JITE, 7 (1) July 2023 ISSN 2549-6247 (Print) ISSN 2549-6255 (Online)

JITE (Journal of Informatics and Telecommunication Engineering)

Available online http://ojs.uma.ac.id/index.php/jite **DOI : 10.31289/jite.v7i1.9674**

Received: 02 June 2023	Accepted: 26 June 2023	Published: 28 July 2023

Design and Build a Network Security System Using Port Knocking, DMZ and IDS Techniques at SMA Negeri 1 Warungkiara

Somantri1)*, Gina Purnama Insany2), & Rahman Zulkarnaen3)

1,2,3)Teknik Informatika, Fakultas Teknik Komputer dan Desain, Universitas Nusa Putra, Indonesia

*Coresponding Email:somantri@nusaputra.ac.id

Abstrak

Sistem keamanan jaringan penting dalam menjaga kerahasiaan, dan aksesibilitas komputer. SMA Negeri 1 Warungkiara menggunakan filterrule sebagai sistem keamanan jaringan. Sistem ini berfungsi memblokir situs berbahaya. Namun, sistem ini kurang dalam melindungi server dari serangan hacker. Oleh karena itu, diperlukan sistem keamanan seperti Port Knocking, DMZ, dan IDS untuk mengatasi serangan tersebut. Teknik Port Knocking digunakan sebagai metode autentikasi yang memungkinkan akses ke jaringan setelah port yang ditentukan diketuk. DMZ digunakan untuk mengisolasi jaringan internal dari jaringan eksternal. IDS digunakan untuk mendeteksi aktivitas mencurigakan. Dalam pengembanganya menggunakan metode NDLC yang dikhususkan untuk sistem jaringan. Sistem keamanan diuji menggunakan serangan seperti port scanning, sniffing, DDoS attack, dan Ping of Death. Pengujian port knocking menunjukkan bahwa port tidak terdeteksi (tertutup), DMZ berhasil mengurangi penggunaan sumber daya server dari 34% menjadi 6% saat diuji dengan DDoS attack, dan IDS dapat mengidentifikasi serangan pada server dan router. Sistem keamanan ini memberikan perlindungan terhadap ancaman keamanan jaringan dan membantu menjaga integritas data di jaringan sekolah. Dengan penerapan teknik keamanan seperti Port Knocking, DMZ, dan IDS, SMA Negeri 1 Warungkiara telah berhasil membangun sistem keamanan jaringan yang efektif.

Kata Kunci: Port Knocking, Demilitarized Zone (DMZ), Intrusion Detection System (IDS), Network Development Life Cycle (NDLC)

Abstract

Network security is essential in safeguarding the confidentiality and accessibility of computer systems. SMA Negeri 1 Warungkiara utilizes a filter rule as its network security system to block harmful websites. However, this system falls short in protecting the server from hacker attacks. Therefore, additional security measures like Port Knocking, DMZ, and IDS are necessary to address these threats. Port Knocking is used as an authentication method that allows network access only after a specific sequence of ports is knocked. DMZ is employed to isolate the internal network from external networks, providing an added layer of protection. IDS is utilized to detect suspicious activities within the network. In its development, the NDLC method specialized for network systems is employed. The security system undergoes testing with attacks such as port scanning, sniffing, DDoS attacks, and Ping of Death. The port knocking test indicates that ports remain undetected (closed). The implementation of DMZ successfully reduces server resource usage from 34% to 6% during DDoS attack tests, and IDS effectively identifies attacks on the server and router. This comprehensive security approach ensures protection against network security threats and helps maintain data integrity within the school's network. By implementing techniques like Port Knocking, DMZ, and IDS, SMA Negeri 1 Warungkiara has successfully built an effective network security system..

Keywords: Port Knocking, Demilitarized Zone (DMZ), Intrusion Detection System (IDS), Network Development Life Cycle (NDLC)

How to Cite: Somantri, S., Insany, G. P., & Zulkarnaen, R. (2023). Design and Build a Network Security System Using Port Knocking, DMZ and IDS Techniques at SMA Negeri 1 Warungkiara. JITE *(Journal of Informatics and Telecommunication Engineering)*, 7(1), 292-307.

I. PENDAHULUAN

Keamanan jaringan sangat penting dalam era digital saat ini, dimana jaringan komputer telah menjadi bagian integral dari kehidupan sehari-hari dan berbagai transaksi bisnis kita semua maupun pemerintahan

dilakukan melalui jaringan. Keamanan jaringan memainkan peran yang penting dalam menjaga integritas, privasi, dan keamanan data yang disimpan dan diteruskan melalui jaringan.(Munawar et al., 2020)

Masalah keamanan jaringan yang sering terjadi, seperti hacking, phishing, malware, dan serangan DDoS, memiliki potensi merusak sistem dan mengambil informasi sensitif. Oleh sebab itu, penting sekali untuk memastikan bahwa jaringan dapat dilindungi dari ancaman keamanan yang mungkin muncul. Serangan Denial of Service (DoS) adalah salah satu jenis serangan yang sering menargetkan jaringan komputer (Dar & Harahap, 2017). Serangan DoS dilakukan dengan menghabiskan sumber daya seperti Unit Pemrosesan Kontrol, bandwidth memori, dan ruang disk untuk menghalangi atau membahayakan pengguna yang berwenang menggunakan jaringan, sistem, atau aplikasi(Bustami & Bahri, 2020).

Dampak dari keamanan jaringan yang lemah atau tidak dilindungi dengan baik dapat terjadinya kebocoran data pribadi, rahasia bisnis. dan data penting lainnya yang dapat merugikan secara financial baik perorangan maupun organisasi. Sistem keamanan jaringan yang lemah juga dapat mengakibatkan menyebabkan downtime sistem, yang mempengaruhi produktivitas dan efisiensi bisnis(Durand et al., 2019).

Untuk menghindari dampak buruk seperti yang diuraikan diatas, penelitian ini akan menggunakan beberapa cara diantaranya port knocking yaitu menutup semua port yang ada, dan hanya user tertentu saja yang dapat mengakses sebuah port yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu (Chandra et al., 2021). Yang kedua dengan teknik keamanan jaringan DMZ (Demilitarized Zone), yang merupakan mekanisme untuk melindungi sistem internal dengan menggunakan filter menolak pihak-pihak yang ingin memasuki sistem tanpa hak akses(Komang et al., 2020). Yang ketiga yaitu Jaringan komputer yang terhubung secara bersamaan ke jaringan lokal dan internet dapat menggunakan sistem deteksi intrusi (IDS) untuk mengidentifikasi serangan dan ancaman(Nurdadyansyah & Hasibuan, 2021). Administrator jaringan akan menerima pemberitahuan awal dari IDS ketika ada aktivitas mencurigakan (anomali) di jaringan komputer(Bayu Rendro & Nugroho Aji, 2020).

Di SMA Negeri 1 Warungkiara sendiri untuk masalah keamanan jaringan tergolong masih kurang memadai karena hanya mengandalkan sistem pembagian bandwidth dan juga mengandalkan firewall rule di keamanannya. Bersumber pada penelitian terdahulu, sehingga dalam penelitian ini penulis mengembangkan penelitian terdahulu yaitu sistem keamanan jaringan menggunakan teknik port knocking , DMZ dan IDS dengan tujuan terciptanya jaringan komputer yang optimal dan aman dari serangan-serangan hacker dengan menggunakan berbagai serangan pengujian mulai dari port scanning, sniffing dan DDoS attack sehingga diharapkan penelitian ini dapat memberikan keamanan jaringan pada sekolah atau tempat yang menggunakannya.

