Available *online*at : http://bit.ly/InfoTekJar

InfoTekJar :Jurnal Nasional InformatikadanTeknologiJaringan

ISSN (Print) 2540-7597|ISSN (Online) 2540-7600

Simulasi Serangan Man-in-the-Middle Menggunakan Virtualbox dan Wireshark di Jaringan Wi-Fi Publik Perpustakaan UIN Ar-Raniry

Fitra Akbar Eka Putra [*], *Oris Krianto Sulaiman*

Program Studi Pendidikan Teknologi Informasi, Fakultas Tarbiyah dan Keguruan, UIN Ar-Raniry Banda Aceh, Banda Aceh, Indonesia

KEYWORDS (*)

Man-in-the-Middle
ARP spoofing
Wireshark
VirtualBox
Wi-Fi publik

CORRESPONDENCE

E-mail: 121212070@student.ar-raniry.ac.id

A B S T R A C T

Penelitian ini mensimulasikan serangan Man-in-the-Middle (MitM) pada jaringan Wi-Fi publik Perpustakaan UIN Ar-Raniry menggunakan lingkungan virtual (VirtualBox) dan analisis trafik dengan Wireshark. Teknik yang digunakan berfokus pada ARP spoofing untuk mengalihkan trafik klien melalui mesin penyerang sehingga lalu lintas dapat dipantau dan dianalisis. Hasil simulasi menunjukkan bahwa MitM berbasis ARP spoofing berhasil mengintersepsi paket tertentu dan membuka peluang kebocoran informasi apabila koneksi tidak terlindungi (misalnya non-HTTPS/tanpa VPN). Sebagai pembanding, uji flooding (DoS) dengan hping3 dalam lingkungan virtual tidak secara signifikan menurunkan kualitas layanan karena keterbatasan antarmuka virtual dan adanya proteksi bawaan perangkat jaringan. Temuan ini menegaskan pentingnya penerapan praktik pengamanan berlapis pada jaringan publik serta edukasi pengguna.

PENDAHULUAN

Perkembangan teknologi informasi telah memberikan kemudahan dalam akses internet, salah satunya melalui layanan Wi-Fi publik di lingkungan pendidikan. Perpustakaan UIN Ar-Raniry menyediakan fasilitas Wi-Fi yang digunakan mahasiswa untuk menunjang aktivitas akademik. Namun, jaringan Wi-Fi publik memiliki risiko keamanan yang tinggi karena dapat diakses oleh siapa saja tanpa kontrol yang ketat. Kondisi ini membuka peluang terjadinya serangan siber, khususnya serangan Man-in-the-Middle (MitM), di mana penyerang dapat menyusup di antara komunikasi antara pengguna dengan penyedia layanan.

Salah satu bentuk serangan MitM yang umum adalah ARP spoofing, yaitu manipulasi tabel ARP pada perangkat korban agar trafik dialihkan melalui host penyerang. Teknik ini memungkinkan penyerang untuk merekam, memantau, atau bahkan memodifikasi data yang dikirimkan oleh pengguna, terutama jika data tidak dilindungi enkripsi yang memadai. Di sisi lain, serangan Denial of Service (DoS) juga sering digunakan untuk mengganggu ketersediaan layanan jaringan dengan cara membanjiri target menggunakan paket palsu, meskipun sebagian besar perangkat modern telah memiliki proteksi bawaan terhadap serangan tersebut.

Berdasarkan permasalahan tersebut, penelitian ini melakukan simulasi serangan Man-in-the-Middle menggunakan VirtualBox dan Wireshark pada jaringan Wi-Fi publik Perpustakaan UIN Ar-Raniry. Lingkungan virtual dipilih agar percobaan dapat dilakukan secara aman tanpa mengganggu jaringan produksi. Penelitian ini bertujuan untuk menunjukkan potensi kerentanan jaringan publik terhadap serangan MitM, menganalisis dampak yang ditimbulkan, serta memberikan gambaran awal mengenai langkah mitigasi yang dapat diterapkan dalam meningkatkan keamanan jaringan Wi-Fi di lingkungan kampus

METODE PENELITIAN

Penelitian ini menggunakan metode simulasi serangan jaringan dalam lingkungan virtual. Simulasi dilakukan menggunakan VirtualBox sebagai platform virtualisasi, dengan dua mesin virtual yang merepresentasikan attacker node dan victim node. Serangan Man-in-the-Middle dilakukan melalui teknik ARP spoofing menggunakan Ettercap, sedangkan proses pemantauan dan analisis paket jaringan dilakukan dengan Wireshark. Sebagai perbandingan, dilakukan pula serangan Denial of Service (DoS) menggunakan hping3 untuk menguji dampaknya terhadap kinerja jaringan.

Alur Penelitian

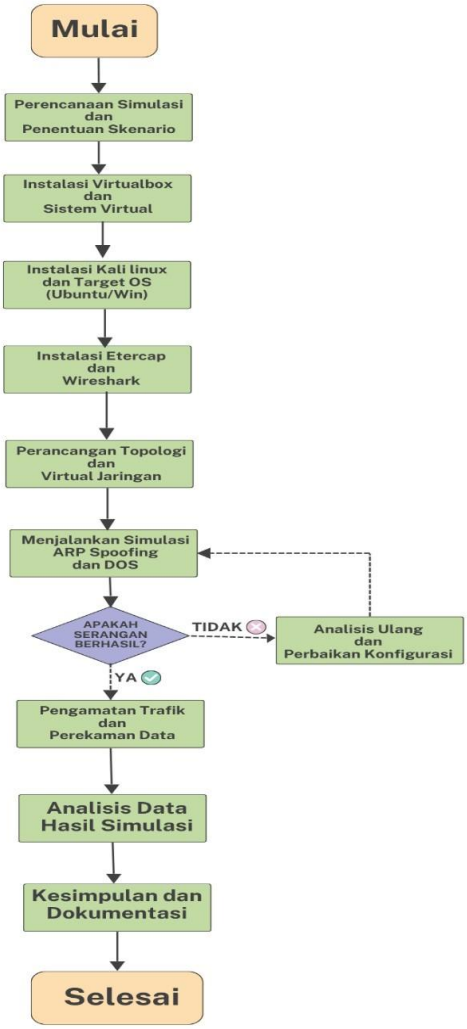
Alur penelitian disusun dalam bentuk flowchart sebagaimana ditunjukkan pada Gambar 1, yang meliputi tahapan:

1. Identifikasi masalah dan studi literatur awal
2. Penentuan pendekatan dan metode penelitian
3. Instalasi VirtualBox, Kali Linux, Windows, serta tools seperti Ettercap dan Wireshark
4. Perancangan topologi jaringan virtual

DOI: https://doi.org/10.30743/infotekjar.v10i1.11939

Attribution-NonCommercial 4.0 International. Some rights reserved

5. Pelaksanaan simulasi serangan ARP Spoofing dan DoS
6. Pengamatan dan dokumentasi hasil simulasi
7. Analisis data dan penyusunan kesimpulan
8. Penyusunan laporan akhir

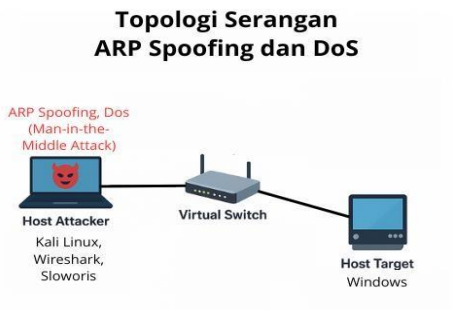


Gambar 1. Flowchart Alur Penelitian

Topologi Jaringan

Topologi jaringan penelitian ditunjukkan pada Gambar 2, yang terdiri dari:

1. **Attacker Node** → menjalankan Ettercap dan hping3.
2. **Victim Node** → menjadi target serangan.
3. **Router Virtual** → berfungsi sebagai gateway jaringan Wi-Fi publik.



Gambar 2. Topologi Alur Penelitian

Spesifikasi Perangkat dan Software

Untuk memastikan replikasi penelitian, spesifikasi perangkat keras dan perangkat lunak digunakan sebagaimana ditunjukkan pada Tabel 1.

Tabel 1. Spesifikasi perangkat keras dan perangkat lunak penelitian

NO	Komponen	Spesifikasi
1	Laptop Host	Intel Core i5, RAM 8 GB, Windows 10
2	Virtualisasi	VirtualBox 7.2.0
3	Sistem Operasi Penyerang	Kali Linux 2023.3
4	Sistem Operasi Router/Gateaway	Debian 13
5	Sistem Operasi Korban	Windows 11
6	Tools	Ettercap, Wireshark, hping3

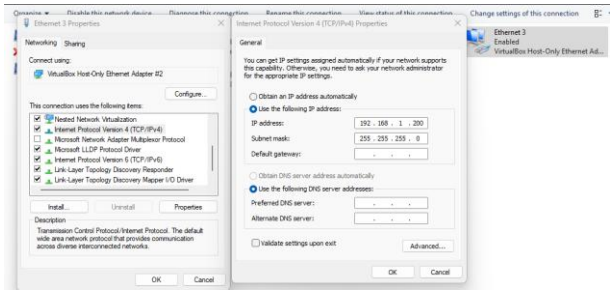
HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan serangkaian simulasi serangan Man-in-the-Middle (ARP spoofing) dan Denial of Service (DoS) yang dilakukan dalam lingkungan VirtualBox. Setiap tahapan dicatat dalam bentuk tangkapan layar (screenshot), kemudian dianalisis untuk mengetahui dampaknya terhadap jaringan. Selain itu, hasil simulasi juga memperlihatkan adanya perbedaan karakteristik antara serangan ARP spoofing dan DoS dari sisi tingkat keberhasilan. ARP spoofing terbukti efektif dalam memperoleh akses terhadap lalu lintas data korban karena memanfaatkan kelemahan protokol ARP yang tidak memiliki mekanisme autentikasi. Sementara itu, serangan DoS yang dijalankan melalui flooding paket tidak mampu menurunkan performa jaringan secara signifikan karena terbatasnya kemampuan antarmuka virtual dan adanya fitur proteksi bawaan pada router. Hal ini menunjukkan bahwa serangan berbasis manipulasi protokol lebih berbahaya pada jaringan publik dibandingkan serangan berbasis traffic flooding, sehingga mitigasi keamanan sebaiknya difokuskan pada pencegahan serangan MitM seperti ARP spoofing.

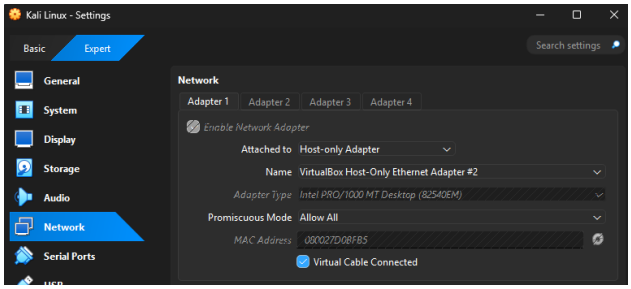
DOI: https://doi.org/10.30743/infotekjar.v10i1.11939

Menyiapkan Perangkat Virtualisasi

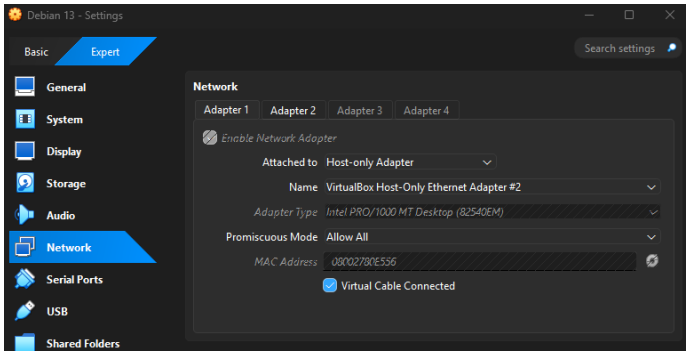
Pada tahap ini dilakukan persiapan lingkungan uji dengan menggunakan VirtualBox. Mesin virtual yang digunakan terdiri dari attacker (Kali Linux) dan victim (Windows 10). Keduanya dihubungkan dalam jaringan Host-Only Adapter agar dapat saling berkomunikasi. Dilakukan pengaturan gateway, konfigurasi IP, serta pengujian konektivitas untuk memastikan jaringan siap digunakan sebelum serangan disimulasikan. Simulasi dilakukan dalam bentuk tahapan praktis yang didokumentasikan dengan 17 tangkapan layar dari "Gambar 3" Sampai pada "Gambar 19".



