Vol 2. No. 1 2023 Hal 88-96

Deteksi Serangan DDoS Dan Sniffing Pada Jaringan Wireless Di Lab Informatika Um Surabaya Dengan Metode Vulnerability Assessment

Rafih Anugerah Julyan Rahmat[1], Nuniek Fahriani[2]
[1,2]Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Surabaya
Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Surabaya, Jawa Timur 60113
e-mail: [1]rafihanugerah16@gmail.com, [2]nuniekfahriani@ft.um-surabaya.ac.id

Abstrak

Masyarakat telah menikmati perkembangan teknologi khususnya di bidang informasi salah satunya yang telah berkembang saat ini adalah internet. Dalam penggunaannya, jaringan yang dipakai oleh masyarakat adalah kabel LAN maupun Wireless LAN (Tanpa Kabel), adapun kerentanan terhadap keamanan jaringan yang melakukan serangan dari pihak yang tidak bertanggung jawab yaitu hacker yang bisa mengeksploitasi data penting dari pengguna, menyadap data seperti password dan mengubah isi data penggunanya. Adapun tools atau aplikasi yaitu Wireshark yang digunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Suatu Jaringan pun bisa down akibat serangan dari DDOS (Disc Denial Of Service) dan jaringan pun dapat juga disadap (Sniffing) dengan mudahnya menggunakan tools – tools yang tersedia. Dari hasil penelitian ini terdapat adanya kerentanan jaringan yang terdapat pada jaringan Lab. Teknik UMSurabaya. Maka diharapkan dengan adanya penelitian ini agar dilakukan tindakan pengamanan pada jaringan Lab. Teknik UMSurabaya agar tidak terjadi hal – hal yang tidak diinginkan.

***Kata Kunci**: DDOS, Sniffing, Wireless LAN*

Abstract

People have enjoyed technological developments, especially in the field of information, one of which has developed today is the internet. In its use, the network used by the community is wired LAN or Wireless LAN (Without Cable), as for the vulnerability to network security that carries out attacks from irresponsible parties, namely hackers who can exploit important data from users, intercept data such as passwords and change the contents of user data. The tools or applications are Wireshark which is used to analyze network protocols and audit network security. A network can also be down due to attacks from DDOS (Disc Denial Of Service) and the network can also be tapped (Sniffing) easily using available tools. From the results of this study, there is a network vulnerability found in the UMSurabaya Engineering Lab network. So it is hoped that with this research security measures will be carried out on the UMSurabaya Engineering Lab network so that unwanted things do not happen.

