TEKNOMATIKA, Vol.12, No.02, September 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X

Pemanfaatan Firewall Rule Base dan SSL dalam Penerapan Sistem Keamanan Jaringan

UTILIZATION OF FIREWALL RULE BASE AND SSL IN APPLICATION OF NETWORK SECURITY SYSTEM

Guntoro Barovih[1*], Muhammad Kholid Hidayat [2], Fahmi Ajismanto[3]

[1,2]S1 Informatika Institut Teknologi dan Bisnis PalComTech
[3]S1 Sistem Informasi Institut Teknologi dan Bisnis PalComTech
Jl. Basuki Rahmat No. 05, Palembang 30129, Indonesia
e-mail: guntoro@palcomtech.ac.id [1], kholidhidayat48@gmail.com [2], fahmi_ajismanto@palcomtech.ac.id[3]

Abstrak

Mengamankan informasi pada jaringan komputer merupakan bagian yang sangat penting dilakukan guna menjaga keaslian dan integritas informasi yang melintas. Penelitian ini bertujuan membangun mekanisme pengamanan informasi jaringan dengan cara melakukan mekanisme filtering agar informasi yang keluar dan masuk pada jaringan aman dari tindakan scanning, fabrikasi dan pembobolan akses dari orang yang tidak memiliki otoritas. Metode dalam penelitian ini menggunakan metode NDLC. Penerapan mekanisme firewall pada jaringan SOHO di Kelurahan Sako, Kota Palembang. Mekanisme penerapan keamanan jaringan menggunakan mekanisme firewall rule base, anti ARP, brute force, blocking off port scanning, consumer authentication dan penerapan kemanan enkripsi. Perangkat lunak penguji yang digunakan dalam penelitian ini antara lain, Wireshark, Hydra, Nmap. Pengujian dilakukan pada dua kondisi, yaitu sebelum dan sesudah penerapan keamanan jaringan. Hasil dari penelitian ini adalah penerapan mekanisme firewall yang sederhana sudah bisa digunakan untuk memproteksi jaringan pada ruang lingkup SOHO dan pemanfaatan router yang memiliki fitur layanan mekanisme firewall rule base.
Kata kunci — *Captive portal, Penetrasi sistem, Ip Firewall, Mikrotik*

Abstract

Securing data on a computer network is a very important part of maintaining the authenticity and integrity of data in transit. This study aims to build a mechanism to secure network data by implementing filtering mechanisms so that data entering and leaving the network is safe from being scanned, fabricated, and violated by unauthorized users. unauthorized person. The methods of this study used NDLC method. The establishment of firewall mechanism on SOHO network in Sako village, Palembang city. The network security enforcement mechanism uses a rule base firewall, anti-ARP, brute force, port scan blocking, user authentication, and cryptographic security enforcement. Testing software used in the study included Wireshark, Hydra, Nmap. The tests were carried out under two conditions, before and after the cybersecurity implementation. The result of this study is the application of a simple firewall mechanism that can be used to protect the network within the framework of SOHO and the use of routers with the firewall rule base of the mechanism. service function.
Keywords *— Captive portal, System penetration, Ip Firewall, Mikrotik*

1. PENDAHULUAN

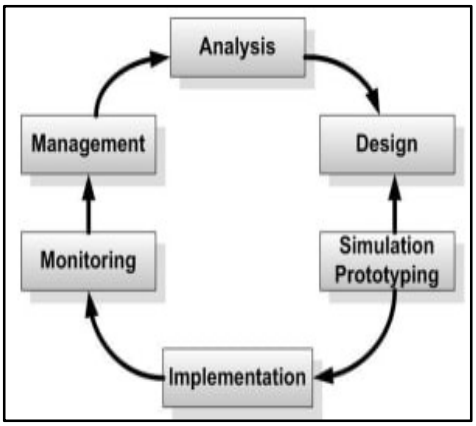
Penggunaan internet selaras dengan hadirnya jaringan komputer. Agar komunikasi data jaringan komputer terjaga dengan baik maka harus dilengkapi dengan mekaninsme keamanan jaringanbaik pada jaringan berbasis kabel maupun jaringan nirkabel. Jaringan nirkabel memiliki feksibelitas yang baik dan mampu menjangkau area yang lebih luas dan mampu mendukung kegiatan mobilitas yang tinggi. Karenanya teknologi nirkabel digunakan secara luas baik dalam industri, perkantoran maupun pemakaian pribadi di rumah. Dibalik kemudahan dalam implementasinya, jaringan nirkabel memiliki kelemahan yaitu disisi keamanannya sehingga banyak para hacker yang ingin mencoba memasuki jaringan walapun vendor-vendor perangkat keras jaringan sudah menerapkan mekanisme kamanan seperti melakukan enkripsi password dan

