ISSN : 2548 – 8112 eISSN: 2622-8890

RANCANGAN KONFIGURASI *SECURITY* MENGGUNAKAN METODE *PORT SCANNING DETECTION* UNTUK MEMPROTEKSI JARINGAN *IP PUBLIC* DI AIRNAV CABANG PEMBANTU PADANG

Yoga Dwi Wicaksono[1], Argo Pragolo[2], Teguh Imam Suharto[3]
[1,2,3)] Politeknik Penerbangan SurabayaJl. Jemur Andayani I/73, Surabaya 60236
Email: ydwi8339@gmail.com

Abstrak

Dalam era digital yang sering berkembang, keamanan jaringan *ip public* menjadi masalah utama. Melakukan aktivitas *port scanning* atau *nmap* (*network mapper*), pengguna dapat melihat *port* terbuka pada *host* jaringan. *Security* jaringan seperti *firewall* diperlukan untuk membatasi aktivitas *nmap* (*network mapper*). Rancangan ini bertujuan menciptakan sistem keamanan jaringan *ip public* yang ringan, dan mudah diatur oleh *administrator* jaringan. *Firewall* ini dirancang menggunakan metode *port scanning detection* yang bertujuan memblokir alamat *internet protocol* (*IP*) yang melakukan aktivitas *nmap* serta terintegrasi dengan *bot telegram* sebagai notifikasi apabila terjadi aktivitas *nmap*. Metode ADDIE digunakan pada penelitian ini yang berisi *Analyze*, *Design*, *Develop*, *Implementation*, dan *Evaluate*. *Security* ini menggunakan *software winbox* untuk konfigurasi *firewall* serta integrasi dengan *bot telegram*. Pengujian lapangan menggunakan *software zenmap* untuk melakukan *nmap* pada jaringan *ip public*. Hasil pengujian lapangan *firewall* dapat memblokir aktivitas *nmap* jaringan dan mengirimkan pesan notifikasi ke *bot telegram.* Hasil *QoS* menunjukkan *troughput* 104 *kbps*, *packet loss* 0,3%, *delay* 18,07 ms, dan *jitter 0,005 ms.* Nilai rata-rata dari validasi *instrument* adalah 90,2%, yang masuk dalam kategori sangat setuju.
Kata Kunci: Keamanan Jaringan, *Port Scanning*, *Firewall*, *Winbox*, *Zenmap.*

Abstract

In the frequently evolving digital era, public ip network security is a major issue. Performing port scanning or nmap (network mapper) activities, users can view open ports on network hosts. Network security such as firewalls are needed to limit nmap (network mapper) activities. This design aims to create a public ip network security system that is lightweight, and easy to manage by network administrators. This firewall is designed using the port scanning detection method which aims to block internet protocol (IP) addresses that carry out nmap activities and is integrated with telegram bots as notifications in the event of nmap activity. ADDIE method is used in this research which contains Analyze, Design, Develop, Implementation, and Evaluate. This security uses winbox software for firewall configuration and integration with telegram bots. Field testing uses zenmap software to nmap the public ip network. The firewall field test results can block network nmap activity and send notification messages to telegram bots. QoS results show a throughput of 104 kbps, packet loss of 0.3%, delay of 18.07 ms, and jitter of 0.005 ms. The average value of instrument validation is 90.2%, which falls into the strongly agree category.
***Keywords**: Network Security, Port Scanning, Firewall, Winbox, Zenmap.*

ISSN : 2548 – 8112 eISSN: 2622-8890

PENDAHULUAN

Pada era digital yang semakin maju, keamanan sistem jaringan dan data menjadi semakin penting. Seiring dengan berkembangnya teknologi, taktik dan metode serangan peretas pun semakin beragam dan canggih [1]. Perusahaan - perusahaan seperti Airnav Indonesia perlu memperhatikan dan meningkatkan keamanan sistem jaringan serta data yang ada didalamnya mereka agar terhindar dari serangan peretas yang dapat mengganggu kelancaran dan keberlangsungan bisnis Perusahaan [2].

Suatu metode yang dapat digunakan untuk proteksi sistem jaringan dan data adalah metode *port scanning detection*. Metode *port scanning* adalah suatu teknik yang dilakukan penyerang untuk *scanning* terhadap *port-port* yang ada pada suatu sistem komputer atau jaringan [3]. *Port scanning* merupakan jenis serangan yang biasanya dilakukan oleh penyerang untuk mencari celah atau celah pada sistem yang ingin diserang [4].

Faktor – faktor yang mendorong penelitian tentang *port scanning detection* antara lain meningkatnya jumlah serangan *port scanning* yang terjadi, kompleksitas jaringan yang semakin tinggi, serta pentingnya keamanan sistem informasi bagi berbagai sektor industri dan pemerintahan. Adanya sistem deteksi yang efektif, diharapkan dapat membantu meningkatkan keamanan sistem informasi dari serangan *port scanning*. Penelitian dengan judul Rancangan Konfigurasi *Security* Menggunakan Metode *Port Scanning Detection* untuk Memproteksi Jaringan *IP Public* di Airnav Cabang Pembantu Padang diharapkan dapat membatasi aktivitas *port scanning* pada jaringan *ip public* dengan cara memblokir *ip* yang melakukan aktivitas *port scanning* pada jaringan.

