# IMPLEMENTASI *ARP WATCH* DENGAN *PFSENSE* UNTUK MEKANISME PENGAMANAN *ACCESS POINT*

**Rifan Ramadhan Chandra Dirgantara**

D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya,
rifandirgantara16050623017@mhs.unesa.ac.id

**I Made Suartana**

Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya,
madesuartana@unesa.ac.id

**Abstrak**

Pengamanan jaringan internet secara *wireless* berupa menggunakan *password* yang saat ini dilakukan oleh kebanyakan pihak seperti di stasiun TV kebanyakan yang terdapat di Jawa Timur terkadang tidak terlalu memiliki tingkat keamanan yang cukup tinggi dikarenakan dapat terjadinya serangan-serangan yang mengancam seperti serangan berupa spoofing dengan menggunakan *tool-tools* yang banyak tersebar di internet, dimana serangan ini cukup sering terjadi di jaringan internet di tasiun TV kebanyakan yang terdapat di Jawa Timur.Untuk menghindari kejadian tersebut dapat dilakukan dengan upaya-upaya untuk mendeteksi terlebih dahulu serangan tersebut dengan menggunakan *tools* atau aplikasi yang banyak terdapat di internet seperti *Arpwatch* yang terdapat dalam *PfSense* untuk melakukan pendeteksisan serangan berupa *spoofing*. Oleh karena itu, dengan melihat dari permasalahan tersebut, maka pada penelitian ini penulis mengangkat judul Implementasi *Arpwatch* Dengan *PFSense* Untuk Mekanisme Pengamanan *Access Point*.Mekanisme pengamanan *Access point* menggunakan *Arpwatch* yang terdapat dalam *PfSense* dirasa cukup untuk mendeteksi serangan *spoofing* dikarenakan dapat diintegrasikan dengan email untuk melihat notifikasi yang masuk jika terjadi atau terdapat serangan *spoofing*.
**Kata kunci**: Pengamanan, Arpwatch, Arpspoofing, PfSnese.

**Abstract**

Securing wireless internet networks in the form of using a password that is currently carried out by most parties such as most TV stations located in East Java sometimes does not have a high enough level of security because it can occur threatening attacks such as attacks in the form of spoofing using tools- tools that are widely spread on the internet, where this attack is quite common in the internet network at most TV stations located in East Java. To avoid these events can be done with efforts to detect these attacks in advance by using tools or applications that are widely available on the internet like Arpwatch contained in PfSense to detect attacks in the form of spoofing. Therefore, by looking at these problems, the authors raise the title Arpwatch Implementation with PFSense for Access Point Security Mechanisms. Access point security mechanisms using Arpwatch contained in PfSense are considered sufficient to detect spoofing attacks because they can be integrated with email to see notifications that come in if there is a spoofing attack.
**Keywords**:Securing, Arpwatch, Arpspoofing, PfSense.

## PENDAHULUAN

Salah satu stasiun lembaga penyiaran televisi di Jawa Timur memiliki sistem jaringan internet yang berupa *access point* dan hanya memiliki sistem keamanan berupa *password* tanpa ada mekanisme keamanan tambahan lainnya. Jaringan internet *wireless* yang terdapat di lembaga tersebut memiliki kelemahan dimana orang dapat mencari atau membobol keamanan passwordnya, bisa menggunakan *tool-tool* atau aplikasi yang banyak beredar di internet. Ketika jaringan dapat mudah diakses

apalagi oleh pihak-pihak yang tidak sah dan tidak bertanggung jawab, mungkin akan menimbulkan serangan-serangan yang bisa merugikan bagi instansi atau pemilik dan pengguna sah dari jaringan tersebut.

Pada saat ini terdapat permasalahan yang berada didalam jaringan internet di lembaga tersebut, yaitu terdapat serangan berupa *spoofing* yang diketahui oleh staff teknik disana, yang menimbulkan kekhawatiran. ARP *spoofing* adalah teknik yang digunakan penyerang untuk mengirim (*spoofed*) ARP (*address Resolution Protocol*) pesan ke jaringan area lokal. Secara umum, tujuannya adalah untuk mengasosiasikan alamat MAC penyerang dengan alamat IP dari host lain, seperti gateway default, menyebabkan lalu lintas yang dimaksudkan agar alamat IP tersebut dikirim ke penyerang sebagai gantinya atau melakukan tindakan-tindakan yang tidak diinginkan. Selain itu pihak lembaga sendiri juga ingin menangkal atau mendeteksi serangan berupa serangan *ARP Spoofing* dimana serangan tersebut dapat melakukan tindakan pencurian dan mengubah data yang ada, dikarenakan lembaga tersebut terdapat data-data pegawai dan keuangan yang setiap hari atau setiap bulannya harus dikirimkan ke lembaga penyiaran yang bertempat di pusat. Data keuangan dan data pegawai sangat riskan untuk diambil atau dimanipulasi, oleh karena itu diperlukan sistem keamanan jaringan tambahan yang dimana sistem keamanan jaringan ini nantinya dapat mendeteksi serangan yang terjadi nantinya di dalam jaringan di lembaga tersebut.

