Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 14, No. 3, Mei 2024, pp. 150 – 233
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

ANALISIS KEAMANAN JARINGAN TERHADAP *SNIFFING* MENGGUNAKAN WIRESHARK

Muhammad Agus Darmawan[1*], Rahayu Ningsih[2], Ahmad Jurnaidi Wahidin[3]

[1,2,3]Teknologi Informasi Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika
*agusdarmawan100821@gmail.com

Abstrak

PT. Mitra Integrasi Informatika merupakan perusahaan garda terdepan bisnis solusi teknologi informasi komunikasi kelompok usaha METRODATA. Indonesia sedang dihadapkan pada banyaknya kasus kebocoran data akibat serangan siber. Kemanan jaringan penting dilakukan oleh administrator jaringan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*. Penulis melakukan penelitian yang berjudul "Analisa Keamanan Jaringan Terhadap *Sniffing*" bertujuan untuk Mengetahui cara mengatasi jika terjadinya ancaman pada jaringan dan Mengetahui pemanfaatan penggunaan software wireshark. Penelitian ini dilakukan dengan cara menguji dan menganalisis hasil pengujian pada keamanan jaringan menggunakan aplikasi *Wireshark* dan *Ettercap* (*OS Kali Linux*) yang mana *wireshark* berguna untuk mengamankan sebuah jaringan lokal dari kegiatan *sniffing* dan *ettercap* sebagai alat *sniffing*. Hasil yang dicapai pada kegiatan ini adalah agar dapat mendeteksi terjadinya *sniffing* pada sebuah jaringan lokal.
Kata Kunci: *Wireshark, Jaringan, Sniffing*

Abstract

PT. Mitra Integrasi Informatika is a company at the forefront of the information technology communication business group METRODATA business group. Indonesia is currently facing many cases of data leakage due to cyber attacks. Network security is important for network administrators to monitor network access and prevent unauthorized misuse of network resources. networks connected to the internet are inherently insecure and can always be exploited by hackers. The author conducted a study entitled "Network Security Analysis of Sniffing" with the aim of knowing how to deal with threats to the network and knowing the use of wireshark software. This research was conducted by testing and analyzing the results of testing on network security using the Wireshark and Ettercap applications (Kali Linux OS) where wireshark is useful for securing a local network from sniffing and ettercap activities as a sniffing tool. The results achieved in this activity are to be able to detect sniffing on a local network.
Keywords: *Wireshark, Jaringan, Sniffing*

p-ISSN 2089-0265
e-ISSN 2598-3016

1. PENDAHULUAN

Indonesia sedang dihadapkan pada banyaknya kasus kebocoran data akibat serangan siber. Para ahli IT menyebut, salah satu penyebabnya adalah kekurangan anggaran yang dialami Badan Siber dan Sandi Negara . Berdasarkan data APBN 2022, alokasi anggaran yang diterima BSSN pada tahun 2022 mencapai Rp 554,6 miliar. Anggaran ini turun 60% dibandingkan outlook 2021 sebesar Rp 1,39 triliun(BSSN, 2022)

Penelitian yang dilakukan oleh (Luthfansa & Rosiani, 2021) *sniffing* dapat dilakukan dengan *Wireshark*. Dari *Wireshark* ini komunikasi data pada jaringan internet bisa dimonitoring dan bisa disadap sehingga bisa mendapatkan infromasi penting. Kemanan jaringan penting dilakukan oleh *administrator* jaringan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*(Rizal Fauzi & Made Suartana, 2018). Jaringan yang baik haruslah memiliki keamanan yang baik agar terhindar dari ancaman kejahatan(Ismail & Pramudita, 2020) Maka dari itu alat yang sangat tepat dalam mengawasi jaringan adalah *Tools Wireshark* dimana alat ini sangat berguna untuk *administrator* dalam memonitoring jaringan, tools *Wireshark* mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan dan aplikasi *wireshark* mampu menangkap dan menganalisa lalu-lintas jaringan lokal (Novita et al., 2021)

2. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini ialah menggunakan studi kasus, studi kasus menggunakan cara- cara yang sistematis dalam melakukan suatu pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya.

