Jurnal Ilmu Komputer Revolusioner

Vol.7 No.12, Desember 2023
ISSN: 24430355

ANALISIS KEAMANAN JARINGAN WIRELESS LAN PADA KEARSIPAN DAN DATA DIPENGADILAN NEGERI KELAS 2A KOTA SIBOLGA

Rion Dui Haryadi Samosir
Universitas Pancabudi Medan
E-mail: rionharyadi4@gmail.com

Abstrak

Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting yang harus di benahi untuk melindungi aset-aset dan berbagai informasi. Keamanan jaringan adalah proses pencegahan yang dilakukan oleh penyerang untuk terhubung kedalam jaringan komputer melalui akses yang tidak sah atau penggunaan secara illegal dari komputer dan jaringan. Faktor-faktor penyebab resiko dalam jaringan komputer meliputi kelemahan manusia (Human error). Kelemahan perangkat keras komputer, kelemahan sistem operasi jaringan dan kelemaha n sistem jaringan komunikasi. Honeypot merupakan salah satu jenis keamanan jaringan yang mampu mengidentifikasikan penyerangan sehingga cocok diusulkan untuk di implementasikan pada Pengadilan Negeri Kelas 2A Kota Sibolaga. Honeypot adalah system palsu yang didesign mirip dengan sistem asli dengan tujuan untuk diserang dan di susupi. Honeypot hanyalah sistem palsu sehingga traffic dari dalam honeypot, itu dapat dicurigai sebagai aktifitas akses, yang tidak sah atau illegal. Dengan begitu, honeypot dapat menjadi alat bantu keamanan jaringan serta monitoring terhadap traffic jaringan. Hasil penelitian ini adalah penggunaan Honeypot sangat membantu dalam proses skema keamanan jaringan. Karena honeypot dapat menipu hacker dalam percobaan masuk ke system admin dengan membuat halaman web atau protocol web palsu. IDS Hasil Analisa dapat dijadikan acuan untuk lebih memperkuat jaringan wireless sehingga keamanan dan kerahasiaan data dapat terjaga dengan baik.

Kata Kunci *— Keamanan Jaringan,Honeypot,IDS.*

1. PENDAHULUAN

Perkembangan teknologi semakin lama semakin maju dengan pesat mendorong manusia untuk menciptakan teknologi baru yang dapat lebih bermanfaat dan mempermudah pekerjaan manusia. Tentunya perkembangan teknologi tersebut akan membuat laju informasi di dunia ini semakin cepat. Laju informasi yang begitu cepatnya membuat manusia harus mampu mengolah berbagai informasi yang ada untuk memperoleh suatu hasil

data yang diinginkan. Perkembangan teknologi komunikasi ini juga didukung dengan semakin meningkatnya kemajuan infrastruktur dan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan wireless. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol Wireless Fidelity (WiFi) yang berbasiskan standar IEEE 802.11. Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan penggunaan internet online services yang semakin cepat mendorong untuk memperoleh keuntungan dari shared data dan shared resources. Berbicara tentang jaringan internet, tentu kita sekarang sudah tidak asing lagi mendengar nama itu, semua orang didunia memanfaatkan internet untuk berbagai kepentingan seperti pendidikan, perusahan, perdagangan bahkan seorang anak kecil sekalipun sekarang sudah banyak menggunakanya. Dari sekian banyak manfaat internet, ada sebuah ancaman yang sangat besar mengintai pengunanya seperti Phising, Sniffing, Hacking, Cracking, Denial of Service Attack, Malcios dan kejahatan lainnya, baik untuk mengetes atau untuk keperluan yang tidak bertanggung jawab, seperti pencurian data, penyalahgunaan hak akses dll.

Dengan adanya ancaman-ancaman tersebut tentu kita sebagai pengguna akan merasa tidak aman karena bisa kapan saja ancaman tersebut dapat menyerang sistem, data dan jaringan kita. Oleh sebab itu diperlukan lah sebuah keamanan jaringan (Network Security) yang baik untuk mencegah dan menangani ancaman-ancaman seperti itu.

Penelitian ini menggunakan metode Penetration Testing, yang bertujuan melakukan analisis terhadap sistem keamanan teknologi WLAN yang sudah diterapkan di Pengadilan Negeri Kelas 2A Kota Sibolga.

