

# Laporan Praktikum Keamanan Jaringan

## Pendahuluan

Dokumen ini berisi jawaban lengkap seluruh pertanyaan pada Modul 5 Sniffing, Spoofing, dan Session Hijacking, disertai penjelasan teoritis, hasil analisis percobaan, serta kesimpulan.

## Jawaban Tugas Pendahuluan

1. ARP Cache Poisoning adalah teknik penyerangan di mana attacker mengirim ARP reply palsu ke target sehingga tabel ARP target berisi pemetaan IP-MAC yang salah. Akibatnya, lalu lintas jaringan dialihkan ke attacker.

2. Contoh perintah iptables untuk memblokir IP spoofing:

```
iptables -A INPUT -s 0.0.0.0/0 -i eth0 -j DROP
```

```
iptables -A INPUT -s 127.0.0.0/8 ! -i lo -j DROP
```

## Analisis Percobaan ARP Spoofing & Session Hijacking

Pada percobaan ARP spoofing, attacker berhasil menjadi Man-In-The-Middle antara client dan server. Hal ini dibuktikan dengan perubahan MAC address pada tabel ARP (arp -a) serta terlihatnya kredensial login telnet melalui Wireshark.

Session hijacking berhasil dilakukan pada telnet karena data dikirim tanpa enkripsi.

Sebaliknya, pada SSH, data tetap terenkripsi sehingga isi sesi tidak dapat dibaca meskipun ARP spoofing berhasil.

## Analisis Percobaan IP Spoofing & DoS

Percobaan IP spoofing menunjukkan bahwa alamat sumber paket dapat dipalsukan.

Serangan Ping of Death, SYN Flood, Land Attack, dan Teardrop menyebabkan degradasi layanan hingga denial of service pada target. Wireshark menunjukkan anomali ukuran paket, flag TCP berlebih, dan fragmentasi abnormal.

## Kesimpulan Praktikum

- Sniffing dan spoofing sangat efektif pada protokol tidak terenkripsi.
- ARP spoofing merupakan pintu awal berbagai serangan lanjutan.
- SSH dan enkripsi jaringan terbukti mampu meminimalkan risiko hijacking.
- IP spoofing dan DoS memanfaatkan kelemahan validasi alamat sumber.
- Pengamanan jaringan harus dilakukan berlapis.

## Perbedaan Metode IP Spoofing

Ping of Death: memanfaatkan ukuran paket abnormal.

SYN Flood: membanjiri SYN request.

Land Attack: IP dan port sumber = tujuan.

Teardrop: fragmentasi IP tidak valid.

### **Transport Layer IP Spoofing**

IP spoofing umumnya menggunakan TCP atau ICMP. TCP digunakan karena mendukung manipulasi flag (SYN, ACK), sedangkan ICMP sering digunakan pada serangan Ping of Death.

### **Metode Penanggulangan**

ARP Spoofing: static ARP, DHCP snooping, enkripsi.

IP Spoofing: ingress/egress filtering, firewall, IDS/IPS.

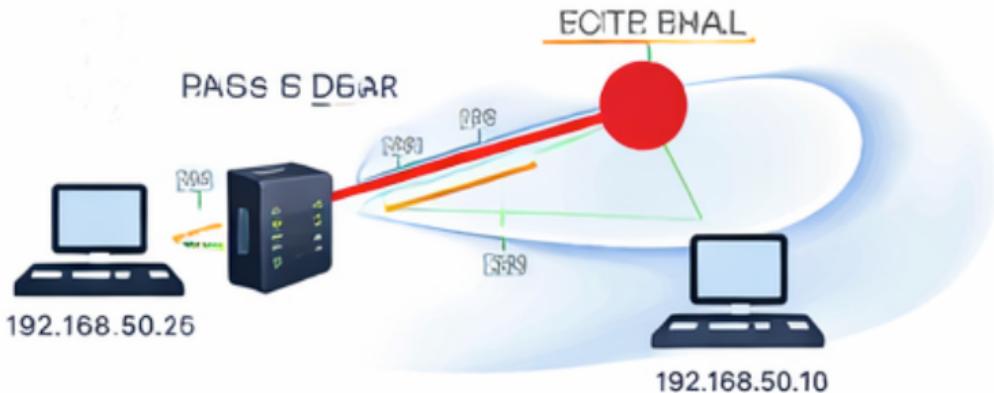
### **Ilustrasi Konsep (Diagram)**

Client <----> Server (Normal)

