Jurnal CoreIT, Vol.6, No.1, Juni 2020
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Implementasi Sistem Keamanan Hotspot Jaringan Menggunakan Metode OpenSSL (Secure Socket Layer)

M. Syaiful Anam[1], Dedy Hermanto[2]
[1]Teknik Informatika, STMIK GI MDP, [2]Teknik Komputer, AMIK MDP
Jl. Rajawali No 14, Palembang 30113
syaifulanam@mhs.mdp.ac.id[1], dedy@mdp.ac.id[2]

***Abstrak* – Keamanan jaringan wireless pada perangkat access point yang sering digunakan adalah metode WEP/WPA/WPA2. Hampir semua pengguna jaringan wireless rata-rata mengimplemetasikan perangkat access pointnya dengan menggunakan metode tersebut. Metode tersebut dikenal baik dalam hal kemampuan pengamanan security jaringan wireless tetapi metode WEP/WPA/ WPA2 masih bisa ditembus oleh aplikasi hacking dengan metode brute-force attack dan dictionary. Proses penelitian ini menggunakan metode action research, yang bertujuan untuk mengembangkan metode kerja yang paling efisien. Dimana akan dilakukan diagnosa, rencana tindakan, tindakan, evaluasi, dan pembelajaran. Salah satu solusi keamanan wireless hotspot adalah dengan menerapkan Metode SSL (Secure Socket Layer). Metode SSL (Secure Socket Layer) telah banyak digunakan untuk pengamanan website yang membutuhkan pengamanan tingkat tinggi seperti website perbankan, hosting, jual beli online dan sebagainya yang biasanya pada website tersebut menggunakan protocol HTTPS (Hyper Text Transfer Protocol Secure). Proses pengujian yaitu sniffing, untuk membobol user dan password login dan konsep duplikasi mac address atau yang dikenal dengan nama ARP spoofing dalam pengujian keamanan jaringan wireless dengan metode Secure Socket Layer (SSL). Hasil yang diperoleh bahwa sistem ini dapat mengamankan jaringan hotspot internet dengan lebih aman dan tidak mudah untuk di tembus.**

Kata Kunci – Mikrotik, Brute-Force Attack, WEP/WPA/WPA2, ARP Spoofing, Secure Socket Layer (SSL)

PENDAHULUAN

Teknologi *wireless* merupakan teknologi yang utama di bidang telekomunikasi. *Wireless* sudah banyak sekali diterapkan jaringan komputer, yang lebih dikenal dengan *WLAN (Wireless Local Area Network)* [6]. *WLAN* mempunyai daya tarik tersendiri bagi para pengguna komputer. Teknologi ini sebagai suatu akses jaringan komputer atau informasi (internet). Pengguna *WLAN* mengalami peningkatan yang begitu pesat seiring dengan peningkatan jumlah pemasangan *AP (Access Point)* ditempat - tempat umum. *WLAN* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Teknologi *wireless* sangat mudah untuk digunakan dan pengguna bisa saling berkomunikasi antar jaringan selama masih berada dalam jangkauan *wireless*.

Keamanan jaringan *wireless* pada perangkat *AP (Access Point)* metode pengamanan yang sering digunakan adalah *WEP (Wired Equivalent Privacy)*, *WPA (WI-FI Protected Access)*, dan *WPA2 (WI-FI Protected Access 2)*, dan hampir semua pengguna jaringan *wireless* rata-rata mengguanakan perangkat *APnya* dengan menggunakan metode tersebut [10]. Dari hasil penelitian Muis Rajab pada tahun 2010 dan Imam Bayu pada tahun 2017 , Metode yang sering digunakan tersebut dikenal baik dalam hal kemampuan pengamanan jaringan *wireless*, tetapi metode *WEP*, *WPA*, dan *WPA2* masih bisa ditembus memakai aplikasi atau yang sering disebut *software hacking* dengan metode *brute-force attack* dan *dictionary*, dimana aplikasi atau *software* itu banyak terdapat di internet dan kelemahan berikutnya adalah metode tersebut hanya menggunakan *password* saat akan terkoneksi perangkat *AP* sehingga metode tersebut mudah tersebarnya *password* jika salah satu pengguna atau *user* memberikan *password*nya kepada pengguna atau *user* lain dan mudah diketahui oleh pengguna atau *user* lain begitu seterusnya. Oleh karena itu diperlukan sebuah sistem yang dapat meningkatkan sistem keamanan *wireless hostpot.*[1, 2]