2.1. Teknik Pengumpulan Data

a. Metode yang digunakan dalam penelitian ini adalah menggunakan studi kasus, cara-cara yang sistematis dalam melakukan pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya.
b. Pengamatan terhadap interaksi paket data dilakukan menggunakan software *wireshark,* pelaksanaan pengamatan dilakukan dengan cara menginstalasi aplikasi *wireshark* pada laptop atau komputer lalu meng-*capture* (menangkap) paket paket data yang berinteraksi dalam jaringan internet menggunakan *wireshark*

2.2. Analisis Kebutuhan Perangkat

Dalam melakukan penelitian ini dibutuhkan berapa perangkat keras dalam mengimplementasikannya perangkat keras yang digunakan ialah laptop yang bersepesifikasi sebagai berikut ini:

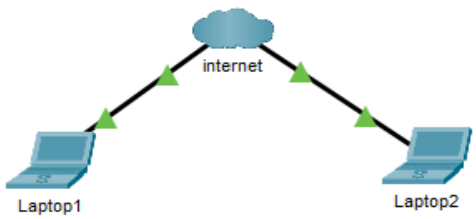
- *Prosesor* : intel core i3-5005u
- Memori : 10240MB
- Ruang : 512 GB
- *OS* : Windows 10 64 bit
- *Hardware* :Laptop

Selain perangkat keras diatas, agar pengujian sistem pendeteksi serangan berjalan, maka dibutuhkan perangkat keras antara lain :

- *Prosesor* : intel core i5
- Memori : 8 GB
- Ruang : 512 GB
- *OS* : Windows 10 64 bit
- *Hardware* :Laptop
-

3. HASIL DAN PEMBAHASAN

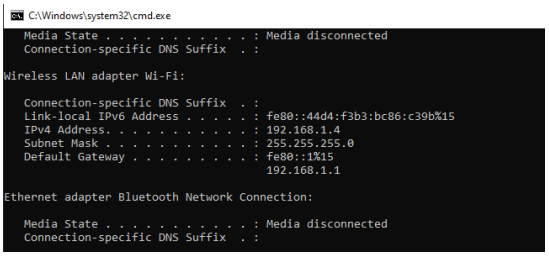
Berikut adalah hasil penelitian pada jaringan *wifi* di PT. Mitra Integrasi Informatika. Dalam penelitian ini penulis melakukan pengujian yaitu menggunakan 2 devices yang saling terhubung dengan *wifi* seperti tertera pada gambar 1.



Gambar 1 bentuk jaringan

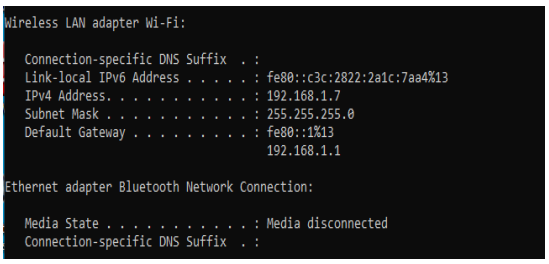
p-ISSN 2089-0265
e-ISSN 2598-3016

Pada gambar 1 melakukan pengecekan *ip address* pada laptop A menggunakan *cmd* dengan mengetikan perintah "*ipconfig*" pada *cmd*



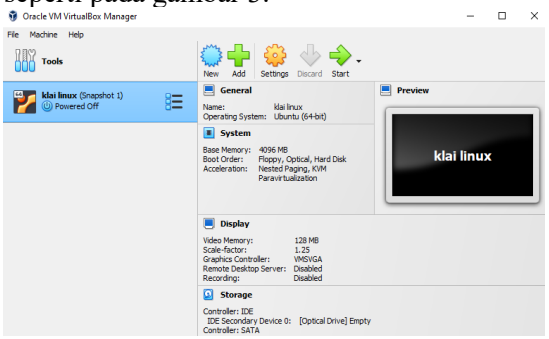
Gambar 2 Pengecekan ip address pada laptop A

