ANALISIS KEAMANAN JARINGAN *WIFI* TERHADAP *PACKET SNIFFING* DI KAMPUS A UNIVERSITAS MUHAMMADIYAH MALUKU UTARA

Aykarahmi Umasugi [(1)], M.Dzikrullah Suratin[(2)], Sahrial Hamza[(3)]
Teknik Informatika Universitas Muhammadiya Maluku Utara
e-mail : *aykarahmiumasugi17@gmail.com*

Abstraksi

Di Kampus Universitas Muhammadiyah Maluku Utara khususnya Kampus A hotspot internet dan kualitas sangat dibutuhkan karena untuk kebutuhan Dosen, Pegawai Kampus, dan juga Mahasiswa. UMMU telah menyediakan fasilitas internet wifi yang bida di akses penggun. Pengguna dapat mengakses hotdpot kapan saja tanpa harus meminta password. Namun hanya saja koneksi tersebut dapat saja di ganggu atau di hack oleh orang-orang yang tidak bertanggung jawab, Sebaba itu dibutuhkan network analizer protokol. Metode yang digunakan untuk membuat implementasi yaitu penganalisaan dan perancangan system yang dimana merancang sebuah topologi, menginstal aplikasi eteercap dan wireshark yang nantinya digunakan oleh peneliti. Prosess pengujian menggunakan metode black box testing dari sisi perangkat hardware dan software sehingga proses pengujian berjalan dengan baik.
***Kata Kunci**: Campus, Wifi Sniffing, Ettercap and Wireshark*

Abstract

AT the Muhammadiyah University Campus Nort Maluku especially Campuas A, internet hotspots and quality are very much needed because for the needs of lecturees, Campus Employees, and also UMMU students, they have provided wifi internet facillites that can be accessed by users, users can access hotpot enytime. Without having to ask for a password. But its just because it requires a network protokol analizer. The method used to make the implementation is system analysis and design which designs a topology, intalis the ettercap and wiresharhk aplications which will be used by researchers, the testing process uses the black testing method in terms of hardware and software device so that the testing process goes well.
***Keywords**: Campus, Wifi Sniffing, Ettercap and Wireshark*

PENDAHULUAN

Dengan berkembangnya teknologi informasi yang sangat cepat terutama internet, memberikan dampak yang sangat besar pada pengguna dan kebutuhan akan jaringan komputer semakin bertambah, baik dalam pendidikan maupun pekerjaan, salah satu hal penting dalam mengelola jaringan komputer yaitu keamanan dari jaringan itu sendiri dengan banyaknya akses ke jaringan maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan tersebut terutama munculnya kejahatan sehingga internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker. baik jaringan Wired LAN maupun wireless LAN. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut.

Universitas Muhammadiyah Maluku Utara merupakan salah satu kampus Swasta yang berada di Kota Ternate Provinsi Maluku Utara. Kampus UMMU menyediakan fasilitas jaringan komputer yang biasanya dikenal dengan Wireless sebagai sarana untuk mencari dan mengetahui sistem informasi seperti mata kuliah, Absensi, Pengisian Kartu Rencana Studi (KRS), Web Portal, penginputan nilai, dan lain – lain. Dari hasil observasi tentu peneliti mengetahui bahwa di Lab Informatika UMMU didapatkan celah keamanan jaringan yang sangat masih rentan akan ancaman serangan ke masing- masing ruangan yang terdapat jaringan Wireless. Untuk menguji keamanan dari jaringan server tersebut. maka peniliti akan melakukan uji penetrasi jaringan menggunakan aplikasi *eteercap Wireshark* atau a*nalyzer* protokol terhadap *Serve*r, dan user atau pengguna yang aktif terutama yang ada dalam cakupan penggunaan jaringan *Wireless* tersebut,

ISSN: 2548-8082/ E-ISSN 2615-6350
Volume 6 No. 2 Edisi 2022

dengan batasan - batasan seperti tidak melakukan perusakan terhadap jaringan atau yang dapat merugikan pihak - pihak yang terkait.

