Jurnal Manajemen Informatika. Volume 09 Nomor 01 Tahun 2019, 42-50

IMPLEMENTASI CAPTIVE PORTAL DENGAN MENGGUNAKAN PFSENSE

Probo Novian Candra
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, probocandra@mhs.unesa.ac.id

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

Abstrak

Wireless merupakan salah satu teknologi bidang telekomunikasi yang berkembang pesat pada saat ini. Namun perlu diketahui celah kemanan pada jaringan masih rentan terhadap pencurian data hak akses seperti membobol *username* dan *password* pada *hostpot*. Contoh lain adalah serangan *DOS (Denial Of Service)* bisa dikenal dengan sebagai tindak kejahatan dengan memanfaatkan serangan terhadap *server* yang akan menghabiskan *resource*. Dari permasalahan tersebut salah satu alternatifnya yaitu dengan menggunakan mekanisme *Captive Portal* sebagai autentikasi *user*. Penelitian ini menerapkan mekanisme *Captive Portal* menggunakan *Router PfSense* dimana pada *platform* tersebut telah tersedia fitur *Captive Portal* serta paket tambahan *Freeradius* dan *Snort IDS (Intrusion Detection System)*. Hasil dari mekanisme tersebut yaitu *user* akan melakukan autentikasi ke halaman *Web Captive Portal* dengan memasukkan *Username* dan *Password*. Sementara itu *Freeradius* sebagai akses kontrol terhadap *user* berdasarkan *challenge/respon* dan *Snort IDS (Intrusion Detection System)* dikonfigurasi dengan *rule* untuk mendeteksi serangan tertentu. Sehingga dengan penerepan *Captive Portal* tersebut diharapkan jaringan *wireless* pada *hostpot* menjadi lebih aman karena tidak hanya memaksa *user* untuk melakukan *login*, mekanisme *Snort IDS (Intrusion Detection System)* akan memberikan *alert* bila terjadi serangan.

Kata Kunci : *Captive Portal, Freeradius, Snort IDS (Intrusion Detection System), DOS (Denial Of Service)*

Abstract

Wireless technology is one of the rapidly growing fields of telecommunications at the moment. But keep in mind network security still vulnerable to attack by non-proprietary user or attacker. For the example security attack to gain access to the system by breaking username and password on the hotspot system. Another example is the DOS(Denial Of Service) attacks, DOS is known as crimes by making attacks against servers that will spend the resource or make server unavailable. One of the solutions for the problems is to use Captive Portal as a mechanism for user authentication. This study uses the Captive Portal which is implemented using the PfSense Router. PfSense already has Captive Portal features an extra package Freeradius and Snort IDS (Intrusion Detection System). Implementation Captive Portal forcing users to authenticate before gaining access to the system. While implementation of Freeradius as access control on user-based challenge/response and Snort IDS (Intrusion Detection System) is configured with a rule to detect specific attacks. The result of this study is expected to make the wireless network more secure because it not only authenticate the user, the mechanism of the Snort IDS (Intrusion Detection System) will provide alerts in case of attack.

Keywords : *Captive Portal, Freeradius, Snort IDS (Intrusion Detection System), DOS (Denial Of Service)*

.

PENDAHULUAN

Wireless merupakan salah satu teknologi bidang telekomunikasi yang berkembang pesat pada saat ini. Teknologi ini memiliki kelebihan dengan menawarkan kemudahan konfigurasi serta flesibilitas dalam mengaksesnya (Abdiansyah,2013). Namun perlu diketehui celah keamanan pada jaringan tersebut masih rentan terhadap pencurian data hak akses seperti membobol *username* dan *password* pada *wireless*. Selain itu, contoh lainnya adalah serangan *DOS (Denial Of Service)* bisa dikenal sebagai tindak kejahatan dengan memanfaatkan serangan terhadap *server* yang menghabiskan *resource*. Tentunya dari hal tersebut maka diperlukan adanya mekanisme untuk meningkatkan kemanan jaringan pada *wirless*. Banyak cara untuk meningkatkan kemanan pada jaringan *wireless* salah satunya yaitu menerapkan teknologi *Captive Portal* dan *Freeradius* dengan mekanisme ketika *user* melakukan *login* pada *hotspot user* tersebut akan dialihkan kehalaman *web login* untuk memasukkan *username* dan *password*. Sementara itu fungsi *Freeradius* sebagai akses kontrol terhadap *user* berdasarkan *Challenge/Respon* pada aktivitas *user*.

Fitur *Snort IDS (Intrusion Detection System)* bisa digunakan sebagai deteksi serangan berupa *alert* dengan menambahkan *rule* secara manual berdasarkan definisi deteksi serangan yang ingin dihasilkan. Penerapan mekanisme *Captive Portal* juga mempunnyai cara seperti yang dilakukan pada studi (Muis Rajab,2010). Pada studi tersebut menerapkan mekanisme Enkripsi *WPA2* dan autentikasi *server RADIUS* yang dibangun pada sistem

operasi *Windows* 2003, namun belum banyak yang menerapkan mekanisme *Captive Portal* menggunakan *Router PfSense*. Pada *Router PfSense* terdapat banyak fitur untuk membantu mengamankan sistem jaringan yang dibangun, salah satunya adalah fitur paket *Freeradius* dan *Snort IDS (Intrusion Detection System)*. Paket fitur ini menarik buat penulis untuk mengetahui bagaimana *Captive Portal* bekerja pada *Router PfSense*. Hasil dari implementasi tersebut yaitu adanya mekanisme otentikasi *Captive Portal* pada *hostpot*, *user* diwajibkan melakukan *login* menggunakan *username* dan *password*. Pada sistem paket *Freeradius PfSense* berfungsi sebagai autentikasi akses kontrol terhadap *user* beradasarkan *metode challenge/ respon*. Selain itu penerapan *SSL* dimaksudkan sebagai enkripsi pada protokol *HTTPS web Captive Portal* serta Konfigurasi *Snort IDS (Intrusion Detection System)* dan *rule TCP Flooding*, *UDP Flooding* yang akan membarikan *alert* bila terjadi serangan *DOS (Denial Of Service)* oleh seorang *attacker*.

