I N F O R M A T I K A
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

PERANCANGAN ARP POISIONING PADA ANALISIS KEAMANAN JARINGAN MAN IN THE MIDDLE ATTACK PADA UNIVERSITAS DUMAI

Rahadatul 'Aisy Riadi[1], Yuhandri[2], Sumijan[3], Fitri Pratiwi[4], Nur Rubiati[5], Mardayulis[6]
[1,2,3]Program Pasca Sarjana Magister Teknik Informatika Universitas Putra Indonesia "YPTK" Padang
[4,5,6,]Fakultas Ilmu Komputer, Universitas Dumai
[1,2,3]Jl. Raya Lubuk Begalung, Lubuk Begalung Nan XX, Kec. Lubuk Begalung, Kota Padang, Sumatera Barat, Kode Pos : 25145
Jl. Utama Karya Bukit Batrem Kec. Dumai Timur Kode pos 28811
e-mail : [1]radhariadi@gmail.com,[2]yuyu@upiyptk.ac.id,[3]sumijan@upiyptk.ac.id

ABSTRAK

Teknologi dan komunikasi telah berkemabang dengan sangat pesat pada era digital saat ini sehingga memiliki peran yang penting bagi masyarakat. Jaringan Komputer merupakan salah satu teknologi yang berkembang dibidang transmisi data dan jaringan komputer memiliki 2 jenis media transmisi data diantaranya kabel dan nirkabel. Jaringan nirkabel atau wireless ini sangat sering digunakan karena merupakan salah satu sarana yang penting dalam peningkatan jumlah pengguna internet di Indonesia. Namun penggunaan Jaringan wireless tidak luput dari kejahatan cyber yang dilakukan oleh orang yang tidak bertanggung jawab sehingga dapat merugikan orang lain. Man In The Middle Attack merupakan serangan terhadap jaringan akses terbuka, bentuk dari serangan ini adalah didalam jaringan komputer dimana penyerang berada ditengah-tengah antara korban dan tujuan korban. Serangan ARP Poisioning sangat merugikan bagi user karena bersifat aktif. Serangan ini dapat digunakan untuk mencuri data sensitif yang dikirimkan melalui jaringan. Metode yang digunakan dalam penelitian ini adalah Live Forensic. Metode ini merupakan proses mendeteksi, menangkap, mencatat dan menganalisa aktivitas jaringan guna menemukan bukti digital suatu serangan yang dilakukan melalui jaringan komputer. Data yang digunakan pada penelitian ini adalah jaringan wireless yang ada pada Universitas Dumai. Data yang diambil pada penelitian ini berupa IP Address dan MAC Address yang bersumber dari jaringan Universitas Dumai. Setelah melakukan percobaan dalam melakukan serangan ARP Poisioning didapatkan hasil bahwa keamanan jaringan wireless di Universitas Dumai dapat ditembus oleh ARP Poisioning dan simulasi serangan ARP Poisioning yang dilakukan berjalan dan berhasil. Sehingga didapatkan bahwa jaringan wireless di Universitas Dumai kurang aman dan memiliki kemungkinan untuk diserang oleh penyerang.

Kata Kunci : *Keamanan Jaringan, Jaringan Wireless, Man In The Middle Attack, ARP Poisioning, Live Forensic*

ABSTRACT

Technology and communication have been very rapidly branching out in today's digital age, thus having an important role for society. Computer networking is an emerging technology in the field of data transmission and computer networking has two types of data transmission media: wired and wireless. This wireless or wireless network is very often used because it is an important tool in increasing the number of internet users in Indonesia. However, the use of wireless networks does not escape the cybercrime committed by irresponsible people that can harm others. Man In The Middle Attack is an attack on an open access network, a form of attack within a computer network where the attacker is in the middle between the victim and the victim's destination. ARP Poisoning attacks are very detrimental to the user because they are active. These attacks can be used to steal sensitive data transmitted over the network. The method used in this study was Live Forensics. This method is the process of detecting, capturing, recording and analyzing network activities in order to find digital evidence of an

I N F O R M A T I K A
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

attack carried out over a computer network. The data used in this study are wireless networks that exist at Dumai University. The data taken in this study are IP Address and MAC Address which are sourced from Dumai University's network. After three experiments on ARP Poisoning attacks, it was found that the security of the wireless network at Dumai University was breached by ARP Poisoning and the simulation of ARP Poisoning attacks was run and successful. Therefore, it was found that the wireless network at Dumai University was not secure and had the possibility of being attacked by an attacker.