A. LANDASAN TEORI

1. Jaringan Komputer
   [1] menyatakan bahwa jaringan adalah kumpulan dua atu lebih komputer yang masing-masing berdiri sendiri dan terhubung melalui sebuah teknologi.
2. Keamanan Jaringan

[2] Keamanan komputer *(computer security)* merupakan keamanan informasi yang terdapat pada komputer atau jaringan. Keamanan komputer juga dikenal sebutan *Cybersecurity* atau *IT Security*. Keamanan komputer bertujuan membantu pengguna agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Berdasarkan level keamanan dapat dibagi menjadi 3 macam, yaitu:

a. Keamanan Level 0, merupakan keamanan fisik (*Physical Security*) atau keamanan tingkat awal. Apabila keamanan fisik sudah terjaga maka keamanan di dalam computer juga akan terjaga.
b. Keamanan Level 1, terdiri dari database *security*, data *security*, dan *device* security. Pertama dari pembuatan database dilihat apakah menggunakan aplikasi yang sudah diakui keamanannya. Selantunya adalah memperhatikan data *security* yaitu pendesaian *databas.*
c. *Device Security* adalah yang dipakai untuk keamanan dari database tersebut.

METODE PENELITIAN

Metode penelitian yang digunakan adalah untuk menguji keamanan dari jaringan server tersebut. maka peniliti akan melakukan uji penetrasi jaringan menggunakan aplikasi *ettercap* dan *Wireshark* atau analyzer protokol terhadap Server, dan user atau pengguna yang aktif terutama yang ada dalam cakupan penggunaan jaringan *Wireless t*ersebut.

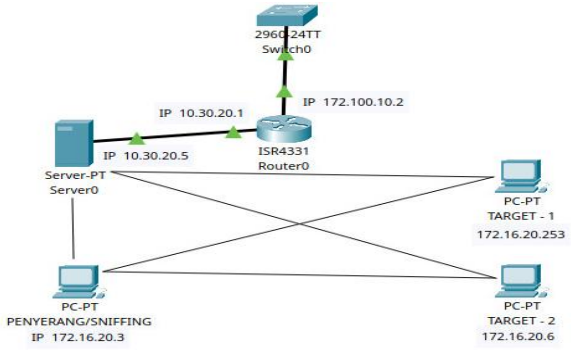
ANALISIS DAN PERANCANGAN SISTEM

A. Analisis Sistem

[3]Analisis sistem adalah penguraian dari suatu sistem yang utuh kedalam bagian- bagian komponennya dengan tujuan untuk mengidentifikasi permasalahan yang ada pada sistem. Analisis sistem dibangun berdasarkan aplikasi yang meliputi perangkat keras (*Hardware),* perangkat lunak (*software*) dan pengguna sistem.

B. Alur Sistem

Untuk mengkoneksikan perangkat sistem, diperlukan rancangan topologi agar dapat mengatahui alur kerja sistem. Topologi yang digunakan untuk mengoptimalkan jaringan *wireless.*



Gambar 1. Topologi Jaringan Yang Dirancang

Topologi jaringan yang dirancang ini menggunakan perangkat yang saling berhubungan, yaitu: jaringan internet, router, switch, server, dan 3 buah laptop yang diantaranya pc penyerang dan pc target 1 target 2

C. Kebutuhan Sistem

Dalam perancangan sistem ini, tersusun atas 2 (dua) kompunen yaitu kompunen perangkat keras (hardware) dan kompunen perangkat lunak *(software)* yang digunakan. Perangkat keras, perangkat lunak yang dibutuhkan dalam analisis tersebut antara lain.

Tabel 1. Kebutuhan Sistem

No	Nama	Fungsi
1.	Laptp/pc	Sebagai perangkat keras untuk membuat pengujian
2.	Windows 10ultimate	Sebagai Operator Sistem yang akan dipakai
3.	Wireshark dan ettercap	Aplikasi yang akan digunakan untuk mengananalisis jaringan

IMPLEMENTASI DAN PEMBAHASAN

Implementasi

Dalam pembahasan ini akan dijelaskan mengenai analisis keamanan jaringan menggunakan aplikasi Ettercap dan *wireshark* berbasis komputer, apakah telah sesuai dengan tujuan yang direncanakan sebelumnya atau tidak.

A. Pemilihan *Interface* Jarinngan.

Gambar 2. Pemilihan *Interface* Jaringan

Mengklik menu sniff kemudian klik unified sniffing dan pilih interface yang akan digunakan. Dalam kasus ini penulis menggunakan i*nterface* wlan0 seperti yang terlihat pada gambar berikut.