sebagainya tetapi hal tersebut belum cukup sehingga perlu dilakukan penambahan mekanisme kemanan[1]. Penerapan mekanisme keamanan pada jaringan bisa dilakukan dengan menggunakan perangkat khusus firewall device atau bisa menggunakan perangkat lunak firewall. Seperti dengan penerapan security detection tools yang mengintegrasikan antara IDS dan IPS pada arsitektur jaringan agar bisa meminimalisir tindakan pencurian data[2]. Beberapa kasus untuk menekan tindak pencurian data pada jaringan bisa menerapkan sistem kemanan berlapis tetapi hal ini jga berdampak pada performa jaringan yang di bangun karena akan terjadi kepadatan data dalam lalu lintas jaringan dikarenakan banyaknya data yang harus di filter pada kegiatan ingoing dan outgoing packet [3]. Penerapan firewall tools lebih banyak digunakan dikarenakan kemudahan untuk diadaptasikan di dalam sistem, kemudahan dalam melakukan pengembangan dan bebas biaya. Seperti penerapan snort yang diintegrasikan dengan honeypot yang mampu memfilter banyak anomali atau bentuk tindakan-tindakan pencurian data mulai dari malware hingga tindakan peretasan dan data dilaporkan secara real time [4]. Selain penerapan firewall software atau firewall tools dalam beberapa penerapan kemanan jaringan juga menerapkan mekanisme port blocking atau menggunakan port knocking. Dimana port hanya dibuka bagi network-network tertentu saja baik ongoing atau ingoing packet. Penerapan metode ini terbilang efektif untuk memproteksi terjadinya peretasan atau tindakan pencuriann data[5],[6]. Penelitian lainnya untuk mengoptimalkan sistem keamanan jaringan juga bisa menerapkan firewall filtering mac address dan hotspot login page untuk memberikan akses kepada user yang terdaftar saja di dalam sistem [7]. Banyak metode yang bisa diterapkan dalam mengamankan suatu jaringan, baik jaringan berbasis kabel ataupun berbasis wireless. Penelitian ini berfokus pada penerapan sistem keamanan jaringan wireless pada infrastruktur jaringan SOHO di kantor kelurahan Sako Palembang, dengan menerapkan metode firewall rule dengan menggunakan tools iptables untuk menjalankan prinsip anti ARP, blocking port, Brutforce blocking, mac filtering serta menerapkan protocol https pada sisi captive portal untuk memproteksi ddos dan peretasan akses login user. Tujuan dari penelitian ini adalah mencari pola sistem keamanan jaringan yang efektif dan mampu memproteksi tindakan peretasan pada jaringan SOHO. Metode yang digunakan dalam penelitian adalah Network Development Life Cycle. Metode ini mencerminkan tahapan-tahapan dalam pengembangan sistem jaringan [8],[9].

2. METODE PENELITIAN

A. Analisis

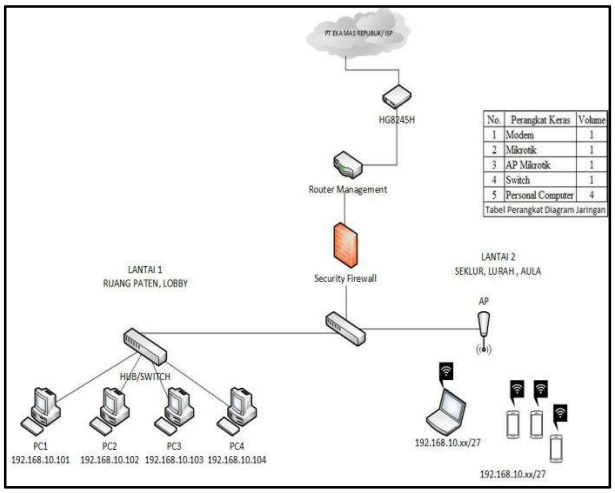
Tahap awal dilakukan yaitu analisa kebutuhan, analisa permasalahan yang muncul, teknologi jaringan dan analisa topologi atau jaringan yang sudah ada saat ini. Metode digunakan pada tahap ini diantaranya, membaca beberapa blueprint atau manual dokumentasi, observasi.



Gambar 1 *Network Development Life Cycle* (NDLC)

B. Desain

Pada tahap ini dilakukan desain topologi keamanan jaringan menggunakan simulator GNS3. Adapun komponen yang diperlukan antara lain: satu buah Router, satu buah modem, empat PC Client dan satu buah PC sebagai Attacker. Desain topologi keamanan jaringan yang dibangun bisa dilihat pada gambar 2.



