Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET TERHADAP SERANGAN *SYSTEM FAILURE* PADA TOKO SERVICES W-ELEKTRIK BATAM

Windri Nofedrinata[1], Andi Maslan[2]

[1]Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam
[2]Dosen Program Studi Teknik Informatika, Universitas Putera Batam
email: pb180210047@upbatam.ac.id

ABSTRACT

The research entitled Analysis of Network Security in Internet Facilities (Wifi) Against System Failure Attacks at the Batam W-Electric Service Shop is expected to help analyze network protocols and review network security. The technique used in this study is a descriptive approach, where this strategy is used to parse information by describing the information that has been collected without making changes when conducting research at the Batam W-Electric Service Store. Based on directed research, this shows how research in the W-Electric Service Store can be intercepted using ettercap and can be easily attacked in the form of a trojan, which is a wiretapping cycle by sending packets. Therefore it is suggested to the W-Elektrik Service Shop to further develop network security so that it is not easily hacked and attacked like a trojan.

Keywords: *Jaringan, Ettercap, System Failure.*

PENDAHULUAN

Pemanfaatan teknologi berbasis *Wireless* (Wi-Fi) sudah semakin banyak, baik digunakan untuk pendidikan maupun untuk komersial. Toko Service w-elektrik batam adalah toko yang bergerak di bidang jasa perbaikan khususnya *handphone* dan laptop serta penyedia *sparepart* elektronik. Toko service w-elektrik dibuka pada tahun 2020, dalam pengerjaan suatu perbaikan membutuhkan komputer dan laptop yang sangat membutuhkan akses internet atau berbasis *Wireless* (Wi-fi).

Wireless Fidility atau yang sering disebut dengan Wi-Fi merupakan perangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (Wireless Local Area Network/WLAN) yang didasari pada spesifikasi IEEE 802.11 dalam (Samsumar, 2017). Jaringan nirkabel atau *wireless* yang saat ini sangat sering digunakan bahkan dikembangkan karena jaringan nirkabel bisa digunakan pada setiap aspek skenario. Namun penggunaan jaringan nirkabel tidak luput dari kejahatan-kejahatan siber yang dilakukan dari pihak yang tidak bertanggung jawab yang bisa berakibat merugikan orang lain. Berdasarkan data Badan Siber dan Sandi Negara (BSSN), pada tahun 2020 terdapat total 495,4 juta upaya kejahatan siber di Indonesia, jauh lebih tinggi di bandingkan tahun 2019 yang hanya berkisar 290,3 juta upaya kejahatan siber. Terjadinya kenaikan serangan siber pada tahun 2020 (BSSN, 2020). Maka dari itu pentingnya menerapkan

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

suatu sistem keamanan jaringan yang cukup aman, sehingga bisa meminimalisir serangan-serangan terhadap jaringan, berupa pencurian data, ketidaktersediaan data atau informasi, hilangnya integritas atau keaslian data atau informasi dan lainnya yang berakibat merugikan. Pada toko service w-elektrik batam diketahui ada serangan trojan pada Jaringan Komputer yaitu serangan aktif. Serangan aktif adalah penyerang mendapatkan akses tidak sah ke jaringan dan kemudian memodifikasi data, baik menghapus, mengenkripsi atau merusaknya. Seperti yang sudah di ketahui toko w-elektrik batam sering terjadinya kegagalan sistem saat menggunakan software baik tools eror dan data yang corrupt oleh serangan trojan pada jaringan internet jelas ini dapat mengakibatkan terkendalanya pengerjaan perbaikian mau *software* ataupun *hardware*. Sehingga peneliti ingin menganalisis apa penyebab sering terjadinya *system failure* pada saat terkoneksi internet mau kabel ataupun nirkabel sehingga peneliti harus menerapkan keamanan jaringan.

Untuk menerapkan sistem keamanan jaringan yang cukup aman perlu dilakukan analisa terhadap sistem keamanan jaringan. Hasil dari analisa terhadap sistem keamanan bisa dijadikan sebagai bahan untuk melakukan evaluasi terhadap sistem keamanan jaringan. Pada toko services w-elektrik telah menyediakan fasilitas berupa jaringan nirkabel untuk digunakan sebagai media dalam membantu memenuhi kebutuhan informasi. Berdasarkan hal tersebut peneliti mengangkat judul Analisis Keamanan Jaringan Pada Fasilitas Internet Terhadap Serangan System Failure Pada Toko Services W-Elektrik Batam.

Berdasarkan uraian latar belakang informasi yang diberikan di atas, maka permasalahan yang dapat diangkat dalam penelitian ini adalah bagaimana menganalisis keamanan jaringan fasilitas internet terhadap serangan *system failure* pada toko service w-elektrik batam.

