KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK, DAN METASPLOIT

Adamsyach Prana Walidin, Fahra Pebiana Putri, Dedy Kiswanto
Ilmu Komputer, Universitas Negeri Indonesia
Jalan Willem Iskandar, Pasar V Medan Estate, Percut Sei Tuan, Deli Serdang, Indonesia
adamsyachpranawalidin@gmail.com

ABSTRAK

Keamanan jaringan merupakan sesuatu yang sangat penting dalam kehidupan bersama internet sehari hari, terutama pada sistem operasi dan komputer yang digunakan. Dengan adanya masalah seperti pencurian data, penyadapan akun, dan pendobrakan akses, dibutuhkan sebuah analisis dalam mencari cara tepat mengamankan jaringan dari gangguan gangguan tersebut. Kali linux adalah salah satu sistem operasi yang sangat dalam pada bidang keamanan baik kemananan jaringan ataupun kemananan *cyber*. Pada kali linux, dilengkapi banyak alat seperti Nmap, Wireshark, dan Metasploit. Ketiga alat ini ternyata memiliki fungsi masing masing. Metode yang digunakan pada penelitian ini ibarat vaksin yang mencari penyelesaian menggunakan masalah yang ada, lebih tepatnya eksperimental kualitatif. Dapat diketahui setelah dilakukannya penelitian ini, bahwa jaringan terbuka merupakan sesuatu yang rentan terhadap serangan siber. Sebagai pengguna yang bijak, tersedia banyak solusi demi melindungi diri dari serangan siber seperti update selalu sistem keamanan dan hindari jaringan terbuka yang minim keamanan.

Kata kunci : *Kali linux, Sistem Operasi, jaringan, Keamanan*

1. PENDAHULUAN

Sistem operasi adalah perangkat lunak utama yang memungkinkan komputer berfungsi dengan baik dan menjadi penghubung antara perangkat keras dan perangkat lunak. Tanpa sistem operasi, komputer hanyalah sekumpulan komponen fisik yang tidak memiliki kemampuan untuk menjalankan perintah atau aplikasi. Sistem operasi bertanggung jawab untuk mengelola berbagai sumber daya komputer, seperti prosesor, memori, perangkat penyimpanan, dan perangkat input/output, sehingga semua elemen tersebut dapat bekerja secara terkoordinasi. Selain itu, sistem operasi menyediakan antarmuka yang memungkinkan pengguna berinteraksi dengan perangkat komputer, baik melalui perintah teks, ikon grafis, maupun kombinasi keduanya. Contoh sistem operasi yang banyak digunakan adalah Windows, yang populer di kalangan pengguna umum, Linux, yang dikenal fleksibel dan banyak digunakan oleh pengembang, serta macOS, yang menawarkan integrasi yang kuat dengan perangkat buatan Apple. Setiap sistem operasi dirancang dengan keunggulan dan pendekatan berbeda, namun semuanya memiliki tujuan yang sama, yaitu memastikan komputer dapat digunakan dengan mudah, efisien, dan stabil.

Berkaitan dengan penelitian dari Marzuki Hasibuan, Kali linux merupakan sistem operasi turunan linux Debian yang sangat kuat atau *powerfull* dalam bidang keamanan. Kali linux memiliki banyak *built in* program yang umumnya perlu dipasang terlebih dahulu pada sistem operasi lainnya. Dikembangkan oleh Offensive Security, Kali Linux dilengkapi dengan lebih dari 600 alat keamanan canggih, seperti Nmap, Metasploit, Wireshark, dan Aircrack-ng, menjadikannya pilihan utama bagi para profesional keamanan siber dan penguji penetrasi. Distribusi ini mendukung berbagai arsitektur perangkat keras, termasuk x86, x64, ARM, dan bahkan platform virtualisasi, serta menawarkan fleksibilitas dalam bentuk antarmuka grafis maupun baris perintah. Keamanannya didukung oleh model pengembangan berbasis repositori aman, memastikan integritas alat yang digunakan. Dengan sifatnya yang open-source dan komunitas yang aktif, Kali Linux menjadi pusat pembelajaran sekaligus eksperimen bagi para pemula maupun ahli di bidang keamanan teknologi informasi.[1]

Internet memainkan peran yang sangat penting dalam kehidupan pribadi dan profesional, namun juga membawa risiko dari peretas yang memanfaatkan kelemahan sistem. Oleh karena itu, pengujian penetrasi sangat diperlukan. Pengujian penetrasi adalah metode untuk mengevaluasi keamanan sistem dengan meniru serangan dari luar guna menemukan dan memperbaiki kerentanan yang ada. Kali Linux adalah distribusi Linux yang dirancang khusus untuk pengujian keamanan dan forensik digital. Dilengkapi dengan berbagai alat seperti Nmap, Wireshark, dan Metasploit, Kali Linux menjadi pilihan utama untuk pengujian penetrasi. [2]

Nmap adalah alat yang digunakan untuk memindai jaringan, membantu mengidentifikasi perangkat dan layanan yang aktif serta kemungkinan kerentanannya. Alat ini bekerja dengan mengirimkan paket data dan menganalisis respons yang diterima untuk mengungkap informasi tentang jaringan .[3]

Wireshark adalah alat untuk menganalisis protokol jaringan yang memungkinkan pengguna untuk menangkap dan memeriksa data yang melintasi jaringan secara detail. Alat ini sangat berguna untuk menyelesaikan masalah jaringan, menganalisis keamanan, dan mempelajari protokol jaringan. [4]

Metasploit adalah kerangka kerja yang digunakan untuk menemukan dan mengeksploitasi kerentanan dalam sistem jaringan. Metasploit menyediakan berbagai modul untuk melakukan serangan dan mendokumentasikan kelemahan yang ditemukan, menjadikannya alat yang sangat penting dalam pengujian penetrasi. [5]