Berdasarkan beberapa permasalahan diatas dan pentingnya masalah tersebut untuk segera diselesaikan, maka penulis akan merancang sebuah penerapan keamanan jaringan menggunakan ARP Watch. ARP Watch merupakan aplikasi komputer yang gratis, yang dapat membantu memonitor aktifitas lalu lintas

Studi dalam bidang implementasi untuk mengenai pengamanan dalam suatu jaringan yang terdapat dalam literatur *ethernet* dalam jaringan internet dan memelihara *database ethernet* atau alamat *ip.* ARP Watch mengahasilkan *log* untuk memberikan notifikasi pencocokan informasi alamat *ip* dan *MAC* yang sama dengan yang sebelumnya. Aplikasi ini dikhususkan untuk administrator jaringan untuk mengawasi aktivitas *ARP* untuk mendeteksi *ARP Spoofing* atau aktivitas modifikasi alamat *ip atau MAC* yang dilakukan oleh pihak yang tidak bertanggung jawab.

Tujuan dilakukannya penelitian ini adalah tidak lain diharapkan agar jaringan internet di lembaga penyiaran tersebut dapat lebih aman untuk menghilangkan kekhawatiran akan pencurian dan manipulasi data dan juga diharapkan agar dapat mengetahui jika di lain hari terdapat serangan yang tidak diinginkan terjadi. Dengan dilakukannya observasi mendorong penulis untuk merancang dan mengimplementasikan suatu sistem keamanan jaringan komputer untuk mengamankan atau setidaknya memberi tanda bahwa terdapat serangan yang nantinya mengancam data yang terdapat di lembaga tersebut, maka penulis mengajukan proposal Tugas Akhir dengan judul "**I**mplementasi Arp Watch Dengan PfSense Untuk Mekanisme Pengamanan Access Point".

Tujuan yang ingin dicapai adalah dapat mengimplementasikan ARP Watch untuk mengatasi serangan *spoofing* yang telah dan mungkin akan terjadi lagi, dan implemetasi ARP Watch tersebut diharapkan dapat membantu menambahkan mekanisme pengamanan dalam *access point*. Manfaat dari implementasi pengamanan Access Point adalah Menambah pengetahuan mengenai perancangan suatu sistem keamanan jaringan menggunakan *Intrusion Detection System,* dan dengan adanya sistem ini diharapkan dapat membantu untuk mengamankan jaringan internet di instansi tersebut

## KAJIAN PUSTAKA

### Penelitian Terdahulu

terdahulu. Literatur tersebut melakukan implementasi pengamanan jaringan me

nggunakan beberapa metode dan jenis serangan yang berbeda. Berikut adalah beberapa dari yang saya gunakan sebagai acuan, *Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux*. Hasil yang didapat dari literatur diatas adalah Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux dapat membantu untuk memonitoring hingga melakukan drop dan melakukan filter jenis serangan, dan juga mengirimkan atau menampilkan jenis serangan yang datang. Selain itu penulis juga mengacu pada literatur berikut, Monitoring Jaringan *Wireeless* Terhadap serangan *Packet Sniffing* dengan menggunakan IDS, yang memiliki hasil berupa implementasi IDS hanya sebatas mendeteksi, ketika berhasil terdeteksi belum terdapat sistem untuk memberitahu admin bahwa terdapat serangan.

**Keamanan Jaringan**

(Firmansyah, t.thn.) Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan. Tujuan dari membuat keamanan jaringan adalah untuk mengantisipasi resiko terjadinya serangan atau ancaman serangan baik berupa ancaman fisik maupun *logic* baik langsung mapun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan. Terdapat beberapa kemungkinan tipe

**Serangan Jaringan Nirkabel atau *Wireless***

**Spoofing**

(Fauzi Y. , 2017)*Spoofing* berasal dari kata *spoof* yang berarti meniru fungsi dari program yang asli. Hal ini biasanya dilakukan oleh seorang peretas. *Spoof* berjalan dalam sistem lokal dan merupakan program hidup yang menampilkan perintah atau tampilan yang palsu kepada pengguna. Menurut Felsen et al *spoofing* dapat didefinisikan sebagai "*Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya"*. Dalam bahasa *networking, spoofing* berarti pura-pura berlaku atau menjadi sesuatu yang sebenarnya bukan..