Solusi keamanan *wireless hotspot* adalah dengan menerapkan Metode *SSL (Secure Socket Layer)*. Metode *Secure Socket Layer* telah banyak digunakan dalam pengamanan *website* atau situs *web* yang membutuhkan pengamanan tingkat tinggi seperti *website* perbankan, *hosting*, jual beli *online* dan sebagainya yang biasanya pada *website* tersebut

menggunakan *protocol HTTPS (Hyper Text Transfer Protocol Secure)*

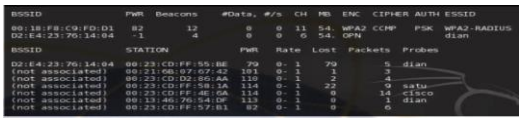
METODE PENELITIAN

Metode yang digunakan untuk melakukan implementasi sistem keamanan hotspot dengan menggunakan SSL yaitu menggunakan *Action Reseacrh* [5].

A. Diagnosing

Tahap awal ini dilakukan kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*. Permasalahan yang sering terjadi sistem koneksi keamanan *wireless* yang terdapat pada *access point* yaitu menggunakan metode *WEP/WPA/WPA2* dimana hasil penelitian Muis Rajab pada tahun 2010 dan Imam Bayu pada tahun 2017, Dimana metode tersebut dikenal baik dalam hal kemampuan pengamanan jaringan *wireless*, tetapi metode *WEP/WPA/WPA2* masih bisa ditembus memakai aplikasi dan metode tersebut masih menggunakan *password*, sehingga *password* tersebut mudah tersebar dan mudah diketahui oleh pengguna lain.

Mencari informasi jaringan *wireless* yang hendak di*hack* dengan menjalankan program *scanner Airodump-ng* dan cari informasi jaringan yang diperlukan seperti Gambar 1 berikut

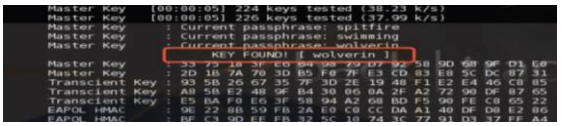


Gambar 1 Informasi Jaringan yang Ditampilkan *Airodump-ng*

Untuk mendapatkan paket *handshake*, seorang *hacker* harus menunggu pengguna melakukan koneksi ke *access point*. Untuk melakukan proses *cracking* hanya dibutuhkan satu paket *handshake* dengan menjalankan program *airodump-ng* dengan memasukkan informasi *channel* dari jaringan *wireless* disertai dengan nama *file* tempat menyimpan paket data yang terlihat.

Gambar 2 Informasi Jaringan oleh *Airodump-ng*

Untuk melakukan proses *cracking password* digunakan program *aircrack-ng* dan sebuah file *dictionary* atau *file* yang berisi *passphrase*. Selanjutnya *aircrack* akan mencoba melakukan *cracking* terhadap *file.cap* untuk mendapatkan *passphrase* yang digunakan oleh *WPA/WPA2*, bila ditemukan *password* maka akan tampil tulisan *" KEY FOUND"* seperti pada Gambar 3.



Gambar 3 Cracking Password WPA/WPA2 Berhasil

B. Action Planning

Penulis melakukan perancangan terhadap sistem jaringan hotspot yang akan dibangun berupa persiapan peralatan *hardware* dan *software* yang dibutuhkan dengan tujuan untuk mengimplementasikan sistem keamanan *wireless internet hotspot* dengan menggunakan metode *security secure socket layer (SSL)*.

Kebutuhan alat dan bahan komponen yang terdapat pada sistem ini meliputi kebutuhan *hardware* dan *software* yang akan digunakan untuk saling mendukung satu sama lainnya.

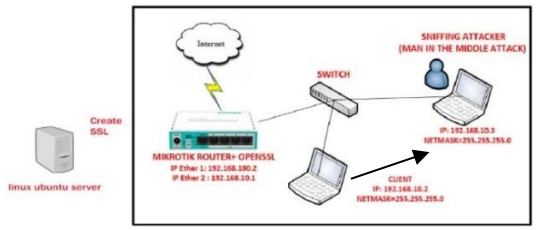
1. Analisis Kebutuhan
   Kebutuhan alat dan bahan komponen yang terdapat pada sistem ini meliputi kebutuhan *hardware* dan *software* yang akan digunakan untuk saling mendukung satu sama lainnya. Berikut kebutuhan alat dan bahan komponen pada Table 1

