# ANALISIS KEAMANAN JARINGAN TERHADAP *SNIFFING* MENGGUNAKAN WIRESHARK

## Muhammad Agus Darmawan<sup>1\*</sup>, Rahayu Ningsih<sup>2</sup>, Ahmad Jurnaidi Wahidin<sup>3</sup>

<sup>1,2,3</sup>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

### 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 vang dilakukan oleh (Luthfansa & Rosiani, 2021) sniffing dapat dilakukan dengan Wireshark. Dari Wireshark ini komunikasi data pada jaringan internet bisa dimonitoring dan bisa disadap sehingga mendapatkan infromasi bisa 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 terhindar dari baik agar 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 paketpaket data atau informasi yang berjalan dalam jaringan dan aplikasi wireshark mampu menangkap dan menganalisa lalulintas 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

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

C:\Windows\system32\cmd.exe
Media State : Media disconnected Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix .: LInk-local IPv6 Address : fe80::44d4:f3b3:bc86:c39b%15 IPv4 Address : 192.168.1.4 Subnet Mask : 255.255.0 Default Gateway : fe88::1%15 192.168.1.1
Ethernet adapter Bluetooth Network Connection:
Media State Media disconnected Connection-specific DNS Suffix . :

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 berialan selavaknva komputer(Andrivanto, 2023). Kali linux adalah distribusi vang 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 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

e =	Q	<b>Ettercap</b> 0.8.3.1 (EB)	
Host List	×		
IP Address	MAC Address	Description	
192.168.1.1	24:58:6E:D0:4F:F2		
192.168.1.2	40:86:4A:C2:67:1B		
192.168.1.5	80:A5:89:B2:66:13		
192.168.1.7	34:02:86:ED:78:DF		

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

	<b>Ettercap</b> 0.8.3.1 (EB)	8 0 : 0 8
HostList ×		
IP Address MAC Address	Description	ARP poisoning
192.168.1.1 24:58:6E:D0:4F:F2		NDP poisoning
192.168.1.2 40:86:4A:C2:67:1B		ICMP redirect
192.168.1.5 80:A5:89:B2:66:13		Port stealing
192.168.1.7 34:02:86:ED:78:DF		DHCP spoofing
		Stop MITM attack(s)
		SSL Intercept

Gambar 6 ARP Posioning

Pada kasus ini penulis menggunakan ARP sebagai sniffing-nya. *"ARP* Posioning 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.

