Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 1, No. 4b, Tahun 2025
doi.org/10.63822/np7skj98
Hal. 2145-2156

Serangan *Man-In-The-Middle* (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan *Password Cracking* Menggunakan Hydra

Rakhmadi Rahman[1], Abriel Yosua Nathanael Leksona[2], Afiqah[3]
Information System Department, Faculty of Science
Bacharuddin Jusuf Habibie Institute of Parepare, Parepare, South Sulawesi, Indonesia[1,2,3]

*Email Korespodensi: nathanaelleskona@gmail.com

Sejarah Artikel:

Diterima 03-07-2025
Disetujui 08-07-2025
Diterbitkan 10-07-2025

ABSTRACT

The rapid development of technology has encouraged various sectors in Indonesia to rely on Internet connectivity. However, along with this progress, public networks such as wi-fi are vulnerable to increasingly complex cybersecurity threats, especially Man-In-The-Middle (MITM) and Password Cracking attacks. This research aims to simulate MITM attacks with ARP Spoofing techniques using the Ettercap tool as well as Password Cracking attacks using Hydra in a controlled virtual environment, while proposing effective mitigation solutions. The experimental method was conducted by configuring two virtual machines, Kali Linux as the attacker and Ubuntu as the web server. Simulation results show that the MITM attack is able to intercept user credentials over HTTP connections in a short period of time, while the brute-force attack with Hydra manages to reveal passwords in less than a minute. The implementation of HTTPS with self-signed certificates as a mitigation measure proved to prevent data interception, although ARP spoofing remained active. This research is expected to provide insight into the vulnerabilities of public networks and practical solutions to strengthen the security of authentication systems.

Keywords: *Man-In-The-Middle (MITM), Password Cracking, Ettercap, ARP spoofing, Hydra, Brute-Force, Network Security.*

ABSTRAK

Perkembangan teknologi yang pesat telah mendorong berbagai sektor di Indonesia bergantung pada konektivitas Internet. Namun, seiring kemajuan ini, jaringan publik seperti wi-fi rentan menghadapi ancaman keamanan siber yang semakin kompleks, terutama serangan Man-In-The-Middle (MITM) dan Password Cracking. Penelitian ini bertujuan untuk mensimulasikan serangan MITM dengan teknik ARP Spoofing menggunakan tool Ettercap serta serangan Password Cracking menggunakan Hydra dalam lingkungan virtual terkontrol, sekaligus mengusulkan solusi mitigasi yang efektif. Metode eksperimen dilakukan dengan mengkonfigurasi dua mesin virtual, yaitu Kali Linux sebagai penyerang dan Ubuntu sebagai server web. Hasil simulasi menunjukkan bahwa serangan MITM mampu mengintersep kredensial pengguna melalui koneksi HTTP dalam waktu singkat, sementara serangan brute-force dengan Hydra berhasil mengungkap kata sandi dalam durasi kurang dari satu menit. Penerapan HTTPS dengan sertifikat self-signed sebagai langkah mitigasi terbukti mampu mencegah intersepsi data, meskipun ARP spoofing tetap aktif. Penelitian ini diharapkan mampu

memberikan wawasan tentang kerentanan jaringan publik dan solusi praktis untuk memperkuat keamanan sistem autentikasi.

Kata Kunci: Man-In-The-Middle (MITM), Password Cracking, Ettercap, ARP spoofing, Hydra, Brute-Force, Keamanan Jaringan.

Bagaimana Cara Sitasi Artikel ini:

Rakhmadi Rahman, Abriel Yosua Nathanael Leksona, & Afiqah. (2025). Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra. Jejak Digital: Jurnal Ilmiah Multidisiplin, 1(4b), 2145-2156. https://doi.org/10.63822/np7skj98

