Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 1, No. 4b, Tahun 2025
doi.org/10.63822/2q8zwz85
Hal. 2138-2144

Serangan dan Deteksi Port Scanning Menggunakan Wireshark dan Snort

Rakhmadi Rahman[1], Abdul Khalik Hartono[2], Eka Tanduklangi[3]
[1,2,3] Program Studi Sistem Informasi Institut Teknologi Bacharuddin Jusuf Habibie Parepare, Indonesia

*Email Korespodensi: rakhmadi.rahman@ith.ac.id

Sejarah Artikel:

Diterima 01-07-2025
Disetujui 07-07-2025
Diterbitkan 09-07-2025

ABSTRACT

In the digital era, network security threats such as port scanning pose significant risks as they serve as reconnaissance for potential cyber attacks. This study evaluates the effectiveness of Wireshark (paket analysis tool) and Snort (Intrusion Detection System) in detecting and analyzing port scanning activities. Using Nmap (Zenmap) as an attack simulator, experiment were conducted on a local Wi-Fi network to capture TCP SYN scans and HTTP sniffing attemps. Wireshark successfully identified suspicious traffic patterns, icluding unacknowledged SYN packets and exposed HTTP login credentials, while Snort, configured with custom rules, generated real-time alert for scanning activities. The findings confirm the complementary roles validation. This study recommends regular Snort rule update, enabling promiscuous mode, and implementing HTTPS/VPN to mitigate sniffing risks. This integrates approach enhances early threat detection and strengthens network protection mechanisms.

Keywords: *Port Scanning, Nmap, Wireshark, Snort, Instrusion Detection System, Network Security*

Bagaimana Cara Sitasi Artikel ini:

Rakhmadi Rahman, Abdul Khalik Hartono, & Eka Tanduklangi. (2025). Serangan dan Deteksi Port Scanning Menggunakan Wireshark dan Snort. Jejak Digital: Jurnal Ilmiah Multidisiplin, 1(4b), 2138-2144. https://doi.org/10.63822/2q8zwz85

PENDAHULUAN

Di tengah pesatnya perkembangan era digital, ketergantungan terhadap jaringan komputer semakin tinggi, baik instansi pemerintah, sektor pendidikan, maupun dunia bisnis. Namun, hal ini juga dapat meningkatkan risiko ancaman terhadap keamanan, salah satunya melalui teknik *Port Scanning*, metode yang digunakan peretas untuk mengidentifikasi *port* yang terbuka sebagai langkah awal untuk mengeksploitasi celah keamanan. Meskipun tidak secara langsung merusak sistem, *Port Scanning* juga dapat menjadi pemicu serangan lebih lanjut, sehingga deteksi dini menjadi semakin krusial. Untuk itu, penelitian ini memanfaatkan dua alat *open source*, yaitu Wireshark (analisis protokol jaringan) dan Snort (sistem deteksi intrusi), guna mengidentifikasi dan menganalisis aktivitas *Port Scanning* secara efektif. Kombinasi kedua alat ini diharapkan mampu memberikan pemantauan yang komprehensif, dengan Wireshark sebagai *tools* analisis forensik dan Snort sebagai pendeteksi otomatis berbasis aturan.

Tujuan penelitian ini adalah (1) memahami karakteristik *Port Scanning* sebagai ancaman awal keamanan jaringan, (2) menganalisis lalu lintas jaringan secara manual menggunakan Wireshark, (3) mendeteksi serangan otomatis dengan Snort, serta (4) mengevaluasi efektivitas integrasi kedua alat tersebut. Simulasi dilakukan dengan Nmap sebagai simulator serangan. Hasil yang diharapkan mencakup dokumentasi aktivitas *Port Scanning*, identifikasi melalui log Snort, dan rekomendasi penguatan sistem deteksi dini. Dengan demikian, penelitian ini diharapkan berkontribusi dalam mitigasi ancaman siber berbasis reconnaissance.