KAJIAN PUSTAKA

Penelitian Terdahulu

Studi dalam bidang implementasi *Captive Portal* telah terdapat pada literatur terdahulu. Literatur-literatur tersebut melakukan sebuah implementasi mekanisme *Captive Portal* dimana pada umumnya melakukan uji coba menggunakan mekanisme enkripsi *WPA2* dan autentikasi *server RADIUS* yang dibangun dengan sistem operasi *Windows 2003*. Penulis pada aritkel (Muis Rajab, 2010) menerapkan teknologi *WPA2 RADIUS* dengan cara melakukan pemasangan *server RADIUS* pada *Windows server* 2003. Implementasi tersebut menggunakan 3 komputer pada jaringan *wireless LAN* yang nantinya akan dilakukan pengujian koneksi *WPA2-RADIUS*. Untuk mengetahui sistem kemanan tersebut dilakukan pengujian *scanning vulnerabilities* pada *server RADIUS* menggunakan *tools Nessus* serta *Backtrack 3*, *K-Mac*, *TsGrinder* dan *TSCrack* sebagai mekanisme serangan sistem kemanan *(hacking)*.

Selain menggunakan mekanisme *WPA2*, juga terdapat perangakat lunak lain yang difungsikan sebagai *Captive Portal*. Penerapan mekanisme *Captive Portal* dengan menggunakan *Easyhostpot*, *Freeradius*, dan *coovachili*, merupakan salah satu cara alternatif untuk mengamankan sebuah layanan akses internet

Pada sisi pengujian serangan, *Captive Portal* artikel (Yoga Adi Pradipta, 2017) & (Dwi Kuswanto, 2014) menggunakan jenis serangan *DOS Attack*, sebagaimana membahas analisis sebuah serangan *DOS (Denial Of Service)*. *DOS* sendiri merupakan aktifitas yang dapat menghambat kerja sebuah sistem komputer utamanya layanan *(service)*, sehingga pengguna yang berekepentingan dan berhak tidak dapat lagi menggunakan layanan tersebut. Menurut (Yoga Adi Pradipta, 2017) ada banyak jenis serangan *DOS* yaitu *SYN Flooding*, *Pentium FOOF Bug*, *Ping Flooding*, *Apache Benchmark*, Menggantung *Socket*, *Input Flooding Attack*, *LAND Attack*, *Smurf Attack*, dan *Tear Drop*. Serangan yang sering menyerang layanan pada server yaitu *SYN Flooding* dimana serangan tersebut menyerang koneksi *TCP* yang terbentuk dengan membanjiri permintaan paket sehingga *server* tidak dapat membalas semua permintaan dan ahirnya *server down* dan layanan pun menjadi tidak dapat di akses.

Keamanan Jaringan

Keamanan Jaringan dapat diartikan sebagai keadaan aman pada suatu susunan yang menjalankan sistem komputer (Abdiansyah,2013). Keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya user yang tidak mempunayi izin (penyusup) dari sistem jaringan komputer. Tujuan dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebauh ancaman yang berupa pengambilan data secara tidak saha atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang berujuan untuk merusak sistem jaringan dari sisi hardware sebuah komputer. Keamanan jaringan dalam aspek keamanan mempunyai 5 aspek yang dijelaskan sebagai berikut:

1) *Confidentiality* yaitu mengharuskan suatu data hanya bisa diakses oleh pengguna yang sah atau memliki izin akses.
2) *Integrity* yaitu mengharuskan suatu data hanya bisa dirubah oleh pengguna yang sah atau memiliki izin wewenang.
3) *Availability* yaitu mengharuskan informasi hanya tersedia bagi pengguna yang sah atau memiliki izin akses untuk kebutuhan tersebut.
4) *Authentication* yaitu mengharusan penerima atau pengirim suatu data dapat dibuktikan dengan identitas yang asli dan tidak palsu yang dapat diidentifikasi.

Nonrepudiation yaitu mengharuskan penerima atau pengirim suatu data tidak dapat menolak adanya pengiriman dan penerimaan pesan.

PfSense

Pfsense merupakan distro *linux* turunan *freebsd*, akan tetapi disesuaikan untuk digunakan sebagai *firewall* dan *router*. Selain menjadi, *platform* yang fleksibel dalam hal *firewall dan routing*, *PfSense* termasuk fitur dan

sistem paket yang memungkinkan *upgrade* lebih lanjut untuk memperbarui fitur dan sistem keamanan yang diterapkan pada *PfSense* tersebut. *PfSense* merupakan proyek populer dengan lebih dari 1 juta *download* sejak awal, dan terbukti dalam *installasi* yang tak terhitung jumlahnya mulai dari jaringan rumah kecil melindungi *PC* dan *Xbox* untuk perusahaan besar seperti universitas dan organisasi lainnya melindungi ribuan perangkat jaringan. Dengan tampilan *web gui administrator* yang sederhana dapat memudahkan *administrator* untuk mengoprasikan *PfSense* meskipun baru belajar *routing* dan *firewall* pada jaringan *local* ataupun *internet.* Kemudian *PfSense* merupakan *opensource* alias *GPL GNU,* yaitu sebuah *software* yang digunakan sebagai alternatif *router, firewall, load balancing,* ataupun *web proxy* dan masih banyak lagi fitur yang diberikan (Wiliamsom, 2005).

Captive Portal

Captive Portal merupakan suatu bentuk teknik autentikasi dan pengamanan data terhadap jaringan *network* internal ke *network* eksternal. *Captive Portal* dapat diartikan sebagai mesin *Router* atau *Gateway* yang membatasi atau tidak mengizinkan adanya trafik sampai *user* melakukan registrasi terlebih dahulu ke dalam sistem. Mekanisme yang diterapkan *Captive Portal* biasanya digunakan pada infrastruktur *wireless* seperti *hotspot* area. Dengan kemudahan *web gui* yang mudah untuk diakses. *Captive Portal* pada *PfSense* memiliki fitur pendukung dalam memanajemen dan mengkonfigurasi aktivitas pada *Captive Portal* (Walt, 2010).