II. STUDI PUSTAKA

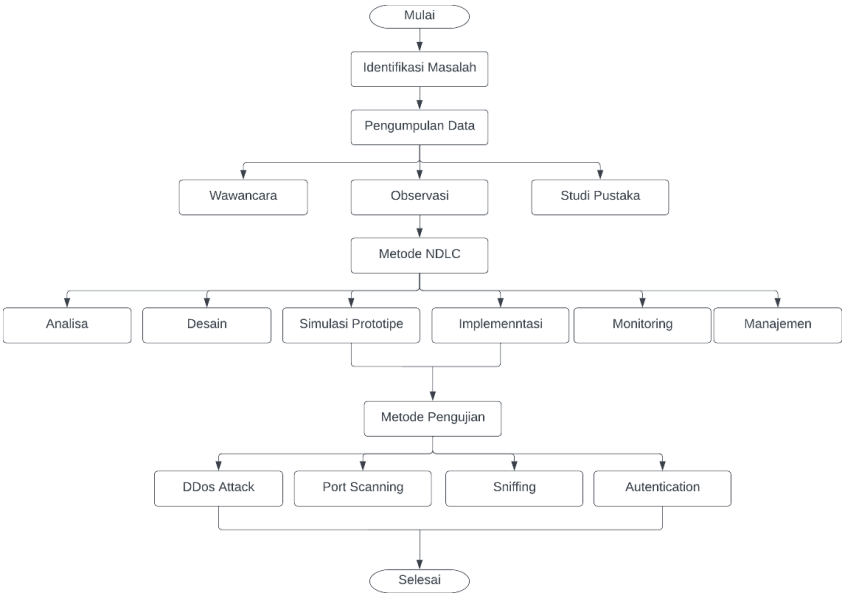
Beberapa penelitian terdahulu mengenai penerapan sistem keamanan yang digunakan penulis sebagai bahan referensi yaitu penelitian yang dilakukan oleh Yudi Mulyanto , M. Julkarnain, Aldela Jabi Afahar pada tahun 2021, pada penelitian ini Implementasi Port Knocking Untuk Keamanan Jaringan SMKN 1 Sumbawa Besar dengan kesimpulan bahwa port knocking sudah berjalan sebagaimana mestinya akan tetapi ketika terjadi sebuah serangan DDoS maka sistem keamanan tersebut tidak dapat menangani sehingga server menjadi down(Quroturohman, 2020) Penelitian yang dilakukan M. Agus Syamsul Arifin dan Antoni Zulius pada tahun 2019 pada penelitian ini sistem keamanan yang diterapkan yaitu sistem keamanan DMZ dengan kesimpulan bahwa penelitian ini menggunakan metode Network Development Life Cycle. Metode serangan yang dijalankan yaitu melakukan ping of death kepada ip server dan ketika terjadi serangan Port Scanning sistem ini tidak dapat melakukan Tindakan atas serangan tersebut(Agus et al., 2019) Penelitian yang dilakukan oleh Dian Novianto, Lukas Tommy, Yohanes Setiawan Japriadi pada tahun 2021 pada penelitian ini mendapatkan kesimpulan pada penelitian Dian dkk menggunakan packet tracer dalam melakukan simulasi nya serta menggunakan metode PPDIOO dalam proses pengembangannya dan hasil yang didapatkan sesuai dengan prinsip dari Port Knocking. Uji coba seranganya menggunakan port scanning dan port tertutup sesuai yang diharapkan akan tetapi ketika melakukan serangan DDos sistem tidak dapat menindak lanjuti serangan tersebut(Pratiwi et al., 2020). Penelitian yang dilakukan oleh Rennie deGraaf, John Aycock, and Michael Jacobson pada tahun 2019 pada penelitian ini mendapatkan kesimpulan bahwa penelitian ini menggunakan Linux Server dan port knocking nya sendiri dijalankan di sisi server, penulis sendiri memberikan 3 port untuk melakukan knock nya karena tiap port mempunyai fungsi nya masing masing dan diberikan ke orang yang memegang bagian port nya tersebut oleh sebab itu sistem pada linux hanya dapat mengantisipasi serangan yang berkaitan dengan scanning port(Degraaf et al., 2019). Penelitian

yang dilakukan oleh Alfin dan Habil pada tahun 2019 penelitian ini menggunakan Firewall Filter yang artinya penulis membuat sebuah rule dimana jaringan public yang mengakses router akan di cek apakah masuk kedalam jaringan local jika masuk maka akan diizinkan sedangkan jaringan yang sudah pasti terdaftar yaitu jaringan laboratorium maka akan diizinkan karena jaringan lab sudah di masukkan ke dalam ACL(Alfin & Habil, 2019).

III. METODE PENELITIAN

A. Diagram Alir Penelitian

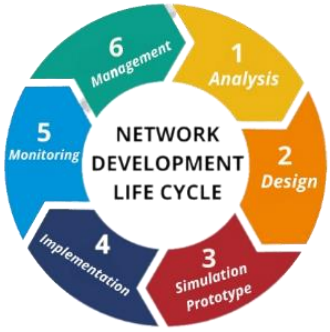
Pada awal penelitian ini dilakukan analisis pada jaringan yang sebelumnya sudah diterapkan di SMA Negeri 1 Warungkiara hasil analisis tersebut akan digunakan untuk membangun topologi jaringan yang sesuai dengan konsep keamanan yang akan di bangun. Tahapan penelitian ini ditunjukan pada Gambar 1 berikut :



Gambar 1. Diagram Alir Penelitian

B. Pengambangan Sistem

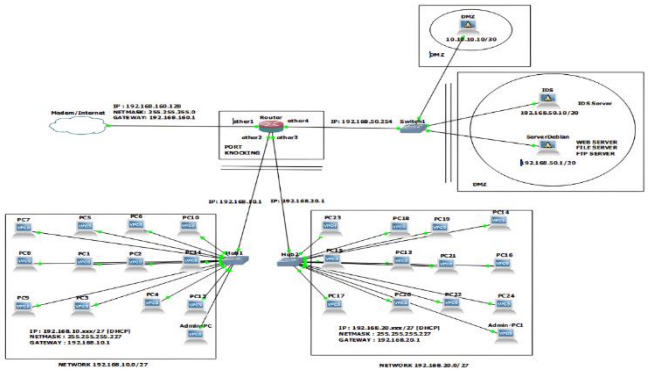
Dalam pengembangan sistem penulis menggunakan metode Network Development Life Cycle (NDLC). NDLC merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan (Anugrah & Rahmanto, 2018). NDLC merupakan salah satu komponen dari sejumlah komponen lainnya. Dengan demikian NDLC hanya dapat dilaksanakan apabila proses sebelumnya sudah selesai dikerjakan seperti melakukan analisis, design, dan analisis pengumpulan data.



Gambar 2. Alur pengembangan Sistem

C. Perancangan Topologi Jaringan

Dalam pengembangan topologi jaringan penulis menggunaakan *software* GNS3. Topologi yang digunakan dalam membangun sistem keamanan ini yaitu menggunakan topologi star dimana dalam topologi star tersebut menggunakan 2 buah hub sebagai penghubung antar jaringan. Adapun kelebihan topologi Star adalah lebih hemat biaya untuk kabel jaringan. Kemudian, kegagalan pengiriman data pada satu rute tidak akan mempengaruhi rute yang lain.



