JITE, 4 (1) Juli 2020 ISSN 2549-6247 (Print) ISSN 2549-6255 (Online)

JITE (Journal of Informatics and Telecommunication Engineering)

Available online http://ojs.uma.ac.id/index.php/jite **DOI : 10.31289/jite.v4i1.3832**

Received: 04 Juni 2020	Accepted: 07 Juli 2020	Published: 20 Juli 2020

Security Design And Testing of Lan and Wlan Network in Mikrotik Router Using Penetration Testing Method FROM Mitm Attack

Haeruddin[1)]*

1) Prodi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, Indonesia

*Coresponding Email:haeruddin@uib.ac.id

Abstrak

Pertumbuhan perangkat pengguna selalu meningkat dan biaya yang dikeluarkan tidak mahal. Pengguna sudah memiliki beberapa alat *end user* jaringan yang canggih untuk penggunaan dalam kehidupan sehari-hari, antara lain laptop, smartphone, dan tablet. Untuk akses internet pengguna menggunakan layanan jaringan LAN dan WLAN baik itu di area publik seperti restoran, sekolah/kampus, hotel dan kantor. Aktivitas yang dilakukan adalah transaksi data maupun perbankan. Kegiatan-kegiatan tersebut berhubungan dengan data krusial seperti data pengguna meliputi *username, password*, rekening, email, dan data sensitif lainnya. Router Mikrotik merupakan router dengan harga yang terjangkau dan fitur yang lengkap baik untuk jaringan LAN maupun WLAN sehingga banyak Administrator menggunakan perangkat ini. Serangan yang banyak digunakan pada jaringan adalah *Man in The Middle Attack*, yaitu penyadapan secara aktif pada koneksi jaringan pengguna, dimana trafik dari pengguna sebelum mencapai tujuan atau pada saat akan melewati router Mikrotik akan dialihkan melalui jaringan penyerang tanpa sepengetahuan pengguna sehingga komuniksi pengguna dengan tujuan dapat dibaca. Oleh karena itu sistem keamanan jaringan pada router Mikrotik sangat dibutuhkan untuk menghindari serangan tersebut. Dalam melakukan pengujian pada sistem keamanan yang telah dibuat maka perlu metode yang tepat, salah satunya adalah *penetration testing*. Dari hasil pengujian dengan menggunakan metode *penetration testing* maka akan didapatkan hasil dan solusi untuk menjaga keamanan jaringan.

Kata Kunci: ***Penetration Testing, Man in The Middle Attack, Keamanan Wireless, Router dan Wireless Mikrotik***

Abstract

The growth of device user is always increasing and the costs are not expensive. Users already have several sophisticated end user networking tools for daily use, including laptops, smartphones and tablets. For internet access users use LAN and WLAN network services in several public areas such as restaurants, schools / campuses, hotels and offices. Activities done by the users are data and banking transactions. These activities relate to crucial data such as user data including usernames, passwords, accounts, emails and other sensitive data. Mikrotik Router is a router with an affordable price and complete features for both LAN and WLAN networks so that many administrators use this device. The most common attack used on the network is Man in the Middle Attack, which is actively tapping on the user's network connection, where traffic from the user before reaching the destination or when going through a Mikrotik router will be diverted through the attacker's network without the user's knowledge so that user communication can be read. Therefore a network security system on a Mikrotik router is needed to avoid such attacks. In testing the security system that has been made, it needs the right method, one of which is penetration testing. From the results of testing using the penetration testing method, results and solutions will be obtained to maintain network security.

Keywords: Penetration Testing, Man in The Middle Attack, Wireless Security, Router dan Wireless Mikrotik.

