Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning

Nuroji
Teknik Informatika, Universitas Muhammadiyah Prof. DR. HAMKA, Indonesia
nuroji@uhamka.ac.id

Abstrak: Keamanan adalah faktor penting yang harus dipertimbangkan saat perangkat terhubung ke jaringan internet publik. Ancaman seperti pencurian informasi, kehilangan atau manipulasi data, dan gangguan layanan sering terjadi pada jaringan publik. Sebagai administrator jaringan, keharusan untuk terus memantau dan mencegah ancaman keamanan, terutama terhadap jaringan, untuk mengurangi risiko dan kerugian yang ditimbulkan oleh tindakan yang tidak bertanggung jawab. Aplikasi Port Scanner digunakan untuk memperoleh informasi atau status protokol dan port yang terbuka pada suatu perangkat. Dari informasi tersebut, serangan terhadap sumber daya jaringan dapat dilakukan, seperti Distributed Denial of Service (DDoS). Oleh karena itu, peneliti melakukan mitigasi terhadap serangan Port Scanner pada Router Mikrotik dengan menerapkan metode Port Scan Detection (PSD).
Kata Kunci: Keamanan Jaringan; Port Scan Detection (PSD); Intrusion Detection System (IDS); Intrusion Prevention System (IPS); Port Scan; Jaringan Komputer;

Abstract: Security is an important factor to consider when devices are connected to public internet networks. Threats such as information theft, data loss or manipulation, and service disruptions often occur on public networks. As a network administrator, it is necessary to continuously monitor and prevent security threats, especially against the network, in order to reduce the risks and losses caused by irresponsible actions. Port Scanner applications are used to obtain information or status of protocols and open ports on a device. From this information, attacks on network resources can be carried out, such as Distributed Denial of Service (DDoS). Therefore, researchers mitigate Port Scanner attacks on Mikrotik routers by applying Port Scan Detection (PSD) methods.
Keywords: Network Security; Port Scan Detection (PSD); Intrusion Detection System (IDS); Intrusion Prevention System (IPS); Port Scan; Computer network;

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

1. PENDAHULUAN

Jumlah dan kompleksitas serangan dunia maya semakin meningkat dengan pesat selama beberapa tahun terakhir. Kita sudah menyaksikan dampak menghancurkan dari serangan seperti WannaCry, Petya, Bruteforce, serta munculnya jenis serangan baru seperti cryptojacking dan web deface. Serangan-serangan tersebut dapat menyebabkan kerugian finansial, kehilangan data penting, atau bahkan membahayakan keselamatan pengguna jaringan. Oleh karena itu, penting untuk selalu meningkatkan kewaspadaan dan mengambil tindakan pencegahan yang tepat untuk melindungi jaringan dan data dari serangan dunia maya**.**[1]

Dengan kecanggihan dan semakin masifnya serangan pada jaringan komputer, maka hal ini memicu kepada penanggung jawab yaitu seorang administrator jaringan untuk memngamankan pada jaringan komputernya. Di era teknologi sekarang ini semakin mudah dalam mengakses suatu data melalui jaringan internet tak terkecuali dari orang-orang yang akan berniat buruk terhadap data tersebut dengan cara akses secara illegal, bahkan seseorang yang dengan sengaja untuk mengganti halaman web dengan metode *deface* menjadi halaman web yang lain seperti halaman web perjuadian online.[2]

Dalam hal tersebut sesorang yang tidak bertanggung jawab selalu melakukan pengintaian *protocol* pada sebuah server yang menampung sebuah web atau aplikasi yaitu dengan cara scanning port yang terbuka pada sebuah perangkat *server web* atau aplikasi.

