# IMPLEMENTASI SNORT SEBAGAI IDS DALAM MENDETEKSI SERANGAN PORT SCANNING NMAP PADA SIMULASI JARINGAN VIRTUAL

**Meilia Intan Sabila, Muhlis Tahir, Saskia Dwi Mardania, Rizky Ilham Arifin**
Pendidikan Informatika, Universitas Trunojoyo Madura
Jalan Raya Telang, PO.Box. 2 Kamal,Bangkalan - Madura
*220631100064@student.trunojoyo.ac.id*

**ABSTRAK**

Keamanan jaringan komputer menjadi semakin krusial seiring meningkatnya frekuensi serangan siber. Port scanning merupakan langkah awal yang sering digunakan penyerang untuk memetakan layanan dan kerentanan pada sistem target. Permasalahan yang dihadapi adalah kurangnya sistem yang mendeteksi secara awal sehingga mampu mengenali aktivitas secara real time terutama yang berbasis open-source. Penelitian ini bertujuan untuk mengimplementasikan Snort sebagai Intrusion Detection System (IDS) dalam mendeteksi berbagai teknik port scanning menggunakan Nmap pada simulasi jaringan virtual berbasis VirtualBox. Metode yang digunakan meliputi simulasi jaringan dengan dua mesin virtual—Debian 12 sebagai penyerang dan Ubuntu 20.04 sebagai target dengan Snort terkonfigurasi pada host target. Konfigurasi meliputi instalasi Snort, penyesuaian file snort.conf, dan pembuatan aturan (local.rules) untuk mendeteksi Syn Scan, Ping Scan, UDP Scan, dan Aggressive Scan. Hasil dari pengujian menunjukkan bahwa Snort secara real time mampu mengenali dan memunculkan peringatan (alert) untuk setiap jenis port scanning. Implementasi ini dapat menjadi acuan bagi pengembangan sistem keamanan berbasis open source di lingkungan akademik dan industri.

***Kata kunci :*** *Snort, Intrusion Detection System, Port Scanning, Nmap, VirtualBox.*

## 1. PENDAHULUAN

Dalam era digital yang semakin berkembang, keamanan jaringan menjadi salah satu aspek krusial dalam menjaga integritas dan ketersediaan sistem informasi. Seiring dengan meningkatnya ketergantungan terhadap sistem digital, berbagai ancaman seperti peretasan, pencurian data, dan serangan siber semakin sering terjadi [1]. Dengan demikian, administrator jaringan harus memastikan bahwa sistem jaringan komputer selalu dalam kondisi aman dan terlindungi dari potensi serangan siber [2]. Menjaga keamanan jaringan komputer dengan baik merupakan aspek yang sangat krusial. Tanpa perlindungan yang memadai, celah keamanan dalam jaringan dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mendapatkan akses ilegal. Hal ini berpotensi menimbulkan berbagai dampak negatif, seperti kehilangan data, gangguan pada sistem server, penurunan kualitas layanan bagi pengguna, hingga kerugian aset berharga bagi suatu institusi.

Untuk menghadapi berbagai ancaman keamanan jaringan, diperlukan sistem yang mampu mendeteksi aktivitas mencurigakan secara real-time. Salah satu solusi yang umum digunakan adalah *Intrusion Detection System* (IDS) [3][4][5]. *Intrusion Detection System* (IDS) merupakan sistem perangkat lunak yang bertugas mendeteksi aktivitas mencurigakan atau lalu lintas yang tidak wajar dalam suatu jaringan. Dengan adanya IDS, potensi serangan seperti port scanning, brute force attack, dan eksploitasi kerentanan sistem dapat dideteksi lebih awal. Hal ini memungkinkan administrator jaringan untuk mengambil langkah mitigasi sebelum serangan berkembang menjadi ancaman yang lebih besar.