Pada gambar 2 pengecekan *ip address* laptop A memiliki *ip address* 192.168.1.4 dan *default gateway* 192.168.1.1 ip address dari *wifi*. Pengecekan ip address pada Laptop B menggunakan *cmd* dengan mengetikan perintah "*ipconfig*" pada *cmd* yang ditunjukan pada gambar 3



Gambar 2 Pengecekan ip address pada laptop B.

Pada gambar 2 pengecekan *ip address* laptop A memiliki ip address 192.168.1.4 dan *default gateway* 192.168.17 *ip address* dari *wifi*. Membuka *software Virtualbox* dan sudah melakukan penginstallan *operation system kali linux* dalam *sofware virtualbox* seperti pada gambar 3.



Gambar 3 Virtualbox

Terlihat pada gambar 3 halaman awal setelah membuka *software virtualbox*. *Kali linux* (*snapshoot* 1) adalah *operation system* (OS) *kali linux* yang sudah diinstal pada *virtualbox* dan masih dalam keadaan *off* atau tidak menyala. *Virtual Box* adalah paket perangkat lunak yang dimana secara fisik tidak dapat disentuh dan di lihat, namun secara fungsi masih bisa berjalan selayaknya komputer(Andriyanto, 2023). *Kali linux* adalah distribusi yang berfokus pada pengujian keamanan, termasuk dalam kategori desktop. dan tidak ada niat untuk membatasi jumlah paket yang dipasang untuk membuat *Kali Linux* lebih sulit diserang(Messier, 2018).Pada pegujian ini penulis menggunakan *software Ettercap* sebagai alat untuk *sniffing*. *Ettercap* adalah alat *sniffing* untuk "*man in the middle attack*" *Ettercap* dapat mengendus ke koneksi langsung dan juga dapat melakukan pemfilteran konten dengan cepat. Ettercap mendukung diseksi aktif maupun pasif dari banyak protokol. terlepas dari semua itu juga mencakup banyak fitur untuk analisis jaringan dan mengendus jaringan.(Rai, 2018)

Gambar 4 Ettercap

Pada gambar 4 bahwa *software Ettercap* telah berjalan dan untuk memulai *sniffing* pada *ettercap* disini penulis men- *setting* terlebih dahulu sebelum memulai sniffing.

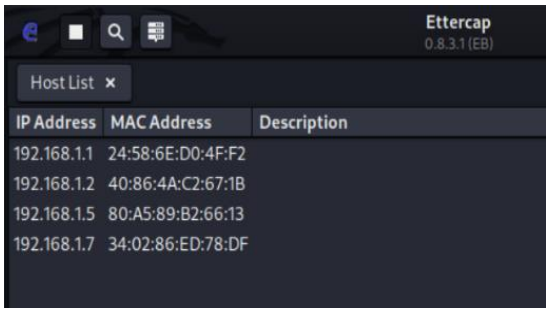
- *Sniffing at startup* di nyalahkan.
- *Primary intreface* pilih *eth0* karena hanya *eth0* saja yang sudah tersambung dengan *wifi*.
- Untuk *Bride sniffing* dinonaktifkan.

Setelah setting selesai klik tombol ceklis untuk memulai.

yang ditunjukan pada gambar 5. Pada gambar dibawah ini pada saat melakukan pengujian terhadap serangan *packet sniffing*, gambar tersebut menunjukkan ketika IP dari laptop