1. Keamanan Jaringan

Perlindungan proteksi sistem jaringan merupakan serangkaian tindakan, ketentuan, dan teknologi yang digunakan untuk melindungi jaringan komputer dari ancaman dan serangan yang dapat menyebabkan akses tidak sah, sabotase, trouble sistem, atau sistem eror. Tujuan utama perlindungan keamanan proteksi jaringan yang utama yaitu menjaga integritas, keamanan, dan ketersediaan data layanan pada jaringan. Aspek penting dari proteksi sistem jaringan meliputi identifikasi dan autentikasi, otorisasi, *enkripsi*, *firewall*, tambalan dan pembaruan, pelacakan dan analisis, serangan *malware*, *sniffing* dan perantara, perlindungan fisik, dan perangkat keamanan [5].

2. Port Scanning Detection

Port scanning detection adalah *firewall* yang dapat dikonfigurasi dalam jaringan dan berfungsi mendeteksi upaya serangan peretas dengan metode *port scanning detection* [6]. *Port scanning detection* dapat beroperasi dengan *software*, seperti IDS (*Intrusion Detection System*) atau IPS (*Intrusion Prevention System*), yang memantau paket data suatu sistem jaringan dan mengidentifikasi pola aktivitas pergerakan mencurigakan [7].

3. Firewall

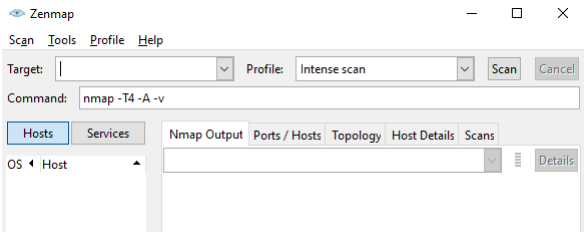
Firewall didefinisikan sebagai suatu metode atau mekanisme yang diterapkan pada *hardware, software* atau sistem itu sendiri dengan tujuan memproteksi atau *filter*, membatasi atau memblokir satu atau semua koneksi/aktivitas. Suatu segmen data, jaringan *private* dengan jaringan *eksternal* yang tidak terhubung. Membatasi, *frewall* digunakan untuk mengontrol akses antara jaringan internet *private*. *Firewall* semakin menjadi fitur *standart* yang dikonfigurasi ke semua *server* yang terhubung pada sistem jaringan [8].

4. Winbox software

Gambar 1 Tampilan *Winbox*

Winbox merupakan *utilitas* atau *software* yang digunakan untuk menghubungkan dan mengkonfigurasi *mikrotik* berdasarkan alamat *MAC address* atau *IP protocol*. Menggunakan *Winbox*, pengguna dapat mengkonfigurasi sistem operasi dan *board Router Mikrotik* dengan menggunakan metode GUI (*Graphical User Interface*) [9]. *Setting proxy* melalui *Winbox* lebih banyak digunakan karena kemudahan penggunaannya, pengguna tidak perlu menghafal perintah konsol. Kelebihan *winbox* ini adalah mudah dikendalikan dari jarak jauh karena berbasis GUI (*Graphical User Interface*).

5. Zenmap Software



Gambar 2 Tampilan *Zenmap*

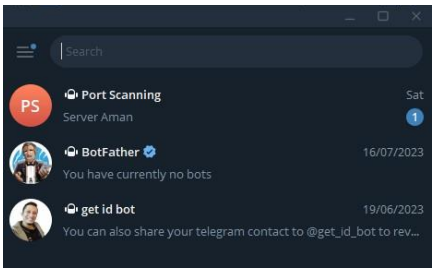
Nmap atau biasa disebut juga *Network Mapper* merupakan sebuah *tools* atau alat yang digunakan untuk eksplorasi jaringan, dengan menggunakan *Nmap* dapat melakukan penelusuran pada jaringan untuk menetahui *service* apa yang aktif pada suatu *port* yang lebih spesifik [10]. Fungsi utama *nmap* adalah pemindaian *port*, yang menurut definisinya adalah operasi *probing* yang diotomatisasi oleh *nmap*. Pemindai ini adalah pemindai *port TCP/IP*, sebuah program yang menyerang *port* dan layanan (*telnet, ftp, http*, dll.). Menggunakan cara ini, pengguna dapat mencari informasi dari *server* target [11].

6. Wireshark

Gambar 3 Tampilan *Wireshark*

Wireshark merupakan *software open-source*, berfungsi untuk monitoring jaringan. Menggunakan *wireshark*, pengguna dapat memantau dan menganalisis lalu lintas jaringan, mengeksplorasi protokol jaringan, dan menganalisis masalah jaringan. *Wireshark* mendukung berbagai protokol jaringan, termasuk protokol *TCP/IP*, *HTTP*, *DNS*, *FTP*, *SSH*, dan banyak lainnya. Selain itu, *software wireshark* memiliki berbagai fitur analisis yang kuat, berupa *filter* paket, kemampuan *reassembling* paket yang terpisah, serta penguraian protokol yang mendetail [12].

