

# 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 Barovich<sup>1\*</sup>, Muhammad Kholid Hidayat<sup>2</sup>, Fahmi Ajismanto<sup>3</sup>**

<sup>1,2</sup>*SI Informatika Institut Teknologi dan Bisnis PalComTech*

<sup>3</sup>*SI Sistem Informasi Institut Teknologi dan Bisnis PalComTech*

*Jl. Basuki Rahmat No. 05, Palembang 30129, Indonesia*

*e-mail: guntoro@palcomtech.ac.id<sup>1</sup>, kholidhidayat48@gmail.com<sup>2</sup>, fahmi\_ajismanto@palcomtech.ac.id<sup>3</sup>*

### 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 keamanan enkripsi. Perangkat lunak pengujian 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

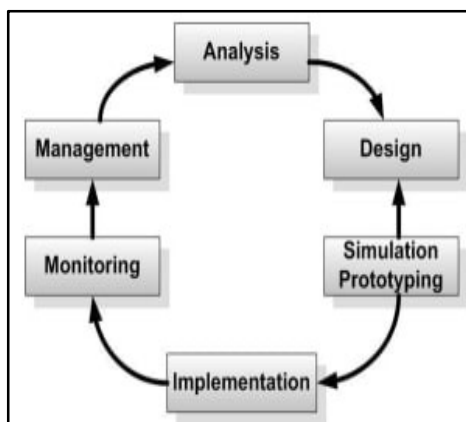
Penggunaan internet selaras dengan hadirnya jaringan komputer. Agar komunikasi data jaringan komputer terjaga dengan baik maka harus dilengkapi dengan mekanisme keamanan jaringan baik pada jaringan berbasis kabel maupun jaringan nirkabel. Jaringan nirkabel memiliki fleksibilitas yang baik dan mampu menjangkau 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 walaupun vendor-vendor perangkat keras jaringan sudah menerapkan mekanisme keamanan seperti melakukan enkripsi password dan

sebagainya tetapi hal tersebut belum cukup sehingga perlu dilakukan penambahan mekanisme keamanan[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 keamanan berlapis tetapi hal ini juga berdampak pada performa jaringan yang dibangun 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 keamanan 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

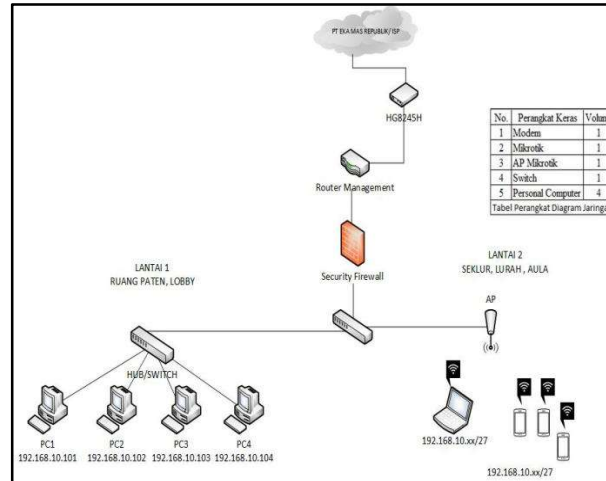
Tahap awal dilakukan yaitu analisa kebutuhan, analisa permasalahan yang muncul, teknologi jaringan dan analisa topologi atau jaringan yang sudah ada saat ini. Metode digunakan pada tahap ini diantaranya, membaca beberapa blueprint atau manual dokumentasi, observasi.