Gambar 3. Topologi Jaringan

D. Pengalokasian IP Address

Dalam membuat daftar kebutuhan IP *Address* penulis menggunakan bantuan *software* GNS3 dari topologi yang sebelumnya dibuat. IP *Address* sangat penting karena agak komputer klien dapat terhubung ke internet dan juga server. Berikut merupkan pengalokasian IP Address yang ditunjukkan pada Tabel 1 :

Tabel 1. Pengalokasian IP *Address*

No.	Penggunaan	IP Address
1	Router Ether1 / IP Modem	192.168.160.128/24
2	Server Web	192.168.50.1/30
3	Server DMZ	10.10.10.10/30
4	Network LAB 1	192.168.10.0/27
5	Network LAB 2	192.168.20.0/27
6	Router Ether2	192.168.10.1/27
7	Router Ether3	192.168.20.1/27
8	Router Ether4	192.168.50.254/30

E. Kebutuhan Hardware

Kebutuhan hardware ini digunakan dalam membangun membangun topologi jaringan sesuai dengan yang dirancang oleh penulis berikut merupakan tabel kebutuhan hardware :

Tabel 2. Kebutuhan *Hardware*

No.	Jenis Perangkat	Spesifikasi	Jumlah (pcs)
1	PC/Komputer	Dell AIO 22 inc 4 GB RAM 256 SSD	45
2	Router	Mikrotik RB750G 5 Port Ether	1
3	Hub/Switch	TP-LINK TL-SG1024D 24 Port	2
4	Server	Intel Core – i7 gen 10 8GB RAM	1

		256 SSD	

F. *Kebutuhan Sofware*

Software adalah merupakan suatu program komputer yang berfungsi untuk melakukan tugasnya masing masing. Dalam penelitian ini berikut merupakan software yang digunakan adalah :

Tabel 3. Kebutuhan *Software*

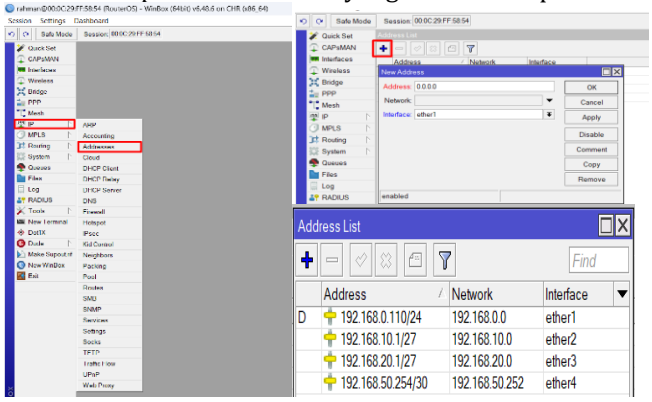
No.	Nama	Spesifikasi	Keterangan
1	Sistem Operasi Klien	Windows 11 Home	Sistem Operasi
2	Sistem Operasi Server	Ubuntu 11 Bullseye	- Web Server (Apache2) - File Server (FTP)
3	Browser	Chrome 113.0.5672.127	*Sofware* untuk browsing
4	Winbox	Winbox 6.42.1	Remote Router
5	Virtual Machine	VMWare 16	Simulasi jaringan
6	Nmap	Nmap v7.93	Tester Tool
7	Wireshark	Wireshark v4.0.3	Tester Tool
8	SSH Client	Putty 64bit- 0.78	Remote SSH

G. *Konfigurasi Sistem Keamanan Jaringan*

Pada tahap Implementasi sistem ini dibuat sebuah sistem keamanan menggunakan topologi yang dirancang sebelumnya. Berikut merupakan implementasi yang dilakukan :

1. Konfigurasi IP Address Pada Router

   Setiap perangkat yang terhubung ke internet memiliki alamat IP, yang merupakan rangkaian angka. Di jaringan internet, perangkat yang berbeda menggunakan kumpulan angka yang berbeda untuk berkomunikasi satu sama lain. Pada tahap ini akan dilakukan pembuatan IP Address untuk keperluan jaringan internet di lokasi penelitian, pembuatan IP Addres ini menggunakan software winbox untuk koneksi ke router nya berikut merupakan IP Address yang dibuat oleh penulis :



Gambar 4. Penggunaan IP Address

Pada Gambar 4 merupakan penggunaan IP Address pada router mikrotik berikut merupakan list penggunaan IP Address yang penulis gunakan :

Tabel 4. IP Address Pada Router

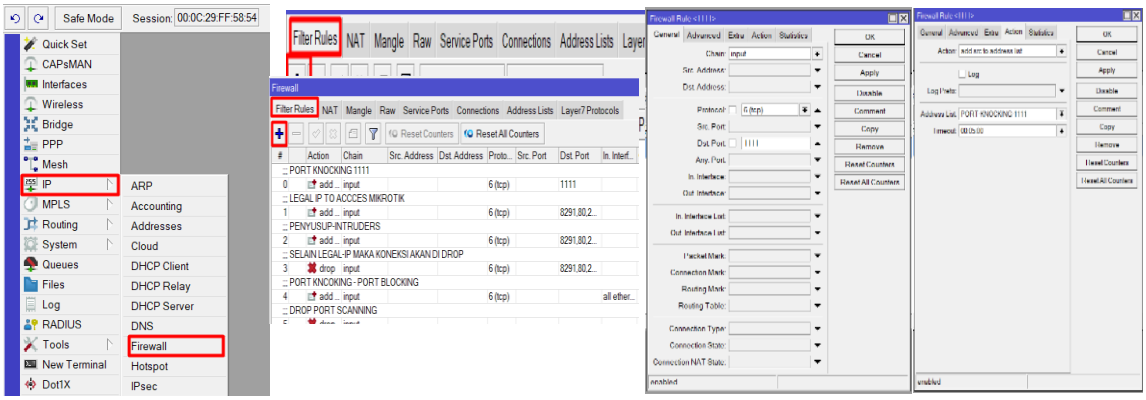
No.	Penggunaan	Interfaces	IP Address
1	IP Internet/Modem	Ether1	192.168.122.240/24
2	Router Ether2 / Gateway LAB1	Ether2	192.168.10.1/27
3	Router Ether3 / Gateway LAB2	Ether3	192.168.20.1/27

No.	Penggunaan	Interfaces	IP Address
4	Router Ether4	Ether4	192.168.50.254/30

Pada Tabel 4 merupakan semua IP Address yang penulis gunakan, untuk penggunaan IP Address pada LAB 1 nantinya akan menghasilkan IP: 192.168.10.xx (1-253) begitupun dengan LAB 2 dan untuk DNS nya sendiri akan menggunakan IP Server tetapi akan menggunakan teknik DMZ sehingga IP Gateway 192.168.10.1 akan dijadikan sebagai pengalihan ke lokasi IP server.

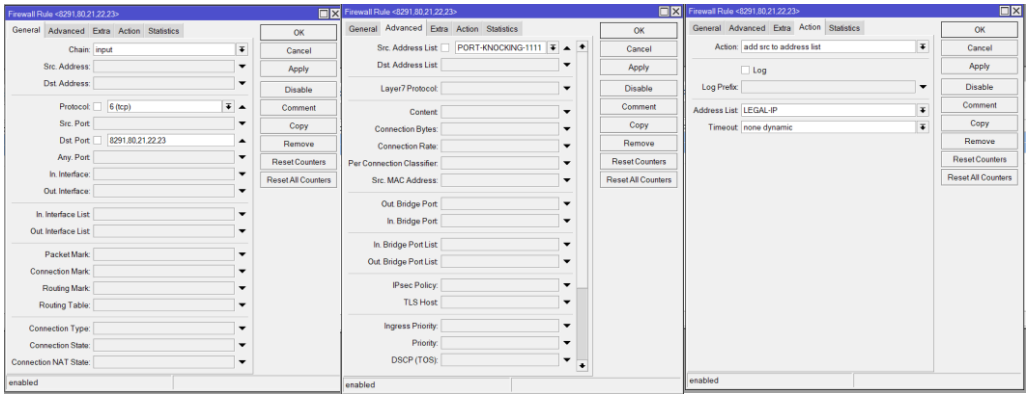
2. Konfigurasi Port Knocking Pada Router

