ANALISIS SERANGAN ARP-SPOOFING DAN HTTPS-SPOOFING PADA JARINGAN WIFI PUBLIK

TUGAS AKHIR

Disusun oleh:

HANNAH IFAH

NIM. 20106050037

PROGRAM STUDI TENIK INFORMATIKA

FAKULTAS SAINS DAN TEKNLOGI

UNIVERSITAS ISLAM NEGRI SUNAN KALIJAGA

YOGYAKARTA

2024

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1493/Un.02/DST/PP.00.9/08/2024

Tugas Akhir dengan judul : Analisis serangan arp spoofing dan https spoofing pada jaringan wifi publik

yang dipersiapkan dan disusun oleh:

Nama : HANNAH IFAH
Nomor Induk Mahasiswa : 20106050037
Telah diujikan pada : Kamis, 08 Agustus 2024
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 66c331c3b8b9e

Penguji I

Dr. Agus Mulyanto, S.Si., M.Kom., ASEAN Eng.
SIGNED

Valid ID: 66c2ce302f526

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 66c1edce5a659

Yogyakarta, 08 Agustus 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 66c474d6942c2

LEMBAR PERNYATAAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Hannah Ifah
NIM	: 20106050037
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 30 Juli 2024

Hannah Ifah
NIM 20106050037

SURAT PERSETUJUAN SKRIPSI

Universitas Islam Negeri Sunan Kalijaga

SURAT PERSETUJUAN TUGAS AKHIR

Hal : Persetujuan Tugas Akhir
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
di-
Yogyakarta

Assalamualaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa tugas tesis Saudara :
Nama : Hannah Ifah
NIM 20106050037
Judul Skripsi : Analisis Serangan Arp Spoofing dan Https Spoofing pada Jaringan Wi-Fi Public

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Program Studi Magister Informatika UIN Sunan Kalijaga untuk diajukan dalam rangka memperoleh gelar Magister Informatika.

Wassalamualaikum wr. wb.

Yogyakarta, 13 Mei 2024

Pembimbing

Dr. Ir. Bambang Sugiantoro, S.SI., M.T., IPM.
NIP: 19751024 200912 1 002

MOTTO

"Ketika aku melibatkan Allah dalam semua rencana dan impianku, dengan penuh keikhlasan dan keyakinan, aku percaya tidak ada yang tidak mungkin untuk diraih"

HALAMAN PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat dirampungkan dengan baik dan tepat pada waktunya. Oleh karena itu, dengan rasa bangga dan bahagia saya ucapkan rasa syukur dan terimakasih saya kepada:

Allah SWT karena hanya atas izin dan karuniaNyalah maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan penguasa alam yang meridhoi dan mengabulkan segala doa.

Kedua orang tua saya tercinta ayah dan ibu yang selalu melangitkan do'a - do'a baik dan menjadikan motivasi untuk saya dalam menyelesaikan skripsi ini, terimakasih sudah mengantarkan saya sampai di tempat ini, saya persembahkan karya tulis sederhana ini dan gelar untuk ayah dan ibu.

Kakak tersayang, terimakasih sudah ikut serta dalam proses penulis menempuh pendidikan selama ini, serta atas semangat dan do'a yang diberikan kepada penulis.

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublishkan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillahirabbil'alamin, segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga skripsi dengan judul "Tingkat Keamanan Jaringan Home Wi-Fi di Kota Yogyakarta terhadap Password Attack" ini bisa diselesaikan tepat waktu. Skripsi ini hadir sebagai tugas akhir perkuliahan serta persyaratan untuk memperoleh gelar Sarjana Strata 1 Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.