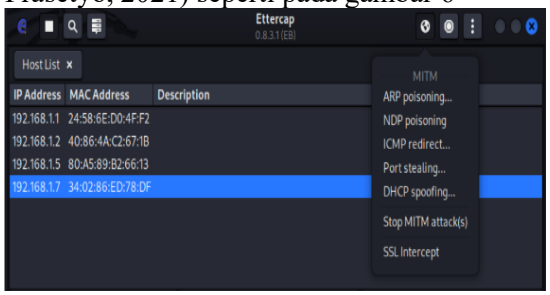
p-ISSN 2089-0265
e-ISSN 2598-3016

korban penyerangan bisa terdeteksi, maka *IP address* dari jaringan kita letakan pada target 1, dan *IP address* korban Penyerangan pada target 2 pada *tools Ettercap*



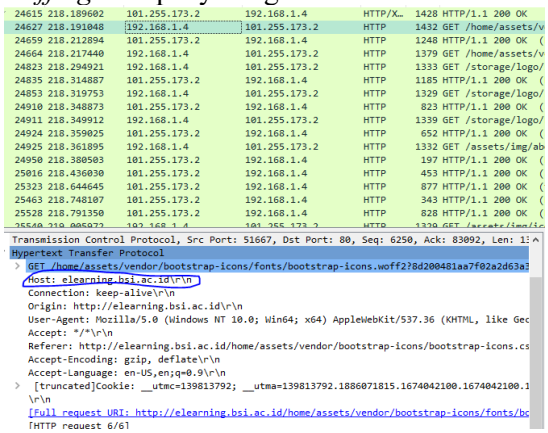
Gambar 5 Ettercap menampilkan host list

Menekan tombol list maka akan muncul beberapa *host* yang telah ter-*scan* dan tersambung dalam jaringan *wifi*.
Ip address 192.168.1.1 = alamat *ip router* atau *wifi*
Ip address 192.168.1.2 = *Host*
Ip address 192.168.1.5 = *Host*
Ip address 192.168.1.7 = *Host*
Pada kasus ini *host* yang memiliki *ip address* 192.168.1.7 adalah *ip* dari laptop B yang akan menjadi penargetan *sniffing*.
Pemilihan *ip address* target yang akan di *sniffing* dan menggunakan *MITM ARP Posioning*. *Man In The Middle* (MITM) merupakan serangan cyber yang terjadi ketika ada pihak ketiga mencegat komunikasi dua orang secara diam-diam(Mujiastuti & Prasetyo, 2021) seperti pada gambar 6



Gambar 6 ARP Posioning

Pada kasus ini penulis menggunakan *ARP Posioning* sebagai *sniffing*-nya. "*ARP Posioning* adalah transmisi ke semua kemungkinan penerima di jaringan lokal, Jika pemilik alamat IP hadir, mereka merespons dengan balasan langsung ke sistem sumber dengan alamat *MAC*-nya" (Stewart, 2021).*ARP Posioning* dapat meracuni *cache ARP* lokal atau mengirimkan balasan *ARP* yang diracuni atau pengumuman. Dalam kedua kasus tersebut, jika *host* memperoleh alamat *MAC* palsu untuk alamat *IP*, transmisinya cenderung pergi ke lokasi yang salah. *ARP Posioning* umumnya digunakan dalam serangan mengendus aktif untuk mengarahkan lalu lintas ke sistem yang dikendalikan peretas.
Pada gambar 6 dibawah ini selanjutnya buka *wireshark*, pada gambar ini menunjukkan hasil dari melakukan *capture*, ketika memulai menekan " *Start capturing packets*" pada *wireshark* akan melakukan *sniffing* sesuai. dengan konfigurasi yang sudah dilakukan, dan proses pengambilan dari paket data yang melintasi suatu jaringan ini yaitu akan berlangsung secara *real time*. Semakin lama melakukan *sniffing*, semakin besar juga file yang akan dihasilkan. Laptop 1 sebagai *sniffing* atau penyerang.