Teknik keamanan pertama yang akan dipakai oleh penulis adalah teknik port knocking. Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah di blok oleh firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupuan ICMP. Berikut merupakan hasil konfigurasi yang telah penulis buat



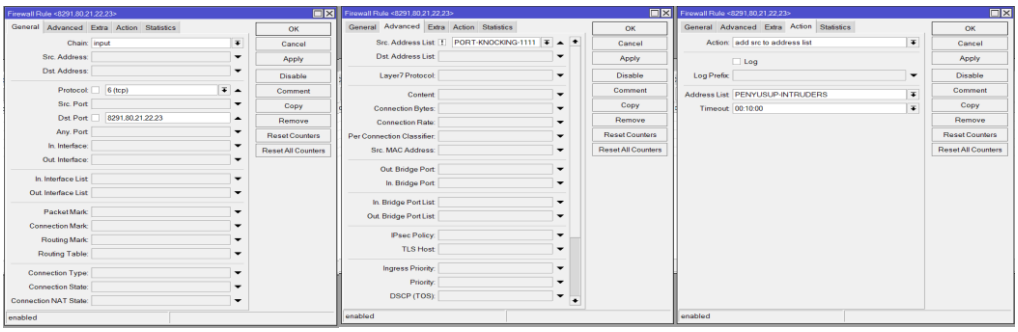
Gambar 5. Konfigurasi Port Knocking Tahap 1

Konfigurasi pada Gambar 5 adalah jika ada yang ingin melakukan akses ke router dari IP manapun menggunakan protokol tcp dan menggunakan Port 1111 maka IP yang melakukan knocking tadi akan disimpan ke dalam address list dengan nama “PORT-KNOCKING-1111” dan address list tersebut akan dihapus setiap 5 menit sekali. Konfigurasi selanjutnya adalah membuat legal IP Address.



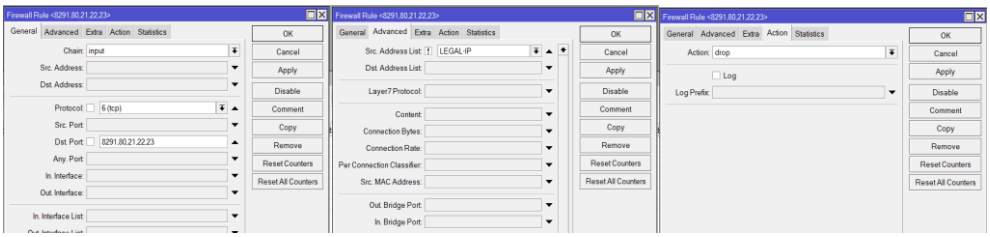
Gambar 6. Konfigurasi Port Knocking Tahap 2

Pada konfigurasi Gambar 6 tersebut dimaksudkan jika ada yang melakukan koneksi ke port 8291(winbox), 80(webfix), 21(ftp), 22(ssh), 23(telnet) menggunakan protokol tcp dan IP yang melakukan koneksi tadi akan dilihat terlebih dahulu apakah sudah melakukan port knocking(terdaftar di address list PORT-KNOCKING-1111) jika IP tersebut sudah terdaftar ke Src. Address list PORT-KNOCKING-111 maka akan dimasukkan ke dalam Src. Address list LEGAL-IP dan IP tersebut akan diberi akses ke Port yang telah disebutkan diatas. Selanjutnya akan melakukan konfigurasi untuk Penyusup/Intruder adalah sebagai berikut :



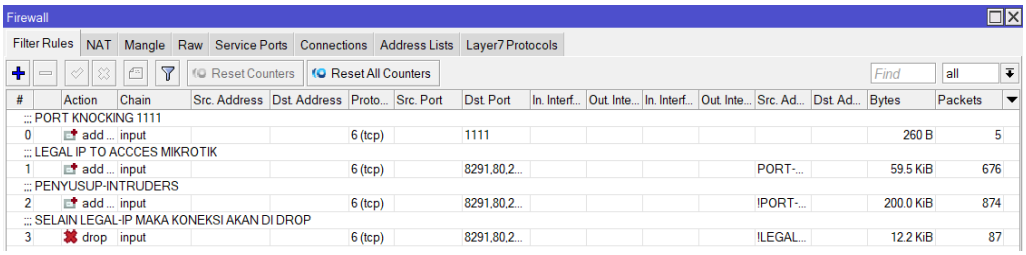
Gambar 7. Konfigurasi Port Knocking Tahap 3

Pada konfigurasi yang ditunjukan pada Gambar 7 dimaksudkan jika ada yang melakukan koneksi ke port 8291(winbox), 80(webfix), 21(ftp), 22(ssh), 23(telnet) menggunakan protokol tcp dan IP yang melakukan koneksi tadi bukan dari Src. Address list PORT-KNOCKING-1111 maka IP yang melakukan koneksi tersebut akan dimasukkan kedalam Src. Address list PENYUSUP/INTRUDERS dan Src. Address tersebut akan di hapus setiap 10 menit sekali sehingga tidak membebani memori dari router yang dipakai. Setelah Konfigurasi ini maka selanjutnya akan membuat konfigurasi untuk melakukan drop koneksi jika ada penyusup yang mencoba untuk masuk ke router kita berikut merupakan konfigurasinya:



Gambar 8. Konfigurasi Port Knocking Tahap 4

Untuk Konfigurasi pada Gambar 8 ini dimaksudkan jika ada yang melakukan koneksi ke port 8291(winbox), 80(webfix), 21(ftp), 22(ssh), 23(telnet) menggunakan protocol tcp selain IP Address yang ada di Src. Address LEGAL-IP maka koneksi pada IP tersebut akan ditolak karena IP tersebut dianggap penyusup/intruder. Berikut merupakan semua konfigurasi yang telah dibuat sebelumnya :

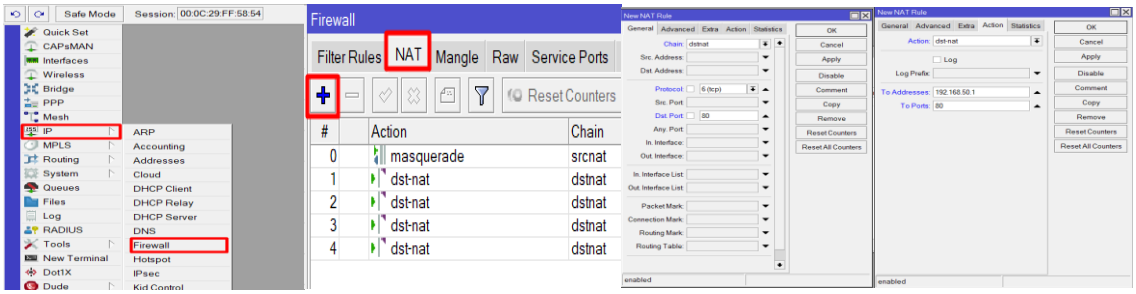


Gambar 9. Hasil Konfigurasi Port Knocking

Hasil konfigurasi port knocking dapat dilihat pada Gambar 9. Terdapat 4 konfigurasi diantaranya : 1. Membuat port untuk port knocking nya sendiri, 2. Membuat legal IP untuk akses ke mikrotik kita, 3. Membuat rule untuk penyusup/intruder, dan terakhir ke 4. Membuat drop koneksi jika ada ip yang bukan legal ip mencoba untuk akses ke router .