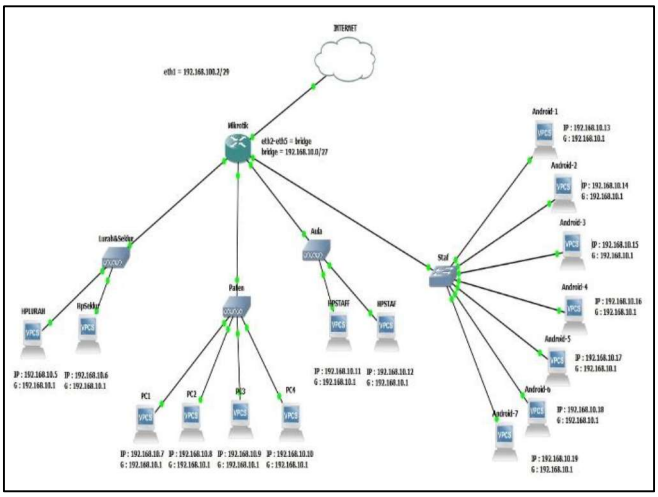
No.	Perangkat Keras	Volume
1	Modem	1
2	Mikrotik	1
3	AP Mikrotik	1
4	Switch	1
5	Personal Computer	4

Tabel Perangkat Diagram Jaringan

Gambar 2 Desain Topologi Yang Diusulkan

C. Simulasi Prototipe

Tahapan ini adalah tahapan simulasi sistem di dalam tools GNS3 untuk mendapatkan hasil yang diharapkan dari penerapan firewall filtering yang telah dikonfigurasikan di dalam perangkat router yang akan digunakan sebagai gateway dan firewall device. Adapun skenario pengujian ini meliputi pengujian sebelum diterapkan firewall filtering security dan sesudah diterapkan firewall filtering security, seperti tampak pada gambar 3.



Gambar 3. Desain Topologi Simulasi Keamanan Jaringan

3. HASIL DAN PEMBAHASAN

Captive Portal adalah suatu teknik otentikasi dan pengamanan data yang melewati *network* internal ke *network* eksternal. *Captive Portal* sendiri diterapkan di dalam router yang nantinya akan memberikan akses jaringan bagi user yang sudah tervalidasi di dalam. Captive portal

P-ISSN : 2087-9571, E-ISSN : 2541-335X

identiknya digunakan pada infrastruktur jaringan wireless, tetapi juga bisa digunakan pada jaringan wired sebagai bentuk autentikasi akses jaringan bagi userTampilan bisa dilihat pada gambar 5.2.

Gambar 4. Halaman *Captive Portal* Menggunakan *Https*

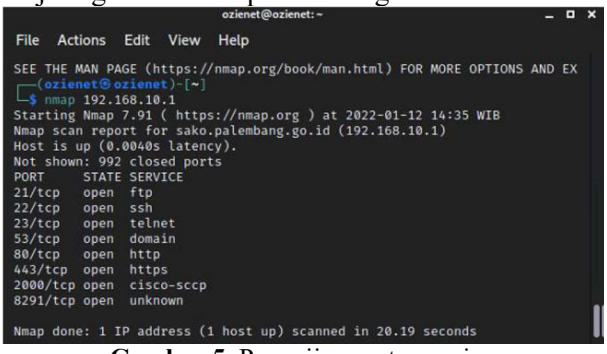
D. Pengujian sebelum penerapan Firewall Filtering dan SSL

Hasil pengujian ini dilakukan sebelum menerapkan mekanisme sistem keamanan firewall filtering dan penambahan SSL pada halaman captive portal.

a. Pengujian kerentanan pada halaman captive portal dari kegiatan peretasan ataupun pencurian data phising. Gambar 4 menunjukan bahwa pada saat halaman ini dilakukan penyadapan data menggunakan tools wireshark menghasilkan user dan password bisa didapatkan dengan mudah tanpa ada proses enkripsi di dalamnya.