Freeradius

Freeradius merupakan protokol *security* berbasis pada *open source* yang bekerja menggunakan sistem *client-server* dan mendukung *MySQL, Freeradius* digunakan untuk melakukan autentikasi *user* melalui komunikasi antara *client* dan *server* untuk mengakses jaringan (Walt, 2011). Mekanisme tersebut dapat dijelaskan sebagai berikut:

1) *Authentication* merupakan suatu proses pada *client* yang diidentifikasi oleh *server AAA* sebelum *client* menggunakan layanan *internet.* Pada proses tersebut nantinya *client* akan meminta hak akses kepada *NAS (Network Attached Storage).* Kemudian *NAS (Network Attached Storage)* akan mengidentifikasi kepada *server AAA* apakah *client* terdaftar pada layanan *internet* atau tidak.
2) *Authorization* merupakan pengalokasian layanan kepada *client* sebagai hak akses ketika *client* telah terdaftar sebagai pengguna layanan *internet.*
3) *Accounting* merupakan proses yang dilakukan oleh *NAS (Network Attached Storage)* dan *AAA server* untuk mencatat aktivitas *client.* Dari informasi yang diperoleh nantinya proses *accounting* akan disimpan pada *server AAA* yang dapat digunakan seperti auditing atau manajemen jaringan.

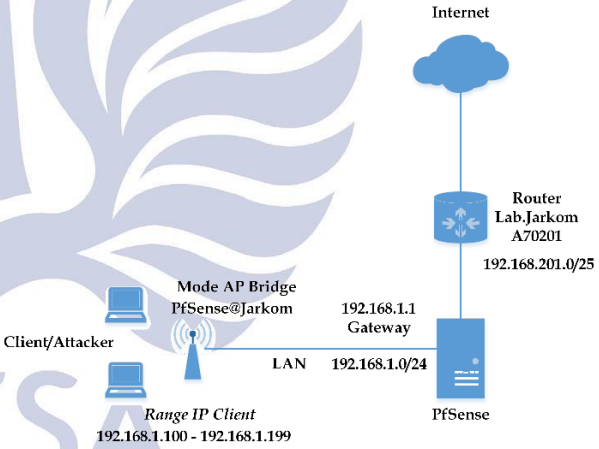
IDS (Intrusion Detection System)

DOS (Denial of Service) merupakan jenis serangan terhadap sebuah komputer atau server di dalam jaringan *internet* dengan cara menghabiskan sumber *(resource)* yang dimiliki. Bentuk umum dari serangan *DOS* ini adalah dengan cara mengirim paket data dalam jumlah yang sangat bersar terhadap suatu *server* dimana *server* tersebut tidak bisa memproses semuanya. Bentuk lain dari serangan *DOS* ini adalah memanfaatkan *port-port* yang rentan dari sistem operasi (Raifudin Rahmat, 2010).

METODE

Arsitektur Sistem

Pada tahapan ini, penulis akan menggambarkan dan menjelaskan mengenai *Captive Portal PfSense* serta topologi jaringan yang digunakan. Berikut adalah topologi jaringan yang digunakan:



Gambar 1. Topologi Jaringan

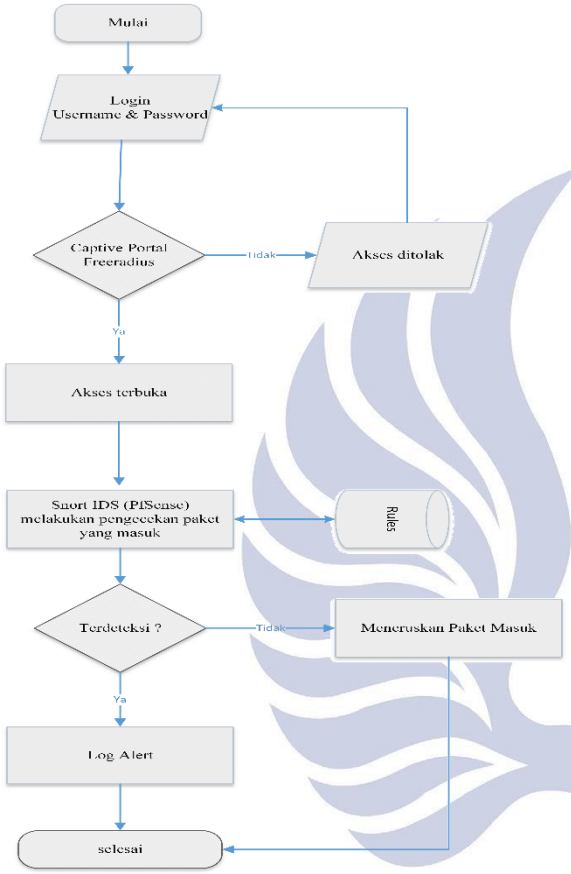
Berikut penjelasan dari topologi jaringan diatas:

1) *Router* Lab.Jarkom A70201 terhubung dengan jaringan *internet* sebagaimana telah dikelola dan dikonfigurasi oleh instansi dengan memberikan *IP Address* 192.168.201.0/25 yang mengarah pada *PC PfSense* secara otomatis *(DHCP).*
2) *PC PfSense* dikonfigurasi sebagai mode *Router* yang terhubung pada *Router* Lab.Jarkom A70201. Ketika *PC PfSense* mendapat *IP Address* 192.168.201.124 sistem *PfSense* akan mengenali *IP* tersebut sebagai *interface WAN* .
3) *LAN PC PfSense* dengan *IP* 192.168.1.1 dikonfigurasi sebagai *DHCP* yang mengarah pada *Access Point* PfSense@Jarkom mempunyai *Network ID* 192.168.1.0/24. Sehingga *client*

mendapat *IP address* dengan *range* 192.168.1.100-192.168.1.199.

4) Mode yang digunakan *Access Point* yaitu *Mode APBridge* sebagai *access point* atau pemancar yang bisa melayani *client* atau bisa disebut *PTMP (Point To Multi Point)* secara otomatis *(DHCP).*

Sistem Kerja



Gambar 2. Sistem Kerja

Sistem kerja ini dirancang untuk menggambarkan bagaimana jalannya *Captive Portal PfSense.* Pada saat *user* berusaha untuk melakukan *browsing* ke *hotspot*, *Captive Portal* akan memaksa pengguna yang belum terautentikasi untuk menuju ke *authentication web Captive Portal* yang akan diberi *prompt login.* Kemudian jika akses ditolak maka user tidak akan bisa mengakses layanan *internet* sampai proses *authentication server* pada *Captive Portal* mengetahui identitas dari pengguna *wireless* yang tersambung, sehingga *wireless gateway* akan dapat menentukan untuk membuka aturan *firewall*-nya. Proses mekanisme *Freeradius* di fungsikan sebagai protokol *connectionless* berbasis *UDP* yang tidak menggunakan koneksi langsung. Artinya jika satu paket *Radius* ditandai dengan *field UDP* menggunakan *port* 1812. Maka pada *transport UDP Radius* memiliki beberapa pemrosesan antara lain otentikasi, otorisasi, dan rinci *accounting*. Kemudian jika *user* mendapat akses layanan *internet*, secara otomatis *Snort IDS (Intrusion Detection System)* akan memonitor lalu lintas pada jaringan bila terjadi serangan terhadap *attacker*. Jika terjadi serangan sistem pada *Snort IDS (Intrusion Detection System)* akan melakukan pengecekan paket berdasarkan *rule* yang telah diaktifkan, apabila paket yang masuk cocok dengan *rule* yang telah diaktifkan maka paket tersebut akan terdeteksi sebagai sebuah serangan dan akan ditampilkan sebuah *log alert*.