Tujuan Pengadilan Negeri Kelas 2A melakukan penetration testing karena masih memiliki banyak celah untuk dieksploitasi dimana hasil penelitian yang dilakukan bahwa dari empat jenis serangan yaitu Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption, dan Man In The Middle, Jaringan WLAN belum memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan pada saat mengakses layanan internet.

Uji penetrasi adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. Dalam menganalisa keamanan jaringan WLAN dilakukan dengan metode Penetration Testing dimana bentuk serangan terhadap jaringan disimulasikan, software yang memiliki spesifikasi yang tepat dalam hal ini adalah Wireshark. Jaringan wireless m Walaupun memiliki sitem keamanan, jaringan wireless masih dapat di diserang oleh para attacked.

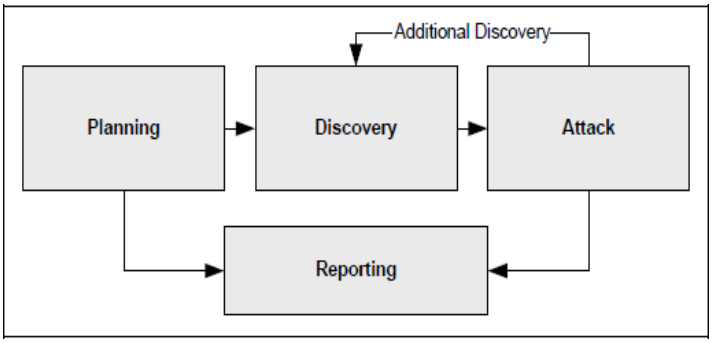
Dengan Wireless Local Area Network (Wireless LAN) pengguna dapat mengakses informasi tanpa mencari tempat untuk plug in dan dapat menset-up jaringan tanpa menarik kabel. Wireless LAN dapat mengatasi masalah kekurangan wired network, karena mempunyai kelebihan dibandingkan antara lain sebagai berikut: Mobility, Scalability, Installation Speed and Simplicity, Installation Fleksibility, Reduced cost of ownership. Teknologi informasi bukan tekonologi wireless yang menghasilkan berbagai kemudahan juga membawa dampak bagi para pengguna jasa internet baik industri, pendidikan dan user mandiri. Perkembangan ini juga dapat dirasakan secara langsung oleh kita dengan banyaknya wireless hotspot yang tersedia dimana-mana. Selain dapat membantu serta melahirkan berbagai inovasi yang positif tetapi juga melahirkan sisi negatif, dan ini selalu

terjadi tidak terkecuali pada perkembangan wireless.

Untuk membatasi permasalahan yang meluas, maka permasalahan yang akan dibahas dalam penelitian ini dibatasi pada infrastruktur protokol keamanan wireless LAN. Analisis dilakukan melalui beberapa kajian white paper yaitu sebuah dokumen yang berisi penjelasan akan sebuah masalah yang ingin diselesaikan suatu projek, serta penjelasan detil project, pembuatannya, dan interaksi dengan pengguna. Dan wacana yang ada serta melakukan eksperimen dengan melakukan serangan (attack) terhadap infrastruktur Wireless LAN. Metode keamanan Wireless LAN yang digunakan dalam penelitian ini yaitu Penetration Testing, dimana tindakan pengujian sistem dengan cara mensimulasikan bentuk-bentuk serangan terhadap sistem tersebut sehingga akan diketahui tingkat kerentanannya, dengan menggunakan tools yaitu Wireshark dan sistem operasi Kali linux.

2. METODE PENELITIAN

Penetration Testing atau disebut juga pentest adalah pengujian keamanan informasi dimana seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan. Pengujian ini dilakukan oleh asesor menggunakan serangan yang nyata, sistem yang nyata, dan data yang nyata menggunakan alat dan teknik yang sering dipakai oleh seorang hacker. Penetration Testing biasanya dilakukan bersamaan dengan Vulnerability Assessment (VA). Vulnerability Assessment adalah sebuah proses untuk mengidentifikasi risiko dan celah kerentanan pada aplikasi, sistem, ataupun jaringan. Sebagian besar pentest mencari kombinasi kerentanan pada satu atau lebih sistem untuk mendapatkan akses lebih dalam pada sistem yang menjadi target dibandingkan dengan hanya mengetahui satu macam kerentanan. Dalam menjalankan pengujian, terdapat 4 tahapan yang dijalankan dalam Penetration Testing yaitu tahap Planning (Perencanaan), Discovery (Penemuan), Attack (Serangan), dan Reporting (Pelaporan) seperti yang dijelaskan pada Gambar 1.



Gambar 1 Tahapan Metodologi Penetration Testing

Departemen Perdagangan AS menerbitkan rekomendasi tentang Pengujian Keamanan Jaringan sebagaimana ditetapkan di Institut Nasional Standar dan Publikasi Khusus Teknologi 800-42 (NIST SP 800-42). Metodologi dasar untuk penetration testing menurut NIST SP 800-42 terdiri dari empat fase yaitu Planning, Discovery, Attack, dan Reporting, lihat Gambar 3.1. Pada tahap awal Discovery, pentester dapat mengidentifikasi dan mengumpulkan informasi yang berpotensi terkait dengan target. Pengumpulan informasi

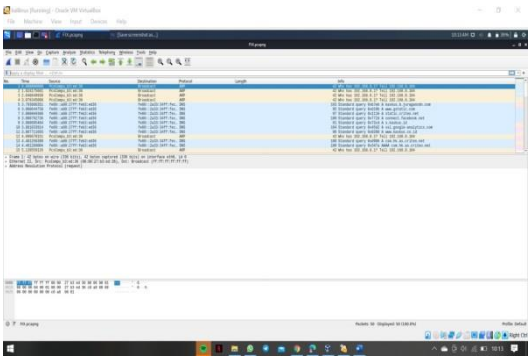
dapat dilakukan dengan berbagai teknik termasuk interogasi Sistem Nama Domain, InterNIC queries, Pencarian informasi dari server web organisasi target, Pencarian server Protokol Akses Direktori Ringan Lightweight Directory Access Protocol (LDAP) organisasi untuk informasi, Pengambilan paket, enumerasi NetBIOS, Sistem Informasi Jaringan, dan Banner grabbing (Rizdqi Akbar Ramadhan et al, 2020 IOP Conf. Ser.: Mater. Sci. Eng. 771 012019).

3. HASIL DAN PEMBAHASAN

Analisis ini perlu dilakukan agar dapat mengetahui seberapa aman tingkat keamanan yang ada dalam sebuah jaringan wireless lan pada Kantor Pengadilan Negeri Kelas 2A Kota Sibolga Seperti umumnya tingkat keamanan bukan berasal dari hardware dan software yang sudah ada namun terdapat peran penting dari manusia / pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri. Hasil dan pembahasan dari penelitian ini akan dilakukan penetration testing pada sistem Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption, dan Man In The Middle terhadap Access Point.

1. Analisa Lalulintas Jaringan Menggunakan Wireshark

Pada tahap ini akan dilakukan monitoring packet list (Daftar Paket) dimana sumber ip (Source Ip) dan tujuan ip (Ip Destination) dengan merekam dan memonitoring aktifitas jaringan pada interface wireless di modem Ruang IT (10.26.5.157) menggunakan wireshark. Dengan capture packet ini kita dapat mengetahui informasi-informasi seperti time, source, destination, protocol, length, dan info. Hasil capture packet dapat dilihat pada Gambar 4.1 dibawah ini.



Gambar 2 Hasil Capture Packet

Terlihat pada Gambar 2, bahwa penulis mengambil sampel sebanyak 10 packet data untuk mengetahui time, source, destination, protocol, length, dan info pada setiap masing-masing ip adress. Berikut penulis akan menyajikannya dalam bentuk hasil tabel, bisa dilihat pada tabel 1.

Tabel 1 Hasil Capture Packet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_b3: ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
2	1.024175	PcsCompu_b3:	Broadcast	ARP	42	Who has 192.168.8.1?

	601	ed:36				Tell 192.168.8.104
3	2.048849 930	PcsCompu_b3: ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
4	3.076345 060	PcsCompu_b3: ed:36	Broadcast	ARP	42	Who has 192.168.8.1? Tell 192.168.8.104
5	3.793886 351	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	103	Standard query 0xb7ebA kaskus.b.juragancdn.c om
6	3.800644 758	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	95	Standard query 0xd19b A www. Gstatic.com
7	3.800669 300	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	97	Standard query 0x1116 A static.criteo.net
8	3.800792 736	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	100	Standard query 0x772d A Connect. Facebook.net
9	3.800895 464	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	91	Standard query 0x73cdA s.kaskus.id
10	3.801033 914	Fe80::a00:27ff :feb3:ed36	Fe80::2a33: 34ff:fec7:fc38	DNS	104	Standard query 0x45d2 A ssl.google- analytics.com

Dari tabel diatas dapat diketahui bahwa terdapat 2 protocol yang berbeda yaitu ARP dan DNS, penulis akan menganalisanya untuk mengetahui infomasi secara detail apa saja yang terjadi didalam lalulintas jaringan sebagai berikut:

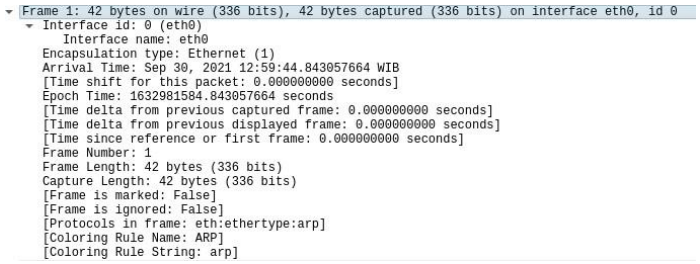
2. Analisis Protocol ARP

Untuk analisa pertama yaitu dengan melihat informasi lalu lintas jaringan pada protocol ARP, penulis akan mengambil sampel dari urutan no 1 dengan Ip sumber (Source) PcsCompu_b3:ed:36 dan tujuan (Destination) Broadcast, untuk mengetahui informasi secara detail dapat dilihat pada Detail Packet yang terdapat pada gambar 4.2 dibawah ini.

Gambar 3 Detail Paket ARP

Dari gambar 3 diatas ini, akan dijelaskan secara detail tentang Analisa lalulintas jaringan dengan menggunakan wireshark untuk mengetahui informasi dan kesimpulan apa saja yang didapatkan, berikut hasilnya akan dijelaskan pada bagian dibawah ini.

- Didalam box Frame 1 terdapat hal sebagai berikut:

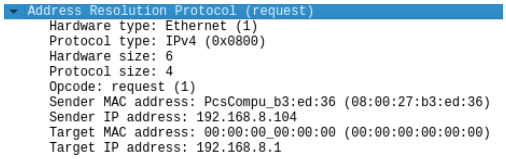


Interface name: eth0, Encapsulation type: Ethernet 1, Waktu kedatangan (Arrival Time) 30 September, 2021 pada jam 12:59.44 WIB.

- Didalam box Ethernet II terdapat hal sebagai berikut:

1. Tujuan (Destination): Broadcast (ff:ff:ff:ff:ff:ff).
2. Sumber (Source): PcsCompu_b3:ed:36 (08:00:27:b3:ed:36).
3. Type: ARP (0x0806).

- Didalam box ARP (Address Resolution) terdapat hal sebagai berikut:



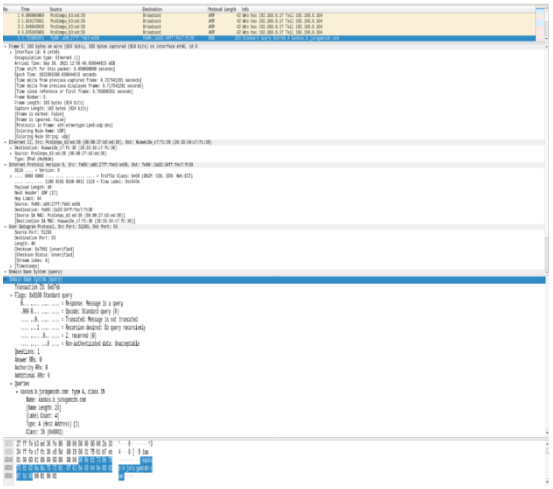
Hardware type: Ethernet (1).

1. Protocol type: IPv4 (0x0800).
2. Sender Mac address: PcsCompu_b3:ed:36 (08:00:27:b3:ed:36).
3. Sender IP address: 192.168.8.104.
4. Target Mac address: 00:00:00_ 00:00:00 (00:00:00:00:00:00).
5. Target IP address: 192.168.8.1.

Kesimpulan dari data yang didapat pada gambar diatas dapat diketahui bahwa ARP yang digunakan jenis Ethernet 1 sebagai tipe enkapsulasi dan eth0 sebagai nama interface. Waktu kedatangan (Arrival Time) 30 September 2021 pada jam 12:59.44 WIB, yang menunjukkan waktu pengiriman data. ARP request untuk sender dan target dapat diketahui berdasarkan ip address dan juga mac address dari protocol tersebut.

3. Analisis Protocol DNS

Untuk analisa kedua yaitu dengan melihat informasi lalulintas jaringan pada protocol DNS, penulis akan mengambil sampel dari urutan no 5 dengan Ip sumber (Source) fe80::a00:27ff:feb3:ed36 dan tujuan (Destination) fe80::2a33:34ff:fec7:fc38, untuk mengetahui informasi secara detail dapat dilihat pada Detail Packet yang terdapat pada gambar 4 dibawah ini.



Gambar 4 Detail Paket DNS

Dari gambar 4 diatas ini, akan dijelaskan secara detail tentang Analisa lalu lintas jaringan dengan menggunakan wireshark untuk mengetahui informasi dan kesimpulan apa saja yang didapatkan, berikut hasilnya akan dijelaskan pada bagian dibawah ini.

- Didalam box Frame 5 terdapat hal sebagai berikut:

```
Frame 5: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface eth0, id 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 30, 2021 12:59:48.636944015 WIB
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632981588.636944015 seconds
  [Time delta from previous captured frame: 0.717541291 seconds]
  [Time delta from previous displayed frame: 0.717541291 seconds]
  [Time since reference or first frame: 3.793886351 seconds]
  Frame Number: 5
  Frame Length: 103 bytes (824 bits)
  Capture Length: 103 bytes (824 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ipv6:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
```

1. Interface id: 0 (eth0), dengan tipe enkapsulasi ethernet 1.
2. Waktu kedatangan (Arrival Time): September 30, 2021. Jam 12:59:48 WIB.
3. Frame & Capture length: 103 bytes (824 bits) jika dikonversikan. Ini merupakan panjang isi paket jika diasumsikan paket sebagai array of char.

- Didalam box Ethernet II terdapat hal sebagai berikut:

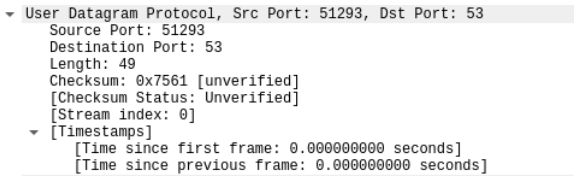
```
Ethernet II, Src: PcsCompu_b3:ed:36 (08:00:27:b3:ed:36), Dst: HuaweiDe_c7:fc:38 (28:33:34:c7:fc:38)
  Destination: HuaweiDe_c7:fc:38 (28:33:34:c7:fc:38)
      Address: HuaweiDe_c7:fc:38 (28:33:34:c7:fc:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: PcsCompu_b3:ed:36 (08:00:27:b3:ed:36)
      Address: PcsCompu_b3:ed:36 (08:00:27:b3:ed:36)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
```

1. Destination (tujuan): HuaweiDe_c7:fc:38 dengan mac address 28:33:34:c7:fc:38.
2. Sorce (sumber): PcsCompu_b3:ed:36 dengan mac address 08:00:27:b3:ed:36.
3. Tipe: IPv6 (0x86dd).

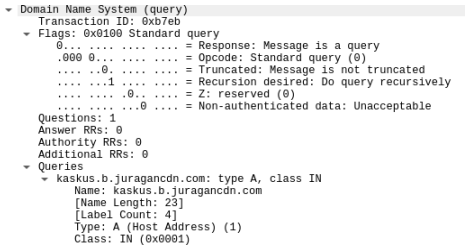
- Didalam box IPv6 terdapat hal sebagai berikut:

1. Source (sumber): fe80::a00:27ff:feb3:ed36.
2. Destination (tujuan): fe80::a00:27ff:feb3:fc38.
3. Payload length: 49, hop limit: 64.

- Didalam box UDP (User Data Protocol) terdapat hal sebagai berikut:



1. Source Port: 51293.
2. Destination Port: 53.
3. Length: 49, Checksum: 0x7561 [unverified] untuk memeriksa kesalahan data.
   - Didalam box DNS (Domain Name System) terdapat hal sebagai berikut:

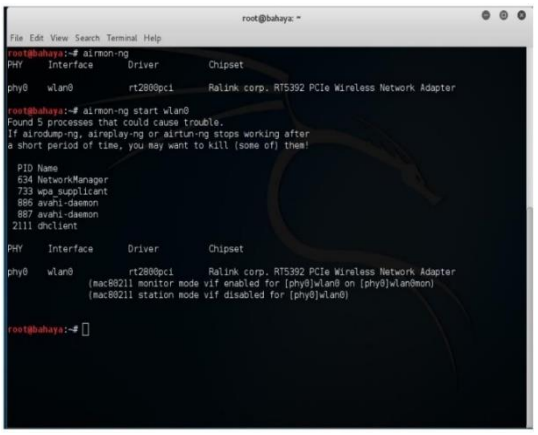


1. ID transaksi: 0xb7eb.
2. Queries: kaskus.b.juragancdn.com: type A, class IN.
3. Name: kaskus.b.juragancdn.com, Name length: 23, Label Count: 4, Type A (host address) dan Class: IN (0x0001).

Kesimpulan dari data yang didapat pada gambar diatas dapat diketahui bahwa DNS yang digunakan jenis Ethernet 1 sebagai tipe enkapsulasi dan eth0 sebagai nama interface. Waktu kedatangan (Arrival Time) 30 September 2021 pada jam 12:59.48 WIB, yang menunjukkan waktu pengiriman data. DNS (Domain Name System) dapat diketahui info yang sedang dibuka atau ditelusuri merupakan situs dari kaskus.b.juragancdn.com. Berhasil mendapatkan informasi berupa Gambar dan Tabel diatas. Informasi ini dinilai krusial karena menyangkut IP dari pengirim dan tujuan, IP ini dapat dimanfaatkan oleh pihak ketiga untuk mendapatkan informasi lebih lanjut yang ada pada komputer yang memiliki IP tersebut. Untuk meningkatkan keamanan jaringan komputer dapat menerapkan mirror server menggunakan Honeypot, agar penyerang tertipu dengan server palsu dengan IP yang sama akan tetapi tidak memiliki folder apapun didalamnya. Cara ini dapat mencegah penyerang yang telah mengetahui IP dari server, yang didapatkan dari teknik Sniffing

4. Cracking The Encryption

Tahapan yang pertama, dimana tujuan dari serangan ini adalah untuk mengetahui apakah semua Access Point dilindungi dengan sistem keamanan enkripsi seperti WEP, WPA ataupun WPA2. Penguji melakukan scanning terhadap Access Point Ruang Kantor (fe80::2a33::34ff:fec7:fc38) kemudian menentukan target untuk dilakukan cracking terhadap key yang digunakan sebagai pengamanan yang ditunjukkan pada Gambar 5.

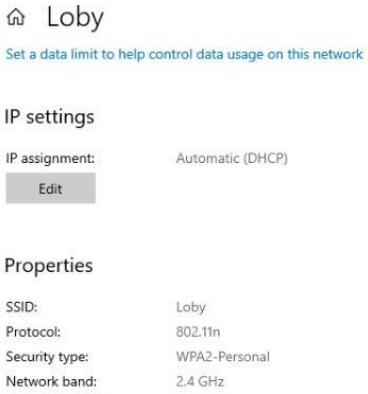


Gambar 5 Perintah Airmon-ng

Dari percobaan Cracking the Encryption dapat ditarik kesimpulan bahwa untuk meningkatkan ketahanan dari password terhadap upaya cracking, maka ada beberapa hal yang harus dilakukan, diantaranya:

- Menggunakan jenis keamanan enkripsi WPA, WPA2, WPA-PSK, atau WPA2 - PSK (PreShared Key) / Personal yang memiliki tingkat keamanan di atas WEP.
- Menggunakan kombinasi dari huruf besar, huruf kecil, angka dan simbol dalam membuat password, untuk mempersulit serangan baik dengan jenis brute-force attack maupun dictionary.
- Membuat password dengan panjang di atas 15 karakter, untuk mempersulit serangan baik dengan metode brute-force attack maupun dictionary.

Sedangkan dalam percobaan Cracking The Encryption hasil pengujiannya gagal, untuk mengetahui tipe keamanan pada access point, penulis akan mengcapture pada bagian properties access point seperti pada gambar 6.

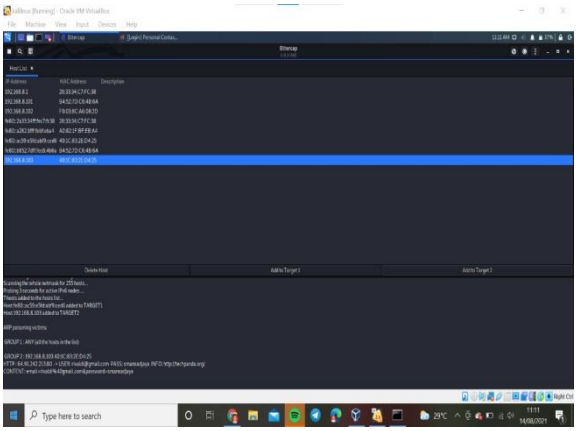


Gambar 6 Tipe Keamanan Access Point

Terlihat dimana type keamanan access point yaitu WPA2 - Personal, dimana WPA2 - Personal menggunakan satu kata sandi untuk semua penggunanya.

5. Man In The Middle (MITM) Attack

Dalam tahap ini dilakukan serangan terhadap user lain jaringan Wireless LAN yang sama dengan melakukan penyadapan paket data. Pengujian ini menggunakan aplikasi Ettercap sebagai alat uji. Tampilan Ettercap ditunjukkan pada Gambar 7.



Gambar 7 Hasil Ettercap

Pada tahapan Man In The Middle Attack, kondisi awal yang dibutuhkan adalah komputer user dan komputer target harus terhubung di jaringan wireless Access Point ‘ruang kantor’. Disini komputer tester berperan sebagai pihak ketiga diantara target dan access point yang menghubungkan antara target dan layanan internet. Dalam hal ini, pada konfigurasi Ettercap yang menjadi target pertama adalah gateway dari access point yaitu fe80::2a33::34ff:fec7:fc38 dan yang menjadi target kedua adalah IP dari komputer target yaitu 192.168.8.103.

Tahap selanjutnya adalah melakukan ARP Poisoning. Address Resolution Protocol (ARP) adalah sebuah protocol dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address). ARP Poisoning adalah suatu teknik menyerang pada jaringan komputer local baik dengan media kabel maupun wireless, yang memungkinkan penyerang bisa mengetahui frames data pada jaringan local atau melakukan modifikasi traffic atau bahkan menghentikan traffic. Pada Prinsipnya ARP poisoning ini memanfaatkan kelemahan pada teknologi jaringan komputer sendiri yang menggunakan ARP broadcast.

Setelah itu proses sniffing dijalankan, untuk kemudian semacam merekam aktifitas komputer target pada saat menggunakan layanan internet. Penulis menyajikannya dalam bentuk Tabel 2 dibawah ini.

Tabel 2 Hasil Ettercap

Target 1	Target 2	Informasi
access point (ip : fe80::2a33::34ff:fec7:fc38)	komputer target (ip:192.168.8.103)	HTTP: 64.91.242.213:80 .> USER: rionharyadi4@gmail.com PASS: rionharyadi99 INFO:http://techpanda.org/

Dari percobaan proses sniffing tersebut kemudian berhasil diperoleh informasi bahwa komputer target mengakses situs http://techpanda.org/ dan memasukkan user rionharyadi4@gmail.com serta passwordnya rionharyadi99. Namun pada saat komputer tester berusaha untuk merekam, pada saat komputer target membuka situs https://www.gmail.com/ ataupun https://www.facebook.com/ aplikasi Ettercap mengalami kegagalan. Setelah dianalisis ditemukan kegagalan dalam proses sniffing berasal dari protocol yang digunakan oleh web server, yaitu https. Perbedaan antara http dan htpps adalah https bekerja melalui system terenkripsi, sehingga dalam teori, informasi tidak dapat

diakses oleh pihak selain klien dan server akhir. Ada dua jenis umum lapisan enkripsi: TLS (Transport Layer Security) dan SSL (secure Socket Layer), yang keduanya menyandikan catatan data yang dipertukarkan.

Setelah itu kemudian pada komputer target dicoba untuk megakses situsfacebook dengan cara mengetikkan manual http://www.facebook.com/ pada kolom url dari web browser yang digunakan yaitu Mozilla Firefox. Namun hasilnya pada saat proses berjalan pada kolom url Kembali lagi menjadi https. Setelah dilakukan analisis kemudian ditemukan bahwa website www.facebook.com ternyata telah menggunakan mekanisme keamanan HSTS. HSTS merupakan singkatan dari (HTTP Strict Transport Security) yaitu mekanisme keamanan website yang memaksa web browser untuk mengakses website hanya via HTTPS. Jadi faktor kegagalan bukan disebabkan karena konfigurasi keamanan yang dimiliki oleh jaringan WLAN yang ada di 'Ruang kantor', namun lebih kepada konfigurasi keamanan yang dimiliki oleh web server dari situs yang di akses.