Di antara berbagai metode yang digunakan oleh penyerang, adalah metode *port scanning* yang merupakan langkah awal yang digunakan penyerang dalam meretas sistem sehingga dapat diketahui post mana yang lemah dan mudah diserang [6]. Port scanning kerap dimanfaatkan oleh penyerang sebagai langkah awal untuk mengeksplorasi permukaan serangan dengan mengirim paket ke berbagai port pada sistem atau jaringan. Salah satu alat yang umum digunakan untuk melakukan port scanning adalah Nmap. Nmap adalah perangkat open-source terkemuka untuk pemetaan jaringan yang mengirimkan probe TC/IP ke berbagai port pada sistem target untuk memetakan port yang dapat diakses dan mengenali layanan yang berjalan, sehingga memudahkan penyerang dalam menentukan celah eksploitasi [7]. Alat ini memungkinkan pemetaan jaringan dengan cara mengidentifikasi port yang terbuka serta layanan yang berjalan di dalamnya. Dengan informasi tersebut, penyerang dapat menentukan potensi eksploitasi terhadap sistem target [8].

Salah satu sistem yang banyak digunakan untuk mendeteksi aktivitas port scanning adalah Snort IDS [9].Snort merupakan sistem deteksi intrusi berbasis open-source yang diterima luas dalam industri untuk memantau lalu lintas jaringan secara real-time. Sistem ini tidak hanya mendeteksi ancaman tetapi juga memberikan peringatan kepada administrator jaringan tentang potensi serangan. Dengan kemampuannya dalam mengenali berbagai jenis serangan, seperti port scanning, Snort menjadi pilihan efektif dalam meningkatkan keamanan jaringan. Dengan kemampuannya dalam mengenali berbagai jenis serangan, seperti port scanning, Snort menjadi pilihan

efektif dalam meningkatkan keamanan jaringan. Alat tersebut membantu dalam menentukan paket yang berbahaya dan membuat peringatan ke pengguna. Hal tersebut dapat dikonfigurasikan pada file snort.conf [10].

## 2. TINJAUAN PUSTAKA

Intrusion Detection System (IDS) adalah aplikasi perangkat lunak yang digunakan untuk mendeteksi aktivitas atau lalu lintas yang tidak wajar dalam sebuah sistem atau jaringan. Intrusion Detection System (IDS) menjadi solusi yang banyak digunakan dalam pengamanan jaringan. IDS dapat mencegah masalah jaringan, mendeteksi serangan dan memberikan informasi mengenai penyerangan yang terjadi [11].

Salah satu implementasi IDS yang paling banyak digunakan adalah Snort, sebuah perangkat lunak open-source yang dapat berfungsi sebagai *packet sniffer*, *packet logger*, dan *network intrusion detection system*. Snort mampu mendeteksi berbagai jenis serangan seperti syn-flooding, TCP/UDP/ICMP flooding, port scanning, *SQL injection*, hingga *ping of death*, dengan menggunakan rule atau signature yang didefinisikan sebelumnya. Snort IDS adalah salah satu jenis IDS yang bersifat open source dan telah menjadi standar IDS di industri. Dengan demikian, Snort menjadi sistem yang dapat mengirimkan *message* atau notifikasi dalam mencegah serangan [12].

Port scanning adalah langkah awal dalam mendeteksi port-port yang terbuka sehingga mendapatkan informasi dari port yang terbuka [13]. Hal ini digunakan oleh administrator maupun oleh penyerang. Nmap merupakan tool untuk mendeteksi jaringan dan melakukan pemindaian keamanan dalam menentukan port yang terbuka dan berjalan pada sistem [14]. Fitur-fitur nmap dapat melakukan pemindaian pada berbagai jenis port secara real-time, selain melakukan pemindaian dapat juga mendeteksi layanan yang berjalan pada sistem [15].

*Virtualbox* merupakan mesin virtual yang menyediakn lingkungan pengujian yang fleksibel, selain itu menjadi *hosted hypervisor hosted hypervisor* yang versi gratis [16]. Selain itu, *virtualbox* menjadi alat implementasi yang mudah diakses tanpa memerlukan jaringan internet.

Penelitian sebelumnya menunjukkan bahwa penerapan sistem deteksi dan keamanan jaringan menggunakan snort dapat memantau lalu lintas *packet* dan mampu mendeteksi serangan sesuai rules yang sudah diatur, selain itu akan muncul alert pada snort berdasarkan hasil deteksi yang dilakukan snort sehingga admin dapat melakukan pencegahan terhadap aktivitas yang menganggu [17].