Keyword *: Network Security, Wireless Network, Man In The Middle Attack, ARP Poisoning, Live Forensics*

1. PENDAHULUAN

Teknologi dan komunikasi telah berkemabang dengan sangat pesat pada era digital saat ini sehingga memiliki peran yang penting bagi masyarakat. Jaringan Komputer merupakan salah satu teknologi yang berkembang dibidang transmisi data dan jaringan komputer memiliki 2 jenis media transmisi data diantaranya kabel dan nirkabel. Jaringan nirkabel memanfaatkan gelombang radio sebagai media untuk terhubung antara perangkat satu dengan perangkat lainnya. Jaringan nirkabel atau *wireless* ini sangat sering digunakan karena merupakan salah satu sarana yang penting dalam peningkatan jumlah pengguna internet di Indonesia. Wifi menawarkan kemudahan dalam mengakses dan kecepatan tinggi serta harga yang terjangkau, sehingga pengguna internet semakin antusias untuk menggunakan *wireless* walaupun dengan tingakat keamanan yang rendah. Namun penggunaan Jaringan *wireless* tidak lutup dari kejahatan *cyber* yang dilakukan oleh orang yang tidak bertanggung jawab sehingga dapat merugikan orang lain.

Analisa investigasi *Static Forensic* Serangan *Man In The Middle Attack* berbasis ARP *Poisioning*. Penelitian ini dilakukan dengan menerapkan pendekatan metode Statik Forensik, untuk mendeteksi aktivitas ilegal yang terjadi pada wi-fi. Proses investigasi dibagi menjadi sepuluh tahapan dimulai dari proses *preparation, detection, incident, respon, collection, examination, presevation, examinations, analysism investiation* dan *reporting*. Penelitian ini akan difokuskan pada serangan *Man In The Middle Attcak berbasis* ARP *Poisioning*. Hasil dari penelitian ini dapat menganalisa data dan menenukan barang bukti maupun informasi pelaku yang dapat dipertanggung jawabkan.

Analisis Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. Penelitian ini menggunakan metode *Penetration test*. Pada penelitian ini dilakukan pengujian dengan serangan *cracking the encrtption*, ARP *Poisioning* dan *denial of service* terhadap jaringan nirkabel. Data yang digunakan pada penelitia ini adalah jaringan pada Kantor Dinas Pendidikan Kabupaten Minahasa. Hasil dari pengujian dnegan serangan-serangan yang dilakukan dapat disimpulkan bahwa penerapan sistem keamanan jaringan yang diterapkan maish belum sepenuhnya dikatakan aman dikarenakan serangan *cracking the encrtption* yang disimulasikan berhasil.

Manajemen Pencegahan Serangan Jaringan *Wireless* Dari Serangan *Man In The Middle Attack*. Pada penelitian ini melakukan kemungkinan dalam penyerangan dengan jenis serangan yang dilakukan adalah *Man In The Middle Attack.* Dari percobaan ini dilakukan sebanyak 5 kali dan dilakukan perhitungan QoS (*Quality of Service*) yaitu mengitung berapa banyak paket *loss* dan hasil yang didapatkan dari percobaain penyerangan ini dengan menghitung paket *loss* nya sebanyak *loss* 0.291%, serangan 1 model 2 dengan paket *loss* 0,124%, serangan 2 model 2 dengan paket *loss* yang diartikan pada serangan ini berhasil untuk menyerang komunikasi *wireless*. Untuk mencagah dari penyerangan ini, terlebih dahulu untuk mengetahui teknik cara serangan itu berjalan pada *wireless*, dengan menggunakan *ettercap* pada *kali linux*.

Analisis Sistem Keamanan Jaringan Menggunakan *Framework* NIST. Keamanan jaringan merupakan aspek yang sangat penting bagi sebuah jaringan komputer. Jaringan komputer memiliki kelemahan-kelemahan yang jika tidak dilindungi dan dijaga dengan baik maka akan menyebabkan kerugian. Maka sudah sepatutnya keamanan jaringan harus lebih diperhatikan untuk mencegah ancaman menyerang sistem, terlebih lagi saat jaringan LAN sudah tersambung ke internet maka ancaman keamanan jaringan akan semakin signifikan. Universitas Sjakhyakirti merupakan universitas yang terletak di kota Palembang yang juga berpartisipasi dalam menyelenggarakan sistem keamanan tersebut. Pentingnya penelitian ini yaitu agar dapat mengurangi adanya ancaman yang berdampak negatif terhadap sistem keamanan informasi, sehingga mengurangi dampak insiden sistem informasi dan meminimalisir resiko-resiko yang mungkin akan

INFORMATIKA
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

terjadi. Selanjutnya dilakukan analisa sistem keamanan jaringan dengan *Framework* NIST *(National Institute Standard Technology), framework* yang dirancang untuk sesuatu perhitungan kualitatif yang didasarkan pada analisis sistem keamanan.