Melalui penelitian ini, penulis berharap kontribusi ilmiah yang dilakukan dapat memberikan manfaat bagi perkembangan ilmu pengetahuan dan praktik khususnya dalam bidang informatika/teknologi. Skripsi ini juga bisa selesai atas bimbingan, arahan, masukan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Bapak Prof. Dr. Phil. Al Makin, S.Ag., MA., selaku Rektor Universitas Islam Negri Sunan Kalijaga Yogyakarta.
2. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
3. Ibu Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Ketua Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
4. Bapak Mandahadi Kusuma, M.Eng. selaku Dosen Pembimbing Akademik yang telah membarengi serta memberikan informasi selama perkuliahan.
5. Bapak Dr. Ir. Bambang Sugiantoro, S.SI., M.T., IPM. selaku Dosen Pembimbing Skripsi yang telah meluangkan waktunya untuk mengarahkan dan mengevalusi selama proses skripsi.

6. Teristimewa kedua orang tua saya Bapak dan Ibuk, gelar sarjana ini saya persembahkan untuk kedua orang tua saya tercinta, yang selalu memberikan dukungan berupa moril maupun material yang tak terhingga serta do'a yang tidak ada putusnya yang diberikan kepada saya sehingga saya mampu menyelesaikan studi sarjana hingga selesai.
7. Seluruh keluarga tercinta kakak, keponakan **:** Terimakasih telah banyak memberikan banyak dukungan, do'a dan bantuan serta hiburan hingga saya bisa menyelesaikan skripsi ini.
8. Teruntuk diri saya sendiri, terimakasih kepada diri saya sendiri Hannah Ifah yang sudah kuat melewati segala lika liku yang terjadi, saya bangga pada diri saya sendiri. Mari bekerjasama untuk lebih berkembang lagi menjadi pribadi yang lebih baik.
9. Dan teruntuk kamu yang tak kalah penting kehadirannya. Terimakasih selalu menemani dan selalu menjadi support system penulis pada hari yang tidak mudah selama proses pengerjaan skripsi, terimakasih telah mendengarkan keluh kesah, memberikan dukungan, semangat, tenaga, pikiran dan senantiasa sabar menghadapi saya.

Yogyakarta, 30 Juli 2024

Penulis

Hannah Ifah

20106050055

DAFTAR ISI

HALAMAN PENGESAHAN i
LEMBAR PERNYATAAN ii
SURAT PERSETUJUAN SKRIPSI iii
MOTTO iv
HALAMAN PERSEMBAHAN v
LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR vi
KATA PENGANTAR vii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
INTISARI xiv
ABSTRACT xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
BAB II KAJIAN PUSTAKA 5
2.1 Tinjauan Pustaka 5

2.2 Landasan Teori 9
2.2.1 Privasi 9
2.2.2 MITM 10
2.2.3 Arp Spoofing 10
2.2.4 Https 11
2.2.5 Wireshark 11
2.2.6 Burp Suite 12
2.2.7 SSL 12
2.2.8 Etercap/Bettercap 13
2.2.9 ARP 13
2.2.10 Social Enggenering 14
BAB III METODE PENGEMBANGAN SISTEM 16
3.1 Alat dan Bahan Penelitian 16
3.1.1 Alat 16
3.1.2 Bahan 16
3.1.3 Bahan Penelitian 17
3.2 Metode Penelitian 17
BAB IV PERANCANGAN DAN EVALUASI SISTEM 22
4.1 Penetration Testing 22
4.1.1 ARP Spoofing 22
4.1.2 Https Spoofing 32
4.2 Analisis Data dan Pembahasan 38
4.2.1 Identifikasi Target 40

4.2.2 Penggunaan Burp Suite 40
4.2.3 Social Engineering 41
4.2.4 Analisis Sumber IP dan Port 41
4.2.5 Keberhasilan dan Kegagalan 41
4.2.6 Mitigasi 42
BAB V PENUTUP 44
5.1 Kesimpulan 44
5.2 Saran 45
DAFTAR PUSTAKA 46
CURRICULUM VITAE 49
LAMPIRAN 48