Kebutuhan Perangkat

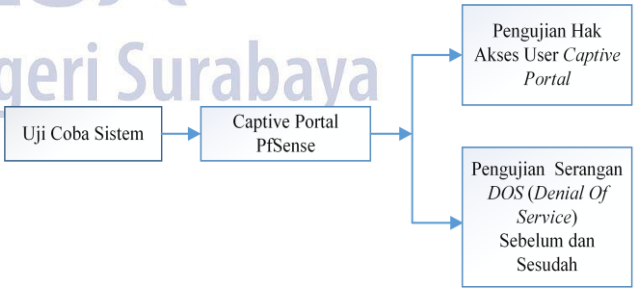
Berikut kebutuhan yang digunakan dalam pembuatan *Captive Portal PfSense*, diantaranya:

Tabel 1. Kebutuhan Perangkat

Sistem Operasi PfSense	Versi CE-2.3.5-RELEASE-i386
Processor	Pentium(R) Dual-Core CPU E5400 @2.70Ghz
RAM	2GB
HDD	250 GB
VGA	Intel HD Graphics
NIC (Ethernet Card) Realtek	Realtek PCI lan card up to 10/100 Mbps
NIC (Ethernet Card) USB	NIC (Ethernet Card) USB lan card up to 10/100 Mbps
Router Mikrotik RB750	LAN port 5, RAM 32 Mb, ArchitectureMIPS-BE, CPU AR7241 400MHz
Wireless Access Point TP-LINK TL-WR720N	Wireless access point speed up to 150Mbps

Skenario Pengujian

Berikut adalah skenario uji coba sistem yang akan dilakukan :



Gambar 3. Skenario Pengujian

1. Pengujian Mekanisme *User Captive Portal*

1) Melakukan pembuatan *user Captive Portal* meliputi *username* dan *password* melalui *Freeradius* yang telah dibuat oleh *admin.*

2) Ketika *client* masuk kedalam *hotspot* PfSense@jarkom, maka akan langsung dialihkan ke halaman *web login* dari *Captive Portal*.
3) *User* melakukan *login* melalui *Captive Portal* dengan *username* dan *password* yang telah dibuat oleh *admin*.
4) Jika *user* dari *Captive Portal* berhasil melakukan *login* maka akan langsung dialihkan oleh sistem *Captive Portal* ke halaman *Direct Google*.
5) Mengetahui *SSL Captive Portal* dengan metode *sniffing* pada aplikasi *Wireshark*.

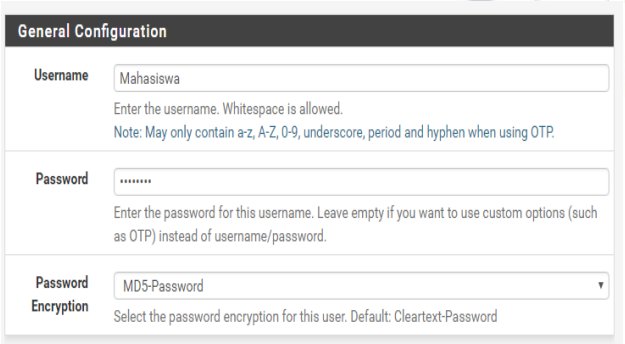
2. Pengujian *Snort IDS (Intrusion Detection System)*

Melakukan pengujian sebelum dan sesudah dengan teknik serangan *DOS (Denial Of Service)* pada protokol *UPD flooding* dan *TCP flooding* dengan menggunakan aplikasi *Hping3 Kali linux* dan *Loic (Low Orbit Ion Cannon)*. Dari proses pengujian dan pengoprasian tersebut nantinya sistem yang sudah diterapkan dengan *Snort IDS (Intrusion Detetction System)* apakah sudah berjalan dengan baik dan benar

HASIL DAN PEMBAHASAN

1. *User* Manajemen

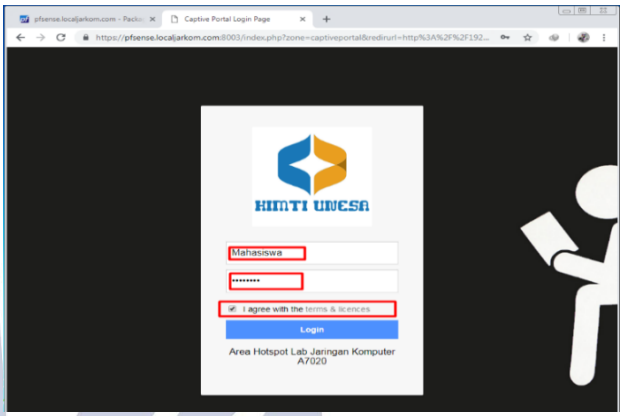
Dalam hal ini seorang *administrator* akan membuat atau mendftarkan *user* baru, dimana *user* tersebut menyimpan data berupa *username* dan *password* yang nantinya akan digunakan dalam melakukan *login hotspot* tersebut, sehingga *user* dapat menggunakan layanan *internet*. Kemudian untuk pembuatan *username* dan *password* dilakukan di *user freeradius*. Buka *tab service*, kemudian masuk pada menu *freeradius* pilih *Add* kemudian beri nama pada *username* "Mahasiswa dan *password* "masukmhs" seperti gambar 4.



