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

Network Security

Pendekatan Metodologis dalam Deteksi Ancaman Siber pada Server Hosting Menggunakan NMAP dan Metasploit

Yudiansyah Fauzi[*], *Rifky Aditia Hamdan*

Prodi Rekayasa Keamanan Siber, Politeknik Piksi Input Serang, Banten, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 23 Mei 2025
Revisi Akhir: 01 Juni 2025
Diterbitkan *Online*: 02 Juni 2025

KATA KUNCI

Keamanan Siber
Deteksi Ancaman
NMAP
Metasploit

KORESPONDENSI (*)

Phone: 0812-8993-2696
E-mail: yudiansyahfauzi@gmail.com

A B S T R A K

Server hosting merupakan salah satu elemen esensial dalam struktur teknologi informasi modern. Meski memiliki peran yang sangat strategis, server ini juga menjadi sasaran utama serangan siber karena tingkat kerentanannya yang tinggi. Oleh sebab itu, deteksi dini terhadap potensi ancaman siber menjadi hal yang sangat penting dalam menjaga keberlangsungan dan keamanan layanan digital. Penelitian ini difokuskan pada penerapan pendekatan metodologis dalam proses identifikasi ancaman siber terhadap server hosting, dengan mengandalkan dua perangkat utama, yakni NMAP dan Metasploit. NMAP berperan dalam pemindaian jaringan guna mendeteksi port yang terbuka, layanan yang aktif, serta sistem operasi yang digunakan pada server target. Adapun Metasploit digunakan dalam tahap eksploitasi untuk menguji kerentanan yang teridentifikasi secara terkendali, sebagai bagian dari proses uji penetrasi. Seluruh tahapan pengujian dilakukan dalam lingkungan server simulatif, sehingga dapat merepresentasikan kondisi ancaman secara lebih realistis. Hasil yang diperoleh menunjukkan bahwa integrasi antara NMAP dan Metasploit secara signifikan mampu mengungkap celah keamanan potensial, serta menyediakan informasi teknis yang berguna untuk perencanaan mitigasi risiko. Berdasarkan temuan tersebut, dapat disimpulkan bahwa penggunaan pendekatan metodologis yang memanfaatkan perangkat open-source seperti NMAP dan Metasploit mampu meningkatkan efektivitas deteksi serta respons terhadap ancaman keamanan siber. Penelitian ini juga memberikan rekomendasi teknis yang dapat dijadikan acuan dalam memperkuat strategi pertahanan siber, khususnya pada sistem server hosting di lingkungan yang berisiko tinggi terhadap serangan digital.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah mengubah paradigma dalam penyediaan layanan digital di berbagai sektor, termasuk pemerintahan, pendidikan, dan industri. Dalam konteks ini, server hosting berfungsi sebagai infrastruktur utama yang menopang sistem informasi dan layanan daring. Peran strategis server hosting dalam manajemen data dan distribusi layanan menjadikannya elemen krusial yang menuntut ketersediaan, integritas, dan kerahasiaan informasi secara berkelanjutan. Namun, ketergantungan yang tinggi terhadap infrastruktur ini secara tidak langsung meningkatkan eksposur terhadap berbagai jenis ancaman siber, terutama yang berkaitan dengan eksploitasi kerentanan sistem dan akses tidak sah.

Ancaman terhadap keamanan server hosting dapat bersumber dari berbagai kelemahan, antara lain konfigurasi sistem yang kurang tepat, kerentanan pada perangkat lunak yang digunakan, serta minimnya pengawasan terhadap aktivitas lalu lintas jaringan. Untuk mengantisipasi potensi risiko tersebut, dibutuhkan pendekatan metodologis yang komprehensif dan sistematis dalam proses identifikasi serta deteksi dini terhadap celah keamanan. Salah satu strategi mitigasi yang dapat diterapkan secara efektif adalah melalui uji penetrasi dan pemindaian keamanan menggunakan perangkat lunak yang telah terbukti kredibel dalam dunia keamanan jaringan.

https://doi.org/10.56211/sudo.v4i1.868

Dalam hal ini, NMAP (Network Mapper) merupakan salah satu alat pemindai jaringan yang mampu mengidentifikasi port terbuka, layanan aktif, serta sistem operasi yang berjalan pada suatu host. Sementara itu, Metasploit adalah kerangka kerja eksploitasi yang umum digunakan dalam kegiatan pengujian penetrasi untuk mengevaluasi tingkat kerentanan sistem secara terkendali. Kedua perangkat ini banyak digunakan oleh profesional keamanan informasi untuk keperluan deteksi, analisis, dan validasi terhadap ancaman yang mungkin mengganggu integritas sistem jaringan dan server.

Penelitian yang dilakukan [1] Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan Sistem Informasi Sekolah MTsN 8 Bantul sebelum diluncurkan, guna mencegah potensi ancaman seperti pencurian data dan penyalahgunaan hak akses. Metode yang digunakan adalah Information System Security Assessment Framework (ISSAF) untuk mengklasifikasikan aspek keamanan sistem, serta penetration testing dengan tool Kali Linux, Nmap, dan Wireshark.