***Keywords**: DDOS, Sniffing, Wireless LAN*

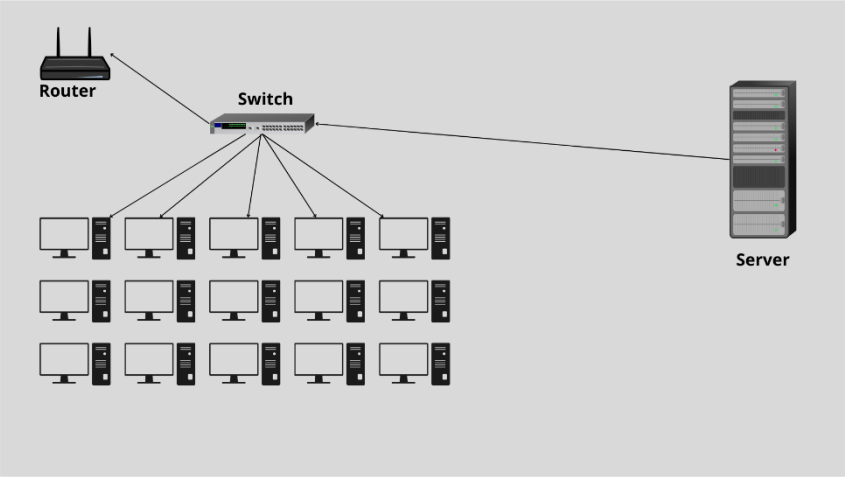
1. PENDAHULUAN

Teknologi wireless saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Jaringan wireless LAN adalah jaringan yang mengkoneksikan dua komputer atau lebih menggunakan sinyal radio, Wireless LAN dapat digunakan pada jaringan peer to peer dalam ruangan dan juga point to point di luar ruangan maupun point to multipoint pada aplikasi bridge. [1] Jaringan Wireless LAN di desain sangat modular dan fleksibel sehingga Jaringan ini dapat dioptimalkan pada lingkungan yang berbeda. Jaringan komunikasi wireless memberikan kemudahan dan fleksibilitas yang tinggi bagi para pemakainya sehingga dapat melakukan hubungan komunikasi dengan

sesama pemakai jaringan wireless maupun dengan pemakai lain yang terhubung dengan jaringan yang memakai media transmisi kabel (wired network) sehingga sangat banyak digunakan, baik untuk komunikasi suara maupun data. [2]

UMSurabaya saat ini telah menyediakan fasilitas jaringan komputer kabel maupun nirkabel atau lebih sering dikenal wireless sebagai sarana untuk pertukaran data, pencarian informasi seperti materi mata kuliah, Pengisian Kartu Rencana Studi (KRS), penginputan nilai, e-learning atau kuliah jarak jauh dan lain – lain. Fasilitas layanan jaringan komputer tersebut diberikan kepada mahasiswa, dosen dan pegawai yang ada di lingkungan Universitas Muhammadiyah Surabaya.

Untuk menguji keamanan dari jaringan server Laboratorium Teknik Informatika UMSurabaya peneliti akan melakukan uji kerentanan dan mengidentifikasi jaringan menggunakan metode Vulnerabillity Assessment terhadap jaringan wireless untuk mencegah serangan DDOS maupun Sniffing terhadap jaringan wireless Laboratorium Teknik Informatika.

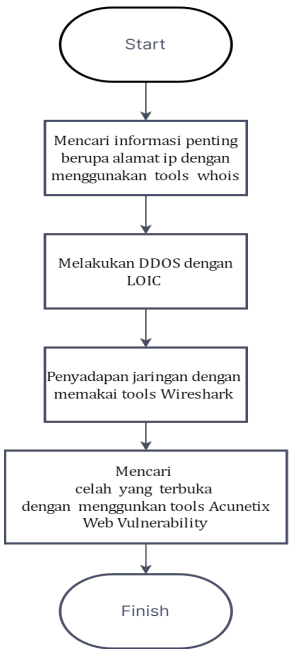


Gambar 1. Topologi jaringan Lab. Teknik UMSurabaya

2. METODE PENELITIAN

Langkah Langkah Penelitian

a. Mencari informasi penting berupa alamat ip dengan menggunakan tools whois dan mendapatkan alamat ip, domain, dan server yang dipakai serta informasi lainnya.
b. Melakukan DDOS dengan LOIC (Low Orbit Ion Canon).
c. Menguji keamanan wifi dengan metode Sniffing / Penyadapan dengan memakai tools Wireshark
d. Mencari celah yang terbuka dengan menggunkan tools Acunetix Web Vulnerability hasilnya terdapat kurang lebih 76 celah yang didapat tapi celah yang ditemukan masih kategori aman karena tingkat ancaman hanya berada pada level 2 saja.



Gambar 2. Tabel Alur

2.1. Melakukan Diagnosa

Pada tahap diagnosa peneliti akan melakukan identifikasikan masalah-masalah pada saat melakukan penelitian Analisis Keamanan Jaringan wireless di Laboratorium Teknik UMSurabaya. Langkah yang ditempuh adalah melakukan tes kepada Jaringan di Laboratorium Teknik yang terkait langsung maupun tidak langsung. Masalah yang terkait langsung dalam penelitian ini adalah mengenai keamanan jaringan .

a. Membuat rencana tindakan (action planning)

Melakukan pemahaman pokok pokok permasalahan yang akan dilanjutkan pada tahap rencana tindakan ini, pada tahap ini melakukan rencana tindakan yang akan dilakukan pada Jaringan LAN dan pengujian sistem keamanannya.