**ARP Watch**

(Saive, 2013)ARP Watch merupakan program perangkat lunak komputer sumber terbuka atau *open source* yang dapat membantu untuk memantau aktivitas lalulintas internet (seperti mengubah alamat ip atau alamat MAC) didalam jaringan internat dan mengelola basis data pemasangan alamat ip. Nantinya ARP Watch akan menghasilkan *log* informasi pemasangan alamat ip dan MAC bersamaan dengan waktunya, sehingga dapat mengawasi dengan cermat ketika aktivitas muncul di jaringan.

**PfSense**

(Kurnia, 2018)PfSense merupakan *software (operating system)* berbasis FreeBSD yang disesuaikan untuk kebutuhan Firewall dan Router. pfSense dimanajemenkan menggunakan interface web / via web dan dapat diinstall pada hardware langsung maupun pada virtualisasi. Selain fungsi untuk *firewalling* dan *routing*, PfSense menyediakan beberapa paket yang sering dibutuhkan untuk kebutuhan *gateway* maupun layanan jaringan pada client, seperti: DNS, VPN Server, CA, FreeRADIUS, HAProxy, dst. Semua paket disediakan tanpa menambah potensi kerentanan keamanan pada distribusi dasar.

## METODE

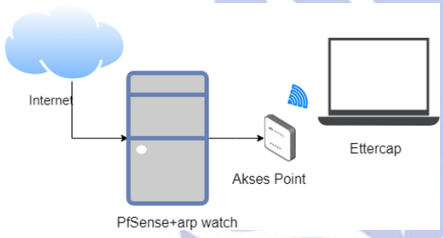
**Analisis**

Dalam proses perancangan sistem dimulai dengan analisi masalah yang diangkat. Dalam analisis masalah tersebut yaitu mengenai perancangan sistem keamanan jaringan menggunakan ARP Watch di salah satu stasiun televisi diJawa Timur. Implementasi ARP Watch pada jaringan disana memudahkan staff IT yang ada untuk memonitoring serangan ARP *spoofing*. Tahap yang akan penulis paparkan merupakan

tahap untuk memahami sistem yang telah berjalan, mengidentifikasi masalah dan kebutuhan, studi literatur, dan survei lapangan. Tahap ini juga mempersiapkan kebutuhan perangkat yang ada di instansi untuk menyesuaikan kelancaran pada tahap selanjutnya.

**Perancangan Sustem**

Tahap selanjutnya adalah perancangan sistem, pada tahap ini diharapkan dapat memberi gambaran kebutuhan dan bagaimana sistem keamanan jaringan akan dibangun. Dalam tahap ini terdapat *design* rancangan topologi yang nantinya akan digunakan sebagai berikut:




Gambar 1. Prototipe Simulasi Jaringan

Pada Prototipe simulasi jaringan diatas merupakan rancangan yang nantinya akan digunakan penulis sebagai acuan topologi jaringan yang berada di sana. Pada topologi diatas terdapat PC yang telah ter*install* PFSense dan ARP Watch yang nantinya akan mendeteksi serangan, PC tersebut terhubung dengan internet dan juga terhubung dengan *Access Point* yang dignakan untuk memancarkan sinyal internet ke komputer lain. Lalu terdapat 1 komputer atau laptop yang telah ter*install* aplikasi untuk melancarkan serangan *spoofing* yaitu Ettercap yang nantinya berkerja sebagai penyerang atau *Attacker*.

1. Kebutuhan Perangkat
   a. Perangkat keras

1) Laptop yang digunakan untuk simulasi serangan.
2) PC untuk simulasi deteksi serangan.
3) Laptop sebagai korban dari serangan yang dilakukan.

b. Perangkat Lunak

1) Laptop yang digunakan untuk simulasi serangan menggunakan sistem operasi Kali Linux.
2) PC yang digunakan untuk mendeteksi serangan menggunakan sistem operasi Ubuntu.
3) ARP Watch untuk mendeteksi serangan ARP *spoofing*.

c. Spesifikasi *Personal Computer*

Berikut ini adalah tabel spesifikasi laptop yang digunakan untuk simulasi:

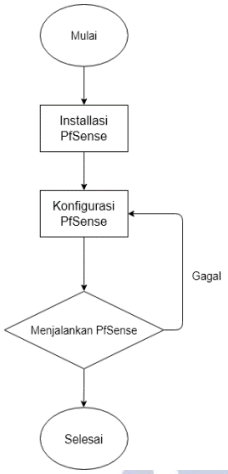
Tabel 1 . Spesifikasi Laptop untuk simulasi

| | |
|---|---|
| Sistem Operasi | Windows 10 64-bit |
| Prosessor | Intel Core i3-5005U |
| RAM | 8 GB |
| HDD | 500 GB |
| VGA | Intel Graphics 5500/AMD Hainan |

**Rancangan Simulasi**

Perancangan sistem keamanan jaringan ini terlebih dahulu akan dibuat *prototipe* simulasi. Dalam proses simulasi ini nantinya akan menggunakan *Virtualbox* sebagai perangkat lunak virtualisasi. Hal ini dilakukan untuk mengetahui bagaimana sistem ini akan dibangun dan berjalan sebagaimana mestinya, selain itu juga meminimalisir kesalahan dalam setiap tahap dalam implementasi secara *real* nantinya. Jadi tahap ini merupakan tahap untuk mencari solusi dari masalah yang kamungkinan terjadi ketika membangun sistem.

Prototipe yang akan dibangun sesuai dengan bab perancangan sistem yang terdapat pada poin sebelumnya, prototipe yang akan dirancang dalam *Virtualbox* memiliki alur sebagai berikut:



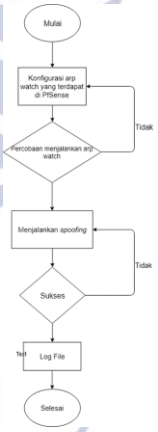

Gambar 2. Alur Konfigurasi PfSense

Menurut alur yang terdapat pada Gambar diatas pertama-pertama menyiapkan ISO PfSense untuk memulai didalam sebuah *flashdisk* yang telah disiapkan, lalu melakukan proses installasi Pfsense pada komputer atau aplikasi virtual yang telah disediakan. Setelah itu melakukan konfigurasi-konfigurasi yang dibutuhkan untuk menggunakan PfSense tersebut, setelah selesai melakukan konfigurasi lalu muulai untuk mencoba menjalankan Pfsense sesuai dengan kebutuhan dan disambungkan dengan *Access Point* yang telahdisediakan sebelumnya.

**Uji Coba Sistem**

Setelah selesai melakukan konfigurasi terhadap Pfsense langkah berikutnya, yaitu melakukan konfigurasi arp watch yang terdapat dalam Pfsense itu sendiri. Setelah melakukan konfigurasi arp watch yang diperlukan sesuai kebutuhan, selanjutnya melakukan percobaan untuk menjalankan arp watch apakah sukses atau tidak, bersamaan dengan itu mulai menjalankan serangan berupa *spoofing* dengan target yang sudah ditentukan, jika serangan berhasil maka akan menghasilkan sebuah *log file*, jika selangan belum berhasil dan arp watch belum melakukan atau mendeteksi adanya serangan maka akan dilakukan lagi untuk konfigurasi arp watch dan spoofing untuk mendapatkan hasil yang dibutuhkan. Setelah berhasil maka *log file* yang diinginkan akan muncul, penjelasan diatas akan divisualisasikan dengan alur sebagai berikut:

Dalam melaksanakan uji coba untuk melakukan serangan berupa spoofing, spoofing sendiri berasal dari kata *spoof* yang berarti meniru fungsi dari program yang asli. Hal ini biasanya dilakukan oleh seorang peretas. *Spoof* berjalan dalam sistem lokal dan merupakan program hidup yang menampilkan perintah atau tampilan yang palsu kepada pengguna. Menurut Felsen et al *spoofing* dapat didefinisikan sebagai "Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya". Dalam bahasa *networking, spoofing* berarti pura-pura berlaku atau menjadi sesuati yang sebenarnya bukan.




Gambar 3. Alur konfigurasi Arpwatch

ARP *spoofing* juga dapat dikatakan merupakan teknik yang digunakan penyerang untuk mengirim (*spoofed*) ARP (*address Resolution Protocol*) pesan ke jaringan area lokal. Secara umum, tujuannya adalah untuk mengasosiasikan alamat MAC penyerang dengan alamat IP dari host lain, seperti gateway default, menyebabkan lalu lintas yang dimaksudkan agar alamat IP tersebut dikirim ke penyerang sebagai gantinya