7. Telegram



Gambar 4 Tampilan *Telegram*

Telegram merupakan software pesan teks instan berbasis *cloud* yang mengutamakan kecepatan dan keamanan. Telegram dirancang untuk memudahkan pengguna saling mengirim pesan *teks*, audio, video, gambar dan *sticker* [13].

8. Quality of Service

Quality of Service merupakan metode pengukuran kecepatan internet untuk memberikan kualitas layanan yang baik dengan menggunakan aplikasi *wireshark*.

ISSN : 2548 – 8112 eISSN: 2622-8890

QoS mencakup *Troughput, Packet Loss, Delay,* dan *Jitter* [14].

a. Troughput

Troughput merupakan jumlah total kedatangan paket yang sukses diamati pada tujuan selama interval waktu tertentu [14].

Tabel 1 Kategori *Troughput*

Kategori *Throughput*	*Throughput* (bps)	Indeks
Sangat bagus	100	4
Bagus	75	3
Sedang	50	2
Buruk	<25	1

b. Packet Loss

Packet loss adalah parameter yang menggambarkan sebagai kegagalan transmisi paket data untuk mencapai tujuannya [14].

Tabel 2 Kategori *Packet Loss*

Kategori *Packet Loss*	*Packet Loss* (%)	Indeks
Sangat bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Buruk	25 %	1

c. Delay

Delay (*Latency*) merupakan waktu yang dibutuhkan suatu data untuk menempuh jarak dari titik asal ke tujuan [14].

Tabel 3 Kategori *Delay*

Kategori *Delay*	*Delay* (ms)	Indeks
Sangat bagus	< 150 m/s	4
Bagus	150 s/d 300 m/s	3
Sedang	300 s/d 450 m/s	2
Buruk	> 450 m/s	1

d. Jitter

Jitter merupakan perbedaan waktu antara kedatangan paket satu dengan yang lainnya.

Tabel 4 Kategori *Jitter*

Kategori *Jitter*	*Jitter*	Indeks
Sangat bagus	0 m/s	4
Bagus	0 s/d 75 m/s	3
Sedang	75 s/d 125 m/s	2
Buruk	125 - 225 m/s	1

METODE

Metode yang dipakai pada pembuatan *firewall port scanning detection* ini yaitu menggunakan metode ADDIE yang terdiri dari *Analysis, Design, Development,* dan *Evaluation.* Perancangan konfigurasi *security* menggunakan metode *port scanning detection* ini diharapkan dapat membatasi aktivitas *port scanning* pada jarinan *ip public* sehingga dapat memproteksi data *client* yang ada didalamnya. Penjabaran metode ADDIE dalam penelitian ini dapat dijabarkan sebagai berikut.

1. Analysis

Analysis merupakan kegiatan mengumpulkan data atas fenomena yang terjadi. *Analysis* dapat dilakukan dengan cara membaca jurnal yang terkait dan relevan dengan permasalahan *port scanning* pada jaringan.

2. Design

Design merupakan kegiatan yang mencangkup pembuatan design untuk *firewall port scanning detection* serta menentukan peralatan *software* dan *hardware* yang diperlukan untuk menunjang keberhasilan *firewall port scanning detection.*

3. Development

Development merupakan aktivitas untuk menimplementasikan *design firewall* yang telah dibuat. *Development* mencakup konfigurasi *firewall port scanning detection,* penambahan *user* pengguna akses *router*, dan integrasi dengan *bot telegram* untuk notifikasi keadaan aman, *warning* dan *critical*. Setelah melakukan konfigurasi dilakukan juga pengujian lapangan, *Quality of Service*, dan juga validasi *instrument*.

4. Implementation

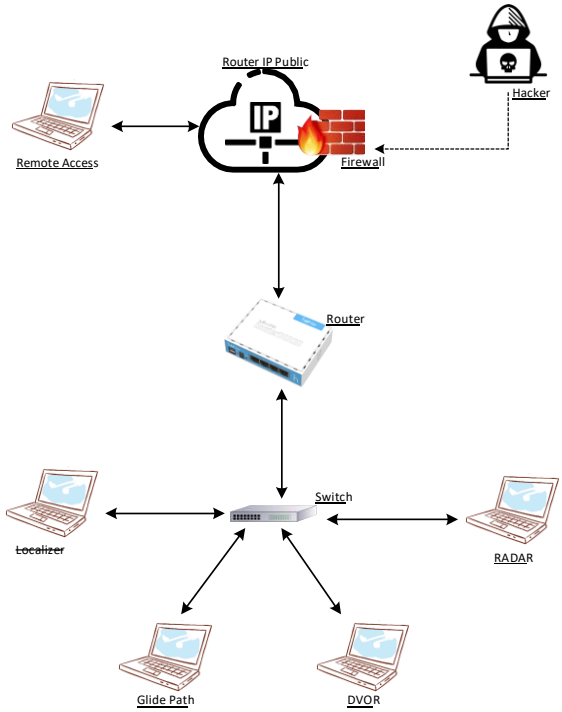
Implementation merupakan tahap penerapan *firewall* yang sudah diuji lapangan, *Quality of Service*, dan Validasi *Instrument* yang memenuhi aspek penilaian.

