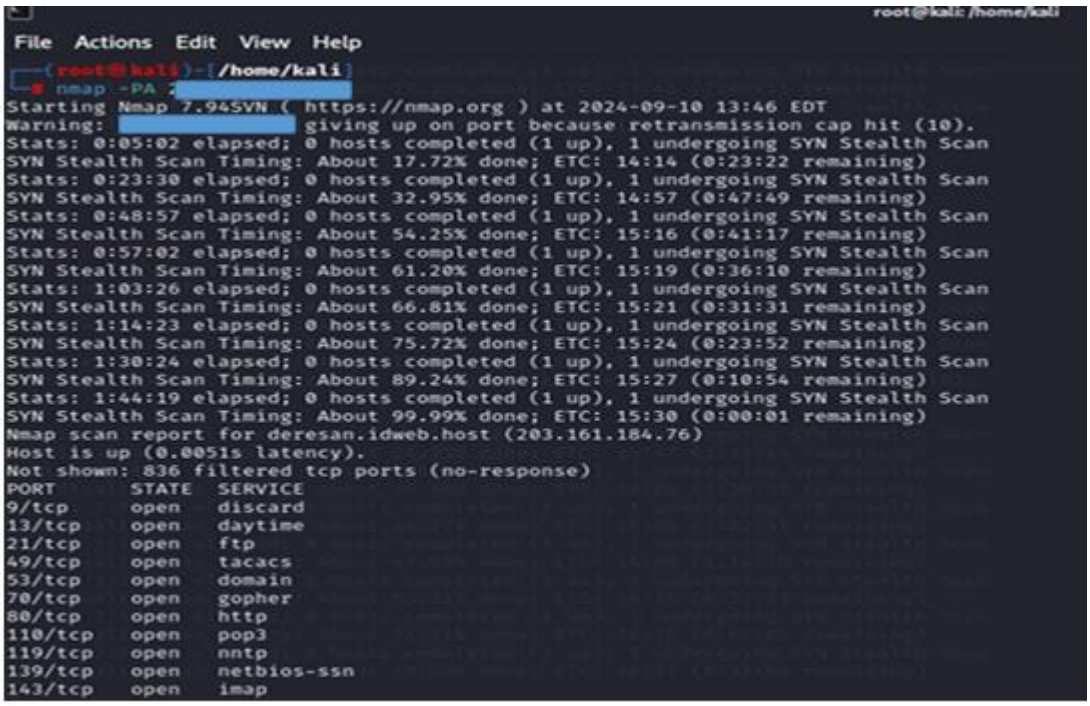
nmap-v xx.161.xx.76
KeteranganMenggunakan pemindaian dasar pada host sambil menampilkan lebih banyak detail tentang proses pemindaian. Hasil Detail informasi tentang port terbuka, layanan yang aktif



nmap-sn xx.161.xx.76
Keterangan: Melakukan pemindaian tanpa port scan . Ini hanya memeriksa apakah host hidup atau mati tanpa melakukan pemindaian ke port.
Hasil Mengetahui apakah host aktif, tanpa rincian port



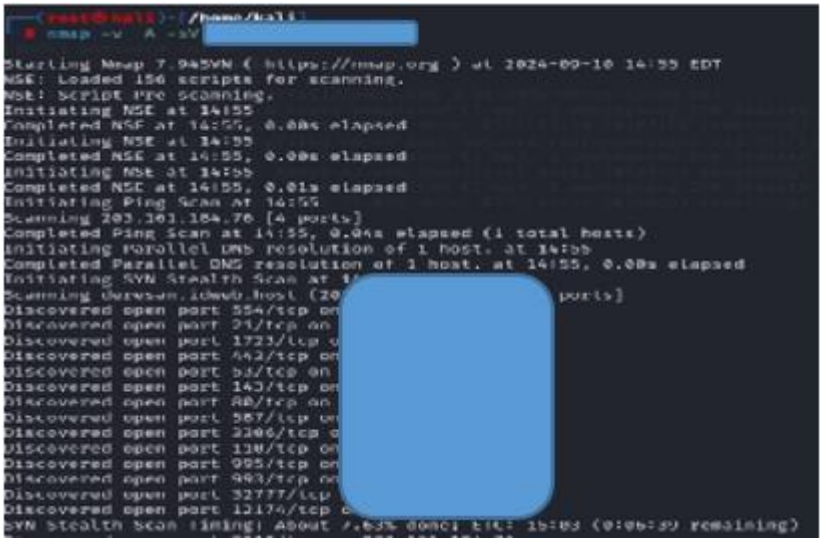
nmap-PA xx.161.xx.76
Keterangan Mengirim paket ke host untuk memeriksa status port open/close, sering digunakan untuk melewati firewall.
Hasiil Mengirim paket ke host untuk memeriksa port, umum digunakan untuk melewati firewall.