Gambar 4. Membuat *User*

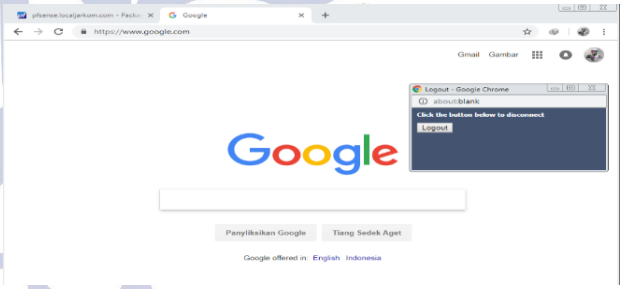
2. *User Login*

Setelah melakukan pembuatan *user* seperti gambar 4. Selanjutnya pengujian dilakukan dengan menyambungkan *PC user* dengan *hotspot* "PfSense@Jarkom" yang secara otomatis mengarahkan ke halaman *web Captive Portal*. Kemuadian masukkan *username* "Mahasiswa" dan *password* "masukmhs", centang pada bagian *"I agree with the theams & licences"* seperti gambar 5. Jika *username* dan *password* salah dalam memasukkan ke dalam *Captive Portal* maka sistem tidak akan mengizinkan *user* untuk mendapatkan layanan akses *internet*.



Gambar 5. Halaman Captive Portal

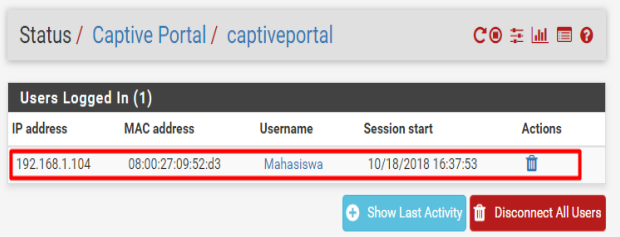
Jika *username* dan *password* benar maka secara otomatis *Captive Portal* akan men-*direct* ke *web www.google.com* dan *user* sudah bisa mengakses layanan *internet* seperti gambar 6.



Gambar 6. *Login* Sukses

3. *Monitoring User*

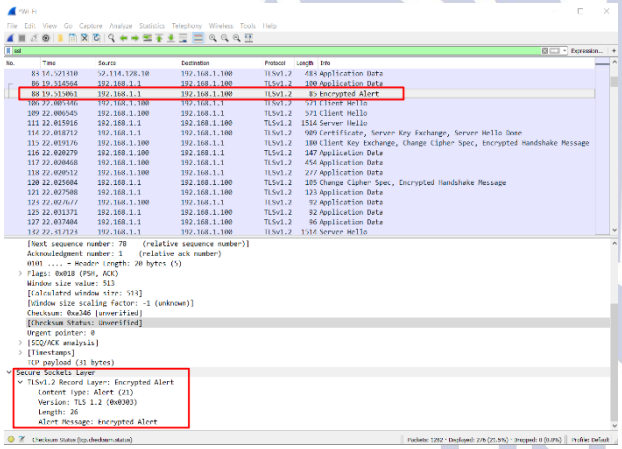
Monitoring user dilakukan untuk melihat siapa saja yang terhubung kedalam jaringan *"valid"* pada *hotspot* "Pfsense@jarkom". Hal ini juga dilakukan untuk mengantisipasi jika ada *client* yang mencurigakan terhubung pada *hostpot* "Pfsense@jarkom" atau tidak. Kemudian jika *user "valid"* artinya *username* dan *password* sesuai dengan yang dibuat *administator* maka pada bagian *status Captive Portal* akan *menunjukan IP address* dan *MAC address*. Begitupun sebaliknya jika tidak ada aktifitas *client* pada *Captive Portal* maka dalam *status Captive Portal* tidak akan menampilkan sebuah informasi seperti gambar 7.



Gambar 7. Informasi *User Valid*

4. *SSL*

Sebagai mekanisme enkripsi pada *web Captive Portal*, terdapat 3 proses dalam mekanisme enkripsi tersebut yang pertama tahap otentikasi *server*, kedua tahap otentikasi *client* dan yang ketiga tahap pemisahan otentikasi dan enkripsi. Yang pertama otentikasi terhadap *user*, ketika user mengirimkan pesan "*client hello"* untuk mengjukan ospi *SSL*. Kemudian *server* tersebut akan memberi respon balasan dengan memilih opsi *SSL* melalui *serverhello*. Dari respon tersebut *server* akan mengirimkan sertifikat kunci pada pesan *certificate* seperti gambar 8.



Gambar 8. Otentikasi *Server*

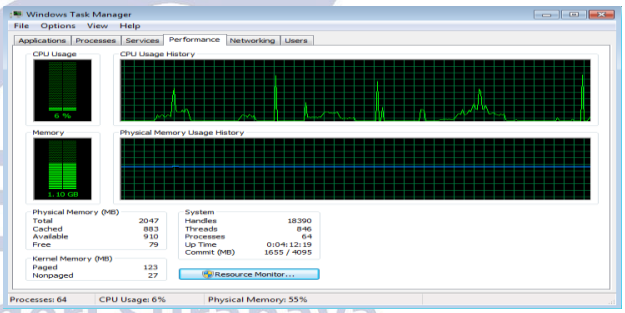
5. Pengujian *DOS (Denial Of Service)*

Langkah ini merupakan pengujian serangan terhadap *Captive Portal* menggunakan *DOS (Denial Of Service)* serta *TCP syn flooding* dan *UDP flooding* sebagai teknik serangan tersebut. Kemudian aplikasi yang akan digunakan sebagai serangan menggunakan *Hping3 Kali linux* dan *Loic (Low Orbit Ion Cannon).* Tujuan dari pengujian serangan yaitu membuat *server* tidak dapat memberikan layanan terhadap komunikasi yang sah karena *server* akan disibukkan dengan banyaknya paket-paket yang terlintas sehingga tidak dapat melayani *service* lain dengan maksimal. Sebagai upaya tindak lanjut dari serangan *DOS (Denial Of Service)* pengujian ini dilakukan dengan mengamati hasil atau alert yang dideteksi oleh *Snort IDS (intrusion Detection System)*. Kemudian dari hasil yang diperoleh nantinya sistem yang sudah diterapkan sebelum dan sesudah menggunakan *IDS (Intrusion Detetction System)* apakah berjalan dengan baik dan benar. Untuk langkah-langkah sebagai berikut :