KAJIAN TEORI

2.1 Keamanan Jaringan Komputer

Menurut Gollmann dalam (Rajendra, 2022) keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer. Sedangkan menurut keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagai sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service).

2.2 Ettercap

Ettercap adalah alat untuk analisis protokol jaringan dan audit keamanan. Ettercap memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap password, dan melakukan menguping aktif terhadap protokol umum. Untuk latihan ini peneliti akan menggunakan ARP untuk mendeteksi virus LAN untuk password yang menggunakan SSL (Hotmail, Gmail, dll). ARP adalah

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

sebuah protokol jaringan komputer link layer untuk menentukan host jaringan atau alamat hardware saat hanya Internet layernya (IP) atau alamat Network Layer dikenal. Fungsi ini sangat penting dalam jaringan area lokal serta untuk lalu lintas internet working routing yang di gateway (router). Berdasarkan alamat IP ketika router hop berikutnya harus ditentukan. Jadi, dalam hal yang normal ARP adalah cara untuk mendapatkan alamat MAC dari Host atau Node dari alamat IP. ARP Spoofing adalah teknik yang akan digunakan untuk menyerang sebuah kabel atau jaringan nirkabel. ARP Spoofing memungkinkan penyerang untuk mendeteksi frame data dari LAN, kemudian memberi kemampuan untuk memodifikasi (baik untuk mengarahkan ke komputer sendiri untuk men-download mengeksploitasi korban) atau menghentikan lalu lintas dari memasuki jaringan yang spesifik komputer.

2.3 inSSIDer

InSSIDer adalah software yang berguna untuk memindai jaringan dalam jangkauan antena wifi komputer, melacak kekuatan sinyal dari waktu ke waktu, dan menentukan pengaturan keamanan yang digunakan (apakah dilindungi oleh password atau tidak)(Rante & Patras, 2018).

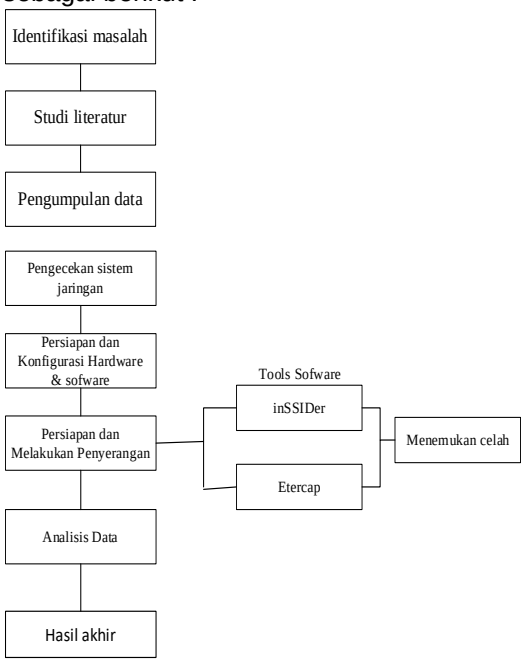
2.4 Trojan

Istilah "trojan" menggambarkan perangkat lunak berbahaya (malware) yang menginfeksi target dengan mendapatkan hak administrator pada sistem operasi Windows. Penyerang dapat mengelola komputer dari jarak jauh dengan membuka akses port pada komputer tersebut. Ide dasar di balik trojan ini adalah penggunaan RAT (Remote Administration Tool), yang sering digunakan untuk melakukan tugas jarak jauh pada mesin ketika izin akses telah disetujui. Trojan contoh ini, terkadang dikenal sebagai Trojan Akses Jarak Jauh, adalah jenis yang dapat beroperasi dari jarak jauh melalui akses jarak jauh. Ini berbeda dari apa yang dilakukan trojan karena tidak ada kesepakatan untuk penggunaannya, yang dapat membahayakan korban dan seringkali mengakibatkan kriminalitas. (Chandra et al., 2016)

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian menyediakan kerangka dan alur kerja mencakup sepanjang proses penelitian. Dalam desain penelitian ini, penulis membagi penelitian menjadi beberapa tahap sebagai berikut :



Gambar 3.1 Disain Penelitian

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

3.2 Analisis Jaringan

3.2.1 Analisis Sistem jaringan

Analisis sistem jaringan adalah proses mengevaluasi kinerja, konfigurasi, dan topologi jaringan komputer untuk menemukan masalah dan meningkatkan kinerja. Analisis ini dapat dilakukan pada jaringan lokal (LAN) atau jaringan luas (WAN). Berikut adalah beberapa elemen yang dapat di analisis dalam sistem jaringan:

1. Hardware: Meliputi perangkat keras seperti router, switch, firewall, server, dan perangkat keras lainnya yang digunakan dalam jaringan.
2. Software: Meliputi sistem operasi, aplikasi jaringan, dan perangkat lunak lainnya yang digunakan dalam jaringan.
3. Topologi: Meliputi arsitektur jaringan, seperti topologi bus, star, atau mesh, dan konfigurasi koneksi fisik antara perangkat keras.
4. Kinerja: Meliputi kecepatan jaringan, pemakaian bandwidth, dan kapasitas jaringan.
5. Keamanan: Meliputi keamanan fisik, keamanan logika, dan keamanan aplikasi dari jaringan.
6. Dokumentasi: Meliputi dokumentasi jaringan yang diperlukan untuk mengelola dan mengkonfigurasi jaringan.

3.2.2 Analisis data pada jaringan

Analisis jaringan menggunakan tools ettercap

Analisis jaringan menggunakan tools Ettercap. ettercap adalah alat open-source yang digunakan untuk melakukan analisis data jaringan dan man-in-the-middle (MITM) attacks.

Berikut ini tabel yang dapat digunakan untuk melakukan analisis data jaringan menggunakan tools Ettercap: Bahwa atribut pada tabel 3.1 berupa dari tools Ettercap. Setelah itu dapat ditentukan rule atau aturan suatu hostpot aman atau tidak yang menyebabkan *system failure*, penentuan rule sebagai berikut :

1. IF 192.168.1.1 Router and Konfigurasi firewall Aktif Routing Static TCP/IP patch update v1.0.2 then Status Aman

2. IF 192.168.1.2 Server and Konfigurasi firwall Aktif Routing Dynamic TCP/IP patch update v1.0.3 then Status Aman

3.IF192.168.1.3 Workstation and Konfigurasi firwall Off Routing there isn't any TCP/IP Patch update v1.0.1 then Status Tidak Aman

Tabel 3. 1 Tools ettercap

IP Address	Nama Host	Jenis Perangkat	Konfigurasi Firewall	Routing	Protokol jaringan	Patch dan Update	Status
192.168.1.1	Router	ACER	Aktif	Static	TCP/IP	v1.0.2 •	Aman
192.168.1.2	Server	Lenovo	Aktif	Dynamic	TCP/IP	v1.0.3 •	Aman
192.168.1.3	Workstation	Dell	Non- Aktif	-	TCP/IP	v1.0.1 •	Tidak aman

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

InSSIDer

Analisis jaringan menggunakan tools InSSIDer, adalah alat yang digunakan untuk menganalisis jaringan nirkabel (Wi-Fi) dan menemukan masalah yang mungkin terjadi.

Tabel 3.2 Tools InSSIDer

SSID	Signal	Chanel	Security	MAC.Addres	802.11
	-85	10	Wpa2/personal	OC:37:47:92:DF:97	n
	-85	10	Wpa2/personal	OE:37:47:B1:DF:97	n
Rumah putri	-80	11	Wpa2/personal	FC:A6:CD:BB:37:CO	n
Toko w-lektrik	-25	11	Open	36:E9:11:3A:75:99	n
Doraemon	-76	1	Open	68:37:47:92:DF:97	n
	- 80	3	Wpa2/personal	C4:A3:66:B1:75:14	n

Maka penentuan rule atau aturan sebagai berikut :

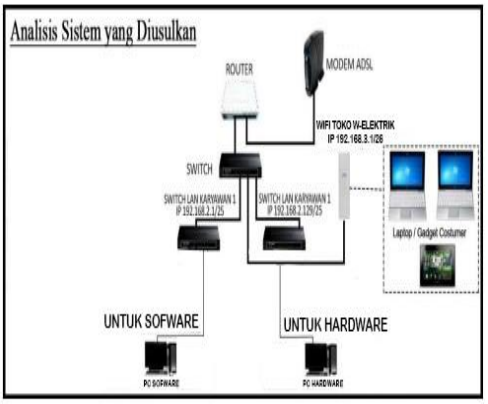
1.IF Rumah putri signal -80 chanel 11 Security Wpa2/personal and MAC Addres 802.11.n then status aman

2.IF Toko w-elektrik -25 chanel 11 security Open And MAC.Addres 802.11n then Status Tidak aman.

3.3 Rancangan Jaringan yang Dibangun/ Diusulkan

Analisis Sistem yang Diusulkan

Analisis sistem yang diusulkan yaitu identifikasi celah keamanan jaringan wifi dengan tools NetStumbler mengaudit keamanan jaringan dan memblokir lalulintas jaringan yang dianggap sebagai ancaman dalam jaringan internet serta melakukan pengecekan terhadap kesalahan pada bagian media, wireless, dan media koneksinya.