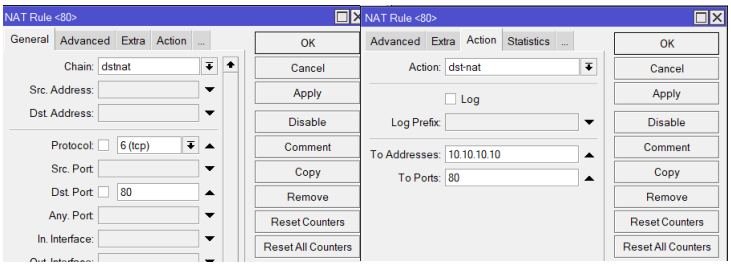
3. Konfigurasi Demilitarized Zone Pada Router

Teknik keamanan selanjutnya yang akan kita pakai adalah Demilitarized Zone (DMZ), DMZ atau zona demiliterisasi, adalah sebuah keamanan firewall yang memisahkan jaringan area lokal (LAN) dari jaringan tidak terpercaya biasanya, internet publik. Jadi keamanan DMZ sendiri adalah untuk mengamankan jaringan lokal yang dianggap penting seperti Server dan data pribadi lainnya. Berikut merupakan hasil konfigurasi yang penulis buat untuk keamanan DMZ ditunjukkan pada Gambar 10 :



Gambar 10. Konfigurasi DMZ Tahap 1

Konfigurasi pada Gambar 10 merupakan konfigurasi untuk teknik keamanan Demilitarized Zone logikanya sendiri cukup mudah di pahami jika ada yang mencoba akses ke ip router (baik eth0, eth1, eth2 dst) dan melalui protokol tcp serta menggunakan port 80 (webfix) maka paket tersebut akan diteruskan ke ip server dengan ip 192.168.50.1. Jadi jika mencoba untuk akses ke ip gateway baik yang berada di LAB 1 maupun LAB 2 maka akan dialihkan ke IP server yang telah di install webserver. Selanjutnya membuat rule baru yang ditunjukkan pada Gambar 11:

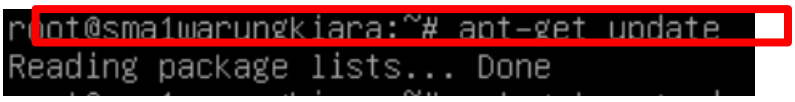


Gambar 11. Konfigurasi DMZ Tahap 2

Pada Gambar 11 ini merupakan konfirgurasi yang berguna jika ada yang menyerang server dengan alamat IP 192.168.50.1 maka ip tersebut akan dialihkan ke area DMZ yang mempunyai IP 10.10.10.10 maka dengan ini server tidak akan terbebani jika terjadi sebuah serangan.

4. Konfigurasi Instrusion Detection System Pada *Server*

Teknik keamanan terakhir yang akan penulis terapkan adalah teknik Intrusion Detection System (IDS). IDS adalah sebuah sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan. Jika aktivitas mencurigakan tersebut ditemukan, IDS akan melaporkannya dalam bentuk peringatan. Dengan kata lain, IDS bisa dibilang sebagai perangkat lunak pemindai sistem atau jaringan guna terhindar dari kegiatan yang melanggar kebijakan. Berikut merupakan hasil konfigurasi yang penulis terapkan pada server web yang menggunakan Debian 11 :

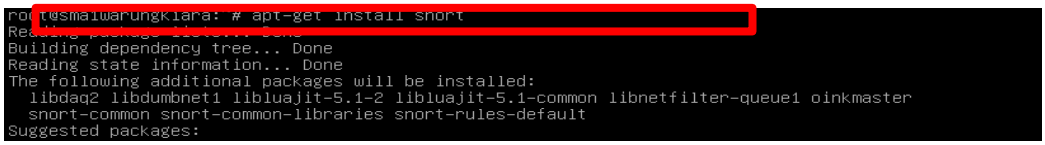


Gambar 12. Perintah apt-get update

Gambar 12 adalah perintah “apt-get update” yang berfungsi untuk memperbarui daftar paket yang ada di sistem linux kita, daftar paket yang di perbaharui tidak hanya paket-paket yang lama saja tapi juga paket yang baru saja datang ke repositori. Setelah itu akan dilanjutkan ke perintah apt-get upgrade yang ditunjukkan pada Gambar 12:

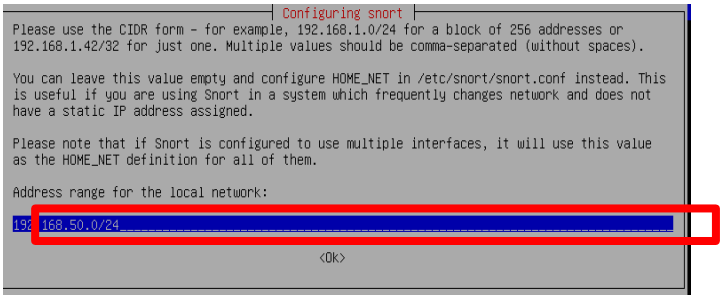
Gambar 13. Perintah apt-get update

Perintah “apt-get upgrade” berfungsi untuk menginstall paket-paket yang ada di dalam repositori ke versi terbaru, paket yang sudah terhapus direpositori tidak akan di upgrade, cara kerja upgrade, biasanya dia akan menghapus terlebih dahulu paket-paket yang sudah terinstall pada sistem linux, kemudian akan mengambil paket-paket terbaru dari repositori yang sudah kita update. Sama seperti sudo apt-get update, sudo apt get-upgrade hanya dapat dijalankan sistem root, jika belum masuk ke sistem root, maka tidak akan upgrade linux. Selanjutkan menginstall Snort yaitu sebuah tool untuk menjalankan Intrusion Detection System (IDS) yang ditunjukkan pada Gambar 14:



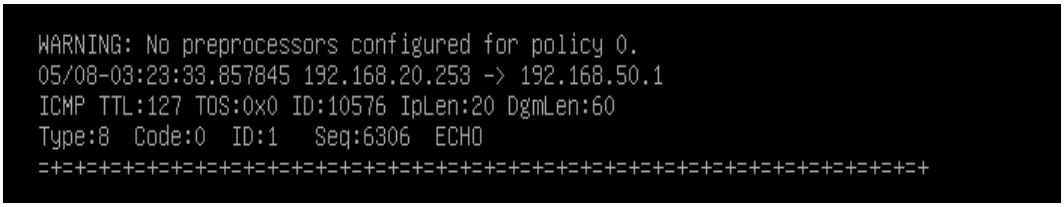
Gambar 14. Perintah Untuk Menginstall Snort

Pada Gambar 14 adalah cara untuk dapat menginstall Snort agar dapat dapat memonitoring jaringan tentu perlu menginstalnya terlebih dahulu dengan perintah apt-get install snort perintah ini akan mendownload dan memasangkan snort ke server yang kita kita buat sebelumnya. Selanjutnya kita akan melakukan konfigurasi pada snort nya:



Gambar 15. Setting IP Pada Snort

Pada Gambar 15 diminta untuk memasukkan IP Address untuk keperluan snort nantinya IP nya sendiri harus menggunakan IP Server karena agar dapat melakukan monitoring jaringannya.



Gambar 16. Hasil Uji Coba Snort

Pada Gambar 16 dapat kita lihat bahwa ip 192.168.20.253 sedang melakukan ping dengan jumlah yang tidak wajar dan snort berhasil mendeteksi Tindakan tersebut karena menganggap bahwa ping yang dilakukan oleh ip tersebut terlihat tidak wajar.

H. Skenario Pengujian

Skenario pengujian yang dilakukan oleh peneliti adalah sebuah serangan-serangan yang ditargetkan kepada *server* maupun router. Berikut merupakan *point of view scenario* pengujian yaitu (a) Melakukan serangan *port scanning, sniffing* dan pengujian *authentication* kepada keamanan *Port Knocking* sebelum dan sesudah keamanan *Port Knoking* di aktifkan; (b) Melakukan serangan *DDos Attack* kepada keamanan *Demilitazed Zone* (DMZ) sebelum dan sesudah keamanan diaktifkan; (c) Melakukan serangan *DDos* dan *Ping of death* kepada *server* dengan dan tanpa penerapan sistem keamanan *Intrusion Detection System* (IDS).