Gambar 4. Pengujian captive portal dengan menggunakan protocol HTTP

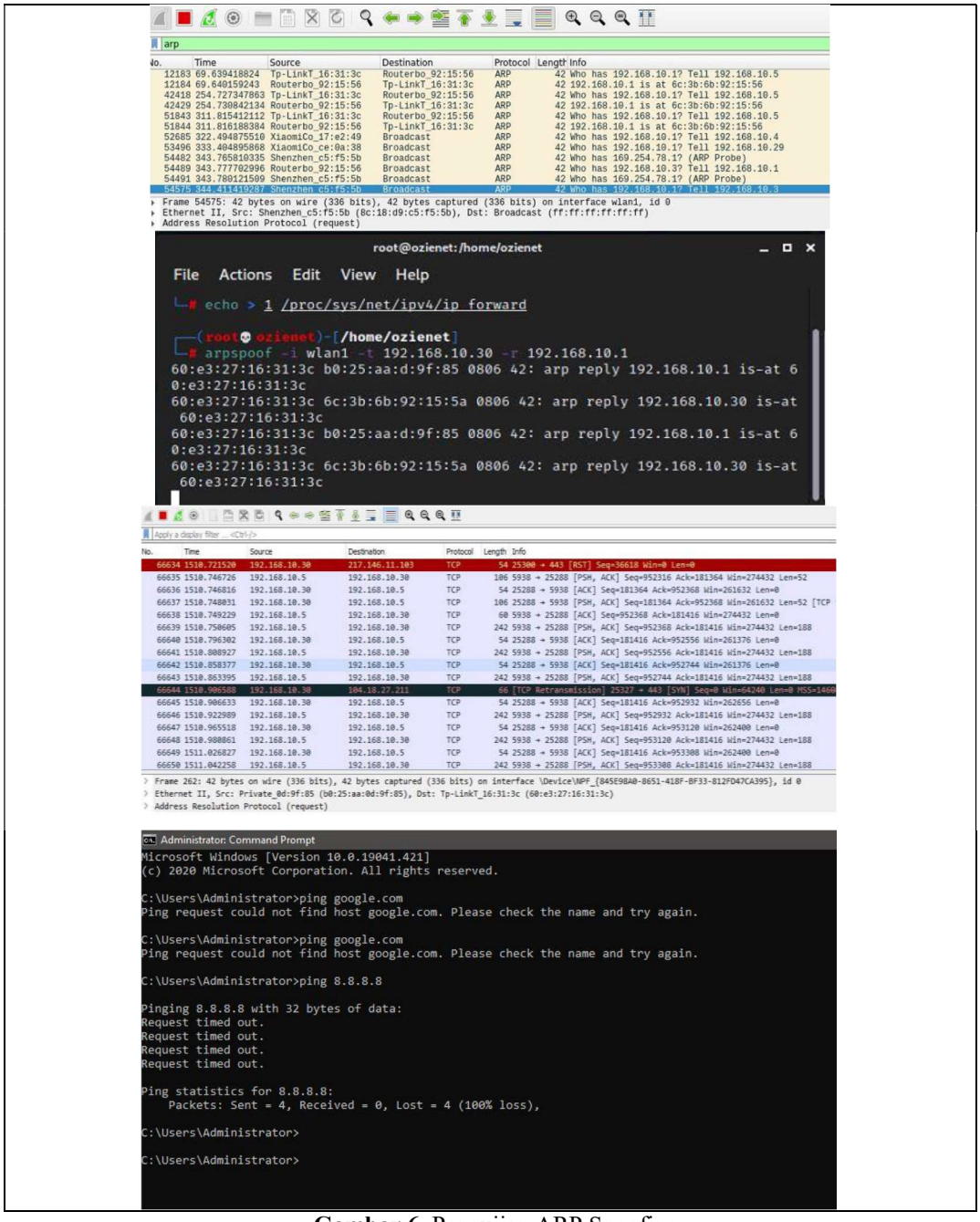
b. Pengujian port service
Setelah dilakukan pengujian port scanning menggunakan tools nmap didapatkan bahwa port yang digunakan dalam jaringan bisa didapatkan dengan mudah.



Gambar 5. Pengujian port scanning

c. Pengujian ARP Spoofing

Pengujian ini dilakukan untuk mendapatkan informasi ARP dan melakukan pembanjiran packet pada jaringan sehingga berdampak pada putusnya jaringan komunikasi. Pengujian ini berhasil dilakukan tanpa adanya mekanisme proteksi jaringan. Seperti tampak pada gambar 6.



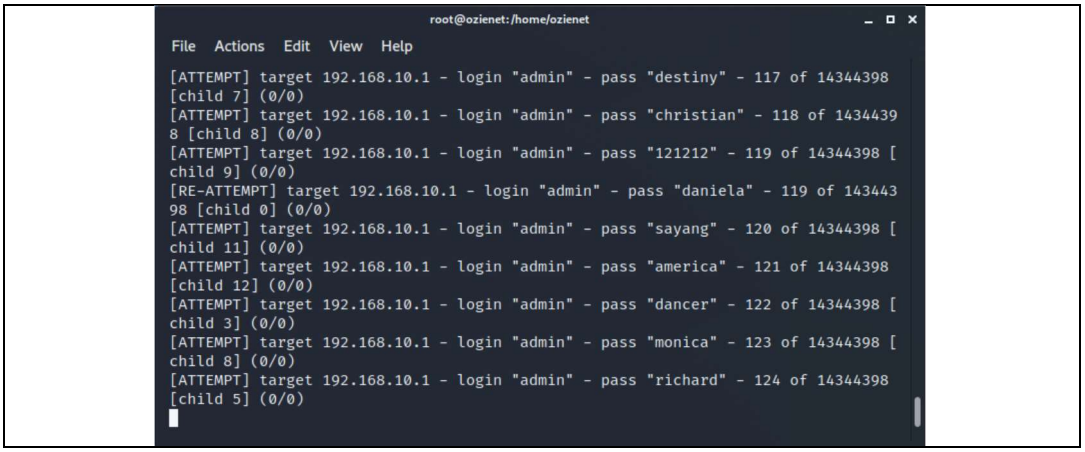
Gambar 6. Pengujian ARP Spoofing

d. Pengujian Bruteforce Telnet dan SSH

Pengujian peretasan ini dilakukan untuk mencoba masuk ke dalam sistem tanpa harus melakukan akses autentikasi, dengan cara menemukan user dan pasword yang digunakan untuk mengakses router. Dari hasil ini didapatkan username dan password bisa didapatkan

