Analisis Celah Keamanan Jaringan terhadap Serangan *Packet Sniffing* dengan Metode *Vulnerability Scanning*

Alya Atiqah[1], Aswandi[2*], Fachri Yanuar Rudi F[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[1]alya.atqh01@gmail.com
[2*]aswandi@pnl.ac.id (penulis korespondensi)
[3]fachri@pnl.ac.id

Abstrak* – Dalam era digitalisasi yang semakin maju, keamanan jaringan komputer menjadi aspek yang sangat krusial untuk melindungi data penting dari ancaman pihak ketiga, terutama serangan *packet sniffing*. Penelitian ini bertujuan untuk menganalisis celah keamanan jaringan PT. X terhadap serangan *packet sniffing* dengan menggunakan metode *Vulnerability Scanning*. Metode ini dipilih karena mampu dalam mengidentifikasi kelemahan potensial dalam jaringan. Alat yang digunakan dalam penelitian ini seperti Nmap, Wireshark, dan Ettercap untuk mengidentifikasi dan menganalisis kerentanan jaringan. Hasil penelitian menunjukkan bahwa (*Network Mapper*) Nmap berhasil mengidentifikasi beberapa port terbuka yang berpotensi menjadi risiko keamanan, dan pengujian *packet sniffing* dengan Ettercap dan Wireshark menunjukkan tingkat keberhasilan 100% dalam mendeteksi ancaman tersebut dari total 100 percobaan (50 dengan Wireshark dan 50 dengan Ettercap), rata-rata tingkat keberhasilan sniffing adalah 100%, dan analisis kinerja keamanan menunjukkan adanya beberapa kerentanan yang perlu segera ditangani. Kesimpulan dari penelitian ini (*Network Mapper*) Nmap efektif dalam mengidentifikasi *port* terbuka yang berisiko terhadap keamanan. Pengujian *packet sniffing* menggunakan Ettercap dan Wireshark juga berhasil mendeteksi ancaman dengan tingkat keberhasilan 100%. Hasil analisis menunjukkan adanya beberapa kerentanan yang perlu segera diperbaiki untuk meningkatkan keamanan sistem.
Kata Kunci: Keamanan Jaringan, *Packet Sniffing*, *Vulnerability Scanning*, (*Network Mapper*) Nmap, Wireshark.

Abstract – In the era of increasingly advanced digitalization, computer network security becomes a very crucial aspect to protect important data from third-party threats, especially packet sniffing attacks. This study aims to analyze the network security gaps of PT. X against packet sniffing attacks using the Vulnerability Scanning method. This method was chosen because it is able to identify potential weaknesses in the network. The tools used in this study such as Nmap, Wireshark, and Ettercap to identify and analyze network vulnerabilities. The results showed that (Network Mapper) Nmap successfully identified several open ports that have the potential to be security risks, and packet sniffing tests with Ettercap and Wireshark showed a 100% success rate in detecting these threats from a total of 100 trials (50 with Wireshark and 50 with Ettercap), the average sniffing success rate is 100%, and security performance analysis shows several vulnerabilities that need to be addressed immediately. The conclusion of this study (Network Mapper) Nmap is effective in identifying open ports that pose a security risk. Packet sniffing tests using Ettercap and Wireshark also successfully detected threats with a 100% success rate. The analysis results showed several vulnerabilities that need to be fixed immediately to improve system security.
Keywords: Network Security, Packet Sniffing, Vulnerability Scanning, (Network Mapper) Nmap, Wireshark.

I. PENDAHULUAN

A. Latar Belakang

Perkembangan digitalisasi memposisikan komunikasi jaringan komputer sebagai elemen penting dalam kehidupan masyarakat, dengan jaringan komputer yang memungkinkan berbagi sumber daya dan informasi antar perangkat [1]. Namun, keamanan data menjadi prioritas, terutama terhadap ancaman penyadapan atau *sniffing*. Serangan *Packet Sniffing* merupakan risiko serius karena dapat memantau dan mencuri informasi dari jaringan.

Penelitian ini berfokus pada analisis celah keamanan jaringan PT. X terhadap serangan *Packet Sniffing*, dengan menggunakan metode *Vulnerability Scanning* sebagai pendekatan utama [2]. Tool seperti Nmap digunakan untuk mengidentifikasi kerentanan port dan layanan, sementara Wireshark dan Ettercap digunakan untuk memantau aktivitas jaringan dan menangkap paket data. Identifikasi kerentanan ini memungkinkan perusahaan untuk mengambil tindakan pencegahan dan meningkatkan keamanan jaringan [3].

B. Rumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka rumusan masaah yang diusulkan pada penelitian ini adalah:

1. Bagaimana mengidentifikasi potensi kelemahan jaringan PT. X yang dapat dieksploitasi serangan *Packet Sniffing*?
2. Bagaimana menentukan tingkat keberhasilan dari percobaan serangan *Packet Sniffing?*
3. Bagaimana performa/kinerja keamanan jaringan pada PT. X?

C. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi potensi kelemahan keamanan jaringan PT. X yang dapat dieksploitasi oleh serangan *Packet Sniffing*.
2. Melakukan pengujian *Packet Sniffing* pada jaringan PT. X.
3. Menganalisis dan mengevaluasi percobaan yang dilakukan terhadap serangan *Packet Sniffing* guna memahami cara-cara serangan tersebut dapat dieskploitasi dan meresnpons secara efektif terhadap potensi celah keamanan yang mungkin ada.

Sniffing atau *packet sniffing* adalah aktivitas memantau dan menangkap data yang melintasi jaringan internet, seringkali dilakukan oleh pihak tak bertanggung jawab untuk mencuri informasi sensitif seperti username, password, dan data pribadi lainnya, yang dapat membahayakan keamanan [4]. Teknik ini sangat berbahaya terutama ketika data dikirim melalui protokol HTTP yang tidak aman, sehingga memungkinkan pencurian informasi penting atau rahasia bisnis.

Packet sniffing dapat dilakukan dalam mode *filtered* untuk mengumpulkan data spesifik atau *unfiltered* untuk menangkap semua data yang melewati jaringan. Hasilnya dianalisis dan dikonversi menjadi data yang bisa dibaca. Selain oleh pihak tak bertanggung jawab, teknik ini juga digunakan oleh admin jaringan sebagai alat investigasi untuk mengidentifikasi masalah jaringan, seperti kesalahan routing [4].

Network security adalah sistem yang dirancang untuk mengenali dan mencegah akses tidak sah ke jaringan, melindungi sistem dari ancaman eksternal yang dapat merusak integritas dan kerahasiaan data [5]. Tujuannya adalah mengantisipasi serangan logika maupun fisik pada jaringan, baik publik maupun privat, serta mengatur hak akses terhadap sumber daya jaringan [5].

scanning adalah proses mendeteksi kerentanan jaringan menggunakan alat pemindai untuk mengidentifikasi port terbuka, bug pada aplikasi server, dan potensi risiko lainnya [6]. Manfaat utamanya adalah meningkatkan keamanan sistem dengan menemukan dan memperbaiki kerentanan sebelum dimanfaatkan oleh penyerang. Proses ini juga membantu organisasi dalam pemantauan berkelanjutan, memastikan kepatuhan terhadap regulasi, dan memberikan gambaran menyeluruh tentang postur keamanan [8].

Beberapa tools populer untuk *vulnerability scanning* meliputi Acunetix untuk mendeteksi kerentanan aplikasi web, Burp Suite untuk pengujian penetrasi, dan OWASP ZAP, alat open-source yang banyak digunakan untuk mengidentifikasi celah keamanan pada aplikasi web. Pemilihan tool bergantung pada kebutuhan dan lingkungan operasional organisasi [9].

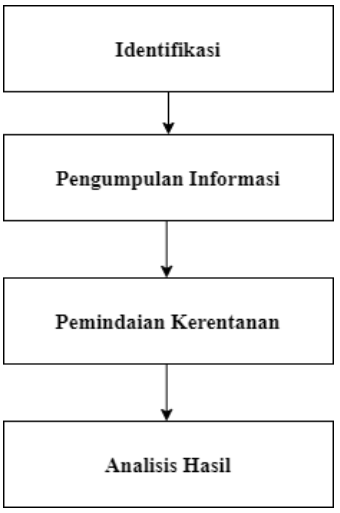
Rasio efektivitas adalah alat untuk menilai sejauh mana tujuan tercapai dengan sumber daya yang ada. Dalam kinerja keamanan jaringan, ini mengukur seberapa baik sistem melindungi aset informasi dari ancaman. Pengujian dilakukan menggunakan dua alat, Ettercap dan WireShark, masing-masing diuji 50 kali. Jumlah ini dipilih karena berada di tengah-tengah penelitian serupa yang menggunakan percobaan antara 5 hingga 76 kali. Rata-rata efektivitas dihitung dengan rumus [10].

$$Rasio\ Efektivitas = \frac{(Output\ yang\ dihasilkan)}{(Input\ yang\ digunakan)} \times 100\% \quad (1)$$

II. METODOLOGI PENELITIAN

A. Metode Penelitian

Metode pengujian dalam peneletian Analisis Celah Keamanan Jaringan Terhadap Serangan *Packet Sniffing* Dengan *Metode Vulnerrability Scanning* melibatkan serangkaian langkah yang akan dilakukan dalam pengujian. Menggunakan metode *Vulnerability Scanning* untuk menganalisis keamanan jaringan PT. X terhadap serangan *Packet Sniffing*. Proses analisis menggunakan Ettercap untuk menangkap informasi dari layanan yang belum dienkripsi dengan efektif, serta Wireshark untuk memonitor lalu lintas yang mencurigakan dan diduga sebagai serangan *Packet Sniffing*. Tahapan Metode Vulnerability Scanning dapat dilihat pada gambar 1.