ISSN : 2548 – 8112 eISSN: 2622-8890

5. Evaluation

Evaluation merupakan kegiatan evaluasi dari setiap tahap pada metode ADDIE. Evaluasi ini dapat berupa saran untuk perbaikan *firewall port scanning detection.*

Blok Diagram Perancangan



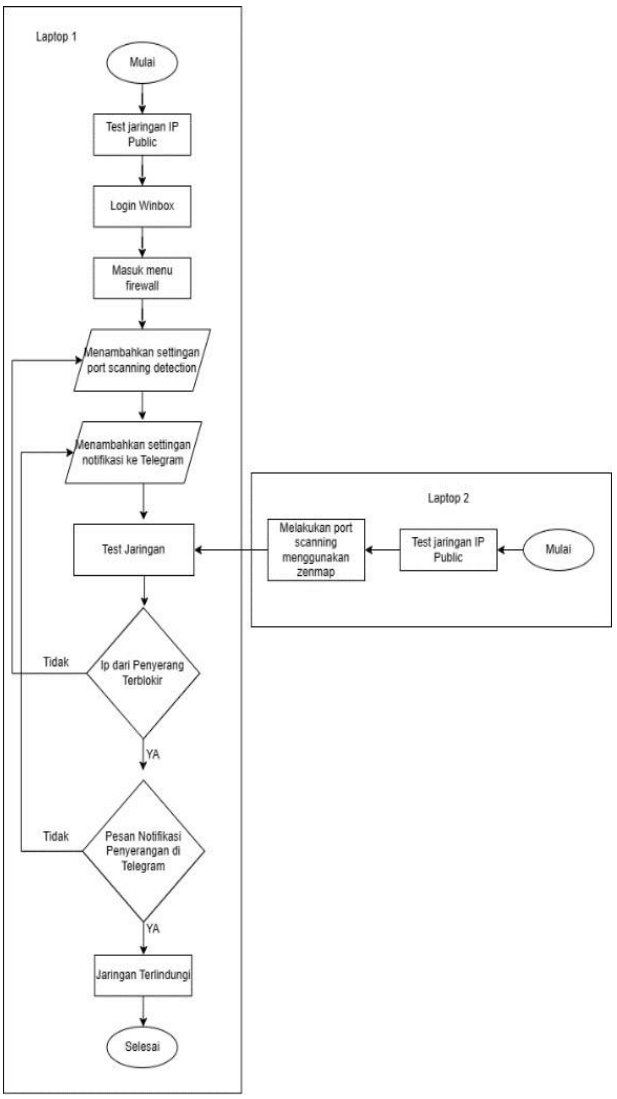
Gambar 5 Blok Diagram

Blok diagram rancangan merupakan skema rancangan *security* menggunakan metode *port scanning detection.* Data – data yang terhubung dalam *ip private* mencakup peralatan di lapangan seperti *localizer, Glide Path*, DVOR, dan RADAR. *Router ip public* berperan sebagai tempat berbagi data dari *router ip* dan *remote accsess* yang ada di lapangan. *Remote access* berfungsi untuk memudahkan teknisi.

Router ip public rentan terkena serangan dari oknum tidak bertanggung jawab seperti *hacker* yang bertujuan untuk mencari celah pada jaringan dan selanjutnya untuk mencuri data informasi atau sabotase data pada *client* yang diinginkan.

Firewall merupakan *security* jaringan yang memberikan proteksi apabila terjadi aktivitas *port scanning* pada *router ip public*. *Firewall* ini juga dapat memblokir *ip* dari penyerang dengana tempo waktu yang dapat disesuaikan dan juga dapat memberikan pesan berupa notifikasi ke aplikasi *telegram*, sehingga pengguna dapat mengetahui apabila terjadi serangan pada *router ip public*.

Flowchart Cara Kerja Alat



Gambar 6 *Flowchart* Alat

Flowchart cara kerja *security* metode *port scanning detection* dimunai dari menghidupkan laptop, kemudian *login* ke aplikasi *winbox.* Konfigurasi *firewall* dilakukan didalam aplikasi *winbox* yang kemudian juga menambahkan *scheduler* yang berfungsi untuk mengirimkan pesan *teks* ke *bot telegram* apabila *router* daalam keadaan aman, *warning* dan *critical*. Selanjutnya

ISSN : 2548 – 8112 eISSN: 2622-8890

melakukan pengujian dengan melakukan aktivitas *port scanning* atau *nmap* pada jaringan *ip public*. Hasil dari percobaan dapat berguna untuk evaluasi *firewall*.

Teknik Pengujian Alat

1. Pengujian Lapangan

Pengujian lapangan digunakan untuk menguji *security port scanning detection.* Uji coba ini dilakukan dengan melakukan aktivitas serangan *port scanning* atau *nmap* pada jaringan *ip public* menggunakan aplikasi *zenmap.*

2.* Pengujian *Quality of Service

Pengujian *Quality of Service* digunakan untuk mengukur kecepatan jaringan internet dalam menyediakan layanan kualitas yang baik menggunakan aplikasi *wireshark. QoS* terdiri dari *Troughput, Packet Loss, Delay*, dan *Jitter*.