Penelitian ini bertujuan untuk mengkaji efektivitas pendekatan metodologis berbasis penggunaan Nmap dan Metasploit dalam mendeteksi ancaman siber pada sistem server hosting. Melalui penerapan skenario pengujian yang terstruktur dan sistematis, penelitian ini diharapkan mampu memberikan kontribusi baik secara akademik maupun praktis dalam penguatan sistem keamanan informasi, khususnya dalam merespons dinamika dan kompleksitas ancaman siber yang terus berkembang. Permasalahan utama yang diangkat dalam penelitian ini adalah rendahnya penerapan mekanisme deteksi kerentanan yang efektif dan terstandar pada berbagai server hosting, terutama pada lingkungan dengan keterbatasan sumber daya. Hal ini menjadi krusial mengingat bahwa serangan siber tidak hanya menyasar infrastruktur berskala besar, tetapi juga sistem yang memiliki pertahanan minimum dan belum melalui pengujian keamanan menyeluruh.

Dalam konteks tersebut, pemanfaatan Nmap sebagai alat pemindaian jaringan dan Metasploit sebagai platform uji eksploitasi menawarkan pendekatan teknis yang terjangkau, praktis, dan terbukti mampu mengidentifikasi titik-titik kerentanan dalam sistem. Meskipun kedua perangkat lunak ini telah dikenal luas dalam dunia keamanan informasi, belum banyak penelitian yang menggabungkan keduanya dalam suatu pendekatan metodologis yang sistematis, khususnya dalam konteks server hosting. Oleh karena itu, penelitian ini menjadi penting untuk mengisi kesenjangan tersebut dan menawarkan solusi berbasis teknologi yang dapat diterapkan secara luas.

TINJAUAN PUSTAKA

Penulis melampirkan penelitian terdahulu yang berkaitan dengan penelitian penulis. Penelitian terdahulu sebagai berikut: penelitian yang dilakukan oleh [2] Network Penetration dan Security Audit Menggunakan Nmap. Ancaman terhadap keamanan jaringan, khususnya yang berasal dari eksternal, merupakan tantangan yang terus berkembang seiring dengan pesatnya kemajuan teknologi informasi dan digitalisasi data. Dalam konteks ini, penting bagi organisasi atau institusi, seperti SMA Alfa Centauri, untuk memiliki sistem pertahanan jaringan yang andal dan adaptif. Salah satu pendekatan yang relevan dalam mengidentifikasi dan mengatasi potensi celah keamanan adalah melalui pengujian penetrasi (penetration testing) menggunakan perangkat lunak Nmap. Penelitian sekarang mengkaji efektivitas pendekatan metodologis berbasis penggunaan NMAP dan Metasploit dalam mendeteksi ancaman siber pada server hosting. Melalui penerapan skenario uji yang sistematis, penelitian ini diharapkan dapat memberikan kontribusi akademik dan praktis terhadap penguatan sistem keamanan informasi, khususnya dalam menghadapi dinamika dan kompleksitas ancaman siber yang semakin berkembang.

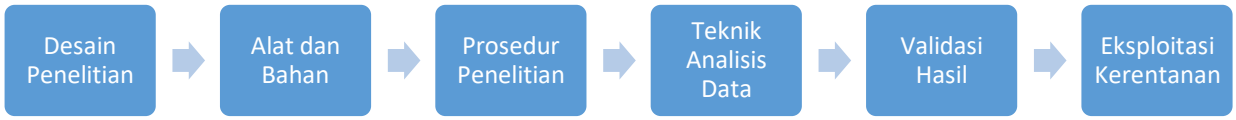
Penelitian yang dilakukan oleh [3] Towards pentesting automation using the metasploit framework. Hasil evaluasi menunjukkan bahwa kerangka kerja yang diusulkan mampu mengeksploitasi sejumlah sistem dengan baik dan memiliki potensi untuk diperluas guna mendukung kelas eksploitasi baru serta metodologi pentesting yang lebih luas. Penelitian sekarang mengkaji efektivitas pendekatan metodologis berbasis penggunaan NMAP dan Metasploit dalam mendeteksi ancaman siber pada server hosting. Melalui penerapan skenario uji yang sistematis, penelitian ini diharapkan dapat memberikan kontribusi akademik dan praktis terhadap penguatan sistem keamanan informasi, khususnya dalam menghadapi dinamika dan kompleksitas ancaman siber yang semakin berkembang.

Penelitian yang dilakukan oleh [4] Implementasi Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Metasploit Exploit Menggunakan Snort Dan Wireshark. Dengan menggunakan Intrusion Detection System Snort bertujuan agar dapat melakukan scaning terhadap setiap serangan yang masuk ke dalam jaringan komputer dan sangat membantu dalam minimalisir kerusakan sistem yang dilakukan oleh penyerang. untuk menganalisis lalu lintas jaringan

dari paket Remote Exploit digunakan Wireshark sebagai pendeteksi serangan, dan dilakukan pembuktian apakah paket tersebut merupakan virus atau bukan dengan menggunakan Virus Total. Penelitian sekarang mengkaji efektivitas pendekatan metodologis berbasis penggunaan NMAP dan Metasploit dalam mendeteksi ancaman siber pada server hosting. Melalui penerapan skenario uji yang sistematis, penelitian ini diharapkan dapat memberikan kontribusi akademik dan praktis terhadap penguatan sistem keamanan informasi, khususnya dalam menghadapi dinamika dan kompleksitas ancaman siber yang semakin berkembang.