Gambar 3. 1 Analisis sistem yang diusulkan

Gambar 3.1 berupa analisis sistem jaringan yang diusulkan ada beberapa komponen yang di tampilkan berupa Modem ADSL,Router,Switch,Wifi Hotspot, Komputer, laptop. Sebelum peneliti menemukan analisis sistem yang diusulkan, perlu ditentukan tujuan dari jaringan tersebut dan kebutuhan yang harus dipenuhi. Kemudian, perlu dilakukan studi kelayakan untuk menentukan konfigurasi jaringan yang

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

sesuai dan memenuhi kebutuhan tersebut. Setelah itu, perlu dilakukan analisis kinerja jaringan untuk menentukan kapasitas yang diperlukan dan untuk mengidentifikasi potensi masalah yang mungkin terjadi.

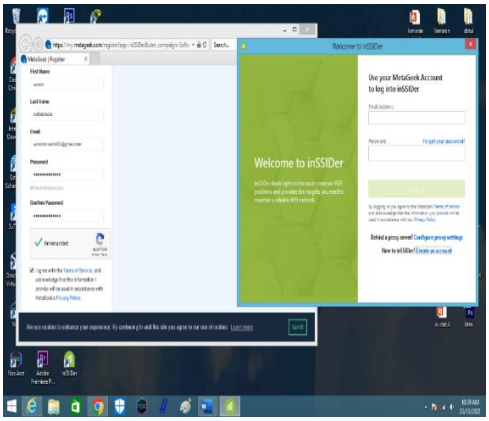
HASIL DAN PEMBAHASAN

4.1.1 Identifikasi keamanan wifi

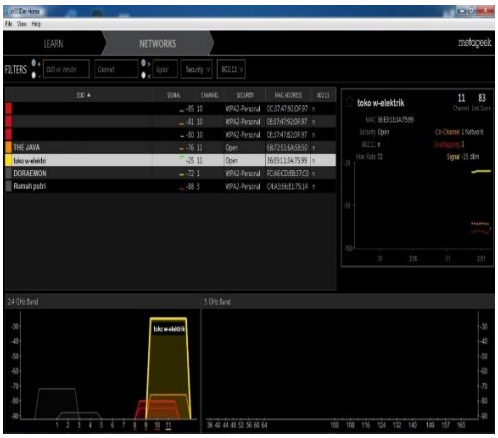
Identifikasi wifi ini dilakukan untuk mengetahui nama SSID, mac address, RSSI, network type dan security ditoko w-elektrik batam. Identifikasi wifi pada penelitian ini menggunakan inSSIDer.Analisis ini dilakukan untuk melakukan uji coba penyadapan jaringan untuk mendapatkan koneksi dengan jaringan wifi yang ada. Dari hasil identifikasi wifi, diketahui bahwa wifi ditoko w-elektri batam tidak ada pengamannya.Sehingga setiap laptop ataupun handphone yang ada di sekitar toko w-elektri batam dapat langsung terkoneksi.

4.1.2 InssIDer

Peneliti menjalankan software inSSIDer pada windows 10 dan secara otomatis akan menampilkan informasi tentang keberadaan *wifi* dengan lengkap dengan nama SSID, *mac address*, RSSI, *vendor, channel* yang dipakai, *network type* dan *security* atau keamanan yang digunakan.



Gambar 4. 1 Tampilan Register inSSIDer



Gambar 4. 2 Tampilan software inSSIDer saat identifikasi wifi.

4.1.3 Ettercap

Menggunakan tools ini dilakukan untuk mendapatkan informasi penting mengenai *account username, password,* akses DNS yang dituju dan informasi lain. Hal ini dimaksudkan agar penyerang dapat melakukan pengaksesan internet secara tidak sah demi keuntungan pribadi yang dapat mengakibatkan kerugian pada pengguna

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

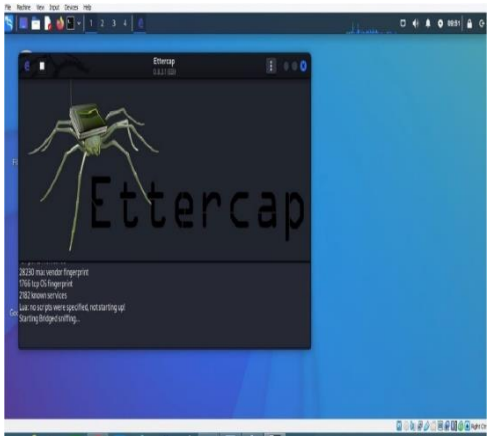
Jurnal Comasie

ISSN (Online) 2715-6265

yang berada dalam jaringan. Pada percobaan ini, berhasil diperoleh informasi mengenai akses DNS yang dituju dan penulis juga mendapatkan *username* dan *password*dari salah satu komputer target setelah melakukan skenario untuk login.Dengan demikian, penulis dapat menyatakan tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudahdicuri.