PENDAHULUAN

Perkembangan teknologi yang pesat saat ini telah mendorong digitalisasi pada berbagai sektor di Indonesia, seperti pemerintahan, pendidikan, layanan publik, hingga bisnis digital kini sangat bergantung pada konektivitas internet. Adanya jaringan *wireless* (nirkabel) membantu serta memudahkan interaksi antar masyarakat. Namun, seiring kemajuan ini, tantangan keamanan siber juga semakin kompleks, terutama pada jaringan publik seperti *wi-fi*, yang rentan terhadap berbagai jenis serangan siber. Salah satu dampak negatif dari layanan *wi-fi* ditempat umum ialah tingginya tingkat kerentanan keamanan data terhadap kasus *hacking*, hal inilah yang dicoba untuk dimanfaatkan oleh segelintir oknum untuk meraup keuntungan secara pribadi (Nugraha et al., 2022). Ancaman ini menuntut pemahaman mendalam tentang kerentanan sistem untuk merancang solusi keamanan yang efektif.

Salah satu ancaman utama dalam jaringan publik adalah serangan *Man-in-the-Middle* (MITM), di mana pelaku menyusup ke komunikasi antara dua pihak untuk mengintai, memodifikasi, atau mencuri data sensitif tanpa sepengetahuan korban. Teknik ARP *spoofing*, yang didukung oleh *tool open-source* seperti Ettercap, memungkinkan pelaku memposisikan diri sebagai perantara dalam lalu lintas jaringan. Teknik ini memungkinkan penyerang bisa mengendus *frames* data pada jaringan lokal dan bisa melakukan modifikasi *traffic* atau bahkan bisa menghentikannya (Saraun et al., 2021). Selain itu, serangan *Password Cracking* dengan metode brute-force, yang dilakukan menggunakan *tool* Hydra, juga menjadi ancaman signifikan karena memanfaatkan kelemahan sistem autentikasi untuk mengungkap kredensial pengguna, terutama pada layanan seperti HTTP, SSH, atau FTP.

Mengingat tingginya risiko yang ditimbulkan oleh serangan MITM dan *Password Cracking*, penelitian ini bertujuan untuk mensimulasikan serangan MITM menggunakan Ettercap dan menguji teknik *password cracking* dengan Hydra dalam lingkungan virtual yang terkontrol, sekaligus mengusulkan strategi mitigasi untuk meningkatkan keamanan.

LANDASAN TEORI

Kali Linux

Kali Linux merupakan sistem operasi *linux* berbasis *debian* yang dikembangkan oleh *offensive security* (Pangestu & Liza, 2022). Sistem operasi ini umumnya digunakan untuk melakukan penetrasi dan pengujian keamanan sistem.

Ubuntu

Ubuntu merupakan salah satu distro *linux* yang *open-source* dan gratis. Sistem operasi ini cukup populer digunakan karena kemudahannya saat dipasang dan digunakan. Salah satu keunggulan Ubuntu adalah pengguna dapat memodifikasi dan mengubah sistem operasi ini tanpa perlu membayar lisensi.

Man-In-The-Middle (MITM)

MITM adalah jenis serangan di mana penyerang menyisipkan dirinya di antara dua pihak komunikasi dan menyamar sebagai perantara tanpa sepengetahuan korban. Dalam skenario ini, pelaku dapat menyadap, memodifikasi, bahkan menyuntikkan data ke dalam komunikasi yang berlangsung. Dampak dari serangan MITM dapat sangat merugikan, termasuk kebocoran data sensitif, kehilangan privasi, pencurian identitas, dan kerugian finansial yang signifikan (Auliafitri et al., 2024).

Password Cracking

Password Cracking adalah sekelompok teknik yang digunakan untuk mendapatkan password pada sebuah sistem data (Dewa Made Julijati Putra et al., 2022). Salah satu teknik yang umumnya digunakan adalah *brute-force attack* yang mencoba seluruh kombinasi password hingga menemukan kombinasi yang tepat.