METODOLOGI

Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan tujuan mengevaluasi efektivitas deteksi ancaman siber terhadap server hosting melalui pemanfaatan perangkat open-source, yaitu NMAP dan Metasploit [5] [6]. Tahapan penelitian disusun secara sistematis untuk memastikan validitas hasil serta keterukuran dalam proses deteksi dan eksploitasi kerentanan.



Gambar 1. Pendekatan Eksperimen Kuantitatif

1. Desain Penelitian
   Penelitian dilakukan dengan metode simulasi pengujian keamanan pada lingkungan server virtual [14]. Server target dikonfigurasi menggunakan sistem operasi Linux berbasis Ubuntu, dengan layanan umum seperti OpenSSH, Apache, dan MySQL [7][8], yang secara sengaja dibiarkan memiliki konfigurasi standar guna mensimulasikan lingkungan yang rentan.
2. Alat dan Bahan
   NMAP (Network Mapper): Digunakan untuk melakukan pemindaian jaringan dan mengidentifikasi port terbuka, layanan aktif, serta sistem operasi yang berjalan. Metasploit Framework: Dimanfaatkan untuk eksploitasi kerentanan secara terkendali [16], sebagai bagian dari proses penetration testing. VirtualBox/VMware [9]: Digunakan untuk menciptakan lingkungan server dan attacker secara virtual. Kali Linux sebagai sistem operasi penyerang (attacker).
3. Prosedur Penelitian
   Langkah-langkah penelitian dilakukan sebagai berikut:
   a. Identifikasi Target
      Server target disiapkan dalam kondisi default dan dihubungkan dalam jaringan internal dengan mesin penyerang.
   b. Pemindaian dengan NMAP [10]
      NMAP dijalankan untuk mengidentifikasi port yang terbuka dan layanan yang sedang berjalan.
   c. Analisis Hasil Scan
      Data dari NMAP digunakan untuk menentukan potensi celah keamanan yang dapat dieksploitasi.
   d. Eksploitasi dengan Metasploit [11]
      Berdasarkan hasil pemindaian, modul eksploitasi yang sesuai dijalankan melalui Metasploit untuk menguji kerentanan yang terdeteksi.
   e. Evaluasi Keberhasilan [12]
      Tingkat keberhasilan eksploitasi, dampak terhadap sistem, dan respon dari server dicatat untuk dianalisis.
4. Teknik Analisis Data
   Data yang diperoleh dianalisis secara deskriptif kuantitatif untuk mengukur:
   a. Jumlah port terbuka dan layanan yang rentan[15]
   b. Jumlah eksploitasi yang berhasil
   c. Tingkat efektivitas integrasi NMAP dan Metasploit [13] dalam mengidentifikasi dan mengeksploitasi celah keamanan

HASIL DAN PEMBAHASAN

Identifikasi Target

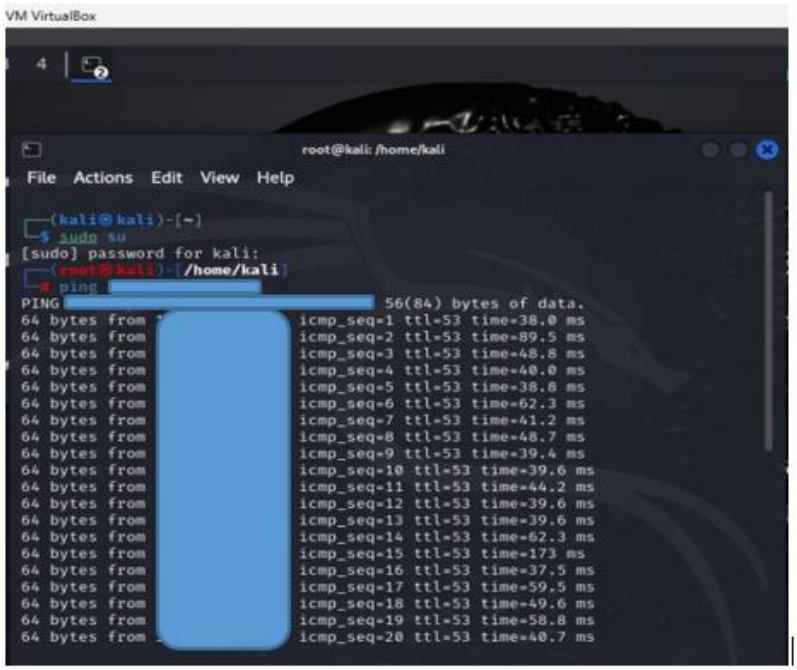
Dalam tahap identifikasi target, dua aktivitas utama yang dilakukan meliputi pengumpulan informasi secara pasif (passive reconnaissance) dan penentuan batas lingkup pengujian (scope definition). Pengumpulan data secara pasif bertujuan untuk mengenali komponen dasar dari sistem yang menjadi sasaran, seperti nama domain, alamat IP, serta konfigurasi sistem hosting yang dapat diakses secara publik. Tahap ini dilakukan tanpa melakukan interaksi langsung dengan sistem target, sehingga tidak memicu sistem deteksi ancaman atau mengganggu operasional jaringan.

Tahapan berikutnya adalah menentukan cakupan pengujian, yang bertujuan untuk memastikan bahwa proses pentesting dilakukan dalam koridor yang aman dan sesuai dengan kebijakan yang berlaku. Pada tahap ini, dilakukan identifikasi terhadap alamat IP, subnet, dan server yang termasuk dalam wilayah yang sah untuk diuji.