Analisis Keamanan Jaringan pada Jaringan *Wireless* dari Serangan *Man In The Middle Attack* DNS *Spoofing*. Namun tetapi, dengan adanya *wireless* tidak sepenuhnya aman dalam melakukan aktivitas interaksi sesama manusia dalam mengirim data dan lain sebagainya, salah satunya kegiatan *illegal man in the middle attack DNS spoofing*. Dengan adanya kegiatan *illegal* tersebut maka dibutuhkan sistem keamanan yang diharapkan dapat mencegah kegiatan *illegal man in the middle attack DNS spoofing*. hasil dari penyerangan yang di dapatkan berdasarkan 7 kali pengujian dengan menghitung *quality of service (QOS)* yaitu *packet loss* dengan hasil serangan 1 model 1 dengan *packet loss* 0,154%, serangan 2 model 1 dengan *packet loss* 0,234%, serangan 3 model 1 dengan *packet loss* 0.291%, serangan 1 model 2 dengan *packet loss* 0,173%, serangan 2 model 2 dengan *packet loss* 0,128%, serangan 3 model 2 dengan *packet loss* 0,028%, serangan 4 model 2 dengan *packet loss* 0,231%, yang dapat diartikan serangan ini dapat berjalan dengan baik. Dan hasil dengan memanfaatkan sistem keamanan *firewall* hanya dapat mencegah dengan memutus interaksi komunikasi antar penyerang dengan korban dan korban dengan penyerang .

Implementasi *Framerwork* MITM (*Man In The Middle Attack*) Untuk Memantau Aktifitas Penggunana Dalam Satu Jaringan. Kemajuan teknologi informasi yang semakin kencang harus diimbangi dengan kemampuan untuk melakukan pengamanan terhadap informasi. Berbagai masalah penyerangan jaringan yang bertujuan merugikan pengguna perlu kita pahami bagaimana konsep penyerangan tersebut. Serangan MITM (*Man In The Middle*) membelokan *traffic packet* data melewati perangkat penyerang. Dalam penelitian ini akan dibahas tentang bagaimana serangan MITM bekerja terutama dari sisi klien dan menggunakan metode *sniffing* serta akan memberikan hasil berupa data proses MITM yang akurat dan dapat dibuktikan menggunakan *framework* MITM. Hasil pengujian menunjukan *website* yang dapat di bypass *username* dan *password* nya adalah *website* dengan protokol keamanan HTTP. Sedangkan terhadap protokol keamanan HTTPS tidak mampu untuk mendeteksi aktivitas *browser*. Akses terhadap *website* dengan protokol keamanan HTTPS bisa dialihkan ke protokol keamanan HTTP.

Analisis Keamanan FTP *Server* Menggunakan Serangan *Man In The Middle Attack*. FTP merupakan metode pilihan yang tepat dalam penyimpanan dengan kecepatan transfer yang lebih baik, akan tetapi seiring perkembangan teknologi semakin banyak *tools* yang dapat melakukan tindak kejahatan diantaranya melakukan *sniffing*. *Sniffing* merupakan tindkan *hacking* paling mudah dan paling sulit untuk diantisipasi, dengan berbagai macam *tool* yang dapat digunakan dan bersifat *free*, yang dapat membahayakan *user* yang tidak teliti atau tidak mengerti sepenuhnya tentang kemanan jaringan computer. Agar *User* dapat terlindung dari serangan *sniffing* maka dibutuhkan Protokol FTPS dimana terdapat penggabungan antara protokol FTP dan aplikasi OpenSSL. OpenSSL berfungsi untuk melindungi data *user* dan *password* melalui enkripsi berupa berkas sertifikat. Setelah melakukan pengujian hal tersebut dapat dihindari dengan dengan menggunakan FTPS. Ketika pengguna akan *login* memasukkan *user name* dan *password* maka protokol FTPS akan melakukan enkripsi data, sehingga informasi *user* dan *password* di jaringan sulit untuk disadap oleh aplikasi-aplikasi *sniffer* yang banyak beredar di internet. Berdasarkan hasil penelitian yang telah dilakukan dengan menggunakan *encrption* makan data akan aman, dan terbebas dari *sniffing*.

Implementasi dan Deteksi Serangan *Man-In-The-Middle-Attack* Berbasis MITM *Proxy* Terhadap Protokol HTTPS Menggunakan Metode K-NN. *Website* menjadi media yang perkembangannya sangat pesat. Banyak metode keamanan yang diterapkan untuk mengamankan data yang tersimpan pada sebuah *website*, namun dari sisi pengguna sering terjadi kecerobohan ketika mengakses *website* dengan protokol *Hypertext Transfer Protocol Secure* (HTTPS) menggunakan perangkat *smartphone*. MITM *proxy* mampu melihat lalu lintas jaringan serta membuat sertifikat palsu ketika pengguna mengakses sebuah *website*. Data sensitif pengguna bisa terlihat dan didapatkan ketika serangan dilakukan, namun serangan yang terjadi menimbulkan anomali pada nilai *Round Trip Time* dan *Throghput*. Dalam mendeteksi serangan dan anomali yang terjadi, algoritma K-*Nearest Neighbor* (K-NN) berjalan dengan baik dan dapat digunakan untuk mendeteksi. Hasil serangan yang dilakukan, informasi sensitif pengguna yaitu *username* dan *password* berhasil didapatkan serta hasil pengujian deteksi serangan menggunakan algoritma K-NN memiliki nilai akurasi sebesar 95.1% dengan *error rate* sebesar 4.9%.