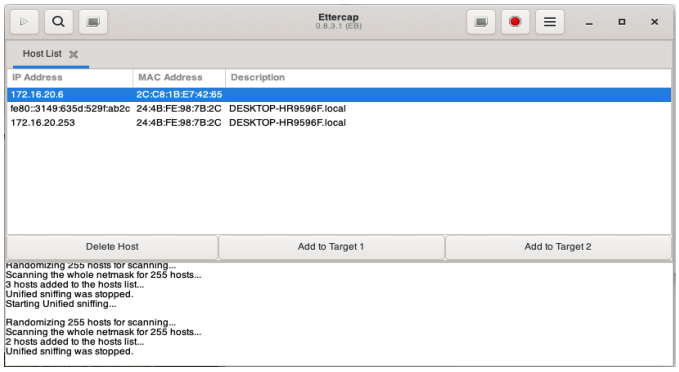
B. Tampilan Setelah Proses *Scanning*

Gambar 3. Pemilihan *Interface Jaringan*

ISSN: 2548-8082/ E-ISSN 2615-6350
Volume 6 No. 2 Edisi 2022

Meng-scan host yang ada di dalam jaringan dengan cara mengklik menu Host kemudian pilih scan for hosts lalu tunggu sampai proses scanning selesai. Setelah proses scanning selesai maka akan terlihat jumlah host yang terhubung pada jaringan yang sama dengan penyerang.

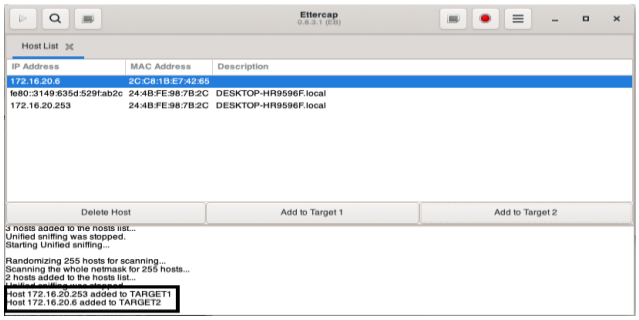
C. Tampilan Daftar Hosts



Gambar 4. Tampilan Daftar Hosts

Untuk melakukan ARP poison, pertama yang dilakukan adalah menentukan gateway dan target denngan cara melihat IP address-nya. Selanjutnya menambahkan IP address 172.16.20.253 sebagai target 1 dengan cara mengklik alamat IP tersebut kemudian pilih " Add to target 1". Karena IP address tersebut merupakan IP *address geteway*.

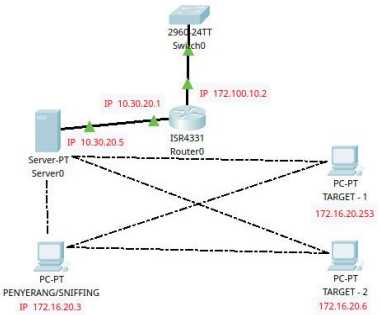
D. Menambahkan IP Korban Sebagai Target 2



Gambar 5. Menambahkan IP Korban Sebagai Target 2

Selanjutnya menambahkan IP address 172.16.20.6 sebagai target 2 denga cara mengklik alamat IP kemudian pilih "Add to Target 2". Karena IP tersebut merupakan IP address korban.

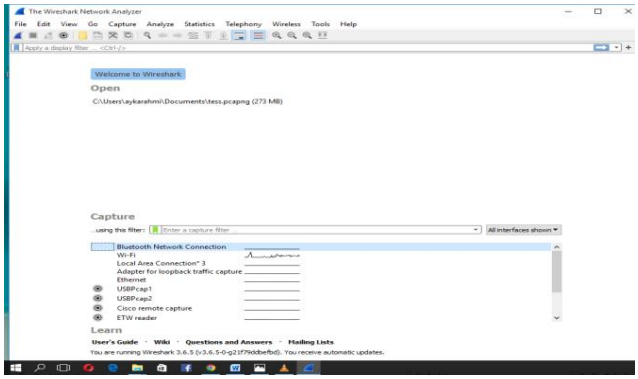
E. Tampilan Simulasi Penyeranng



Gambar 6. Tampilan Simulasi Peyerang

Adalah gambaran skenario dimana attacker melakukan penyerangan secara acak terhadap target 1 dan target 2 yang sedang aktif.