Langkah ini penting untuk menghindari pelanggaran hukum serta mencegah dampak yang tidak diinginkan terhadap sistem di luar ruang lingkup yang telah ditentukan. Penetapan ruang lingkup pengujian menjadi dasar penting dalam menjamin integritas, tanggung jawab, dan profesionalisme selama kegiatan uji keamanan berlangsung.

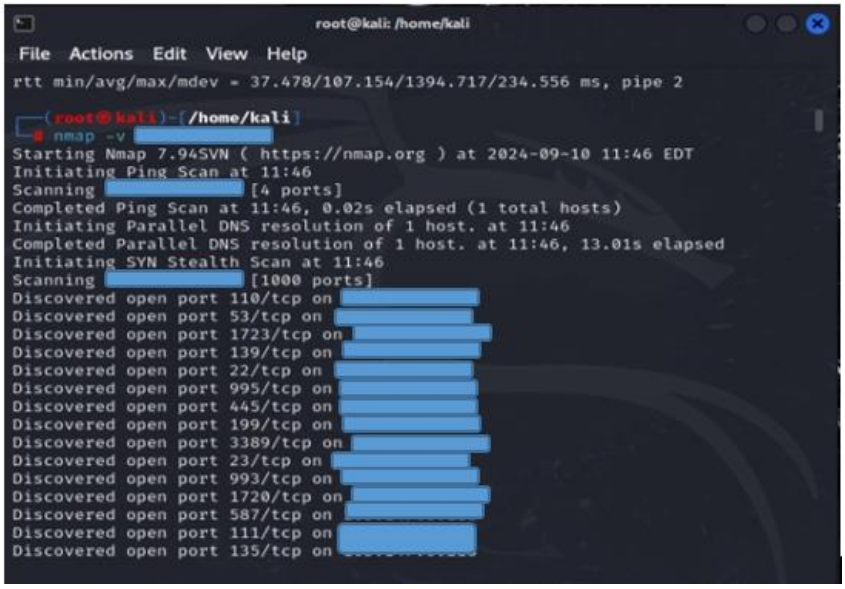
Pemindaian dengan NMAP

Ping digunakan untuk memeriksa konektivitas pada sebuah domain web. Dengan menggunakan ping, kita dapat memeriksa sebuah server web terkoneksi atau tidak.



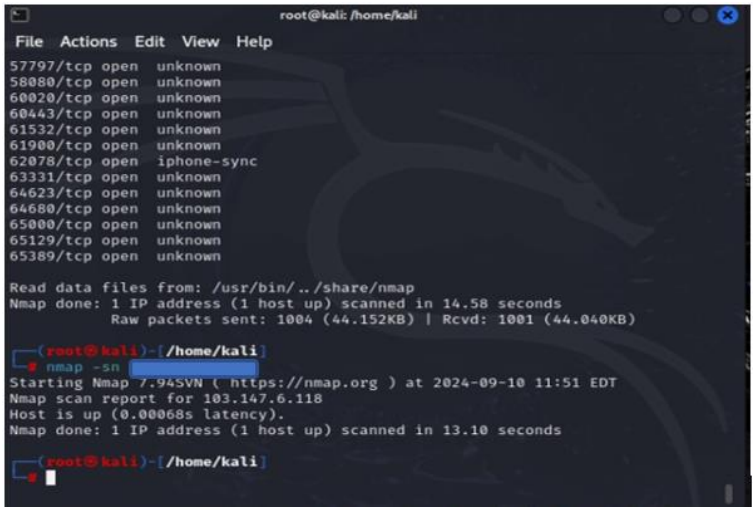
Gambar 2. Ping Nmap

Perintah nmap –v digunakan untuk memindai alamat IP dan ditampilkan seluruh informasi terkait port mana yang terbuka



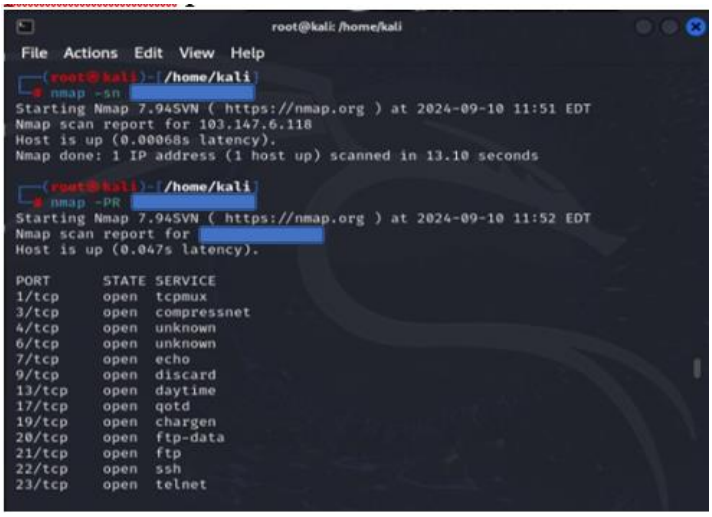
Gambar 3. Perintah nmap –v

Perintah nmap –sn digunakan untuk mencari perangkat aktif dalam rentang IP tertentu secara detail.