Framework Man In The Middle Attack

INFORMATIKA
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

Menggunakan *Linux* pada Lembaga Penyiaran Publik RRI Bengkulu. Perkembangan teknologi yang sangat maju mengakibatkan tingkat kebutuhan terhadap kemanan jaringan menjadi sangat penting. Metode yang digunakan adalah metode (NDLC) *Network Development Life Cycle* suatu siklus tahapan perancangan jaringan yang dapat menuntun sebuah perancangan jaringan, yang bergantung pada besarnya proyek yang akan dilaksanakan dan tujuan dari pembuatan proyek tersebut. Pengujian keamanan wireless menggunakan MITM yang digunakn untuk memencari informasi dan analisis keamanan menggunakan metode Teknik *Arp Spoofing*.yang akan di uraikan pada aplikasi *Framework* MITM. Berdasarkan dari analisis dan percobaan serangan yang dilakukan maka masih perlu peningkatan, hal ini dengan aplikasi *airodamp-ng* mendeteksi WiFi yang ada di sekitar dan serangang *packet snoofing* dapat menampilkal informasi alamat *website,username* dan *password* dengan menggunakan aplikasi *Framework* MITM.

Analisis *Address Resolution Protocol Poisoning Attack* Pada *Router Wlan* Menggunakan Metode *Live Forensics*. Perkembangan Teknologi Pada Zaman Sekarang Membuat Hampir Setiap Orang Menjadikan *Wireless Local Area Network* Sebagai Kebutuhan. Beberapa Badan Usaha Bahkan Instansi Sudah Lebih Memilih Menggunakan Teknologi *Wireless* Dikarenakan Pemakaiannya Yang Sangat Mudah, Akan Tetapi Masih Sangat Sedikit Yang Memperhatikan Keamanan Komunikasi Data Pada Jaringan *Wireless. Address Resolution Protocol Poisoning Attack* Merupakan Salah Satu Jenis Serangan Pada Jaringan *Wireless* Dengan Akses Terbuka Dan Juga Sangat Mudah Dilakukan Dengan Menggunakan Berbagai Aplikasi, Salah Satu Contoh Aplikasi Yang Dapat Digunakan Adalah Netcut. Serangan Tersebut Mampu Mengendus Data *Frame* Dan Melakukan Modifikasi *Traffic* Atau Bahkan Menghentikan *Traffic* Internet. Pada Kasus Ini Serangan Dapat Dianalisis Menggunakan Metode *Live Forensics* Karena Data Yang Diteliti Berupa *Volatile* Bersifat Sementara Dan Hanya Dapat Ditemukan Pada Penyimpanan *Random Access Memory* Atau Pada *Traffic* Jaringan. *Volatile* Data Hanya Akan Ada Pada Saat Sistem Masih Menyala, Sehingga Perilaku Dari Attacker Serta Informasi Bukti Digital Yang Dapat Diketahui Berupa *Ip Address* Dan *Mac Address Source Destination* Yang Dianalisis Menggunakan Aplikasi *Wireshark*. Terdapat Pendeteksian Pada Penelitian Ini Dengan Menggunakan Aplikasi *Instruction Detection System Snort* Yang Dapat Mengirimkan *Aler*t Ketika Sistem Diserang.

Penggunaan jaringan wifi di ruang publik memiliki risiko perampokan data akses pengguna di dunia maya, seperti perbankan transaksi, media sosial dan akses online lainnya. Ancaman serangan *Man In The Middle Attack* (MITM) dilakukan di depan umum jaringan wifi untuk mendapatkan akses ke informasi pengguna dengan cara ilegal. Proses simulasi vektor serangan dilakukan pada akses situs exampleriset.com/dvwa/login.php . Serangan keracunan ARP dengan perangkat Ettercap melakukan intersepsi dan manipulasi yang memberikan 08.00: 27: 22: 99 MAC *address* informasi ke target. Simulasi serangan Pembajakan Sesi dilakukan menggunakan *cookie plugin manajer* pada protokol HTTP dan HTTPS. Serangan SSL *Stripping* dengan mencegat dan menurunkan HTTPS ke HTTP dengan lebih baik protokol komunikasi. Serangan ARP keracunan mendapatkan informasi dari target seperti Alamat MAC IP Seluler 192.168.3.249 F4:09: D8: EA: EC: E7 dan *Server* 192.168.3.508:00; 27: CC: 59: OE dan pengguna: admin Lulus: kata sandi. Hasil Sesi Pembajakan serangan pada protokol HTTP mendapatkan id sesi dalam bentuk php sesiid = 4f1pnfr081e4jero11truspb60\r\n yang digunakan waktu id sesi yang ditentukan tanpa memasukkan otentikasi pengguna. Serangan Pembajakan Sesi pada protokol HTTPS adalah gagal dan serangan SSL Striping pada protokol HTTPS tidak berhasil.