1) Searangan *UDP FLOOD* merupakan serangan yang bersifat *connectionless* artinya mengurangi sambungan terhadap target yang akan diserang. *Flood attack* ini bekerja pada *protocol UDP* dengan membanjiri *port* secara acak dalam jumlah besar. Skenario mekanisme penyerangan ini nantinya akan mengirimkan paket *DOS* antara 2 *client*, *client* A bertindak sebagai target dengan *IP* 192.168.1.1, sedangkan *client* B bertindak sebagai *attacker* dengan *IP* 192.168.1.109 *Kali Linux*.

a. Kondisi Awal

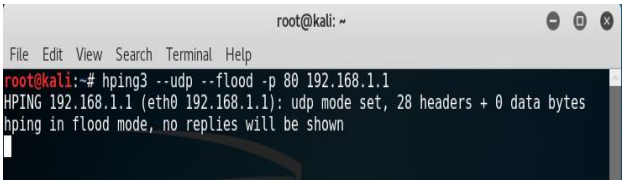
Penyerangan dilakukan pada *Host PfSense IP* 192.168.1.1 penyerangan tersebut dilakukan untuk melihat *peformance* katika *client* A dengan *IP* 192.168.1.101 sedang terhubung dengan layanan *Captive Portal*. Pada kondisi awal ketika memasuki *Captive Portal* normal artinya tidak terjadi permasalahan pada koneksi jaringan. Presentase *peformance* pada *PC client* A gambar 136 menunjukan *traffic CPU* 6% dan *RAM* 55% dimana *RAM avaible* 910 *Mb* dan *Cached* 883 *Mb* artinya kondisi tersebut bisa dikatakan normal. Hal ini juga ditunjukkan dengan kondisi *peformance host PfSense* pada CPU usage 7% seperti gambar 9.



Gambar 9. Kondisi Awal *Peformance* Komputer Target

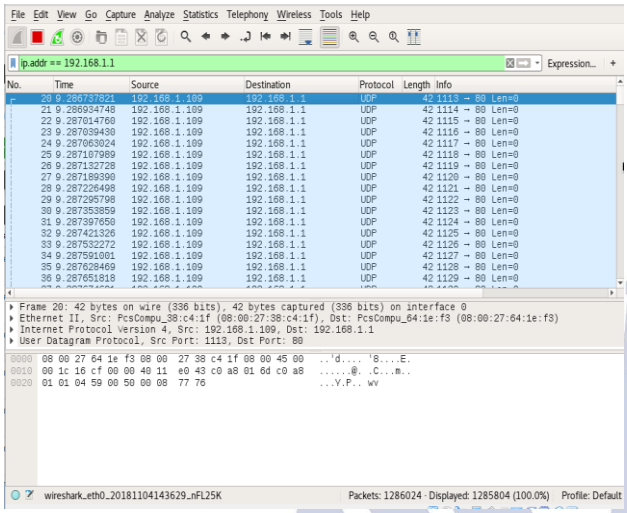
b. Proses Serangan

Buka terminal pada *kali linux*, dengan perintah (hping3 --UDP –-flood -p 80 192.168.1.1) 80 merupakan identitas *port* dan 192.168.1.1 sebagai target *IP* yang akan diserang gambar 10. Dan berikut hasil perintah serangan *DOS* yang dilakukan.



Gambar 10. Pernyataan Pertama

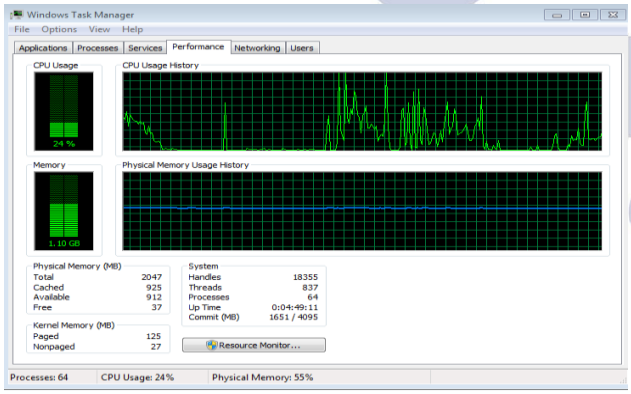
Pada tampilan gambar *wireshark* 11, dapat dilihat paket yang dikirim *attacker* dengan *IP* 192.168.1.109 mengarah pada *IP* 192.168.1.1 dengan *status protocol UDP* pada *port 80* dari jaringan target. Kemudian paket yang dikirim mencapai 1286024 dan itu akan terus bertambah selama *DOS Attack* masih berjalan.



Gambar 11. *Capture* Paket *Pada Wireshark*

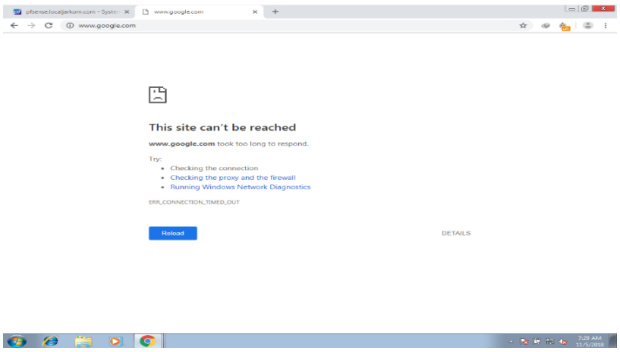
c. Kondisi Akhir

Karena *packet UDP* tersebut di *spoofing* oleh *PC attacker* tersebut, maka yang terjadi adalah banyaknya *packet* yang dikirim oleh seorang *attacker* tanpa henti yang tidak berguna bagi *PC* target. Dampak yang terjadi *connectionless* dan mempengaruhi presentase pada *CPU* yang meningkat menjadi 24 % dan *RAM* 55 % *avaible* 912 *Mb*, *Cached* 925 *Mb* seperti gambar 12 hal ini mempengaruhi komputer menjadi tidak stabil dan terkesan lama.



Gambar 12. Kondisi Akhir *Performance* Komputer Target

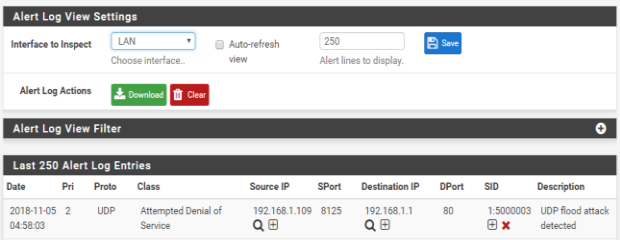
Dampak serangan tersebut juga mengakibatkan putusnya koneksi layanan *internet* dengan ditandai "*This site can't be reached*" pada komputer target seperti gambar 13.