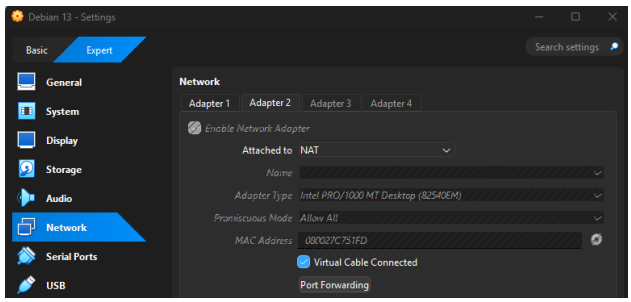
Gambar 3. Samakan gateway pada Windows dan Debian agar jalur masuk jaringan dapat terhubung dengan Host-Only Adapter. Hal ini dilakukan agar victim dan attacker berada dalam satu jaringan.



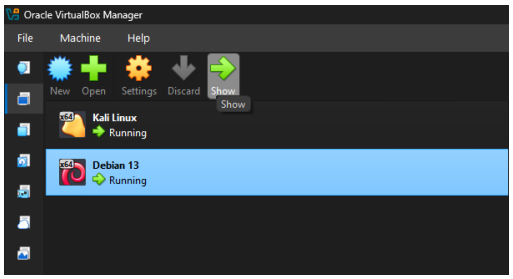
Gambar 4. Konfigurasi network pada mesin virtual attacker dilakukan agar sesuai dengan gateway jaringan



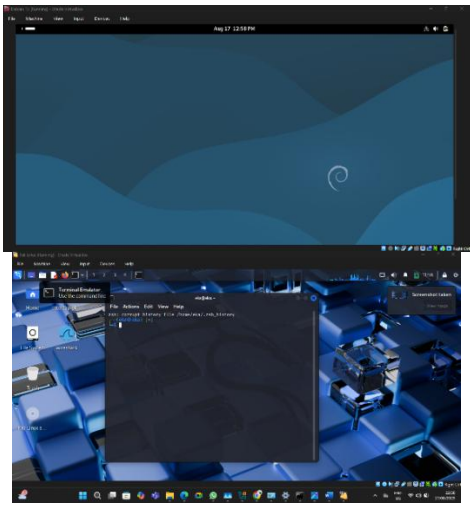
Gambar 5. Pengaturan interface pada VirtualBox di Oprasi sistem Debian 13 untuk untuk terhubung ke konfigurasi Host-Only Adapter.



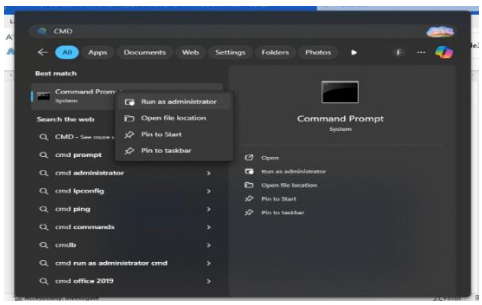
Gambar 6. Pembuatan jalur jaringan debian untuk dapat mengakses internet di adapter ke 2 yaitu NAT, agar dapat mengakses ke internet.



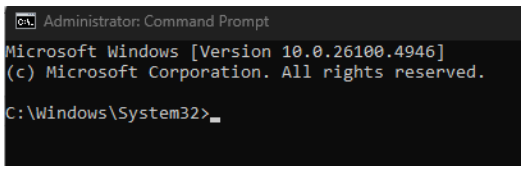
Gambar 7. Membuka semua OS, untuk penyerangan, dan untuk gateaway, dari virtualbox, pada Kali Linux untuk aplikasi penyerangan, Debian 13 untuk Gateaway yang menghubungkan OS penyerangan dan korban.



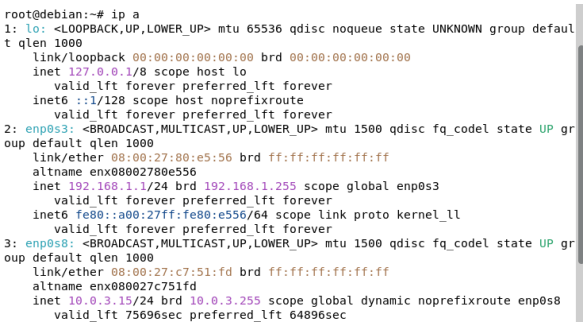
Gambar 8. Debian dan kali linux sudah terbuka, dan siap untuk konfogurasi ip untuk menjalankan snifing.



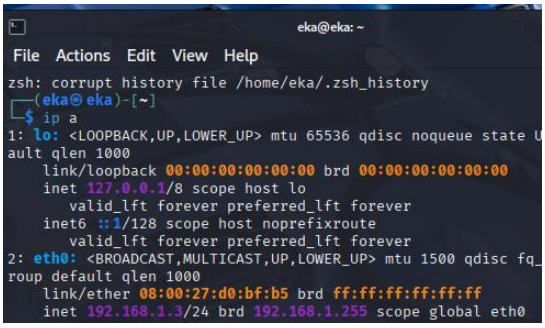
Gambar 9. Korban menggunakan Windos asli (menggunakan device asli/OS pada pc) dan windows harus tersambung pada gateaway debian melalui Command Promt dan jalankan menggunakan run administrator.



Gambar 10. Command Promt sudah terbuka , siap untuk menghubungkan pada gateaway di os debian.