Penelitian sebelumnya menunjukkan bahwa Snort mampu mendeteksi serangan *syn-flooding* terhadap server Samsat, dan diimplementasikan sebagai bentuk proteksi awal terhadap serangan tersebut [5]. Untuk meningkatkan respons terhadap serangan secara real-time, beberapa penelitian sebelumnya mengintegrasikan IDS dengan aplikasi pesan instan seperti WhatsApp dan Telegram. Melalui penggunaan API seperti Twilio untuk WhatsApp dan Bot API untuk Telegram, sistem dapat mengirimkan notifikasi otomatis dan cepat kepada administrator saat terjadi serangan. Snort juga terbukti efektif dalam lingkungan akademik dan organisasi lainnya [18].

Dengan mengintegrasikan IDS seperti Snort dan sistem notifikasi real-time berbasis aplikasi pesan instan, serta memanfaatkan teknik analisis kerentanan dan forensik digital, pengamanan jaringan dapat ditingkatkan secara signifikan. Kajian pustaka ini menunjukkan bahwa pendekatan multidimensi yang mencakup deteksi, respons, dan analisis menjadi strategi yang komprehensif dalam menghadapi ancaman keamanan jaringan modern [19][20].

## 3. METODE PENELITIAN

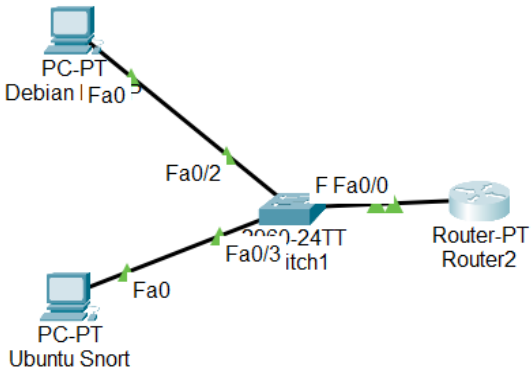
### 3.1. Simulasi Jaringan

Pada implementasi snort sebagai IDS dalam mendeteksi serangan Port Scanning NMAP menggunakan simulasi jaringan virtual yang dibangun dengan alat simulasi virtualbox. Pada simulasi yang dilakukan terdapat dua mesin virtual sebagai berikut :

a. Penyerang (Attacker)
   Mesin virtual yang digunakan sebagai penyerang yaitu Debian 12. Debian 12 digunakan untuk melakukan serangan port scanning menggunakan Nmap. Selain itu debian 12 digunakan untuk mengakses target.
b. Target
   Mesin virtual yang digunakan sebagai target yaitu Ubuntu 20.04. Ubuntu 20.04 digunakan sebagai sistem deteksi intrusi menggunakan snort. Selain itu digunakan untuk menangkap dan mencatat aktivitas scanning dari penyerang.

Konfigurasi jaringan menggunakan Host only adapter sebagai jaringan virtual. Hal ini mempermudah jaringan untuk melakukan komunikasi karena berada pada jaringan yang lokal.

Berikut gambar simulasi jaringan.

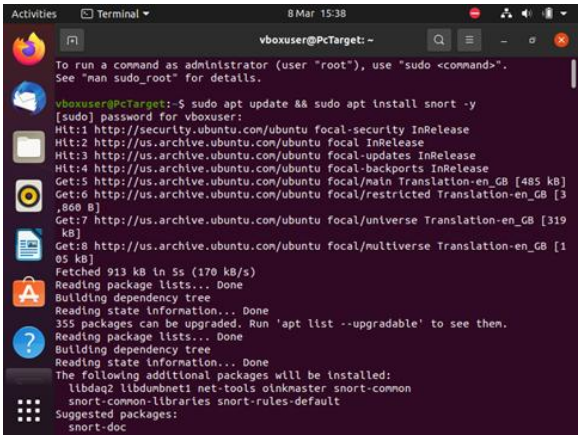



Gambar 1. Simulasi Jaringan

### 3.2. Instalasi dan konfigurasi snort

Snort adalah perangkat lunak untuk mendeteksi intrusi-intrusi jaringan dan dapat mencegah masalah jaringan [21]. IDS berbasis snort dapat menghemat

biaya dalam pengadaan software karena bersifat gratis dan dapat mendeteksi serangan keamanan [22]. Proses instalasi snort dengan menjalankan **sudo apt update && sudo apt install snort** –y. Instalasi snort dapat dilihat pada gambar 2.