b. Melakukan tindakan (action taking)

Pada tindakan action taking menerapkan rencana dengan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan mengikuti fase penetrasi testing terhadap website cybercampus-umsurabaya untuk mencari celah keamanan pada website . Pada tahapan ini, Peneliti sebagai penguji mengimplementasikan rencana tindakan denganharapan dapat menemukan celah keamanan Website Unsrat Proses pelaksanaannya, pertama kali peneliti mengecek menggunakan aplikasi Aplikasi Whois untuk mendapatkan informasi seperti alamat ip dan informasi lainnya, kemudian dilanjutkan dengan menggunakan tools WireShark untuk melakukan Sniffing pada jaringan Lab. Dan untuk DDoS menggunakan tools LOIC.

2.2. Pembelajaran

a. Metode pengumpulan data

1. Pengamatan

   Mengadakan peninjauan langsung jaringan LAN serta meninjau lokasi yang bisa dijadikan spot untuk melakukan penelitian di Lab. Teknik UMSurabaya dengan objek penelitian yang ada.

2. Pengujian

   Untuk mendapatkan informasi dan mendapatkan data-data secara langsung, maka dalam hal ini peneliti melakuakan pengujian terhadap jaringan yang akang diteliti agar bisa memperoleh gambaram model pengujian yang lebih detail.

3. Studi kepustakaan

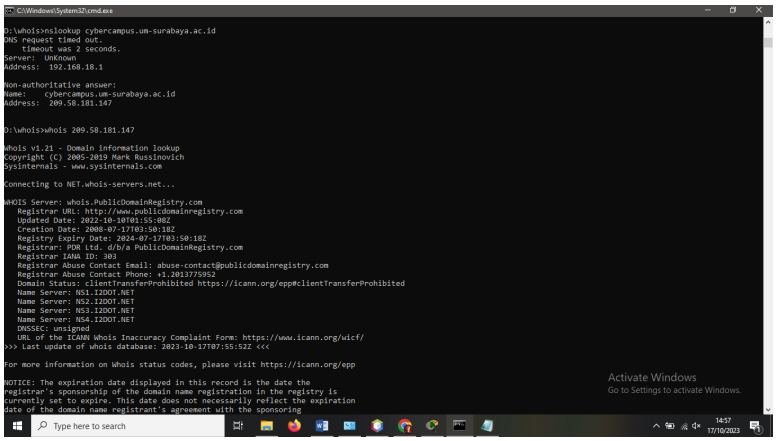
   Data juga diperoleh melalui studi kepustakaan (literature) yaitu dengan cara mencari bahan dari internet, jurnal dan perpustakaan serta buku yang sesuai dengan objek yang akan diteliti.

b. Tools yang digunakan

1. Whois

   Tools Whois adalah alat atau layanan yang digunakan untuk mendapatkan informasi tentang kepemilikan domain dan data terkait lainnya. WHOIS merupakan protokol yang digunakan untuk mencari informasi tentang domain tertentu, seperti nama pemilik domain, alamat kontak, informasi pendaftaran, dan informasi teknis terkait domain tersebut. [3]

   Dalam konteks alat atau layanan Whois, pengguna dapat memasukkan nama domain yang ingin diketahui informasinya, dan alat tersebut akan menghubungi server Whois yang relevan untuk mendapatkan informasi terkait domain tersebut. Informasi yang dihasilkan dapat mencakup informasi pemilik domain, tanggal pendaftaran, tanggal kedaluwarsa, server nama (name server) yang digunakan, dan informasi kontak terkait. [4] Contoh kegunaannya dapat dilihat pada Gambar 2. Informasi pada website *cybercampus.um-surabaya.ac.id*