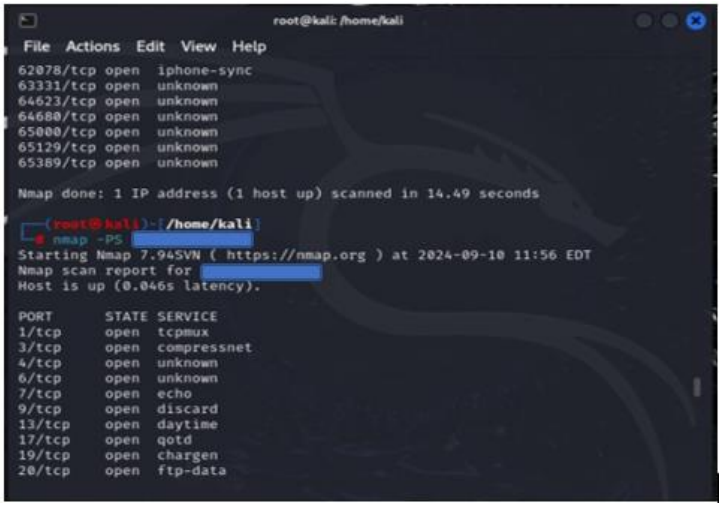
Gambar 4. Perintah nmap –sn

Perintah nmap –PR digunakan untuk mendeteksi host yang hidup tanpa melakukan pemindaian port



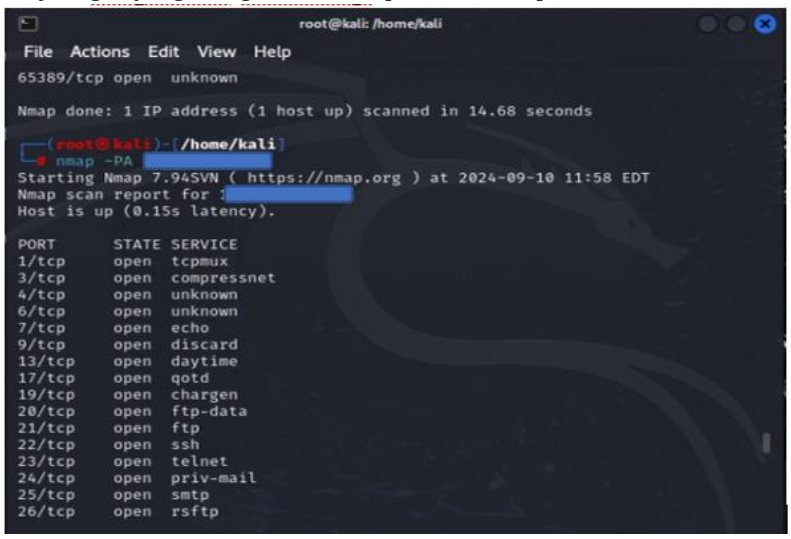
Gambar 5. Perintah nmap –PR

Perintah nmap –PS digunakan untuk melakukan penemuan host yang aktif pada jaringan dengan menggunakan TCP SYN



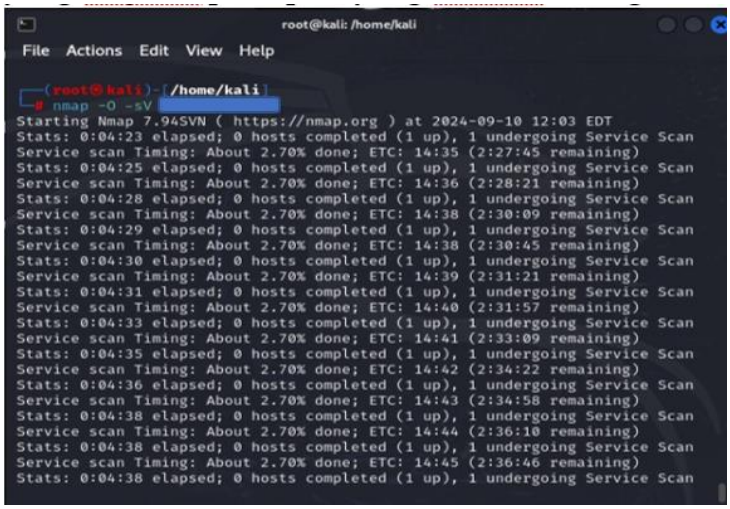
Gambar 6. Perintah nmap –PS

Perintah nmap –PA digunakan untuk melakukan penemuan host dengan menggunakan TCP ACK dimana lebih efektif dalam mendeteksi perangkat di jaringan yang mungkin tidak responsif terhadap ICMP atau TCP SYN



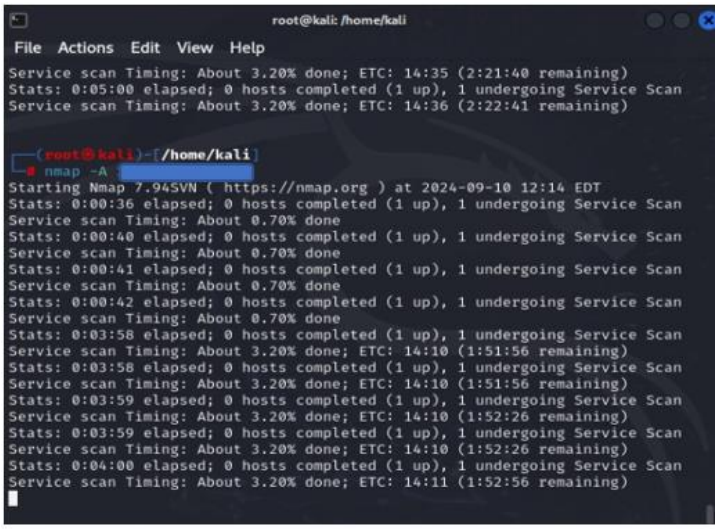
Gambar 7. Perintah nmap –PA

Perintah nmap –O –sV digunakan untuk mendeteksi sistem operasi dan versi dari layanan yang berjalan pada port yang terbuka di target