Gambar 1. Tahapan Metode *Vulanerability Scanning*

Berikut adalah penjelasan setiap tahap pada Gambar 1. Metode *Vulnerability Scanning*:

1) *Identifikasi:* Menentukan target atau jaringan yang akan dipindai, termasuk alamat IP, *domain*, atau perangkat.
2) *Pengumpulan Informasi:* Mengumpulkan data terkait target, seperti layanan yang berjalan, port terbuka, dan versi perangkat lunak, untuk mengetahui konfigurasi dan potensi titk lemah.
3) *Pemindaian Kerentanan:* Menggunakan alat pemindai untuk mengidentifikasi kerentanan dalam sistem atau

jaringan, termasuk pemindaian *port* dan pengecekan versi perangkat lunak.

4) *Analisis Hasil:* Menganalisis hasil pemindaian dan informasi yang terkumpul.

B. *Data dan Pengumpulan Data*

Pada penelitian ini, data yang dikumpulkan berupa data primer dan data sekunder yang akan dipergunakan peneliti. Berikut adalah data yang akan dikumpulkan:

1) *Data Primer*

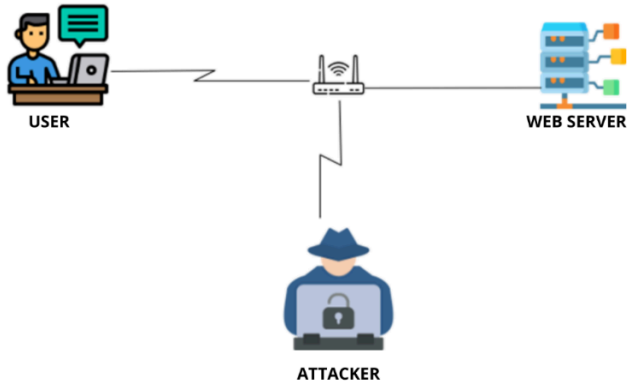
Data *primer* adalah data yang diperoleh dari sumber pertama secara langsung. Dalam penelitian ini, data primer diperoleh melalui analisis langsung oleh peneliti. Data primer yang akan dikumpulkan dalam penelitian ini adalah data mengenai kerentanan jaringan terhadap serangan *packet sniffing*. Data ini akan diperoleh melalui pengujian kerentanan jaringan terhadap serangan *packet sniffing* yang dipilih sebagai sampel penelitian.

2) *Data Sekunder*

Data sekunder adalah data yang diperoleh dari sumber kedua atau sumber yang tidak langsung. Dalam penelitian ini, data *sekunder* yang dikumpulkan meliputi. Data sekunder diperoleh dari sumber-sumber yang telah ada, guna memberikan dukungan pada penelitian ini, peneliti akan melakukan kajian pustaka dengan mengumpulkan materi dari berbagai sumber seperti internet, jurnal, artikel, buku, dan beberapa referensi lainnya.

C. *Rancangan Struktur Jaringan*

Rancangan sistem dibuat untuk memberikan gambaran dari penelitian "Analisis Celah Keamanan Jaringan Terhadap Serangan *Packet Sniffing* Dengan Metode *Vulnerrability Scanning* (Studi Kasus: PT. X Lhokseumawe)" yang akan dianalisis dapat divisualisasikan seperti yang ditunjukkan pada Gambar 2.



Gambar 2.Ilustrasi serangan *Packet Sniffing* Pada perusahaan

Berdasarkan gambar 2. Langkah yang dilakukan adalah sebagai berikut:

1. Penyerang menempatkan dirinya di jalur komunikasi antara pengguna (User) dan server.
2. Penyerang menggunakan perangkat lunak khusus seperti ettercap dan wireshark untuk menangkap paket data yang dikirimkan antara pengguna dan server. Paket-paket ini berisi informasi yang dikirimkan melalui jaringan, termasuk data yang mungkin sensitif seperti *username* dan *password*.
3. Penyerang menganalisis paket data yang telah ditangkap untuk mencari informasi sensitif, seperti mencari kata sandi, informasi login, atau data lainnya yang dapat digunakan untuk tujuan jahat.
4. Jika penyerang menemukan informasi sensitif, mereka dapat mencuri data tersebut dan menggunakannya untuk keuntungan pribadi atau menjualnya kepada pihak ketiga.