Gambar 3. Informasi Website *cybercampus.um-surabaya.ac.id*

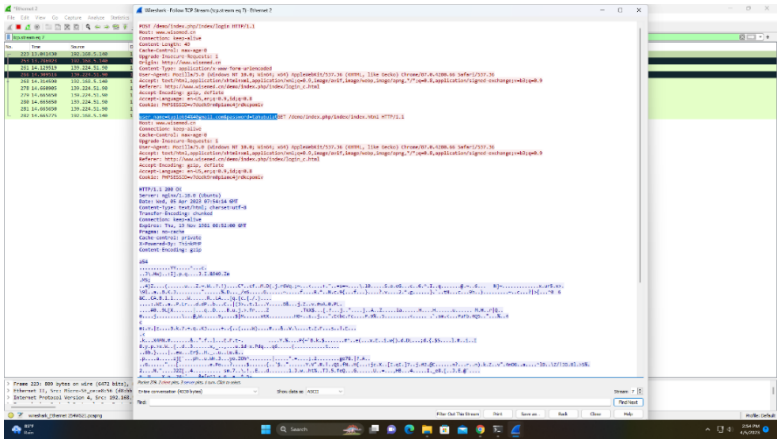
Tools Whois sering digunakan oleh berbagai pihak, seperti perusahaan web hosting, penyedia layanan domain, penegak hukum, dan peneliti keamanan

siber. Informasi yang diperoleh melalui Whois dapat membantu dalam mengidentifikasi pemilik domain, menyelesaikan sengketa domain, atau melacak aktivitas yang mencurigakan di internet. [5]

2. Wireshark

Wireshark adalah sebuah perangkat lunak (software) yang digunakan untuk menganalisis lalu lintas jaringan. Dengan menggunakan Wireshark, pengguna dapat melihat dan memeriksa paket data yang dikirim dan diterima oleh komputer atau perangkat dalam jaringan. [6]

Wireshark dapat digunakan untuk memantau dan menganalisis berbagai protokol jaringan, seperti TCP/IP, UDP, HTTP, DNS, FTP, dan banyak lagi. Dengan melihat paket data yang dikirim dan diterima, pengguna dapat mempelajari dan menganalisis interaksi antara perangkat dalam jaringan, mengidentifikasi masalah jaringan, menemukan celah keamanan, atau memeriksa kinerja jaringan. [7]



Gambar 4. Hasil uji coba wireshark pada jaringan lab

Seperti gambar yang ditampilkan diatas bahwa penyadapan yang dilakukan dengan tools Wireshark bisa dikatakan berhasil karena pada penyadapan tersebut dapat dilihat bahwa system keamanan jaringan pada LAB sangatlah rentan terhadap penyadapan.

Fitur utama Wireshark meliputi:

- Pemantauan Paket: Wireshark dapat merekam dan menampilkan semua paket data yang dikirim dan diterima dalam jaringan, termasuk informasi protokol, header, dan payload.

- Analisis Protokol: Wireshark dapat menganalisis dan mendekode berbagai protokol jaringan, memungkinkan pengguna untuk memahami bagaimana komunikasi terjadi antara perangkat.

- Penyaringan dan Pencarian: Wireshark menyediakan fitur penyaringan yang kuat, yang memungkinkan pengguna untuk memfilter dan mencari paket data berdasarkan berbagai kriteria, seperti alamat IP, port, protokol, atau kata kunci tertentu.

- Statistik Jaringan: Wireshark dapat menghasilkan statistik tentang lalu lintas jaringan, seperti jumlah paket, bandwidth, waktu respons, dan lain-lain. [8]

3. LOIC

LOIC (Low Orbit Ion Cannon) adalah sebuah alat serangan yang dirancang untuk melakukan serangan DDoS (Distributed Denial of Service). LOIC awalnya dikembangkan sebagai alat pengujian jaringan oleh sekelompok pengembang, tetapi juga dapat digunakan oleh individu atau kelompok dengan niat jahat untuk menargetkan dan menonaktifkan situs web atau layanan online. [9]