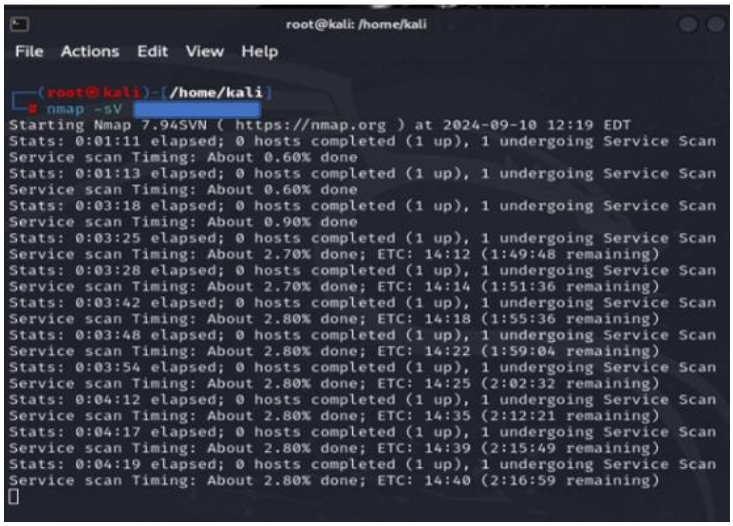
Gambar 8. Perintah nmap –O –sV

Perintah nmap –A digunakan untuk melakukan pemindaian yang lebih mendalam untuk mencari kerentanan atau mengumpulkan informasi tambahkan



Gambar 9. Perintah nmap –A

Perintah nmap –sV digunakan untuk mendeteksi port-port yang terbuka dimana dapat memberikan informasi tentang aplikasi dan versi yang sedang berjalan

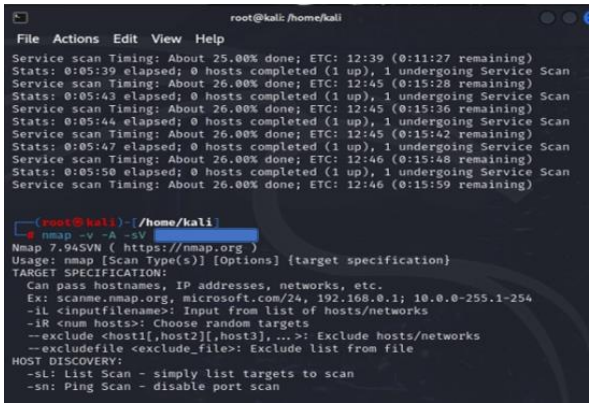


Gambar 10. Perintah nmap –A

Perintah nmap –F -sV digunakan untuk mendapatkan informasi tentang port-port yang paling umum dibuka

Gambar 11. Perintah nmap –F -sV

Perintah nmap –v –A –sV digunakan untuk memberikan informasi tentang sistem operasi, versi layanan, serta output dari pemindaian tersebut



Gambar 12. Perintah nmap –v –A –sV

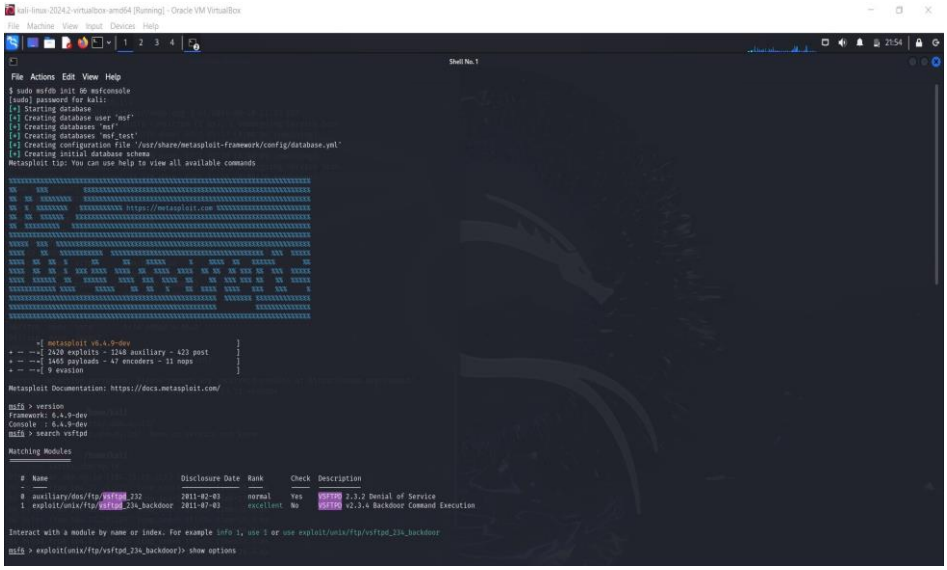
Analisis Hasil Scan

Setelah proses pemindaian jaringan dilakukan menggunakan Nmap, langkah selanjutnya adalah menganalisis hasil pemindaian tersebut untuk mengidentifikasi potensi kerentanan yang terdapat pada server hosting. Analisis hasil scan berfokus pada interpretasi data teknis yang diperoleh dari proses pemindaian, termasuk informasi mengenai port terbuka, layanan yang berjalan, versi aplikasi, serta sistem operasi yang terdeteksi.