P-ISSN : 2087-9571, E-ISSN : 2541-335X

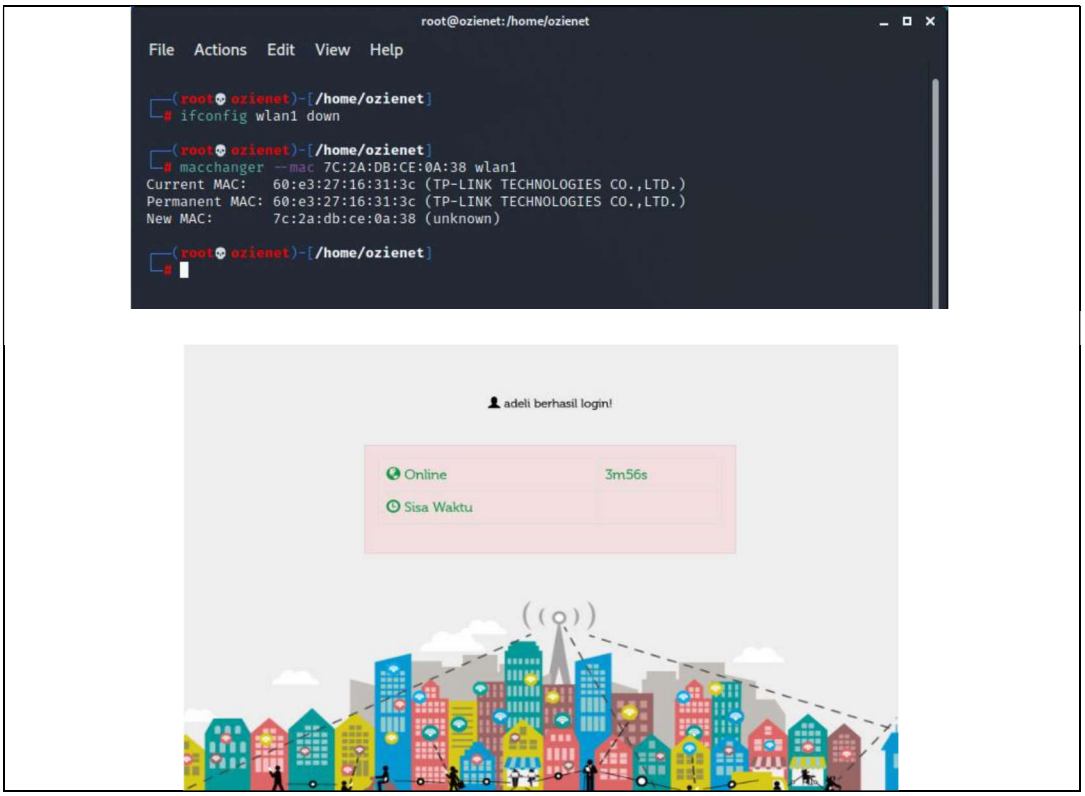
dengan mudah dan berdampak pada kinerja prosesor router yang melebihi kinerja normal yaitu diatas 50%.



Gambar 7. Pengujian Bruteforce

e. Pengujian Mac Cloning

Pengujian ini dilakukna untuk melihat apakah dengan cara mengcloning mac address peretas bisa mengakses jaringan tanpa harus melakukan login di captive portal. Dari hasil pengujian ini macloning bisa dilakukan dan peretas bisa mengkases jaringan tanpa melakukan login.



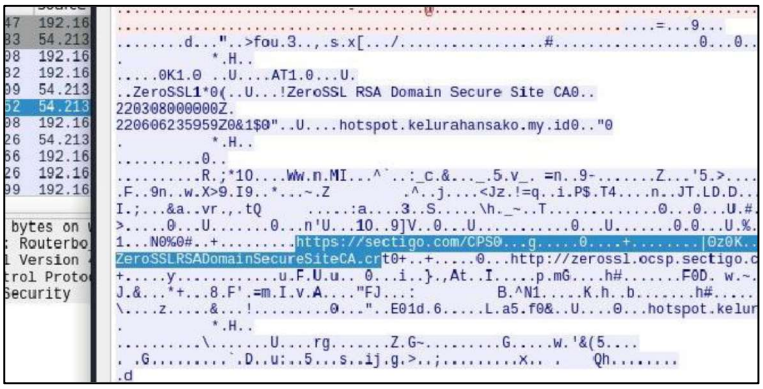
Gambar 8. Pengujian Mac Cloning

E. Pengujian Setelah Penerapan Firewall Filtering

Setelah diterapkan mekanisme firewall filtering maka didapatkan pengujian-pengujian yang dilakukan sebelumnya berhasil di proteksi, pengujian tersebut meliputi :