3.* Validasi *Instrument

Validasi *instrument* ditujukan ke pada ahli yang bertujuan untuk mengetahui penilaian, kritik, dan saran pada *firewall port scanning detection.*

Tabel 5 Skala Likert

Penilaian	Nilai/ Skor
Sangat Setuju	5
Setuju	4
Kurang Setuju	3
Tidak Setuju	2
Sangat Tidak Setuju	1

Tabel 5 menunjukkan skala likert dengan rentang skor 5 sangat setuju, 4 setuju, 3 kurang setuju, 2 tidak setuju, dan 1 sangat tidak setuju. Skor yang diperoleh dari tes validasi akan diubah menjadi persentase yang ditentukan dengan rumus berikut:

$$\boldsymbol{Indeks = \frac{Skor\ yang\ diperoleh}{Jumlah\ skor\ maksium}\ x\ 100\%}$$

Persentase hasil validasi *instrument* para ahli dikumpulkan dan dihitung sesuai rumus diatas. Hasil dari perhitungan presentase disesuaikan dengan tabel 4.6 dibawah

Tabel 6 Indeks Validitas Instrument

Kriteria	Presentase Validitas *Instrument*(%)
Sangat Layak	86-100
Layak	71-85
Cukup Layak	56-70
Kurang Layak	41-55
Tidak Layak	≤40

Teknik Analisis Data

Teknik analisis data yang digunakan untuk mengumpulkan data pada penelitian ini menggunakan teknik eksperimen. Eksperimen terkait *security port scanning detection* mencakup, uji coba lapangan, *Quality of Service*, dan validasi *instrument.*

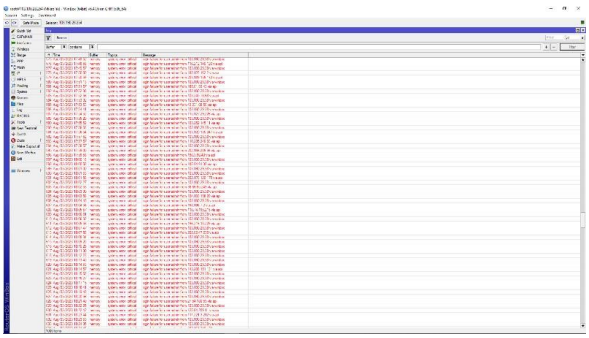
HASIL DAN PEMBAHASAN

1. Analysis

Analysis merupakan tahapan untuk menganalisa kebutuhan, mengidentifikasi masalah dan analisis penelitian yang anak dilakukan.

a. Analisis Kebutuhan

Ip public sangat rentan akan aktivitas serangan dari oknum tidak bertanggung jawab. Salah satunya dengan melakukan kegiatan *port scanning* yang dapat membahayakan data *client* didalam jaringan.



Gambar 7 Aktivitas Penyerangan Pada Server

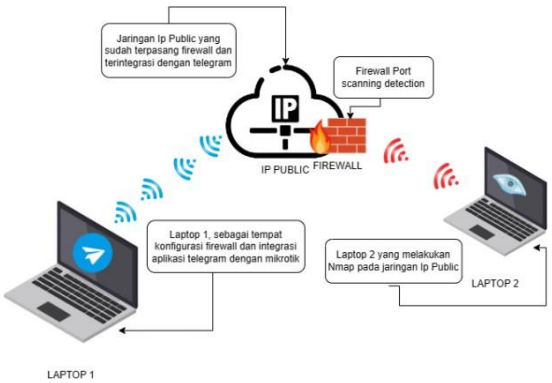
Melihat aktivitas *port scanning* yang dapat membahayakan keamanan data *client* yang ada didalamnya. Perlu dibuat *security* jaringan atau *firewall* yang dapat membatasi aktivitas *port scanning.*

ISSN : 2548 – 8112 eISSN: 2622-8890

b. Analisis Penelitian

Hasil dari studi literatur dengan pencarian jurnal, serta diskusi dengan senior teknisi, penulis memutuskan untuk membuat sebuah *security* menggunakan metode *port scanning detection*, yang dapat juga terintegrasi dengan *bot telegram* untuk sarana pemberi notifikasi keadaan router aman, *warning*, dan *critical*.

2. Design



Gambar 8 *Design* blok diagram transmis yang diinginkan

Pada gambar 1 Merupakan *design* dari *firewall port scanning* yang terdiri dari 2 buah laptop. Laptop 1 berfungsi sebagai *server* yang akan melakukan konfigurasi *firewall port scanning detection*, menambahkan *user* pengguna untuk akses *router*, konfigurasi notifikasi yang terintegrasi dengan *bot telegram* untuk mengetahui *router* dalam kondisi aman, *waring dan critical.*

Sedangkan Laptop 2 berfungsi untuk menguji konfigurasi sudah dilakukan pada jaringan *ip public*. Pengujian ini menggunakan *zenmap* untuk melakukan kegiatan *port scanning*. Hasil dari pengujian dari laptop 2 dapat menjadi referensi untuk perbaikan *firewall port scanning detection.*

a. Laptop

Laptop berfungsi sebagai media untuk melakukan install aplikasi penunjang *firewall port scanning detection* dan monitoring notifikasi.