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

a. Judul
   Strategi Pencegahan Efektif terhadap Serangan DDoS Slowloris menggunakan Kali Linux dan Linux Mint
b. Penulis
   Keinanjung Ruswandi, Muhammad Reza Zulva Pohan, Kevin Viriya Halim, Shelvie Nidya Neyman
c. Ringkasan
   Penelitian ini membahas strategi pencegahan terhadap serangan Distributed Denial of Service (DDoS) tipe Slowloris dengan menggunakan Kali Linux sebagai mesin serangan dan Linux Mint sebagai target. Serangan Slowloris mengeksploitasi kelemahan protokol HTTP dengan mempertahankan koneksi yang tidak selesai, sehingga menghabiskan sumber daya server dan menyebabkan layanan menjadi tidak responsif. Studi ini menggunakan metode campuran, yakni data sekunder dari literatur dan eksperimen praktis untuk menguji efektivitas langkah pencegahan seperti pengaturan timeout dan pembatasan koneksi di server NGINX. Hasil penelitian menunjukkan bahwa langkah-langkah tersebut secara signifikan mengurangi dampak serangan, menjaga ketersediaan layanan, dan meningkatkan ketahanan sistem. Penelitian ini memberikan wawasan penting dalam melindungi infrastruktur jaringan dari ancaman serangan DDoS.[6]
d. Kesamaan
   Penelitian ini melakukan uji keamanan dengan berbasis kali linux serta melakukan tes penetrasi untuk mengantisipasi serangan keamanan melalui jaringan.
e. Perbedaan
   Penelitian ini menggunakan Linux mint dan tidak terbatas dengan Nmap, Wireshark, Metasploit. Penelitian ini juga melakukan penelitian terhadap objek yang berbeda, yaitu menggunakan protokol HTTP.

2.2. Sistem Operasi

Sistem operasi adalah perangkat lunak yang berfungsi sebagai perantara antara pengguna dan perangkat keras komputer. Tugas utama SO adalah memastikan komunikasi yang efisien antara komponen perangkat keras dan aplikasi yang dijalankan pengguna. Sistem operasi populer seperti Windows, Linux, dan macOS mengimplementasikan konsep-konsep ini dengan pendekatan yang berbeda, menyesuaikan dengan kebutuhan pengguna dan perangkat yang didukung. SO juga bertanggung jawab mengelola proses-proses yang berjalan di komputer, termasuk proses pembuatan, penjadwalan, hingga penghentian program. Selain itu, SO menjamin koordinasi antarproses melalui mekanisme sinkronisasi dan komunikasi yang efisien.

Selain manajemen proses, sistem operasi memiliki peran penting dalam pengelolaan memori utama atau RAM. Ini mencakup alokasi memori untuk proses-proses yang aktif serta dealokasi memori saat proses selesai dijalankan. Dengan memastikan penggunaan memori yang optimal, SO memungkinkan banyak aplikasi berjalan secara bersamaan tanpa mengganggu kinerja sistem. Pengelolaan sumber daya yang dilakukan oleh SO tidak hanya mendukung kinerja sistem secara keseluruhan, tetapi juga memastikan pengalaman pengguna yang lebih lancar dan responsif.. [7]

2.3. Kali Linux Sebagai *Provider* Pengujian Keamanan

Keamanan data pengguna adalah elemen penting yang harus diperhatikan dan dapat digunakan sebagai ukuran kualitas situs web. Beberapa faktor kualitas mempengaruhi kualitas konten website; contohnya, kualitas informasi dapat menggambarkan kualitas konten. Ada tiga faktor mempengaruhi kualitas website: kualitas sistem, kualitas layanan, dan kualitas informasi. [8]

2.4. Virtual Machine

Virtual Machine (VM) adalah perangkat lunak yang mensimulasikan lingkungan komputer sehingga dapat menjalankan program seperti yang dilakukan pada komputer fisik. VM memanfaatkan sumber daya perangkat keras dari komputer host untuk menjalankan sistem operasi dan aplikasi di dalamnya. Salah satu alasan utama penggunaan VM adalah kemampuannya dalam mendukung simulasi skenario tertentu, seperti serangan DDoS yang memerlukan banyak host, tanpa memengaruhi perangkat fisik secara langsung. Sistem operasi, sebagai komponen inti dalam sistem komputer, berperan penting dalam mengelola dan mengontrol jalannya program-program lain. Dengan menggunakan VM, sistem operasi dapat diimplementasikan dengan lebih fleksibel, memudahkan pengembang dalam mengakses dan bekerja dengan perangkat keras melalui antarmuka yang terstruktur.[9]

2.5. Nmap, Wireshark, dan Metasploit

Nmap adalah alat penting dalam keamanan jaringan yang digunakan untuk mendeteksi kerentanan server, mengevaluasi kinerja firewall, dan memverifikasi sistem deteksi intrusi (IDS). Namun, alat ini juga dimanfaatkan oleh penyerang untuk mengumpulkan informasi dari host target, seperti menemukan port terbuka dan layanan. Dengan

memanfaatkan basis data sidik jari IP/TCP, Nmap dapat mendeteksi sistem operasi target selama fase pengintaian. Selain digunakan untuk analisis keamanan, Nmap sering dipakai untuk menguji IDS, seperti Snort dan Suricata. Oleh karena itu, deteksi perilaku pemindaian Nmap dalam jaringan menjadi penting untuk mencegah penyalahgunaan oleh peretas.[10]

Wireshark, jaringan yang banyak digunakan Deteksi Penyusupan Jaringan Menggunakan Wireshark dan Machine alat analisis paket, dengan algoritme pembelajaran mesin yang canggih. Kemampuan Wireshark yang kuat untuk menangkap dan menganalisis data komunikasi jaringan menyediakan data yang kaya untuk mengidentifikasi kerentanan dan potensi gangguan. Dengan menggunakan model klasifikasi pembelajaran mesin seperti Random-Forest, K-NearestNeighbors, Naïve-Bayes, Support vector machine, dan Gradient Boosting, model kami dirancang untuk meningkatkan kinerja dan efisiensi deteksi intrusi, memungkinkan peserta untuk secara proaktif mengidentifikasi dan memitigasi ancaman siber secara real-time.[11]