a. Pengujian SSL

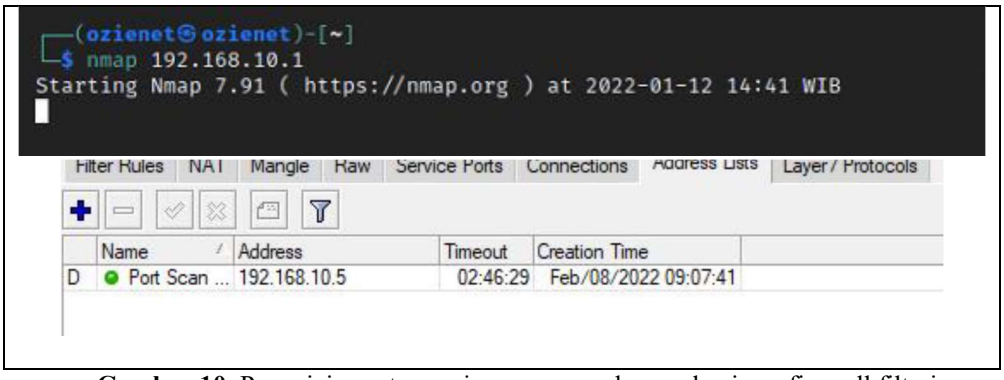
Captive portal sebelumnya yang telah dibangun menggunakan protocol http, kemudian dilengkapi dengan SSL key yang sudah di buat. Domain yang sebelumnya sako.palembang.go.id di ubah menjadi sako.palembang.my.id dikarenakan terkendala berkas validasi pada saat pembuatan SSL key dari vendor. Dari hasil pengujian SSL didapatkan username dan password tidak bisa di akses dikarenakan file tersebut di enkripsi. Seperti tampak pada gambar 9.



Gambar 9. Pengujian captive portal menggunakan SSL Key

b. Pengujain port scaning

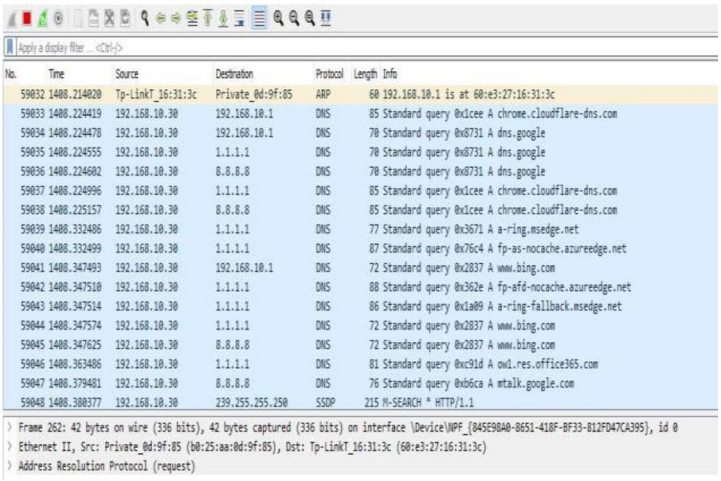
Setelah diterapkan firewall filtering maka port komunikasi yang sebelumnya terbuka pada pengujian sebelumnya pada pengujain ini port tidak bisa di buka karena di proteksi dengan mekanisme firewall filtering dan ip address attacker terekam dalam router untuk di blok. Seperti tampak pada gambar 10.