METODE PENELITIAN

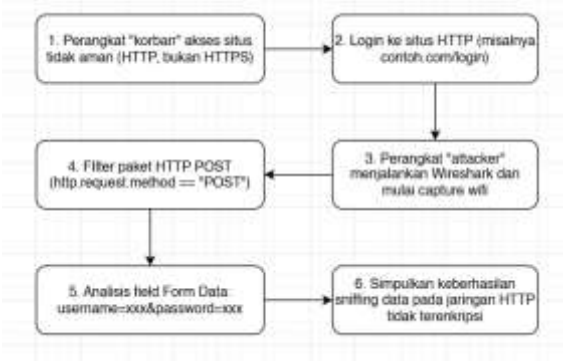
Penelitian ini menggunakan metode eksperimen dengan melakukan simulasi serangan jaringan berupa *Port Scanning* dan *Sniffing* untuk menganalisis bagaimana kemampuan Wireshark dan Snort dalam mendeteksi suatu aktivitas yang mencurigakan. Fokus pengamatan meliputi seberapa efektif kedua alat tersebut dalam mengidentifikasi pola serangan, khususnya pada jaringan *Wi-Fi* lokal.

Tujuan eksperimen meliputi: (1) melakukan simulasi serangan *Port Scanning* menggunakan Zenmap (Nmap GUI); (2) menguji deteksi aktivitas *Port Scanning* dan *Sniffing* oleh Wireshark dan Snort; serta (3) mengevaluasi tingkat akurasi dan respons kedua alat terhadap serangan. Simulasi dilakukan dengan perangkat keras berupa laptop dengan OS Windows dan *Virtual Machine* Kali Linux, serta perangkat lunak pendukung penelitian seperti Wireshark (analisis paket), Snort (IDS), dan Nmap (simulasi serangan).

Adapun prototipe simulasi digambarkan dalam tiga tahap utama. Pertama, Wireshark untuk menganalisis paket TCP SYN dari hasil pemindaian oleh Nmap terhadap IP lokal untuk mengidentifikasi pola *Port Scanning*. Dibawah ini adalah gambar alur simulasi untuk melakukan *Port Scanning* dan mendeteksinya menggunakan Wireshark.

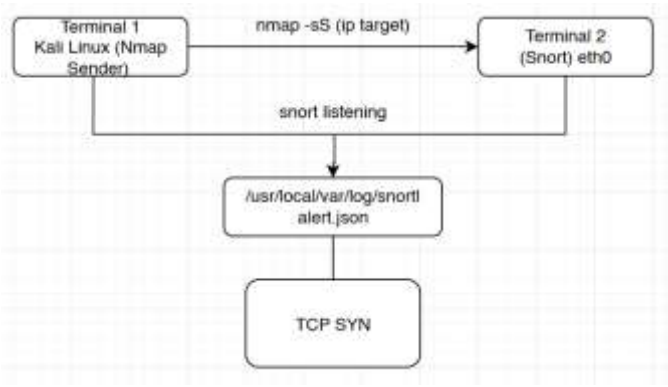
Gambar 1 Prototipe Simulasi Deteksi *Port Scanning* Wireshark

Kedua, Wireshark mendeteksi aktivitas *Sniffing* dengan menangkap data HTTP yang tidak terenkripsi, termasuk informasi login yang dikirim via form POST. Dibawah ini adalah alur dari serangan *Sniffing* informasi login menggunakan menggunakan Wireshark.



Gambar 2 Prototipe Simulasi Srangan *Sniffing* Wireshark

Ketiga, Snort memantau lalu lintas jaringan pada *interface eth0* dan mencatat *alert* berupa paket mencurigakan ke dalam *log alert.json* sebagai bukti *Port Scanning.* Dapat dilihat dibawah ini simulasi dilakukan di terminal Kali Linux yang dimana terminal 1 melakukan *Port Scanning*, dan terminal 2 menjalankan Snort untuk mendeteksi *Port Scanning*



Gambar 3 Prototipe Simulasi Deteksi *Port Scanning* Snort

HASIL DAN PEMBAHASAN

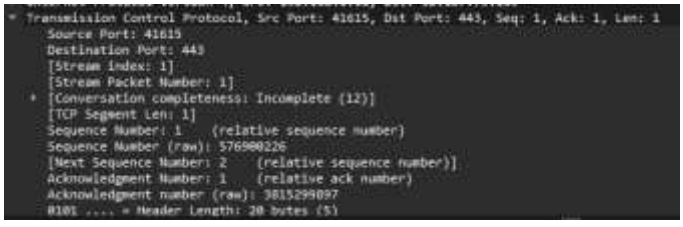
1. Deteksi *Port Scanning* dan *Sniffing* Menggunakan Wireshark