b. Winbox

Winbox berfungsi sebagai aplikasi konfigurasi *firewall* pada jaringan.

c. Zenmap

Zenmap berfungsi untuk melakukan aktivitas *nmap* pada jaringan.

d. Wireshark

Wireshark berfungsi untuk mengukur *Troughput, Packet Loss, Delay (Latency),* dan *Jitter.*

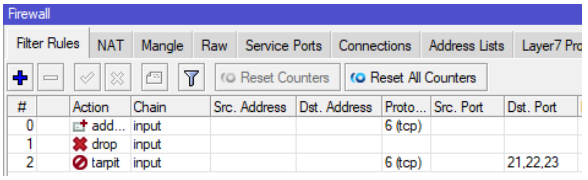
e. Telegram

Telegram berfungsi sebagai sarana penyedia notifikasi *teks.*

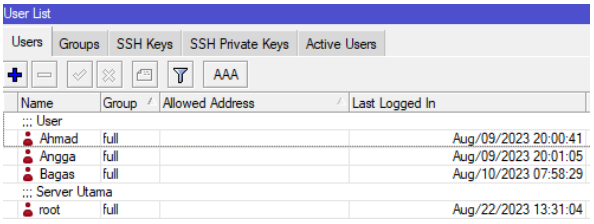
3. Development

Development merupakan tahap yang mencakup konfigurasi *firewall port scanning detection*, pembuatan *user* untuk konfigurasi router, dan integrasi notifikasi ke *bot telegram* untuk mengetahui kondisi *router* dalam keadaan aman, *warning*, dan *critical*.

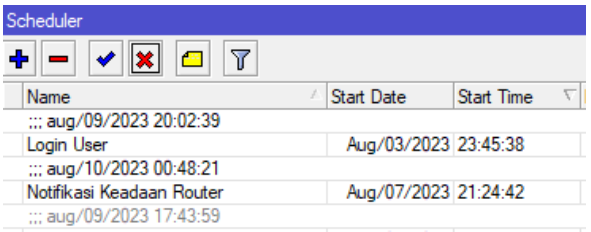
a.* Tampilan Konfigurasi *Firewall



Gambar 9 Konfigurasi *firewall port scanning detection*



Gambar 10 Penambahan akun *user*

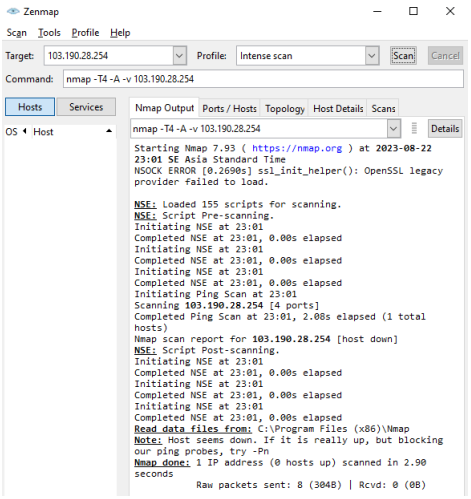


Gambar 11 Integrasi notifikasi *bot telegram*

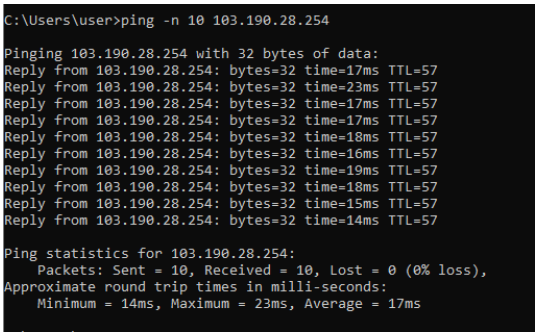
Gambar 9 merupakan konfigurasi *firewall port scanning detection*. Gambar 10 merupakan konfigurasi penambahan akun untuk konfigurasi *router*. Gambar 11 merupakan integrasi *router* dengan *tegelram* sebagai sarana notifikasi.