Gambar 10. Pengujain port scanning menggunakan mekanisme firewall filtering

c. Pengujian ARP Spoofing

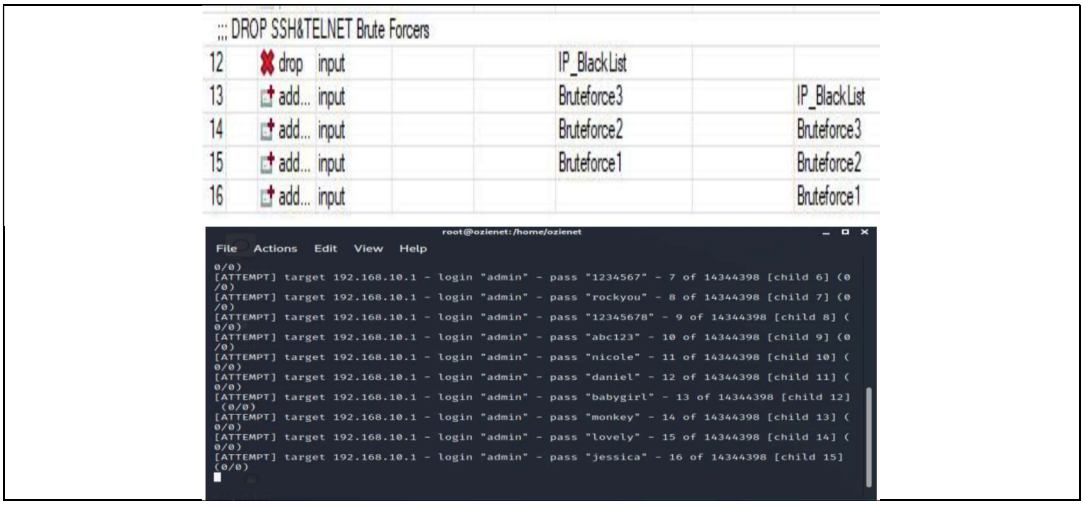
Setelah diterapkan mekanisme firewall filtering, maka ARP yang sebelumnya bisa di tangkap oleh aplikasi etheral seperti wireshark maka ARP tidak bisa lagi dikenali oleh wireshark sehingga kegiatan ARP Spoofing tidak bisa dilakukan seperti pada kondisi sebelumnya yang tanpa adanya pengamanan. Seperti tampak pada gambar 11.



Gambar 11. Hasil traping ARP wireshark

d. Pengujian Bruteforce

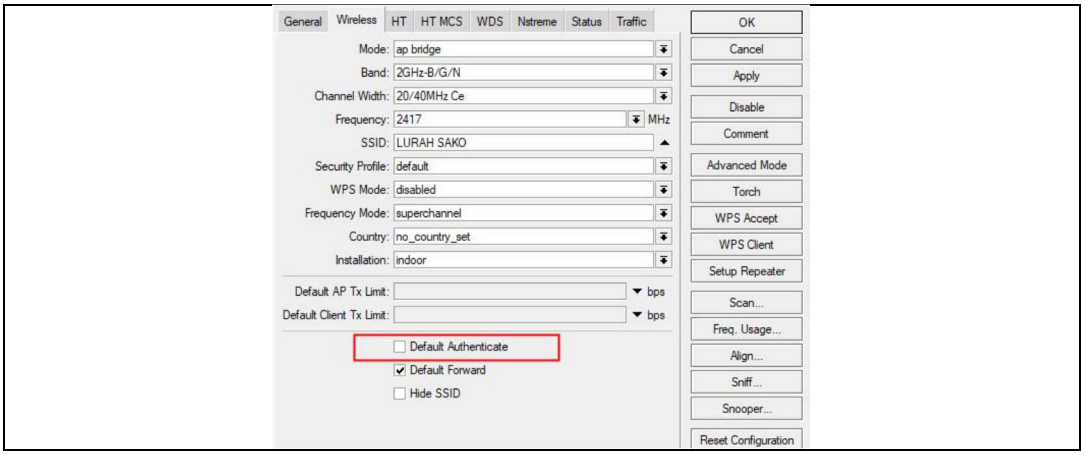
Pengujian brutfoce didapatkan bahwa ip address attacker di drop dari jaringan dikarenakan mekanisme firewall rule yang diterapkan drop ip address-list. sehingga attacker tidak akan bisa konek ke jaringan. Seperti tampak pada gambar 12.



Gambar 12. Pengujian Bruteforce setelah penerapan firewall rule

e. Pengujian Mac Cloning

Guna mencegah terjadinya mac cloning maka firewall policy yang diterapkan pada router adalah melakukan pemberlakuan mac filtering. Dimana hanya mac address yang terdaftar saja yang bisa terkoneksi ke jaringan dan tidak di izinkan untuk melakukan koneksi ulang dengan mac address yang sama. Seperti tampak pada gambar 13



Gambar 13. Pemberlakuan access list policy

F. Hasil Monitoring atau Pengujian

Adapun hasil perbandingan sebelum dan sesudah penerapan mekanisme firewall filtering dan SSL key dengan metode *port scanning, brute force,* serta *arp spoofer*, *mac address cloning* dan penerapan *SSL Key* pada halaman captive portal, dapat dilihat pada tabel 1.

Tabel 1. Hasil perbandingan sebelum dan sesudah penerapan optimalisasi keamanan jaringan

Serangan	Sebelum Penerapan	Sesudah Penerapan
Scanning Port	Berhasil dapat informasi berupa *port* yang terbuka pada sistem *mikrotik*	Penyerang tidak mendapatkan informasi berupa *port* yang terbuka pada sistem *mikrotik*
Arp Spoofing	Penyerang berhasil ke trafik sinyal antar *client* ke *router* namun dialihkan ke penyerang dengan memanfaatkan *arp spoofing*	Penyerang tidak berhasil karena trafik sinyal antar *client* ke *router* namun gagal dialihkan ke penyerang dengan memanfaatkan fitur *arp leases* dan *reply-only interfaces*
Brute Force Telnet	Berhasil mendapatkan *username* dan *password* di *router* dan yang mudah ditebak pada *service telnet.*	Penyerang tidak mendapatkan *username* dan *password* di *router di service telnet.*
Brute Force SSH	Berhasil mendapatkan *username* dan *password* di *router* dan yang mudah ditebak pada *service ssh.*	Penyerang tidak mendapatkan *username* dan *password* di *router di service ssh.*
Mac Clone	Berhasil mendapatkan identitas pada *mac address client* yang sudah terkoneksi serta *username* dan *password*.	Penyerang tidak bisa terhubung ke *wireless* karena telah di *filter* sebagai penyerang dan tidak mendapatkan *username* dan *password captive portal.*
SSL Key	Berhasil pendapatkan informasi username dan password login pada halaman captive portal yang tidak dilengkapi dengan SSL Key dengan melakukan trapping data menggunakan wireshark	Tidak berhasil dalam mendapatkan informasi username dan password pada halaman captive portal yang telah dilengkapi dengan SSL

4. KESIMPULAN

Adapun simpulan dari penelitian yang telah dilakukan, antara lain :Infrastruktur jaringan pada kelurahan Sako, kota Palembang tidak mengalami peruhan secara keseluruhan hanya menambahkan router device sebagai gateway dan firewall device.

1. Router yang digunakan adalah router mikrotik yang sudah dilengkapi dengan fitur firewall dan captive portal.
2. Menggunakan captive portal berdampak pada akses jaringan bisa lebih secure, karena setiap pengguna menggunakan user dan password yang berbeda.
3. Penerapan SSL pada halaman captive portal membuat user dan password menjadi terenkripsi pada saat data dilakukan penyadapan pada saat melintas di jaringan sehingga sulit untuk bisa di baca secara langsung
4. Penerapan blocking port berdampak positif bagi pengguna jaringan karena attacker mengalami kesulitan dalam melakukan identifkasi target dikarenakan jalur data informasi jaringan di tutup.
5. Penerapan Anti-ARP pada router memberikan dampak positif dalam jaringan karena attacker akan merasa kesulitan dalam melakukan floading atau pembanjiran packet sehigga bisa menyebabkan jaringan terganggu dan disconnected.
6. Penerapan firewall rule dan memberlakukan mekanisme drop address-list dalam kegiatan bruteforce baik pada komunikasi telnet atau SSH, sehingga kegiatan brute force pada jaringan bisa di proteksi.
7. Menerapkan access list policy dalam penerapan mekanisme firewall berdampak positif untuk menghindari terjadinya kegiatan duplikasi mac address untuk bisa terkoneksi dan masuk ke dalam jaringan.

DAFTAR PUSTAKA

[1] J. Gondohanindijo, “Sistem Keamanan Jaringan Nirkabel,” *Maj. Ilm. Inform.*, vol. 3, no. 2, hal. 1–217, 2012.

[2] M. Khari, M. Gaur, dan Y. Tuteja, “Meticulous Study of Firewall Using Security Detection Tools,” *Int. J. Comput. Appl. Inf. Technol.*, vol. 2, no. 1, hal. 1–9, 2014.

[3] M. M. ; Mustofa dan E. Aribowo, “Penerapan Sistem Keamanan Honeypot Dan Ids Pada,” *J. Sarj. Tek. Inform.*, vol. 1, no. 1, hal. 111–118, 2013.

[4] A. R. Gunawan, N. P. Sastra, dan D. M. Wiharta, “Snort dan Honeypot Sebagai Pendeteksi dan,” *Maj. Ilm. Teknol. Elektro*, vol. 20, no. 1, hal. 81–88, 2021, doi: https://doi.org/10.24843/MITE.2021.v20i01.P09.

[5] U. Faruk dan Amarudin, “Desain Keamanan Jaringan Pada Mikrotik Router Os,” *J. TEKNOINFO*, vol. 12, no. 2, hal. 72–75, 2018.

[6] R. N. Dasmen, M. H. ; Firmansyah, M. . Khadafi, dan T. Yolanda, “Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port,” *Decod. J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, hal. 1–7, 2022.

[7] R. A. Purnama, “Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address,” *Indones. J. Netw. Secur.*, vol. 8, no. 4, hal. 43–47, 2019.

[8] Y. Mulyanto dan S. B. Prakoso, “Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (Ndlc): Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC),” *J. Inform. Teknol. dan Sains*, vol. 2, no. 4, hal. 223–233, 2020, doi: 10.51401/jinteks.v2i4.825.

[9] T. Sanjaya dan D. Setiyadi, “Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim,” *J. Mhs. BINA Insa.*, vol. 4, no. 1, hal. 1–10, 2019.