IV. HASIL DAN PEMBAHASAN

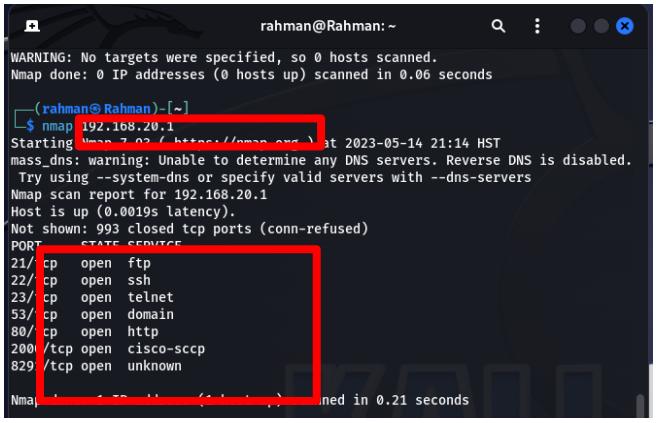
Penelitian yang dilakukan penulis diatas diimplementasikan di sekolah SMA Negeri 1 Warungkiara. Setelah proses konfigurasi selesai maka selanjutnya adalah proses pengujian. Pada proses pengujian ini menggunakan beberapa *software* bantuan seperti *nmap, wireshark, hping3* dan sistem operasi Kali Linux. Berikut merupakan hasil pengujian yang penulis lakukan dalam penelitian ini :

A. Pengujian Sistem Keamanan Port Scanning

Pada pengujian port knocking ini akan menggunakan serangan Port Scanning dan Sniffing, dalam serangannya sendiri akan menggunakan sistem operasi kali linux dan menggunakan software nmap serta wireshark berikut hasil serangannya :

1. Pengujian *Port Scanning* Mode *Disable*

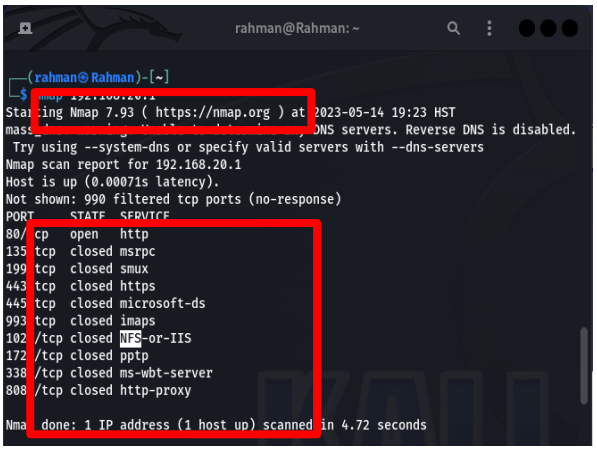
Pada titik ini, pemindaian dilakukan dalam keadaan jaringan standar (mekanisme port knocking belum diterapkan). Pemeriksaan Router pada alamat (192.168.20.1/27). Port jaringan masih dapat dibaca dan dipindai dalam mode biasa, ditemukan berdasarkan temuan pemindaian. Gambar 17 menampilkan hasil scan:



Gambar 17. Pengujian Port Scanning Mode Disable

2. Pengujian *Port Scanning* Mode *Enable*

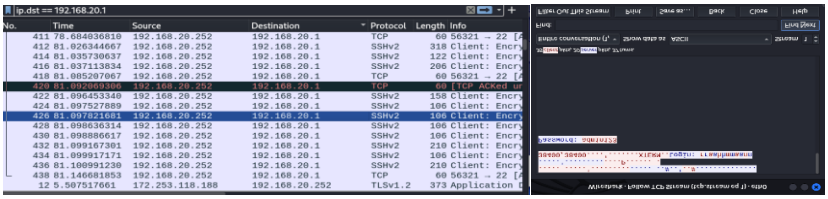
Berdasarkan hasil scanning yang dilakukan pada tahap ini didapatkan hasil bahwa port yang ada pada jaringan pada mode disable tidak bisa discan (tidak terbaca) kecuali port 80(webfix) karena akan menggunakan untuk keamanan Demilitarized Zone. Adapun hasil scanning bisa dilihat pada Gambar 18.



Gambar 18. Pengujian Port Scanning Mode Enable

3. Pengujian *Sniffing* Mode *Disable*

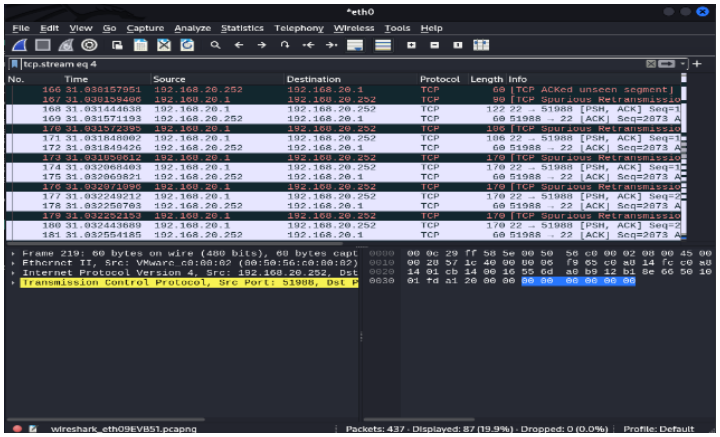
Hasil pengujian mode sniffer menunjukkan bahwa router tidak bisa diakses melalui winbox (8291) atau webfix (80). Namun ternyata username dan password yang digunakan untuk masuk ke router masih dapat disadap dan tidak dienkripsi pada login telnet, oleh karena itu penyadapan relatif mudah ketika router diakses menggunakan Telnet (23). Gambar 19 menunjukkan hasil dari sniffing:



Gambar 19. Pengujian Sniffing Mode Disable

4. Pengujian *Sniffing* Mode *Enable*

Hasil pengujian sniffing mode enable menunjukkan bahwa baik username maupun password tidak dapat di-capture ketika router diakses melalui winbox (8291), telnet (23), atau webfix (80), dan terenkripsi sehingga sulit untuk membaca paket yang lewat. Gambar 20 menampilkan hasil dari sniffing menggunakan winbox, telnet, dan webfig.



Gambar 20. Pengujian Sniffing Mode Enable

Tabel 5. Hasil Pengujian *Port Knocking*

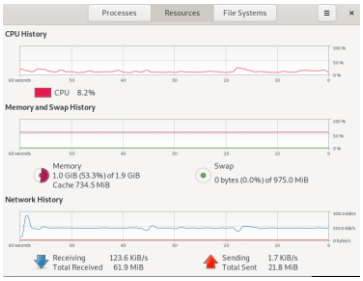
No.	Mode	Target	Jenis Pengujian	Alat Uji (*tools*)	Hasil Pengujian
1.	Mode Disable	192.168.20.1	*Scanning*	Nmap	*Discovered open port*
2.	Mode Disable	192.168.20.1	*Sniffing*	Wireshark	Terenkripsi, kecuali Telnet.
3.	Mode Disable	192.168.20.1	*Authentication*	Winbox, Putty, Chrome	Berhasil login
4.	Mode Enable	192.168.20.1	*Scanning*	Nmap	Port Disable, hanya port webfix(80) saja yang open port
5.	Mode Enable	192.168.20.1	*Sniffing*	Wireshark	Terenkripsi.
6.	Mode Enable	192.168.20.1	*Authentication*	Winbox, Putty, Chrome	Gagal Login