Tabel 1 Kebutuhan Alat dan Bahan Komponen

Kebutuhan *Hardware*	**Kebutuhan *Software***
Mikrotik RouterBoard RB750.	*Mikrotik Router OS*
CPU Linux Ubuntu Server.	*Linux Ubuntu Server*
Komputer Penguji.	*OpenSSL*
Laptop Pengguna/*Client*.	*Google Chrome*
Kabel *UTP* (*Unshielded Twisted Pair).*	*Wireshark*
Modem Internet.	*Ettercap*
Switch Hub.	*NetCut*

2. Topologi Pengujian
   Pada tahap ini dilakukan perancangan sistem dengan menggunakan *Mikrotik Router Board RB750* sebagai operasi sistem *Router* dan *Openssl* dengan menggunakan *Linux Ubuntu Server*. Topologi jaringan adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan. Perancangan topologi menggunakan sebuah *Mikrotik Router Board RB750* dengan dua *interface network ether1* dan *ether2.*

Interface ether1 diberi *IP address network* 192.168.100.2/24 yang terhubung dengan sebuah *Modem Router indihome Telkom* dengan *IP address* 192.168.100.1/24. Sedangkan *ether2* diberi *IP address network* 192.168.10.1/24 yang terhubung dengan pengguna melalui perantara *switch.* Untuk pengguna diberi *IP address* secara dinamis menggunakan *DHCP Server (Dynamic Host Configuration Protocol)* dengan *network* 192.168.10.0/24 .



Gambar 4 Topologi Pengujian

C. Action Taking

Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya dengan model dibuat berdasarkan sketsa infrastruktur jaringan *wireless* dilanjutkan dengan melakukan analisis terhadap sistem yang sedang berjalan dengan melakukan proses pengambilan data dan analisa sistem keamanan *wireless hotspot* dengan metode *security secure socket layer (SSL)* menggunakan aplikasi *wireshark*.

1. Membuat File Sertifikat dan File Kunci

   Implementasi *Server Router Mikrotik* menggunakan *mikrotik routerboard RB 750* kemudian membuat *file* sertifikat dan *file* kunci di sistem operasi *linux* dengan menggunakan *software openssl*. Untuk dapat membuat sertifikat diperlukan aplikasi *openssl* dengan menggunakan perintah *apt-get install* , dan kemudian membuat kunci *hotspot* dengan nama *hotspotssl.key* seperti pada Gambar 5.

```
root@serverdata:/# apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 123 not upgraded.
root@serverdata:/#
```

Gambar 5 *Installasi Openssl*

Perintah *genrsa* digunakan untuk menciptakan sepasang *key*, *des3* menunjukkan bahwa *private key* harus dienkripsi dan dilindungi oleh *passphrase*, *out* menunjukkan *filename* yang akan menyimpan hasil *output*, 1024 menunjukkan jumlah *bit* dari *key* yang dibuat, Kemudian menggunakan perintah openssl membuat *file key* dan *file CSR* dimana *CSR* ini kependekan dari *certificate signing request.* Seperti pada Gambar 6 dan Gambar 7.

```
root@serverdata:/# openssl genrsa -des3 -out hotspotssl.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................................++++++
.........++++++
e is 65537 (0x10001)
Enter pass phrase for hotspotssl.key:
Verifying - Enter pass phrase for hotspotssl.key:
root@serverdata:/#
```

Gambar 6 Membuat *File Kunci.*

```
root@serverdata:/# openssl req -new -key hotspotssl.key -out hotspotssl.csr
Enter pass phrase for hotspotssl.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:id
State or Province Name (full name) [Some-State]:sumsel
Locality Name (eg, city) []:palembang
Organization Name (eg, company) [Internet Widgits Pty Ltd]:stmik_mdp
Organizational Unit Name (eg, section) []:192.168.1.1
Common Name (e.g. server FQDN or YOUR name) []:192.168.1.1
Email Address []:admin@mikrotik.co.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
root@serverdata:/#
```