**Gambar 1** *Network Development Life Cycle (NDLC)*

## B. Desain

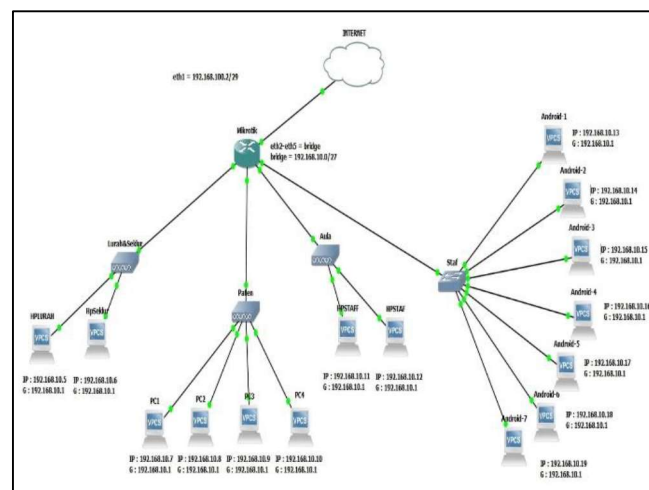
Pada tahap ini dilakukan desain topologi keamanan jaringan menggunakan simulator GNS3. Adapun komponen yang diperlukan antara lain: satu buah Router, satu buah modem, empat PC Client dan satu buah PC sebagai Attacker. Desain topologi keamanan jaringan yang dibangun bisa dilihat pada gambar 2.



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 dikonfigurasi 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*

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

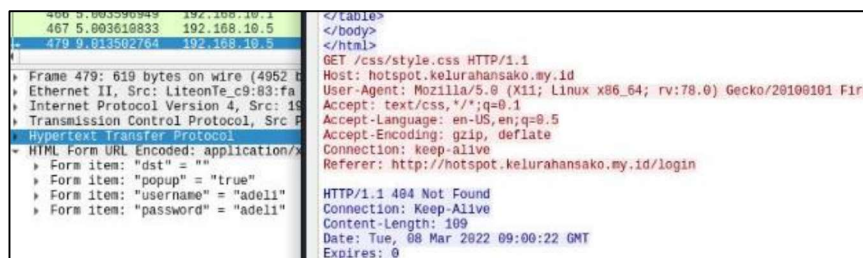


Gambar 4. Halaman *Captive Portal* Menggunakan *Https*

#### D. Pengujian sebelum penerapan Firewall Filtering dan SSL

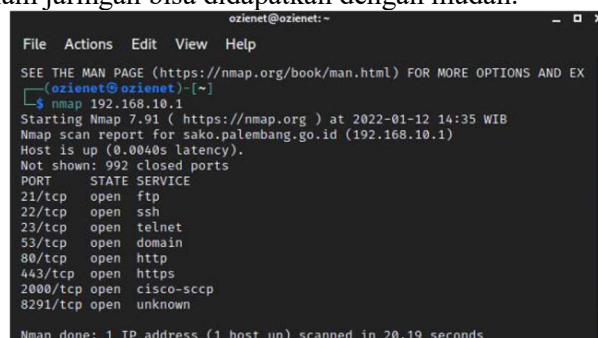
Hasil pengujian ini dilakukan sebelum menerapkan mekanisme sistem keamanan firewall filtering dan penambahan SSL pada halaman captive portal.