B. Pengujian Sistem Keamanan Demilitarized Zone

Pada pengujian sistem keamanan Demilitarized Zone ini akan menggunakan serangan *DDos Attack* dalam serangannya sendiri akan menggunakan sistem operasi kali linux dan menggunakan tools *hping3* serangannya :

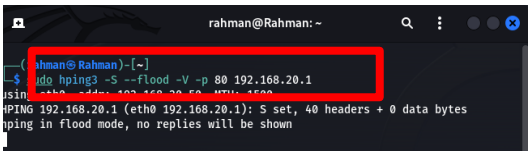
1. Pengujian *DDoS Attack* Mode *Disable*

Pada tahap ini dilakukan serangan berupa DDoS attack dengan tipe serangan seperti HTTP Flooding tanpa menerapkan sistem keamanan yang telah dibuat sebelumnya ditunjukan pada Gambar 21 berikut



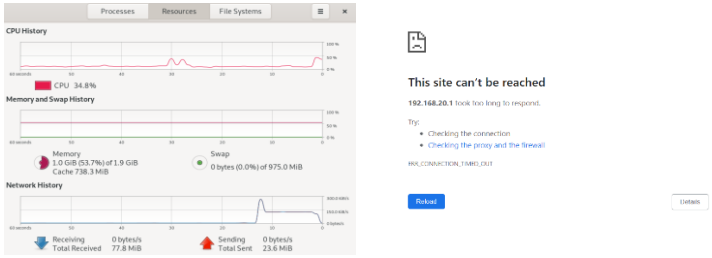
Gambar 21. *Resources* Sebelum Serangan

Pada Gambar 21 merupakan resources jaringan normal tanpa adanya gangguan serangan pada jaringan, berikut merupakan serangan yang dilakukan terhadap keamanan jaringan:



Gambar 22. *DDoS Attack Mode Disable*

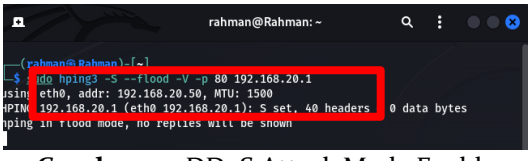
Pada Gambar 22 merupakan jenis serangan DDoS Attack menggunakan protokol dari HTTP atau web server serangan tersebut dilakukan kepada ip router yang memiliki IP Address 192.168.20.1 berikut merupakan hasil serangannya :



Gambar 23. Hasil Serangan DDoS Mode Disable

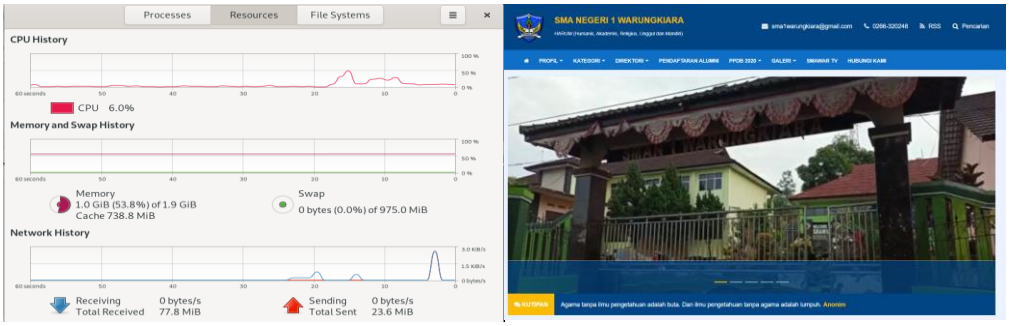
2. Pengujian *DDoS Attack* Mode *Enable*

Pada tahap ini dilakukan serangan berupa DDoS attack dengan tipe serangan seperti HTTP Flooding dengan menerapkan sistem keamanan yang telah dibuat sebelumnya ditunjukan pada Gambar 24 :



Gambar 24. DDoS Attack Mode Enable

Pada Gambar 24 merupakan jenis serangan DDoS Attack menggunakan protokol dari HTTP atau web server serangan tersebut dilakukan kepada ip router yang memiliki IP Address 192.168.20.1 dengan port 80 berikut merupakan hasil serangannya :



Gambar 25. Hasil Serangan *DDoS* Mode *Enable*

Tabel 6. Hasil Pengujian *DMZ*

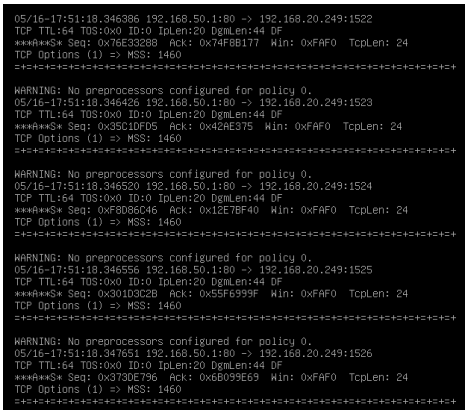
Metode Pengujian	Resources	
	CPU (%)	Bukti Gambar
DDoS Mode Disable	34%	Gambar 23
DDoS Mode Enable	6%	Gambar 25

C. Pengujian Sistem Keamanan Intrusion Detection System (IDS)

Pada pengujian sistem keamanan Intrusion Detection System (IDS) ini akan menggunakan serangan DDos Attack, serangannya sendiri akan menggunakan sistem operasi kali linux dan menggunakan tools hping3. Sistem Snort dapat dikonfigurasi menggunakan tiga mode utama yaitu sniffer dan packet logger dan NIDS:

1. Pengujian *Sniffer* Mode

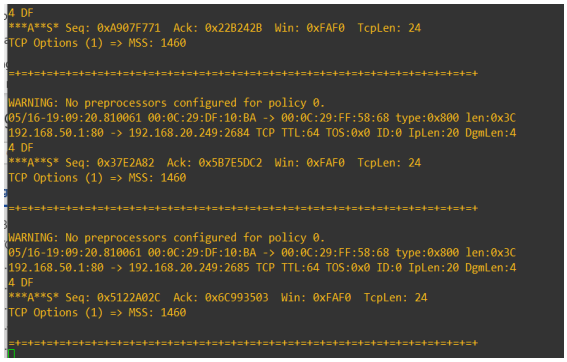
Pada tahap ini dilakukan serangan berupa DDoS attack dan Snort akan menggunakan mode sniffer yaitu membaca paket yang lewat dan menampilkannya ke layar. Berikut merupakan perintah untuk memulai snort mode sniffer ditunjukan pada Gambar 26:



Gambar 26. Hasil Serangan IDS mode *Sniffer*

2. Pengujian *Logger* Mode

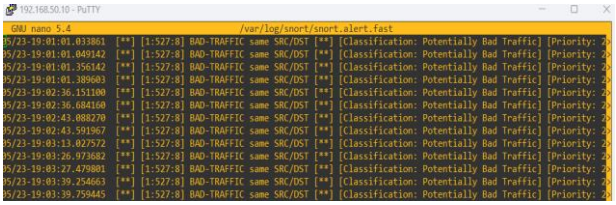
Pada tahap ini dilakukan serangan berupa DDoS attack dan Snort akan menggunakan mode logger yaitu membaca paket yang lewat dan menyimpannya ke dalam disk. Berikut merupakan cara menjalankan snort mode logger yang ditunjukan pada Gambar 27:



Gambar 27. Hasil Serangan IDS Mode Logger

3. Pengujian *Logger* Mode

Pada tahap ini dilakukan serangan berupa DDoS attack dan Snort akan menggunakan mode NIDS yaitu membaca paket yang lewat dan membandingkannya dengan rule yang telah dibuat. Berikut merupakan cara menjalankan snort mode NIDS yang ditunjukan pada Gambar 28:



Gambar 28. Hasil Serangan IDS Mode NIDS

V. SIMPULAN

Berdasarkan hasil penelitian dan setelah dilakukannya pengujian keamanan jaringan maka dapat disimpulkan bahwa sistem telah berjalan dengan baik dan seluruh sistem keamanan jaringan sudah bekerja. Hasil uji coba pada port knocking sesuai dengan yang seharusnya port-port yang ada pada router sudah berhasil dihilangkan pada saat terjadi serangan selanjutnya pada pengujian DMZ sudah dapat memblokir serangan serangan seperti DDOS Attack resources juga menjadi lebih aman karena dari mode disable ketika terjadi serangan memakan 34% dan ketika DMZ diterapkan hanya memakai 6% CPU. Sistem keamanan yang terakhir yaitu IDS pada pengujian dapat memakai tiga mode yaitu sniffer, logger dan NIDS pada IDS ini masih harus dikembangkan menjadi lebih sehingga IDS ini dapat diintegrasikan dengan Telegram sehingga akan memberikan notifikasi.