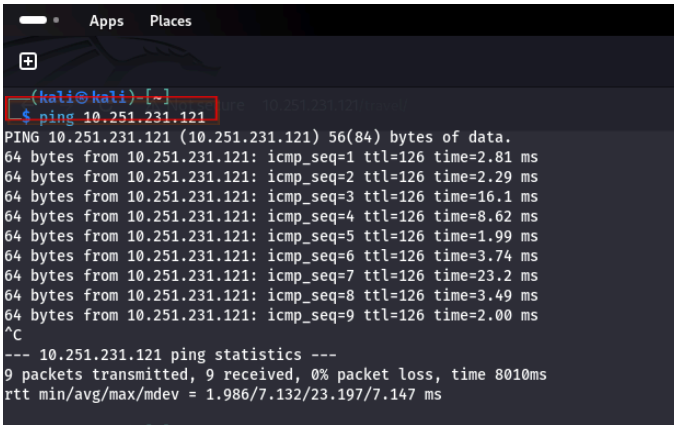
D. *Teknik Pengujian*

Teknik pengujian dalam "Analisis Celah Keamanan Jaringan Terhadap Serangan Packet Sniffing Dengan Metode Vulnerability Scanning" melibatkan langkah-langkah berikut: Pertama, menggunakan Nmap untuk melakukan pemindaian kerentanan pada jaringan perusahaan, mengidentifikasi potensi kelemahan yang dapat dieksploitasi oleh serangan Packet Sniffing. Hasil pemindaian mencakup informasi tentang port, status port, layanan, dan versi layanan, yang digunakan untuk mengevaluasi kerentanan. Selanjutnya, Wireshark digunakan untuk memvalidasi dan mengonfirmasi kerentanan yang diidentifikasi, sementara Ettercap melakukan pengujian packet sniffing secara langsung. Teknik ini memberikan gambaran komprehensif tentang kerentanan terhadap serangan Packet Sniffing di jaringan PT. X dan mendasari tindakan pencegahan dan perbaikan keamanan jaringan.

III. HASIL DAN PEMBAHASAN

A. *Vulnerability Scanning menggunakan Nmap*

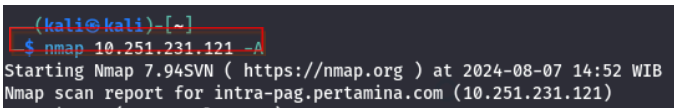
Sebelum melakukan *Vulnerability Scanning*, dilakukan ping ke alamat IP tujuan untuk melakukan pengecekan. *Ip address* yang tertera pada gambar 3.



Gambar 3. Ping ke alamat IP tujuan

Kemudian memasukkan *command* "nmap 10.251.xxx.xxx -A" untuk melakukan pemindaian terhadap alamat IP tersebut.

Tampilan *command* pada kali linux dapat dilihat pada gambar 4.



Gambar 4. *Command* nmap yang digunakan

Setelah melakukan *Vulnerability Scanning* peneliti mendapatkan informasi tentang *host* yang dipindai tertera di Tabel I.

TABEL I
VULNERABILITY SCANNING INFORMASI YANG DI DAPAT

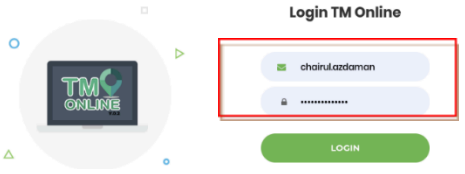
Port	Status	Layanan	Versi/Info	Kerentanan
80/tcp	Terbuka	HTTP	Microsoft IIS httpd 8.0	- Metode berisiko: TRACE - Situs tidak memiliki judul (text/html; charset=UTF-8
113/tcp	Tertutup	Ident		
135/tcp	Terbuka	MSRPC	Microsoft Windows RPC	
139/tcp	Terbuka	NetBIOS-SSN	Microsoft Windows netbios-ssn	
445/tcp	Terbuka	Microsoft-DS	Windows Server 2012 Datacenter 9200 microsoft-ds	
2000/tcp	Terbuka	Cisco-SCCP	Tidak pasti (Mungkin Cisco-SCCP)	
2179/tcp	Terbuka	VMRDP	Tidak pasti (Mungkin VMRDP)	
3260/tcp	Terbuka	iSCSI	Tidak pasti (Mungkin iSCSI)	
3389/tcp	Terbuka	SSL/MS-WBT-Server?	Sertifikat SSL: Nama Umum: intra-pag.pertamina.com	- Berlaku dari: 2024-05-21 hingga 2024-11-20
5060/tcp	Terbuka	SIP	Tidak pasti (Mungkin SIP)	
7070/tcp	Terbuka	SSL/RealServer	Sertifikat SSL: Nama Umum: AnyDesk Client	- Berlaku dari: 2021-03-16 hingga 2071-03-04 - Randomness TLS tidak mewakili waktu
49153/tcp	Terbuka	MSRPC	Microsoft Windows RPC	
49155/tcp	Terbuka	MSRPC	Microsoft Windows RPC	