How to Cite: Haeruddin (2020). Security Design And Testing of Lan and Wlan Network in Mikrotik Router Using Penetration Testing Method FROM Mitm Attack. *JITE (Journal Of Informatics And Telecommunication Engineering)*. 4 (1): 119-127

I. PENDAHULUAN

Pertumbuhan perangkat pengguna selalu meningkat dengan biaya yang tidak mahal, pengguna sudah memiliki beberapa alat perangkat akhir jaringan yang canggih untuk digunakan dalam kehidupan sehari-hari. Alat-alat ini termasuk laptop, ponsel cerdas, dan tablet. Untuk akases ke internet banyak pengguna menggunakan layanan jaringan nirkabel baik itu di area publik seperti restoran, sekolah/kampus, hotel dan bahkan kantor. Ada perusahaan yang telah menerapkan Bring Your Own Device (BYOD) yaitu meggunakan perangkat pribadi mereka untuk terhubun kejaringan perusahaan menggunakan jaringan nirkabel.

Jaringan nirkabel atau biasa disebut Wireless Local Area Network (WLAN) merupakan jaringan yang paling digemari oleh pengguna, karena tidak dibatasi tempat dan jumlah perangkat yang terhubung pada satu media. Berbeda dengan penggunaan kabel atau biasa disebut Local Arena Network (LAN), dimana hanya memungkinkan satu kabel satu perangkat, tempat terbatas, dan hanya perangkat tertentu yang memiliki Network Interface Card (NIC) yang dapat terkoneksi (Ari et al., 2019).

Untuk mengakses informasi dan konten pada internet banyak pengguna menggunakan jaringan LAN dan WLAN pada tempat mereka bekerja atau menggunakan jaringan WLAN pada area publik. Aktifitas yang dilakukan, seperti: mencari informasi, video streaming, musik, sosial media, dan melakukan transaksi pada e-commerce, e-banking, e-trade, e-government, e-business, e-retailing, e-education. Dari kegitan-kegiatan tersebut berhubungan dengan data krusial seperti data pengguna meliputi username, password, rekening, email, dan data sensitif lainnya. Namun banyak pengguna awam yang tidak menyadari dan mengetahui bahaya yang dapat ditimbulkan akibat kebocornya data-data penting (Ikhwan & Elfitri, 2014).

Jaringan WLAN yang bersifat publik dan global yang mudah di akses oleh pengguna, sehingga menyediakan celah untuk terjadinya tindak kejahatan pada dunia maya atau cybercrime (Baihaqi et al., 2018). Pada Jaringan LAN maupun WLAN memungkinkan juga terjadinya serangan dari sesama pengguna jaringan itu sendiri. Tindak kejahatan pada dunia maya terjadi karena adanya celah sistem kemanan dalam jaringan. Oleh sebab itu diperlukan upaya untuk meningkatkan sistem keamanan pada jaringan yang ada (Herdiana, 2014).

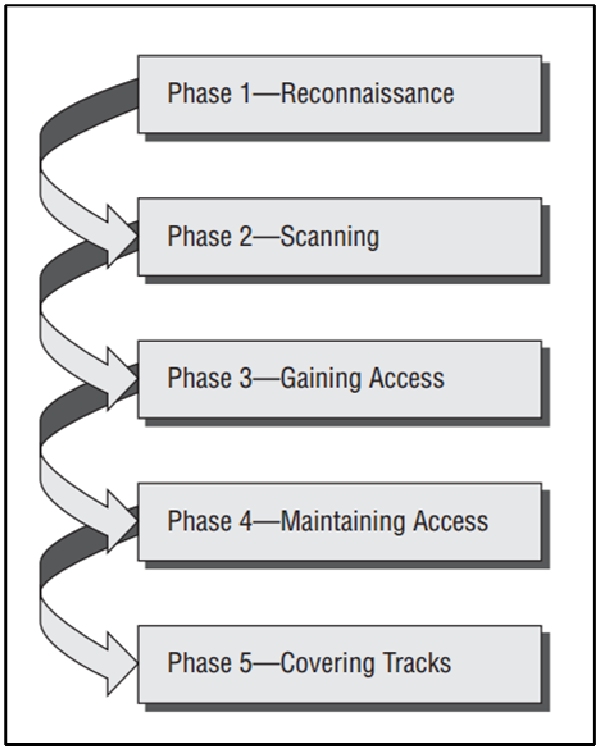
Serangan yang banyak digunakan pada aksi kejahatan untuk menyerang jaringan LAN dan WLAN adalah Man in