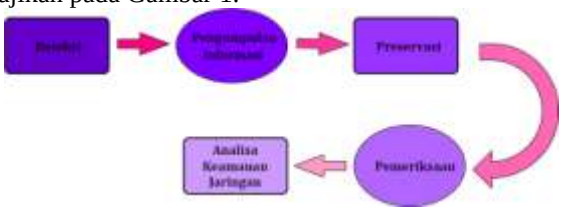
Jaringan komputer dan internet sangatlah berperan penting untuk kelancaran berbagai bidang pekerjaan. Salah satu contoh teknologi informasi dan komunikasi tersebut adalah *Wireless Local Area Network* (WLAN) atau disebut juga teknologi jaringan lokal nirkabel. Metode yang digunakan pada penelitian yaitu dengan metode *Penetration Testing*, dengan maksud melakukan analisis kepada sistem keamanan komputer *Wireless Network* yang ada pada Laboratorium STMIK Bina Patria. Pengujian dilakukan dengan beberapa kegiatan yang diantaranya dengan cara mengidentifikasi serta mengeksploitasi kerentanan pada keamanan jaringan komputer. Dalam menganalisa keamanan jaringan WLAN dilakukan dengan metode *Penetration Testing* dimana bentuk serangan terhadap jaringan disimulasikan, salah satu sistem operasi yang memiliki spesifikasi yang tepat dalam hal tersebut adalah Kali Linux. Jaringan *wireless* merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Walaupun memiliki sitem keamanan, jaringan *wireless* masih dapat di diserang oleh para *attacker* .

INFORMATIKA
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

Berdasarkan penelitian sebelumnya, penelitian ini akan membahas tentang perancangan serangan ARP *Poisioning* dalam menganalisa keamanan jaringan *wireless* dari *Man in the middle attack*. Penelitian ini akan menggunakan metode *live forensic* saat melakukan analisis keamanan jaringan. Penelitian ini bertujuan untuk mengetahui keamana jaringa wireless dan mengetahui apakah simulasi serangan *ARP Poisioning* yang dilakukan berhasil atau tidak. Kebaruan dalam penelituan ini menghadirkan pengetahuan baru tentang ARP *Poisioning*. Hasil yang didapatkan dari penelitian ini dapat membantu administrator jaringan dalam menganalisa keamanan jaringan *wireless.*

2. METODE PENELITIAN

Tujuan dari penelitian ini adalah melakukan simulasi serangan ARP *Poisioning* yang akan dilakukan secara sistematis yang dapat digunakan sebagai pedoman dalam melaksanakan penelitian agar hasil yang dicapai tidak menyimpang dan tujuan yang diinginkan tercapai. Proses perancangan serangan ARP *Poisioning* pada penelitian ini dapat digambarkan dalam kerangka penelitian yang akan disajikan pada Gambar 1.



Gambar 1 Metodologi Penelitian

a. Deteksi

Pada dasarnya serangan MITM akan selalu memandatkan *broadcast* ARP untuk mencoba melakukan *poisioning*, dan ketika pelaku memulai serangannya, maka dengan otomatis Xarp akan membetrikan notifikasi bahwa adanya serangan ARP.

b. Pengumpulan Informasi

Melakukan aktivitas *sniffing* atau menyadap dan melakukan *capture* atau perekaman terhadap paket data lalu lintas jaringan *wifi* yang sudah terdeteksi ARP *Poisoning* dengan menggunakan aplitasi *wireshark.*

c. Preservasi

Tahap Preservasi dilakukan dengan menyalin dan mengamankan data maupun informasi yang ditemukan dalam tahap pengumpulan informasi yang sebelumnya telah dilakukan. Kemudian dilakukan dengan mengamankan file hasil perekaman lalu lintas data dalam bentuk ekstrak file berkstensi *p.cap* menggunakan aplikasi *wireshark.*

d. Pemeriksaan

Proses pemeriksaan dilakukan dengan cara memanfaatkan modul hirarki dan *comand-comand* filterisasi paket dari alat bantu *software wireshark.* Dari hasil pemeriksaan tabel hirarki terdapat 2 objek yang dapat dijadikan sebagai bahan analisa yaitu *port* HTTP dan *port* ARP.

e. Analisis Keamanan Jaringan

Pemeriksaan *Port* ARP Pada Nomor Paket 127078 Ditemukan Kegiatan ARP *Broadcast* Dari MAC *Address* Azurewav/ *Source* B2:6d:97. Isi Pesan *Broadcast Request* ARP Dengan IP 192.168.100.238 Mencoba Mengubungi Kepada 192.168.100.1.