Gambar 13. Layanan *Internet* Terputus

a. Hasil Alert

Hasil *alert* terlihat *protocol* yang terdeteksi yaitu *UDP*, kemudian *type class* serangan yang dihasilkan *Attempted Denial Of Service* dan *source IP* merupakan *IP attacker* yang menyerang *IP 192.168.1.1* pada *destination IP* dengan *port* 80 yang dilaluinya seperti gambar 14.



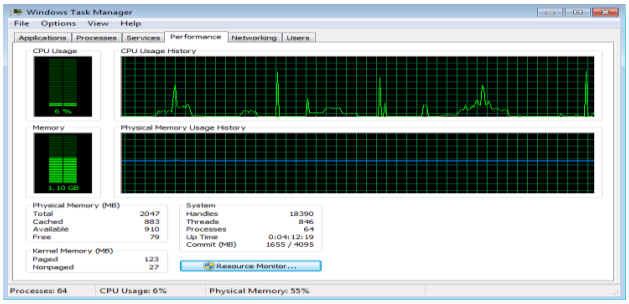
Gambar 14. Hasil *Alert UDP Floodimg*

2) Selanjutnya yaitu menguji dengan *serangan TCP Flooding* dengan *LOIC Low Orbit Ion Cannon*. *TCP Flooding* merupakan serangan *DOS* yang memanfaatkan *"loophole"* pada saat koneksi *TCP/IP* terbentuk. Mekanisme dari *TCP Flooding* ini ketika *client* akan mengirimkan paket data berupa *SYN* untuk mensinkronasikan kepada *server*, kemudian *server* menerima *request* dari *client* dan akan memberikan jawaban ke *client* berupa *ACK* (*Acknowledgement*) sebagai tanda pengiriman dan penerimaan data maka *client* akan kembali mengirimkan kembali sebuah paket *SYN* secara berulangkali.

a. Kondisi Awal

Dalam hal ini target yang akan diserang yaitu *host PfSense IP* 192.168.1.1 kemudian *IP* 192.168.1.120 bertindak sebagai *attacker*. Sama dengan mekanisme sebelumnya ketika *client* memasuki *Captive Portal* normal artinya tidak terjadi putusnya koneksi layanan *internet*. Presentase *peformance* komputer *client* gambar 124 menunjukan *traffic CPU* 6% dan *RAM* 55% dimana *RAM avaible* 910 *Mb* dan *Cached* 883 *Mb* artinya kondisi tersebut bisa dikatakan normal. Hal ini juga ditunjukkan pada *host PfSense CPU*

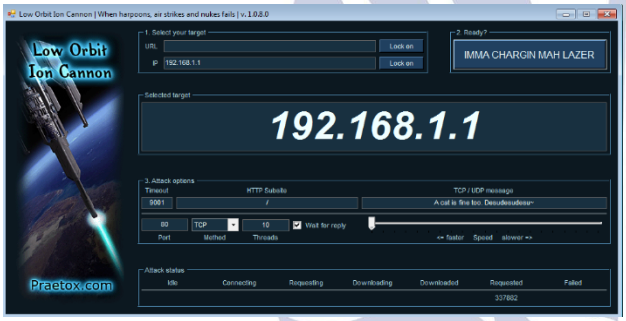
dengan presentase 9% yang normal pada gambar 15.



Gambar 15. Kondisi Awal *Peformance* Komputer Target

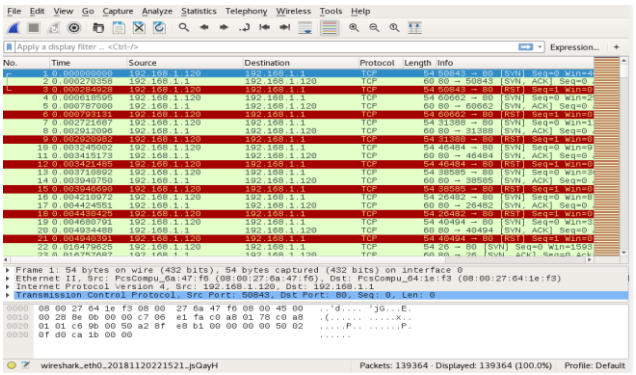
b. Proses Serangan

Select your target IP 192.168.1.1 sebagai terget *client* yang diserang. Kemudian *Lock on* dan akan tampil *IP* target yang akan dituju. Pilih *Method TCP* sebagai target p*rotocol* yang akan dilalui. Setelah semua telah ter-*setting*, klik pada bagian *IMMA CHARGIN MAH LAZER* untuk memulai penyerangan seperti gambar 16.



Gambar 16. *DOS* Menggunakan *Loic*

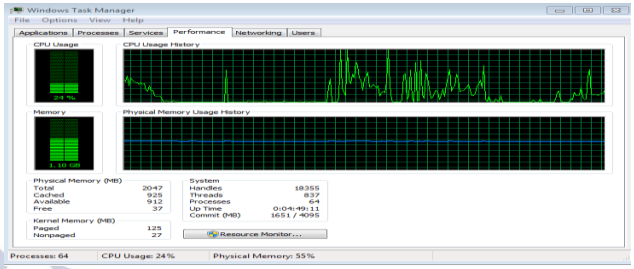
Dapat dilihat pada hasil *capture wireshark* gambar 17 bahwa *IP* 192.168.1.120 mengirimkan permintaan *SYN* ke *server*. Kemudian *server* dengan *IP* 192.168.1.1 memberi jawaban *SYN-ACK* ke *client IP* 192.168.1.1120 dengan menggunakan *TCP port* 80 sebagai *packet* yang dilaluinya. Kemudian dalam mekanisme tersebut *client* banyak mengirimkan *SYN* dan *server* banyak menjawab *SYN-ACK* tetapi *client* tidak menerima *ACK* sehingga *server* mempunyai status yang menggantung hal tersebut bisa menyebabkan sistem *down*.