The Middle Attack yang selanjutnya disingkat MITM. Jenis serangan ini melakukan penyadapan secara aktif pada koneksi jaringan pengguna, dimana trafik dari pengguna sebelum mencapai tujuan akan dialihkan melalui jaringan penyerang tampa sepengetahuan pengguna sehingga komunikasi pengguna dengan tujuan dapat dibaca oleh penyerang (Celiktas et al., 2018)

MITM merupakan jenis serangan yang sulit dilacak oleh pengguna, meskipun jaringan WLAN telah didukung sistem autentikasi yang baik. Kebanyakan pelaku MITM merupakan orang yang terhubung pada jaringan yang sama dengan pengguna. Jika penyerang berhasil mendapatkan data krusial pengguna, maka dampak yang ditimbulkan sangat besar (Zulfikar et al., 2017).

II. METODE PENELITIAN

Penelitian ini menggunakan penelitian terapan dengan metode penetration testing. Penelitian terapan merupakan penerapan langsung pada objek yang akan diteliti guna memecahkan masalah yang dihadapi. Dari peneltian terapan akan memberikan hasil berupa solusi yang didapatkan dari proses implementasi penelitian. Penetration testing adalah salah satu metode dalam mengevaluasi atau menilai suatu keamanan jaringan secara aktif dengan melakukan pengujian serangan terhadap kemanan jaringan yang ada.



Gambar 1. Metode Penetration Testing

Tujuan metode penetration testing untuk mengetahui dan memastikan celah keamanan pada jaringan, sehingga dapat dikendalikan dengan baik, selain itu celah keamanan dapat diatasi dan dihilangkan sebelum dapat menimbulakan kerusakan ataupun kerugian pada pengguna (Tarigan et al., 2017). Pada metode penetration testing terdiri dari 5 tahapan seperti pada gambar 1 diatas, Adapun tahapannya yaitu:

1. *Reconnaissance*, merupakan tahapan melakukan perencanaan penelitian. Meliputi pemilihan topik, ruang lingkup, tujuan pengujian, dan pemilihan aplikasi yang akan digunakan dalam pengujian. Pada

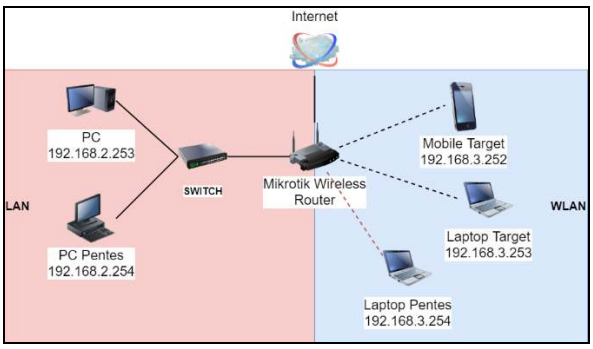
pengujian ini *tools* yang akan di gunakan untuk melakukan serangan MITM adalah Cain & Abel dan Wireshark.