3. HASIL DAN PEMBAHASAN

a. Data

Data diperoleh dengan menggunakan *tools wireshark* dengan cara memantau lalu lintas ARP dalam jaringan. Dengan menganalisis paket-paket ARP yang masuk, *user* dapat melihat adanya aktivitas yang mencurigakan seperti permintaan ARP yang tidak biasa atau *respons* yang tidak seharusnya. Tabel 1 dibawah ini merupakan tabel dari hasil data scanning jaringan *wireless* menggunakan *tools wireshark* saat jam kerja berlangsung.

Tabel 1 Data Hasil Scanning Jaringan Wireless

No	Source Address	Destination Address	Protokol
1	InterCor_b0:c9:d5	Broadcast	ARP
2	AzureWav_2b:6d:97	Broadcast	ARP
3	HuaweiTe_39:24:39	AzureWav_b2:6d:97	ARP
4	AzureWav_2b:6d:97	Broadcast	ARP
5	AzureWav_2b:6d:97	Broadcast	ARP
6	AzureWav_2b:6d:97	Broadcast	ARP
7	AzureWav_2b:6d:97	Broadcast	ARP
8	AzureWav_2b:6d:97	Broadcast	ARP
9	46:9e:82:90:8f:7c	AzureWav_b2:6d:97	ARP
10	TP-Link_9c:83:84	AzureWav_b2:6d:97	ARP
11	AzureWav_2b:6d:97	Broadcast	ARP
12	AzureWav_2b:6d:97	Broadcast	ARP
13	AzureWav_2b:6d:97	Broadcast	ARP
14	AzureWav_2b:6d:97	Broadcast	ARP
16	192.168.3.1	10:32:7E:7	ARP

I N F O R M A T I K A
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

		C:BE:EB	
17	192.168.3.60	3C:6A:A7:SE:77:E8	ARP
18	192.168.3.87	F4:60:E2:36:44:B4	ARP
19	192.168.3.106	C0:E4:34:8A:33:ID	ARP
20	192.168.3.107	3C:B6:B7:22:51:8D	ARP

b. Perancangan Serangan ARP Poisioning

Perancangan serangan ARP *Poisioning* bertujuan untuk mendapatkan informasi-informasi secara ilegal dari pengguna yang sedang berada pada jaringan *wireless* yang sedang disadap. Cara kerja dari serangan ini menggunakan teknik serangan *man in the middle attack.*

Penggunaan *tools* dan informasi yang dibutuhkan pada serangan *poisioning* dapat dilihat pada tabel 2.

Tabel 2. Tools ARP Poisioning

Nama Serangan	Tools	Informasi Yang Dibutuhkan
ARP *Poisioning*	Etercap	IP *Address user*
	Wireshark	IP *Address access point*

c. Skema Penyerangan ARP Poisioning

Serangan ARP *poisoning* menggunakan jaringan *access point* yang ada pada Universitas Dumai. Cara kerja dari Perancangan Serangan ARP *Poisioning* sebagai berikut:

1. Proses saat melakukan serangan, penyerang perlu berada di dalam jaringan *access point.*
2. Ketika telah berada di dalam jaringan *access point,* akan dilanjutkan ke tahap *scanning.* Pada tahap ini serangan akan dilakukan menggunakan *tools etercap.*
3. Dari hasil *scanning* akan ditemukannya IP *Address* berserta MAC *Address* yang terlihat sedang terhubung ke jaringan *access point.*
4. Pada *tools ettercap* ada yang namanya *access point isolation,* dimana bisa disimpulkan bahwa fitur ini membuat pembatasan antara semua *user* yang berada di jaringan tersebut sehingga semua *user* tidak dapat berkomunikasi secara bebas antar *user* yang satu dengan *user* lainnya. Maka sebaliknya jika tidak mengaktifkan fitur *access point isolation* dapat membuat semua *user* yang berada dalam satu jaringan yang sama bisa berkomunikasi secara bebas tanpa dibatasi.
5. Kemudian akan dilanjutkan dengan mensimulasikan serangan ARP *Poisioning* pada jaringan *access point* yang dijadikan target yaitu jaringan yang *wireless* pada Universitas Dumai dengan menggunakan *tools ettercap.*
6. ARP *Poisioning* bekerja dengan memanipulasi tabel ARP, dimana penyerang akan mengirimkan paket ARP palsu ke jaringan sehingga membuat isi tabel ARP akan tertimpa dengan ARP palsu yang dikirimkan oleh penyerang, sehingga membuat paket akan mengarah ke perangkat penyerang.
7. Ketika serangan berhasil, informasi-informasi dari pengguna bisa dicuri oleh penyerang.