Berdasarkan hasil analisa Nmap terhadap IP 10.251.xxx.xxx (intra-pag.pertamina.com), ditemukan bahwa host ini aktif dengan latensi 0.0036 detik. Beberapa *port* yang terbuka termasuk *port* 80/tcp yang menjalankan layanan HTTP dengan Microsoft IIS 8.0. Terdapat potensi risiko karena metode TRACE diizinkan. *Port* 135/tcp, 139/tcp, dan 445/tcp terbuka untuk layanan msrpc, netbios-ssn, dan microsoft-ds, menunjukkan bahwa server ini menjalankan berbagai layanan Windows kritis. Port lain yang terbuka termasuk 2000/tcp (cisco-sccp), 2179/tcp (vmrdp), 3260/tcp (iscsi), 3389/tcp (ssl/ms-wbt-server), 5060/tcp (sip), dan 7070/tcp (ssl/realserver) dengan sertifikat SSL yang teridentifikasi sebagai *AnyDesk Client* yang valid hingga 2071. *Server* ini menjalankan Windows Server 2012 Datacenter 9200 dengan nama komputer intra-pag dan berada dalam domain pertamina.com. Analisis SMB menunjukkan bahwa message signing diaktifkan namun tidak diwajibkan, dan ada beberapa konfigurasi keamanan yang perlu ditingkatkan seperti message signing yang dinonaktifkan pada SMB, yang dapat menimbulkan risiko keamanan. Sertifikat SSL pada beberapa port perlu diperhatikan, terutama pada port 7070 yang memiliki validitas yang sangat lama hingga 2071.

B. Pengujian Packet Sniffing

Dalam penelitian ini, pengujian *Packet Sniffing* dilakukan untuk mengevaluasi kerentanan jaringan PT. X terhadap serangan *sniffing*. Pengujian ini melibatkan penggunaan dua perangkat lunak utama: Ettercap dan Wireshark. Berikut adalah tahapan dan hasil dari pengujian ini.

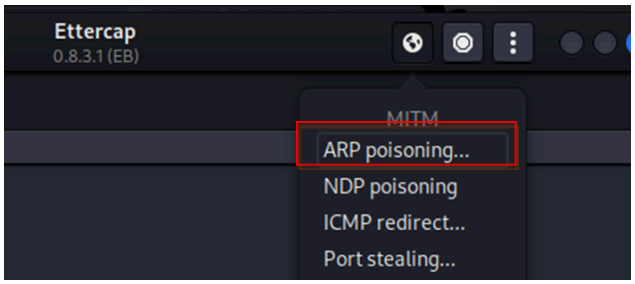
1) *Login ke halamanWebsite: Username* dan *password* dimasukkan pada halaman login *website* TM Online. Tampilan login *website* TM Online dapat dilihat pada gambar 5.



Gambar 5. Masuk ke halaman *website* TM Online

2) *Melakukan pengujian dengan Ettercap:* Proses dimulai dengan membuka Ettercap dan melakukan host scanning untuk mengidentifikasi perangkat target. Setelah

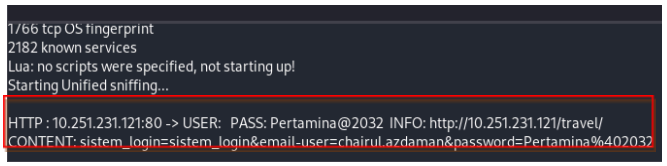
menetapkan alamat IP target, langkah berikutnya adalah mengaktifkan mode ARP *Poisoning*, yang memungkinkan menjalankan *Packet Sniffing* secara efektif. Mengkatifkan Mode ARP *Poisoning* dapat dilihat pada gambar 6.



Gambar 6. Mengaktifkan mode *ARP Poisoning*

Setelah mengaktifkan mode ARP *Poisoning*, Ettercap mulai mengirim pesan ARP *Reply* palsu ke perangkat-perangkat dalam jaringan. Pesan ARP *Reply* ini mengklaim bahwa alamat MAC penyerang adalah alamat MAC yang terkait dengan alamat IP dari target lain, seperti *gateway* jaringan atau perangkat lain yang menjadi target serangan.

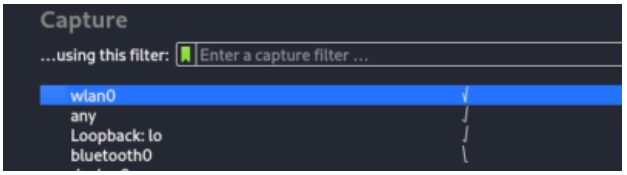
Perangkat-perangkat dalam jaringan yang menerima pesan ARP *Reply* palsu akan memperbarui ARP *cache* mereka dengan informasi yang salah. Ini berarti mereka akan menyimpan bahwa alamat IP dari target sekarang terkait dengan alamat MAC penyerang. Dengan ARP *cache* yang telah diracuni, lalu lintas jaringan yang seharusnya dikirimkan ke target asli sekarang akan dialihkan ke penyerang. Ini memungkinkan penyerang untuk mendapatkan semua paket data yang seharusnya dikirimkan ke target. Hasil dari pengujian *Packet Sniffing* dapat dilihat pada gambar 7.