Gambar 7 Membuat Kunci *Request.*

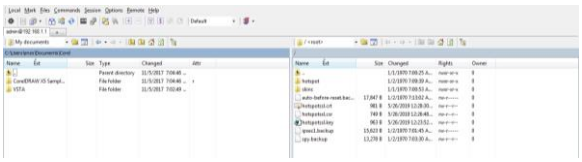
Perintah untuk *operasi SSL* menggunakan *req - X.509* yaitu *certificate signing request* (*CSR*), *X.509 - self-signed*, kemudian *days* 10000 untuk validasi selama 10000 hari atau 3 tahun, Perintah *keyout* merupakan nama *outfile* dari *private key* yang dibuat sedangkan *out* merupakan nama *certificate file* yang dibuat.

```
root@serverdata:/# openssl x509 -req -days 10000 -in hotspotssl.csr -signkey hotspotssl.key -out hotspot
ssl.crt
Signature ok
subject=/C=id/ST=sumsel/L=palembang/O=stmik_mdp/OU=192.168.1.1/CN=192.168.1.1/emailAddress=admin@mikroti
k.co.id
Getting Private key
Enter pass phrase for hotspotssl.key:
root@serverdata:/#
```

Gambar 8 Membuat File Sertifikat dan File Kunci

2. Import File Sertifikat dan File Kunci

   Unggah file sertifikat dan *file* kunci (*key*) yang telah di buat dengan menggunakan aplikasi *winscp* ke *server mikrotik*. Setelah proses *upload* selesai maka menggunakan perintah *file print* untuk melihat hasil *upload file* sertifikat dan *file* kunci (*key*) di *server mikrotik*, seperti pada Gambar 9

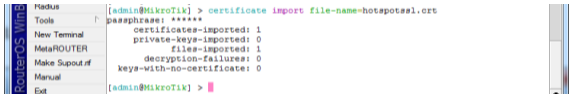


Gambar 9 Unggah Certificate dan Key Security Hotspot Mikrotik

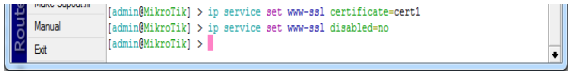
3. Pemasangan File Sertifikat dan File Kunci

   Kemudian installasi file kunci (*key*) yang telah dibuat di*mikrotik router* dengan menggunakan perintah *certificate import* kemudian

mengaktifkan *service www-ssl* agar *server mikrotik support ssl* setelah itu *setting* menggunakan *file* sertifikat yang telah dibuat sebelumnya seperti pada Gambar 10 dan Gambar 11

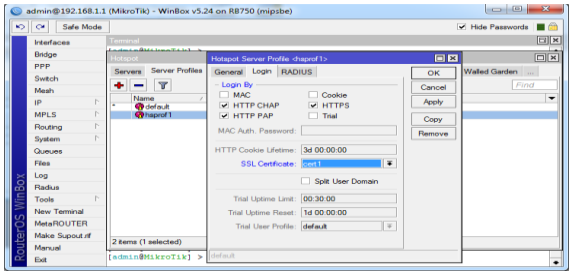


Gambar 10 Mengimpor File Certificate



Gambar 11 Mengaktifkan Service SSL Menggunakan Certificate

Pada gambar dibawah ini merupakan konfigurasi *service www-ssl* pada *aplikasi winbox*. seperti pada Gambar 12



Gambar 12 Mengaktifkan *Service SSL* Menggunakan *Certificate*

D. Evaluating

Dari hasil implementasi jaringan *wireless hotspot* yang memakai metode *secure socket layer (SSL)* dan akan di analisis keamanan menggunakan Menggunakan *Wireshark*, *enttercap* dan *netcut* yang akan di evaluasi mengenai kelebihan sistem keamanan yang dibangun.

E. Learning/Reflacting

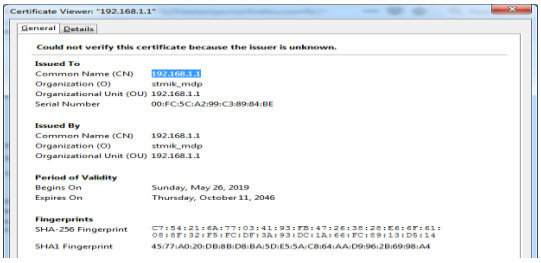
Setelah semuanya selesai, maka tahap akhir adalah peneliti melaksanakan *review* atau kesimpulan tahap demi tahap kemudian penelitian ini dapat berakhir. Seluruh perubahan dalam situasi akan dievaluasi oleh peneliti. Lalu hasilnya juga mempertimbangkan untuk tindakan kedepan.[11]

HASIL DAN PEMBAHASAN

Proses pengujian yang dilakukan dalam penelitian ini, dengan menggunakan login Hotspot mikrotik melalui browser. Login hotspot mikrotik yang digunakan telah menggunakan fasilitas *secure socket layer*, hal ini tampak pada *url login* yaitu https://192.168.1.