Gambar 2 Skenario Penyerangan ARP Poisioning

d. Hasil Penyerangan ARP Poisioning

Tabel 3 merupakan data hasil dari *scanning* yang dilakukan menggunakan *tools ettercap* pada jaringan *wireless* di Universitas Dumai sebelum dilakukannya serangan ARP *Poisioning.*

Tabel 4. Data Sebelum dilakukan ARP Poisioning

No	IP Address Client	MAC Address	Ket
1	192.168.100.62	DC:41:A9:4E:50:AC	Target 1
2	192.168.3.60	3C:6A:A7:SE:77:E8	Non Target
3	192.168.3.87	F4:60:E2:36:44:B4	Non Target
4	192.168.100.1	84:AD:58:39:24:39	Target 2
5	192.168.3.107	3C:B6:B7:22:51:8D	Non Target

Pada tabel 4 diatas dapat dilihat bahwa Target 1 memiliki MAC *Address* DC:41:A9:4E:50:AC dan target 2 memiliki MAC *Address* 84:AD:58:39:24:39 yang mana MAC Address tersebut merupakan MAC

INFORMATIKA
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

Address Asli yang belum diubah.

Tabel 5 merupakan data hasil dari *scanning* yang dilakukan menggunakan *tools ettercap* pada jaringan *wireless* di Universitas Dumai setelah dilakukannya serangan ARP *Poisioning*.

Tabel 5 Data Sesudah dilakukan ARP Poisioning

No	IP Address Client	MAC Address	Status	Ket
1	192.168.3.1	10:32:7E:7C:BE:0	MAC Address Asli	Berhasil
2	192.168.3.60	3C:6A:A7:SE:77:E8	MAC Address Asli	-
3	192.168.3.87	F4:60:E2:36:44:B4	MAC Address Asli	-
4	192.168.100.1	80:C5:F2:B2:6D:97	MAC Address Sudah Tertukar/ sudah di ganti dengan MAC si penyerang.	Berhasil
5	192.168.3.107	3C:B6:B7:22:51:8D	MAC Address Asli	-

Pada tabel diatas dapat dilihat bahwa Target 2 yang awalnya memiliki MAC *Address* 84:AD:58:39:24:39 dan setelah dilakukan serangan ARP *Poisioning* MAC *Address* nya berubah menjadi 80:C5:F2:B2:6D:97.

Tabel 6 Data Hasil Scanning Jaringan Wireless Setelah Serangan ARP Poisioning

No	Source Address	Destination Address	Protokol	Ket
1	HuaweiTe_39:24:39	Broadcast	ARP	Asli
2	IntelCor_4e:50:ac	AzureWav_b2:6d:97	ARP	Asli
3	AzureWav_2b:6d:97	IntelCor_4e:50:ac	ARP	Duplicate
4	AzureWav_2b:6d:97	IntelCor_4e:50:ac	ARP	Duplicate
5	AzureWav_2b:6d:97	IntelCor_4e:50:ac	ARP	Asli
6	AzureWav_2b:6d:97	Broadcast	ARP	Asli
7	AzureWav_2b:6d:97	Broadcast	ARP	Asli
8	IntelCor_4e:50:ac	AzureWav_b2:6d:97	ARP	Asli
9	HuaweiTe_39:24:39	AzureWav_b2:6d:97	ARP	Asli
10	AzureWav_b2:6d:97	HuaweiTe_39:24:39	ARP	Duplicate
11	AzureWav_2b:6d:97	HuaweiTe_39:24:39	ARP	Duplicate
12	AzureWav_2b:6d:97	IntelCor_4e:50:ac	ARP	Duplicate
13	AzureWav_2b:6d:97	IntelCor_4e:50:ac	ARP	Duplicate
14	AzureWav_b2:6d:97	HuaweiTe_39:24:39	ARP	Duplicate
15	AzureWav_2b:6d:97	HuaweiTe_39:24:39	ARP	Duplicate
16	AzureWav_2b:6d:97	Broadcast	ARP	Asli
17	HuaweiTe_39:24:39	Broadcast	ARP	Asli
18	AzureWav_2b:6d:97	Broadcast	ARP	Asli
19	HuaweiTe_39:24:39	Broadcast	ARP	Asli
20	HuaweiTe_39:24:39	AzureWav_2b:6d:97	ARP	Duplicate
21	AzureWav_b2:6d:97	HuaweiTe_39:24:39	ARP	Duplicate
22	AzureWav_2b:6d:97	HuaweiTe_39:24:39	ARP	Asli
23	AzureWav_b2:6d:97	HuaweiTe_39:24:39	ARP	Asli
24	AzureWav_2b:6d:97	HuaweiTe_39:24:39	ARP	Asli

Pada table 6 diatas merupakan hasil setelah melakukan serangan dengan ARP *Poisioning* dilakukan *scanning* pada jaringan *wireless* di Universitas Dumai dan didapatkan hasil dimana ada satu buah MAC *Address* yang sudah berubah. Setelah dilakukan serangan dengan ARP *Poisioning* dan MAC *Address* nya sudah berubah, maka dapat dilakukan pencurian data seperti *username* dan *password*.