Port yang terbuka menjadi indikator awal terhadap kemungkinan vektor serangan. Misalnya, port 21 (FTP), port 22 (SSH), port 80 (HTTP), atau port 3306 (MySQL) yang terbuka tanpa pengamanan dapat memberikan celah bagi penyerang untuk melakukan eksploitasi. Oleh karena itu, identifikasi terhadap layanan yang berjalan pada masing-masing port sangat penting untuk menentukan apakah layanan tersebut menggunakan versi yang rentan atau memiliki konfigurasi yang tidak aman.

Eksploitasi dengan Metasploit

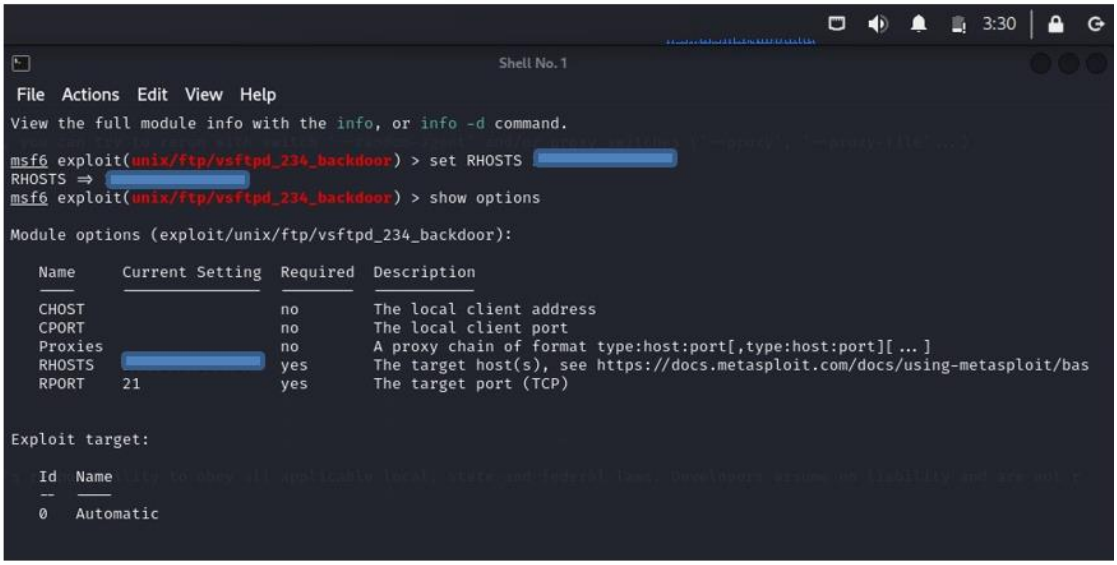
Perintah Version Digunakan Untuk Menampilkan Versi Dari Metasploit Framework Yang Sedang Gunakan.



Gambar 13. Perintah Version

Perintah search vsftpd akan mencari dan menampilkan semua modul dalam Metasploit yang terkait dengan vsftpd. Ini termasuk eksploitasi (exploits), payloads, dan modul lain yang berhubungan dengan vsftpd.

perintah set RHOSTS digunakan untuk mengatur alamat IP atau rentang alamat IP dari target yang akan dieksploitasi. RHOSTS (Remote Hosts) adalah parameter yang menentukan lokasi atau host target yang akan diserang atau diuji oleh modul eksploitasi.



Gambar 14. Perintah Set RHOSTS

Evaluasi Keberhasilan

Dalam penelitian ini, keberhasilan dievaluasi dengan menilai sejauh mana efektivitas penggunaan Nmap dan Metasploit dalam proses identifikasi dan eksploitasi celah keamanan pada server hosting. Penilaian dilakukan berdasarkan tiga indikator utama. Pertama, kemampuan deteksi kerentanan, yang menggambarkan tingkat akurasi dan kelengkapan dalam mengidentifikasi potensi celah keamanan. Kedua, relevansi eksploitasi, yaitu kesesuaian antara hasil pemindaian yang dilakukan menggunakan Nmap dan keberhasilan Metasploit dalam mengeksekusi eksploitasi terhadap celah yang ditemukan. Ketiga, dilakukan evaluasi risiko, yang berfokus pada tingkat keparahan dan dampak yang mungkin ditimbulkan apabila kerentanan tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab. Secara keseluruhan, ketiga indikator ini memberikan pemahaman menyeluruh mengenai efektivitas pendekatan metodologis yang diterapkan dalam mendeteksi dan menilai potensi ancaman siber pada sistem yang diuji.