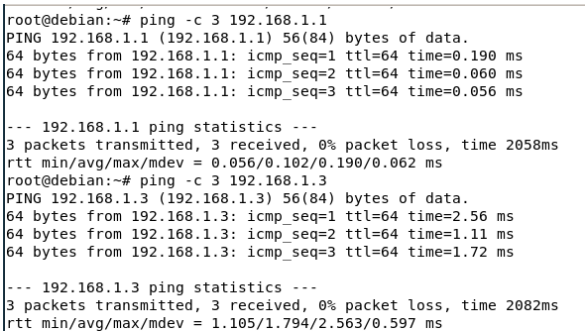
Gambar 11. Cek ip yang sudah dibuat pada debian dengan menjalankan perintah “ip a” enp0s3 adalah adapter gateaway yang terhubung ke adapter 1 yaitu “Host-Only Adapter” dengan ip debian itu sendiri yaitu 192.168.1.1. Gateaway ip debian yang tergubung ke internet adalah enp0s8 yang terhubung ke adapter NAT yaitu dengan ip 10.0.3.15 di debian.



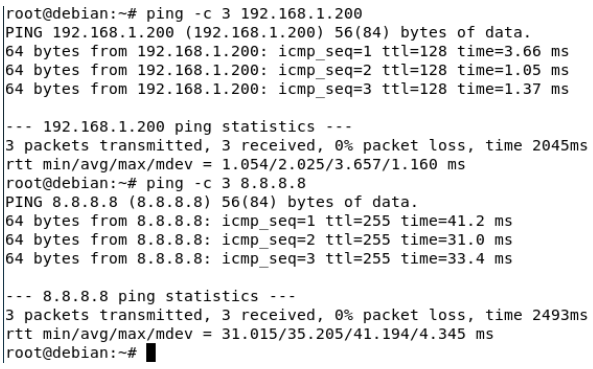
Gambar 12. Cek ip yang sudah dibuat pada kali linux dengan menjalankan perintah “ip a”, enp0s3 adalah adapter gateaway yang terhubung ke adapter 1 yaitu Host-Only Adapter, dengan ip kali linux itu sendiri yaitu 192.168.1.3 yang akan terhubung ke alamat ip debian.



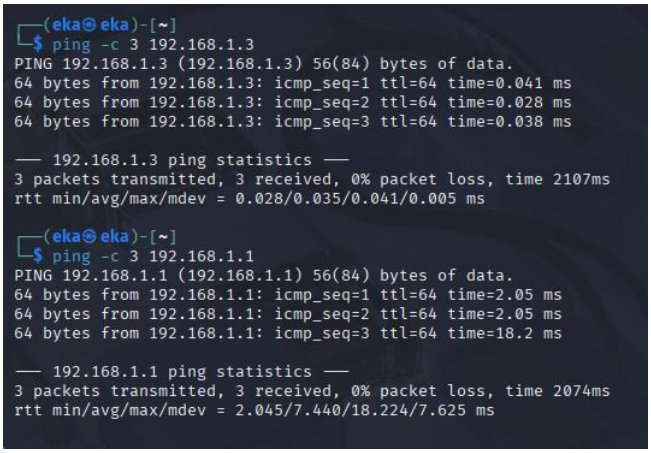
Gambar 13. Cek ip yang sudah dibuat di control panel windows, yaitu adapter network windows yang akan disambungkan ke debian yang akan menjadi ip windows itu sendiri yaitu 192.168.1.200 dengan menjalankan perintah “ipconfig”.



Gambar 14. Sambungkan sesama ip pada os debian, alasannya adalah untuk memanggil semua ip agar tersambung pada debian, debian berhasil ping alamat ip sendiri yang sudah dibuat untuk debian dengan perintah “ping -c 3 192.168.1.1”, debian berhasil memanggil alamat ip kali linux dengan perintah “ping -c 3 192.168.1.3”.

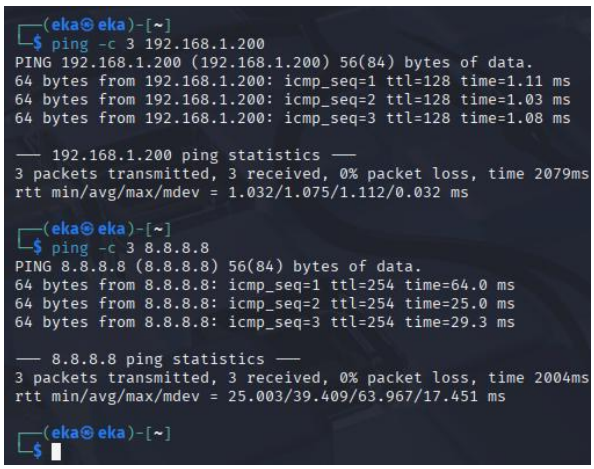


Gambar 15. Debian berhasil memanggil alamat ip pada windows dengan perintah “ping -c 3 192.168.1.200” debian berhasil memanggil alamat ip internet dengan perintah “ping -c 3 8.8.8.8”.

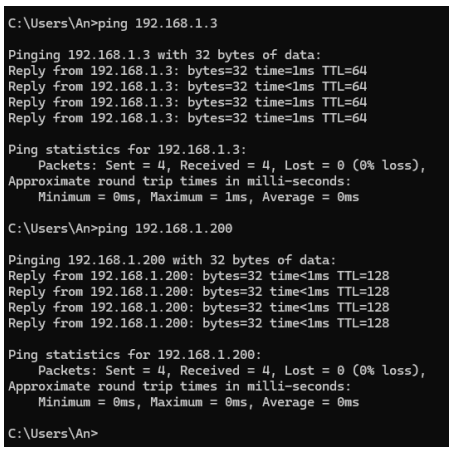


Gambar 16. Sambungkan sesama ip pada os kali linux, alasannya adalah untuk memanggil semua ip agar tersambung pada kali linux, kali linux berhasil ping alamat ip sendiri yang sudah dibuat untuk tersambung ke debian dengan perintah “ping -c 3 192.168.1.3”, kali linux berhasil memanggil alamat ip debian dengan perintah “ping -c 3 192.168.1.1”.