Ettercap

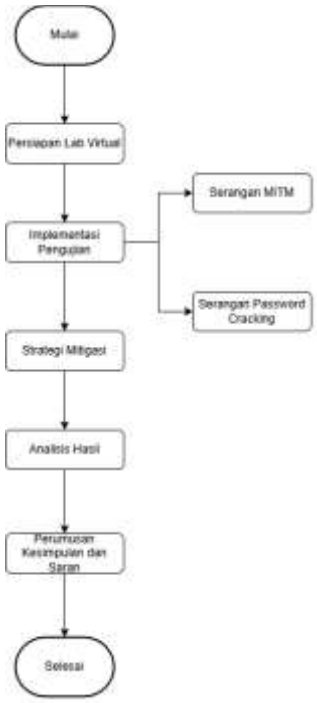
Ettercap adalah alat populer untuk melakukan MITM melalui ARP *spoofing*. Alat ini memiliki kemampuan yaitu dapat memblokir lalu lintas jaringan LAN, mencuri kata sandi, dan secara aktif menguping protokol umum (Diansyah et al., 2023).

Hydra

Hydra merupakan salah satu *tool* yang disediakan Kali Linux yang umumnya digunakan dalam pengujian penetrasi (*Penetration Testing*) untuk menguji keamanan sistem. *Tool* ini bekerja dengan cara mencoba semua kemungkinan kombinasi kata sandi secara otomatis untuk mencoba mendapatkan akses ke sistem yang dilindungi oleh kata sandi (Az Zahra et al., 2024).

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen kuantitatif untuk mengamati, menguji, dan menganalisis proses serta dampak serangan siber dalam lingkungan virtual terkontrol, sehingga skenario serangan *Man-In-The-Middle* (MITM) dan *Password Cracking* dapat dilakukan tanpa menggangu sistem atau jaringan asli. Tahapan simulasi yang akan dilakukan dalam penelitian ini dapat dilihat pada gambar 1 di bawah ini.



Gambar 1. Tahapan Simulasi Penelitian

Desain Eksperimen

Dua mesin virtual dijalankan menggunakan *software* Oracle VM VirtualBox di host Windows 11:

- Kali Linux (*Attacker*): Versi 2025.1 (64-bit), dilengkapi Ettercap dan Hydra.
- Ubuntu Desktop (Server Web): Versi 24.04.2 (64-bit), dengan pemasangan Apache2 dan PHP untuk halaman login.

Kedua VM dihubungkan melalui:

1. Host-Only Network (Adapter pertama), dengan subnet 192.168.56.0/24
2. NAT (Adapter kedua), memberikan akses internet untuk pembaruan paket.

IP Addres tiap OS akan menjadi seperti berikut:

- Windows (*Victim*): 192.168.56.1
- Kali Linux (*Attacker*): 192.168.56.101
- Ubuntu (*Server*): 192.168.56.102

Lingkungan Virtual dan *Tools*

1) VirtualBox sebagai *hypervisor*.
2) Kali Linux, dengan mengaktifkan fitur *ip forwading* menggunakan perintah "echo 1 > /proc/sys/net/ipv4/ip_forward" pada terminal. Tujuannya agar bisa meneruskan paket data ke jaringan yang berbeda.
3) Ubuntu, yang didalamnya sudah ter*install* paket Apache2 & PHP untuk pembuatan form login palsu.
4) Ettercap versi 0.8.3
5) Hydra versi 9.5

Konfigurasi Web Server (Ubuntu)

1. Pasang Apache2 dan PHP
2. Buat program didalam folder '/var/www/html/' yang berisi:
    - index.php: Halaman form login

```
 GNU nano 7.2                                  /var/www/html/index.php
<!DOCTYPE html>
<html>
 <head><title>Login</title></head>

 <body>
   <form method= "POST" action="login.php">
         <h2>Username: </h2>
         <input type="text" name="username"><br>

         <h2>Password: </h2>
         <input type="password" name="password"><br>

         <input type="submit" value="Login"><br>
   </form>
 </body>
</html>
```

Gambar 2. Kode Index.php

    - login.php: Proses autentikasi memeriksa username/password.

```
 GNU nano 7.2                                  /var/www/html/login.php
<?php
$valid_users = array(
        "user1" => "master123",
        "user2" => "abel123",
        "user3" => "fika123"
);

if($_SERVER["REQUEST_METHOD"] == "POST") {
        $username = $_POST['username'] ?? '';
        $password = $_POST['password'] ?? '';

        if(array_key_exists($username, $valid_users) && $valid_users[$username] === $password) {
                header("Location: welcome.php");
                exit();
        } else {
                echo "<h2>Username/Password Salah</h2>";
                //header("Location: login.html");
        }
}
?>
```

Gambar 3. Kode Login.php

    - welcome.php: Halaman dashboard setelah login berhasil.