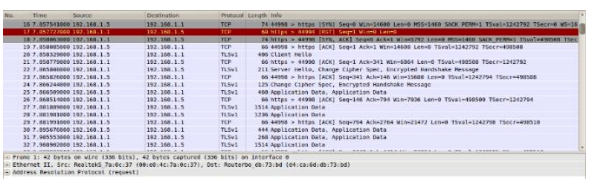
Gambar 13 Tampilan *Login Hotspot Mikrotik*

Pada Gambar 14 merupakan informasi halaman *hotspot login* identitas *website* berupa *ip address* atau nama domain, kepemilikan *website*, verifikasi dan waktu *expire security SSL*. Dari info tersebut diperoleh informasi bahwa *web login* telah terenkripsi menggunakan *security SSL*.

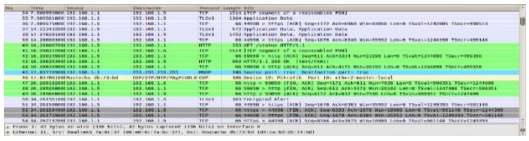


Gambar 14 Tampilan Identitas Login SSL

Protokol *SSL* mengotentikasi *server* kepada *client* menggunakan kriptografi kunci publik dan sertifikat digital. Untuk mengaktifkan *SSL* pada halaman *login mikrotik* perlu memasang sertifikat *SSL* yang sesuai dengan *server* dan halaman *web login* mikrotik hotspot. Setelah *SSL* terpasang, maka *URL* login mikrotik hotspot yang sebelumnya *http://* menjadi *https://*. Pada Gambar 15. dan 16 merupakan hasil *capture* menggunakan aplikasi *wireshark*, hasil yang diperoleh adalah *ip address* yang didapat *client hotspot* yaitu 192.168.1.5 kemudian dapat dilihat paket data yang bertipe *SSL* sedang melakukan *handshake protocol* yaitu *client hello*. Setelah melakukan *handshake Client Hello*, paket dilanjutkan dengan *server Hello*, kemudian sertifikat dikirim. Paket data jaringan yang telah menggunakan *SSL* berimplikasikan pada terenkripsinya seluruh data yang ditransfer antara *server* dan *client*.

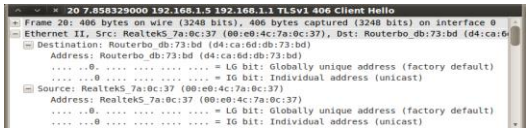


Gambar 15 Tampilan Protocol TLS



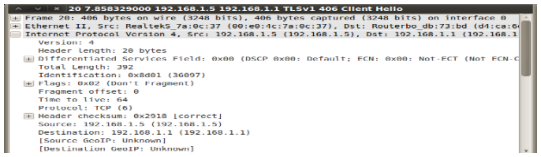
Gambar 16 Tampilan Enkripsi SSL

Pada baris *Ethernet II* menunjukan *client* sumber (*Source*) dengan *mac address* 00:E0:4C:7A:0C:37 melakukan koneksi ke *server routerboard mikrotik* (*Destination*) dengan informasi *mac address* D4:CA:6D:DB:73:BD seperti pada Gambar 17



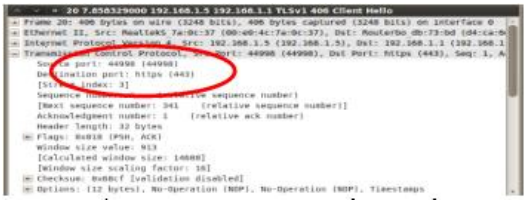
Gambar 17 Ethernet Protocol Wireshark

Saat terkoneksi pada *server hotspot* dengan *ip address* 192.168.1.1 diperoleh *ip address client* melalui *DHCP Server* dengan *ip address* 192.168.1.5 dengan menggunakan *ip versi 4*, dengan *header length* 20 *bytes* seperti pada Gambar 18



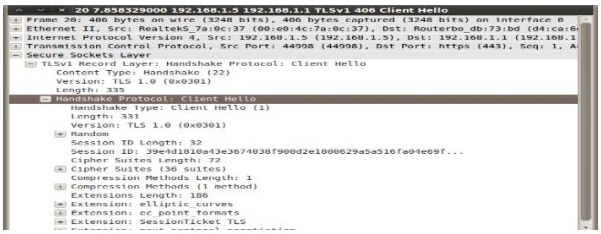
Gambar 18 Internet Protocol Wireshark

Pada baris *Transmission Control Protocol* diperoleh informasi dimana *client* menggunakan *port* 44998, melakukan koneksi ke *server hotspot* dengan *port* tujuan 443 yaitu *port https*, dimana *port https* merupakan protokol komunikasi data antara *server* dan *web client* (*browser*) yang telah terenkripsi sedangkan *port http* yaitu *port* 80 , untuk transmisi data tidak aman karena tidak terenkripsi. Seperti pada Gambar 19