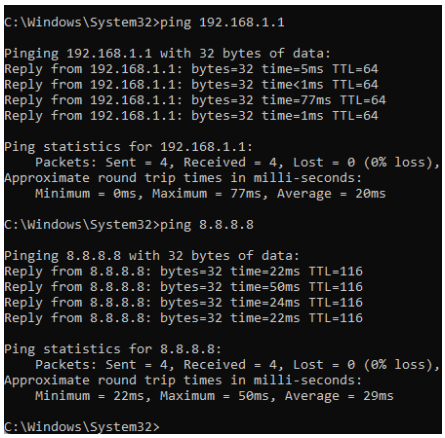
 DOI: https://doi.org/10.30743/infotekjar.v10i1.11939



Gambar 17. Kali linux berhasil memanggil alamat ip pada windows dengan perintah "ping -c 3 192.168.1.200" kali linux berhasil memanggil alamat ip internet dengan perintah "ping -c 3 8.8.8.8".



Gambar 18. Windows berhasil terhubung ke kali linux untuk menjadi target snifing kali linux dengan ping alamat ip kali linux dengan perintah "ping 192.168.1.3', Windows berhasil terhubung ke alamat ip yang dibuat pada windows yang akan dihubungkan ke debian dengan perintah "ping 192.168.1.200"



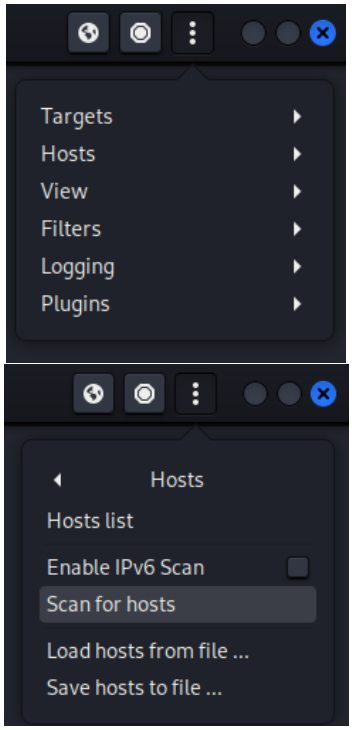
Gambar 19. Windows berhasil terhubung ke debian untuk menjadi korban snifing kali linux dengan ping pada debian dengan perintah "ping 192.168.1.1', Windows berhasil terhubung ke internet dengan perintah "ping 8.8.8.8".

Simulasi ARP Spoofing

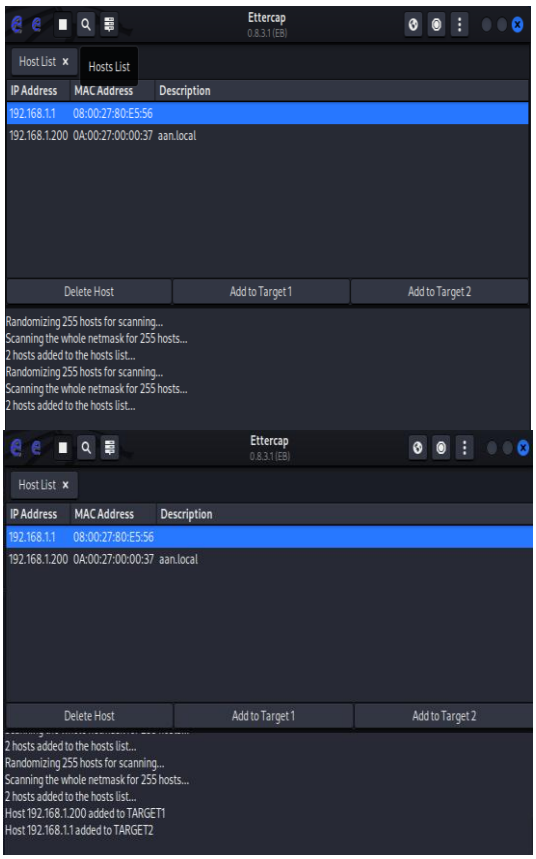
Tahapan ini mensimulasikan serangan *Man-in-the-Middle* dengan teknik ARP spoofing menggunakan Ettercap. Attacker melakukan manipulasi tabel ARP victim sehingga seluruh trafik jaringan dialihkan melalui attacker. Wireshark digunakan untuk memantau lalu lintas data korban, terutama untuk melihat paket HTTP yang bisa dibaca dan paket HTTPS yang tetap terenkripsi. Hasil simulasi menunjukkan kerentanan nyata jaringan Wi-Fi publik terhadap serangan ini. Simulasi dilakukan dalam bentuk tahapan praktis yang didokumentasikan dengan 9 tangkapan layar dari "Gambar 20" Sampai pada "Gambar 28".



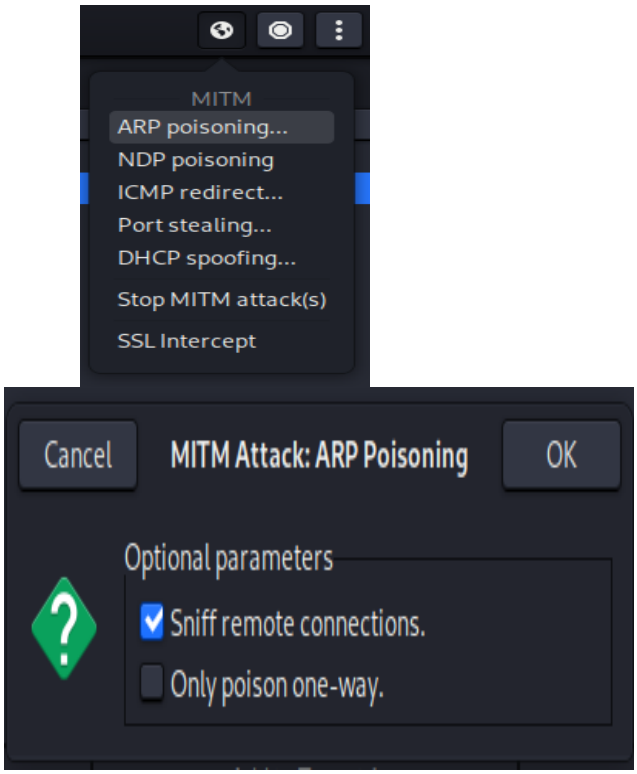
Gambar 20. Jalankan ettercap pada terminal baru di kali linux dengan perintah "sudo ettercap -G" untuk membuka ettercap, dan tekan tanda centang pada sudut kanan ettercap untuk memulai melakukan penyerangan snifing.