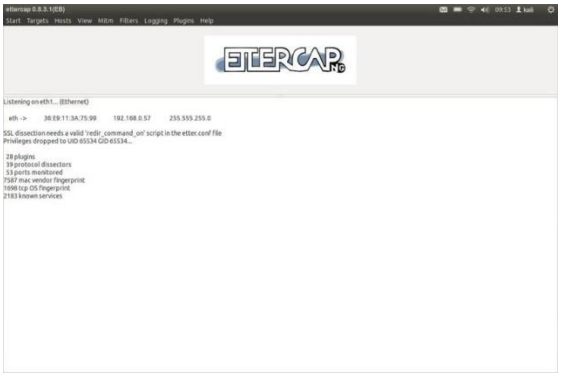
software ettercap pada *wifi*dilakukan dengan langkah – Langkah sebagai berikut :

a. Langkah pertama penulis menghidupkan *software ettercap* melalui terminal dengan perintah # *sudo ettercap –gtk*



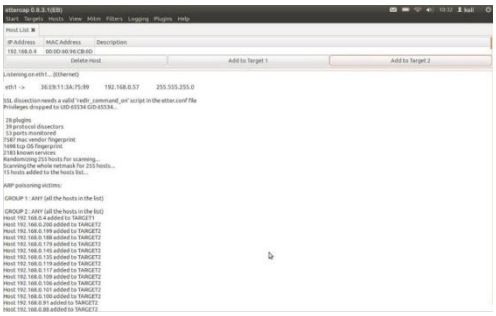
Gambar 4. 3 Tampilan Langkah pertama ettercap

b. Kemudian langkah kedua klik menu *sniff* pilih *unified sniffing*, lalu pilih *device eth1/device wifi* agar dapat berjalan pada jaringan *wifi* dan pilih *device eth0/device LAN Card*



Gambar 4. 4 Tampilan langkah kedua untuk device eth1.

Gambar 4.4. adalah tampilan *software ettercap* yang sudah berjalan/masuk pada jaringan wifi, terdapat beberapa informasi yaitu IP Address penyerang yang terdaftar pada jaringan wifi, jika terjadi kesalahan konfigurasi juga akan ditampilkan seperti gambar diatas terdapat tulisan “SSL dissection needs a valid “redir_command_on”script in the etter.conf”.



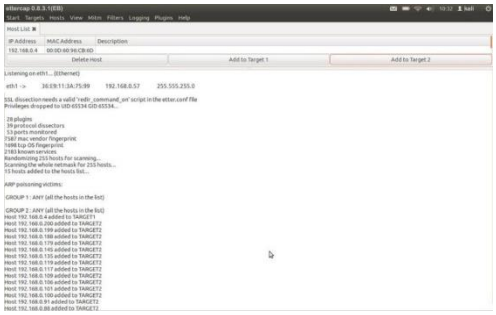
Gambar 4. 5 Tampilan langkah kedua untuk device eth0.

Gambar4.5.adalah tampilan *software ettercap* yang sudah berjalan/masuk pada jaringan. Langkah ketiga klik *host* untuk mencari host target pilih *scan host*

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

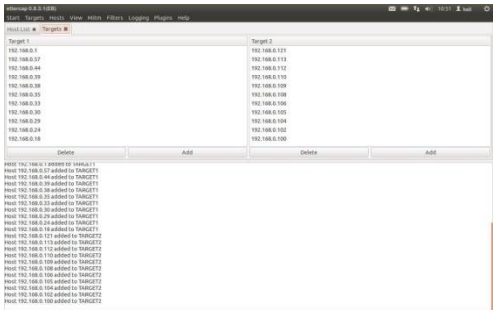
Jurnal Comasie

ISSN (Online) 2715-6265



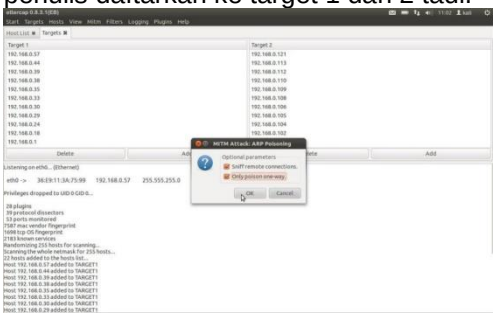
Gambar 4. 6 Tampilan langkah ketiga scan host target.