- a. Pengujian kerentanan pada halaman captive portal dari kegiatan peretasan ataupun pencurian data phishing. Gambar 4 menunjukkan 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

```
arp
No.      Time      Source      Destination      Protocol      Length      Info
12183 69.639418824 Tp-Link 16:31:3c Routerbo 92:15:56 ARP 42 Who has 192.168.10.17 Tell 192.168.10.5
12184 69.640159243 Routerbo 92:15:56 Tp-Link 16:31:3c ARP 42 192.168.10.1 is at 6c:3b:6b:92:15:56
42418 254.727347863 Tp-Link 16:31:3c Routerbo 92:15:56 ARP 42 Who has 192.168.10.17 Tell 192.168.10.5
42420 254.730842134 Routerbo 92:15:56 Tp-Link 16:31:3c ARP 42 192.168.10.1 is at 6c:3b:6b:92:15:56
51843 311.815421212 Tp-Link 16:31:3c Routerbo 92:15:56 ARP 42 Who has 192.168.10.17 Tell 192.168.10.5
51844 311.816188384 Routerbo 92:15:56 Tp-Link 16:31:3c ARP 42 192.168.10.1 is at 6c:3b:6b:92:15:56
52685 322.494875518 XiaomiCo 17:62:49 Broadcast ARP 42 Who has 192.168.10.17 Tell 192.168.10.4
53496 333.404895048 XiaomiCo ce:8a:38 Broadcast ARP 42 Who has 192.168.10.17 Tell 192.168.10.29
54482 343.765810335 Shenzhen cs:f5:5b Broadcast ARP 42 Who has 169.254.78.17 (ARP Probe)
54489 343.77702996 Routerbo 92:15:56 Broadcast ARP 42 Who has 192.168.10.37 Tell 192.168.10.1
54491 343.780121509 Shenzhen cs:f5:5b Broadcast ARP 42 Who has 169.254.78.17 (ARP Probe)
54519 344.311510209 Shenzhen cs:f5:5b Broadcast ARP 42 Who has 192.168.10.17 Tell 192.168.10.3

> Frame 54575: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan1, id 0
> Ethernet II, Src: Shenzhen cs:f5:5b (8c:18:d9:c5:f5:5b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

root@ozienet:/home/ozienet
File Actions Edit View Help
echo > 1 /proc/sys/net/ipv4/ip_forward

(root@ozienet)-[/home/ozienet]
arp spoof -i wlan1 -t 192.168.10.30 -r 192.168.10.1
60:e3:27:16:31:3c b0:25:aa:d9:f8:85 0806 42: arp reply 192.168.10.1 is-at 6
0:e3:27:16:31:3c
60:e3:27:16:31:3c 6c:3b:6b:92:15:5a 0806 42: arp reply 192.168.10.30 is-at
60:e3:27:16:31:3c
60:e3:27:16:31:3c b0:25:aa:d9:f8:85 0806 42: arp reply 192.168.10.1 is-at 6
0:e3:27:16:31:3c
60:e3:27:16:31:3c 6c:3b:6b:92:15:5a 0806 42: arp reply 192.168.10.30 is-at
60:e3:27:16:31:3c

Apply a display filter: «Ctrl+F»
No.      Time      Source      Destination      Protocol      Length      Info
66634 1518.721258 192.168.10.30 217.146.11.103 TCP 54 25380 + 443 [RST] Seq=36618 Win=0 Len=0
66635 1518.746726 192.168.10.5 192.168.10.30 TCP 186 5938 + 25280 [PSH, ACK] Seq=952316 Ack=181364 Win=274432 Len=52
66636 1518.748616 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181364 Ack=952368 Win=261632 Len=0
66637 1518.748831 192.168.10.30 192.168.10.5 TCP 186 25280 + 5938 [PSH, ACK] Seq=181364 Ack=952368 Win=261632 Len=52 [TCP
66638 1518.749229 192.168.10.5 192.168.10.30 TCP 68 5938 + 25280 [ACK] Seq=952368 Ack=181416 Win=274432 Len=0
66639 1518.750605 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=952368 Ack=181416 Win=274432 Len=188
66640 1518.756382 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181416 Ack=952556 Win=261376 Len=0
66641 1518.760892 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=952556 Ack=181416 Win=274432 Len=188
66642 1518.768377 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181416 Ack=952744 Win=261376 Len=0
66643 1518.763395 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=952744 Ack=181416 Win=274432 Len=188
66644 1518.766388 192.168.10.30 194.18.27.211 TCP 86 [TCP Retransmission] 25327 + 443 [RST] Seq=6 Win=64240 Len=0 MSS=1460
66645 1518.906633 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181416 Ack=952932 Win=262656 Len=0
66646 1518.922899 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=952932 Ack=181416 Win=274432 Len=188
66647 1518.965518 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181416 Ack=953128 Win=262400 Len=0
66648 1518.968861 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=953128 Ack=181416 Win=274432 Len=188
66649 1511.026827 192.168.10.30 192.168.10.5 TCP 54 25280 + 5938 [ACK] Seq=181416 Ack=953388 Win=262400 Len=0
66650 1511.042258 192.168.10.5 192.168.10.30 TCP 242 5938 + 25280 [PSH, ACK] Seq=953388 Ack=181416 Win=274432 Len=188

> Frame 262: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF{045E088B-8651-41B8-BF33-812FD47CA395}, id 0
> Ethernet II, Src: Private-8d:9f:85 (d8:25:aa:8d:9f:85), Dst: Tp-Link 16:31:3c (60:e3:27:16:31:3c)
> Address Resolution Protocol (request)

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.421]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com
Ping request could not find host google.com. Please check the name and try again.

C:\Users\Administrator>ping google.com
Ping request could not find host google.com. Please check the name and try again.

C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>

C:\Users\Administrator>
```