Metasploit adalah platform keamanan siber yang dirancang untuk pengujian penetrasi, eksploitasi kerentanan, dan pengembangan exploit secara terintegrasi. Dikembangkan oleh Rapid7, Metasploit menawarkan ribuan modul yang mencakup eksploitasi, payload, dan post-exploitation untuk menguji keamanan jaringan, aplikasi, maupun sistem operasi. Dengan antarmuka yang fleksibel, baik melalui command-line maupun GUI seperti Armitage, Metasploit memudahkan penggunanya untuk menemukan celah keamanan, mensimulasikan serangan, serta mengembangkan strategi pertahanan. Alat ini banyak digunakan oleh profesional keamanan siber untuk mengidentifikasi kerentanan, namun juga sering dimanfaatkan oleh peretas untuk tujuan yang kurang etis, sehingga pemahaman mendalam tentang penggunaannya sangat penting dalam dunia keamanan teknologi informasi.[12]

2.6. Tes Penetrasi

Pengujian penetrasi adalah pendekatan keamanan yang banyak dipelajaridalam literatur. Mayoritas pekerjaan yang tersedia bertujuan untuk menemukan kerentanan di tingkat jaringan dan sebagian besarsebagian besar bergantung pada prosedur yang dijalankan secara manual oleh ahli keamanan.Seperti yang dibahas dalam makalah ini, dibandingkan dengan penelitian yang sudah ada, pendekatan kami untuk pengujian penetrasi berfokus pada menemukan yang terbaik eksploitasi yang cocok dan bergantung pada proses otomatis.[13]

3. METODE PENELITIAN

Pada bagian ini memuat metode yang digunakan pada pembuatan skripsi. Penelitian ini menggunakan metode eksperimental kualitatif untuk melakukan tes keamanan yang ditujukan pada ubuntu sebagai target. Tes ini bertujuan untuk memahami apa yang menyebabkan kerentanan pada jaringan.

3.1. Identifikasi Masalah

Masalah utama yang diidentifikasi dalam penelitian ini adalah meningkatnya kerentanannya keamanan jaringan yang sering kali menjadi target serangan siber. Banyak organisasi dan individu menghadapi kesulitan dalam mendeteksi dan mengatasi potensi ancaman yang ada, terutama dengan kompleksitas serangan yang terus berkembang. Seringkali, alat analisis keamanan yang tersedia tidak cukup efektif untuk mengidentifikasi dan mengatasi masalah tersebut. Dalam konteks ini, alat seperti Nmap, Wireshark, dan Metasploit yang ada di Kali Linux dapat menjadi solusi, namun tantangannya adalah bagaimana mengoptimalkan penggunaannya untuk memindai port terbuka, menganalisis lalu lintas jaringan, dan menguji kerentanannya tanpa merusak infrastruktur yang ada. Selain itu, masih diperlukan pemahaman yang lebih mendalam mengenai bagaimana cara terbaik untuk menerjemahkan hasil analisis menjadi langkah-langkah mitigasi yang praktis dalam upaya meningkatkan keamanan jaringan secara menyeluruh. Penelitian ini bertujuan untuk mengatasi permasalahan-permasalahan tersebut dengan mengeksplorasi efektifitas penggunaan Kali Linux dan alat-alat analisis keamanannya dalam mengidentifikasi dan mengurangi risiko serangan jaringan.

3.2. Pemasangan Kali Linux & Ubuntu pada Virtual Machine

Untuk memasang Kali Linux pada VirtualBox, pertama-tama unduh file ISO Kali Linux dari situs resminya. Setelah itu, buka VirtualBox dan buat mesin virtual baru dengan memilih "Linux" sebagai tipe sistem dan "Debian" sebagai versi (karena Kali berbasis Debian). Ram yang kami gunakan sebanyak 3125 MB dan alokasi ruang hard disk yang digunakan sebanyak 52 GB, kemudian pilih "Create" dan pilih file ISO Kali Linux yang telah diunduh sebagai sumber instalasi. Selanjutnya, mulai mesin virtual, yang akan memulai proses instalasi Kali Linux. Ikuti langkah-langkah instalasi seperti memilih bahasa, zona waktu, pengaturan partisi, serta pengaturan pengguna dan password. Setelah instalasi selesai, restart mesin virtual.

Untuk memasang Ubuntu pada VirtualBox, pertama-tama unduh file ISO Ubuntu dari situs resminya. Setelah itu, buka VirtualBox dan buat mesin virtual baru dengan memilih "Linux" sebagai tipe sistem dan "Ubuntu" sebagai versi. Jumlah RAM yang digunakan 3000 MB dan alokasi ruang hard disk untuk sebanyak 24 GB, kemudian pilih "Create" dan pilih file ISO Ubuntu yang telah diunduh sebagai sumber instalasi. Selanjutnya, mulai mesin virtual, yang akan memulai proses instalasi Ubuntu. Ikuti langkah-langkah instalasi seperti memilih bahasa, zona waktu, pengaturan partisi, serta pengaturan pengguna dan

password. Setelah instalasi selesai, restart mesin virtual.

3.3. Skema Pengujian Keamanan Jaringan

Pada penelitian ini, proses yang dilakukan untuk menganalisis dan menguji kerentanannya jaringan melibatkan tiga tahap utama yaitu Nmap scanning, Wireshark sniffing, dan Metasploit exploit.