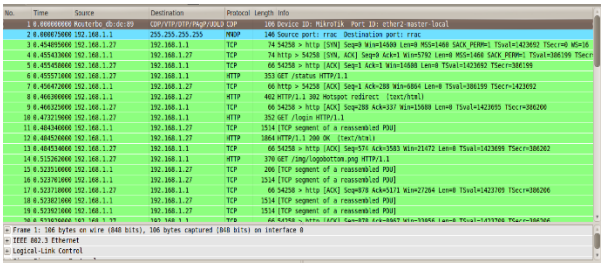
Gambar 19 Transmission Control Protocol

Pada Gambar 20 diperoleh informasi dimana *server* mengirim informasi paket *SSL* ke *client* , dikenal dengan transaksi *handshake*, setelah saling bertukar kunci (*key*), kemudian paket data dikirim melalui *SSL* pada bagian *encrypted application* data dapat terlihat data sudah terenkripsi, untuk melakukan desripsi paket data diperlukan *private key*.



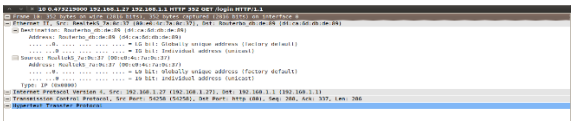
Gambar 20 Paket Header Secure Sockets Layer

Sebagai hasil perbandingan jika *wireless hotspot* tidak menggunakan *protocol* atau keamanan *Secure Sockets Layer (SSL)* pada aplikasi *network forensic wireshark* akan tampil seperti pada Gambar 21, dimana saat *user login* pertama kali akan muncul *protocol login http://* yang menggunakan *port* 80, dimana pada keterangan pada baris pertama diperoleh informasi bahwa *client hotspot* terhubung dengan mikrotik *routerboard* melalui port *ether2-master-local*, adapun *ip address* yang diperoleh melalui *DHCP Server hotspot mikrotik* yaitu 192.168.1.27 dengan *gateway routerboard* menggunakan *ip address* 192.168.1.1.



Gambar 21 Paket Header Tanpa Secure Sockets Layer

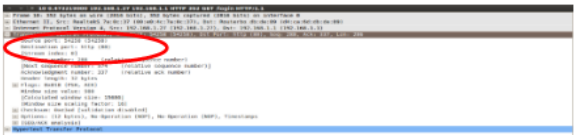
Pada paket *Header Ethernet Protocol* diperoleh informasi identitas *mac address* atau *physical address wireless ethernet client hotspot* dan *mac address mikrotik router board* dengan menggunakan bilangan *hexadesimal* seperti pada Gambar 22



Gambar 22 Paket Ethernet Protocol Wireshark Tanpa SSL

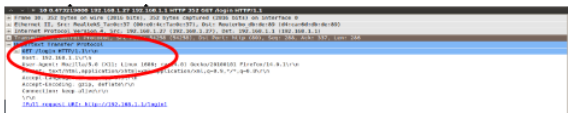
Pada baris *Transmission Control Protocol* diperoleh informasi dimana *client* menggunakan *port* 54258, melakukan koneksi ke *server hotspot* dengan *port* tujuan 80 yaitu *port http*, dimana *port http* merupakan *protocol* komunikasi data antara

server dan *web client* (*browser*) *standard* yaitu *port* 80 dimana *port* tersebut untuk transmisi atau komunikasi data tidak aman karena tidak terenkripsi. Seperti pada Gambar 23



Gambar 23 Paket Transmission Control Protocol Tanpa SSL

Pada Gambar 24 diperoleh informasi dimana *server* mengirim informasi paket *Hypertext Transfer Protocol* ke *client* dengan menanpilkan halaman *login* atau *url* http://192.168.1.1, *HTTP* atau *Hypertext Transfer Protocol* berfungsi untuk melakukan format terhadap paket data yang sudah ditentukan dan ditransimisikan menjadi sebuah data atau *file* dengan format yang bisa direspon oleh *browser* sehingga mampu memunculkan data yang sudah dikirim tanpa terenkripsi.