Gambar 4.6 adalah tampilan *software* ettercap ketika melakukan *scan* host, didalamnya terdapat informasi *IP Address* host yang tersambung pada jaringan *wifi*. Langkah keempat pilih host target



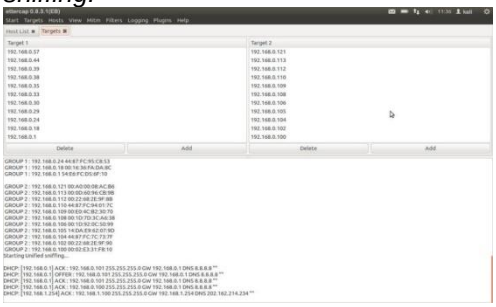
Gambar 4. 7 Tampilan langkah keempat memilih Host Target.

Gambar 4.7 adalah langkah untuk memilih host yang akan dijadikan target penyerangan, terdapat dua klasifikasi target yaitu target 1 adalah target utama yang akan diserang, target 2 adalah target alternatif jika target 1 tidak mendapatkan hasil. Melanjut ke langkah kelima klik MITM *Attack* untuk menyerang pilih ARP *poisoning* centang *sniff remote connections* dan *only poison oneway* untuk melakukan ARP *Poisoning* ke host yang telah penulis daftarkan ke target 1 dan 2 tadi.



Gambar 4. 8 Tampilan langkah kelima melakukan serangan pada wifi.

Gambar 4.8 adalah tampilan langkah untuk melakukan serangan *packet sniffing*, penulis memilih ARP *Poisoning* dan mencentang *sniff remote connections* dan *only poison one-way* agar dapat merekam *user* dan *password* akun email dan dns yang dituju oleh target. Kemudian langkah keenam klik *start*, pilih *start sniffing.*

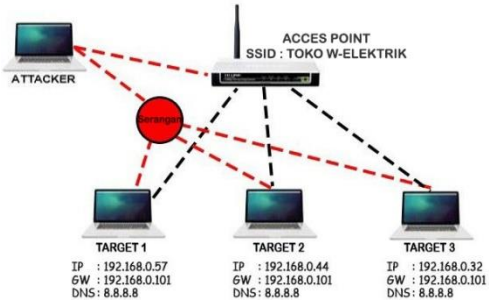


Gambar 4. 9 Tampilan serangan ettercap.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

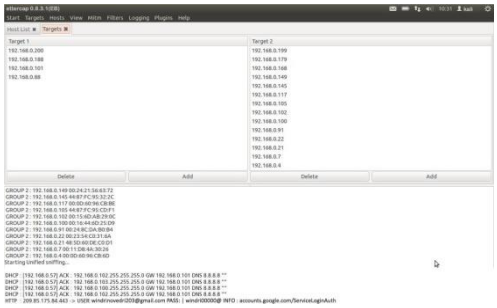


Gambar 4. 10 Tampilan simulasi penyerangan.

Gambar 4.10 adalah gambaran skenario dimana *attacker* melakukan penyerangan secara acak terhadap 3 komputer target yang dimana ketika target PC 1 tidak melakukan aktifitas maka penyerangan akan berpindah ke target PC 2 atauPC 3 begitu pula sebaliknya hingga *attacker* dapat merekam semua aktifitas yang berjalan. Karena dalam penelitian selama beberapa kali dalam jam kerja tidak menemukan aktifitas yang mengakses akun dan *password*, penulis melakukan duaskenario yaitu :

a. Skenario pertama dengan langkah sebagai berikut :

1. Membuat akun dan *password* baru.
2. Akun dicoba *login* menggunakan komputer kantor.
3. Penulis merekam aktifitas yang terjadi menggunakan *software ettercap*.



Gambar 4. 11 Hasil penyerangan Packet pada wifi.

Gambar 4.11 dapat diterangkan bahwa *software* dapat merekam beberapa aktifitas yang sedang terjadi pada komputer dalam satu jaringan. Kemudian pada baris yang di beri tanda garis merah menerangkan bahwa ada salah satu komputer *client* yang mengakses akun *google mail* terekam dengan *username*“windrinovedri203@gmail.com” dan *password*-nya“windri00000”

b. Skenario kedua melakukan penggantian *password* lama dengan *password* baru.

Gambar 4. 12 Hasil penyerangan Packet akun.

Gambar 4.12 menerangkan bahwa walaupun *password* dari akun“windrinovedri203@gmail.com” telah di ganti menjadi “pass123456”, tetapi masih tetap dapat direkam oleh aplikasi *ettercap*, dan bahkan masih dapat memantau aktifitas dari korban yang mengakses akun gmail dan youtube.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Berdasarkan uraian di atas, maka secara keseluruhan, hasil analisis dapat dilihat dalam tabel di bawah.