Gambar 7. Hasil pengujian menggunakan Ettercap

Berdasarkan hasil pengujian, ettercap berhasil menangkap *username* dan *password* yang mengakses dan menganalisis lalu lintas jaringan. Pertama, Ettercap dijalankan dalam mode promiscuous, yang memungkinkan antarmuka jaringan untuk menangkap semua paket data yang melewati jaringan tersebut, bukan hanya paket yang ditujukan untuk antarmuka tersebut. Selain itu, Ettercap menggunakan teknik ARP spoofing atau ARP poisoning, yang mengelabui perangkat di jaringan untuk mengirimkan lalu lintas melalui komputer yang menjalankan Ettercap, sehingga komputer tersebut untuk melihat dan mencatat data yang seharusnya tidak dilewatinya. Karena lalu lintas yang ditangkap adalah HTTP, yang merupakan protokol tidak terenkripsi, semua data yang dikirimkan, termasuk kredensial login seperti username dan password, dapat dibaca dengan mudah. Dalam contoh ini, Ettercap berhasil menangkap *username* "chairul.azdaman" dan *password* "Pertamina%402023" yang digunakan untuk mengakses URL "http://10.251.xxx.xxx/travel/". Keberhasilan ini menunjukkan kelemahan signifikan dalam protokol HTTP dan pentingnya menggunakan protokol terenkripsi seperti HTTPS untuk melindungi data sensitif dari serangan *sniffing*.

3) *Melakukan pengujian dengan Wireshark:* Proses dimulai dengan membuka halaman depan Wireshark dan memilih jaringan eth0 untuk pemantauan lalu lintas data. Setelah itu, dilakukan persiapan pada kedua perangkat lunak untuk memastikan pengumpulkan data dengan akurat dan efisien. Wireshark dijalankan pada perangkat penyerang, dan interface jaringan yang sesuai dipilih untuk monitoring. Pada menu Wireshark mulai menangkap semua paket data yang dikirimkan antara user dan server. Paket-paket ini bisa berisi informasi sensitif seperti *username* dan *password*. Melalui proses ini, interaksi antara pengguna dan sistem serta keefektifan protokol keamanan dapat dievaluasi secara sistematis. Halaman menu Wireshark dapat dilhat pada gambar 8.



Gambar 8. Persiapan monitoring menggunakan Wireshark

Setelah itu, Wireshark memonitoring jaringan wlan0 yang menjadi sumber internet dari kali linux virtual box. Hasil monitoring menggunakan Wireshark dapat dilihat pada gambar 9.

Gambar 9. Hasil monitoring menggunakan Wireshark

Berdasarkan gambar 4.9 dapat dilihat bahwa Wireshark berhasil mendapatkan *username* dan *password*. Wireshark dapat menangkap data sensitif yang tidak terenkripsi karena berfungsi sebagai alat pemantauan pasif yang menangkap lalu lintas jaringan. Tangkapan Wireshark menunjukkan proses permintaan dan *respons* HTTP selama upaya *login* ke sistem. Klien mengirimkan permintaan POST ke endpoint /travel/auth_sistem di *server* dengan IP 10.251.xxx.xxx, menggunakan *username* chairul.azdamand dan *password* Pertamina%402023. Klien menggunakan *browser* Chrome versi 127.0.0.0. *Server* merespon dengan kode status HTTP/1.1 200 OK, menunjukkan bahwa *login* berhasil. Respons *server* mengatur agar tidak disimpan dalam *cache* dan memiliki jenis konten HTML dengan encoding UTF-8. *Server* menggunakan Microsoft IIS 8.0, PHP 7.0.25, dan ASP.NET.

Selanjutnya, terdapat permintaan GET ke endpoint /travel/sistem di server yang sama dengan header yang mirip. Tangkapan ini memberikan wawasan tentang proses *login* dan bagaimana server menangani permintaan, termasuk langkah-langkah keamanan seperti tidak adanya *caching*. Sementara itu, tetapi tidak banyak mempengaruhi Wireshark yang berfungsi dalam mode *promiscuous* untuk menangkap semua lalu lintas yang melewati antarmuka jaringan yang dipilih.

C. Menghitung Kinerja Jaringan

Pengukuran kinerja keamanan dilakukan dengan menguji *tool* Ettercap dan Wireshark masing-masing sebanyak 50 kali. Pengujian ini bertujuan untuk mengumpulkan data yang cukup guna menilai seberapa efektif dan efisien *tool* tersebut dalam mengidentifikasi dan menganalisis kerentanan dalam jaringan. Setelah data dari setiap pengujian dikumpulkan, hasilnya dianalisis dan dirangkum untuk memberikan gambaran yang jelas tentang kinerja keamanan jaringan. Hasil pengujian dapat dilihat pada Tabel II.