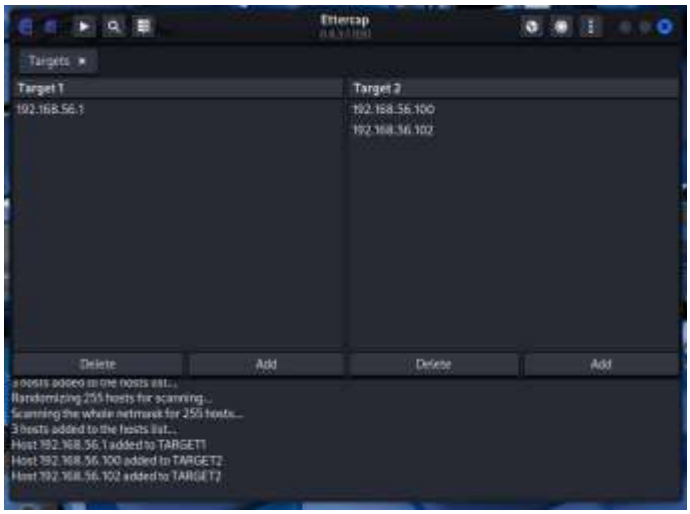
```
 GNU nano 7.2                                  /var/www/html/welcome.php
<!DOCTYPE html>
<html>
        <head><title></title></head>
        <body>
                <h1><center>Selamat Datang!</center><h1>
                <h4><center>Anda berhasil login.</center><h4>
        </body>
</html>
```

Gambar 4. Kode Welcome.php

3. Pastikan server Apache sudah berjalan.

3.1. Simulasi Serangan MITM dengan Ettercap

1. Jalankan Ettercap GUI.
2. Pilih *interface* 'eth0', nonaktifkan "Sniffing at Startup".
3. Lakukan *scan host*, tambahkan IP *Victim* ke target 1 dan IP server serta IP *gateaway* ke target 2 seperti pada gambar 5.

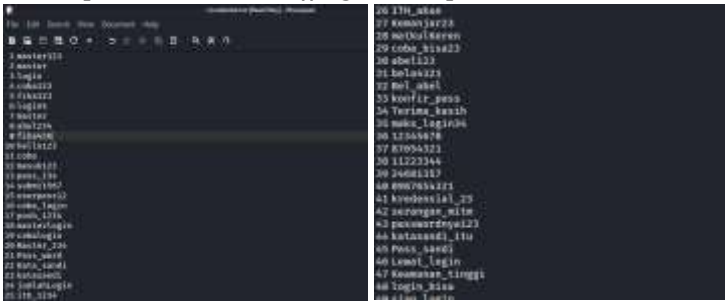


Gambar 5. Target Host yang Dipilih

4. Mulai ARP *Poisonings*: MITM *menu* -> ARP poisoning -> centang "*Sniff remote connections*" -> OK.
5. Dari Windows, akses 'http://192.168.56.102/', masukkan username dan password yang sudah dipersiapkan sebelumnya.
6. Perhatikan *output* Ettercap yang menampilkan kredensial login berbentuk *plaintext*. Hasil output dapat dilihat pada gambar 11.

Simulasi *Password Cracking* dengan Hydra.Setelah memperoleh username dan password melalui hasil *Sniffing* pada langkah sebelumnya, *Attacker* kemudian memfokuskan serangan *brute-force* hanya pada salah satu akun tersebut (contoh: user2). Tujuan dari pendekatan ini adalah untuk menguji efektivitas Hydra dalam menebak password berdasarkan satu target yang telah diketahui, sebagaimana sering dilakukan dalam dunia nyata ketika penyerang hanya memiliki sebagian kredensial. Adapun langkah - langkah simulasinya sebagai berikut:

1. Siapkan *wordlist* khusus password hasil *Sniffing* Ettercap.



Gambar 6. *Wordlist password* hasil *Sniffing*

2. Eksekusi Hydra dengan perintah berikut.

Gambar 7. Perintah *brute-force* Hydra

Tabel 1 menjelaskan perintah yang digunakan pada gambar 7.