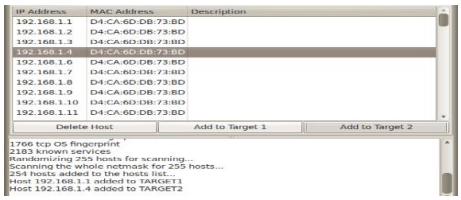


Gambar 24 Paket Hypertext Transfer Protocol

Untuk pengujian selanjutnya penulis mengunakan *software sniffing* yang cukup terkenal yaitu *software ettercap* pada komputer penyusup (*sniffer*), dimana *ettercap* merupakan aplikasi yang terdapat pada sistem hacking *Backtrack 5R3.*

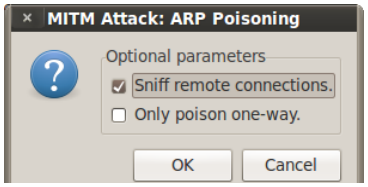
Gambar 25 Setting interface card Komputer Penyusup

Pastikan *lan card / interface card* pada komputer penyusup Kemudian *scan host* pada jaringan yang akan disusupi dengan mengklik pada menu *host* kemudian *scan for hosts.* Pada saat *scan* terdapat *IP address* dan *mac address Server Hotspot* (Target 1) dan *Client Hotspot* (Target 2), *IP address Server Hotspot* yaitu 192.168.1.1 sedangkan *IP address Client Hotspot* yaitu 192.168.1.4 seperti pada Gambar 26



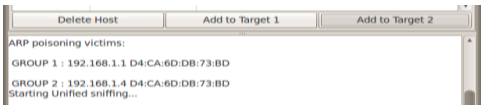
Gambar 26 Scan Host dan Hasil Scanning

Kemudian pilih *IP address 192*.168.1.1 (*IP Server Hotspot / target* 1) dengan cara memilih *add to target 1* dan Kemudian pilih *IP address* 192.168.1.4 (*IP address Client Hotspot* / *target* 2) dengan memilih *add to target 2*. Kemudian aktifkan *arp poisoning* untuk memulai penyusupan dengan mengamati paket data yang melewati dari *target1* ke *target2* maupun sebaliknya.



Gambar 27 Mengaktifkan Arp Poisoning

Dari hasil pengujian pada Gambar 28 diperoleh hasil dimana penyusup atau *sniffing* tidak dapat mengamati *user login* dan *password* yang digunakan saat *Client hotspot* melakukan koneksi ke *Server Hotspot*, hal ini disebabkan *protocol SSL* melakukan enkripsi terhadap proses koneksi antara *server* dan *client.*

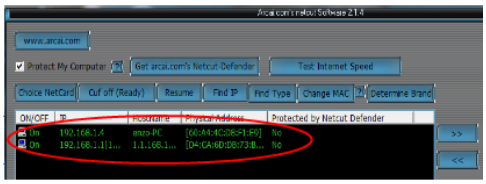


Gambar 28 Hasil Sniffing Ettercap

Pengujian berikutnya menggunakan aplikasi *NetCut*. *Netcut* adalah suatu aplikasi yang diluncurkan oleh *vendor arcai.com*. *NetCut* bekerja pada sistem Windows dan berfungsi untuk memutus, mematikan, atau menghidupkan koneksi *user* pada sebuah area *LAN* atau *Hotspot.* Aplikasi Netcut bekerja menggunakan teknik *spoofing* atau penyadapan, dimana seseorang bisa mendapatkan akses yang tidak sah ke dalam suatu komputer dan ia dapat berperan sebagai *host*. Oleh karena itu, dengan menggunakan *NetCut*, seseorang dapat mengalihkan jaringan pada *gateway* kapan saja.

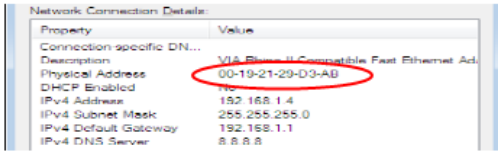
Konsep *Netcut* dikenal dengan nama *ARP Spoofing*, *ARP Spoofing* adalah salah satu teknik serangan (*hacking)* yang dilakukan dengan cara mengirimkan pesan *ARP* (*Address Resolution Protocol*) palsu (*spoofed ARP*) pada jaringan *LAN*.