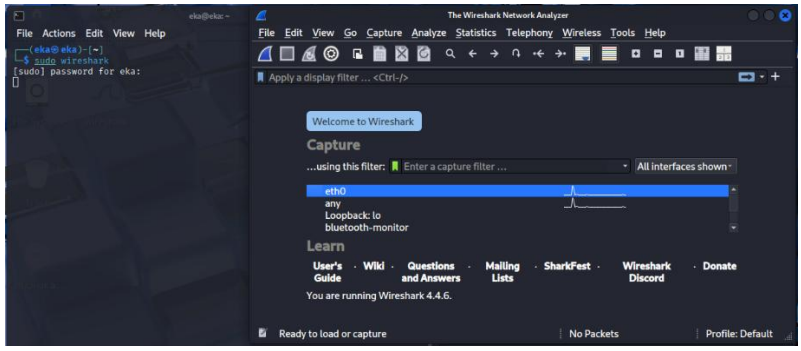
Gambar 21. Tekan titik 3 pada ettercap dan klik pilihan host,dan klik pilihan scan for hosts untuk memeriksa alamat ip yang terkena snifing pada ettercap.



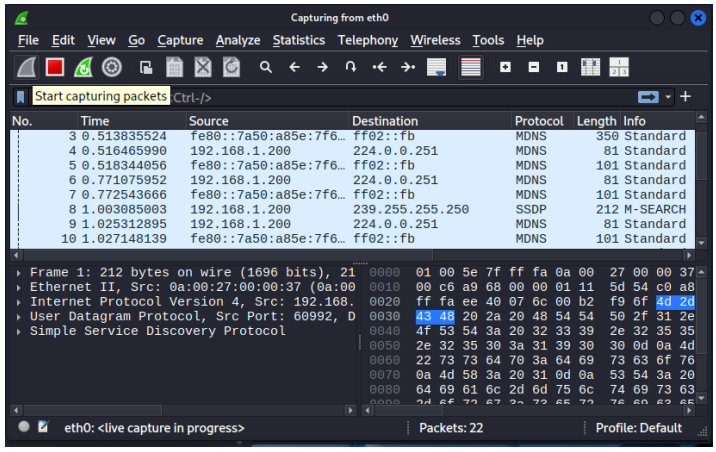
Gambar 22. Klik ikon pada sudut kiri atas di ettercap di lambang garis 3 gambar host list untuk melihat alamat ip yang terkena snifing, lalu tambahkan target 1 tekan pada alamat ip windows 192.168.200 jika sudah biru tekan add to target 1, untuk menjalankan ARP Spoofing dan juga lakukan hal yang sama pada alamat ip debian 192.168.1.1 add to target 2.



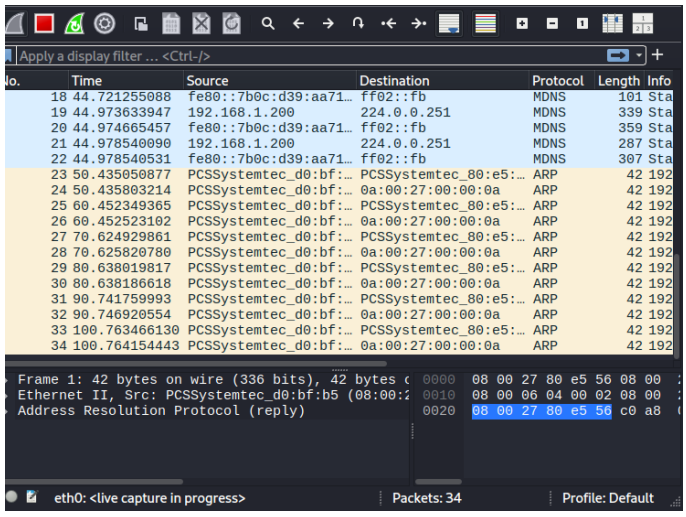
Gambar 23. Klik icon lambang bumi bulat untuk memulai serangan ARP poisoning, lalu centang pada pilihan sniff remote connection, dan klik ok.



Gambar 24. Selanjurnya buka wireshark dengan perintah "sudo wireshark" dan masukan pasword root untuk menjalankan wireshark, wireshark siap untuk dijalankan untuk menganalisis dan menampilkan data penyerangan, dan tekan icon sirip biru pojok kiri atas untuk memulai menganalisis.

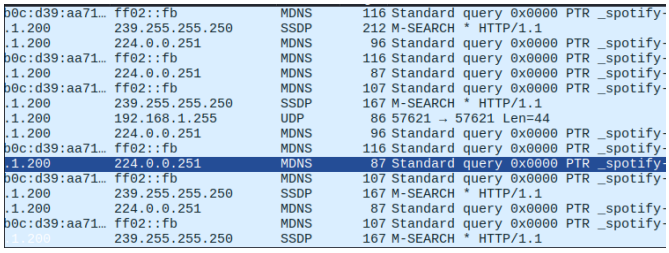


Gambar 25. Terlihat data dalam jaringan gateaway yang dipakai oleh windows, dan kegiatan yang dilakukan oleh windows dalam jaringan.

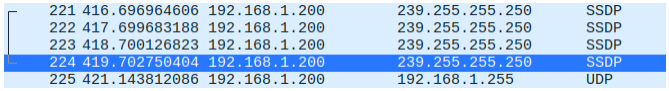


Gambar 26. Terlihat dalam wireshark serangan ARP spoofing berjalan dengan sukses, terlihat pada data protocol, dengan tulisan ARP.

DOI: https://doi.org/10.30743/infotekjar.v10i1.11939



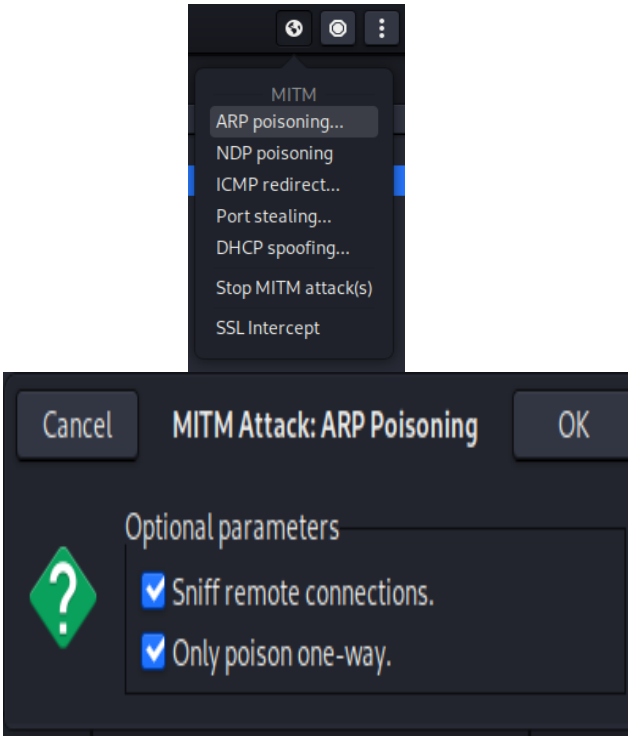
Gambar 27. Terlihat windows sedang mengakses spotify, dan juga mengakses situs web, terlihat pada data info bertulisan "PTR_spotify.connect" menandakan windows sedang membuka Spotify.



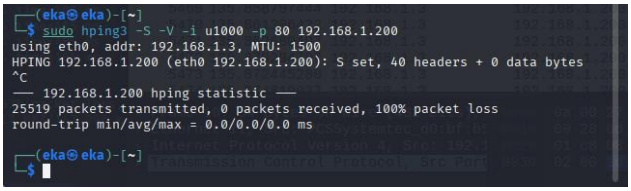
Gambar 28. Pada windows juga terlihat pada data info bertulisan "M-SEARCH * HTTP/1.1" menandakan bahwa windows sedang mengakses situs web, menandakan serangan arp spoofing berhasil dan dapat melihat data akses pada jaringan windows.

Simulasi Serangan DoS

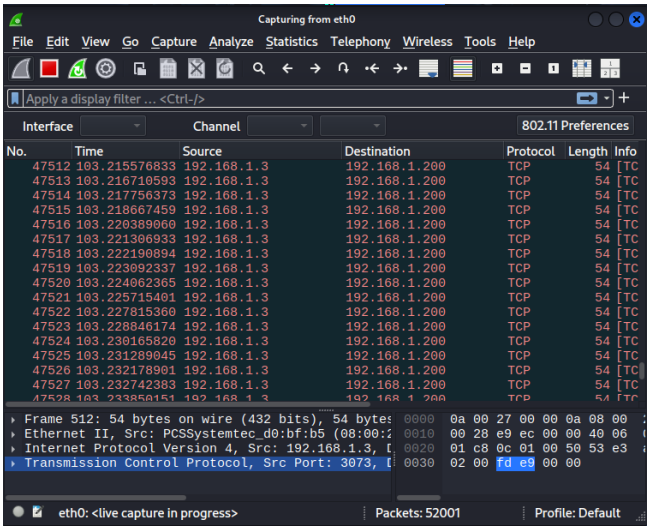
Setelah simulasi ARP spoofing, dilakukan pengujian serangan Denial of Service (DoS) menggunakan hping3. Serangan ini dilakukan dengan membanjiri target menggunakan paket TCP kecil secara berulang. Hasilnya ditampilkan melalui terminal attacker dan tangkapan Wireshark pada victim. Walaupun ribuan paket berhasil dikirim, jaringan victim tidak sepenuhnya lumpuh karena adanya proteksi bawaan router. Simulasi dilakukan dalam bentuk tahapan praktis yang didokumentasikan dengan 9 tangkapan layar dari "Gambar 29" Sampai pada "Gambar 31".



Gambar 29. Untuk memulai serangan DoS matikan dulu snifing dan nyalakan lagi, Klik icon bulat putih pada pojok kanan dan hentikan snifing lalu ok, lalu mulai lagi snifing dan tekan lambang bumi bulat untuk menjalankan snifing, lalu Jika ingin menjalankan Serangan DoS matikan centang sniff remote connections dan centang yang only poison one-way untuk menyerang ip gateaway.



Gambar 30. Salankan perintah "sudo hpinh3 -S -V -i u1000 80 192.168.1.200" untuk menjalankan perintah penyerangan DoS, agar mengirimkan satu paket setiap 1000 mikrodetik, jika ingin menghentikan jalankan perintah"crtl+c".



Gambar 31. Terlihat pada wireshark penyerangan DoS sudah berhasil dan mengirimkan paket tcp kecil sebanyak 5201.

Analisis Hasil Simulasi

Berdasarkan hasil pengujian, ARP spoofing terbukti lebih berbahaya karena dapat menyadap dan melihat komunikasi korban. Sementara itu, serangan DoS dalam skala simulasi virtual tidak efektif menurunkan kualitas jaringan secara signifikan. Dengan demikian, fokus mitigasi pada jaringan publik sebaiknya diarahkan pada pencegahan Man-in-the-Middle melalui enkripsi, VPN, dan firewall rule yang ketat.

KESIMPULAN

Penelitian ini berhasil mensimulasikan dua jenis serangan jaringan pada lingkungan virtualisasi menggunakan VirtualBox, yaitu serangan Man-in-the-Middle (ARP spoofing) dan Denial of Service (DoS). Hasil pengujian menunjukkan bahwa ARP spoofing mampu menunjukan tabel ARP pada victim dan mengalihkan lalu lintas jaringan melalui attacker. Dari proses ini, data yang tidak terenkripsi seperti HTTP dapat dengan mudah dilihat, sementara komunikasi berbasis HTTPS tetap terlindungi oleh mekanisme enkripsi. Serangan DoS dengan hping3 menunjukkan peningkatan trafik yang signifikan dengan total ribuan paket terkirim,

namun dampaknya tidak menyebabkan gangguan besar pada koneksi victim karena keterbatasan lingkungan virtual dan proteksi bawaan router modern.

Dari hasil tersebut dapat disimpulkan bahwa kerentanan terbesar pada jaringan Wi-Fi publik bukan berasal dari serangan flooding seperti DoS, melainkan dari serangan Man-in-the-Middle yang mampu menyadap informasi sensitif pengguna. Oleh karena itu, diperlukan penerapan langkah-langkah mitigasi seperti penggunaan VPN, enkripsi end-to-end, serta pengaturan firewall yang ketat untuk mengurangi risiko penyadapan data. Selain itu, penelitian lanjutan dapat difokuskan pada pengujian serangan dalam lingkungan non-virtual agar hasilnya lebih mendekati kondisi nyata, serta pada pengembangan sistem deteksi dini serangan ARP spoofing di jaringan publik.

REFERENSI

[1] Ilham Firdaus, Januar Al Amien, and S. Soni, "String Matching untuk Mendeteksi Serangan Sniffing (ARP Spoofing) pada IDS Snort," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 44–49, 2020, doi: 10.37859/coscitech.v1i2.2180.

[2] A. Arini, M. Luthfi Arsalan, and H. Teja Sukmana, "Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co)," *Cyber Secur. dan Forensik Digit.*, vol. 6, no. 2, pp. 30–38, 2024, doi: 10.14421/csecurity.2023.6.2.4075.

[3] D. Auliafitri, E. RizkiSuro, M. R. M. Malik, and A. Setiawan, "Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 12, 2024, doi: 10.47134/pjise.v1i3.2620.

[4] H. Setiawan, L. E. Erlangga, S. Siddiq, and Y. A. Gunawan, "Analisis Kerawanan Pada Aplikasi Website Menggunakan Standar OWASP Top 10 Untuk Penilaian Risk Rating," *Info Kripto*, vol. 17, no. 1, pp. 15–21, 2023, doi: 10.56706/ik.v17i1.64.

[5] T. M. Diansyah, I. Faisal, and D. Siregar, "Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack," *Kesatria J. Penerapan Sist. Inf. (Komputer dan Manajemen)*, vol. 4, no. 1, pp. 224–233, 2023, [Online]. Available: http://tunasbangsa.ac.id/pkm/index.php/kesatria/article/view/134

[6] F. Setiawan, J. Informatika, F. T. Industri, and U. I. Indonesia, "Jurnal Sains , Nalar , dan Aplikasi Teknologi Informasi Effectiveness Analysis of Gamification Based on Google TV," vol. 4, no. 2, pp. 200–206, 2025, doi: 10.20885/snati.v4.i2.40823.

[7] D. Phqlpexondq, N. Edjl, and P. Ri, "Network Development Life Cycle," vol. 2, 2015.

[8] D. P. K. Veny Charnita Br Ginting1, Mahendra Data2, "Deteksi Serangan ARP Spoofing berdasarkan Analisis Lalu Lintas Paket Protokol ARP," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 5, pp. 5049–5057, 2019, [Online]. Available: e-issn: 2548-964X http://j-ptiik.ub.ac.id

[9] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 115–123, 2020, doi: 10.37034/jsisfotek.v2i4.32.

[10] TAMSIR ARIYADI, I. Irwansyah, and M. S. Huda Mubarok, "Analisis Keamanan Jaringan Wifi Mahasiswa Ubd Dari Serangan Packet Sniffing," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 53–58, 2024, doi: 10.33884/jif.v12i01.8739.

[11] T. Safitrah, A. B. G. Sinaga, M. Alghifari, and S. N. Neyman, "Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2663.

[12] W. Haniyah, M. C. Hidayat, Z. F. I. Putra, V. A. Pertama, and A. Setiawan, "Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux," *J. Internet Softw. Eng.*, vol. 1, no. 2, p. 8, 2024, doi: 10.47134/pjise.v1i2.2654.

[13] Della Yunika Zebua, Carolina Sayangi Cahaya Waruwu, Kesadaran Zebua, Mardin Zai, Agusdamai Lase, and O. L. Ofel, "Simulasi Serangan DOS Menggunakan SLOWHTTPTEST," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 2, pp. 409–419, 2025, doi: 10.62712/juktisi.v4i2.402.

[14] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 12, 2024, doi: 10.47134/pjise.v1i4.2681.

[15] H. Alfidzar and B. P. Zen, "Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif Guna Untuk Mendeteksi Serangan DDOS Pada Server," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 4, no. 2, pp. 32–45, 2022, doi: 10.20895/inista.v4i2.534.

[16] F. jagi. . Jagi, "Simulasi Uji Keamanan Jaringan Windows 7 Pemblokiran Akses Situs Dengan Metode Protokol Layer 7 Berbasis Mikrotik Di Virtualbox," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 3, pp. 313–320, 2025, doi: 10.23960/jitet.v13i3.6811.

DOI: https://doi.org/10.30743/infotekjar.v10i1.11939

[17] R. H. W. Murti, I. Riadi, N. Anwar, and T. Ismail, "Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode Network Forensic Development Life Cycle," *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 11, no. 3, p. 107, 2023, doi: 10.12928/jstie.v11i3.26544.

[18] R. Rahman, A. Y. N. Leksona, and Afiqah, "Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra)," *Jejak Digit. J. Ilm. Multidisplin*, vol. 1, no. 4b, pp. 2145–2156, 2025, [Online]. Available: https://doi.org/10.63822/np7skj98