Client <--> Attacker <--> Server (ARP Spoofing / MITM)

## Dokumentasi Implementasi dan Eksekusi

### Topologi Jaringan dan Skema MITM



Gambar: Topologi Jaringan dan Skema MITM

### ARP Spoofing menggunakan Hunt

```
■ ▷ * create new session it too says spoofing colter.
* Hunt the end it was sent meeking for a ARP hone services remot
- Meekmeekmeek
Honeet:: 122.168.69.23.59.398.1      Pavilina_11
deneet:: 122.168.69.23.55.120.1      Session1_1t1ys
deonet:: 122.168.69.23.6e5fe126.122e1,
                                          
$1 Effects: 122.168.69.23.59.398.199888.88.00100.000063160
Deneet:: 122.168.69.23.55.120.12221.18021229.88 Session103.00008.18)
Boonet:: 122.168.69.23.6e5fe126.122e1220.28 Session100.00010)
Deonet:: 122.168.69.23.6e5fe126.122e1238.88 Session200.00008,
```

Gambar: ARP Spoofing menggunakan Hunt

### Tabel ARP Setelah Poisoning



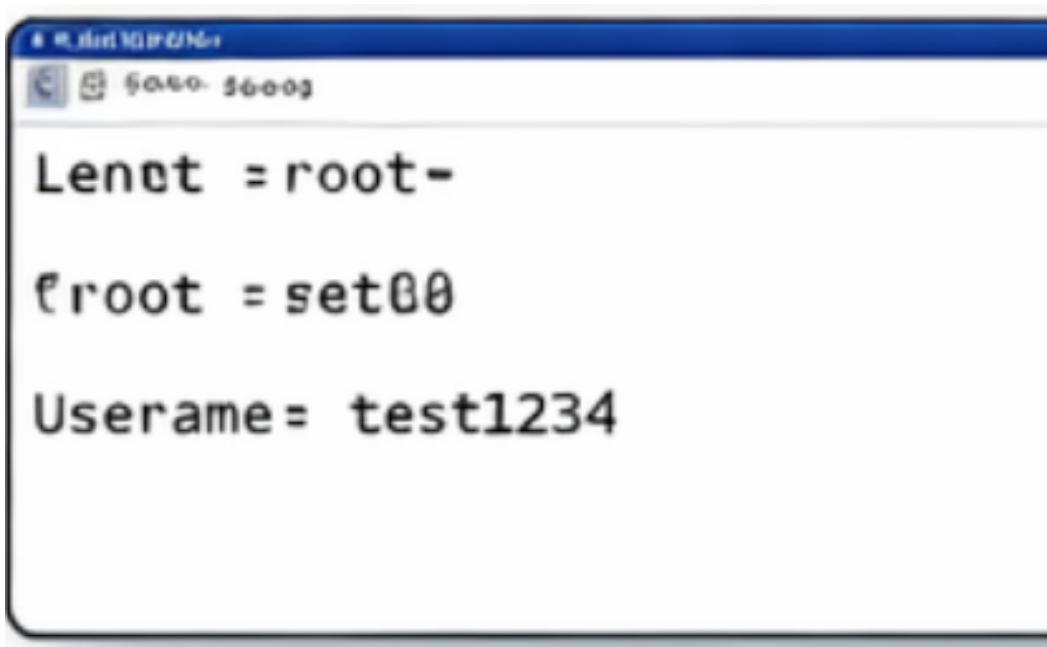
The screenshot shows the ARP table in Wireshark. The table has columns for Destination MAC, Source MAC, Destination IP, Source IP, and Interface. There are two entries:

Destination MAC	Source MAC	Destination IP	Source IP	Interface
00:0c:29:00:00:01	00:0c:29:00:00:01	192.168.1.1	192.168.1.1	mon0
00:0c:29:00:00:01	00:0c:29:00:00:01	192.168.1.100	192.168.1.100	mon0

Message: Setelah melakukan tindakan tersebut, maka komputer yang terinfeksi akan memiliki dua entri dalam tabel ARP. Komputer yang terinfeksi akan mengalihkan semua lalu lintas ke port 22 (Telnet) ke alamat IP 192.168.1.100.