nmap-v-A-Sv 203.161.184.76

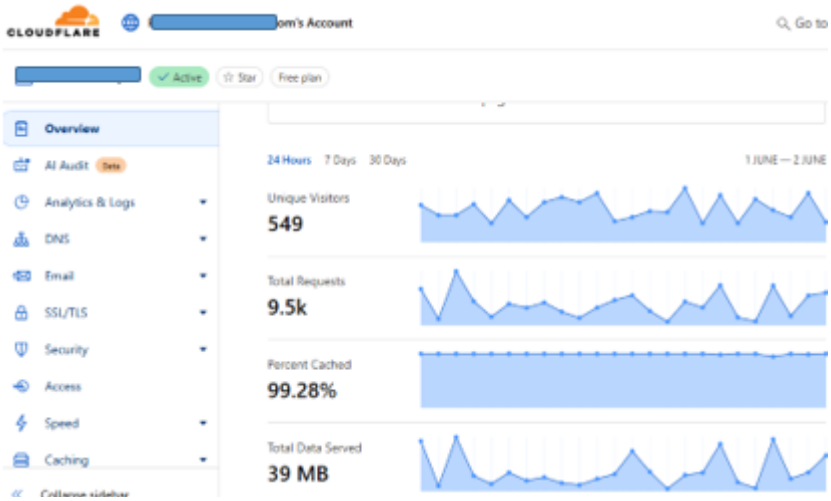
Keterangan: Pemindaian verbose (-v) dengan mode agresif (-A) serta deteksi versi layanan (-sV), memberikan hasil pemindaian yang sangat rinci.

Hasil: Deteksi sistem operasi, layanan, versi, traceroute, dan informasi rinci lainnya tentang host target.



 https://doi.org/10.56211/sudo.v4i1.902

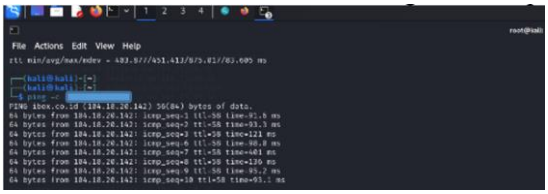
Konfigurasi Cloudflare



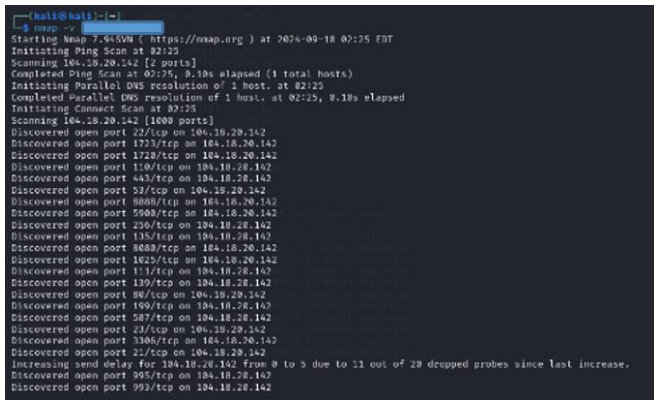
Pengumpulan dan Analisis Data

Setelah konfigurasi Cloudflare selesai dilakukan, langkah selanjutnya adalah melakukan pengujian ulang untuk mengevaluasi hasil dari konfigurasi tersebut. Adapun tahapan pengujian yang dilakukan adalah sebagai berikut:

Melakukan ping target
Keterangan Target xxxxxx.com



Nmap -v



Nmap -o -Sv

Analisis data dalam penelitian ini bertujuan untuk membandingkan hasil pengujian antara dua skenario, yaitu server yang tidak menggunakan Cloudflare dan server yang berada di balik layanan Cloudflare. Data yang dianalisis meliputi hasil pemindaian menggunakan Nmap dan percobaan eksploitasi menggunakan Metasploit pada kedua skenario. Pada skenario tanpa Cloudflare, hasil pemindaian menunjukkan bahwa sejumlah port terbuka dapat dengan mudah diidentifikasi, dan informasi mengenai versi layanan serta sistem operasi target berhasil dikumpulkan. Hal ini memberikan celah bagi penyerang untuk melakukan eksploitasi, yang dalam pengujian terbukti berhasil mengakses sistem melalui celah keamanan yang ditemukan.

Sebaliknya, pada skenario dengan Cloudflare, data menunjukkan bahwa permintaan dari Nmap cenderung dibatasi atau diblokir. Sebagian besar port tidak terdeteksi, informasi sistem tidak dapat diperoleh, dan upaya eksploitasi melalui Metasploit gagal dilakukan karena akses ke IP asli server tidak tersedia. Selain itu, fitur proteksi tambahan seperti rate limiting dan Web Application Firewall (WAF) secara aktif memblokir permintaan yang mencurigakan, yang terlihat dari log dan notifikasi pada dashboard Cloudflare. Hasil ini mengindikasikan bahwa Cloudflare mampu memberikan perlindungan signifikan terhadap serangan tahap awal seperti scanning dan reconnaissance, serta menghambat proses eksploitasi secara langsung.