Tabel 1. Fungsi perintah Hydra

No.	Perintah	Fungsi
1	hydra	Menjalankan *tools* Hydra.
2	-l	Menentukan satu username yang akan digunakan selama percobaan.
3	user2	Username spesifik yang menjadi target uji.
4	-P	Mengarahkan Hydra untuk menggunakan file tertentu sebagai sumber daftar password.
5	192.168.56.102	Alamat IP server yang menjadi target serangan.
6	http-post-form	Modul Hydra untuk menyerang form login web yang mengirimkan data melalui metode HTTP POST.
7	/login.php	*Path* dari halaman login yang akan diuji pada sisi server.
8	username=^USER^&password=^PASS^	Parameter *form* yang akan diganti secara dinamis oleh Hydra selama pengiriman permintaan autentikasi.
9	:Username/Password Salah	String indikator yang digunakan untuk mendeteksi kegagalan login berdasarkan respon server.
10	-V	Mengaktifkan mode *verbose* untuk menampilkan detail proses selama pengujian berlangsung.
11	-f	Menghentikan proses *brute-force* segera setelah ditemukan kombinasi kredensial yang valid.

3. Pada gambar 12, proses berjalan hingga Hydra menemukan kombinasi username dan password yang valid atau hingga seluruh entri wordlist habis diuji.

3.2. Implementasi Mitigasi HTTPS (SSL/TLS)

1. Pasang modul SSL pada server:

Gambar 8. Perintah Mengaktifkan Modul SSL

2. Buat direktori untuk sertifikat *self-signed* dengan perintah: 'sudo mkdir /etc/apache2/ssl'.
3. Buat format untuk pengisin sertifikat SSL *self-signed*. Pengisian informasi umum diperlukan saat proses pembuatan sertifikat, di mana sebagian besar bidang dapat dikosongkan dengan menekan tombol *enter*. Namun, bagian *Common Name (CN)* harus diisi dengan alamat IP server Ubuntu, agar sesuai dengan domain tujuan dan mengurangi peringatan keamanan pada saat browser mengakses situs melalui HTTPS.
4. Salin dan modifikasi konfigurasi SSL default (/etc/apache2/sites-available/default-ssl.conf) menjadi 'default-ssl-mitigasi.conf' lalu sesuaikan konfigurasinya:

Gambar 9. Konfigurasi SSL Mitigasi

5. Aktifkan virtual host SSL.

Gambar 10. Perintah Mengaktifkan Konfigurasi SSL Mitigasi

6. Dari Windows, akses 'https://192.168.56.102' (akan muncul peringatan "Not Secure" karena sertifikat *self-signed*). Klik lanjut, dan login seperti percobaan sebelumnya.
7. Jalankan kembali Ettercap ARP *poisoning* dan *sniffing*. Perhatikan pada gambar 13, bahwa kredensial HTTPS tidak muncul.