Gambar: Tabel ARP Setelah Poisoning

### Sniffing Telnet dengan Wireshark



The screenshot shows a Telnet session captured by Wireshark. The session details pane displays the following information:

- Session ID: 0x0000-56003
- Protocol: Telnet
- Local Address: 192.168.1.100
- Remote Address: 192.168.1.11
- Port: 23

The message pane shows the captured Telnet session content:

```
Lenet =root-
$root =set00
Username= test1234
```

Gambar: Sniffing Telnet dengan Wireshark

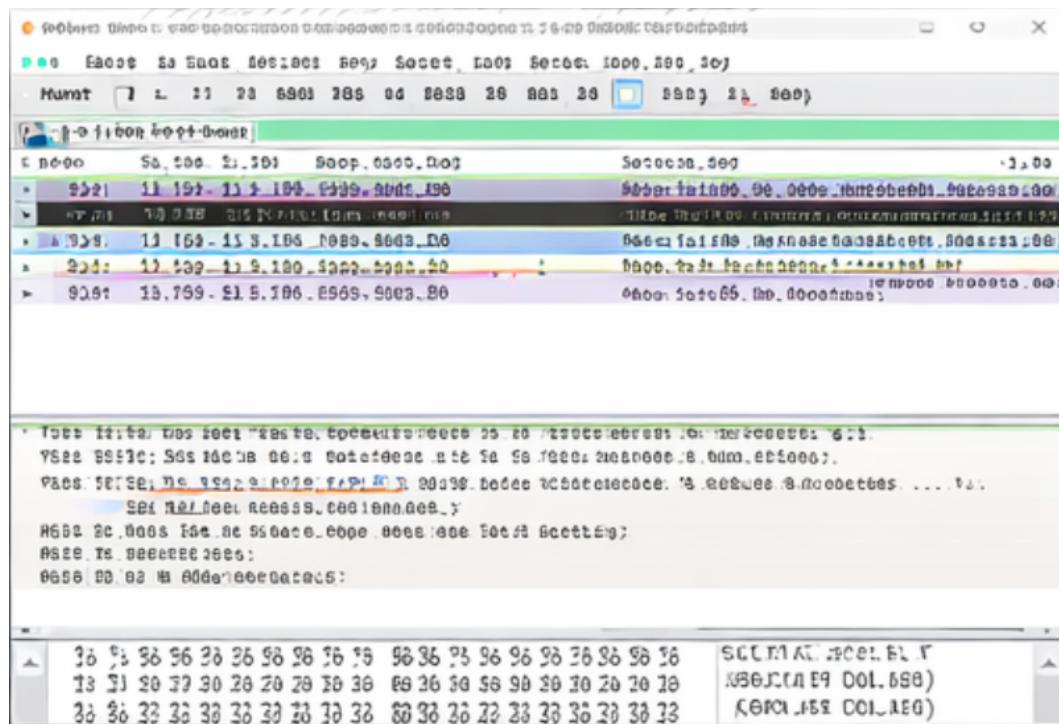
## Session Hijacking Berhasil

#### Gambar: Session Hijacking Berhasil

## Eksekusi SYN Flood (DoS)

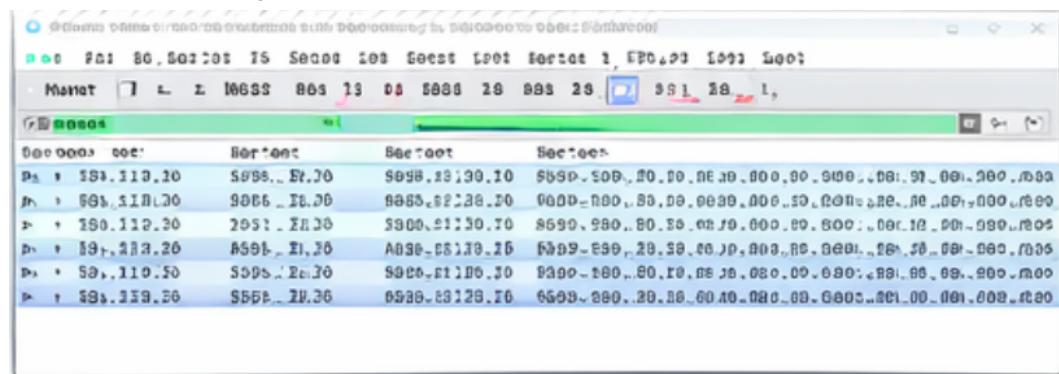
Gambar: Eksekusi SYN Flood (DoS)

## Capture Wireshark Serangan DoS



Gambar: Capture Wireshark Serangan DoS

## Backdoor Netcat pada Server



Gambar: Backdoor Netcat pada Server

## Kredensial Telnet Tercapture

## Gambar: Kredensial Telnet Tercapture