Secara keseluruhan, analisis ini memperkuat hipotesis bahwa implementasi layanan Cloudflare dapat mempersulit dan bahkan mencegah proses serangan yang dilakukan dengan metode umum, seperti yang disimulasikan dalam pengujian ini. Data kuantitatif dan kualitatif yang diperoleh dari kedua skenario mendukung kesimpulan bahwa Cloudflare berfungsi tidak hanya sebagai penyembunyi IP dan pengatur lalu lintas, tetapi juga sebagai lapisan keamanan aktif yang efektif dalam konteks pertahanan siber.

Evaluasi Keamanan

Perkembangan teknologi informasi yang semakin pesat telah mendorong berbagai institusi, baik pemerintah maupun swasta, untuk bergantung pada sistem berbasis web dalam menjalankan aktivitas operasional, komunikasi, dan pelayanan publik. Ketergantungan ini, meskipun meningkatkan efisiensi, juga memperbesar permukaan serangan (attack surface) terhadap sistem digital, sehingga risiko serangan siber menjadi lebih nyata dan kompleks. Salah satu jenis ancaman yang paling umum dan sering dijadikan tahap awal dari serangan yang lebih besar adalah reconnaissance—yakni proses pengintaian atau pemetaan jaringan—yang biasanya dilakukan melalui network scanning menggunakan tools seperti Nmap. Tahap ini sering diikuti oleh eksploitasi, yang dapat dilakukan dengan memanfaatkan framework seperti Metasploit untuk memanfaatkan celah keamanan yang terdeteksi. Kedua tools ini, Nmap dan Metasploit, meskipun digunakan secara luas dalam pengujian keamanan yang etis, juga merupakan alat yang sangat umum digunakan oleh aktor jahat untuk mengeksekusi serangan terhadap target yang rentan. Dalam skenario riil, serangan pemindaian dan eksploitasi ini dapat membuka akses tidak sah ke server, memungkinkan penyisipan malware, hingga pencurian informasi sensitif. Oleh karena itu, evaluasi terhadap efektivitas sistem pertahanan yang mampu mencegah atau meminimalkan dampak dari tahapan serangan ini sangat penting dalam pengembangan kebijakan keamanan informasi.

Dalam konteks ini, Cloudflare hadir sebagai salah satu solusi yang menyediakan lapisan keamanan tambahan melalui teknologi reverse proxy, Web Application Firewall (WAF), Content Delivery Network (CDN), serta proteksi terhadap serangan DDoS, bot, dan aktivitas pemindaian mencurigakan. Fitur-fitur ini dirancang tidak hanya untuk mempercepat kinerja website, tetapi juga untuk mengamankan sistem dengan cara menyembunyikan IP asli server, memblokir trafik berbahaya, dan membatasi akses ke endpoint penting. Penelitian ini mengevaluasi efektivitas implementasi Cloudflare melalui dua skenario pengujian: pertama, server yang langsung terekspos ke internet tanpa perlindungan Cloudflare; dan kedua, server yang dilindungi oleh Cloudflare. Evaluasi dilakukan dengan mengamati perbedaan hasil pemindaian Nmap serta upaya eksploitasi Metasploit pada kedua konfigurasi. Parameter yang dianalisis mencakup jumlah dan jenis port yang terdeteksi, identifikasi sistem operasi dan layanan, keberhasilan payload eksploitasi, serta respons server terhadap serangan.

KESIMPULAN DAN SARAN

Penerapan layanan Cloudflare terbukti mampu melindungi informasi server asli dari berbagai upaya pemindaian dan eksploitasi siber. Hasil pengujian menggunakan Nmap menunjukkan bahwa detail penting seperti alamat IP publik, port aktif, serta jenis sistem operasi menjadi sulit untuk diidentifikasi setelah Cloudflare diaktifkan. Hal ini karena Cloudflare berfungsi sebagai reverse proxy yang menghubungkan pengguna dengan server di belakangnya, sehingga menyembunyikan identitas asli server dari akses langsung. Dalam pengujian lebih lanjut dengan Metasploit, serangan terhadap IP asli tidak berhasil karena Cloudflare mampu memfilter dan menolak koneksi yang langsung menuju server backend. Fitur keamanan seperti Web Application Firewall (WAF) memungkinkan Cloudflare mendeteksi dan mencegah serangan umum, seperti SQL injection, remote code execution (RCE), maupun cross-site scripting (XSS).