HASIL DAN PEMBAHASAN

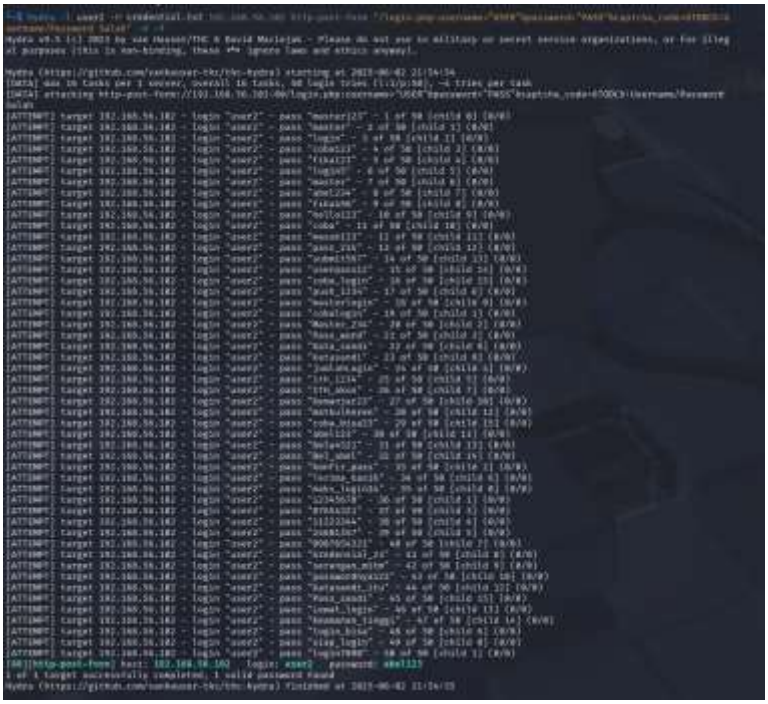
Hasil Simulasi MITM

Dalam beberapa percobaan login HTTP di dalam lingkungan virtual, Ettercap berhasil menyadap seluruh kredensial *Victim* (100% berhasil). Setiap kali pengguna (Windows) mengakses halaman 'http://192.168.56.102/' dan memasukkan kombinasi username & password (misal user1:master123 atau user2:coba123), Ettercap langsung menampilkan kredensial *plaintext*. Rata-rata waktu yang dibutuhkan antara saat korban menekan tombol '*Login*' hingga kredensial muncul di terminal Ettercap adalah sekitar 1,5 detik.

Gambar 11. Hasil Simulasi Serangan MITM

Hasil Simulasi *Password Cracking*

Setelah memperoleh username ‘user2’ melalui *sniffing*, peneliti menjalankan serangan *brute-force* menggunakan *Hydra* dengan daftar kata sandi berisi 50 kredensial password hasil MITM. Dalam simulasi ini, hanya satu akun yang menjadi target pengujian, yakni ‘user2’. Hydra berhasil menemukan kombinasi username dan password yang valid dalam waktu yang sangat singkat, yaitu kurang dari satu menit. Hal ini menunjukkan bahwa apabila penyerang memiliki informasi sebagian kredensial dan *wordlisti* dan relevan, serangan *brute-force* terhadap form login berbasis HTTP POST dapat dieksekusi dengan cepat dan efektif. Jika password target tidak terdapat dalam *wordlist*, Hydra akan mengakhiri proses setelah seluruh entri selesai diuji tanpa menemukan kecocokan.

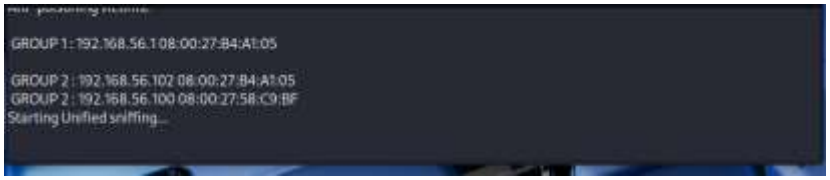


Gambar 12. Hasil Simulasi Serangan *Password Cracking*

Hasil Mitigasi HTTPS (SSL/TLS)

Setelah penerapan HTTPS menggunakan sertifikat *self-signed*, peneliti kembali menjalankan *ARP poisoning* dengan Ettercap dan melakukan 5 percobaan login melalui ‘http://192.168.56.102/’. Meskipun

ARP poisoning masih berhasil dijalankan, Ettercap gagal menampilkan kredensial di semua lima percobaan (0% keberhasilan). Hal ini terjadi karena trafik sudah terenkripsi oleh TLS sehingga *payload* HTTP tidak dapat didekripsi tanpa kunci privat server.