Nmap Scanning: Proses pertama yang dilakukan adalah pemindaian jaringan menggunakan Nmap untuk mengidentifikasi perangkat yang terhubung dan port yang terbuka. Nmap digunakan untuk memindai jaringan dan mengidentifikasi port terbuka pada perangkat yang diuji, seperti port SSH, HTTP, atau FTP. Pemindaian ini membantu dalam mengetahui potensi celah atau kerentanannya yang dapat dimanfaatkan oleh penyerang. Selain itu, Nmap juga bisa digunakan untuk mengetahui versi perangkat lunak yang berjalan di port terbuka, yang memungkinkan analisis lebih lanjut terkait kelemahan yang ada.

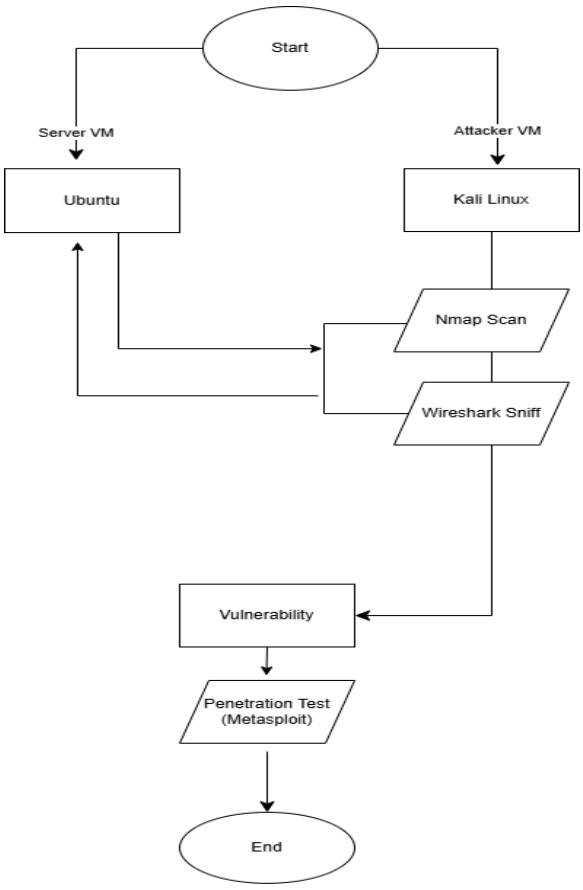
Wireshark Sniffing: Setelah pemindaian menggunakan Nmap, Wireshark digunakan untuk melakukan sniffing atau pemantauan lalu lintas jaringan. Wireshark akan menangkap paket-paket data yang dikirimkan melalui jaringan, termasuk informasi yang dapat berupa data sensitif seperti username, password, atau informasi lainnya. Dengan melakukan sniffing, peneliti dapat menganalisis bagaimana data dikirimkan dan apakah ada potensi kebocoran informasi yang dapat dieksploitasi. Wireshark juga digunakan untuk memantau dan menganalisis jenis protokol yang digunakan, serta mendeteksi adanya aktivitas mencurigakan atau tanda-tanda serangan.

Metasploit Exploit: Setelah mengidentifikasi kerentanannya melalui pemindaian dan sniffing, langkah berikutnya adalah menggunakan Metasploit untuk menguji dan mengeksploitasi kerentanannya yang ditemukan. Metasploit adalah framework yang memungkinkan peneliti untuk melakukan simulasi serangan dengan mengeksploitasi celah keamanan yang ada pada perangkat atau aplikasi yang terhubung ke jaringan. Proses ini bertujuan untuk menguji sejauh mana sistem dapat dipengaruhi oleh eksploitasi dan untuk menunjukkan potensi risiko yang dapat digunakan oleh penyerang untuk mendapatkan akses tidak sah ke dalam sistem. Metasploit memungkinkan peneliti untuk menguji serangan pada sistem secara aman dan terkontrol tanpa merusak infrastruktur yang ada.

Urutan pengujian dilakukan secara bertahap untuk membuktikan kerentanan jaringan yang dimiliki Ubuntu agar dapat dilakukan tes penetrasi. Dengan informasi alamat dari nmap dan bocoran aktivitas pengguna dari wireshark, analisis kerentanan seperti port, alamat ip, -bahkan data data yang terenkripsi digunakan untuk melakukan simulasi serangan terhadap server, yang pada kasus ini merupakan ubuntu. Urutan pengujian dapat dilihat pada gambar 1.

Melalui tahapan ini, penelitian memberikan gambaran menyeluruh tentang bagaimana alat-alat yang ada di Kali Linux dapat digunakan untuk mengidentifikasi, menganalisis, dan mengeksploitasi kerentanannya pada jaringan, yang pada gilirannya dapat membantu meningkatkan langkah-langkah mitigasi untuk menjaga keamanan jaringan.

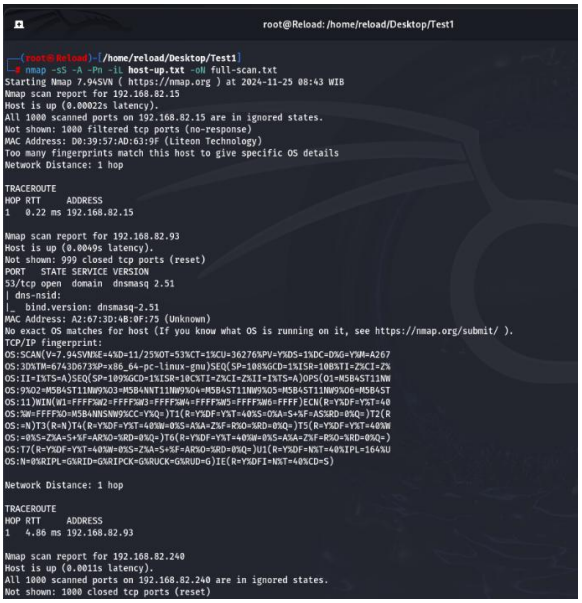
Hasil pengujian ini tidak hanya mengungkap kelemahan dalam sistem jaringan, tetapi juga menekankan pentingnya melakukan pembaruan perangkat lunak secara berkala, memperketat konfigurasi firewall, dan menggunakan protokol enkripsi yang lebih baik. Selain itu, penerapan pemantauan jaringan secara real-time menggunakan alat seperti Wireshark dapat membantu mendeteksi aktivitas mencurigakan sebelum dampak yang lebih besar terjadi. Temuan ini memberikan rekomendasi praktis bagi administrator jaringan untuk meningkatkan keamanan sistem, mengurangi risiko serangan, serta memperkuat kepercayaan terhadap keamanan infrastruktur teknologi informasi yang dikelola.