DAFTAR GAMBAR

Gambar 3. 1 Topologi Jaringan Wifi Publik 19
Gambar 3. 2 Topologi Arp Spoofing 20
Gambar 3. 3 Diagram Https Spoofing..... 20
Gambar 4. 1 Ping Target 23
Gambar 4. 2 Analisis Paket 23
Gambar 4. 3 Web Target 24
Gambar 4. 4 Capture Data..... 25
Gambar 4. 5 Bettercap..... 26
Gambar 4. 6 Penentuan Target 27
Gambar 4. 7 Proses Pemindaian 28
Gambar 4. 8 Capture Data..... 28
Gambar 4. 9 konfigurasi ettercap 28
Gambar 4. 10 Host List 30
Gambar 4. 11 Pemilihan Target 31
Gambar 4. 12 Capture Data..... 32
Gambar 4. 13 Capture Data Daring UIN SuKa..... 35
Gambar 4. 14 capture data si unu jogja..... 37
Gambar 4. 15 capture data daring uin suka.....**Error! Bookmark not defined.**
Gambar 4. 16 capture data kampus merdeka .....**Error! Bookmark not defined.**
Gambar 4. 17 capture data spotify .....**Error! Bookmark not defined.**

DAFTAR TABEL

Table 2. 1 Tinjauan Pustaka 8
Tabel 3. 1 Tahapan Penelitian 18
Tabel 4. 1 Hasil Capture Data 39
Tabel 4. 2 Sumber Capture 39

DAFTAR LAMPIRAN

Lampiran 1 Data Analisis Password

Lampiran 2 gambar hasil serangan

INTISARI

Penelitian ini mengeksplorasi risiko keamanan yang terkait dengan penggunaan jaringan Wi-Fi publik, terutama dalam menghadapi serangan ARP-Spoofing dan HTTPS-Spoofing. Serangan-serangan ini memungkinkan penyerang untuk mengintersepsi dan memanipulasi data sensitif yang ditransmisikan melalui jaringan. Dalam penelitian ini, permasalahan utama yang diangkat adalah bagaimana serangan ini dapat dieksploitasi di lingkungan Wi-Fi publik dan seberapa besar dampaknya terhadap keamanan data pengguna.

Metode yang digunakan dalam penelitian ini melibatkan eksperimen dengan alat-alat seperti Wireshark, Ettercap/Bettercap, dan Burp Suite. Alat-alat ini digunakan untuk menganalisis lalu lintas jaringan, mengidentifikasi kerentanan, dan menguji efektivitas serangan. Pendekatan eksperimental ini memungkinkan peneliti untuk secara langsung mengamati bagaimana ARP-Spoofing dapat mengalihkan lalu lintas jaringan dan bagaimana HTTPS-Spoofing dapat digunakan untuk memanipulasi sesi komunikasi yang seharusnya aman.

Hasil penelitian menunjukkan bahwa serangan ARP-Spoofing efektif dalam mengalihkan lalu lintas jaringan, sementara serangan HTTPS-Spoofing dapat dengan sukses memanipulasi komunikasi yang dienkripsi. Temuan ini mengungkapkan potensi risiko keamanan yang signifikan bagi pengguna jaringan Wi-Fi publik, menekankan perlunya tindakan preventif untuk melindungi data sensitif dari ancaman semacam ini.

Kata kunci : MITM, ARP-Spoofing, dan HTTPS-Spoofing, Wi-Fi

ABSTRACT

This study explores the security risks associated with using public Wi-Fi networks, particularly in the face of ARP-Spoofing and HTTPS-Spoofing attacks. These attacks allow malicious actors to intercept and manipulate sensitive data transmitted over the network. The primary issue addressed in this research is how these attacks can be exploited in a public Wi-Fi environment and the extent of their impact on user data security.

The methods used in this research involved experimental procedures with tools such as Wireshark, Ettercap/Bettercap, and Burp Suite. These tools were utilized to analyze network traffic, identify vulnerabilities, and test the effectiveness of the attacks. This experimental approach enabled the researchers to directly observe how ARP-Spoofing can redirect network traffic and how HTTPS-Spoofing can be used to manipulate communication sessions that are supposed to be secure.

The findings of this research demonstrate that ARP-Spoofing is effective in redirecting network traffic, while HTTPS-Spoofing can successfully manipulate encrypted communications. These results reveal significant security risks for public Wi-Fi users, emphasizing the need for preventive measures to protect sensitive data from such threats.

Keywords : MITM, ARP-Spoofing, and HTTPS-Spoofing, Wi-Fi

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju dan tak terelakkan saat ini, akses terhadap internet telah berkembang menjadi sebuah kebutuhan yang sangat mendasar dan esensial bagi kehidupan masyarakat modern, serta data yang di didapat dari hasi crawling data sesuai dengan perhitungan yang telah dilakukan pengguna internet sebanyak 143,26 juta orang pada periode 2016-2017, Jumlah tersebut meningkat 54,7%.[1] Metode akses internet yang populer dan mudah dimanfaatkan oleh masyarakat luas adalah melalui jaringan Wi-Fi publik yang kini dapat ditemukan hampir di mana-mana, mulai dari kafe-kafe yang nyaman, bandara-bandara internasional, hotel-hotel mewah, pusat-pusat perbelanjaan yang ramai, hingga berbagai lokasi publik lainnya yang menjadi titik kumpul masyarakat. Kemudahan akses yang ditawarkan oleh jaringan Wi-Fi publik ini memang memberikan berbagai kemudahan dalam berkomunikasi dan mengakses informasi. Namun, di sisi lain, keberadaan jaringan Wi-Fi publik ini juga sering kali diiringi oleh berbagai kerentanan yang dapat dimanfaatkan oleh individu-individu dengan niat jahat untuk melancarkan serangan-serangan siber.

Salah satu jenis serangan siber yang cukup sering terjadi dan memiliki potensi kerusakan yang signifikan terhadap korban adalah serangan yang dikenal dengan istilah "Man-in-the-Middle" (MitM). Dalam tipe serangan ini, seorang penyerang berhasil dengan cekatan menempatkan dirinya secara strategis di antara korban—yakni pengguna jaringan—dan sumber komunikasi yang seharusnya aman.[2] Posisi ini memberikan penyeran

kemampuan yang sangat berbahaya untuk mengintersep, mengubah, atau bahkan mengalihkan data yang dikirim dan diterima oleh korban tanpa sepengetahuan dan persetujuan dari kedua belah pihak yang terlibat dalam komunikasi. Dengan demikian, penyerang dapat dengan mudah mencuri informasi yang sangat sensitif dan pribadi, seperti kata sandi, rincian kartu kredit, dan berbagai jenis data lainnya yang seharusnya dilindungi.

Kurangnya kesadaran dari sebagian besar pengguna jaringan Wi-Fi publik terhadap potensi bahaya serangan ini, ditambah lagi dengan kurangnya implementasi lapisan-lapisan keamanan yang memadai oleh pihak-pihak penyedia layanan, menjadikan serangan MitM semakin merajalela dan menjadi ancaman nyata dalam penggunaan jaringan Wi-Fi publik. Mengingat pertumbuhan penggunaan internet dan jaringan Wi-Fi publik yang terus meningkat secara eksponensial, menjadi sangat penting bagi kita untuk memiliki pemahaman yang luas dan mendalam tentang mekanisme kerja serangan MitM serta memahami strategi-strategi efektif untuk melindungi diri dari berbagai ancaman yang mungkin timbul akibat serangan tersebut.

Dalam konteks serangan MitM, perhatian khusus memang seharusnya diberikan kepada dua bentuk serangan yang paling umum dan mencolok, yakni Arp Spoofing dan Https Spoofing. Arp Spoofing berpotensi besar dalam memanipulasi dan mengambil alih data kita di dunia maya dengan cara yang sangat halus namun destruktif, sementara Https Spoofing memiliki kemampuan untuk merekam dan mengawasi setiap aktivitas yang kita lakukan di internet tanpa sepengetahuan kita. Realitas yang mengkhawatirkan ini harus dijadikan sebagai peringatan serius bagi kita semua bahwa beberapa lokasi publik dengan akses Wi-Fi mungkin sangat rawan terhadap potensi serangan MitM. Ketidawaspadaan dan kurangnya pengetahuan mengenai tindakan pencegahan yang efektif dalam situasi tertentu dapat berakibat sangat fatal terhadap privasi dan keamanan pribadi kita.

Maka dari itu, penelitian ini bertujuan untuk tidak hanya melakukan analisis yang mendalam dan komprehensif terhadap fenomena serangan MITM dalam konteks jaringan Wi-Fi publik, namun juga untuk mengidentifikasi dan menjadi edukasi yang dapat diadopsi oleh pengguna untuk melindungi diri mereka dari serangan-serangan siber yang berbahaya ini. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya meningkatkan kesadaran dan keamanan siber di tengah masyarakat luas, khususnya dalam penggunaan jaringan Wi-Fi publik yang semakin tidak terelakkan dalam kehidupan sehari-hari kita.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Rendahnya keamanan Wi-Fi public di *Cafe*
2. Bagaimana melakukan analisis dan identifikasi serangan Arp dan Https spoofing pada jaringan Wi-Fi public?

1.3 Batasan Masalah

1. Lingkup Jaringan: Penelitian ini hanya fokus pada jaringan Wi-Fi publik seperti hotspot di kafe. Jaringan Wi-Fi pribadi atau korporat tidak termasuk dalam analisis ini.
2. Jenis Serangan: Walaupun ada berbagai jenis serangan yang dapat dilancarkan pada jaringan Wi-Fi, penelitian ini hanya membatasi pada serangan Man-in-the-Middle (Arp dan Https spoofing). Serangan lain seperti Evil Twin atau serangan WPA2 cracking tidak termasuk.
3. Alat dan Teknologi: Penelitian akan membatasi alat dan teknologi yang digunakan untuk menganalisis serangan. Ini mungkin terbatas pada alat yang paling umum digunakan dalam serangan MitM atau yang paling relevan untuk jaringan Wi-Fi publik.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan, maka diperoleh tujuan untuk menyelesaikan masalah tersebut :

1. Menganalisis rendahnya keamanan Wi-Fi public di *Cafe*
2. Menganalisis dan Mengidentifikasi serangan MITM (Arp dan Https spoofing) yang dapat terjadi di jaringan Wi-Fi public.

1.5 Manfaat Penelitian

1. Meningkatkan kesadaran masyarakat tentang risiko menggunakan WiFi publik tanpa pengamanan yang memadai, terutama di tempat-tempat umum seperti kafe. Dengan pemahaman ini, pengguna dapat lebih waspada dan mengambil langkah-langkah pencegahan untuk melindungi data pribadi mereka.
2. Memberikan panduan praktis yang dapat membantu organisasi atau penyedia layanan WiFi publik untuk melindungi pengguna dari potensi serangan MITM.
3. Hasil penelitian dapat menjadi dasar untuk penelitian lebih lanjut dalam mengembangkan teknik deteksi dan pencegahan yang lebih efektif terhadap serangan MITM, khususnya dalam lingkungan WiFi publik.
4. Menginspirasi penelitian lanjutan yang mungkin mengeksplorasi kolaborasi antara teknik-teknik serangan siber dengan pendekatan social engineering, serta pengembangan strategi keamanan yang lebih komprehensif untuk melindungi pengguna di jaringan publik.

BAB V
PENUTUP

5.1 Kesimpulan

Dari rumusan masalah yang ada, kenapa wi-fi public café tidak aman, karena berdasarkan hasil pentesting kita bisa melihat bagaimana rentanya keamanan wi-fi café terhadap serangan ARP jika kita tidak sadar kalau kita sembarangan mengakses protocol http. Selain itu Penelitian ini berhasil melakukan analisis dan identifikasi serangan ARP Spoofing dan HTTPS Spoofing dalam jaringan Wi-Fi publik. Melalui eksperimen langsung dan observasi, terbukti bahwa:

- ARP Spoofing efektif dalam mengubah tabel ARP target untuk mengalihkan lalu lintas jaringan, sehingga memungkinkan penyerang untuk mengintersepsi, memodifikasi, atau mengalihkan data.
- HTTPS Spoofing juga berhasil dilakukan melalui manipulasi sertifikat keamanan, memungkinkan penyerang untuk memata-matai dan mencuri informasi sensitif yang ditransmisikan melalui HTTPS.

Ditemukan bahwa meskipun protokol keamanan seperti HTTPS dirancang untuk melindungi data, masih ada celah yang bisa dimanfaatkan oleh penyerang. Hal ini menegaskan pentingnya edukasi kepada pengguna tentang keamanan jaringan dan verifikasi keaslian situs web dalam lingkungan publik.

Penelitian ini menyarankan perlunya solusi keamanan yang lebih kuat dan adaptif, terutama dalam mengamankan jaringan Wi-Fi publik yang rentan terhadap serangan Man-in-the-Middle. Ini termasuk pengembangan dan implementasi algoritma deteksi serangan yang lebih canggih serta strategi pencegahan yang proaktif untuk melindungi pengguna dan data mereka.

5.2 Saran

Mengingat keterbatasan yang dihadapi, penelitian masa depan harus mengadopsi pendekatan yang lebih luas dengan menguji berbagai jenis jaringan Wi-Fi publik di berbagai lokasi untuk mengumpulkan data yang lebih representatif. Penelitian masa depan juga bisa mengeksplorasi penggunaan algoritma pembelajaran mesin untuk mendeteksi pola serangan secara otomatis, yang bisa meningkatkan respons keamanan terhadap serangan MitM. Selain itu, ada kebutuhan untuk mengembangkan dan menguji solusi keamanan baru yang dapat diintegrasikan dengan teknologi jaringan saat ini untuk mengurangi kerentanan terhadap serangan ARP Spoofing dan HTTPS Spoofing.

Dengan memperluas basis pengetahuan tentang taktik dan strategi penyerang, serta mengembangkan teknologi yang dapat secara proaktif mengidentifikasi dan merespons ancaman keamanan, komunitas penelitian dan industri dapat bekerja sama untuk menciptakan lingkungan jaringan yang lebih aman untuk semua pengguna.

DAFTAR PUSTAKA

[1] 'jurnal lontar vol.7 no.1 januari-juni 2019'.

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

[3] S. M. Morsy and D. Nashat, 'D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing', *IEEE Access*, vol. 10, pp. 49142–49153, 2022, doi: 10.1109/ACCESS.2022.3172329.

[4] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, 'Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks', *IJEMR*, vol. 10, no. 3, pp. 153–158, Jun. 2020, doi: 10.31033/ijemr.10.3.23.

[5] L. D. Samsumar and K. Gunawan, 'ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (WIRELESS LAN); STUDI KASUS DI KAMPUS STMIK MATARAM', *jitter*, vol. 4, no. 1, Dec. 2017, doi: 10.33197/jitter.vol4.iss1.2017.152.

[6] M. Noviansyah and H. Saiyar, 'PEMANFAATAN WEB PROXY SEBAGAI PENGOPTIMAL KEAMANAN JARINGAN WIRELESS LAN', *JKI*, vol. 8, no. 1, Jun. 2020, doi: 10.31294/jki.v8i1.8356.

[7] A. R. Fauzi, 'MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS', vol. 8, 2018.

[8] B. Pingle, A. Mairaj, and A. Y. Javaid, 'Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use', in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, Rochester, MI: IEEE, May 2018, pp. 0192–0197. doi: 10.1109/EIT.2018.8500082.

[9] B. Bhushan, G. Sahoo, and A. K. Rai, 'Man-in-the-middle attack in wireless and computer networking — A review', in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, Dehradun: IEEE, Sep. 2017, pp. 1–6. doi: 10.1109/ICACCAF.2017.8344724.

[10] A. Kumar Baitha and Prof. Smitha Vinod, 'Session Hijacking and Prevention Technique', *IJET*, vol. 7, no. 2.6, p. 193, Mar. 2018, doi: 10.14419/ijet.v7i2.6.10566.

[11] R. Komala, 'Literasi Digital Untuk Perlindungan Data Privasi: Di Balik Kemudahan Belanja Daring', *JISIP (Jurnal Ilmu Sosial dan Pendidikan)*, vol. 6, no. 4, 2022, [Online]. Available: https://ejournal.mandalanursa.org/index.php/JISIP/article/view/3527/2938

[12] S. Gangan, 'A review of man-in-the-middle attacks', *arXiv preprint arXiv:1504.02115*, 2015, [Online]. Available: https://arxiv.org/pdf/1504.02115.pdf

[13] A. Aman, 'Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ', *digitech*, vol. 3, no. 2, pp. 824–831, Dec. 2023, doi: 10.47709/digitech.v3i2.3378.

[14] Y. Hae, 'ANALISIS KEAMANAN JARINGAN PADA WEB DARI SERANGAN SNIFFING DENGAN METODE EKSPERIMEN', *JATISI*, vol. 8, no. 4, pp. 2095–2105, Dec. 2021, doi: 10.35957/jatisi.v8i4.1196.

[15] D. Irawan, 'Analisis dan Penyadapan Transmisi Paket Data Jaringan Komputer Menggunakan Wireshark', *MIKROTIK: Jurnal Manajemen Informatika*, vol. 7, no. 1, 2017, [Online]. Available: https://ojs.ummetro.ac.id/index.php/mikrotik/article/view/552/398

[16] M. A. A. Hilmi and R. K. Yunan, 'Pengujian Keamanan Fitur Upload File pada Sistem Aplikasi Web', *JPIT*, vol. 7, no. 1, pp. 37–42, Jan. 2022, doi: 10.30591/jpit.v7i1.3336.

[17] A. Aziz Khozindani, Y. Muhyidin, and M. A. Sunandar, 'PERBANDINGAN KINERJA TOOLS WIRESHARK DAN BURPSUITE

UNTUK PENYERANGAN WEBSITE DENGAN METODE SNIFFING', *jati*, vol. 7, no. 3, pp. 2026–2031, Dec. 2023, doi: 10.36040/jati.v7i3.7013.

[18] H. E. Wahanani, 'Uji Coba Serangan Man In The Middle Pada Keamanan SSL Protokol HTTP', *Jurnal Sistem Informasi dan Bisnis Cerdas*, vol. 13, no. 1, pp. 21–26, Feb. 2020, doi: 10.33005/sibc.v13i1.1769.

[19] M. R. Choiruman, J. G. A. Ginting, and N. Iryani, 'Analisis Pendeteksian Serangan ARP Poisoning Dengan Menggunakan Metode LiveForensic', vol. 6, no. 2, 2022.

[20] D. Kurnia, 'PEMANFAATAN BETTERCAP SEBAGAI TEKNIK SNIFFING PADA PAKET TRAFIK JARINGAN WIFI', 2019.

[21] M. N. Hafizh, I. Riadi, and A. Fadlil, 'Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic', *InComTech*, vol. 10, no. 2, p. 111, Aug. 2020, doi: 10.22441/incomtech.v10i2.8757.

[22] H. Ahmadian and A. Sabri, 'TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA', *Com, Engine, Sys, Sci*, vol. 2, no. 1, pp. 13–20, Jul. 2021, doi: 10.46576/djtechno.v2i1.1251.

[23] E. W. Tyas Darmaningrat *et al.*, 'Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi', *SWGT*, vol. 6, no. 2, Feb. 2022, doi: 10.12962/j26139960.v6i2.92.