ISSN : 2548 – 8112 eISSN: 2622-8890

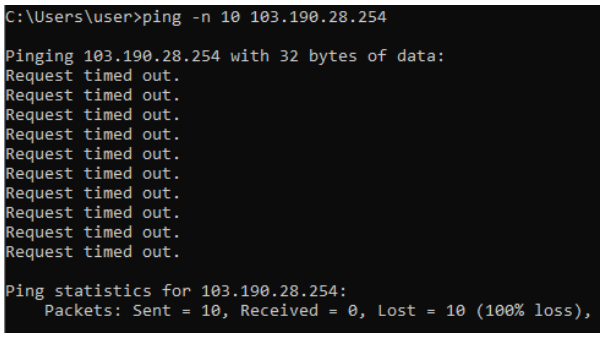
b. Uji Coba Lapangan



Gambar 12 Aktivitas nmap menggunakan *zenmap*

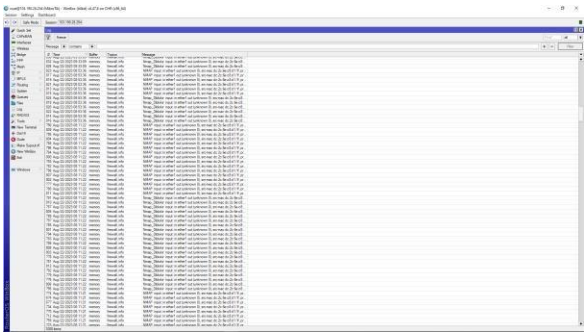


Gambar 13 *Test Cmd* sebelum *nmap*

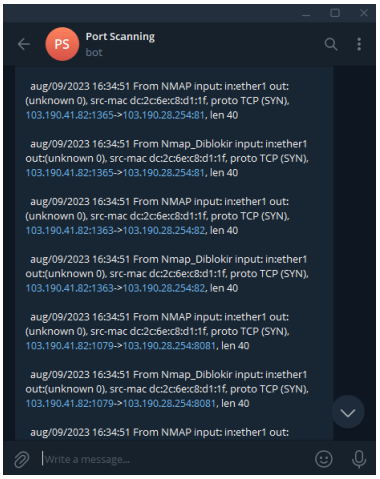


Gambar 14 *Test Cmd* setelah *nmap*

Uji coba lapangan dengan melakukan nmap menggunakan *zenmap* pada gambar 12. Hasil *test cmd* sebelum *firewall* aktif (gambar 13) laptop dapat terhubung dengan jaringan setelah melakukan *nmap*. Hasil *test cmd* setelah *firewall* aktif (gambar 14) laptop tidak dapat terhubung dengan jaringan setelah melakukan *nmap*, dikarenakan terhalang oleh *firewall*.



Gambar 15 *log history* setelah *nmap*



Gambar 16 Notifikasi *bot telegram*

Gambar 15 merupakan tampilan dari *log history* yang menampilkan aktivitas *nmap* dan pemberitahuan aktivitas *nmap* telah diblokir. Gambar 16 merupakan tampilan pesan *teks* pada *bot telegram* yang mengirimkan pesan *teks* berupa terjadi aktivitas *nmap* dan aktivitas *nmap* telah diblokir.

c. Quality of Service

Tabel 7 *QoS* Pagi Hari

Pagi Hari				
Parameter	**Waktu**	**Nilai**	**Indeks**	**Kategori**
***Throughput* (bps)**	60 detik	89 k	4	Sangat bagus
***Packet loss* (%)**		0,3	4	Sangat bagus
***Delay* (ms)**		18,07	4	Sangat bagus
***Jitter* (ms)**		0,005	4	Sangat bagus

Tabel 8 *QoS* Siang Hari

Siang Hari				
Parameter	**Waktu**	**Nilai**	**Indeks**	**Kategori**
***Throughput* (bps)**	60 detik	98 k	4	Sangat bagus
***Packet loss* (%)**		1,9	4	Sangat bagus
***Delay* (ms)**		23,77	4	Sangat bagus
***Jitter* (ms)**		0,113	4	Sangat bagus

Tabel 9 *QoS* Sore Hari

Sore Hari				
Parameter	**Waktu**	**Nilai**	**Indeks**	**Kategori**
***Throughput* (bps)**	60 detik	70 k	4	Sangat bagus
***Packet loss* (%)**		1,4	4	Sangat bagus
***Delay* (ms)**		43,85	4	Sangat bagus
***Jitter* (ms)**		0,013	4	Sangat bagus

Tabel 10 *QoS* Malam Hari

Malam Hari				
Parameter	**Waktu**	**Nilai**	**Indeks**	**Kategori**
***Throughput* (bps)**	60 detik	104 k	4	Sangat bagus
***Packet loss* (%)**		1,5	4	Sangat bagus
***Delay* (ms)**		26,69	4	Sangat bagus
***Jitter* (ms)**		0,080	4	Sangat bagus

Hasil analisa pengamatan *Quality of Service* (*QoS*) yang ditujukan pada tabel 7-10, menunjukkan indeks 4 dan termasuk dalam kategori sangat bagus saat pengamatan pagi, siang, sore, dan malam hari. Nilai parameter terbaik untuk kategori *troughput* 104 *kbps*, *packet loss* 0,3%, *delay* 18,07 *ms*, dan *jitter* 0,005 *ms*.

d. Validasi Instrument

Tabel 11 Skor Validasi Instrument

No	Aspek Penilaian	Skor Validator			Skor Maximal	Presentase	Nilai Validasi	Kategori
		1	2	3				
1	Konfigurasi Security	28	34	34	35	91,4%	90,2%	Sangat Setuju
2	Metode Port Scanning Detection	24	29	29	30	91,1%		Sangat Setuju
3	Memproteksi Jaringan	28	34	34	35	91,4%		Sangat Setuju

Berdasarkan hasil validasi *instrument* yang dapat dilihat pada tabel 11, *firewall port scanning detection* dapat digunakan di lapangan dengan tambahan revisi.

4. Implementation

Implementation merupakan tahap penerapan *firewall port scanning detection* setelah melakukan uji coba lapangan, pengukuran *Quality of Service*, dan hasil dari validasi *instrument*. Penerapan *firewall* ini diharapkan dapat bermanfaat untuk meminimalisir aktivitas *nmap* pada jaringan.