2. *Scanning*, merupakan tahapan melakukan analisa dan memahami cara kerja target untuk melakukan penyerangan. Tahapan ini menggunakan Cain & Abel untuk melihat host atau pengguna yang aktif pada jaringan yang akan diserang.
3. *Gaining Access*, merupakan tahapan yang paling penting dalam penelitian ini. Tahapan dimana dilakukan serangan pada jaringan untuk mengetahui celah yang ada. Pada serangan ini akan menggunakan teknik *Man in The Middle Attack* dengan tools Cain & Abel untuk mengalihkan lalulintas trafik jaringan ke perangkat yang akan melakukan penyadapan data. *Tools* penyadapan data menggunakan Cain & Abel atau Wireshark. *Man in The Middle Attack* adalah salah satu jenis serangan pada jaringan komputer dimana seorang penyusup berada ditengah komunikasi antara pengguna jaringan dan mengambil informasi atau mengirim pesan palsu ke pengguna jaringan tersebut (Pathak & Raza, 2014). MITM adalah salah satu bentuk serangan yang sangat berbahaya pada jaringan LAN dan WLAN yang menyebabkan kebocoran data pengguna jaringan (Rachel & Subhashkar, 2017).
4. *Maintaining Access*, merupakan tahapan mempertahankan akses yang telah didapatkan dari hasil sebelumnya. Pada penelitian ini tidak dilakukan, setelah mendapatkan hasil dari serangan sebelumnya, maka akan membuat laporan tentang celah keamanan yang di dapatkan dan memberikan solusi dari temuan tersebut.

Covering Tracks, tahapan terakhir bahwa penyerang harus mengambil langkah-langkah yang diperlukan untuk menghapus semua kemiripan deteksi. Setiap perubahan yang dibuat, otorisasi yang ditingkatkan dll. Sehingga semua kelihatan normal dan tidak terseteksi oleh administrator jaringan. Pada tahapan ini tidak dilakukan.

III. HASIL DAN PEMBAHASAN

Pada penelitian ini menggunkan simulasi jaringan LAN dan WLAN seperti pada gambar 2 di bawah ini.



Gambar 1 Topologi penelitian

Adapun konfigurasi pada *router* Mikrotik sebagai berikut:

1. Konfigurasi *IP address*

```
/ip address
add address=192.168.1.2/24
interface=WAN network=192.168.1.0
add address=192.168.2.1/24
interface=LAN network=192.168.2.0
add address=192.168.3.1/24
interface=WLAN network=192.168.3.0
```

2. Konfigurasi *NAT*

```
"/ip firewall nat
add action=masquerade chain=srcnat
```

3. Konfigurasi static *routing*

```
/ip route
add distance=1 gateway=192.168.1.1
```

4. Konfigurasi DNS

```
/ip dns
set servers=8.8.8.8
```

5. Konfigurasi DHCP Server

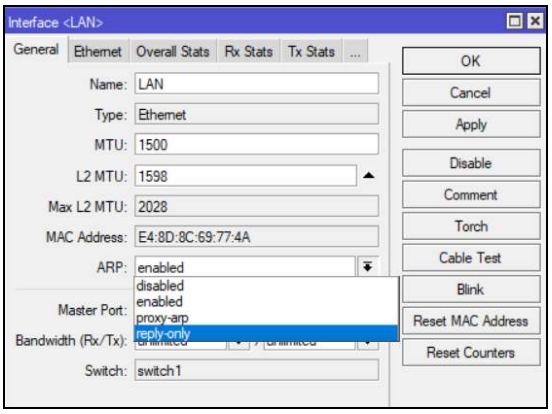
```
/ip dhcp-server network
add address=192.168.2.0/24 dns-
server=8.8.8.8,192.168.1.1
gateway=192.168.2.1
add address=192.168.3.0/24 dns-
server=8.8.8.8,192.168.1.1
gateway=192.168.3.1
/ip pool
add name=dhcp_pool1
ranges=192.168.2.2-192.168.2.254
add name=dhcp_pool2
ranges=192.168.3.2-192.168.3.254
```

6. Konfigurasi WLAN

```
/interface wireless security-profiles
add authentication-types=wpa-psk,wpa2-
psk eap-methods="" \
   management-protection=allowed
mode=dynamic-keys name=WLAN \
   supplicant-identity="" wpa-pre-shared-
key=1234567890 wpa2-pre-shared-key=\
   1234567890
/interface wireless
set [ find default-name=wlan1 ] default-
forwarding=no disabled=no l2mtu=1600 \
   mode=ap-bridge name=WLAN security-
profile=WLAN ssid=Publik
```