Dalam percobaan ini penulis nantinya akan menggunakan beberapa aplikasi spoofing yang terdapat di Kali Linux sebagai referensi untuk

mencari cara serangan yang memiliki dampak yang cukup signifikan, hingga tercapainya tujuan dari penelitian yang diangkat oleh penulis. Cara yang digunakan oleh penulis untuk melakukan spoofing dengan menggunakan 2 aplikasi spoofing yang terdapat di Kali Linux, yaitu Ettercap dan Syntax terminal Kali Linux. Ketika melakukan percobaan menggunakan 2 aplikasi atau cara tersebut dapat disimpulkan menurut tabel berikut:

Tabel 2 Perbandingan Serangan

| No | Jenis Serangan | Terdeteksi | Notifikasi/alert |
|---|---|---|---|
| **1** | Ettercap | Ya | Muncul Sekali ketika serangan dimulai dan bertambah dengan menunggu beberapa menit sekali |
| **2** | Syntax Kali Linux | Ya | Muncul terus-menerus saat serangan sedang terjadi |

Dengan tabel diatas dapat disimpulkan bahwa serangan yang digunakan menggunakan 2 aplikasi atau cara diatas menampilkan efek notifikasi atau alert yang berbeda, dimana Syntax Kali Linux menimbulkan efek notifikasi yang beruntun ketika serangan sedang terjadi, agar pihak admin dapat segera mengetahui jika sedang terjadi serangan spoofing. Ettercap yang meskipun serangan berhasil namun untuk notifikasi yang muncul hanya sekali diawal dan hanya muncul beberapa menit. Penjelasan mengenai isi nantinya akan dijelaskan di Bab IV Pembahasan

## HASIL DAN PEMBAHASAN

Dalam bab ini akan dijelaskan mengenai hasil dan pembahasan dari uji coba yang sebelumnya telah direncanakan oleh penulis yang berjudul Implementasi ARP WATCH dengan Pfsense Untuk Mekanisme Pengamanan Access Point. Langkah yang akan dilakukan, yaitu pemasangan atau meng*install software* meliputi sistem operasi *Pfsense* sebagai *server*. Kemudian didalam *Pfsense* atau *sever* tersebut akan dipasang paket Arpwatch sebagai mekanisme pengamanan jaringan yang akan mendeteksi jaringan yang melewati *server* dan juga sebagai *alert* jika terjadi serangan atau penyalahgunaan layanan jaringan *internet* yang dilakukan oleh oknum-oknum yang tidak bertanggung jawab. Untuk uji coba serangan Arp Spoof nantinya akan menggunakan Kali linux yang akan dijalankan secara *Virtual* menggunakan *Virtualbox* untuk menjalankan uji coba serangannya. Proses konfigurasi akan dijelakan lebih detail pada bab ini.

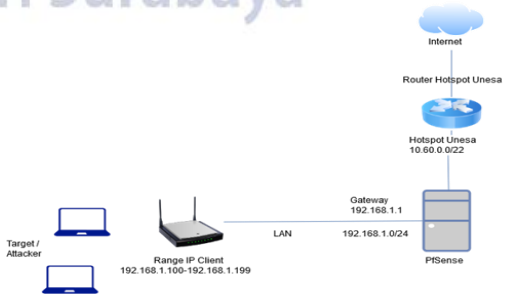
### Hasil Implementasi dan Pembahasan

Sebelum melakukan implementasi, penulis melakukan simulasi terlebih dahulu di Lab Rekayasa Perangkat Lunak A10, untuk memaksimalkan ketika melakukan implementasi.

Berikut langkah-langkah implementasi yang akan dilakukan:

1. Pemasangan dan konfigurasi Pfsense.
2. Pemasangan dan konfigurasi paket Arpwatch sebagai *alert* jika terjadi serangan.
3. Pemasangan dan konfigurasi Kali Linux kedalam *Virtualbox* sebagai uji coba serangan arpspoof.

Berikut topologi jaringan yang telah direncanakan sebelumnya. Topologi dibawah merupakan topologi siulasi yang akan diambil, yaitu Gambar 8 sebagai berikut:




Gambar 4. Topologi Jaringan Simulasi di Lab RPL

Berikut adalah penjelasan dari topologi diatas:

1. Router Hotspot Unesa terhubung dengan internet sesuai dengan bagaimana yang telah dikelola oleh instansi terkait dengan

memberikan *IP Address* 10.60.0.0/22 yang mengarah ke *PfSense* secara otomatis (*DHCP*).