Gambar 7 proses capturing

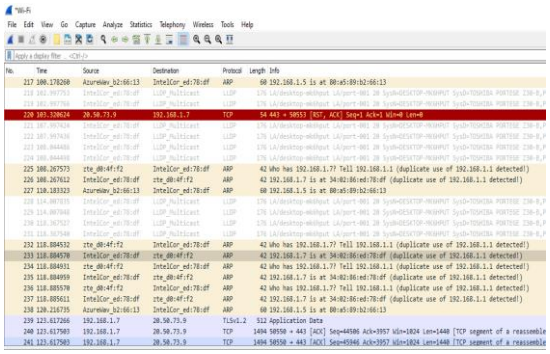
Pada gambar 7 adalah proses *capture* lalu lintas jaringan dari *software wireshark*. *Wireshark* adalah penganalisis protokol yang dapat menangkap lalu lintas dan kemudian mempresentasikannya pada format yang dapat dibaca. fungsionalitas secara keseluruhan dari *Wireshark* bagaimana memecahkan masalah monitor lalu lintas jaringan untuk keamanan masalah dan men-*debug* aplikasi(Bock, 2022).
Pada gambar 7 beberapa menu yang telah tercapture yaitu.

- *Time*
- *Source*, alamat *ip* dari sebuah *user* yang sedang tersambung dengan *wifi*.

p-ISSN 2089-0265
e-ISSN 2598-3016

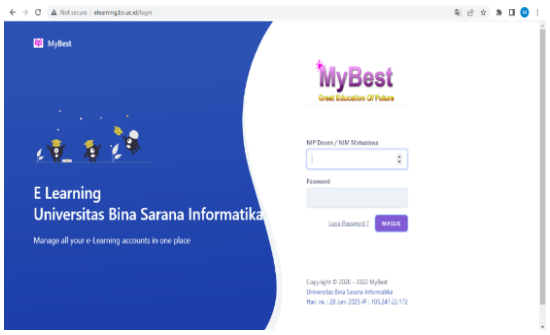
- *Destination*, tujuan alamat *ip user* yang sedang berkomunikasi dengan tujuannya .
- *protocol*, beberapa *protocol* yang tercapture seperti *tcp*, *icmp*, *http*, dan lain lain.
- Info, kegiatan yang sedang dilakukan.

Melakukan pengecekan *capturing* pada *wireshark* seperti pada gambar 8



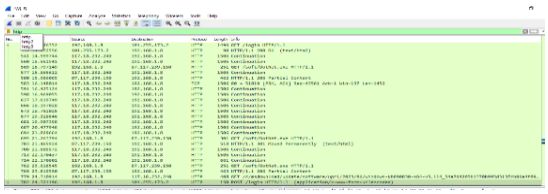
Gambar 8 duplicate ip

Dalam gambar 8 terlihat bahwa *software wireshrak* sedang melakukan capture jaringan dan terlihat seperti digambar 8 adanya proses lalu lintas jaringan yang mencurigakan seperti men- *duplicate ip address* "*duplicate use of* 192.168.1.1 *detected*".
percobaan melakukan *login* salah satu *website* yaitu *elearning* bsi seperti pada gambar 9.



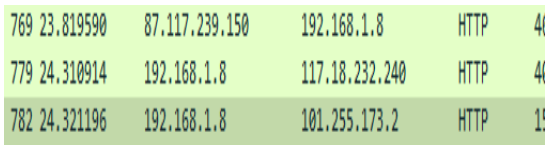
Gambar 9 Login website

Pada tahap ini penulis melakukan pembukaan *website* dan memasuki halaman *login* pada *website mybest*. Dalam hal ini penulis juga melakukan *capturing* pada *sofware* wireshrak. Melakukan *filtering* protokol *HTTP* pada *wireshark* seperti pada gambar 10.



Gambar 10 Pemfilteran http pada wireshark

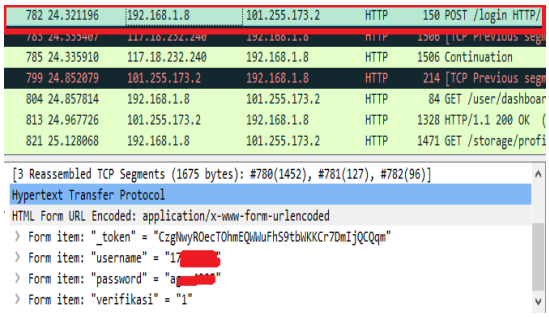
Terlihat pada gambar 10 *website mybset* memiliki *protocol HTTP* dan tercapture pada *wireshark* dan memiliki *ip* 101.255.173.2.