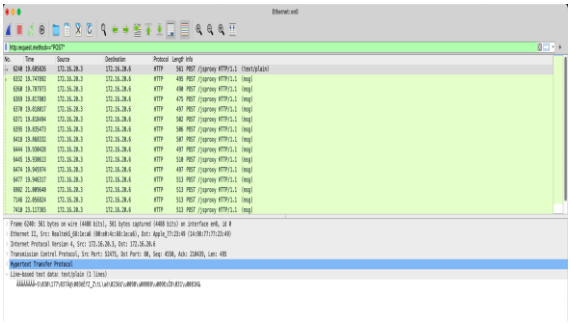
F. Tampilan Utama Wireshark



Gambar 7. Tampilan Utama *Wireshark*

Kemudian masuk kedalam interface yang memiliki paket data jaringan yanng ditandai dengan adanya diagram gelombang.

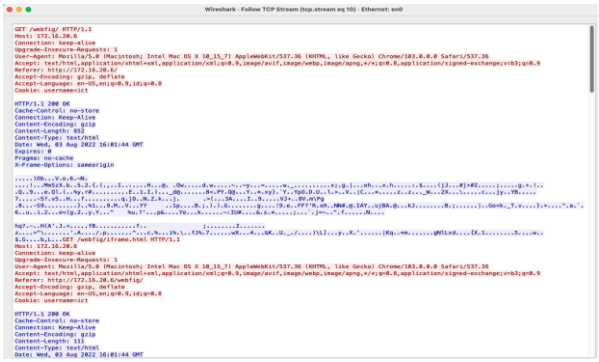
G. Tampilan Paket Data dengan Protokol HTTP.



Gambar 8. Tampilan Paket Data Dengan Protokol HTTP

Tampilan ini merupakan tampilan yang memiliki protokol HTTP, maka sisa paket data yang dimana pada menu info terdapat beberapa keterangan seperti GET, HTTP, dan POST. Untuk menganalsis data tersebut dapat dilakukan dengan cara mengklik kanan paket data pada listing paket panel yang ingin dianalisis kemudian pilih follow HTTP stream.

H. Detail Paket Data POST



Gambar 9. Detail Paket Data POST

 ISSN: 2548-8082/ E-ISSN 2615-6350
Volume 6 No. 2 Edisi 2022

Dapat dijelaskan bahwa dari detail paket data protokol HTTP terdapat dua warna teks yang dimana dua warna ini mempunyai data-data tersendiri seperti username dan password yang digunakan.

Hasil

Hasil ini menunjukan penelitian jaringan wifi yang ada di kampus UMMUbelum aman sesui dengan pengujian, lebih jelasnya dapat dilihat pada tabel berikut ini:

Analisis Serangan	Penganalisaan	Situs	Hasil Keteraga
Packet	Hotspot Jaringan	ICT	Tidak aman
Sniffing	Wifi Gedung A		

KESIMPULAN

Berdasarkan penelitian yang dilakukan di kampus UMMU khususnya dikampus A ruangan ICT tentang analisis keamanan jaringan *wi-fi* terhadap serangan *packet sniffing* yang dimana kemanan *wifi* masih sangat rentan dan masih butuh keamanan jaringan yang lebih maksimal lagi.

SARAN

1. Sebaiknya dilakukan penggantian password wifi secara berkala untuk menghundari terjadinya penyusupan oleh pihak yang tidak bertanggung jawab.

2. Setiap pengguna diikat IP Addres dan MAC addresss sehingga gateway T idak akan salah mengirimkan paket kepada user.

DAFTAR PUSTAKA

[1].Tanembaum, A.S 1996. Jaringan Komputer Jilid 1-Edisi Bahasa Indonesia Dari Computer Networks 3rd ed.Prenhalindo, Ja

[2]. Fauji dan Suartana, 2017. (Hendriana, 2012)

[3]. Kesuma Rifaldi Kagi, Muchammad Ficky, Hamidillah Ajiei. 2018. Desain Dan Implementasi Pada Wifi Pustikom *Free Accses* Di Pusat Teknologi Informasi Dan Komunikasi UNIVERSITAS NEGERI Jakarta.

[4].Turkhamun Adi Kurniawan Analisis. 2020 Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksprimen. Semarang.

[5].Yacob Hae Sulistyo. 2018. Analisis Keamanan Jaringan Wifi Terhadap Serangan *Packet Sniffing* Jakarta

Biodata Penulis

Aykarahmi Umasugi memperoleh gelar sarjana teknik (S.T) Program studi teknik informatika UMMU, lulus pada tahun 20222, saat ini belum bekerja