24615 218.189602	101.255.173.2	192.168.1.4	HTTP/X	1428 HTTP/1.1 200 OK			
24627 218.191048	192.168.1.4	101.255.173.2	HTTP	1432 GET /home/assets/v			
24659 218.212894	101.255.173.2	192.168.1.4	HTTP	1248 HTTP/1.1 200 OK (			
24664 218.217440	192.168.1.4	101.255.173.2	HTTP	1379 GET /home/assets/v			
24823 218.294921	192.168.1.4	101.255.173.2	HTTP	1333 GET /storage/logo/			
24835 218.314887	101.255.173.2	192.168.1.4	HTTP	1185 HTTP/1.1 200 OK (			
24853 218.319753	192.168.1.4	101.255.173.2	HTTP	1329 GET /storage/logo/			
24910 218.348873	101.255.173.2	192.168.1.4	HTTP	823 HTTP/1.1 200 OK (			
24911 218.349912	192.168.1.4	101.255.173.2	HTTP	1339 GET /storage/logo/			
24924 218.359025	101.255.173.2	192.168.1.4	HTTP	652 HTTP/1.1 200 OK (			
24925 218.361895	192.168.1.4	101.255.173.2	HTTP	1332 GET /assets/img/ab			
24950 218.380503	101.255.173.2	192.168.1.4	HTTP	197 HTTP/1.1 200 OK (			
25016 218.436030	101.255.173.2	192.168.1.4	HTTP	453 HTTP/1.1 200 OK (			
25323 218.644645	101.255.173.2	192.168.1.4	HTTP	877 HTTP/1.1 200 OK (			
25463 218.748107	101.255.173.2	192.168.1.4	HTTP	343 HTTP/1.1 200 OK (			
25528 218.791350	101.255.173.2	192.168.1.4	HTTP	828 HTTP/1.1 200 OK (			
255/0 210 005072	192 168 1 4	101 255 173 2	NTTO	1339 GET /accets/ima/ic			
Transmission Contro	1 Protocol, Src Port:	51667, Dst Port: 80,	Seq: 6250	, Ack: 83092, Len: 1:∧			
Hypertext Transfer	Protocol						
> GET /home/assets.	/vendor/bootstrap-icor	ns/fonts/bootstrap-ic	ons.woff23	8d200481aa7f02a2d63a3			
Host: elearning.	osi.ac.id\r\n						
Connection: keep	-alive\r\n						
Origin: http://e	learning.bsi.ac.id\r\r	1					
User-Agent: Mozi	lla/5.0 (Windows NT 10	0.0; Win64; x64) Apple	WebKit/53	7.36 (KHTML, like Gec			
Accept: */*\r\n							
Referer: http://elearning.bsi.ac.id/home/assets/vendor/bootstrap-icons/bootstrap-icons.cs							
Accept-Encoding: gzip, deflate\r\n							
Accept-Language: en-US,en;q=0.9\r\n							
> [truncated]Cookie:utmc=139813792;utma=139813792.1886071815.1674042100.1674042100.1							
\r\n	\r\n						
[Full request UR	I: http://elearning.bs	<pre>si.ac.id/home/assets/</pre>	/endor/boo	tstrap-icons/fonts/bc			
[HTTP request 6/	61						

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*.