Gambar 13. Hasil Mitigasi SSL

KESIMPULAN

Berdasarkan hasil simulasi yang telah dilakukan, penelitian ini menyimpulkan bahwa serangan *Man-in-the-Middle* (MITM) yang memanfaatkan teknik *ARP spoofing* dengan dukungan *tool* Ettercap menunjukkan efektivitas tinggi dalam mengintersep dan mengungkap kredensial pengguna pada koneksi HTTP. Dalam uji coba yang dilakukan, kredensial akun berhasil diperoleh secara *real-time* dalam waktu yang sangat singkat, yaitu dalam hitungan detik. Selanjutnya, serangan *brute-force* menggunakan *tool* Hydra terhadap satu akun target (user2) dengan wordlist berisi 50 entri berhasil mengungkapkan password yang valid dalam durasi kurang dari satu menit. Sebaliknya, ketika protokol HTTPS diimplementasikan pada server, meskipun ARP spoofing tetap berjalan, Ettercap tidak mampu mendekripsi data sensitif karena komunikasi dilindungi oleh enkripsi TLS. Temuan ini secara empiris membuktikan bahwa penggunaan HTTPS secara signifikan dapat memutus rantai serangan MITM dan mencegah eksfiltrasi data kredensial pengguna.

Namun, penelitian ini tidak luput dari beberapa keterbatasan. Simulasi yang dilakukan hanya menargetkan satu akun dengan *wordlist* yang sangat terbatas, sehingga belum sepenuhnya merefleksikan skenario serangan dalam kondisi nyata yang melibatkan banyak akun dan wordlist yang lebih kompleks. Selain itu, uji coba *brute-force* terhadap form login yang dilindungi HTTPS tidak dieksplorasi secara mendalam dalam penelitian ini. Oleh karena itu, penelitian selanjutnya direkomendasikan untuk menguji efektivitas serangan *brute-force* pada halaman login berbasis HTTPS dengan menerapkan *wordlist* berskala besar guna mengevaluasi ketahanan sistem dalam situasi yang lebih realistis. Lebih lanjut, integrasi sistem deteksi intrusi (*Intrusion Detection System/IDS*) seperti Snort atau Suricata disarankan untuk mendeteksi aktivitas mencurigakan, termasuk ARP *spoofing* dan upaya *brute-force* login. Sebagai langkah mitigasi tambahan, penggunaan sertifikat yang ditandatangani oleh *Certificate Authority* (*CA-signed*) serta implementasi keamanan *Firewall Iptables* juga direkomendasikan untuk meningkatkan keamanan jaringan, terutama pada jaringan publik yang rentan terhadap serangan.

DAFTAR PUSTAKA

[1] Auliafitri, D., Rizkisuro, E., Rangga, M., Malik, M., & Setiawan, A. (2024). *Optimalisasi Pengujian Penetrasi : Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit*. *3*, 1–12.

[2] Az Zahra, D. R., Ilham, F. P., Ramdhani, H. N., & Setiawan, A. (2024). Penerapan dan Pengujian

Keamanan SSH Pada Server Linux menggunakan Hydra. *Journal of Internet and Software Engineering*, *1*(3), 10. https://doi.org/10.47134/pjise.v1i3.2627

[3] Dewa Made Julijati Putra, I Nyoman Namo Yoga Anantra, Putu Adhitya kusuma, Putu Damar Jagat Pratama, Gede Arna Jude Saskara, & I Made Edy Listartha. (2022). Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada Password Attack. *Jurnal Informatika Teknologi Dan Sains*, *4*(4), 461–466. https://doi.org/10.51401/jinteks.v4i4.2192

[4] Diansyah, T. M., Faisal, I., & Siregar, D. (2023). Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack. *Kesatria : Jurnal Penerapan Sistem Informasi (Komputer Dan Manajemen)*, *4*(1), 224–233. http://tunasbangsa.ac.id/pkm/index.php/kesatria/article/view/134

[5] Nugraha, A. D., Husaini, H., & Anwar, A. (2022). Analisis Keamanan Data Dalam Jaringan Terhadap Kegiatan Sniffing Menggunakan Serangan Man In The Middle Attack. *Jurnal Teknologi Rekayasa Informasi Dan Komputer*, *5*(2), 3–7. http://e-jurnal.pnl.ac.id/TRIK/article/view/4757

[6] Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60–67. https://doi.org/10.35447/jitekh.v10i2.571

[7] Saraun, A., Lumenta, A. S. M., & Febrian Sengkey, D. (2021). An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs. *Jurnal Teknik Informatika*, *17*(1), 565–572.