7. Konfigurasi keamanan LAN

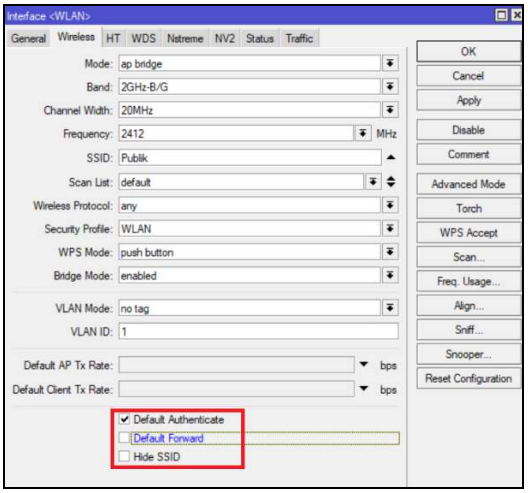
Pada *interface* LAN klik dua kali interface tersebut makan akan muncul tampilan seperti pada gambar 3 di bawah ini. Pada kolom ARP pilih *reply-only*



Gambar 2 ARP reply-only

8. Konfigurasi keamanan WLAN

Pada *router* Mikrotik masuk ke menu *Wireless*, pilih *interface* WLAN kemudian akan muncul dialog tampilan *interface* WLAN dan masuk ke *Tab Wireless*, pada bagian bawah *unceklist default forward* seperti pada gambar 4 di bawah ini.

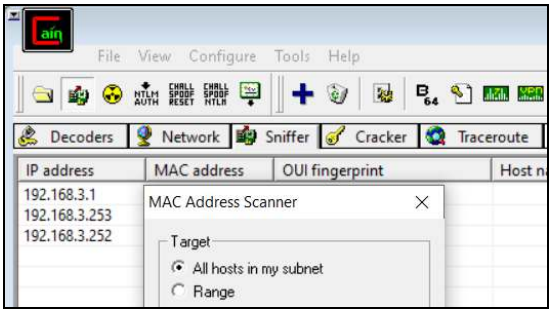


Gambar 3 *unceklist default forward*

Setelah konfigurasi selesai makan peneliti akan melakukan pengujian sistem keamanan jaringan LAN dan WLAN menggunakan metode *Penetration Testing* dengan teknik *Man in The Middle Attack* dengan *tools* Cain & Abel, dan Wireshark.

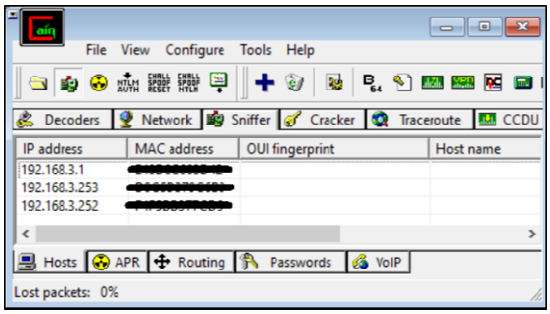
a. *Reconnaissance*, pada pengujian ini *tools* yang akan di gunakan untuk melakukan serangan MITM adalah Cain & Abel dan Wireshark.

b. *Scanning*, pada tahapan ini dapat menggunakan *tools* Cain & Abel dengan menggunakan fitur *sniffer*, dan melakukan *scanning* MAC *Address* pada *host* yang aktif pada jaringan tersebut, seperti pada gambar 5 di bawah ini. Perlu diingat bahwa serangan ini hanya berlaku dalam segmen jaringan yang sama jika suda memiliki segmen jaringan yang berbeda maka serangan ini tidak dapat dilakukan. Ini disebabkan protocol ARP hanya dapat bekerja pada *broadcast* domain yang sama, jika sudah memilik *broadcast* domain yang berbeda maka serangan ARP tidak dapat dilakukan. Contoh pada kasus ini, jaringan LAN dengan *network* 192.168.2.0/24 tidak dapat melakukan serangan pada jaringan WLAN dengan *network* 192.168.3.0/24.