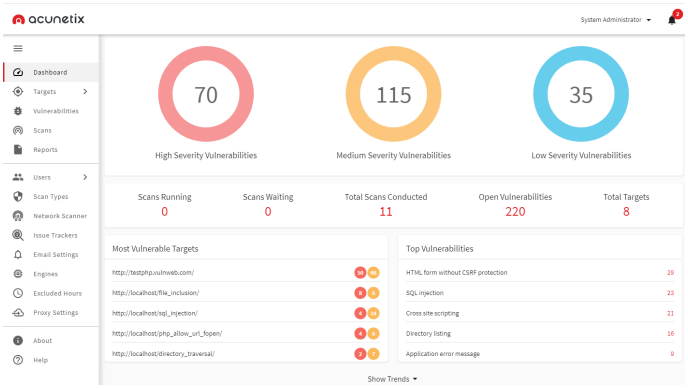
LOIC bekerja dengan mengkoordinasikan serangan dari banyak komputer yang terhubung ke jaringan yang sama. Komputer-komputer ini saling berkomunikasi dan mengirimkan permintaan ke target yang ditentukan. Dengan membanjiri target dengan lalu lintas data yang besar, serangan DDoS seperti ini dapat mengakibatkan penurunan kinerja atau bahkan penonaktifan sementara target tersebut. [5]

3. HASIL DAN PEMBAHASAN

1. Solusi Testing Acunetix Web Vulnerability Scanner

Berikut adalah uraian celah keamanan yang terbuka pada hasil celah keamanan yang ditemukan dalam hasil scan terdapat ancaman yang didapat dalam tingkatan level yang ada dalam tools Acunetix Web Vulnerability Scanner celah yang ditemukan selai tertulis dalam kotak juga terdapat warna yang menunjukkan tingkat ancaman celah keamanan dengan warna serta jumlah nilai ancaman dalam bentuk angka.

Merah (High), dengan jumlah nilai 70
Kuning (Medium), dengan jumlah nilai 115
Biru (Low), dengan jumlah nilai 35



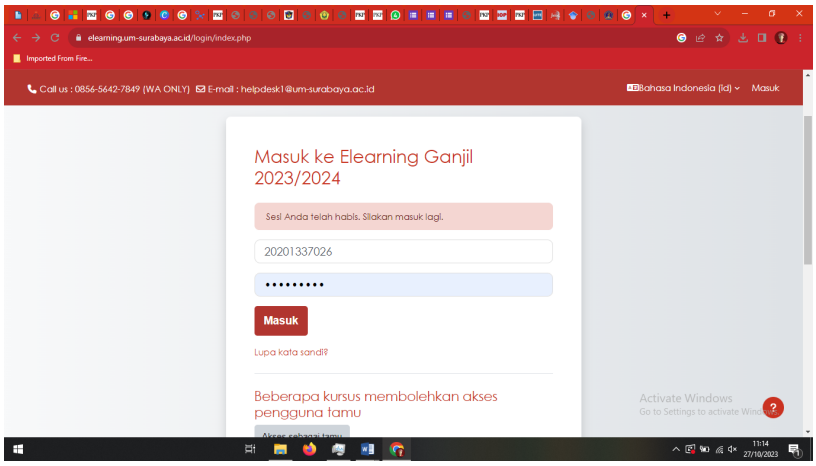
Gambar 5. Informasi Celah Keamanan Website

Dapat juga dilihat pada gambar diatas bahwa terdapat permintaan Lintas-Situs (CSRF, atau XSRF) adalah kerentanan di mana penyerang dapat menipu korban untuk membuat permintaan yang tidak diinginkan korban. Oleh karena itu, dengan CSRF, penyerang menyalahgunakan kepercayaan yang dimiliki suatu aplikasi web dengan browser korban.