a. *Port Scanning*

Simulasi *Port Scanning* dilakukan dengan Zenmap (Nmap GUI) terhadap target IP lokal (misal: 192.168.1.100) menggunakan menggunakan metode *Intense Scan* (TCP SYN). Wireshark berhasil menangkap aktivitas yang mencurigakan dengan *filter* berupa "tcp.flags.syn", yang mengidetifikasi paket SYN yang dikirimkan oleh sender tanpa respons ACK indikator khas *Port Scanning*. Analisis lebih lanjut yang menunjukkan pola pengiriman paket SYN ke port acak dan berturut-turut.

Gambar 4 TCP dengan Flags SYN

Gambar diatas menunjukkan bahwa terdapat 6 paket TCP dengan volume tinggi (5+ paket/detik) yang mengkonfirmasi aktivitas *Scanning*. Berdasarkan hasil analisis menggunakan Wireshark, teridentifikasi paket TCP yang berasal dari mesin penyerang dengan *source port* acak menuju *destination port* tertentu pada sistem target. Paket tersebut memiliki flags SYN, mengindikasi permintaan inisiasi koneksi TCP. Informasi tambahan berupa *Sequence Number*, TCP *Lenght*, dan *checksum* juga terekam secara lengkap.

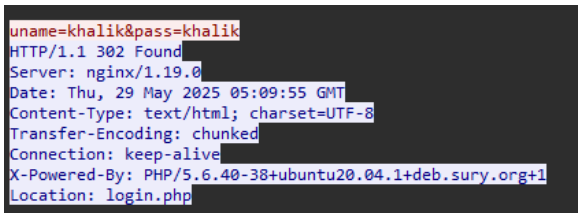


Gambar 5 Informasi Lengkap Paker TCP

Memvalidasi bahwa proses pemindaian berjalan sesuai ekspektasi. Analisis ini membantu administrator jaringan menedeksi aktivitas mencurigakan.

b. *Sniffing* Password HTTP

Pada simulasi *Sniffing*, Wireshark berhasil mengekstrak kredensial *login* (username dan password) dari lalu lintas HTTP yang tidak terenkripsi. *Filter* "http.request.method == "POST"" mengisolasi payload *form login*, dimana data sensitif bisa nampak jelas dalam teks biasa



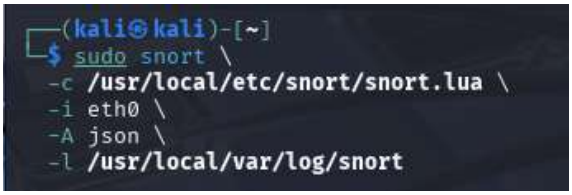
Gambar 6 Payload HTTP Berisi Kredensial Login

Hasil ini membuktikan kerentanan jaringan *Wi-Fi* lokal terhadap serangan *passive Sniffing*, apalagi jika menggunakan protokol HTTP. Oleh karena itu, enkripsi wajib digunakan (HTTPS, VPN) dan menerapkan *network segmentation* untuk membatasi akses.

2. Deteksi *Port Scanning* Menggunakan Snort

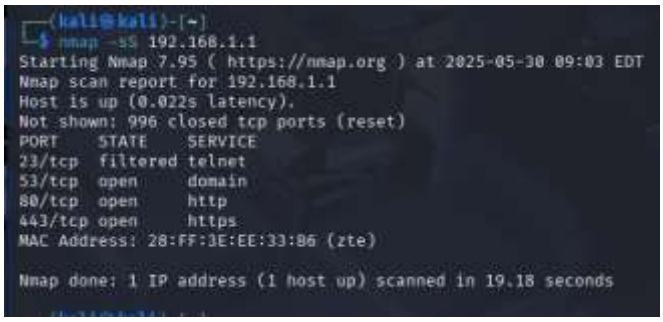
a. Konfigurasi dan Simulasi

Snort versi 3 di Kali Linux dikonfigurasi dengan *custom rule* untuk mendeteksi TCP SYN *scan* (sid: 1000001). Saat Nmap dijalankan dengan perintah "nmap -sS 192.168.1.1" , Snort memantau antarmuka *eth0* dan mencatat aktivitas *scanning* dalam *log* JSON yang akan ditampilkan jika snort dijalankan. Gambar dibawah adalah perintah untuk mengaktifkan Snort:



Gambar 7 Menjalankan Snort Sebagai IDS

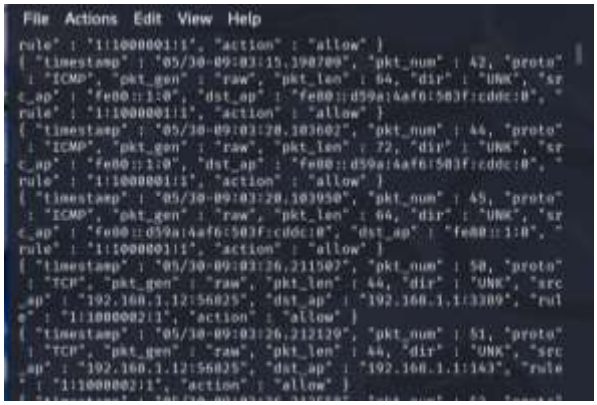
Setelah mengaktifkan Snort, lakukan perintah nmap untuk mengetahui port apa saja yang terbukan dan bisa dijadikan target:



Gambar 8 Hasil *Port Scanning* Menggunakan Nmap

Log yang ada pada terminal yang menjalankan Snort:

a) Flag TCP: SYN tanpa kelanjutan handshake & ICMP



Gambar 9 Paket TCP dan ICMP

b. Analisis Log

Log Snort (/usr/local/var/log/snort/alert.json) menunjukkan efektivitas *rule* dalam melakukan identifikasi *scanning*:

a) TCP SYN Scan: Terdeteksi sebagai *alert* dengan pesan “SCAN SYN DETECTED”.

Gambar 10 Log Snort untuk Paket TCP

b) ICMP *Ping Sweep*: Tercatat tetapi tidak dianggap ancaman

Gambar 11 Log Snort untuk Paket ICMP

KESIMPULAN

Wireshark (Windows) dan Snort (Kali Linux) merupakan dua alat krusial dalam keamanan jaringan yang saling melengkapi: Wireshark menyediakan analisis paket mendalam dengan antarmuka visual, ideal untuk *troubleshooting* dan investigasi manual, sementara Snort berfungsi sebagai sistem deteksi intrusi berbasis aturan yang berjalan otomatis, mampu memantau ancaman seperti *Port Scanning* atau serangan eksploitasi secara *real-time*. Namun, implementasi Snort memerlukan pemahaman teknis yang lebih tinggi, termasuk konfigurasi terminal, manajemen *rule*, dan pengaturan *interface* jaringan, sehingga disarankan bagi administrator untuk rutin memperbarui *rule* Snort, memastikan mode *promiscuous* aktif, serta memadukan kedua alat ini guna mencapai deteksi ancaman yang komprehensif Snort sebagai peringatan dini dan Wireshark sebagai alat verifikasi lanjutan.

REFERENSI

[1] Alsharabi, N., Alqunun, M., & Murshed, BAH (2023). Mendeteksi aktivitas yang tidak biasa di jaringan lokal menggunakan alat snort dan wireshark. Jurnal Kemajuan Teknologi Informasi , 14 (4), 616-624.
[2] Fauzi, A. R., & Suartana, I. M. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. J. Manaj. Inform, 8(2), 7.
[3] Jain, G. (2021, Maret). Aplikasi snort dan wireshark dalam analisis lalu lintas jaringan. Dalam IOP Conference Series: Materials Science and Engineering (Vol. 1119, No. 1, p. 012007). IOP Publishing.
[4] Mabsali, NA, Jassim, H., & Mani, J. (Januari 2023). Efektivitas Alat Wireshark untuk Mendeteksi Serangan dan Kerentanan dalam Lalu Lintas Jaringan. Dalam Konferensi Internasional ke-1 tentang Inovasi dalam Teknologi Informasi dan Bisnis (ICIITB 2022) (hlm. 114-135). Atlantis Press.
[5] Nugroho, B. A. (2012). Analisis Keamanan Jaringan Pada Fasilitas Internet (WiFi) Terhadap Serangan Packet Sniffing (Doctoral dissertation, Universitas Muhammadiyah Surakarta).
[6] https://www.wireshark.org/download.html
[7] https://www.kali.org/get-kali/#kali-virtual-machines