Gambar 1. Flowchart Skema Uji Coba

3.4. Tahap Scanning menggunakan Nmap

Pada tahap ini, dilakukan scanning pemindaian dengan menggunakan kemampuan pemindai milik nmap seperti gambar berikut.

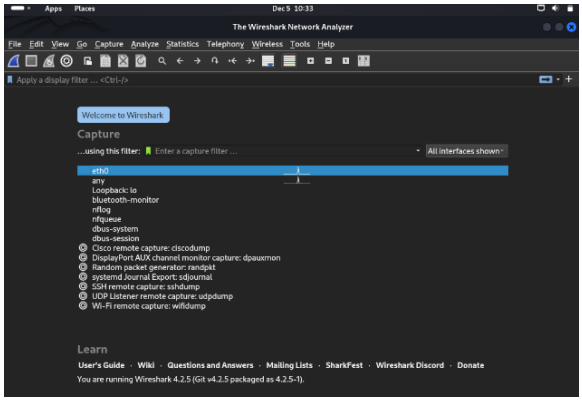


Gambar 2. Hasil Penggunaan Nmap

Seperti yang terlihat pada gambar, dilakukan proses scan secara menyeluruh, menggunakan perintah "sudo nmap -sS -A -Pn" dengan file yang berisi barisan dari kode ip yang tersambung pada jaringan yang sama.

3.5. Tahap Sniffing menggunakan Wireshark

Pada tahap ini, menggunakan terminal Kali, dengan perintah "sudo wireshark" dan proses ini akan langsung membuka interface dari alat wireshark yang berfokus pada penyadapan aktivitas target yang mana menggunakan ubuntu pada penelitian ini.



Gambar 3. Tampilan Awal Wireshark

Setelah tampilan muncul, pilihlah jenis jaringan yang ingin dilakukan proses *sniffing*, pada kasus ini yaitu ethernet. Masukkan filter yang spesifik untuk membatasi data yang diperoleh hanya seputar target yaitu ubuntu. Filter yang digunakan disini adalah "ip:src == <kode ip ubuntu>".

Filter akan bekerja memilah proses yang berhubungan hanya dengan ip yang spesifik, setelah melihat aktivitas ini, bisa dimulai proses pengaliran data yang dibutuhkan dari aktivitas tersebut atau dikenal dengan *Follow the stream.*

3.6. Tahap Exploite menggunakan Metasploit

Setelah informasi yang didapat seputar target telah didapat, proses eksploitasi dapat dimulai dengan perintah "sudo msfconsole" untuk mendapat tampilan dari Metasploit.

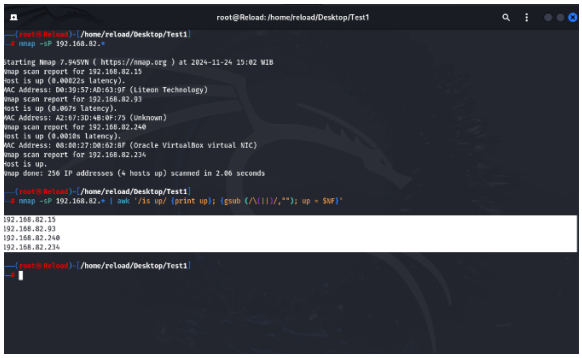
Tahap pertama eksploitasi, yaitu pemilihan modul sesuai dengan informasi yang didapat. Setelah modul eksploitasi dipilih, langkah berikutnya adalah menyesuaikan parameter eksploitasi sesuai dengan konfigurasi target, seperti alamat IP, port, atau parameter spesifik lainnya. Metasploit kemudian menjalankan eksploitasi dengan memanfaatkan celah keamanan yang ada, seperti buffer overflow, kesalahan konfigurasi, atau kerentanannya aplikasi. Jika eksploitasi berhasil, Metasploit akan membuka sesi akses pada target, yang dikenal sebagai *meterpreter session*. Sesi ini memungkinkan pengguna untuk mengontrol target, menjalankan perintah, atau mengakses data sensitif dalam sistem.

Setelah akses ke sistem target diperoleh, tahap pasca-eksploitasi dimulai. Pada tahap ini, pengguna dapat melakukan berbagai tindakan seperti mencuri data, memasang *backdoor*, meningkatkan hak akses, atau menjalankan payload untuk tujuan tertentu. Metasploit juga menyediakan modul pasca-eksploitasi untuk mengumpulkan informasi lebih lanjut, seperti *hash* kata sandi, log aktivitas, atau konfigurasi sistem. Setelah semua data yang dibutuhkan diperoleh, sesi eksploitasi dihentikan, dan hasil analisis digunakan untuk mengevaluasi tingkat keamanan target. Proses ini bertujuan untuk membantu administrator jaringan memahami risiko yang ada dan mengambil langkah mitigasi yang sesuai untuk mencegah eksploitasi di masa mendatang.

