

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

1. Sniffing dan spoofing sangat efektif pada protokol tidak terenkripsi.
2. ARP spoofing merupakan pintu awal berbagai serangan lanjutan.
3. SSH dan enkripsi jaringan terbukti mampu meminimalkan risiko hijacking.
4. IP spoofing dan DoS memanfaatkan kelemahan validasi alamat sumber.
5. 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.

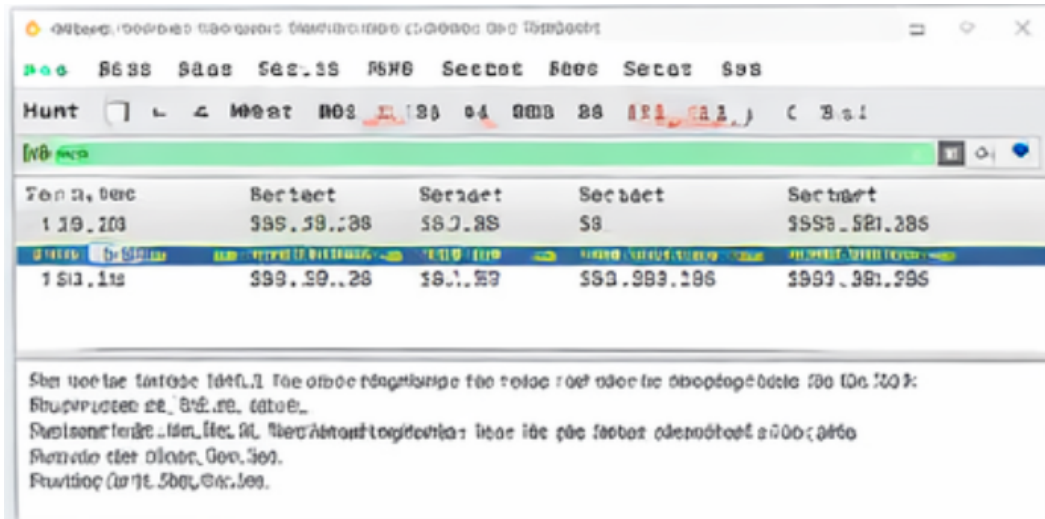
IP Spoofing: ingress/egress filtering, firewall, IDS/IPS.

Ilustrasi Konsep (Diagram)

Client <----> Server (Normal)

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

Tabel ARP Setelah Poisoning

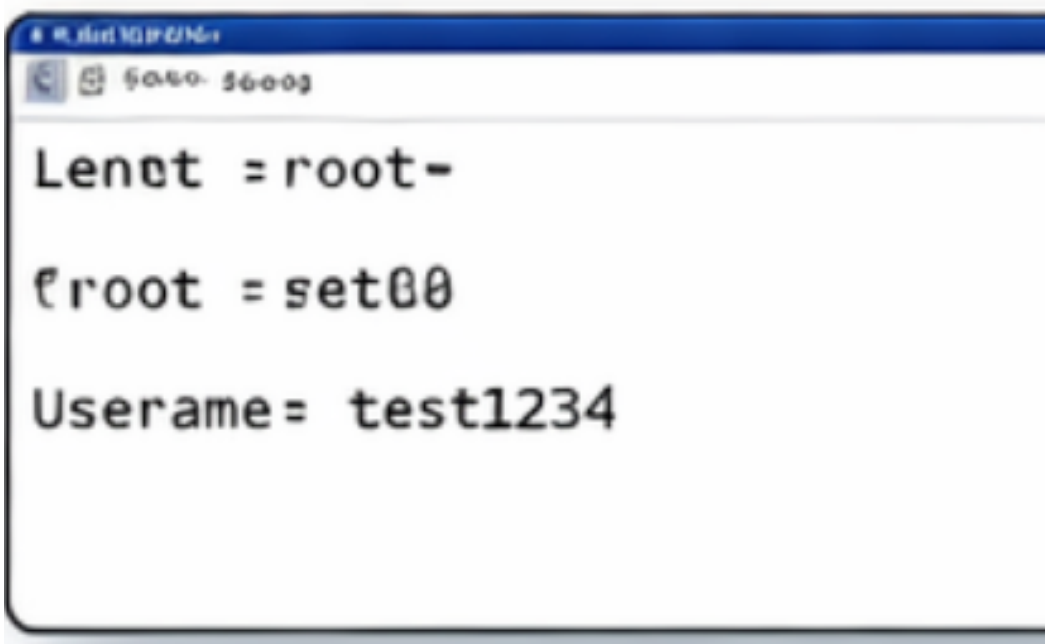


Tenaga, Ber	Berdest	Serdest	Serdest	Serdest
1 192.168.1.100	999.99.99.99	999.99.99.99	999.99.99.99	999.99.99.99
1 192.168.1.101	999.99.99.99	999.99.99.99	999.99.99.99	999.99.99.99

Setelah melakukan poisoning, maka akan terdapat dua entri di tabel ARP. Entri pertama adalah entri yang benar, yaitu entri yang memiliki IP 192.168.1.100. Entri kedua adalah entri yang salah, yaitu entri yang memiliki IP 192.168.1.101. Entri yang salah ini adalah entri yang dibuat oleh penyerang.

Gambar: Tabel ARP Setelah Poisoning

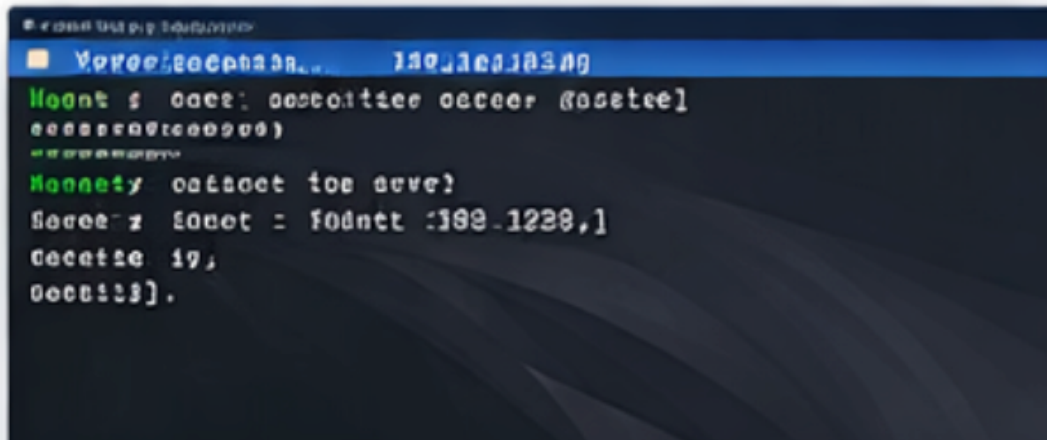
Sniffing Telnet dengan Wireshark



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

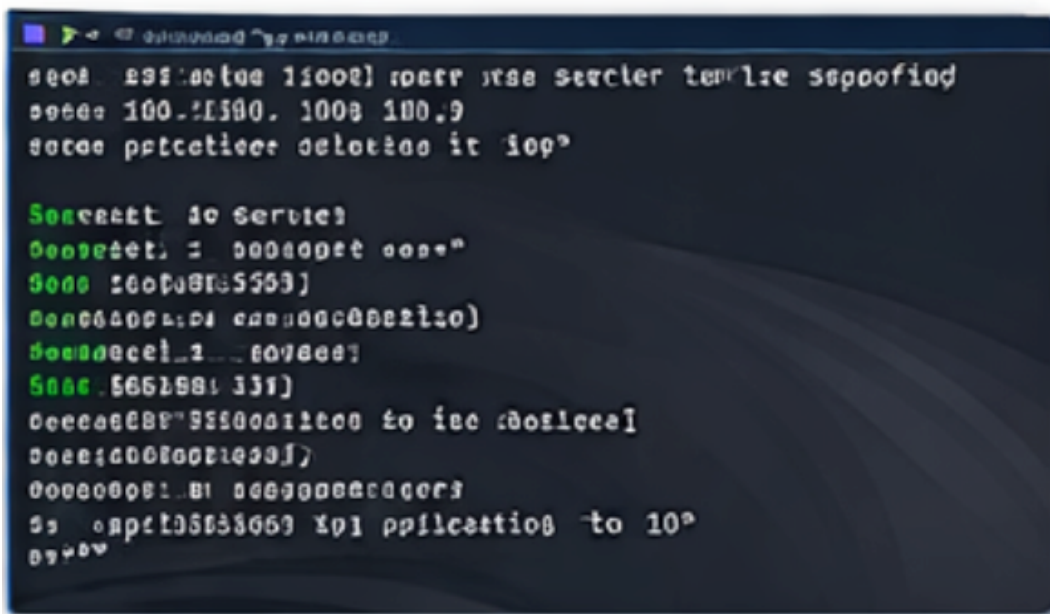
Gambar: Sniffing Telnet dengan Wireshark