- *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

A (stop) = 4 dapler filter _ <ch -=""></ch>									
No, Time	Source	Destination	Protocal	Length Info					
217 100.178268	Azurekiav b2:66:13	IntelCor_ed:78:df	ARP	60 192.168.1.5 is at 80:a5:89:b2:66:13					
		LLDP_Multicent	LLDP	176 LA/desktop-skilgut LA/port-001 20 Sys0-dESKTOP-NORMUT Sys0-TOSHIBA PORTESE IN-8,					
			LUP	176 (A/desktop-skillput (A/port-M01 20 Syst-deskTOP-MORPHIT Syste-TopHIDA PORTED 230-0,					
229 103.320624	28.58.73.9	192.168.1.7	TOP	54 443 + 58553 [RST, ACK] Seq+1 Ack+1 Win+0 Len+0					
	latel(or_ed:70:df	LLEP Aulticest	1100	176 (A/desktop-skilput LA/port-001 28 SyductSi(10P-WORK) Sydu-TOSKIDA FORTERE IND-8,					
223 100.044455	IntelCor_ed:70:df		LLDP	176 LA/desktop-skikput LA/port-601 20 Sysh-DESKTOP-REGMUT Sysb-TOSKIBA PIRTESE 238-8,					
224 288.044438			LIDP	176 LA/desktop-ekilout LA/port-001 20 Syst-DESKTOP-MERROT Syst-TOSHIBA PORTEDE 230-8,					
225 188.267573	zte_d0:4f:f2	IntelCor_ed:78:df	ARP	42 Who has 192.168.1.7? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)					
226 188.267612	IntelCor_ed:78:df	zte_d0:4f:f2	ARP	42 192.168.1.7 is at 34:02:86:ed:78:df (duplicate use of 192.168.1.1 detected!)					
227 110.183323	Azureilav_b2:66:13	IntelCor_ed:78:df	ARP	60 192.165.1.5 is at 80:a5:89:b2:66:13					
228 114,007835				176 LA/desktop-mkshout LA/port-001 20 Sysh-DESKTOP-MEMPUT SysD-TOSKDAA PORTEEE 230-9.					
229-114-097048	Intellor ed:75:df		LIEP	176 LAIdesktop-okiligut LA/port-001 20 SystedESETCP-9KildWT SysteTCSHIBA PORTESE 238-8.					
			1100	178 LA/desktop-ekilgut LA/port-001 20 Sys0-DESk10P-WORRUT SysD-TOSHIDA PORTEE ISB-0.					
211 218, 307548			Lize	176 LA/desktop-miniput (A/port-M01 28 Syst-DESkTOP-MOMPUT Syste-TotalDLA PORTER 238-8.					
232 118.884532	zte d0:4f:f2	IntelCor ed:78:df	ARP	42 Who has 192.168.1.7? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)					
233 118.884578	IntelCor ed:78:df	zte d0:4f:f2	ARP	42 192.168.1.7 is at 34:02:86:ed:78:df (duplicate use of 192.168.1.1 detected!)					
234 118.884931	zte d0:4f:f2	IntelCor ed:78:df	ARP	42 Who has 192.168.1.77 Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)					
235 118.884959	IntelCor_ed:78:df	zte_d0:4f:f2	ARP	42 192.168.1.7 is at 34:82:86:ed:78:df (duplicate use of 192.168.1.1 detected)					
236 118.885578	zte_d0:4f:f2	IntelCor_ed:78:df	ARP	42 Who has 192.168.1.7? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)					
237 118.885611	IntelCor_ed:78:df	rte_d8:4f:f2	ARP	42 192.168.1.7 is at 34:82:86:ed:78:df (duplicate use of 192.168.1.1 detected!)					
238 120.216735	Azurekiav_b2:66:13	IntelCor_ed:78:df	ARP	60 192.168.1.5 is at 80:a5:89:b2:66:13					
239 123.617266	192.168.1.7	28.50.73.9	TLSv1.2	512 Application Data					
240 123.617503	192.168.1.7	28.50.73.9	TCP	1494 58558 + 443 [ADX] Sep-44585 Ack-3957 Win-1824 Len-1448 [TCP segment of a reassemb]					
241 123.617503	192,168,1.7	18 58 73 0	TCP	tata 50558 + 443 [arv] Gened5046 Arb+3057 bine1834 (anni445 [T/P segment of a reassant)					

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.

	782 24.321196	192.168.1.8	101.255.173.2	HTTP	150 POST /logi	.n HTTP/		
	/03 24.00040/	117.10.202.240	192.100.1.0	пне	דורא און ממכד	ous segn		
	785 24.335910	117.18.232.240	192.168.1.8	HTTP	1506 Continuati	on		
	799 24.852079	101.255.173.2	192.168.1.8	HTTP	214 [TCP Previ	lous segn		
	804 24.857814	192.168.1.8	101.255.173.2	HTTP	84 GET /user/	dashboar		
	813 24.967726	101.255.173.2	192.168.1.8	HTTP	1328 HTTP/1.1 2	00 OK (		
	821 25.128068	192.168.1.8	101.255.173.2	HTTP	1471 GET /stora	ge/profi		
	[3 Reassembled TCP	Segments (1675 byte	es): #780(1452), #781(	127), #782	(96)]	٨		
Hypertext Transfer Protocol								
HTML Form URL Encoded: application/x-www-form-urlencoded								
> Form item: " token" = "CzgNwyROecTOhmEQWWuFhS9tbWKKCr7DmIjQCQqm"								
> Form item: "username" = "17								
	> Form item: "pass	sword" = "a						
	> Form item: "veri	ifikasi" = "1"				v		

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 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/NwO9EAAA QBAJ?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/finansi al/631ee56d5701b/marak-kebocorandata-anggaran-keamanan-siber-2023hanya-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/FD11DwAAQBA J?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/semna stek/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 )*, *I*(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/lg YTEAAAQBAJ?hl=id&gbpv=0