Tabel 4.1. Hasil Aktifitas Penyerangan

No	Aktivitas	*Software*	Keterangan	Hasil
1	Mengidentifikasi *Wifi*	*In*SSID*er*	Berhasil	Menampilkan nama SSID, *mac address*, RSSI, *network type* dan*security.*
2	Proses mengirim paket	*Ettercap*	Berhasil	Mendapatkan *username*serta *password*admin

4.1.4 Identifikasi Trojan

Tujuan dari identifikasi trojan di toko service elektrik batam adalah untuk mengetahui apakah ada trojan yang menyebar di jaringan komputer tersebut, dan jika ada, mengidentifikasi trojan tersebut agar dapat diambil tindakan pencegahan dan penanganan yang tepat. Identifikasi trojan juga bertujuan untuk mencegah penyebaran virus ke sistem lain di jaringan, serta untuk mengurangi risiko keamanan yang disebabkan oleh trojan.

Ada beberapa tools atau perangkat lunak yang dapat digunakan untuk mengidentifikasi trojan pada komputer:

1. Antivirus: Antivirus adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus virus, Trojan, dan ancaman lain yang mungkin ada pada komputer. Banyak antivirus memiliki fitur pemindaian yang dapat memindai sistem komputer dan menemukan ancaman yang terdeteksi.
2. Malware scanner: Malware scanner adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus malware, termasuk trojan. Beberapa malware scanner hanya menyaring file yang terinfeksi, sementara yang lain juga dapat memindai sistem untuk menemukan ancaman yang tersembunyi.
3. Security suite: Security suite adalah perangkat lunak yang menyediakan pelindung keamanan lengkap untuk komputer, Termasuk antivirus, firewall, dan fitur-fitur keamanan lainnya. Security suite dapat membantu mengidentifikasi dan menghapus virus trojan yang mungkin ada pada komputer.
4. Online virus scanner: Online virus scanner adalah layanan yang menyediakan pemindaian virus secara online. Dapat menggunakan online virus scanner untuk memindai komputer tanpa perlu menginstall perangkat lunak tambahan.
5. Command-line tools: Command-line tools adalah perangkat lunak yang dapat dijalankan dari command prompt atau terminal. Beberapa command-line tools yang dapat digunakan untuk mengidentifikasi trojan termasuk ClamAV, Chkrootkit, dan Rootkit Hunter.
6. Jika mencurigai adanya trojan pada komputer, Disarankan untuk menggunakan salah satu dari tools tersebut untuk memindai sistem dan menghapus ancaman yang terdeteksi.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Selalu pastikan untuk menjaga perangkat lunak
up-to-date agar dapat mendeteksi dan menghapus trojan yang terbaru.

Pembahasan

Hasil analisis yang didapat dalam penelitian ini adalah pembahasan pihak pengelola jaringan komputer pada toko service w-elektrik batam dan mendapatkan beberapa alasan mengapa *wifi* sangat rentang di serang virus:

1. Kurangnya keamanan : Jika jaringan *wifi* tidak dilindungi dengan benar, Dapat menjadi sasaran yang mudah bagi para penyerang untuk menyusup ke dalamnya dan menyebarkan trojan. Jaringan *wifi* yang tidak dilindungi dengan benar juga dapat dengan mudah ditembus oleh orang-orang yang tidak diinginkan, seperti pengguna *wifi* yang tidak sah.
2. Penggunaan password yang lemah: Jika menggunakan password yang lemah atau terlalu sederhana untuk jaringan *wifi*, Mudah bagi para penyerang untuk menebak password tersebut dan masuk ke jaringan.
3. Penggunaan perangkat yang tidak terlindungi: Jika menggunakan perangkat yang tidak terlindungi atau tidak diperbarui dengan benar, dapat menjadi sasaran yang mudah bagi trojan untuk masuk ke dalamnya dan menyebar ke jaringan *wifi*.
4. Pengunduhan file atau program yang tidak aman: Jika secara tidak sengaja mengunduh file atau program yang tidak aman ke perangkat yang terhubung ke jaringan *wifi*, Dapat menjadi cara bagi trojan untuk masuk ke jaringan.

Untuk menghindari serangan trojan pada jaringan *wifi*, Disarankan untuk mengaktifkan keamanan *wifi* dengan benar, menggunakan password yang kuat dan tidak mudah ditebak, memastikan bahwa semua perangkat yang terhubung ke jaringan dilindungi dengan benar, dan hanya mengunduh file atau program dari sumber-sumber yang terpercaya. Juga disarankan untuk menggunakan perangkat lunak antivirus yang terbaru untuk memindai jaringan *wifi* secara berkala dan menghapus ancaman yang terdeteksi.