Di samping itu, Cloudflare juga menambahkan lapisan proteksi terhadap ancaman otomatis dengan menyediakan fitur CAPTCHA, pembatasan laju akses (rate-limiting), dan pengelolaan bot, yang efektif dalam mengurangi risiko serangan brute force serta pemindaian masif. Meski demikian, tingkat perlindungan ini sangat bergantung pada keamanan IP asli

 https://doi.org/10.56211/sudo.v4i1.902

server. Apabila IP tersebut bocor—melalui celah seperti DNS leak, kesalahan konfigurasi subdomain, atau metadata—maka potensi serangan langsung ke server tetap ada. Selain itu, layanan non-web seperti FTP dan SSH tidak sepenuhnya terlindungi oleh Cloudflare kecuali dilakukan konfigurasi tambahan secara khusus.

DAFTAR PUSTAKA

[1] M. F. Susanto, A. Nurcahyo, and M. Rahayu, "Website Threat Monitoring Untuk Pemantauan dan Analisis Ancaman Pada Web Server," *Pros. Ind. Res. Work. Natl. Semin.*, vol. 13, no. 01, pp. 369–374, 2022, [Online]. Available: https://jurnal.polban.ac.id/ojs-3.1.2/proceeding/article/view/4213

[2] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," *Transmisi*, vol. 24, no. 3, pp. 83–91, 2022, doi: 10.14710/transmisi.24.3.83-91.

[3] H. Jayusman and F. Mahardika, "Mobile-Based Event Decoration Ordering System Using UAT Method with PIECES Framework," *J. Innov. Inf. Technol. Appl.*, vol. 7, pp. 1623–172, 2024.

[4] D. Supriadi, E. Suryadi, R. Muslim, L. D. Samsumar, and U. T. Mataram, "IMPLEMENTASI VULNERABILITY ASSESSMENT OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA WEBSITE," vol. 1, no. 4, pp. 232–240, 2024.

[5] G. T. A. Ramadhani, M. R. R. Steyer, M. H. Maulidan, and A. Setiawan, "Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 15, 2024, doi: 10.47134/pjise.v1i4.2613.

[6] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 9, 2024, doi: 10.47134/pjise.v1i4.2623.

[7] R. R. Rezki Rusydi, Yuhandri, and S. Arlis, "Penerapan Acunetix Vulnerability Scanner dari Serangan Siber pada Keamanan Website Kampus," *J. KomtekInfo*, vol. 11, pp. 173–180, 2024, doi: 10.35134/komtekinfo.v11i3.569.

[8] M. Saputra, D. W., Pradini, R. S., & Anshori, "Analisis dan Rekomendasi Keamanan Website Kampus X," *J. Indones. Manaj. Inform. dan Komun.*, vol. 6, no. 1, pp. 830–843, 2025.

[9] N. Amelia, "Audit Keamanan Aplikasi Web: Studi Kasus pada Website E-Commerce Warung Ayam Goreng Selimut Griya Cirebon," *TEKNOFILE J. Sist. Inf.*, vol. 3, no. 4, pp. 1–23, 2025.

[10] D. Intan *et al.*, "IoT-Based Smart Air Conditioner as a Preventive in the Post-COVID-19 Era: A Review," *journal.umy.ac.idDIS Saputra, IPD Suarnatha, F Mahardika, A Wijanarko, SW HandaniJournal Robot. Control (JRC), 2023•journal.umy.ac.id*, vol. 4, no. 1, 2023, doi: 10.18196/jrc.v4i1.17090.

[11] R. B. B. Sumantri, G. Subari, F. Mahardika, and H. Jayusman, "Perbandingan Efisiensi Waktu Proses Pengaksesan Data Antara Query Berbentuk Join Dengan Subselect," *METHOMIKA J. Manaj. Inform. dan Komputerisasi Akunt.*, vol. 7, no. 1, pp. 25–33, 2023, doi: 10.46880/jmika.vol7no1.pp25-33.

[12] A. A.-P. Y. P. A. Teknik and undefined 2021, "Managemen Sistem Basis Data (SQL dan MySql)," *penerbit.stekom.ac.id*, Accessed: Aug. 18, 2024. [Online]. Available: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/307

[13] F. Mahardika *et al.*, "Review FotoForensic.com dengan Teknik Eror Level Analysis dan JPEG untuk mengetahui Citra Asli," *J. Inform. J. Pengemb. IT*, vol. 3, no. 1, pp. 71–75, Jan. 2018, doi: 10.30591/JPIT.V3I1.690.

[14] F. Mahardika, A. Fitriani, and M. Al Amin, "Testing Sistem pada Dealer Management System Service Menggunakan Metode Black Box Testing," *Hello World J. Ilmu Komput.*, vol. 2, no. 3, pp. 110–119, 2023.