4. HASIL DAN PEMBAHASAN

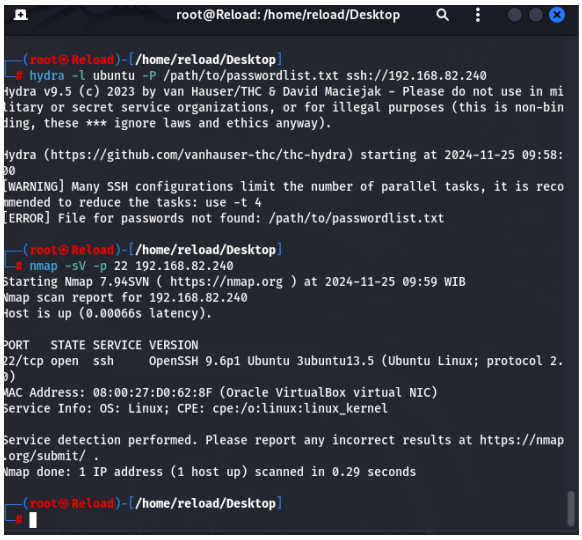
Penelitian diawali dengan menjalankan kedua mesin virtual (*Virtual Maxhine)* untuk mengawali proses simulasi serangan pada ubuntu menggunakan Kali linux. Ubuntu menggunakan konfigurasi dasar tanpa adanya proses pengubahan pada firewall maupun keamananannya yang berarti menggunakan firewall tipe UFW (*Uncomplicated Firewall)* sebagai firewall bawaan.

Pada Kali linux, buka terminal dalam mode *super user* atau mode admin dengan perintah "sudo su" agar memudahkan proses simulasi serangan. Sebelum masuk pada langkah *mapping* menggunakan nmap, perlu dilakukan pengecekkan alamat ip pada kali linux yang terhubung pada jaringan yang sama menggunakan perintah "ip a". Setelah berhasil mengidentifikasi alamat ip milik kali linux, jalankan nmap menggunakan 3 bagian dari alamat ip tanpa memasukkan digit terakhir dengan dituttup tanda '*'. Hal ini akan memberi perintah pada nmap untuk melakukan pemindaian terhadap alamat ip apa saja yang dibawah jaringan yang sama.



Gambar 4. Proses *Mapping* Menggunakan Nmap

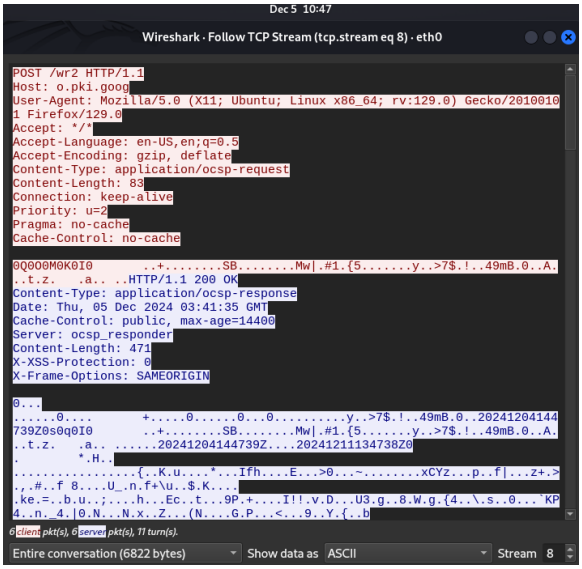
Setelah mendapatkan alamat ip dari target (ubuntu), dapat dilakukan proses lanjutan sesuai tujuan. Selanjutnya dilakukan proses *scan* menggunakan nmap untuk melakukan pengecekan terhadap port.



Gambar 5. Port Scanning dari Nmap

Dengan didapatnya alamat IP serta jenis port tujuan, proses selanjutnya akan dilakukan pada wireshark dimana simulasi serangan dilakukan dalam bentuk sniffing atau dengan makna lain, melihat aktivitas apapun itu dari target (Ubuntu) baik behubungan dengan internet maupun tidak.

Menggunakan perintah "sudo wireshark", wireshark akan mulai beroperasi setelah dilakukan pemilihan terhadap pada jaringan yang mana yang akan dilakukan proses sniffing. Ada indikator gelombang yang menandakan bahwa jaringan tersebut sedang aktif digunakan yang bisa menjadi pertanda bahwa pada jaringan tersebut lah bisa dilakukan proses sniffing. Untuk memberi tujuan spesifik pada wireshark, perlu menggunakan filter agar hanya aktivitas target (Ubuntu) yang hanya terekam menggunakan perintah "ip.src == 192.168.229.240".

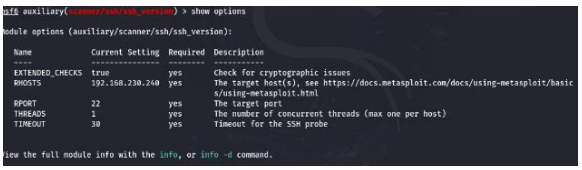


Gambar 6. *Follow the stream* Pada wireshark

Pada gambar 6, dapat diakses ketika user telah memilih paket aktivitas apa yang akan dilakukan proses sniffing dari wireshark. Data dari stream paket aktivitas tersebut biasanya terdiri dari alamat tujuan, proses aktivitas serta password yang biasanya terenkripsi. Data yang terenkripsi inilah yang dapat dikelola atau didekripsi menggunakan tools lainnya untuk mempermudah akses serangan terhadap target.

Setelah indormasi yang dibutuhkan telah didapat, tahap selanjutnya merupakan uji vulnerabilitas sistem menggunakan Metasploit. Pada terminal kali linux, masukkan perintah "sudo msfconsole" dan tunggu beberapa saat sampai Metasploit terakses. Setelah mendapat akses, menggunakan informasi layanan service dari port yang dituju yang telah didapat dari nmap, masukkan perintah "search <service>" pada konsol Metasploit untuk mendapat modul yang diinginkan, lalu pilih.

Setelah konsol menunjukkan telah masuk pada modul tersebut, berikan perintah "show options" untuk mengetahui apa saja yang dibutuhkan untuk mengakses modul tersebut. Pada kasus ini, diperlukan RHOST dan RPORT untuk akses seperti yang ditunjukkan pada gambar berikut.