TABEL II
KEBERHASILAN *TOOLS* DALAM MENGIDENTIFIKASI ANCAMAN *PACKET SNIFFING*

No	*Tool*	Jumlah Percobaan	Keberhasilan Mengidentifikasi *Packet Sniffing*	Persentase Keberhasilan	Status
1	Ettercap	50	50	100%	Sukses
2	Wireshark	50	50	100%	Sukses

Jumlah percobaan menunjukkan bahwa kedua *tool* diuji sebanyak 50 kali dalam kondisi yang sama untuk mengidentifikasi ancaman *packet sniffing*. Baik Ettercap maupun Wireshark berhasil mengidentifikasi ancaman *packet sniffing* pada semua percobaan, dengan keberhasilan 50 dari 50 kali. Persentase keberhasilan untuk keduanya adalah 100%. Status akhir dari kedua alat adalah "Sukses", Pertama, baik Ettercap maupun Wireshark menunjukkan kinerja optimal dalam mendeteksi ancaman *packet sniffing* dalam kondisi pengujian yang dilakukan. Kedua, persentase keberhasilan 100% untuk kedua alat mengindikasikan tingkat reliabilitas yang tinggi, hasil ini menunjukkan bahwa kedua alat ini efektif dalam melakukan tugasnya, yaitu menangkap dan menganalisis paket data untuk mengidentifikasi adanya aktivitas *packet sniffing.*

1) *Persentase Keberhasilan Packet Sniffing*

Dalam pengujian ini, hasil dari kedua *tool* packet sniffing, Ettercap dan Wireshark, menunjukkan tingkat keberhasilan yang sama dalam mendeteksi ancaman jaringan. Ettercap berhasil dalam 50 dari 50 percobaan, memberikan persentase keberhasilan sebesar 100%. Perhitungan ini didasarkan pada rumus berikut. Rasio Efektivitas dihitung menggunakan persamaan (1).

$$Persentase\ Keberhasilan\ Ettercap = \frac{(50)}{(50)} \times 100\%$$

= 1 x 100 %
= 100%

Hasil ini menunjukkan bahwa Ettercap tidak mengalami kegagalan dalam semua percobaan yang dilakukan, dengan tingkat efektivitas penuh dalam kondisi pengujian.

Demikian pula, Wireshark juga menunjukkan tingkat keberhasilan yang sama, dengan 50 percobaan berhasil dari total 50 percobaan yang dilakukan. Rasio Efektivitas dihitung menggunakan persamaan (1).

$$Persentase\ Keberhasilan\ Wireshark = \frac{(50)}{(50)} \times 100\%$$

= 1 x 100%
= 100%

Dalam pengujian ini, dapat disimpulkan bahwa kedua *tool* tersebut memiliki tingkat keberhasilan 100% dalam skenario pengujian yang dilakukan, menunjukkan efektivitas tinggi dalam mendeteksi ancaman jaringan pada percobaan tersebut.

2) Performa Keamanan Jaringan

Total Percobaan yang dilakukan adalah 100, yang terdiri dari 50 Percobaan menggunakan Wireshark dan 50 Percobaan menggunakan Ettercap. Untuk menilai efektivitas kedua alat tersebut, dapat menghitung rata-rata keberhasilan *sniffing*.

Total Percobaan = 50 (wireshark) + (ettercap)
= 100

Rata – Rata *sniffing* dihitung sebagai berikut:

$$Rata - rata\ keberhasilan\ sniffing = \frac{100}{100} = 100\%$$

Percobaan sniffing dilakukan dengan total 100 percobaan, di mana masing-masing 50 percobaan menggunakan Wireshark dan Ettercap. Tujuan dari percobaan ini adalah untuk membandingkan efektivitas kedua alat tersebut dalam melakukan *sniffing*. Hasil menunjukkan bahwa rata-rata tingkat keberhasilan *sniffing* untuk kedua *tools* secara keseluruhan adalah 100%.