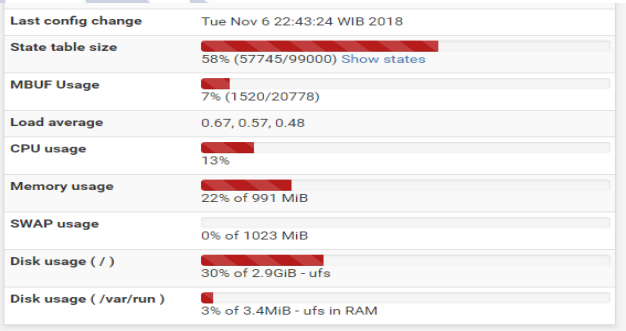
Gambar 17. *Capturing* Packet *Pada* Wireshark

c. Kondisi Akhir

Presentase pada *CPU* yang meningkat menjadi 24 % dan *RAM* 55 % *avaible* 912 *Mb*, *Cached* 925 *Mb*. Pada gambar 18 kondisi ini juga dipengaruhi pada *Host PfSense State table size* mengalami peningkatan dengan presentase 58%, CPU 13% dan *Memory usage* 22% seperti gambar 19 berikut:



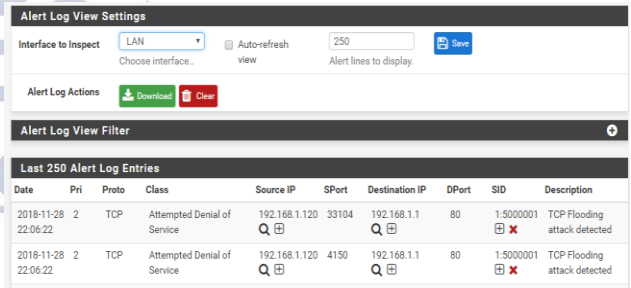
Gambar 18. Kondisi Akhir *Performance* Komputer Target



Gambar 19. Kondisi Akhir *Host PfSens*

d. Hasil Alert

Hasil *alert* terlihat *protocol* yang terdeteksi yaitu *TCP Flooding*, kemudian *type class* serangan yang dihasilkan *Attempted Denial Of Service* dan *source IP* merupakan *IP attacker* yang menyerang *IP 192.168.1.1* pada *destination IP* dengan *port* 80 yang dilaluinya seperti gambar 20.



Gambar 20. Hasil *Alert TCP Floodimg*

PENUTUP

Simpulan

Setelah melakukan impelementasi *Captive Portal* menggunakan *PfSense* dari semua konfigurasi dan pengujian maka didapatkan beberapa kesimpulan yaitu Dengan adanya mekanisme otentikasi *Captive Portal* pada *hotspot*, *user* diwajibkan untuk melakukan *login*

menggunakan *username* dan *password* sehingga *user* yang terdaftar dapat terkoneksi kedalam jaringan *wireless*. Sistem *Radius* pada *Captive Portal* berfungsi sebagai akses kontrol dimana untuk mengecek dan mengauntentikasi *user* atau pengguna berdasarkan mekanisme autentikasi dengan menggunakan metode *challenge/response*. Pada *SSL* yang dibuat di internal *certificate manager PfSense* berfungsi sebagai enkripsi pada *protocol HTTPS Captive Portal*. Implementasi kemanan *Snort IDS Intrusion Detection System* di *PfSense, rules* yang dibuat dapat mendeteksi serangan *DOS (Denial Of Service)* pada *TCP flooding* dan *UDP flooding* yang hanya menghasilkan *alert* jika terjadi serangan oleh *attacker*.

Saran

Dalam penerapan *ssl* dan sertifikat yang dibuat di *PfSense* masih diperlukan pemasangan sertifikat terhadap *user*. Maka dari itu perlunya *SSL* bersifat *public* artinya *domain* dengan *SSL* yang telah di *hosting*. Kemudian penggunaan *proxy* salah satu alternatif untuk *user* mempermudah melakukan proses pemasangan sertifikat tersebut. Penerapan *Captive Portal* pada *PfSense* mempunyai beberapa mekanisme untuk diterapkan sepertihalnya *Local Voucer User* merupakan pengganti mekanisme *Package Freeradius* yang telah disediakan *PfSense* tanpa harus *mendownload* terlebih dahulu *package* tersebut. Penerapan mekanisme keamanan *IDS* pada *PfSense* seharusnya bisa dikembangkan menjadi *IPS* karena *IPS* bisa memblokir aktivitas *attacker* yang ingin menyalahgunakan layanan *captive portal* tersebut.

DAFTAR PUSTAKA

Abdiansyah, "Definisi Keamanan Jaringan Komputer,"2013.[Online].Available:https://nugi.biz/2013/05/05/definisikeamananjaringan-komputer.xhtml. [Accessed 16 Maret 2018].

Arifin, Z., 2005 Langkah Mudah membangun Jaringan Komputer. Yogyakarta: Penerbit Andi.

Arifin, Z., 2006. Mengenal Wireless LAN. Yogyakarta: Penerbit Andi.

Dwi Kuswanto, "Unjuk Kerja Intrusion Prevention Sistem (Ips) Berbasis Suricata Pada Jaringan Lokal Area Network Laboratorium Tia+ Teknik Informatika, Universitas Trunojoyo," Jurnal Ilmiah NERO, vol. I, no. 2, pp. 73-81, 2014.

Eichel, Z., 2008. *Attacking ASWB Backtrack*. Versi 2 ed. Jakarta: PT.pinhard indonesia.

F. Seventeen, "Aspek Yang Meliputi Sistem Keamanan Jaringan Komputer," 2016. [Online]. Available: https://www.galitekno.com/2016/10/aspek-yangmeliputi-sistem-keamanan.html. [Accessed 15 Maret 2018].

Muis Rajib, "Analisa dan perancangan wireless security menggunakan WPA Radius. Jurnal sskripsi teknik informatika 1431 H./2010.

Seventeen, F., 2016 Aspek Yang Meliputi Sistem Keamanan Jaringan Komputer. [Online] Avaible at: https://www.galitekno.com/2016/10/aspek-yang-meliputi-sistem-keamanan.html [Assceseed 20 April 2018].

Walt, D.v., 2011. *Manage your network resources with freeradius.* Birmingham: Packt Publishing Ltd

Yoga W. Pradipta, "Iplementasi Intrusion Prevention System (IPS) Menggunakan SNORT Dan IP Tables Berbasis Linux," Jural Manajemen Informatika, vol. VII, no. 1, pp. 21-28, 2017.

Wiliamson, M., 2005. PfSense 2 Coockbook Birmingham: Packt Publishing.Ltd. Yurindra, 2017. *Software Engineering.* Yogyakarta: Deepublish.