Gambar 7. Options dari modul yang akan diakses

Biasanya semakin penting sebuah modul, semakin banyak hal yang dibutuhkan untuk dapat mengakses dan eksploitasi modul tersebut, seperti username, password, payload dan sebagainya. Setelah persyaratan terpenuhi, pada konsol berikan perintah "exploit" dan Metasploit akan mengakses modul tersebut. Output dari satu modul dapat beragam dan berbeda satu sama lainnya, pada kasus ini output yang

dihasilkan oleh Metasploit adalah versi korup dari target yang akan memberi tahu kelemahan lebih dalam lainnya.

Gambar 8. Hasil eksploitasi dari Metasploit.

4.1. Hasil Analisis Kemampuan Program

Tabel 1. Kemampuan Program

No	Alat	Info	Sniff	Exploit	Scan
1	Nmap	✓	X	✓	✓
2	Wireshark	✓	✓	X	✓
3	Metasploit	✓	X	✓	X

Nmap, Wireshark, dan Metasploit memiliki peran yang saling melengkapi dalam analisis keamanan jaringan. Nmap digunakan untuk pemetaan jaringan, seperti mengidentifikasi host aktif, port terbuka, layanan yang berjalan, dan kerentanan dasar. Wireshark, di sisi lain, fokus pada analisis lalu lintas jaringan secara rinci untuk memantau paket data yang melewati jaringan dan mendeteksi anomali. Metasploit kemudian digunakan untuk mengeksploitasi kerentanan yang ditemukan untuk menguji sejauh mana ancaman dapat dimanfaatkan. Dengan peran ini, ketiganya berkontribusi dalam memastikan pengamanan jaringan dari berbagai sudut.

Ketiga alat ini memiliki tujuan yang sama, yaitu meningkatkan keamanan jaringan melalui pemahaman menyeluruh tentang potensi ancaman dan celah keamanan. Nmap membantu memetakan permukaan serangan, Wireshark mengidentifikasi pola lalu lintas mencurigakan, dan Metasploit menguji seberapa jauh celah keamanan dapat dimanfaatkan. Kombinasi penggunaan alat-alat ini memungkinkan analis keamanan untuk mengambil langkah preventif dan responsif dalam melindungi jaringan, memastikan ancaman dapat diminimalkan sebelum menjadi masalah serius.

4.2. Hasil Analisis Penanggulangan Keamanan Jaringan

Setelah dilakukannya uji jaringan menggunakan alat, dapat dianalisis penyebab adanya kerentanan jaringan dari ubuntu melalui eksploitasi dari kali. Dengan bersumber yang sama yaitu port serta jaringan terbuka, cara yang didapat untuk menanggulangi keamanan jaringan adalah sebagai berikut:

a. Minimalkan port yang terbuka:
   Meminimalkan jumlah port yang terbuka adalah langkah pertama yang sangat penting dalam mengamankan jaringan. Anda dapat menggunakan firewall seperti iptables atau perangkat keras firewall untuk menutup semua port yang tidak diperlukan. Dengan membatasi akses hanya pada port yang penting, kita mengurangi peluang bagi penyerang untuk mengeksploitasi sistem.
b. Gunakan iptables daripada ufw
   Penggunaan Iptables lebih disarankan daripada ufw karena iptables menawarkan kontrol yang lebih mendetail dan fleksibel atas aturan firewall. Walaupun ufw lebih mudah digunakan, iptables memberikan kemampuan konfigurasi yang lebih mendalam sehingga lebih cocok untuk kebutuhan keamanan yang kompleks dan kritis.
c. Hindari menggunakan internet wifi dengan koneksi terbuka:
   Sangat penting untuk menghindari penggunaan wifi dengan koneksi terbuka, terutama di tempat umum karena wifi di tempat umum merupakan jaringan yang tidak aman dan rentan terhadap serangan. Studi menunjukkan bahwa perangkat seperti Kali Linux dan Ubuntu yang terhubung ke jaringan yang sama dapat mendeteksi kerentanannya, yang menunjukkan betapa mudahnya penyerang mendapatkan data pribadi.
d. Deteksi scanning:
   Sistem deteksi intrusi (IDS) seperti Snort atau Suricata dapat mendeteksi aktivitas scanning peretas dengan melacak lalu lintas jaringan untuk pola yang mencurigakan dan memberikan peringatan dini untuk membantu Anda mengambil tindakan pencegahan segera.
e. Selalu update patch dari sistem terbaru:
   Untuk menutup celah keamanan, sangat penting untuk terus memperbarui sistem dan aplikasi dengan patch terbaru. Teknik port-knocking juga dapat digunakan untuk meningkatkan keamanan dengan memastikan bahwa port hanya terbuka setelah pola koneksi tertentu dilakukan.
f. Gunakan enkripsi:
   Penggunaan enkripsi sangat krusial dalam melindungi data. Menerapkan protokol terenkripsi seperti HTTPS untuk web, SSH untuk akses jarak jauh, dan FTPS untuk transfer file akan memastikan bahwa data yang dikirimkan aman dari penyadapan. Selain itu, menggunakan VPN untuk mengenkripsi semua lalu lintas jaringan adalah langkah yang efektif untuk menjaga privasi dan keamanan data dalam perjalanan.
g. Segmentasi jaringan:
   Cara lainnya adalah segmentasi jaringan dengan VLAN memisahkan jaringan internal dan publik, sehingga orang tidak dapat mengakses jaringan internal. Ini mengisolasi sumber daya vital dan

mengurangi risiko orang yang tidak diinginkan mendapatkan data sensitif.

h. Deteksi sniffing:
Alat seperti ARP Watch dapat mendeteksi modus promiscuous atau ARP spoofing, yang membantu mencegah aktivitas penyadapan di jaringan. ARP Watch melacak lalu lintas ARP dan memberikan peringatan jika terdeteksi perubahan yang mencurigaka

i. Implementasi TLS/SSL:
Sangat penting untuk menerapkan sertifikat SSL/TLS pada aplikasi web atau server internal untuk melindungi data yang bergerak. TLS/SSL mengenkripsi komunikasi antara klien dan server, menjaga kerahasiaan dan integritas data dari pihak ketiga yang mungkin menyadap koneksi.

5. KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini adalah bahwa Kali Linux, melalui penggunaan alat seperti Nmap, Wireshark, dan Metasploit, terbukti efektif dalam menganalisis keamanan jaringan dengan mengidentifikasi kerentanannya, menganalisis lalu lintas data, dan melakukan simulasi serangan. Nmap dapat memberikan informasi mendetail mengenai perangkat yang terhubung dan port yang terbuka, Wireshark memungkinkan pengawasan dan analisis paket data secara real-time untuk mendeteksi aktivitas mencurigakan, sementara Metasploit memungkinkan eksploitasi kerentanannya secara terkontrol untuk menguji tingkat risiko yang dihadapi oleh sistem. Kombinasi alat ini memberikan pendekatan menyeluruh untuk memahami dan meningkatkan keamanan jaringan. Namun, penggunaan alat-alat ini memerlukan pemahaman mendalam agar tidak disalahgunakan, sehingga penggunaannya harus dilakukan secara etis dan dalam lingkungan pengujian yang aman. Sebagai saran, organisasi perlu menerapkan kebijakan keamanan jaringan yang lebih ketat, termasuk memblokir port yang tidak diperlukan, mengenkripsi data yang dikirimkan, serta secara berkala melakukan pengujian penetrasi untuk mengidentifikasi potensi kerentanannya. Selain itu, pelatihan keamanan siber bagi administrator jaringan dan pengguna umum sangat penting untuk meningkatkan kewaspadaan terhadap ancaman keamanan yang terus berkembang. Penelitian lanjutan dapat diarahkan untuk mengeksplorasi alat keamanan lainnya atau membandingkan metode ini dengan teknologi keamanan otomatis berbasis AI untuk memberikan solusi yang lebih komprehensif.

DAFTAR PUSTAKA

[1] M. Hasibuan and A. M. Elhanafi, “Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box,” *Sudo Jurnal Teknik Informatika*, vol. 1, no. 4, pp. 171–177, Dec. 2022, doi: https://doi.org/10.56211/sudo.v1i4.160.

[2] R. R. Asaad, "Penetration testing: Wirelessnetwork attacks method on Kali Linux OS," *Academic Journal of Nawroz University*, vol. 10, no. 1, pp. 7-12, 2021. [Online]. Available: https://scholar.google.com/scholar?as_ylo=2020&q=network+penetration+testing&hl=id&as_sdt=0,5#d=gs_qabs&t=1734329764717&u=%23p%3DnjiZw-JDFH4J

[3] S. Sunny and A. G. Christy, "Comparison of TCP scanning techniques using nmap," *Journal of Pharmaceutical Negative Results*, pp. 919-925, 2022. [Online]. Available: https://mail.pnrjournal.com/index.php/home/article/view/8075/10783

[4] L. Bock, *Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark*. Packt Publishing Ltd., 2022.

[5] S. Raj and N. K. Walia, "A study on metasploit framework: A pen-testing tool," in *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, pp. 296-302.

[6] K. Ruswandi, M. Reza Zulva Pohan, K. Viriya Halim, and S. Nidya Neyman, “Strategi Pencegahan Efektif Terhadap Serangan DDoS Slowloris Menggunakan Kali Linux Dan Linux Mint,” *IO Publishing: Journal of Technology and System Information*, vol. 1, no. 4, pp. 11–11, Jun. 2024, doi: https://doi.org/10.47134/jtsi.v1i4.2645.

[7] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, dan A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," *Journal of Internet and Software Engineering*, vol. 1, no. 4, hlm. 1-12, Okt. 2024. [Daring]. Tersedia:https://doi.org/10.47134/pjise.v1i4.2681.

[8] Zata Ismah Sumayyah, S. Dimas, Muhammad Tsabit, and A. Setiawan, “Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux,” *Deleted Journal*, vol. 1, no. 2, pp. 14–14, Jun. 2024,doi:https://doi.org/10.47134/pjise.v1i2.2694.

[9] R. Hefiana dan Y. Fernando, "Analisis Perbandingan Elastic Compute Service (ECS) Instance Alibaba Cloud Dengan Virtual Machine Azure," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 4, pp. 2158-2168, Feb. 2024. DOI: 10.30865/klik.v4i4.1655. [Online]. Available: https://djournals.com/klik.

[10] S. Liao *et al.*, “A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments,” *IEEE Xplore*, Oct. 01, 2020. https://ieeexplore.ieee.org/document/9329410

[11] I. Sumaiya Thaseen, B. Poorva, and P. S.

Ushasree, “Network Intrusion Detection using Machine Learning Techniques,” *IEEE Xplore*, Feb.01,2020.https://ieeexplore.ieee.org/abstract/document/907782/ (accessed Apr. 14, 2023).

[12] J. E. Varghese and B. Muniyal, "A Pilot Study in Software-Defined Networking Using Wireshark for Analyzing Network Parameters to Detect DDoS Attacks," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, M. S. Kaiser, J. Xie, and V. S. Rathore, Eds. Lecture Notes in Networks and Systems, vol. 190, Singapore: Springer, 2021, pp. [specific page range if known]. DOI: 10.1007/978-981-16-0882-7_41.

[13] A. Ghafar Jaafar, S. Adli Ismail, A. Habir, K. Akram, and O. Mohd Yusop, “A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 5, Jan. 2024, doi: https://doi.org/10.14569/ijacsa.2024.0150568.