2. Pfsense tersebut dikonfigurasi sesuai kebtuhan penulis yaitu sebagai mode *Router* yang terhubung dengan *router* Hotspot Unesa. Ketika pfsense mendapatkan *IP Address* 10.60.103.69 atau akan diberikan secara *random*. *PfSense* akan mengenali *IP Address* tersebut sebagai *interface WAN*.
3. *Interface LAN Pfsense* dengan *IP* 192.168.1.1 dikonfigurasi *DHCP* yang mengarah ke *Access point* TP-LINK WR840N yang mempnyai *Network* 192.168.1.0/24. Sehingga *target / attacker* mendapatkan rentang *IP* 192.168.1.100- 192.168.1.199.
4. Mode yang digunakan pada *Wireless* and *Router* TP-Link WR840N adalah mode sebagai *access point* atau pemancar sinyal / jaringan internet atau yang bisa disebut *PTMP* (*Point To Multi Point*).

Selanjutnya seperti yang telah dijelaskan sebelumnya, tahapan dari implementasi sistem yang akan penulis kerjakan sebgai berikut:

1. Pemasangan dan konfigurasi *PfSense access wireless target/attacker.*
2. Pemasangan dan konfigurasi Arpwatch yang terdapat di *Pfsense* sebagai *alert* terjadi serangan.
3. Pemasangan dan konfigurasi Kali linux ke dalam *Virtualbox* sebagai uji coba serangan Arpspoof.

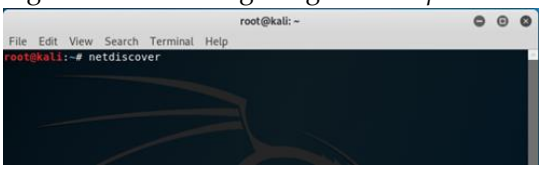
**Pengujian**

Setelah konfigurasi selsesai dilakukan, tahap yang akan dilakukan selanjutnya, yaitu pengujian. Pengujian ini dilakukan dengan tujuan untuk melihat kinerja dari skenario yang dibuat sebelumnya apakah dapat berfungsi sesuai dengan fungsinya dan sesuai dengan apa yang ditargetkan.

Pengujian yang dilakukan adalah mekanisme penetrasi serangan Arpspoofing, dari proses tersebut nanti akan dilihat apakah sistem yang sudah terpasang dapat berjalan dengan baik dan benar.

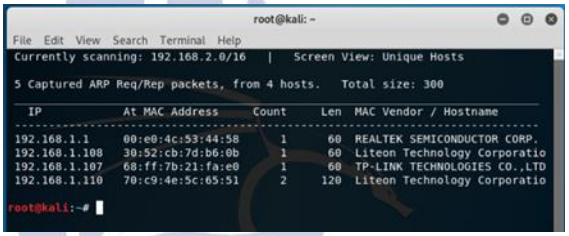
Proses penetrasi

1. Buka terminal *kali linux* kemudian masukkan perintah *netdiscover* untuk melihat *IP* berapa saja yang telah tersambung dengan *access point.*



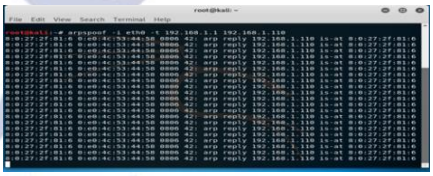

Gambar 5. Perintah Netdiscover

2. Setelah itu akan muncul beberapa *IP* yang telah terdaftar seperti gambar 41 berikut ini.




Gambar 6. IP yang terdaftar

3. Kemudian masukkan perintah seperti (arpspoof -i eth0 -t 192.168.1.1 192.168.110) untuk memulai serangan dengan target 192.168.1.110.

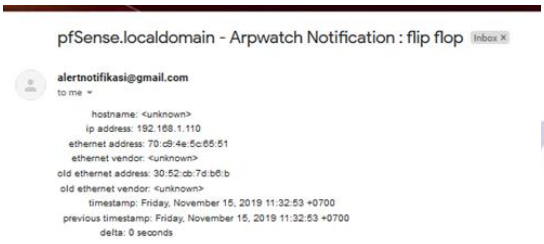


Gambar 7. Hasil dari Serangan

4. Kemudian akan muncul berupa *alert* yang disambungkan dengan *email*, nantinya akan terlihat perubahan pada *MAC Address* dapat terlihat pada gambar 4.34 berikut ini.