Aplikasi port scanner dapat menjadi awal dari serangan pada sumber daya di jaringan. Ketika seorang 'hacker' berhasil mendapatkan informasi tentang protokol atau port yang digunakan, mereka dapat memanfaatkannya untuk melakukan eksploitasi. Contohnya adalah serangan Distributed Denial of Service (DDoS). Ada banyak aplikasi port scanner yang umum digunakan, seperti nmap, netcut, dan unicornscan.Indonesia menjadi salah satu negara yang terkena paparan virus Corona (COVID-19) sejak awal tahun 2020. Untuk mengatasi situasi pandemi COVID-19, masyarakat harus memiliki pola hidup baru yang diterapkan dalam segala aspek kehidupan. Dalam sektor kerja dan pendidikan, telah diterapkan sistem kerja dan belajar dari rumah, yang mayoritas didukung oleh media internet. Data survei Penetrasi dan Perilaku Penggunaan Internet, yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada bulan Juni 2022 menunjukkan bahwa penggunaan internet menjadi bagian penting dari pola hidup baru ini. jumlah pengguna internet Indonesia meningkat menjadi 210.026.769 jiwa dari total populasi 272.682.600 jiwa penduduk Indonesia Tahun 2021. Adapun persentase jumlah pengguna internet tersebut sebesar 77,02%.[3]

Penyebab meningkatnya serangan siber di Indonesia adalah karena meningkatnya jumlah pengguna internet secara linier. Menurut data Badan Siber dan Sandi Negara (BSSN), terdapat sekitar 266.741.784 upaya serangan siber di Indonesia pada rentang waktu Januari hingga Agustus 2021. [4]

Dalam jaringan internet yang terbuka, orang yang tak bertanggung jawab dapat dengan mudah mengaksesnya dan melakukan serangan yang mengganggu fungsi sistem. Maka dari itu, diperlukan sistem keamanan jaringan yang mampu mendeteksi serangan dan gangguan keamanan. Salah satu serangan yang sering terjadi adalah penyusupan ke dalam sistem jaringan, yang lebih dikenal dengan istilah network intrusion.[5]

Dalam hal ini, penulis melaukan merancang dan mengimplementasikan Intrusion Detection dan Sistem Pencegahan (IDPS). Detection dan Sistem Pencegahan IDPS merupakan sistem pertahanan yang terus memantau jaringan untuk aktivitas yang tidak biasa dan lalu lintas jaringan berbahaya dan menerapkan tindakan pencegahan terhadap serangan siber, gangguan yang terdapat dalam jaringan berupa port scanner. [1] Sistem Deteksi Intrusi (IDS) melakukan pengawasan terhadap aktivitas yang mencurigakan dan traffic jaringan. Jika aktivitas yang tidak normal ditemukan, IDS akan memberikan peringatan ke administrator atau sistem jaringan. Dalam beberapa kasus, IDS juga dapat

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : https://doi.org/10.58602/dimis.v1i2.35
Page 41-49

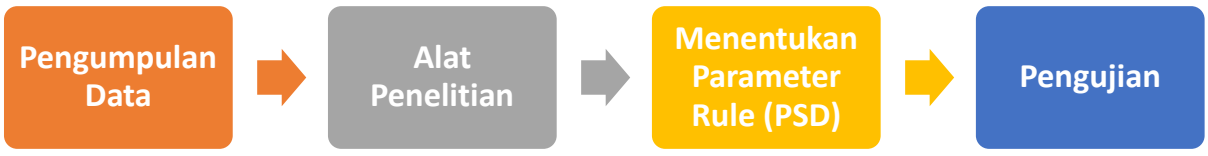
memblokir akses pengguna atau alamat IP sumber yang melakukan usaha untuk mengakses jaringan melalui tindakan pencegahan untuk traffic yang tidak normal.[6]

Intrusion Detection System (IDS) melakukan pengawasan terhadap aktivitas yang mencurigakan dan traffic jaringan. Jika aktivitas yang tidak normal ditemukan, IDS akan memberikan peringatan ke administrator atau sistem jaringan. Dalam beberapa kasus, IDS juga dapat memblokir akses pengguna atau alamat IP sumber yang melakukan usaha untuk mengakses jaringan melalui tindakan pencegahan untuk traffic yang tidak normal.[6] Metode pengamanan jaringan yang disebut Intrusion Prevention System (IPS) dapat dilakukan melalui software atau hardware. IPS berfungsi memantau aktivitas tidak diinginkan dari intrusion dan meresponsnya secara cepat untuk mencegah aktivitas tersebut.[6]. Dengan meningkatnya perangkat terhubung Internet secara masif, mungkin ada peningkatan aktivitas diam-diam di balik Internet.