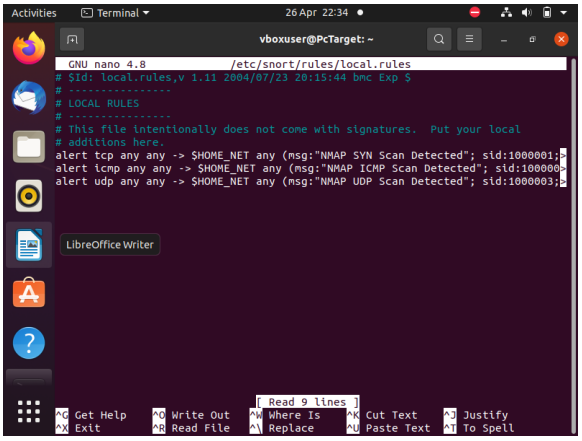



Gambar 2. Instalasi snort

Kemudian untuk mengkonfigurasikan snort yaitu dengan membuka file snort.conf dengan **sudo nano /etc/snort/snort.conf**.

### 3.3. Konfigurasi rules

Selanjutnya sebelum menjalankan snort maka dibutuhkan mengkonfigurasikan rules agar snort bekerja dengan baik dengan perintah yaitu **sudo nano /etc/snort/rules/local.rules**. Rules yang ditambahkan pada snort dapat dilihat pada gambar 3.




Gambar 3. Konfigurasi Rules

### 3.4. Simulasi serangan NMAP

Simulasi serangan dilakukan untuk menguji snort dalam mendeteksi aktivitas serangan port scanning. Dalam simulasi yang dilakukan, nmap digunakan sebagai tools penyerang yang dilakukan pada debian 12. Beberapa teknik serangan yang disimulasikan menggunakan nmap adalah :

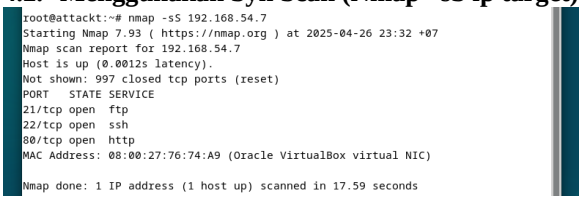
a. Syn Scan (Nmap –sS)
   Nmap yang hanya mengirimkan paket syn atau permintaan awal koneksi TCP.
b. Ping Scan (Nmap –sP)
   Nmap yang hanya mengirimkan paket ping guna mengetahui host aktif atau tidak sehingga hanya untuk mendeteksi host.
c. UDP Scan (Nmap –sU)
   Mendeteksi port yang terbuka menggunakan protokol UDP. Pada UDP Scan sedikit lambat dalam menjalankannya.
d. Aggressive Scan (Nmap –A)
   Untuk mengumpulkan informasi menyeluruh mengenai sistem target.

## 4. HASIL DAN PEMBAHASAN

### 4.1. Teknik Serangan Port Scanning NMAP

Teknik serangan port scanning bertujuan untuk mengetahui port mana yang telah terbuka pada pc target dan untuk mendapatkan informasi penting yang terdapat pada jaringan. Teknik serangan port scanning menggunakan nmap ada beberapa cara yaitu

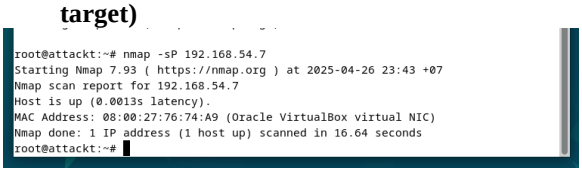
### 4.2. Menggunakan Syn Scan (Nmap –sS ip target)




Gambar 4. Syn Scan

Gambar 4 merupakan hasil serangan dengan teknik port scanning SYN Scan menggunakan Nmap -sS**.** Berdasarkan Gambar 4, serangan ini berhasil mendeteksi bahwa perangkat dengan IP address 192.168.54.7 aktif dalam jaringan. Layanan yang terbuka yaitu terdapat port 21 yang digunakan untuk layanan ftp, port 22 yang digunakan oleh ssh dan port 80 yang digunakan oleh http. Sehingga hal ini dimanfaatkan oleh peretas (attacker) untuk mengidentifikasi port yang terbuka dalam perangkat target.

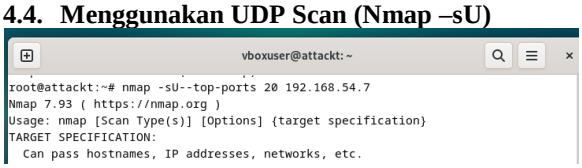
### 4.3. Menggunakan Ping Scan (Nmap –sP Ip target)




Gambar 5. Ping Scan

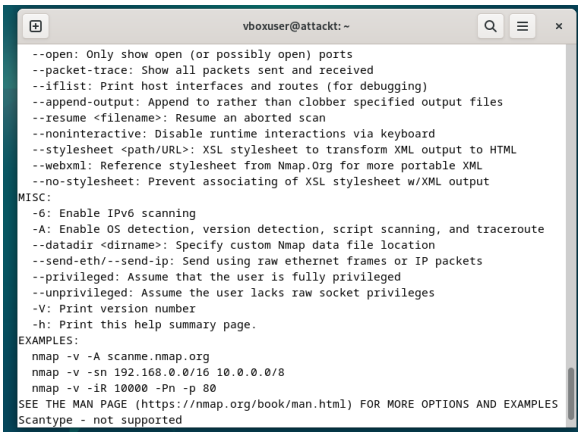
Gambar 5 merupakan hasil serangan dengan port scanning Ping Scan menggunakan Nmap -sP. Berdasarkan gambar 5, serangan ini berhasil mendeteksi bahwa perangkat dengan IP address 192.168.54.7 aktif dalam jaringan dan dapat merespon permintaan dari ICMP selain itu juga terdeteksi bahwa perangkat dijalankan pada oracle virtualbox. Disini teknik ini hanya mengkonfirmasi satu perangkat yang aktif sehingga ini langkah sebelum mendeteksi layanan.

### 4.4. Menggunakan UDP Scan (Nmap –sU)




Gambar 6. UDP Scan

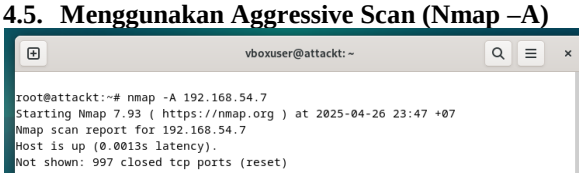
Gambar 6 merupakan serangan port scanning menggunakan UDP Scan.




Gambar 7. Pengujian UDP Scan

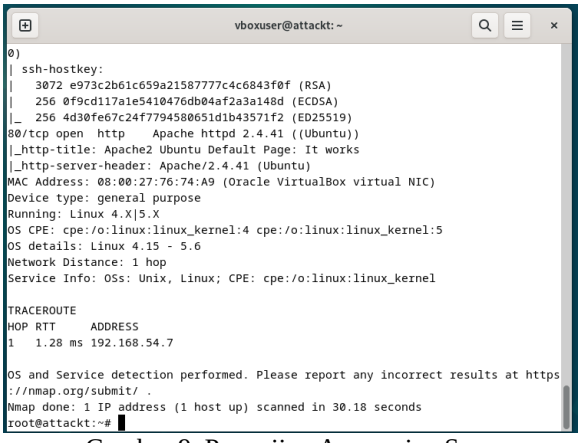
Gambar 7 Pengujian dilakukan untuk mendeteksi kemungkinan adanya port UDP terbuka pada mesin target dengan alamat IP 192.168.54.7 menggunakan tool *Nmap*. Perintah yang digunakan adalah nmap -sU --top-ports 20 192.168.54.7, yang bertujuan untuk melakukan pemindaian terhadap 20 port UDP teratas berdasarkan frekuensi penggunaannya.

### 4.5. Menggunakan Aggressive Scan (Nmap –A)




Gambar 8. Aggressive Scan

Gambar 8 merupakan serangan port scanning Aggressive Scan.