3) Analiis Hasil Pengujian Packet Sniffing

Hasil dari *vulnerability scanning* menggunakan Nmap menunjukkan beberapa *port* yang terbuka pada *server* PT. X termasuk port 80/tcp yang menjalankan layanan HTTP dengan Microsoft IIS 8.0. Beberapa *port* lain seperti 135/tcp, 139/tcp, dan 445/tcp juga terbuka, menunjukkan bahwa s*erver* ini menjalankan berbagai layanan Windows kritis. Analisis ini mengindikasikan adanya potensi risiko, terutama pada *port* yang mengizinkan metode TRACE dan konfigurasi keamanan yang perlu ditingkatkan. Pengujian *packet sniffing* dilakukan untuk mengevaluasi kerentanan jaringan terhadap serangan sniffing menggunakan dua alat Ettercap dan Wireshark. Keduanya diuji sebanyak 50 kali dalam kondisi yang sama untuk mengidentifikasi ancaman *packet sniffing*. Hasilnya menunjukkan bahwa baik Ettercap dan Wireshark memiliki tingkat keberhasilan 100% dalam mengidentifikasi ancaman tersebut, dengan masing-masing *tool* berhasil dalam 50 dari 50 percobaan. Dari total 100 percobaan (50 menggunakan Wireshark dan 50 menggunakan Ettercap), rata-rata tingkat keberhasilan *sniffing* adalah 100%. Pengujian ini menunjukkan bahwa kedua tools tersebut efektif dalam mendeteksi ancaman *packet sniffing* dengan tingkat reliabilitas yang tinggi. Hasil pengujian menunjukkan bahwa Nmap berhasil mengidentifikasi beberapa *port* terbuka yang berpotensi menjadi risiko keamanan pada jaringan PT. X. Selain itu, Ettercap dan Wireshark efektif dalam mendeteksi ancaman packet *sniffing* dengan tingkat keberhasilan 100%. Secara keseluruhan, metode yang digunakan dalam pengujian ini mampu memberikan gambaran yang jelas tentang kinerja keamanan jaringan dan efektivitas *tool* yang digunakan. Analisis ini dapat digunakan sebagai dasar untuk meningkatkan keamanan jaringan dengan menutup *port* yang tidak diperlukan dan mengkonfigurasi ulang pengaturan keamanan pada *port* yang berisiko tinggi.

IV. KESIMPULAN

Dari hasil penelitian tentang celah keamanan jaringan terhadap serangan packet sniffing dengan metode vulnerability scanning, dapat disimpulkan bahwa pemindaian menggunakan Nmap menemukan beberapa port terbuka di server PT. X, termasuk port 80/tcp untuk layanan HTTP dengan Microsoft IIS 8.0 serta port 135/tcp, 139/tcp, dan 445/tcp, yang menunjukkan potensi risiko keamanan. Pengujian packet sniffing menggunakan Ettercap dan Wireshark, dengan 50 kali percobaan masing-masing, menunjukkan tingkat keberhasilan 100% dalam mendeteksi ancaman. Ini membuktikan bahwa kedua alat sangat efektif dalam mendeteksi packet sniffing dengan keandalan yang tinggi.

V. REFERENSI

[1] "Putu et al. - 2019 - Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus Intranet Jurusan Teknologi Inform-annotated.pdf."

[2] "Yudiastuti, Panjaitan - 2022 - Analisis dan Monitoring WIFI pada Universitas Islam Negeri Palembang-annotated.pdf."

[3] A. Majid dan T. D. Purwanto, "Analisis Dan Monitoring Sniffing Paket Data Jaringan Lokal Bps Sumsel Dengan Network Analyzer Wireshark," 2021.

[4] Z. M. Luthfansa dan U. D. Rosiani, "Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet," *J. Inf. Eng. Educ. Technol.*, vol. 5, no. 1, hlm. 34–39, Jun 2021, doi: 10.26740/jieet.v5n1.p34-39.

[5] Khashaaisha Al Fikri dan Djuniadi, "InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)", doi: 10.30743/infotekjar.

[6] R. Pradana Aji, Y. Prayudi, dan A. Luthfi, "Analysis Of Brute Force Attack Logs Toward Nginx Web Server On Dashboard Improved Log Logging System Using Forensic Investigation Method," *J. Tek. Inform. Jutif*, vol. 4, no. 1, hlm. 39–48, Feb 2023, doi: 10.52436/1.jutif.2023.4.1.644.

[7] M. G. A. Danialdo, F. A. Bakhtiar, dan M. Data, "Pengujian Efektivitas OWASP ZAP dalam Menemukan Kerentanan dari Metasploitable".

[8] K. A. Suputri, M. D. Maharani, G. A. Pratama, N. D. I. Sudiasta Putri, I. M. E. Listartha, dan G. A. J. Saskara, "Perbandingan Tools Vulnerability Scanning Pada Pengujian Sebuah Website," *Inform. J. Ilmu Komput.*, vol. 18, no. 3, hlm. 269, Des 2022, doi: 10.52958/iftk.v18i3.5133.

[9] Ni Putu Ana Rainita, Anak Agung Istri Callysta Athalia, Made Diva Putera Ananta, I Ketut Pratista Tri Pramana, Gede Arna Jude Saskara, dan I Made Edy Listartha, "Analisis Perbandingan Vulnerability Scanning Pada Website Dvwa Menggunakan Owasp Nikto Dan Burpsuite," *J. Inform. Dan Tekonologi Komput. JITEK*, vol. 3, no. 2, hlm. 89–97, Jul 2023, doi: 10.55606/jitek.v3i2.908.

[10] E. P. Silmina, A. Firdonsyah, dan R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," *Transmisi*, vol. 24, no. 3, hlm. 83–91, Agu 2022, doi: 10.14710/transmisi.24.3.83-91.