Solusi Pencegahan terjadinya *system failure*

Ada beberapa solusi pencegahan yang dapat lakukan untuk mencegah terjadinya *system failure* pada komputer:

1. Update sistem operasi dan perangkat lunak: Pastikan untuk selalu mengupdate sistem operasi dan perangkat lunak yang terinstall pada komputer. Update ini biasanya menyertakan patch atau perbaikan keamanan yang dapat membantu mencegah terjadinya *system failure.*
2. Gunakan perangkat lunak antivirus: Antivirus dapat membantu mencegah terjadinya *system failure* dengan memindai sistem komputer ecara berkala dan menghapus virus, malware, dan ancaman lain yang mungkin ada. Pastikan untuk selalu menjaga perangkat lunak antivirus terbaru.
3. Back up data secara teratur: Selalu lakukan backup data secara teratur untuk mencegah hilangnya data jika terjadi *system failure*. Dapat menggunakan media penyimpanan

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

eksternal atau layanan cloud storage untuk menyimpan backup data.

4. Gunakan perangkat lunak pemeliharaan: Perangkat lunak pemeliharaan dapat membantu membersihkan sistem computer dari file sampah yang tidak diperlukan dan memperbaiki file yang rusak, sehingga dapat mencegah terjadinya *system failure*.
5. Gunakan power supply yang andal: Pastikan untuk menggunakan power supply yang andal dan tidak mudah rusak. Power supply yang tidak andal dapat menyebabkan masalah pada komputer, Termasuk *system failure*.
6. Jaga kebersihan komputer: Selalu pastikan untuk menjaga kebersihan komputer, Terutama pada bagian-bagian yang mudah terkontaminasi debu, seperti fan dan heatsink. Debu yang menumpuk dapat menyebabkan overheating dan menyebabkan *system failure*.
7. Gunakan kabel yang baik: Pastikan untuk menggunakan kabel yang baik dan tidak mudah rusak. Kabel yang rusak dapat menyebabkan masalah pada komputer, termasuk *system failure*.

SIMPULAN

Berdasarkan hasil analisis keamanan jaringan pada fasilitas internet terhadap serangan *system failure* pada toko service w-elektrik batam dapat diambil kesimpulan identifikasi dilakukan menggunakan fitur SSID, *mac address*, RSSI, *vendor*, *channel* yang dipakai, *network type security* dan hasilnya didapatkan *wifi* yang berada di area penelitian ini pengaman tidak kuat.

Percobaan yang dilakukan berhasil diperoleh informasi mengenai akses DNS yang dituju dan peneliti juga mendapatkan *username* dan *password email* dari salah satu target dan menyimpulkan bahwa *wifi* yang ada di toko services w-elektrik batam tidak aman karena semua kegiatan dapat dengan mudah terekam dan mudah dicuri.

DAFTAR PUSTAKA

BSSN, P. (2020). (I. S. Incid, Produser) Dipetik Desember 15, 2022, dari https://cloud.bssn.go.id/s/nM3m DzCkgycRx4S/down load

Samsumar, L. D. (2017). *Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan)*, 73–82. Retrieved Desember 15, 2022

E. S. 1 H. D. L. 2 A. C. D., Pendidikan Teknologi Informasi dan Komunikasi, FakultasTeknik, U. N. M., & Tondano, K. U. (2018). ANALISIS DAN PERANCANGAN JARINGAN KOMPUTER DI DINAS KOMINFO KABUPATEN MINAHSA.pdf. In *Engineering Education Journal (E2J-UNIMA)* (Vol. 6, Issue 1).

Aykarahmi Umasugi. (2022). *ANALISIS KEAMANAN JARINGAN WIFI TERHADAP PACKET SNIFFING DI Teknik Informatika Universitas Muhammadiya Maluku Utara Abstraksi*. *6*(2), 597–602.

Chandra, S. C. Y., Yulianto, F. A., & Satrya, G. B. (2016). Malware Analysis On Windows Operating System To Detect Trojan. *E-Proceeding of Engineering*, *3*(2), 3590–3595.

Rante, J. C., & Patras, M. A. R. (2018). Analisis Kekuatan Sinyal Wi-Fi

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Menggunakan Inssider. *Jurnal Ilmiah Realtech*, *14*(1), 97–102. https://doi.org/10.52159/realtech.v14i1.124

	Biodata Penulis pertama, windri Nofedrinata, merupakan mahasiswa Prodi Teknik Informatika Universitas Putera Batam
	Biodata Penulis kedua, Andi Maslan, merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam.