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 WIFI TERHADAP SERANGAN SNIFFING DI PT DUTA *COMPUTER*

Putri Rosayanti Silalahi[1] , Sunarsan Sitohang[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

Technological developments and dependence on WiFi networks have brought many benefits in the business world, including at PT Duta Computer. However, network security is becoming a critical issue as cyber attacks become increasingly complex and sophisticated. One potential attack is a sniffing attack, in which the attacker tries to steal sensitive data that is sent over a WiFi network. This study aims to conduct an in-depth analysis of network security on WiFi facilities at PT Duta Computer against sniffing attacks. The results of this study are expected to provide deeper insight into the level of security of the WiFi network at PT Duta Computer and help companies to identify and address potential security vulnerabilities. By enhancing network security, PT Duta Computer can ensure that sensitive customer data and corporate information remain safe from sniffing attacks.

***Keyword**: Analisis keamanan ,Sniffing,Wireshark*

PENDAHULUAN

Karena sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat di pantau oleh para *hacker*, Baik jaringan *wired LAN* maupun jaringan *wireless LAN*, Maka banyak permasalahan mengenai keamanan jaringan dan keamanan jaringan yang sangat penting untuk diperhatikan. Pengguna atau peretas lain dapat mencegat atau mengubah data ketika *file* atau data yang perlu dikirim melewati beberapa terminal di jaringan. Sistem keamanan jaringan yang akan terhubung ke internet harus direncanakan dan dipahami dengan baik saat membangun jaringan karena harus dapat melindungi sumber daya seperti *file* atau data di jaringan secara efektif dan aman serta mengurangi serangan hacker. Fasilitas WiFi adalah salah satu teknologi yang banyak digunakan dalam jaringan komputer saat ini. WiFi memungkinkan pengguna untuk terhubung ke jaringan nirkabel dan mengakses internet tanpa harus menggunakan kabel. Namun, karena sifat nirkabelnya, jaringan WiFi rentan terhadap serangan sniffing. Sniffing adalah teknik yang digunakan untuk menangkap dan memonitor lalu lintas data yang melewati jaringan(Hidayat et al., 2018). Sniffer adalah perangkat lunak atau perangkat keras yang dapat digunakan untuk melakukan sniffing. Sniffer dapat memantau lalu lintas data yang dikirimkan dan diterima melalui jaringan, termasuk *username, password,* dan informasi pribadi lainnya. Serangan sniffing dapat membahayakan keamanan jaringan dan privasi pengguna. Sniffing dapat digunakan oleh penjahat siber untuk mencuri informasi pribadi pengguna, termasuk *username* dan *password*, atau bahkan informasi kartu kredit. Serangan sniffing juga dapat digunakan oleh pengguna jaringan yang tidak sah untuk memonitor aktivitas pengguna lainnya(Hidayat et al., 2018). Untuk mencegah serangan sniffing pada jaringan WiFi, diperlukan analisis keamanan jaringan. Analisis keamanan jaringan melibatkan pengecekan sistem keamanan jaringan, menemukan celah keamanan yang mungkin ada, dan menentukan strategi keamanan yang tepat untuk melindungi jaringan dari serangan sniffing*Wireshark* adalah *tools pakcet sniffing* yang digunakan

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

Jurnal Comasie
ISSN (Online) 2715-6265

untuk menganalisa terhadap protokol jaringan dan mengaudit keamanan jaringan. *Wireshark* juga mempunyai kemampuan untuk memblock lalu lintas yang lewat pada jaringan *LAN*, mencuri *password*, dan menyadap protokol-protokol umum yang aktif, dengan adanya *wireshark* maka dipastikan di selesaikan terhadap masalah yang timbul agar tidak terjadi, bisa diartikan bahwa *wireshark* merupakan aplikasi atau *software* untuk menganalisa gerak-gerik yang mencurigakan(Jaya et al., 2022). PT DUTA *COMPUTER* Sudah menerapkan jaringan *LAN* dan *WLAN* sebagai cara untuk berbagi data dan informasi tentang personel, layanan komersial atau publik, dan informasi penting lainnya. Setiap kamar memiliki jaringan yang terpasang, tetapi WiFi di setiap kamar seringkali rentan terhadap peretas atau orang yang ceroboh. Banyak orang yang menggunakan jaringan WiFi tidak menyadari risiko yang terkait dengan penggunaan titik akses nirkabel (WPA). Kebutuhan terhadap jaringan personal komputer sangatlah bertambah penting dalam pekerjaan, pendidikan maupun pada permainan dan dalam mengelola sebuah keamanan jaringan personal komputer itu sendiri, menggunakan banyaknya akses masuk kedalam itu jaringan tadi maka banyak peluang oleh para *hacker* untuk kejahatan yg akan terjadi pada jaringan tersebut, misalkan adanya peretas atau mencuri data/informasi penting yang terjadi pada jaringan tadi atau pun adanya hacker yang sengaja mematikan sumber daya jaringan itu tersebut (Hidayat et al., 2018).

KAJIAN TEORI

2.1.1 Jaringan komputer

Jaringan komputer (jaringan) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer(Astuti, 2018).

Berdasarkan kutipan dari (Komputer & Komputer, 2020), Jaringa komputer merupakan sekumpulan komputer. Ini artinya komputer tersebut lebih dari satu buah yang terpisah-pisah akan tetapi dapat saling berhubungan delam melaksanakan suatu tugas. Sekelompok komputer tersebut bekerja secara otonom. Ini artinya hanya dapat melakukan pertukaran dalam suatu area atau member tertentu. Pembuatan jaringan komputer ini menggunakan protocol komunikasi melalui media komunikasi yang saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Jaringan komputer juga dapat dikatak sebagai kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri dari satu atau lebih komputer yang saling terkoneksi seperti yang dijelaskan diatas.

2.1.5 KEAMANAN JARINGAN

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalah gunaan informasi *Internet of Things,* penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer. Pertama Kesalahan Informasi *Internet of Things*, Biasanya, dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs web dan mengunduh gambar, file, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer. jaringan wireless LAN atau jaringan WiFi adalah suatu jaringan area lokal nirkabel yang menggunakan gelombang radio sebagai media transmisinya, link terakhir yang digunakan adalah nirkabel, untuk memberi sebuah koneksi jaringan ke seluruh pengguna dalam area sekitar. Area

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

Jurnal Comasie
ISSN (Online) 2715-6265

dapat berjarak dari ruangan tunggal ke seluruh jaringan luas. Jaringan biasanya menggunakan kabel, dengan satu atau lebih titik akses jaringan menyambungkan pengguna nirkabel ke jaringan berkabel

2.2.1 *SNIFFING*

"Sniffing" atau "sniffing attack" adalah serangan yang dilakukan dengan cara memonitor atau mengawasi lalu lintas data yang melewati jaringan komputer, baik itu jaringan kabel atau nirkabel (wireless), untuk mencuri informasi sensitif seperti username, password, nomor kartu kredit, atau informasi penting lainnya yang dapat digunakan untuk tujuan penipuan atau kejahatan lainnya. Sniffing biasanya dilakukan dengan menggunakan alat atau program yang disebut "sniffer" atau "packet sniffer"(Hidayat et al., 2018). Sniffing sebenarnya bukanlah teknik hacking yang kompleks atau sulit dilakukan, namun dapat sangat efektif dalam mencuri informasi jika dilakukan dengan benar dan tanpa diketahui oleh korban atau pengelola jaringan. Oleh karena itu, penggunaan teknik sniffing untuk tujuan ilegal atau tanpa izin dapat dikenakan tindakan hukum dan merugikan banyak pihak(Hidayat et al., 2018).

2.2.2 Wireshark

Wireshark adalah sebuah program perangkat lunak yang digunakan untuk menganalisis jaringan dan paket data yang dikirim melalui jaringan. Program ini dapat digunakan untuk menangkap dan menganalisis paket data dari berbagai protokol jaringan, termasuk TCP/IP, HTTP, DNS, dan lain sebagainya(Jaya et al., 2022). Wireshark menyediakan antarmuka grafis yang memudahkan pengguna untuk menganalisis paket data dan mengidentifikasi masalah dalam jaringan. Program ini juga menyediakan fitur untuk menyimpan dan memuat file dump paket data, sehingga memudahkan analisis paket data yang terjadi pada waktu yang berbeda-beda(Jaya et al., 2022). Dalam konteks keamanan jaringan, Wireshark dapat digunakan untuk mendeteksi dan menganalisis serangan jaringan, seperti serangan DDoS, serangan phishing, dan lain sebagainya. Program ini juga dapat digunakan untuk memantau kinerja jaringan dan memperbaiki masalah jaringan yang terjadi(Jaya et al., 2022).

METODE PENELITIAN

3.1 Disain Penelitian

Desain penelitian dapat dijabarkan seperti pada gambar berikut:

Gambar 3. 1 *Disain Penelitian*

Sumber: Peneliti

Berikut adalah pembahasan dari gambar pada atas :

Identifikasi masalah, artinya dasar pada penelitian yang telah dibahas pada bab 1.

1. Pengumpulan bahan, yang dibutuhkan dalam sebuah penelitian dari segi *hardware* dan *software*.
2. Implementasi *wireshark*, yaitu aplikasi untuk capture data dari jaringan komputer yang dianalisa.
3. Analisa paket data, menganalisa data yang telah di capture dari aplikasi *wireshark* untuk mengetahui serangan yang datang.
4. Penarikan kesimpulan.

3.2 Analisis 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 dianalisis dalam sistem jaringan:

Hardware: Meliputi perangkat keras seperti router, switch, firewall, server, dan

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

Jurnal Comasie

ISSN (Online) 2715-6265

perangkat keras lainnya yang digunakan dalam jaringan.

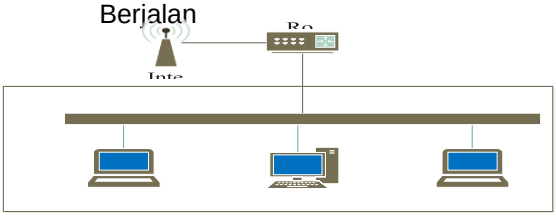
1. Software: Meliputi sistem operasi, aplikasi jaringan, dan perangkat lunak lainnya yang digunakan dalam jaringan
2. Topologi: Meliputi arsitektur jaringan, seperti topologi bus, Star, Atau mesh, dan konfigurasi koneksi fisik antara perangkat keras.
3. Kinerja: Meliputi kecepatan jaringan pemakaian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

3.2.1 Jaringan yang sedang berjalan

Analisa jaringan yang sedang berjalan pada perusahaan yang diteliti merupakan tahapan yang penting agar bisa mengetahui alur jaringan yang digunakan.

Berikut alur jaringan yang digunakan pada perusahaan yang akan diteliti :

1. Topologi Jaringan yang Sedang Berjalan



Gambar 3. 2 *Jaringan yang sedang berjalan*

2. Hardware
   Pada jaringan yang lama/sedang berjalan, ada beberapa perangkat keras yang sedang berjalan di PT.Duta Computer. Berikut ini perangkat-perangkat keras yang sedang berjalan :

Tabel 3. 1 *Perangkat keras yang sedang berjalan*

Nama Perangkat	Fungsi
Internet	suatu jaringan komunikasi yang menghubungkan satu mediaelektonik menggunakan media yang lainnya.
Router	menentukan jalur yang akan dilewati paket dari satu device kedevice yang berada di dalam jaringan

3. Kebijakan Bidang Jaringan yang Sedang Berjalan

Kebijakan pada jaringan digunakan sebagai manajemen keamanan di PT.Duta *Computer* agar mendapatkan alur kerja yang baik, aman, dan tentram. Kebijakan di perusahaan yang diteliti mencakup hal-hal berikut ini :

1. Tidak adanya pengaturan pembagian kuota internet pada setiap komputer.
2. Pada internet/wi-fi di PT.Duta *Computer* belum ada pembatasan pendaftaran menggunakan MAC Address sehingga pihak luar yang mengetahui password internet dapat langsung mengakses.
3. Tidak ada pemblokiran pada file/software pada setiap komputer sehingga user dapat install/download dengan bebas.

3.2.2 Jaringan yang sedang dibangun/diusulkan

Rancangan jaringan yang akan dibangun merupakan usulan dari peneliti agar mendapatkan hasil yang lebih efektif dan efisien dibanding jaringan yang sekarang dijalankan. Berikut usulan jaringan yang akan dibangun guna mendapat hasil yang lebih baik.

1. Topologi Jaringan yang

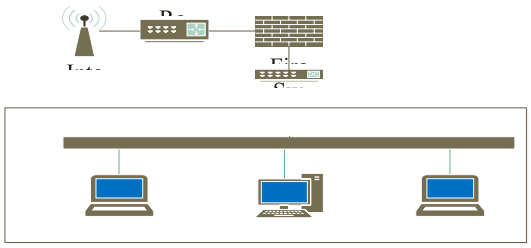
Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Diusulkan

Topologi jaringan yang diusulkan oleh peneliti untuk digunakan pada perusahaan yaitu Topologi Star. Berikut gambaran dari topologi jaringan yang sedang digunakan.



***Gambar 3. 3** Topologi Jaringan yang Diusulkan*

2. Hardware

Pada jaringan yang akan dibangun, terdapat beberapa perangkat keras yang diusulkan peneliti untuk digunakan di PT.Duta *Computer* Kota Batam. Berikut ini perangkat-perangkat keras yang diusulkan

Tabel 3. 2 Perangkat Keras yang Diusulkan

Nama Perangkat	Fungsi
Internet	suatu jaringan komunikasi yang menghubungkan satu media elektonik dengan media yang lainnya.
Router	menentukan jalur yang akan dilewati paket dari satu device kedevice yang berada di dalam jaringan
Firewall	Mengontrol dan mengawasi paket data yang mengalir dijaringan komputer.
Switch	Suatu jenis komponen jaringan komputer yang digunakan untuk menghubungkan beberapa *Switch/Router* dalam membentuk jaringan komputer yang lebih besar.

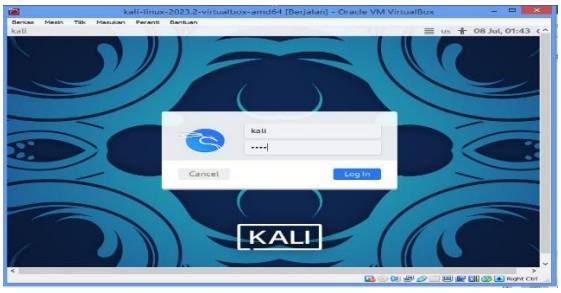
HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

4.1.1 Persiapan Tools

Disini peniliti melakukan instalasi *wireshark* menggunakan virtualbox.

1. Pada penelitian ini menggunakan *kali linux* dengan virtualbox. Sebelumnya peneliti sudah melakukan instalasi *Kali Linux*, Setelah berhasil menginstall barulah *Kali Linux* dapat dioperasikan seperti pada gambar 4.1.
2. Peneliti Membuat *Virtual Machine* dengan nama kali lalu mengkonfigurasikan *Operating System (OS) Kali Linux*.



Gambar 4. 1 Tampilan Login
(Sumber: Peneliti, 2024)

3. Selanjutnya penulis menekan tombol *Log in* untuk menjalankan *Operating System (OS) Kali Linux.* Seperti Gambar 4.2.

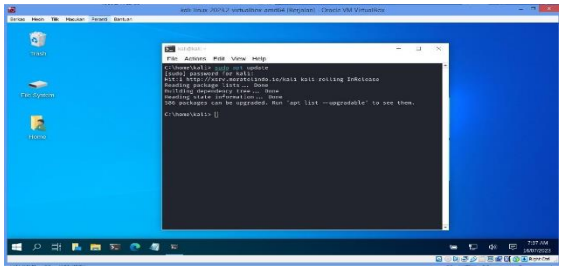
Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Gambar 4. 2 Tampilan dekstop *kali linux* undercover mode
(Sumber: Penelitian,2024)

4. PenulisMemasukkan *Username* kali dan *password* kali. Sesuai dengan yang diset pada saat menginstalasi *Operating System Kali Linux* Pada Gambar 4.2.
5. Instalasi *Wireshark* kedalam komputer menggunakan virtualbox Disini peniliti melakukan instalasi *wireshark* menggunakan virtualbox median terminal di*Kali linux*

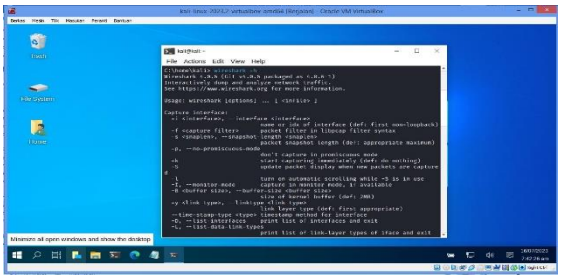


Gambar 4. 3 Melakukan Update
(Sumber: Penelitian,2024)

6. Peneliti melakukan *Update* terlebih dahulu sebelum melakukan penginstalan pada *wireshark* dengan perintah ($sudo apt update) dan masukan *Username* dan *Password.* Setelah selesai melakukan *update.* Bisa dilihat pada gambar 4.3.

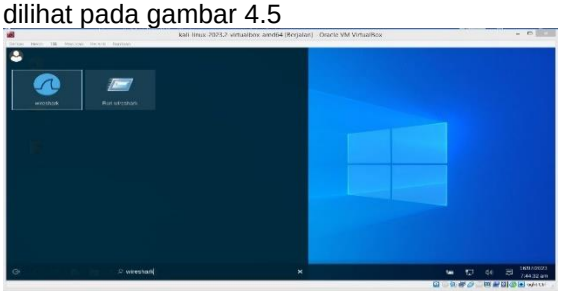
Gambar 4. 4 Tampilan terminal saat menginstal *wireshark*
(Sumber: Penelitian, 2024)

7. Selanjutnya peneliti melakukan instalasi pada *wireshark* menggunakan perintah ($sudo apt-get install wireshark) melalui terminal. Setelah memasukkan perintah melalui terminal akan dikasih pilihan saat penginstalan apakah ingin melanjutkan atau tidak dengan menekan Y melanjukan atau N tidak melanjutkan. Bisa dilihat pada gambar 4.4



Gambar 4. 5 Memeriksa utilitas *wireshark* disistem
(Sumber: Peneliti, 2024)

8. Setelah selesai melakukan instalasi pada *wireshark,* Ketik dua perintah berikut untuk memeriksa utilitas *wireshark disystem* ($ wireshark -h atau $ tshark -h) melalui terminal. Bisa dilihat pada gambar 4.5



Gambar 4. 6 Membuka *wireshark*
(Sumber: Peneliti, 2024)

9. Setelah sudah melakukan penginstalan selesai, Selanjutnya membuka tools wireshark. Bisa dilakukan dengan pencarian yang sudah tersedia di*kali linux.* Bisa dilihat pada gambar 4.6.

4.1 Pembahasan

4.1.2 Hasil analisis serangan *sniffing*

a. Berikut langkah-langkah terhadap target PT Duta *Computer* dari skenario yang dilakukan:

1. peneliti memastikan target berada didalam satu jaringan yang sama pada saat analisis.
2. Peneliti mulai menganalisis pada website PT Duta *Computer* apakah website tersebut aman atau tidak.

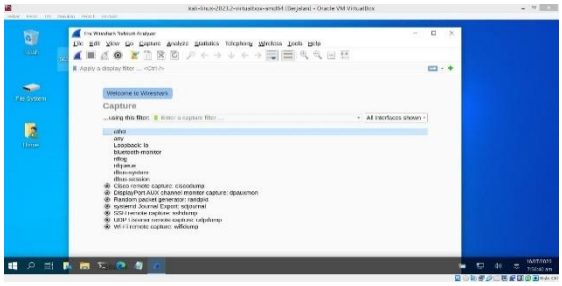
Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

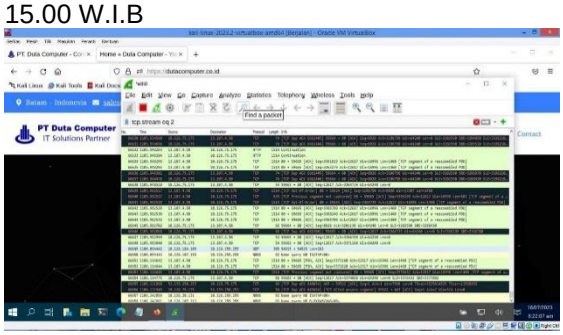
3. Selanjutnya peneliti akan melakukan penyerangan proses keamanan pada sistem website tersebut.
4. Peneliti menganalisis aktivitas dari target dan software *wireshark* dapat merekam beberapa *packets list* yang masuk.

b. Berdasarkan website PT Duta *Computer* yang akan dianalisis, Peneliti menggunakan WiFi yang sama pada saat analisis berlangsung.



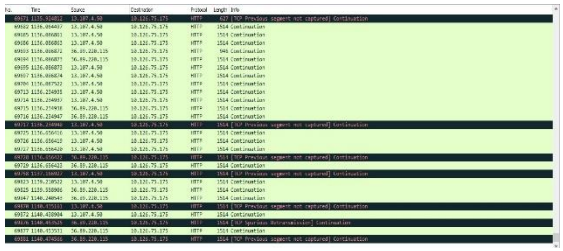
Gambar 4. 7 Tampilan *interface* pada *wireshark*
(Sumber: Peneliti, 2024)

1. peneliti membuka *software wireshark.* Langkah pertama analisis adalah pilih *interface* jaringan yang diinginkan.Terdapat beberapa *interface* yang bertugas untuk meng*capture packet.* Pada tahap ini penulis memilih *interface eth0.* Seperti gambar 4.9. Tampilan awal membuka aplikasi *Wireshark* divirtualbox pada gambar 4.9 bisa dilihat beberapa menu ditampilan awal seperti file, Edit, Vew, Go, Capture, Analyze, Statistics, Telephony, Wirelees, Tools dan Help.
2. Jam kerja pukul 08:00 W.I.B – pukul 15.00 W.I.B



Gambar 4. 8 Monitoring jaringan wifi hari I
(Sumber: Peneliti, 2024)

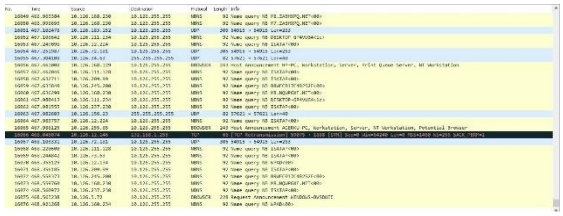
3. Pukul 08:22 W.I.B – Pukul 10:00 W.I.B
4. Peneliti mulai monitoring jaringan *wifi* dengan satu jaringan PT.Duta *Computer*.



Gambar 4. 9 Monitoring jaringan *wifi* hari II

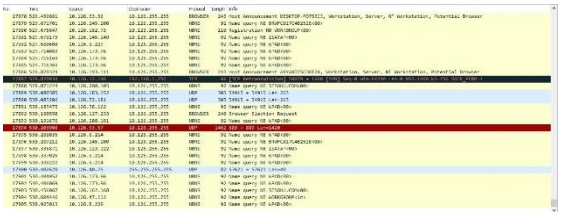
(Sumber: Peneliti, 2024)

5. Pukul 10:00 W.I.B – Pukul 11:00 W.I.B



Gambar 4. 10 Monitoring jaringan *wifi* hari II
(Sumber: Peneliti, 2024)

6. Pukul 11:00 W.I.B – Pukul 13.00 W.I.B



Gambar 4. 11 Monitoring jaringan *wifi* hari II

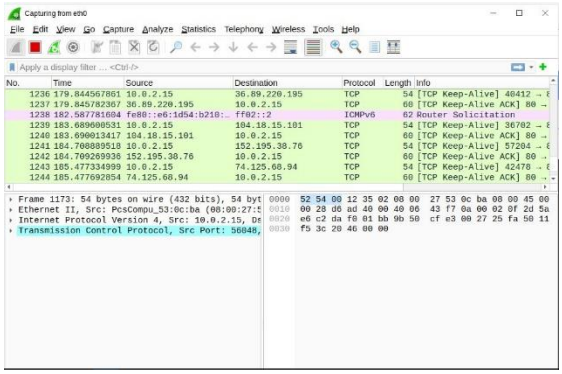
(sumber: Peneliti, 2024)

7. Pukul 13:00 W.I.B – Pukul 14.00 W.I.B
8. Pada gambar 4.9 menunjukkan sedang melakukan menangkap *packets* yang sedang berjalan, Peneliti sudah *runningkan* tools *wireshark* tersebut sudah berlangsung selama lima jam. Bisa dilihat hasil pada gambar 4.9, gambar 4.10, gambar 4.11.
9. Peneliti mulai monitoring kembali, Dengan satu jaringan *wifi* dihari yang berbeda PT.Duta *Computer*, Dihari ke dua. Bisa dilihat pada gambar 4.13

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

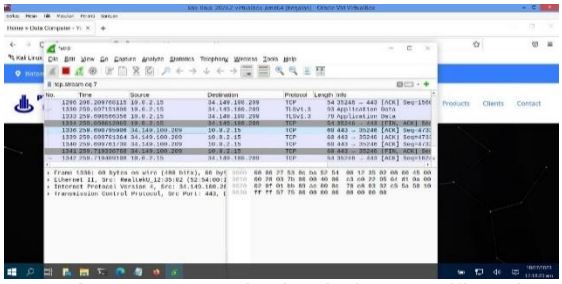
Jurnal Comasie

ISSN (Online) 2715-6265



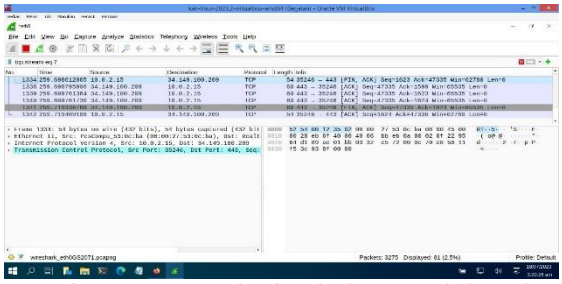
Gambar 4. 12 Monitoring jaringan WiFi hari II
(Sumber: Peneliti, 2024)

10. Pukul 08:00 W.I.B – Pukul 09:00 W.I.B



Gambar 4. 13 Monitoring jaringan *wifi* Hari II
(Sumber: Penelitian, 2024)

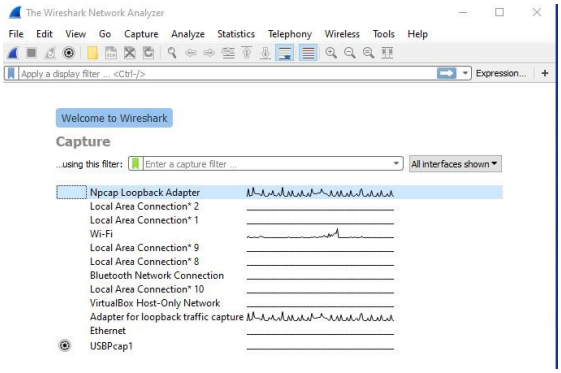
11. Pukul 09:00 W.I.B – Pukul 12:16 W.I.B



Gambar 4. 14 Monitoring jaringan WiFi Hari II
(Sumber: Peneliti, 2024)

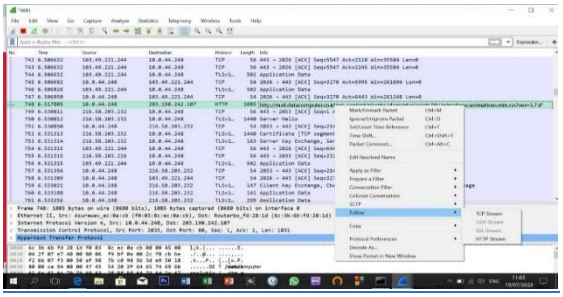
Pukul 12:16 W.I.B – Pukul 13:00 W.I.B

12. Pada gambar 4.15 menunjukkan tidak ada penyerangan *sniffing,* Peneliti sudah *runningkan* tools *wireshark* tersebut sudah berlangsung selama lima jam.
13. Peneliti akan melakukan skanario penyerangan *sniffing* untuk memastikan apakah website PT.DUTA *COMPUTER* aman terhadap *sniffing*



Gambar 4. 15 Skanario penyerangan Hari III
(Sumber: Peneliti, 2024)

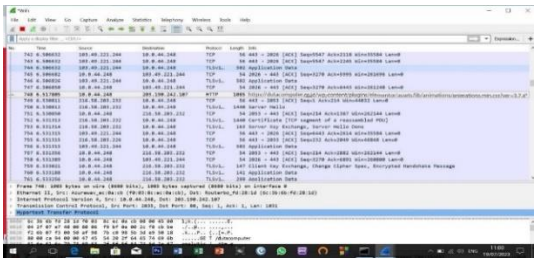
14. Setelah memilih jaringan yang ingin diiginkan penyerang dapat melihat aktifitas jaringan tersebut seperti gambar 4.17.



Gambar 4. 16 Analisis menggunakan menu *follow stream*
(Sumber: Peneliti, 2024)

Pukul 08:00 W.I.B – Pukul 11:00 W.I.B

1. Pada gambar 4.16 menu *follow stream* diatas dapat dilihat bahwa ada beberapa paket jaringan, namun disini juga dilihat bahwa komputer yang beralamat 10.0.44.248 sedang mencoba mengakses 203.190.242.107 atau membuka website http://mail.dutacomputer.co.id/ dengan menggunakan protocol HTTP.

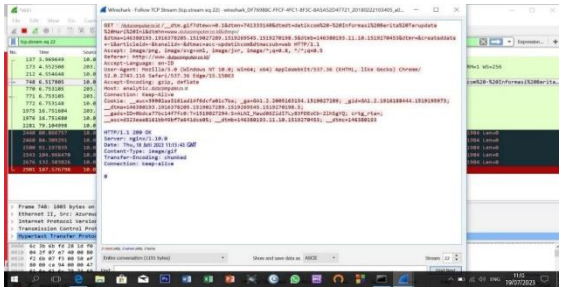


Gambar 4. 17 Analisis menggunakan menu follow stream

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

Jurnal Comasie

ISSN (Online) 2715-6265



(Sumber: Penelitian, 2023)

2. Pada gambar 4.17 memiliki protocol http dan klik langsung analyze kemudian follow dan pilih TCP Stream

Gambar 4. 18 Analisis data

Tabel 4. 2 *Hasil Aktifitas Sniffing Mengguanakan wireshark*

No	Waktu	Sumber IP	Tujuan IP	Protokol	Deskripsi Aktivitas
1	09:15:23.456	192.168.0.10	216.58.207.46	TCP	Permintaan HTTP GET ke google.com
2	09:15:23.789	216.58.207.46	192.168.0.10	TCP	Tanggapan HTTP 200 OK dari google.com
3	09:15:24.123	192.168.0.10	52.14.154.89	DNS	Permintaan DNS untuk mengonversi alamat IP google.com
4	09:15:24.456	52.14.154.89	192.168.0.10	DNS	Tanggapan DNS dengan alamat IP google.com
5	09:15:25.678	192.168.0.10	74.125.24.102	TCP	Permintaan HTTP GET ke google.com dengan parameter pencarian
6	09:15:26.012	74.125.24.102	192.168.0.10	TCP	Tanggapan HTTP 200 OK dengan hasil pencarian dari google.com
7	09:15:27.345	192.168.0.10	172.217.164.14	TCP	Permintaan HTTP GET ke google.com/maps
8	09:15:27.678	172.217.164.14	192.168.0.10	TCP	Tanggapan HTTP 200 OK dari google.com/maps
9	09:15:28.901	192.168.0.10	151.101.65.69	HTTPS	Permintaan HTTPS GET ke api.github.com
10	09:15:29.234	151.101.65.69	192.168.0.10	HTTPS	Tanggapan HTTPS 200 OK dari api.github.com

Pada tabel 4.2 mencakup beberapa aktivitas yang bisa terjadi saat *sniffing* xmenggunakan Wireshark. Setiap aktivitas memiliki nomor urut, waktu terjadinya, alamat IP sumber, alamat IP tujuan, protokol yang digunakan, dan deskripsi singkat tentang aktivitas tersebut.

Adapun rule/aturan yang digunakan saat proses *sniffing* menggunakan *wireshark.* Mungkin mengacu pada pembuatan aturan (rule) filter menggunakan fitur Display Filters di Wireshark. Display Filters memungkinkan user memfilter dan menampilkan paket yang spesifik berdasarkan kriteria tertentu.

1. Menampilkan paket dari alamat IP sumber tertentu:

```
ip.src == 10.0.44.248
```

2. Menampilkan paket ke alamat IP tujuan tertentu:

```
ip.dst == 203.190.242.107
```

3. Menampilkan paket dari atau ke port tertentu:

```
tcp.port == 80
```

4. Menampilkan paket yang menggunakan protokol HTTP:

```
http
```

5. Menampilkan paket dengan kata kunci atau string tertentu dalam isi (payload):

```
contains "username"
```

6. Menampilkan paket DNS:

```
arp
```

7. Menampilkan paket ARP:

```
arp
```

8. Menampilkan paket yang memiliki panjang lebih dari jumlah tertentu:

```
frame.len > 1000
```

9. Menampilkan paket ICMP (ping):

```
icmp
```

10. Menampilkan paket dengan alamat IP sumber dan tujuan tertentu:

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

Jurnal Comasie

ISSN (Online) 2715-6265

ip.src == 10.0.44.248&& ip.dst == 203.190.242.107

Pengguna dapat menggabungkan berbagai kriteria dan operator logika (seperti && untuk AND dan || untuk OR) untuk membuat aturan filter yang lebih kompleks sesuai dengan kebutuhan. Durasi penggunaan *Wireshark* untuk *sniffing* dapat bervariasi tergantung pada beberapa faktor, seperti kompleksitas jaringan yang sedang dipantau, jumlah lalu lintas yang dilewati, daan tujuan dari *sniffing* tersebut. Peneliti untuk mendapatkan data yang diingin setidaknya satu jam saat melakukan scaning mendapatkan data yang diperoleh berbentuk text berupa waktu, Sumber IP, Tujuan IP, Protokol dan Deskripsi Aktivitas (TCP,DNS dan HTTPS). Dalam kondisi normal, Pengguna dapat menjalankan *Wireshark* selama yang diinginkan dan memberhentikannya kapan pun merasa sudah mencukupi. Pengguna dapat memilih untuk membatasi waktu perekaman dengan menggunakan fitur filtrasi pada *Wireshark* untuk memfokuskan analisis pada periode waktu tertentu atau jenis paket tertentu.

simpulan

berdasarkan hasil penelitian,

1. keamanan pt duta *computer* sebenarnya perlu ditingkatkan, akses domain name server (dns) yang dituju serta informasi lainnya. selain itu masih banyak pengguna jaringan internet yang masih awam dengan yang namanya *sniffing* pada jaringan komputer.
2. bisa disipulkan alamat website pada pt duta *computer* tidak aman, karena keamanan kuki (cookies): kuki adalah file kecil yang dikirim oleh server web dan disimpan diperamban pengguna. sering digunakan untuk menyimpan informasi otentikasi dan sesi. ketika kuki dikirim melalui protokol http, dengan mudah dicuri dan digunakan

DAFTAR PUSTAKA

anugrah, k. (2018). *pengenalan osi layer kata kunci : pengenalan osi layer*. 1–5.

astuti, i. k. (2018). fakultas komputer indah kusuma astuti section 01. *jaringan komputer*, 8. https://id.scribd.com/document/503304719/jaringan-komputer

hidayat, m. t., sn, f. m., & kurniati, n. i. (2018). *analisis keamanan jaringan pada fasilitas internet (wifi) gratis terhadap serangan packet sniffing*. *1*(2), 112–119.

sanjaya, m. d. (2019). *analisis keamanan jaringan pada fasilitas internet (wifi) terhadap serangan packet sniffing pada kantor indosat ooredoo pekanbaru* (doctoral dissertation, universitas islam riau).

rizkyani, r. (2019). *analisis keamanan jaringan pada fasilitas internet (wifi) terhadap serangan packet sniffing di kantor koran seruya* (doctoral dissertation, universitas cokroaminoto palopo).

kurniawan, t. a. (2020). analisa keamanan jaringan wifi terhadap serangan packet sniffing. jurnal ilmiah fakultas teknik limit's vol, 16(2), 11.

sundari, s. (2021). analisis keamanan jaringan komputer pada fasilitas wireless fidelity (wifi) terhadap serangan paket sniffing di sentral yamaha palopo (doctoral dissertation, universitas cokroaminoto palopo).

	biodata penulis pertama, putri rosayanti silalahi , merupakan mahasiswa prodi teknik informatika universitas putera batam
	biodata penulis kedua, sunarsan sitohang, s.kom., m.ti. , merupakan dosen prodi teknik informatika universitas putera batam.