 Acunetix menemukan bentuk HTML tanpa perlindungan anti-CSRF yang jelas diterapkan. [10]

2. Hasil Uji DDOS dan Sniffing

Dari hasil pengujian flooding selama kurang lebih 30 menit dengan menggunakan tools Loic pada website *elearning.um-surabaya.ac.id* dapat dipastikan bahwa website tersebut down untuk sementara waktu sehingga akses user untuk mengakses website tersebut terganggu seperti yang terlihat pada Gambar 5. Website Elearning UMSurabaya



Gambar 6. Website Elearning UMSurabaya

Dari masalah yang terdapat pada acunetix peneliti mencoba menggali informasi penting yang terdapat pada website *cybercampus.um-surabaya.ac.id* dengan melakukan metode sniffing yang bertujuan untuk menyadap aktifitas yang dilakukan, dan melakukan scanning sniffing menggunakan tools wireshark. Setelah mendapat hasil peneliti mencoba menggali apa yang ditemukan dalam hal ini peneliti berhasil mendapatkan email dan password yang terekam seperti yang disimulasikan yang ditampilkan pada Gambar 3. Hasil uji coba wireshark pada jaringan LAB. Makadari hasil ini bisa dipastikan admin Lab. Teknik tidak menggunakan semacam alat anti penyadapan / tools untuk menghalau aktifitas penyadapan / sniffing untuk menjaga keamanan data dan user.

Tabel Rekap

No	Jenis serangan	Tools	Keterangan	Status
1	Sniffing	WireShark	Melakukan Penyadapan	Berhasil

2	DDOS	LOIC	Melakukan Flooding	Berhasil

4. KESIMPULAN

Berdasarkan hasil penelitian serta pembahasan yang telah diuraikan, maka dapat disimpulakan bahwa : Bahwa keamanan jaringan pada Lab. Teknik UMSurabaya belum sepenuhnya dapat dikatakan aman, walaupun masih dikatakan belum aman tetapi tingkat ancaman yang ditunjukkan hanya berada di level 2 dan tidak mendapatkan tingkat keamanan pada level high pada web alert akan tetapi jaringan Lab. Teknik UMSurabaya masih bisa terkena Flooding dan metode penyerangan DDOS masih bisa dilakukan. Sedangkan pada level Medium yang mengandung informasi sensitif, dan sehingga keamanan pada website elearning UMSurabaya berhasil dan dapat penetrasi dan server terganggu.

UCAPAN TERIMAKASIH

Saya ingin menyampaikan terima kasih kepada Dosen Pembimbing atas bimbingan dan nasihat yang berharga dalam menyelesaikan paper ini. Bimbingan Anda telah membantu Saya dalam memahami konsep dan metodologi yang digunakan.

DAFTAR PUSTAKA

[1] H. R. C. K. Yudi Mulyanto, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing," p. 10, 2022.

[2] J. S. A. S. H. S. Sondy Kumajas, "Wireless Local Area Network Security through Protocol Wireless Protected Access," *International Journal of Information Technology and Education (IJITE),* p. 12, 2022.

[3] J. P. P. I. P. M. H. T. Jayvirsinh, "Analysis and Implementation of Domain Hosting and WHOIS Data Web Application," p. 6, 2021.

[4] M. L. S. G. C. H. G. a. T. F. Florian Streibelt, "Back-to-the-Future Whois: An IP Address," p. 18, 2023.

[5] A. S. L. X. B. N. Abraham Yano Suharmanto, "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi," p. 10, 2018.

[6] M. T. A. L. L. D. ,. I. C. ,. I. C. ,. F. N. H. ,. D. M. S. ,. D. A. ,. A. A. P. ,. A. M. Putri Tsania Mahmud, "SNIFFING JARINGAN MENGGUNAKAN WIRESHARK," p. 4, 2019.

[7] A. G Jain, "Application of SNORT and Wireshark in Network," p. 9, 2021.

[8] I. A. U. D. G. S. M. I Kadek Noppi Adi Jaya1, "Implementation of Wireshark Application in Data Security Analysis on LMS Website," *Journal of Computer Networks, Architecture and High Performance Computing,* p. 8, 2022.

[9] Y. F. H. Y. B. F. N. O. Yunanri W, "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology(NIST)," *KLIK: Kajian Ilmiah Informatika dan Komputer,* p. 7, 2023.

[10] S. R. S. B. Frenly Kristianto, "ANALISIS KERENTANAN PADA WEBSITESERVIO MENGGUNAKAN ACUNETIX WEB VULNERABILITY," p. 10, 2022.