5. Evaluation

Evaluation merupakan tahap terakhir dalam metode ADDIE, dalam tahapan ini berisi tentang evaluasi dari kinerja *firewall port scanning detection* dari uji lapangan, pengukuran *Quality of Service*, dan hasil validasi *instrument.*

PENUTUP

Simpulan

1. Konfigurasi *security* menggunakan metode *port scanning detection* dapat ditambahkan menggunakan *software winbox* dengan menggunakan *rule firewall PSD.*
2. Kegiatan *nmap* ke jaringan *ip public* akan diblokir ketika *rule PSD* berjalan yang akan memberikan *input* ke *rule drop*, dan cara mengetahui *ip* dari penyerang dapat dilihat melalui *log history* atau pesan notifikasi pada *bot telegram.*
3. *History* aktivitas pada jaringan *ip public* dapat dimonitoring di *menu log* sebagai penanda aktivitas apa saja yang terjadi di jaringan *ip public*.
4. *Mikrotik* dan *bot telegram* telah terintegrasi dengan melakukan konfigurasi pada *menu scheduler*.
5. Hasil pengujian lapangan didapatkan hasil firewall dapat memblokir aktivitas *nmap* yang terjadi pada jaringan serta mengirimkan pesan notifikasi ke *bot telegram.* Hasil dari *QoS* didapatkan hasil

ISSN : 2548 – 8112 eISSN: 2622-8890

tertinggi untuk *troughput* 104 *kbps, packet loss* 0,3%, *delay* 18,07 *ms*, dan *jitter* 0,005 *ms*. Hasil dari validasi *instrument* mendapat jumlah nilai rata – rata sebesar 90,2% dan termasuk kategori sangat setuju.

Saran

1. Diharapkan pada penelitian selanjutnya, *firewall* yang dibuat dapat meminimalisir aktivitas penyerangan jaringan yang lain dan lebih kompleks.
2. Perlu diperhatikan dan ditingkatkan untuk pengiriman pesan ke *bot telegram* dari mikrotik agar lebih cepat dan efisien.
3. Diharapkan implementasi pada *network* di Airnav cabang pembantu padang bisa mendukung operasional kegiatan di tempat tersebut.
4. Diharapkan pada penelitian selanjutnya untuk menambahkan *backup firewall port scanning detection* untuk mengantisipasi *rule port scanning detection* tidak berjalan.

DAFTAR PUSTAKA

[1] Sistem J, Jscr R, Tristianto D and Joseph B 2022 Penerapan Keamanan Jaringan pada PT . Globalindo Perdana Sejahtera Menggunakan Metode Kriptografi **4** 1–7

[2] Reza R F 2020 Penerapan Keamanan Server dengan Teknik Hardening pada Sistem Operasi Ubuntu Server

[3] Anif M, Hws S and Huri M D 2015 Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang *J. TELE, Vol. 13 Nomor 1* **13** 25–30

[4] Anandita S, Rosmansyah Y, Dabarsyah B and Choi J U 2016 Implementation of dendritic cell algorithm as an anomaly detection method for port scanning attack *2015 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2015 - Proc.*

[5] Azahro A, Wulandari D and Sari U 2019 Network Address Translation Penghubung Ip Public

[6] Ananin E V., Nikishova A V. and Kozhevnikova I S 2017 Port scanning detection based on anomalies *11th Int. IEEE Sci. Tech. Conf. "Dynamics Syst. Mech. Mach. Dyn. 2017 - Proc.* **2017-Novem** 1–5

[7] Atmadji E S J, Susanto B M and Wiratama R 2017 Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server *Teknika* **6** 19–23

[8] Sudirman D and Akma Nurul Yaqin 2021 Network Penetration dan Security Audit Menggunakan Nmap *SATIN - Sains dan Teknol. Inf.* **7** 32–44

[9] Khafif F 2021 Peningkatan Pelayanan Internet Menggunakan Mikrotik Dan Software Winbox Di Ptipd Uin Walisongo Semarang *3rd Natl. Semin. Marit. Interdiscip. Stud.* **3** 3–6

[10] Ardiyanto Y 2022 Portabel Intrusion Prevention System Untuk Mengamankan Koneksi Internet Saat

ISSN : 2548 – 8112 eISSN: 2622-8890

Menggunakan WiFi Publik *J. Sisfokom (Sistem Inf. dan Komputer)* **11** 107–13

[11] Arie Y 2014 Penggunaan Nmap Dan Hping 3 Dalam Menganalisa

[12] Luthfansa Z M and Rosiani U D 2021 Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet *J. Inf. Eng. Educ. Technol.* **5** 34–9

[13] Jaringan T, Arsadi A A and Haryatmi E 2021 InfoTekJar : Jurnal Nasional Informatika dan Pemanfaatan Aplikasi Telegram dan Internet of Things pada Pemantauan Tempat Sampah **2**

[14] Rivai F R, Rendy M M T and Sunarya U 2018 ANALISIS DAN IMPLEMENTASI PROTOTIPE PENGATUR KELEMBABAN BERBASIS INTERNET OF THINGS (IoT) PADA PENYIMPANAN SAYUR Analysis and Implementation Prototype of Controlling Humidity based Internet of Things (IoT) on Vegetable Storage *e-Proceeding Eng.* **5** 4366