Gambar 4 Scanner Host pada jaringan

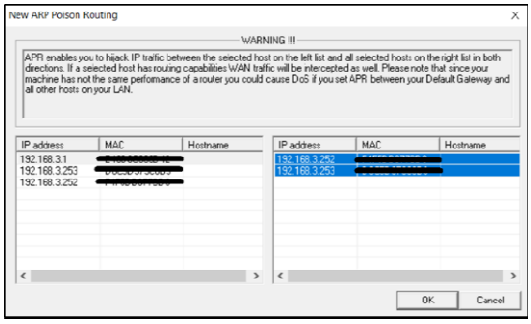
Jika berhasil makan akan muncul daftar IP dan MAC *Address* target, seperti pada gambar 6 di bawah ini.



Gambar 5 Hasil Scanner host

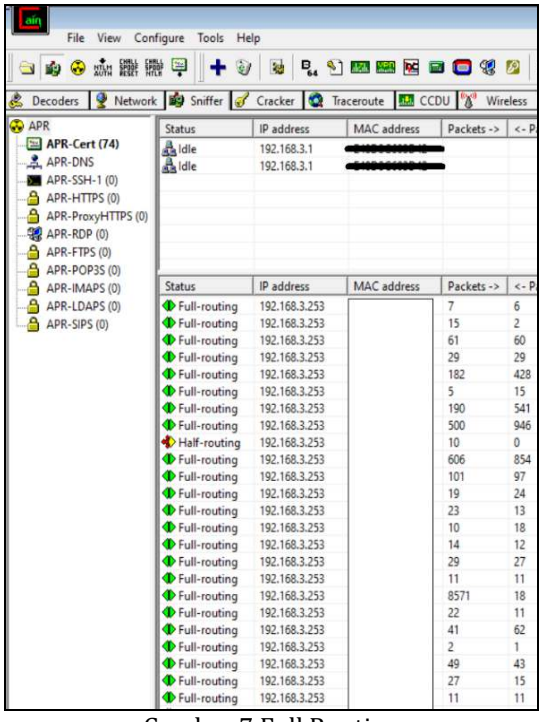
c. *Gaining Access*, merupakan tahapan yang paling penting dalam penelitian ini. Tahapan dimana dilakukan serangan pada jaringan LAN dan WLAN untuk mengetahui celah yang ada. Pada serangan ini masih menggunakan *tools* yang sama yaitu Cain & Abel. Melanjutkan tahapan sebelumnya, proses berikutnya adalah memilih

target yang akan diserang dari daftar hasil *scanner* seperti pada gambar 7 di bawah ini.



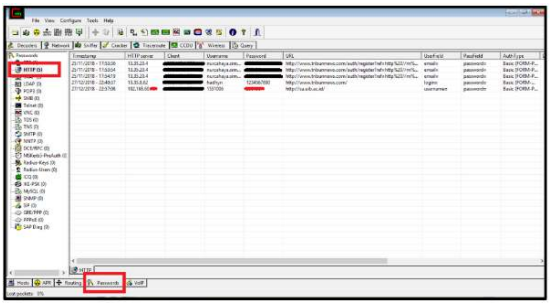
Gambar 6 Daftar target serangan

Setelah memilih target maka dilakukan serangan ARP *Poisioning* pada aplikasi Cain & Abel untuk mengalihkan lalulintas pengguna jaringan keperangkat atau laptop penyerang yaitu Pentes. Proses ini ditandai dengan status *Full-Routing* seperti pada gambar dibawa 8 di bawah ini.