KESIMPULAN DAN SARAN

Berdasarkan penelitian Pendekatan Metodologis dalam Deteksi Ancaman Siber pada Server Hosting Menggunakan NMAP dan Metasploit, maka dapat disimpulkan sebagai berikut: Pendekatan metodologis dalam deteksi ancaman siber melalui pemanfaatan Nmap dan Metasploit merupakan strategi yang bersifat sistematis dan terstruktur, yang dirancang untuk mendeteksi, menganalisis, serta menguji potensi kerentanan pada sistem keamanan server hosting. Penggunaan Nmap memungkinkan pelaku uji penetrasi untuk melakukan pemetaan jaringan secara komprehensif, termasuk dalam mengidentifikasi port-port yang terbuka, layanan yang aktif, serta sistem operasi yang digunakan oleh server target. Data tersebut berfungsi sebagai pijakan utama dalam menentukan arah pengujian keamanan lebih lanjut;

Selanjutnya, Metasploit berperan sebagai kerangka kerja eksploitasi yang digunakan untuk menguji secara aktif kerentanan yang telah diidentifikasi sebelumnya. Langkah ini bertujuan untuk menilai tingkat risiko serta potensi dampak yang dapat ditimbulkan jika kerentanan tersebut dimanfaatkan oleh pihak tidak berwenang. Dengan demikian, pendekatan ini tidak hanya bersifat responsif terhadap ancaman, tetapi juga proaktif dalam mendeteksi celah keamanan sebelum disalahgunakan;

Metodologi yang diterapkan, mencakup tahapan mulai dari perencanaan awal, pengumpulan informasi (reconnaissance), pemindaian dan enumerasi, analisis kerentanan, eksploitasi, hingga penyusunan laporan teknis. Proses ini sejalan dengan prinsip ethical hacking dan praktik penetration testing yang sah dan terstandar, serta mendukung penerapan keamanan informasi yang berkelanjutan; Dengan mengintegrasikan kedua alat tersebut, pendekatan ini memberikan kontribusi signifikan terhadap penguatan sistem pertahanan siber, khususnya dalam konteks pengelolaan infrastruktur server hosting yang andal dan resilien terhadap ancaman siber.

Pendekatan metodologis menggunakan Nmap dan Metasploit bukan hanya mendeteksi kerentanan, tetapi juga membuktikan eksploitabilitasnya secara langsung. Ini menjadikannya strategi penting dalam manajemen risiko siber yang praktis dan efisien, serta mendukung praktik keamanan informasi modern dalam pengelolaan server hosting.

DAFTAR PUSTAKA

[1] 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.

[2] D. Sudirman and Akma Nurul Yaqin, "Network Penetration dan Security Audit Menggunakan Nmap," *SATIN - Sains dan Teknol. Inf.*, vol. 7, no. 1, pp. 32–44, 2021, doi: 10.33372/stn.v7i1.702.

[3] O. Valea and C. Oprisa, "Towards Pentesting Automation Using the Metasploit Framework," *Proc. - 2020 IEEE 16th Int. Conf. Intell. Comput. Commun. Process. ICCP 2020*, no. September 2020, pp. 171–178, 2020, doi: 10.1109/ICCP51029.2020.9266234.

[4] J. L. J. Pandari and W. Sulistyo, "Implementasi Intrusion Detection System (IDS) untuk Mendeteksi serangan Metasploit Exploit Menggunakan Snort dan Wireshark," *J. Pendidik. Teknol. Inf.*, vol. 6, no. 1 SE-Artikel, pp. 41–50, 2023, [Online]. Available: https://ojs.cbn.ac.id/index.php/jukanti/article/view/861

[5] 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.

[6] M. O. Kadang, J. Perintis, and K. Km, "Pengujian Kelemahan Keamanan Aplikasi Web Menggunakan Peretasan Etis," vol. XIII, no. 2, pp. 234–243, 2019.

[7] F. Mahardika and R. B. B. Sumantri, "Implementation of Payment Gateway in the Mobile-Based Pawon Mbok ` E Eating House Ordering System," *J. Innov. Inf. Technol. Appl.*, pp. 60–70, 2024.

[8] M. Fadhli, "Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities," vol. 4, no. June, pp. 15–22, 2024.

[9] 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.

[10] A. P. Walidin, F. P. Putri, and D. Kiswanto, "KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK, DAN METASPLOIT," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1188–1196, 2025.

[11] M. Rizki *et al.*, "UJI PENETRASI MENGGUNAKAN HYDRA DAN METASPLOIT PADA PROTOKOL SECURE SHELL," vol. 9, no. 1, pp. 1017–1024, 2025.

[12] I. Tyshyk and H. Hulak, "Testing an organization's information system for unauthorized access," *CEUR Workshop Proc.*, vol. 3826, pp. 17–29, 2024.

[13] M. Anis, A. Hilmi, and F. Herdiyanti, "Linux Operating System Security Testing Case Study : FTP Security in Metasploitable 2," vol. 14, no. August 2022, pp. 62–67, 2023.

[14] 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

[15] H. Sharma, D. Lindskog, and E. Schmidt, "Exploting Vulnerabilities of Metasploitable 3 (Windows) Using Metasploit Framework," vol. 3, pp. 1–22, 2020.

[16] D. A. Andhika, Slamet, and N. Ningsih, "Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES)," *J. Technol. Informatics*, vol. 3, no. 2, pp. 55–61, 2022, doi: 10.37802/joti.v3i2.222.