#### 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 password yang digunakan untuk mengakses router. Dari hasil ini didapatkan username dan password bisa didapatkan



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

```

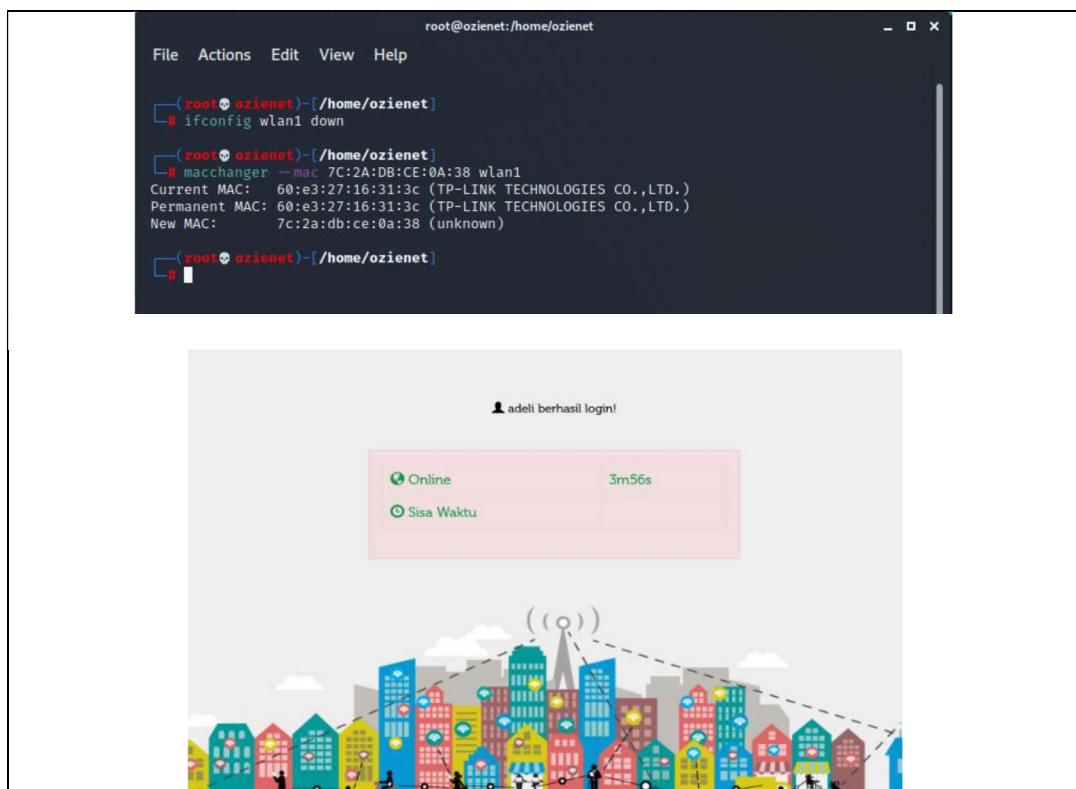
root@ozienet:/home/ozienet
File Actions Edit View Help
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "destiny" - 117 of 14344398
[child 7] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "christian" - 118 of 14344398
8 [child 8] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "121212" - 119 of 14344398 [
child 9] (0/0)
[RE-ATTEMPT] target 192.168.10.1 - login "admin" - pass "daniela" - 119 of 143443
98 [child 0] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "sayang" - 120 of 14344398 [
child 11] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "america" - 121 of 14344398
[child 12] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "dancer" - 122 of 14344398 [
child 3] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "monica" - 123 of 14344398 [
child 8] (0/0)
[ATTEMPT] target 192.168.10.1 - login "admin" - pass "richard" - 124 of 14344398
[child 5] (0/0)

```

Gambar 7. Pengujian Bruteforce

#### e. Pengujian Mac Cloning

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

```

87 192.16 ..... = .9
88 54.213 ..d...">fou.3...s.x[/../..#.....0....H.
      *.H.
89 192.16 ...0K1.0.U...AT1.0...U.
90 192.16 ...ZeroSSL10(.U...)ZeroSSL RSA Domain Secure Site CA0..
91 54.213 Z20308000000Z.
92 54.213 Z20606235959Z0&1$0".U...hotspot.kelurahansako.my.id0.."0
      *.H.
93 192.16 .....0...
94 54.213 ..F..n.w.X9.I9...Z...^...c.&...5.v...=n.g-...Z...'5.>.
95 192.16 I...a.&.v.r.tq.....a...3...S...h...T...0...0...U...%
      >...U...n.U...0...U...0...U...X
          NOk0#. https://getinfo.com/getinfo.aspx?getinfo=
ZeroSSL.RSA.Domain.Secure.Site.CA.cer10+...http://zerossll.ocsp.setigo.
Y...y...f.U.F.u...0...i...At...m.m6...h.h...F0D.w-
J.&...&...F...m.i.v.A...&...FJ...B.*M1...K.h.b...h.h#
\...z...&...&...0"...E01D.6...L.a.5.f0&.U...hotspot.kelu
      *.H.
97 192.16 ....U...rg...Z.G-...G...w.'&(5...
      G...D...u.:5...s.j.g>;...G...x... Qh.....

```

b. Pengujian port scanning



```
(ozienet@ozienet)~[~]
$ nmap 192.168.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 14:41 WIB
```

Filter Rules	NAI	Mangle	Raw	Service Ports	Connections	Address Lists	Layer / Protocols
+	-	✓	✗	📄	🔍		
Name	Address	Timeout	Creation Time				
D	Port Scan ... 192.168.10.5	02:46:29	Feb/08/2022 09:07:41				

### c. Pengujian ARP Spoofing

Setelah diterapkan mekanisme firewall filtering, maka ARP yang sebelumnya bisa ditangkap 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.

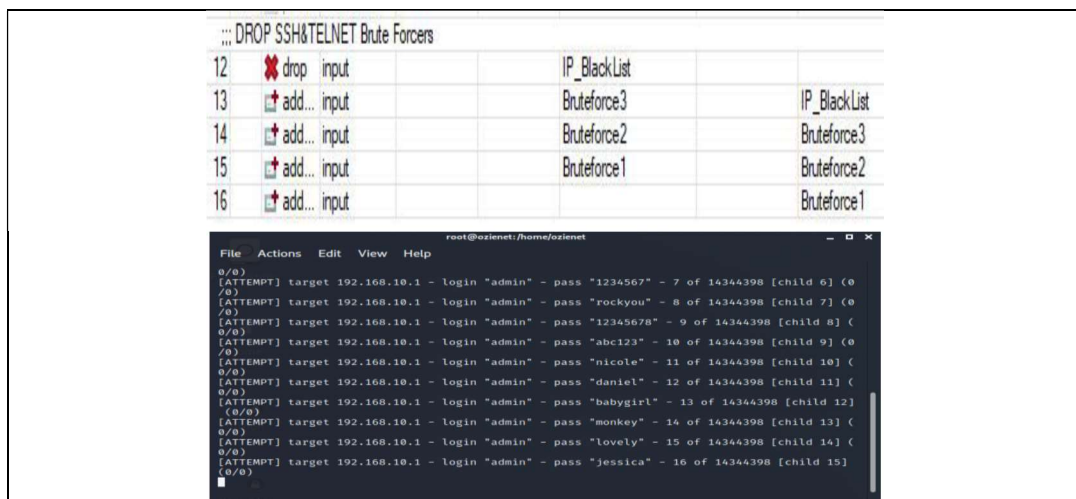
No.	Time	Source	Destination	Protocol	Length	Info
59032	1480.214020	Tp-LinkT_16:31:3c	Private_0d:9f:85	ARP	60	192.168.10.1 is at 60:e3:27:16:31:3c
59033	1480.224419	192.168.10.30	192.168.10.1	DNS	85	Standard query 0xc1ee A chrome.cloudflare-dns.com
59034	1480.224478	192.168.10.30	192.168.10.1	DNS	70	Standard query 0xc731 A dns.google
59035	1480.224555	192.168.10.30	1.1.1.1	DNS	70	Standard query 0xc731 A dns.google
59036	1480.224602	192.168.10.30	8.8.8.8	DNS	70	Standard query 0xc731 A dns.google
59037	1480.224996	192.168.10.30	1.1.1.1	DNS	85	Standard query 0xc1ee A chrome.cloudflare-dns.com
59038	1480.225157	192.168.10.30	8.8.8.8	DNS	85	Standard query 0xc1ee A chrome.cloudflare-dns.com
59039	1480.332406	192.168.10.30	1.1.1.1	DNS	77	Standard query 0xc671 A a-ring.msedge.net
59040	1480.332499	192.168.10.30	1.1.1.1	DNS	87	Standard query 0xc6c4 A fp-as-nocache.azureedge.net
59041	1480.347493	192.168.10.30	192.168.10.1	DNS	72	Standard query 0xc837 A www.bing.com
59042	1480.347510	192.168.10.30	1.1.1.1	DNS	80	Standard query 0xc61e A fp-afd-nocache.azureedge.net
59043	1480.347514	192.168.10.30	1.1.1.1	DNS	86	Standard query 0xc1a09 A a-ring-fallback.msedge.net
59044	1480.347574	192.168.10.30	1.1.1.1	DNS	72	Standard query 0xc837 A www.bing.com
59045	1480.347625	192.168.10.30	8.8.8.8	DNS	72	Standard query 0xc837 A www.bing.com
59046	1480.363406	192.168.10.30	1.1.1.1	DNS	81	Standard query 0xc91d A owl.res.office365.com
59047	1480.379481	192.168.10.30	8.8.8.8	DNS	76	Standard query 0xc6ca A mtalk.google.com
59048	1480.380377	192.168.10.30	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

> Frame 262: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF{045E98A0-8651-418F-BF33-812FD47CA395}, id 0  
> Ethernet II, Src: Private\_0d:9f:85 (00:25:aa:0d:9f:85), Dst: Tp-LinkT\_16:31:3c (60:e3:27:16:31:3c)  
> Address Resolution Protocol (request)

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.

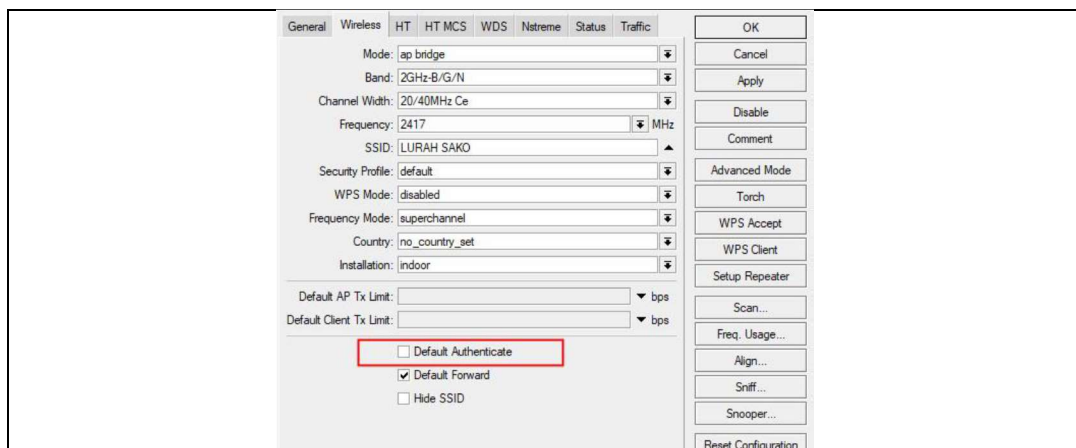


Gambar 12. Pengujian Bruteforce setelah penerapan firewall rule

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

#### 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 identifikasi 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 flooding atau pembanjiran packet sehingga 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.