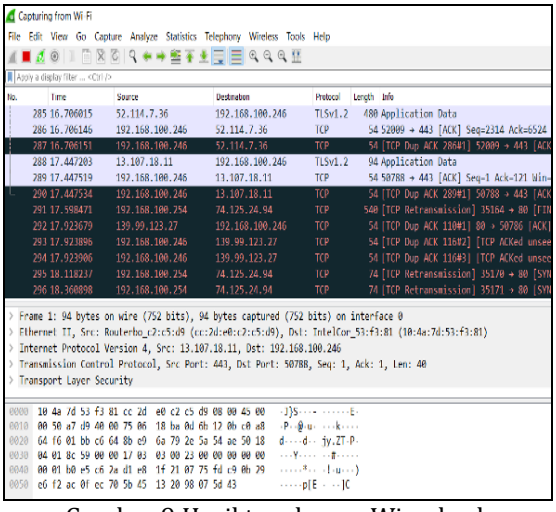
Gambar 7 Full Routing

Untuk mendapatkan informasi penting seperti data krusial meliputi *username* dan *password* dapat menggunakan Cain & Abel atau Wireshark. Pada pengujian ini. Jika belum menerapkan sistem kemanan jaringan pada router Mikrotik, maka pada saat mengakses *sign in/log in* halaman yang yang menggunakan protokol *http*, secara langsung dapat menangkap *username* dan *password* seperti pada gambar 9 di bawah ini.



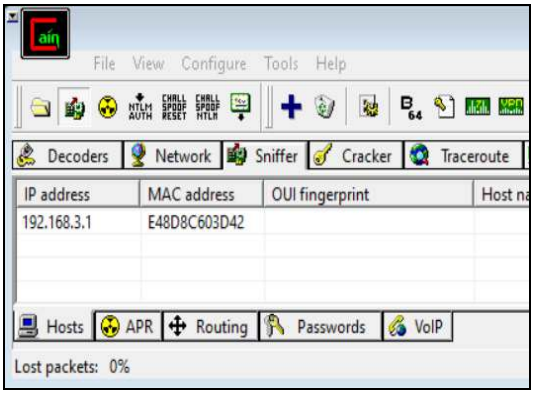
Gambar 8 Tampilan username dan password

Selain itu kita dapat menangkap pake data yang melalui laptop Pentes dengan Aplikasi Wireshark seperti pada gambar 10 di bawah ini.



Gambar 9 Hasil tangkapan Wireshark

Setelah melakukan penerapan sistem keamanan pada jaringan LAN dan WLAN pada router Mikrotik, maka dilakkan pengujian menggunakan metode yang sama. Namu pada saat melakukan tahapan scanning, target yang akan diserang tidak di temukan seperti pada gambar 11. Sehingga Pentes tidak dapat melakukan serangan.



Gambar 10 Scanning Jaringan

Pengujian secarangan *Man in The Middle Attack* memanfaatkan celah keamanan pada protokol ARP. Secara *default* protokol ARP akan mengirimkan ARP *request* secara *broadcast* ke semua komputer atau perangkat pada jaringan yang sama, sehingga siapun yang berada dalam jaringan tersebut dapat merespon pesan ARP *broadcast* tersebut meskipun isi pesan bukan di tujukan untuknya. Selain itu pada jaringan yang sama siapapun dapat mengirim ARP *request* dengan berpura-pura menjadi *host* dengan memalsukan MAC *Address*. Seperti pada gambar 12 di bawa ini kita dapat melihat MAC *Address gateway* yaitu xx:xx:xx:xx:3d:42 pada laptop target yang belum diserang.

```
C:\Users\husnul>arp -a

Interface: 192.168.3.253 --- 0x8
  Internet Address      Physical Address      Type
  192.168.3.1           [illegible]-3d-42     dynamic
  192.168.3.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Gambar 11 ARP Tabel target sebelum diserang

Setelah melakukan serangan, maka pada tabel ARP laptop target MAC *Address gateway* akan berubah menjadi MAC *Address* laptop Pentes seperti pada gambar 13 di bawah ini, sehingga pada saat akan mengakses data di jaringan internet maka laptop target akan melalui laptop Pentes, sehingga semua data target dapat di tangkap oleh Pentes.