Gambar 8. Hasil dari Alert

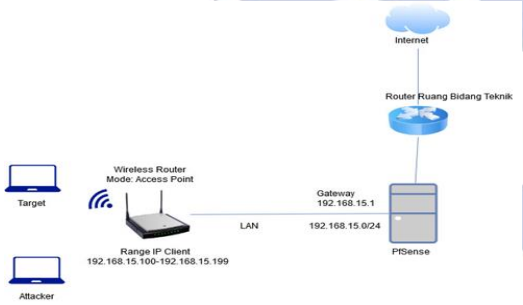
5. Dalam gambar 4.35 terdapat penjelajan dari alert yang masuk melalui email sebagai berikut:
   a. Hostname: nama dari pemilik IP.
   b. IP Address: alamat IP.
   c. Ethernet Address: alamat fisik dari device yang digunakan.
   d. Ethernet vendor: vendor ethernet




Gambar 9. Terlihat Perubahan MAC Address

**Proses Implementasi**

1. Topologi yang nantinya akan diterapkan




Gambar 10. Topologi Real

2. Implementasi Real

Pada tahap ini akan ditunjukkan proses yang akan dilakukan di salah satu stasiun televisi di Jawa Timur yang mana langkah yang diambil sama seperti yang dilakukan ketika proses simulasi yang di lakukan di Lab RPL A10. Tahap pertama yang dilakukan adalah mempersiapkan perangkat dan install PfSense. Berikut adalah tahapan yang diambil:

a) Mempersiapkan Perangkat

Perangkat yang disiapkan adalah:

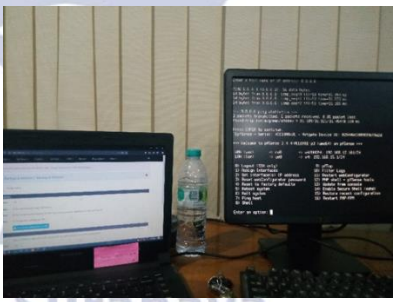
i) PC yang akan di*install* PfSense dengan 2 kartu jaringan, port 1 untuk sumber internet, dan port 2 yang akan digunakan untuk meremote dan setelah itu akan digunakan ke access point.
ii) Flashdisk yang berisi iso PfSense 2.4.4
iii) Kabel LAN
iv) Laptop untuk remote
v) Access Point

Proses menginstall PfSense menggunakan flashdisk yang telah disiapkan sebelumnnya. Ketika selesai semua proses menginstall akan seperti pada gambar 15.

Gambar 11. Tampilan Awal PfSense

b) Remote

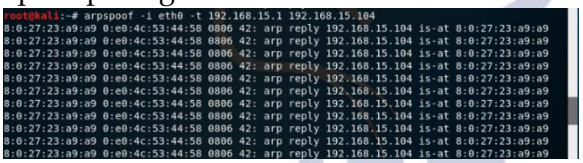
Untuk remote Pfsense dapat menggunakan cara wired dengan disambungkan ke kabel LAN atau dengan cara wireless setelah disambungkan dengan wifi dari access point.



Gambar 12. Remote Pfsense

3. Uji coba Serangan

Disini penulis melakukan uji coba serangan dengan menggunakan kali linux sebagai yang melakukan serangan dan menggunakan ponsel genggam dari penulis sebagai korban serangan. Serangan yang digunakan melalui terminal dengan perintah arpspoof -i eth0 -t 192.168.15.1 192.168.15.104 seperti pada gambar 4.39 berikut ini.



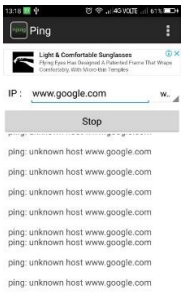

Gambar 13. Serangan *arpspoof*

Penjelasan mengenai perintah serangan sebagai berikut:

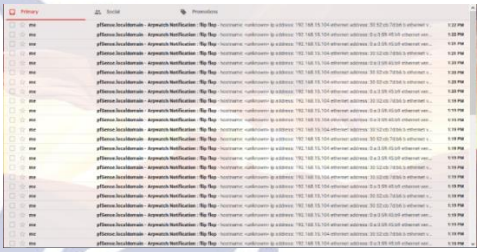
Arpspoof: jenis serangan yang dilakukan.

a. -i : interface yang akan diserang contohnya seperti wlan0 atau eth0 atau yang terdaftar pada kali linux.
b. Eth0: interface yang terdaftar pada kali linux.
c. -t: adalah perintah untuk memasukkan target serangan.
d. Lalu dua ip dibelakang adalah roter ip dan victim ip yang akan diserang.

Ketika serangan terjadi maka target tidak dapat tersambung dengan koneksi internet dikarenakan serangan ini mengganti mac address dari ip target sehingga tidak dapat menyambungkan ke internet seperti pada gambar 18.