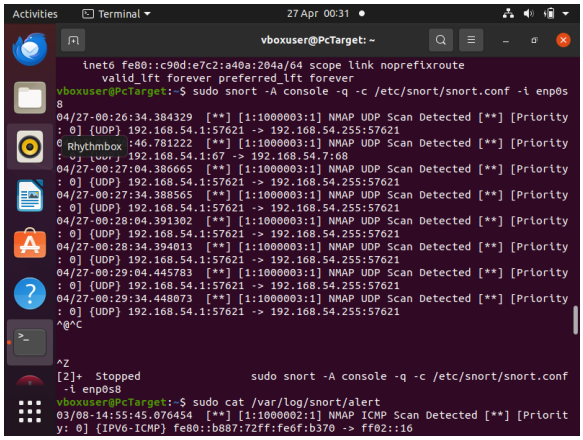



Gambar 9. Pengujian Aggressive Scan

Gambar 9 merupakan hasil serangan dengan port scanning Aggressive Scan menggunakan Nmap -A. Berdasarkan gambar 9, pada hasil serangan nmap Aggressive Scan jaringan target berada sama dengan jaringan penyerang. Pemindaian berhasil mendeteksi bahwa port 80 (HTTP) dalam keadaan terbuka dan menjalankan layanan web Apache2 versi 2.4.41 yang berasal dari distribusi Ubuntu. Selain itu, deteksi sistem operasi menunjukkan bahwa target menggunakan kernel Linux versi 4.x hingga 5.x dan tampaknya dijalankan di lingkungan virtualisasi VirtualBox (ditunjukkan oleh alamat MAC VirtualBox). Hasil ini menunjukkan bahwa target menjalankan layanan web yang dapat diakses dari jaringan lokal. Aktivitas pemindaian seperti ini termasuk dalam kategori pengintaian (reconnaissance), yang umumnya menjadi salah satu indikasi awal dari potensi serangan.

### 4.6. Hasil Deteksi Snort

Setelah melakukan serangan maka snort akan mengirim semua serangan yang dilakukan berupa alert. Sehingga alert dapat dilihat pada gambar 10.




Gambar 10. Hasil pemberitahuan snort

Gambar 10 merupakan pemberitahuan jika ada percobaan penyerangan sehingga akan muncul alert seperti “UDP Scan Detected” atau “ICMP Scan Detected”.

## 5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pengujian pada simulasi virtual, dapat disimpulkan bahwa Snort sebagai Intrusion Detection System (IDS) mampu mendeteksi serangan port scanning yang dilakukan menggunakan berbagai metode Nmap seperti TCP Syn Scan, ICMP Ping Scan, UDP Scan, dan Aggressive Scan. Snort berhasil mengidentifikasi pola lalu lintas mencurigakan dan memberikan notifikasi peringatan secara real-time melalui file alert. Penggunaan Snort dengan konfigurasi rule yang tepat terbukti dapat meningkatkan keamanan jaringan, khususnya dalam mendeteksi upaya reconnaissance sebelum serangan yang lebih serius terjadi. Dengan demikian, Snort

dapat dijadikan sebagai salah satu solusi proteksi awal terhadap ancaman siber berbasis jaringan.

## DAFTAR PUSTAKA


[1] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[2] R. W. Ismail and R. Pramudita, "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT," vol. 5, no. 1, pp. 53–62, 2020.

[3] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.

[4] S. Suhartono and A. R. Patta, "Sistem Pengamanan Jaringan Admin Server Dengan Metode Intrusion Detection System (Ids) Snort Menggunakan Sistem Operasi Clearos," *J. Teknol. Elekterika*, vol. 1, no. 2, p. 145, 2022, doi: 10.31963/elekterika.v1i2.1220.

[5] M. Pitriyanti, N. Khairani Daulay, and M. Agus Syamsul Arifin, "KLIK: Kajian Ilmiah Informatika dan Komputer Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort," *Media Online*, vol. 3, no. 4, pp. 323–329, 2023, [Online]. Available: https://djournals.com/klik

[6] M. Arhami, A. Arianda, A. Fata, Yassir, A. Desiani, and M. Arifai, "Detection using Intrusion Detection System (IDS) and SMS Gateway Controller," *Int. J. Electron. Telecommun.*, vol. 70, no. 2, pp. 449–453, 2024, doi: 10.24425/ijet.2024.149565.

[7] N. G. Pandey and R. S. Thakur, "Abstract : -," vol. 2, no. 3, pp. 9–12.

[8] Y. M. Hange, "a Review on Nmap and Its Features," *Int. Res. J. Eng. Technol.*, no. May, pp. 1175–1180, 2023, [Online]. Available: www.irjet.net

[9] F. Ardiyansyah, K. Setiawan, and N. Sutisna, "Implementation of IDS on Computer Networks Using Snort Based on Telegram Chatbot Implementasi IDS pada Jaringan Komputer Menggunakan Snort Berbasis Chatbot Telegram," vol. 4, no. October, pp. 1614–1623, 2024.

[10] K. Kunci, "The Indonesian Journal of Computer Science," vol. 13, no. 4, pp. 6549–6562, 2024.

[11] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[12] R. Achmad, E. V. Manullang, and E. R. Sanmas, "Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan Ddos Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer," *J. Teknol. Inf.*, vol. 8, no. 1, pp. 2–11, 2020.

[13] S. A. Valianta, T. Salim, and D. Stiawan, "Identifikasi Serangan Port Scanning dengan Metode String Matching," *Annu. Res. Semin.*, vol. 2, no. Fakultas Ilmu Komputer Unsri, pp. 466–471, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id466

[14] J. Pebrianto, "Perlindungan Port dari Pemindaian NMAP dan Meningkatkan Efisiensi IPv4 dengan MikroTik dan Nginx," *Media J. Inform.*, vol. 16, no. 1, p. 54, 2024, doi: 10.35194/mji.v16i1.4012.

[15] A. Aryapranata, Y. Al Rasyid, Y. P. Agsena, and S. Hermanto, "Keamanan Siber dalam Era Digital : Tantangan dan Solusi," no. October, 2024, doi: 10.55886/infokom.v8i2.932.

[16] R. M. Sinaga, S. Putra, P. Halawa, and D. Kiswanto, "IMPLEMENTASI CI / CD MENGGUNAKAN JENKINS PADA APLIKASI DI LINGKUNGAN PENGEMBANGAN FEDORA WORKSTATION 40," vol. 9, no. 1, pp. 1202–1209, 2025.

[17] I. M. Amir, Y. Mardiana, S. Kom, M. Kom, and D. Bengkulu, "Simulasi Intrusion Detection System (IDS) Dalam Keamanan Web Server Pada Jaringan," *Snasikom*, vol. 3, no. 1, pp. 69–82, 2023.

[18] T. Purnama, Y. Muhyidin, and D. Singasatia, "Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi," *J. Teknol. Inf. Dan Komun.*, vol. 14, no. 2, pp. 358–369, 2023, doi: 10.51903/jtikp.v14i2.726.

[19] N. ardi S. P. Pratama and Y. Servanda, "Analisis Serangan Forensik Terhadap Serangan Ddos Ping Of Death Menggunakan Tools NMAP dan HPING3," *J. Sains dan Teknol.*, vol. 4, no. 2, pp. 209–216, 2024, doi: 10.47233/jsit.v4i2.1842.

[20] J. B. Aceh, M. Km, B. Indonesia, and L. Belakang, "Analisis Celah Keamanan Jaringan terhadap Serangan Packet Sniffing dengan Metode Vulnerability Scanning," vol. 4, no. 2, pp. 255–261, 2024.

[21] N. Santi and Y. Mulyanto, "Analisis Kelayakan Jaringan Komputer Menggunakan Alat Sniffing Dan Intrusion Detection System (Ids)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 4, pp. 6141–6147, 2024, doi: 10.36040/jati.v8i4.10079.

[22] D. Hidayat and R. Ramli, "Mengoptimalkan Pencegahan Serangan Brute Force pada Linux melalui Penerapan Metode Aplikasi IDS Snort," *JiTEKH*, vol. 11, no. 2, pp. 57–61, 2023, doi: 10.35447/jitekh.v11i2.764.