e. Hasil

Berdasarkan hasil simulasi serangan dan analisis keamanan jaringan wireless , maka dapat disajikan hasil penelitian sebagai laporan Jaringan. Hasil simulasi dan analisis dapat dirangkum pada tabel 7

I N F O R M A T I K A
Jurnal Informatika, Manajemen dan Komputer, Vol. 16 No. 1, Mei 2024
eISSN : 2580-3042
pISSN : 1979-0694

Tabel 7 Hasil Simulasi dan Analisa

No	Analisis	Keterangan
1	Serangan ARP *Poisioning* menggunakan aplikasi *Ettercap* pada Kali Linux	Berhasil melakukan serangan pada jaringan *wireless.*
2	*Protocol* serangan yang berhasil ditembus	*Protocol* ARP.
3	*Log Activity*	Terdapat duplicate yang cukup banyak pada *protocol* ARP dan dicurigai sebagai aktivitas yang tidak wajar.
4	a. *IP Address* Target *1* b. MAC *Address* Target 1 c. *IP Address Server* (Target 2) d. MAC *Address Server* (Target 2)	a. 192.168.100.62 b. DC:41:A9:4E:50:AC c. 192.168.100.1 d. 84:AD:58:39:24:39

Pada tabel 7 didapatkan hasil dari analisis serangan ARP Poisioning pada jaringan wireless menggunakan *tools Wireshark* dan mengunakan aplikasi *Ettercap* di Kali Linux.

Pengujian simulasi serangan ARP Poisioning ini membuat admin jaringan bisa mengetahui apakah jaringan wireless rentan terhadap serang seperti ARP Poisioning. Skenario seimulasi serangan ARP Poisioning pada jaringan wireless didapati hasil bahwa jaringan wireless di Universitas Dumai masih dapat tembus oleh serangan ARP Poisioning dan kemanan jaringannya masih kurang aman.

4. KESIMPULAN

Berdasarkan hasil analisis dan pengujian ARP *Poisioning* pada jaringan *wireless* di Universitas Dumai mengambil kesimpulan yaitu:

1. Perancangan ARP *Poisioning* dalam menganalisa keamanan jaringan *wireless* dari serangan *Man In The Middle Attack* berjalan lancar dan berhasil.
2. Pengujian rancangan ARP *Poisioning* menggunakan aplikasi *Ettercap* sebagai *tools* untuk melakukan penyerangan dan aplikasi *Wireshark* untuk melakukan analisis keamanan jaringan.
3. Tes simulasi serangan ARP ini memungkinkan administrator jaringan untuk menentukan apakah jaringan *wireless* rentan terhadap serangan seperti ARP *Poisioning*. Pada skenario simulasi serangan ARP *Poisioning* pada jaringan *wireless*, ditemukan bahwa jaringan *wireless* Universitas Dumai masih dapat ditembus oleh serangan ARP *Poisioning*, dan keamanan jaringan masih lemah.

5. REFERENSI

Ajharie, M. A., & Sulistiyono, M. (2022). Implementasi Framework Mitm (Man In The Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan. *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, *7*(1), 45-49.

Akbi, D. R. (2021). Analisis Address Resolution Protocol Poisoning Attack Pada Router Wlan Menggunakan Metode Live Forensics. *Jurnal Komputer Terapan*, *7*(1), 62-73.

Andriyansa, M. Z., & Panjaitan, F. (2020, August). Analisis Sistem Keamanan Jaringan Menggunakan Framework NIST. In *Bina Darma Conference on Computer Science (BDCCS)* (Vol. 2, No. 1, pp. 265-271).

Diansyah, T. M., Faisal, I., & Siregar, D. (2023). Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, *4*(1), 224-233.

Kamajaya, G. E. A. (2020). Analisa Investigasi Static Forensics Serangan Man in the Middle Berbasis Arp Poisoning. *JIKO (Jurnal Informatika dan Komputer)*, *3*(1), 6-12.

Panjaitan, A. F., Supardi, R., & Al Akbar, A. (2021). Penerapan Framework Man in the Middle Menggunakan Linux Pada Lembaga Penyiaran Publik Rri Bengkulu. *Journal of Technopreneurship and Information System*, *4*(3), 35-41.

Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60-67.

Saraun, A., Lumenta, A. S., & Sengkey, D. F. (2022). Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. *Jurnal Teknik Informatika*, *17*(1), 19-26.

Setiadi, R. R., Suryani, V., & Triawan, M. A. (2021). Implementasi dan deteksi serangan man-in-the-middle berbasis mitm proxy terhadap protokol https menggunakan metode k-

nn. *eProceedings of Engineering*, *8*(5).

Tammami, A. G. (2021). *Analisis Address Resolution Protocol Poisoning Attack Pada Router Wlan Menggunakan Metode Live Forensics* (Doctoral dissertation, Universitas Muhammadiyah Malang).

Zulkarnain, Z. (2020). Analisis Keamanan FTP server Menggunakan Serangan Man-In-The-Middle Attack. *Telcomatics*, *5*(1).