```
C:\Users\husnul>arp -a

Interface: 192.168.3.253 --- 0x8
  Internet Address      Physical Address      Type
  192.168.3.1           [illegible]f3-81      dynamic
  192.168.3.254         [illegible]f3-81      dynamic
  192.168.3.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Gambar 12 ARP Tabel target setelah diserang

Menerapkan sistem keamanan pada *Interface* LAN dengan mode *ARP-Reply Only* dapat mengamankan jaringan LAN dan mematikan *default forward* pada pengaturan *Interfae wireless* maka serangan ARP *Poisioning* tidak dapat dilakukang, sehingga jaringan aman digunakan oleh pengguna.

IV. SIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan, peneliti dapat

menyimpulkan beberapa hal terkait penelitian ini, yaitu:

a. Sistem keamanan jaringan LAN dan WLAN yang memiliki *network* / segmen jaringan yang sama memiliki celah keamanan yang dapat diserang dengan teknik *Man in The Middle Attack*, sehingga mengakibatkan kebocoran data seperti *username* dan *password* yang sangat fatal dampaknya bagi pemilik data.
b. Penerapan fitur mode *ARP-Reply Only* pada *Interface* LAN dapat mencegah serangan ARP *Poisioning,* sehingga jaringan LAN Tetap Aman.
c. Dengan menonaktifkan *default forward* pada pengaturan *Interface wireless* di perangkat Mikrotik serangan ARP *Poisioning* tidak dapat dilakukang, sehingga jaringan aman digunakan oleh pengguna.
d. Penggunaan metode *Penetration Testing* membatu melakukan pengujian secara terstruktur dengan hasil akhir dari pengujian ini adalah berupa keamanan jaringan LAN dan WLAN yang tidak dapat ditembus oleh serangan *Man in The Middle Attack*.

Pada penelitian ini penulis hanya menggunakan satu metode yaitu *penetration testing,* penulis juga menyarankan untuk menggunakan metode pengujian keamanan yang berbeda sehingga bisa dijakan sebagai acuan perbandingan.

DAFTAR PUSTAKA

Ari, I. M., Suta, D., Gede, I. N., Astawa, A., & Sukarata, P. G. (2019). Pengembangan Jaringan Internet Wireless Dengan Wifi Overview Pada Obyek Wisata Blangsinga Waterfall. 11(1), 28–32.

Baihaqi, Yanti, Y., & Zulfan. (2018). Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi. Jurnal Serambi Engineering, 3(1), 248–254. https://doi.org/10.32672/jse.v3i1.353

Celiktas, B., Serkan Tok, M., & Unlu, N. (2018). Man in the Middle (MITM) Attack Detection Tool Design. International Journal of Engineering Sciences & Research Technology, 7(8), 90–99. https://doi.org/10.5281/zenodo.1336698

Herdiana, Y. (2014). Keamanan Pada Jaringan Wireless. Isu Teknologi STT Mandala, 7(2), 25–36.

Ikhwan, S., & Elfitri, I. (2014). Analisa Delay Yang Terjadi Pada Penerapan Demilitarized Zone (DMZ) Terhadap Server Universitas Andalas. Jurnal Nasional Teknik Elektro, 3(2), 118. https://doi.org/10.25077/jnte.v3n2.75.2014

Pathak, M., & Raza, Ni. (2014). Comprehensive Analysis of Man in the Middle Attack and Propose Statistical Detection Approach. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 3(5), 269–272. http://ijarcsee.org/index.php/IJARCSEE/article/view/480

Rachel, S., & Subhashkar, S. (2017). An Overview of the Man-In-The-Middle Attack. 1–6. http://www.ijetjournal.org

Zulfikar, M. I., Rizal, M. F., & Rosmiati, M. (2017). Implementasi Badusb Mitm Attacks. 3(3), 1909–1916.