769 23.819590	87.117.239.150	192.168.1.8	HTTP	4
779 24.310914	192.168.1.8	117.18.232.240	HTTP	4
782 24.321196	192.168.1.8	101.255.173.2	HTTP	1

Gambar 11 Protokol http tercapture wireshark

Pada gambar 11 *ip* yang tertera yaitu 192.168.1.8 adalah ip pada *user* yang meminta *requset* pada *ip* 101.255.173.2. *ip address* 101.255.173.2 adalah *ip* dari *website mybest*.



Gambar 12 informasi pada list yang caputre

Jika mengklik salah satu *list* yang berada pada kotak merah seperti yang tunjukan pada gambar 11 maka akan muncul informasi yang terletak di bawah *list* lalu mengklik Hypertext Tranfer *Protocol* akan terlihat *password* dan *username*. *Password* dan *username* tersebut adalah hasil *login* dari *website mybest*.

4. KESIMPULAN

Dari hasil penelitian yang di lakukan dapat di simpulkan :

Dari hasil penilitian yang dilakukan penulis tidak terjadi hal mencurigakan dan bahwa

p-ISSN 2089-0265
e-ISSN 2598-3016

dalam lalu lintas jaringan yang dipakai dalam keadaan aman dan aplikasi *wireshark* dapat melakukan proses *capturing* atau merekam terjadinya lalu lintas jaringan yang mencurigakan seperti halnya pada pengujian ini terpadat *duplicate ip* pada *wireshark*.

DAFTAR PUSTAKA

Andriyanto. (2023). *Membangun Sserver Berbasis Debian Menggunakan Aplikasi Virtualbox*. Penerbit Lakeisha. https://www.google.co.id/books/edition/MEMBANGUN_SERVER_BERBASIS_DEBIAN_MENGGUN/NwO9EAAAQBAJ?hl=id&gbpv=0

Bock, L. (2022). *Troubleshooting Networks Using Wireshark*. Packt Publishing. https://www.google.co.id/books/edition/Learn_Wireshark/4HF5EAAAQBAJ?hl=id&gbpv=0

BSSN. (2022). *Marak Kebocoran Data, Anggaran Keamanan Siber 2023 Hanya Rp 120 M*. Katadata. https://katadata.co.id/agustiyanti/finansial/631ee56d5701b/marak-kebocoran-data-anggaran-keamanan-siber-2023-hanya-rp-120-m

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53–62.

Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal of Information Engineering and Educational Technology*, *5*(1), 34–39. https://doi.org/10.26740/jieet.v5n1.p34-39

Messier, R. (2018). *Learning Kali Linux Security Testing, Penetration Testing, and Ethical Hacking*. Penerbit O'Reilly. https://www.google.co.id/books/edition/Learning_Kali_Linux/FD1lDwAAQBAJ?hl=id&gbpv=0

Mujiastuti, R., & Prasetyo, I. (2021). Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE. *Prosiding Semnastek*, *November 2021*. https://jurnal.umj.ac.id/index.php/semnastek/article/view/11484

Novita, R. T., Gunawan, I., Marleni, I., Grasia, O. G., & Valentika, M. N. (2021). Analisis Keamanan Wifi Menggunakan Wireshark. *JES (Jurnal Elektro Smart)*, *1*(1), 1–3.

Rizal Fauzi, A., & Made Suartana, I. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. *Jurnal Manajemen Informatika*, *8*(2), 7.

Stewart, J. M. (2021). *CompTIA Security+ Review Guide*. Wiley. https://www.google.co.id/books/edition/CompTIA_Security+_Review_Guide/lgYTEAAAQBAJ?hl=id&gbpv=0