Gambar 14. Hasil Ping www.google.com



Gambar 15. Alert Notifiasi

## PENUTUP

### Simpulan

Setelah melakukan simulasi terlebih dahulu di Lab Rekayasa Perangkat Lunak (RPL) Gedung A10 Teknik Informatika menggunakan Pfsense dari semua hasil konfigurasi dan pengujian maka didapatkan beberapa kesimpulan, yaitu:

1. Dengan adanya mekanisme pengamanan Access point ini dengan tujuan agar dapat mendeteksi serangan berupa arpspoofing.
2. Mekanisme pengamanan ini dapat menampilkan alert jika terjadi serangan yang dilakukan oleh attacker lalu alert tersebut dapat diintegrasikan dengan email yang telah didaftarkan di pfsense.
3. Sistem pengamanan ini masih belum sempurna dikarenakan kurangnya informasi yang didapatkan oleh penulis, sistem ini menurut penulis cukup efekti untuk mendeteksi sebuah serangan, dengan keterbatasan sumber informasi yang ada.

### Saran

1. Mekanisme pengamanan untuk menangkal serangan arp spoofing dengan menggunakan Arpwatch masih belum

maksimal karena masih kurangnya informasi mengenai konfigurasi Arpwatch yang benar di PfSense.

2. Mekanisme alert notifikasi yang terdapat pada PfSense seharusnya bisa dikembangkan agar dapat diintegrasikan dengan aplikasi-aplikasi konvensional yang dapat diinstall di telepon seluler sehingga memudahkan untuk menerima notifikasi dari Arpwatch tersebut.

## DAFTAR PUSTAKA


Darmawan. (2015, November 12). *http://labgis.si.fti.unand.ac.id/pengenalan-aplikasi-ettercap-dan-tutorial/*. Diambil kembali dari labgis.si.fti.unand.ac.id: http://labgis.si.fti.unand.ac.id/pengenalan-aplikasi-ettercap-dan-tutorial/

Fauzi, A. R. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan IDS. *Jurnal Manajemen Informatika, 8*, 11-17.

Fauzi, Y. (2017, January 20). *https://netsec.id/jenis-serangan-jaringan-komputer/*. Diambil kembali dari https://netsec.id/jenis-serangan-jaringan-komputer/: https://netsec.id/jenis-serangan-jaringan-komputer/

Firmansyah, E. (t.thn.). *http://itgeek.id/sistem-keamanan-jaringan-komputer/*. Diambil kembali dari http://itgeek.id/sistem-keamanan-jaringan-komputer/: http://itgeek.id/sistem-keamanan-jaringan-komputer/

KIJ, M. (2017, May 31). *http://ajk.if.its.ac.id/?p=910*. Diambil kembali dari http://ajk.if.its.ac.id/?p=910: http://ajk.if.its.ac.id/?p=910

Kurnia, A. (2018, 8 14). *Apa itu pfsense*. Diambil kembali dari https://bnet.id/apa-itu-pfsense/: https://bnet.id/

pklbptik. (2016, Februari 1). *http://blog.unnes.ac.id/widiyanti/2016/02/01/pengertian-ubuntu/*. Diambil kembali dari blog.unnes.ac.id: http://blog.unnes.ac.id/widiyanti/2016/02/01/pengertian-ubuntu/

Pradipta, Y. W. (2017). Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan OP Tables Berbasis Linux. *Jurnal Manajemen Informatika, 7*, 21-28.

Ramachandran, V., & Nandi, S. (t.thn.). Detecting ARP Spoofing: An Active Technique.

Saive, R. (2013, April 16). *https://www.tecmint.com/monitor-ethernet-activity-in-linux/*. Diambil kembali dari https://www.tecmint.com/monitor-ethernet-activity-in-linux/: https://www.tecmint.com/monitor-ethernet-activity-in-linux/

Sutrisno. (2017, Maret 3). *http://blog.unnes.ac.id/sutrisno/2017/03/03/jenis-jenis-jaringan-komputer-dan-pengertiannya/*. Diambil kembali dari http://blog.unnes.ac.id/sutrisno/2017/03/03/jenis-jenis-jaringan-komputer-dan-pengertiannya/: http://blog.unnes.ac.id/sutrisno/2017/03/03/jenis-jenis-jaringan-komputer-dan-pengertiannya/

Williamson, M. (2005). *PfSense 2 Cookbook.* Birmingham: Packt Publishing.Ltd.

Zonggonau, K., & Sajati, H. (2015). MEMBANGUN SISTEM KEAMANAN ARP SPOOFING MEMANFAATKAN ARPWATCH DAN ADDONS FIREFOX. *MEMBANGUN SISTEM KEAMANAN ARP SPOOFING MEMANFAATKAN ARPWATCH DAN ADDONS FIREFOX*, 49.