ARP adalah protokol komunikasi yang digunakan untuk melakukan translasi antara *network layer* dengan *link layer*. Untuk mempercepat translasi biasanya *ARP* memiliki *table database* sederhana yang berisi informasi *MAC address* dan *IP* yang saling berhubungan. Secara umum cara kerja teknik *ARP spoofing* adalah dengan memberitahukan informasi palsu mengenai *ARP message* kepada komputer target. Dengan mengirimkan *ARP* palsu *attacker* dapat membohongi korban pada saat komputer . Dengan teknik ini orang dapat melakukan serangan *DoS* atau dapat juga melakukan serangan *MITM* (*Man In The Middle Attack*). Pada pengujian ini diperoleh informasi dari aplikasi *Netcut*, dimana *client hotspot* yang terkoneksi dengan *ip address* 192.168.1.4 dengan informasi *mac address* 60:A4:4C:D8:F1:E9.



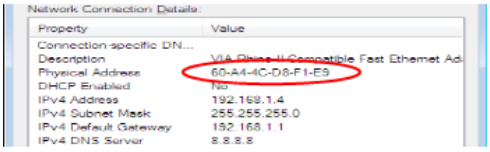
Gambar 29 Spoofing Mac Address Menggunakan Netcut

Informasi *mac address* penyusup sebelum melakukan *spoofing* menggunakan *netcut* dimana *physical address* asli yaitu 00:19:21:29:D3:AB



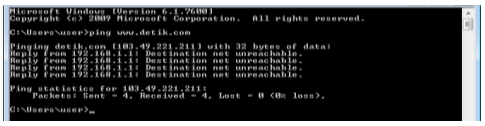
Gambar 30 Tampilan Mac Address Asli Penyusup

Ketika *client hotspot* saat terkena *ARP Spoofing*, dimana *mac address pc client hotspot* sama dengan *mac address* penyusup. Gambar 31 menunjukkan *mac-address* asli penyusup berubah menjadi mac address *client hotspot* 60:A4:4C:D8:F1:E9.



Gambar 31 Hasil Perubahan Mac Address

Walaupun *client hotspot* terkena *ARP Spoofing* tetapi penyusup tidak bisa mengakses internet karena terhalang oleh enkripsi yang dilakukan oleh protokol *SSL* pada *server hotspot.*



Gambar 32 Ping Tes Detik.com

KESIMPULAN DAN SARAN

Dari penelitian ini diperoleh kesimpulan adalah sebagai berikut :

1. Proses ARP *Spoffing* dapat dilakukan, akan tetapi hasil proses duplikasi tidak dapat menggunakan jaringan yang sama.
2. Sistem keamanan *hotspot* berbasis *Secure Socket Layer* (*SSL*) dapat digunakan, hal ini dikarenakan jaringan terenkripsi.

REFERENSI

Referensi harus diurutkan berdasarkan pertama yang disitasi. Referensi ditulis menggunakan style IEEE.

[1] Rajab, Muis. (2010). *Analisa dan Perancangan Wireless dan Security Menggunakan WPA2-Radius*. Teknik Informatika, UIN Syarif Hidayatullah

[2] Bayu, Imam . (2017) . *Analisa Keamanan Jaringan WLAN dengan Metode Penetration Testing*. Teknik Informatika Universitas Halu Oleo Kendari, 3, (3), 68-78

[3] Laudon, K, & Laudon, J. (2010). *Management Information System 11th edition*. *New Jersey. Prentice Hall*

[4] *Fatta, Al Hanif. (2007). Analisis dan Perancangan Sistem Informasi Untuk Keunggulan Bersaing Perusahaan Dan Organisasi Modern. Yogyakarta: Andi Offset*

[5] Nazir, Moh. (2005). *Metodologi Penelitian*. Bogor: Ghalia Indonesia

[6] *Andi. (2010). Sistem Jaringan Komputer Untuk Pemula. Yogyakarta: Andi Offset*

[7] Herlambang Linto, Catur Azis. (2008). *Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS*. Yogyakarta: Andi Offset

[8] Wahana. (2010). *Tips Jitu Optimasi Jaringan Wi-fi*. Semarang:Wahana Komputer

[9] Towidjojo, Rendra. (2013). *Mikrotik Kungfu Kitab 1*. Jakarta: Jasakom

[10] Kurniawan, Agus. (2012). *Network Forensic Panduan Analisis dan Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta: Andi Offset

[11] Kock, Ned. (2007). Information Systems Action Research An Applied View Of Emerging Concepts And Methods. *Texas A & M International University. US*