6. Hasil Penetration Testing

Dari hasil Secara keseluruhan, implementasi dari pengujian keamanan jaringan wireless local area network (WLAN) dengan metode penetration testing dapat dilihat pada Tabel 3.

No.	Jenis Serangan	Informasi yang Dibutuhkan	Status Serangan
1	Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark	Ip Source dan IP Destination.	Berhasil
2	Cracking The Encryption	Dictionary Word, handshake user lain, Channel yang digunakan dan BSSID dari access point.	Gagal
3	MITM	Attacker harus berada dalam jaringan WLAN, IP address dari user yang terkoneksi.	Berhasil

4. KESIMPULAN

Berdasarkan pengujian yang dilakukan Analisis Sistem Keamanan Jaringan Wireless Local Area Network dengan Metode Penetration Testing (Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, Cracking The Encryption, Man In The Middle) menggunakan kali linux Pengadilan Negeri Kelas 2A Kota Sibolga dapat disimpulkan sebagai berikut:

1. Dengan Analisa Lalulintas Jaringan (Traffic Network) Menggunakan Wireshark, dapat ditangkap komunikasi data dari protokol ARP & DNS, sehingga mampu di dapatkan informasi yang berupa IP address, time, source, destination, protocol, length, dan info.
2. Keamanan yang dimiliki oleh jaringan WLAN 'PT.PLN (Persero)' masih memiliki banyak celah untuk dieksploitasi. Hal ini dibuktikan dengan hasil penelitian yang dilakukan bahwa dari tiga jenis serangan yang dilakukan, hanya satu yang berstatus gagal

yaitu pada jenis serangan cracking the encryption.

3. Pengujian Man In The Middle (MITM), jaringan WLAN belum bisa memberi keamanan kepada user yang terkoneksi agar tidak mendapatkan gangguan maupun penyadapan dari user lain pada saat mengakses layanan internet yang sama

DAFTAR PUSTAKA

Alfurqon,D., Assegaff,S, 2018, Analisa Perancangan Jaringan Local Area Network Pada Laboratorium SMK Negeri 1 Kota Jambi, Jurnal Manajemen Sistem Informasi, Vol 3, No 3, ISSN: 2528-0082.

Basten, 2019, Analisa Manejemen Hotspot dengan Captive Portal, Skripsi, Program Pasca Sarjana Universitas Negeri Semarang, Unpublished

Jonathan, 2012, Manejemen Jaringan Wireless Menggunakan server Radius, Vol. 20 Nomor 1, ISSN 0853 – 6732

Muttaqin,A.H., Rochim,A.F., dan Widianto,E.D., 2016, Sistem Outentikasi Hotspot Menggunakan LDAP Dan Radius Pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer, Jurnal Teknologi dan Sistem Komputer, Vol. 4 Nomor 2, hal Jtsiskom 282 – 288, E-ISSN:2338-0304

Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), Bianglala Informatika,Vol. 2,No 2, Hal. 112-119

Purwanto,D., Dana,RD., 2015, Sistem Keamana Jaringan Model Client Server Menggunakan Enksripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebone, Jurnal Online ICT STMIK IKM, Vol. 13 Nomor 1

Riyasa,S., Mulyadi,A., dan Purwanto,Y., 2018, Analisa Dan Implementasi Sistem Redundasi Hot Standby Network Security Menggunakan Metode Intrusion Prevention System (IPS) Dan Captive Portal Pada Jaringan Nirkabel, Jurnal Teknik Komputer, No. 1 Vol.10

Setiawan,H, 2018, Rancangan Bangun Captive Portal Untuk Jaringan Wireless Berbasi open Source pada CV. Gempar production Palembang, Jurnal Teknologi Informasi, Vol. 7 No. 1, Hal. 36-44.

Sumarianta, 2011, Instalasi dan Konfigurasi Jaringan Komputer, Pustaka Setia, Bandung.

Suprianto,A., Riadi,I., 2013, Rancang Bangun Sistem Hotspot Menggunakan Captive Portal, Jurnal Sarjana Teknik Informatika, Vol. 1 Nomor 1, hal 172-180, E-ISSN: 2338-5197.

Wijaya,I.H., 2015, Analisis Dan Implementasi Proxy Server Sebagai Web Caching, Blocking Situs, Dan Monitoring Menggunakan Centos 6 Di Smkn Ganesha Tama Boyolali, Jurnal Teknologi Informasi & Pendidikan, Vol. 3, No.1.