Tindakan awal yang dilakukan dalam Port Scan adalah untuk mendapatkan informasi atau status dari protokol dan port yang terbuka pada suatu perangkat. Setelah mendapatkan informasi terkait protokol atau port, maka peretas dapat memanfaatkannya untuk melakukan eksploitasi melalui protokol atau port tersebut. Biasanya ada jumlah besar port yaitu 65.535 port tcp dan 65.535 port udp. Nomor port mulai dari nol hingga 1024 adalah port terkenal. Sebagai contoh, port 80 terkait dengan http; port 21 termaping ke ftp, port 25 ke smtp, dan seterusnya.[7]. Dengan kondisi seperti tersebut maka peneliti melakukan Mitigasi terhadap serangan Port Scanner pada Router Mikrotik dengan metode Port Scan Detection (PSD). Port Scan Detection (PSD) adalah sebuah sistem yang digunakan untuk mendeteksi aktivitas mencurigakan pada jaringan. PSD digunakan untuk menangani atau mencegah serangan sedini mungkin, karena serangan semacam itu dapat menjadi awal dari serangan terhadap sumber daya di jaringan. Setelah informasi protokol atau port didapatkan, dapat dimanfaatkan untuk melakukan eksploitasi pada protokol atau port tersebut, seperti serangan Brute Force.

2. METODE PENELITIAN

Metodologi penelitian yang dilakukan dalam penelitian ini mempunyai beberapa tahapan, tahapan yang dilakukan dalam penelitian dapat dilihat pada Gambar 1.



Gambar 1. Metodologi penelitian

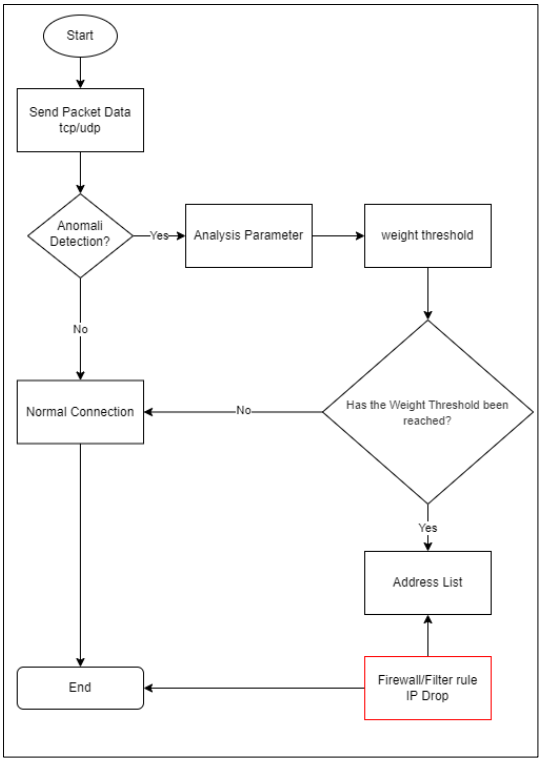
Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dengan melakukan observasi lapangan dengan pengecekan IP Services List dalam hal ini Port yang terbuka pada jaringan komputer, dari hasil observasi terdapat logs ilegal akses ke perangkat jaringan sehingga peneliti melakukan mitigasi preventif dengan melakukan Port Scan Detection (PSD).

Berikut ini adalah flowchart yang menggambarkan proses deteksi yang akan diterapkan:

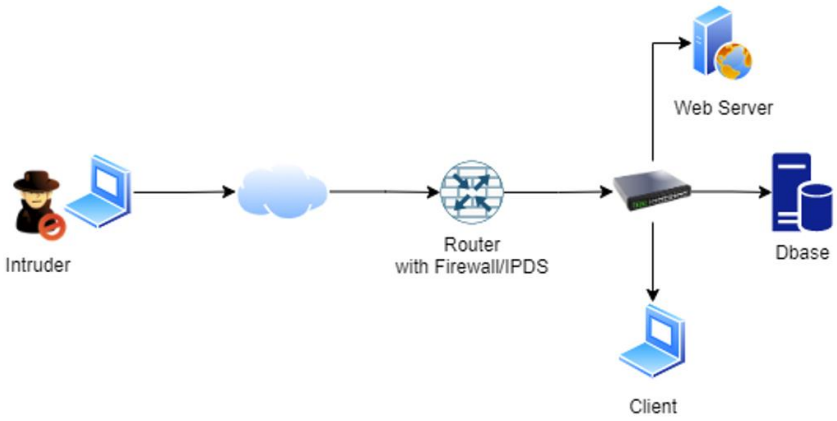
Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49



Gambar 2. Flowchart sistematika penerapan IPDS

Skema penerapan IPDS ini seperti yang terlihat pada gambar 2, satu seorang intruder yang akan melakukan scaning port terhadap service protocol/port ke beberapa perangkat jaringan diantaranya router mikrotik, web server, database server yang sebagai target untuk di ambil informasi dari perangkat yang ada disebuah jaringan dan ketika intruder mendapatkan informasi maka bisa di lakukan penyerangan selanjutnya.



Gambar 3. Skema Penerapan IPDS

Alat Penelitian

Perangkat keras dan perangkat lunak yang digunakan pada penelitian ini adalah Mikrotik CCR1036-8G-2S+ dengan sepesifikasi sebagai berikut:

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

Tabel 1. Spesifikasi Perangkat

Nama	Spesifikasi
Architecture	TILE
CPU	TLR4-03680
CPU core count	36
CPU nominal frequency	1.2 GHz
RouterOS license	6
Operating System	RouterOS
Size of RAM	4 GB
Storage size	1 GB

Menentukan Parameter Rule (PSD)

Penentuan parameter pada *Port scan detection* (PSD) Ada empat parameter penting yang harus ditentukan yaitu *Weight Threshold, Delay Threshold, Low Port Weight, dan High Port Weight*. Parameter-parameter ini digunakan untuk memantau dan mengontrol lalu lintas jaringan guna mendeteksi dan mencegah ancaman keamanan.

Tabel 2. Nilai Parameter *rule* PSD

Nama Parameter	Nilai Parameter
Weight Threshold	21, 22, 23
Delay Threshold	00:00:03
Low Port Weight	3
High Port Weight	1

Pengujian

Pada pengujian ini peneliti menggunakan *Software tools Advanced Port Scanning* dan *Nmap* dengan skema tanpa menggunakan IPDS dan sesudah menggunakan IPDS.

3. HASIL DAN PEMBAHASAN

Rule Pengaturan PSD

Pada pengaturan rule ini merupakan langkah untuk mengaktifkan PSD, pada rule ini di buatkan lima rule, pada rule ini untuk melindungi port di antara lain port 21, 22, 23, 80, 443, Pembuatan chain yang digunakan Forward dan protocol yang digunakan tcp serta Connection State nya adalah New.

Parameter Rule PSD

a. **Weight Threshold (WT)**
   Akan dihitung jumlah nilai gabungan antara 'LowPortWeight' dan 'HighPortWeight' untuk setiap paket TCP/UDP yang berasal dari alamat IP yang sama, namun memiliki tujuan port yang berbeda. Dalam implementasinya, aturan PSD akan diterapkan ketika nilai total dari kedua bobot mencapai angka 21, 22, 23, 80, atau 443. Hal ini bertujuan untuk meminimalkan dampak dari serangan yang mungkin terjadi pada jaringan, serta menjaga keamanan dan kinerja jaringan yang optimal.
b. **Delay Threshold (DT)**
   Aplikasi port scanner yang berasal dari alamat IP host atau sumber yang sama akan memiliki nilai waktu jeda (delay) sebesar 3 detik (00:00:03) untuk setiap trafik atau paket yang dikirimkan dengan tujuan port yang berbeda.
c. **Low Port Weight (LPW)**
   Dalam sistem, apabila terdeteksi adanya trafik atau paket dari Port Scanner yang diarahkan ke 'Low Port', yakni port dengan nomor yang lebih kecil dari 1024 atau

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

termasuk dalam kategori System/Well-Known Port, maka sistem akan memberikan nilai 3, Port yang sering digunakan dalam jaringan antara lain: Port 80 untuk protokol HTTP, Port 443 untuk protokol HTTPS, Port 53 untuk protokol DNS, Port 22 untuk protokol SSH, Port 23 untuk protokol Telnet, Port 110 untuk protokol POP3, dan Port 25 untuk protokol SMTP.

d. High Port Weight (HPW)

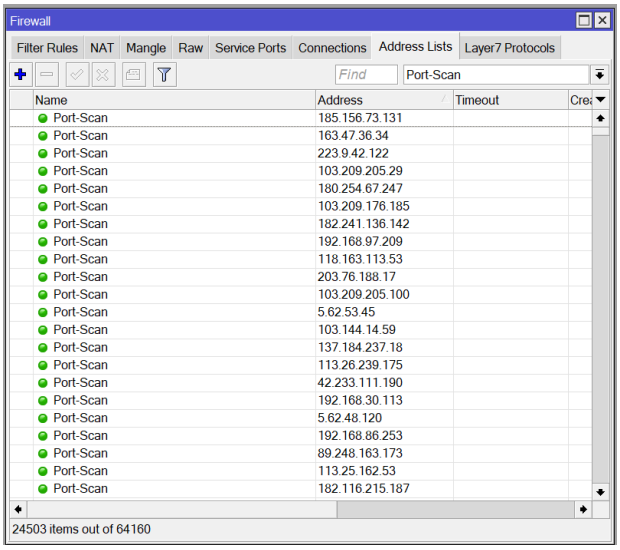
Sistem akan memberikan nilai 1 jika terdapat lalu lintas paket dari Port Scanner yang ditujukan ke 'High Port', yaitu port dengan nomor di atas 1024 atau termasuk dalam kategori registered port dan dynamic/private port. Contohnya adalah port 3128 untuk Squid web-Proxy, 1080 untuk SOCKS Proxy, 1701 untuk L2TP, dan 1723 untuk PPTP. Hal ini dilakukan untuk mempermudah identifikasi dan analisis terhadap jenis lalu lintas jaringan yang masuk ke dalam sistem.

Aksi Tindakan

Setelah menentukan rule parameter PSD adalah melakukan aksi Tindakan yang akan dilakukan setelah parameter terpenuhi. Setelah di parameter terpenuhi maka akan dilakukan Tindakan Address-list dari IP Host yang melakukan port scanning dengan nama Port-Scan.

Address Lists

Rule yang dibuat seperti yang terlihat pada Gambar 5 menyebabkan IP Address perangkat yang menjalankan aplikasi port scanner secara otomatis dimasukkan ke dalam daftar 'Address-List'. Tindakan ini bertujuan untuk mempermudah manajemen jaringan serta memastikan keamanan jaringan dari serangan yang tidak diinginkan.



Gambar 4. Address Lists

Filter Rule block IP Address

Di dalam filter rule ini menggunakan chain input, tujuannya untuk melindungi perangkat jaringan dari serangan yang dari luar jaringan masuk ke jaringan.

Aksi Tindakan

Pada aksi Tindakan di filter rule ini akan melakukan Tindakan eksekusi pemblokiran terhadap IP Address yang di dapat dari rule parameter yang di anggap pelaku yang melakukan port scanning.

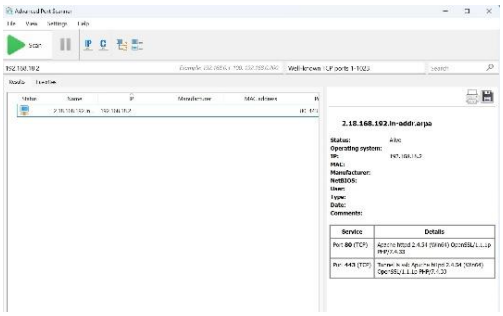
Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

Pada parameter rule ini setiap kali terdeteksi koneksi baru (state=new) dengan protokol TCP menuju port 21, 22, 23, 80, atau 443 dengan pola (PSD) yang mencurigakan, maka alamat IP pengirim akan ditambahkan ke daftar alamat (address list) bernama "port scanner" dengan waktu timeout 10 menit. selanjutnya, semua koneksi dengan alamat IP pengirim yang masuk dalam daftar "port scanner" akan di-drop/ditolak.

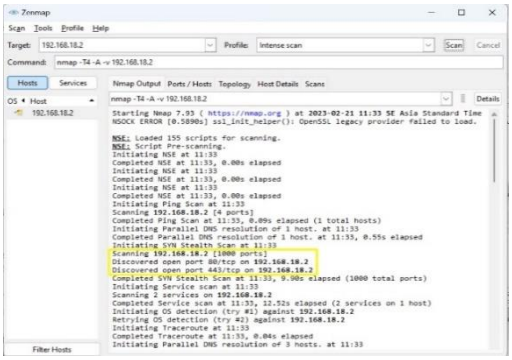
Pengujian Penggunaan IPDS

Setelah melakukan pengujian menggunakan *Advanced Port Scanning* tanpa menggunakan IPDS terlihat terdeteksi port yang ada di web server seperti terlihat di Gambar 5.



Gambar 5. Pengujian pertama terdeteksi port

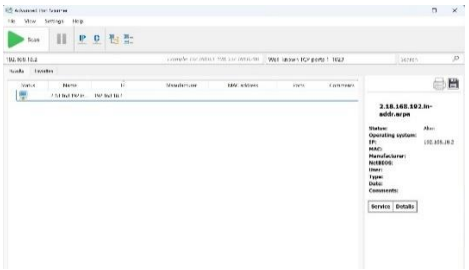
Hasil pengujian kedua yaitu dengan menggunakan *tools Nmap* maka terlihat port yang ada di web server terdeteksi seperti terlihat di Gambar 6.



Gambar 6. Pengujian kedua terdeteksi port

Hasil penerapan IPDS

Hasil pengujian pertama dengan cara menerapkan IPDS dan hasilnya port yang ada di web server tidak terdeteksi oleh *Advanced Port Scanning* seperti terlihat di Gambar 7.

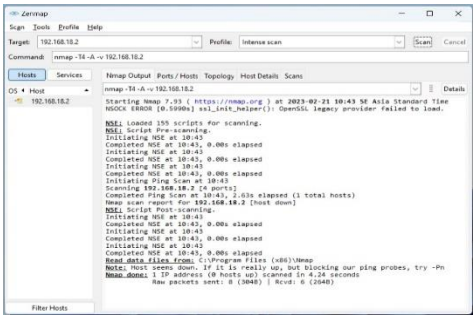


Gambar 7. Pengujian tidak terdeteksi port

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

Hasil pengujian pertama dengan cara menerapkan IPDS dan hasilnya port yang ada di web server tidak terdeteksi oleh *Nmap* seperti terlihat di Gambar 8.



Gambar 8. Pengujian Nmap tidak terdeteksi port

Pada Tabel 3 menyajikan secara ringkas hasil pengujian penyerangan port scanning ke target, baik yang dilindungi IPDS maupun yang tidak dilindungi. Dari hasil tersebut, terlihat bahwa tanpa menggunakan IPDS, jaringan menjadi rawan diserang karena penyerang dapat mendeteksi semua port target yang aktif melalui port scanning. Port scanning sendiri merupakan langkah awal dari serangan lanjutan, karena port menjadi pintu masuk untuk masuk ke dalam komputer korban. Namun, dengan menerapkan IPDS, penyerang tidak dapat mendeteksi keberadaan port yang aktif sehingga serangan selanjutnya dapat dihindari.

Tabel 3. Pengujian

No	Tool Serangan	Keberadaan Port yang Aktif	
		Tanpa IPDS	Dengan IPDS
1	Nmap	Terdeteksi	Tidak Terdeteksi
2	Advanced Port Scanner	Terdeteksi	Tidak Terdeteksi

Dari hasil yang didapat dari penerapan IPDS dari penyerangan dari luar jaringan public ke perangkat kami seperti Tabel 2.

Tabel 2. Jumlah serangan

No	Waktu	Jumlah Serangan
1	Hari 1	342
2	Hari 2	373
3	Hari 3	428

4. KESIMPULAN

Dari hasil penelitian yang diberi judul " Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning di Universitas Muhammadiyah Prof. DR. HAMKA", dapat disimpulkan bahwa penerapan IPDS dengan parameter PSD sangat penting dalam mencegah dan menangani

Nuroji: *Penulis Korespondensi

Journal of Data Science and Information System (DIMIS)
Website : https://ejournal.techcart-press.com/index.php/dimis
E-ISSN 2985-5608
P-ISSN 2985-5594
Volume 1, Number 2, May 2023
DOI : **https://doi.org/10.58602/dimis.v1i2.35**
Page 41-49

serangan Port Scanning pada Router dan server web di dalam jaringan. Kesimpulan tersebut didasarkan pada hasil permasalahan yang telah dibahas dan analisis dari penelitian tersebut.

5. REFERENCES

[1] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *Journal of Network and Computer Applications*, vol. 136, pp. 71–85, Jun. 2019, doi: 10.1016/j.jnca.2019.03.005.

[2] E. S. Alim and H. Jin, "Data Security and Privacy Assurance for Cloud Computing in Education Based on a Third Party Auditor," *Basic Clin Pharmacol Toxicol*, vol. 124, no. S3, pp. 142–144, Apr. 2019, doi: 10.1111/bcpt.13217.

[3] Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei Penetrasi dan Perilaku Penggunaan Internet," Jakarta, 2022, pp. 1–104.

[4] M. T. Andi Yusuf *et al.*, "Laporan Tahunan Honeynet Project BSSN - IHP," *Direktorat Deteksi Ancaman Badan Siber dan Sandi Negara*, vol. 1, pp. 1–94, Jan. 2019.

[5] Agustini Rodiah Machdi, Waryani, and Sugeng, "Analisa dan Implementasi Sistem Kemananan Jaringan Intrusion Detection System (IDS) Berbasis Mikrotik," *JET Jurnal Elektro Teknik*, vol. 1, no. 1, pp. 1–6, Mar. 2021.

[6] E. S. J. Atmadji, B. M. Susanto, and R. Wiratama, "Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server," *Teknika*, vol. 6, no. 1, pp. 19–23, Nov. 2017, doi: 10.34148/teknika.v6i1.55.

[7] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Jan. 2019, pp. 1–6. doi: 10.1109/ICOMET.2019.8673520.

[8] Ari Muzakir and Maria Ulfa, "ANALISIS KINERJA PACKET FILTERING BERBASIS MIKROTIK ROUTERBOARD PADA SISTEM KEAMANAN JARINGAN," *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, vol. 10, no. 1, pp. 15–20, Apr. 2019.

[9] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Information Management & Computer Security*, vol. 18, no. 4, pp. 277–290, Oct. 2010, doi: 10.1108/09685221011079199.

Nuroji: *Penulis Korespondensi