VI. UCAPAN TERIMAKASIH

Puji syukur kepada Allah SWT karena atas rahmat-Nya penulis dapat menyelesaikan penelitian ini. Terima kasih penulis juga ucapkan atas terlaksananya penelitian, kepada prodi Informatika Universitas Nusa Putra yang telah memberikan dukungan baik secara langsung maupun tidak langsung selama penelitian ini dilakukan, kepada pihak sekolah SMA Negeri 1 Warungkiara dan kepada pihak-pihak yang tidak dapat penulis sebutkan.

DAFTAR PUSTAKA

Agus, M., Arifin, S., & Zulius, A. (2019). PERANCANGAN SISTEM KEAMANAN JARINGAN PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ). In *Antoni Zulius STMIK MUSIRAWAS Lubuklinggau* (Vol. 4, Issue 1).

Alfin, & Habil. (2019). *Alfin,Habil,Keamanan Jaringan Dengan Firewall Fillter Berbasis Mikrotik Pada Laboratorium Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Alfin 1 , Habil 2 (Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning)*. https://osf.io/frd69/download

'Andik, S., 'Daniel, T., & 'Dwi, R. (2022). Implementasi Port Knocking Untuk Keamanan Jaringan Komputer Dengan Metode Demilitarized Zone. *Jurnal INFORMA*.

Anugrah, I., & Rahmanto, R. H. (2020). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *5*(2), 91–106. https://doi.org/10.33558/piksel.v5i2.271

Bayu Rendro, D., & Nugroho Aji, W. (2020). *ANALISIS MONITORING SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP (STUDI KASUS DI SMK NEGERI 1 KOTA SERANG)*. *7*(2).

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review. In *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK)* (Vol. 7, Issue 2).

Chandra, J., Hermanto, H., & Rahman, A. (2021). DETEKSI SERANGAN PORT SCANNING MENGGUNAKAN ALGORITMA NAIVE BAYES. *Julyxxxx*, *x, No.x*, 1–5.

Dar, M. H., & Harahap, S. Z. (2020). Implementasi Snort Intrusion Detection System (Ids) Pada Sistem Jaringan Komputer. *Jurnal Informatika*, *6*(3), 14–23. https://doi.org/10.36987/informatika.v6i3.1619

Dar, M. H., Harahap, S. Z., Sisteminformasi, D., Sains, F., & Teknologi, D. (2021). IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER. *Muhammad Halmi Dar*, *1*(3).

Degraaf, R., Aycock, J., & Jacobson, M. (2020). *Improved Port Knocking with Strong Authentication*. https://ieeexplore.ieee.org/abstract/document/1565272

Durand, G. M., Tooy, D., & Pakasi, S. E. (2021). *DESIGN AND DEVELOPMENT OF THE COCONUT INDUSTRIAL INFORMATION SYSTEM IN NORTH SULAWESI PROVINCE BASED ON WEB-GIS 1)*. http://industrikelapasulut.unaux.com/.

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037

Gani, A. G. (2019). *KONFIGURASI SISTEM KEAMANAN JARINGAN*.

Hidayat, A., Stekpi, J., & TMP Kalibata Jakarta Selatan, T. (2019). RANCANG BANGUN SISTEM INFORMASI PENYEWAAN LAHAN PARKIR BERBASIS WEB GIS. In *Jurnal Sistem Informasi dan Sains Teknologi* (Vol. 1, Issue 1).

Komang, I., Marta1, K. A., Nyoman, I., Hartawan2, B., Kadek, I., & Satwika3, S. (2020). ANALISIS SISTEM MONITORING KEAMANAN SERVER DENGAN SMS ALERT BERBASIS SNORT. *INSERT: Information System and Emerging Technology Journal*, *1*(1).

Luthfansa, Z. M., & Rosiani, U. D. (2021). *Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet*.

Mulyanto, Y., Julkarnain, M., & Afahar, A. J. (2021). IMPLEMENTASI PORT KNOCKING UNTUK KEAMANAN JARINGAN SMKN 1 SUMBAWA BESAR. In *JINTEKS* (Vol. 3, Issue 2).

Munawar, Z., Kom, M., & Putri, N. I. (2020). KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA. In *Jurnal Sistem Informasi-J-SIKA* (Vol. 02).

Novianto, D., Tommy, L., & Setiawan Japriadi, Y. (2021). Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router Implementasi Sistem Keamanan Jaringan Menggunakan Metode Simple Port Knocking Pada Router Berbasis Mikrotik. *JURNAL KOMITEK*, *1*(2), 407–417. https://doi.org/10.53697/jkomitek.v1i2

Nurdadyansyah, N., & Hasibuan, M. (2021). *Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah*.

Pratiwi, Alit, M., & Made, N. (2020). PERBANDINGAN DDOS ATTACK MENGGUNAKAN TOOLS LOIC, HOIC DAN HULK DALAM MELAKUKAN PENYERANGAN PADA SUATU WEBSITE. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, *4*(4), 467–471. http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/2190

Prisscilya, V., Santoso, T., Teknik Informatika, J., & Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta, S. (n.d.). *Prisscilya, implementasi keamanan jaringan menggunakan intrusion detection system (ids) pada pt. Mega esa farma 1 IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN INTRUSION DETECTION SYSTEM (IDS) PADA PT. MEGA ESA FARMA*.

Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*(Agustus), 143–158.

Quroturohman, D. (2020). PENETRATION TESTING DALAM FORENSIK DIGITAL PADA JARINGAN FAKULTAS TEKNIK UNIVERSITAS IBN KHALDUN BOGOR DENGAN PING OF DEATH. *IJCCS*, *x, No.x*, 1–5.

Riska, P., Sugiartawan, P., & Wiratama, I. (2021). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi Dan Komputer Terapan Indonesia (JSIKTI)*, *1*(2), 53–64. https://doi.org/10.33173/jsikti.12

Saputro, A., Saputro, N., & Wijayanto, H. (2020). *METODE DEMILITARIZED ZONE DAN PORT KNOCKING UNTUK KEAMANAN JARINGAN KOMPUTER* (Vol. 3, Issue 2).

Sistem Keamanan Jaringan Sman, P., Sutarti, C., Putranto Pancaro, A., & Isnanto Saputra, F. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM). *Jurnal PROSISKO*, *5*(1).

Suteja, E., Kumalasari, E. N., & Raharjo, S. (2021). *PERANCANGAN SISTEM KEAMANAN JARINGAN UNTUK MENGURANGI KEJAHATAN CYBER MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ) DAN FIREWALL RULES (Studi Kasus: Laboratorium Basis Data IST AKPRIND)* (Vol. 09, Issue 01).

Ulum, F. (2020). DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING. In *Jurnal TEKNOINFO* (Vol. 12, Issue 2).