Session Hijacking Berhasil



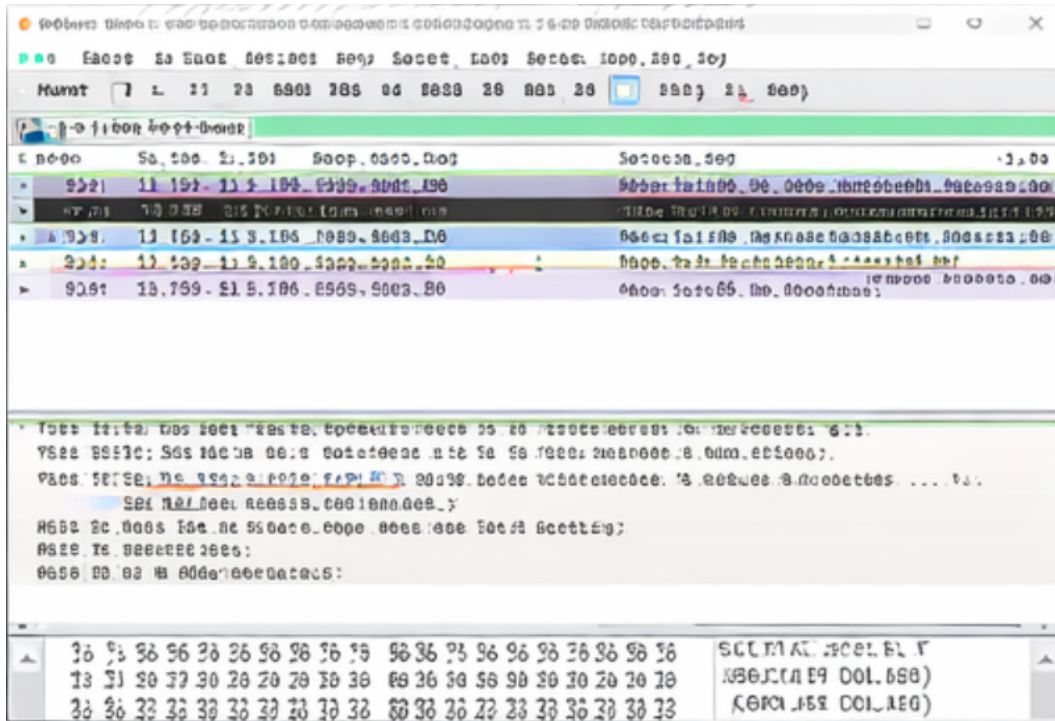
Gambar: Session Hijacking Berhasil

Eksekusi SYN Flood (DoS)



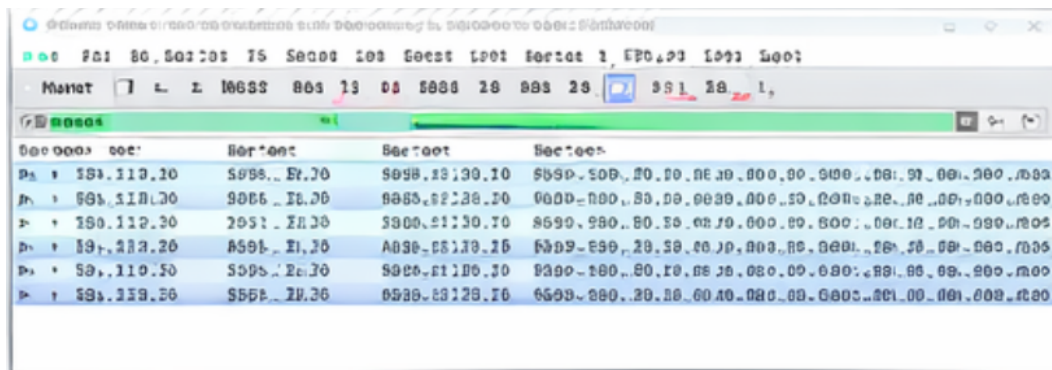
Gambar: Eksekusi SYN Flood (DoS)

Capture Wireshark Serangan DoS



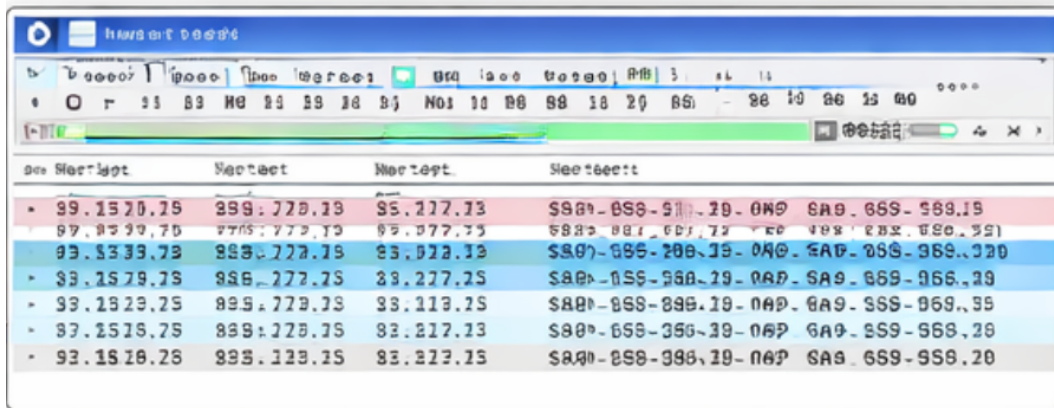
Gambar: Capture Wireshark Serangan DoS

Backdoor Netcat pada Server



Gambar: Backdoor Netcat pada Server

Kredensial Telnet Tercapture



No	Start	End	Protocol	Length	Info
1	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
2	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
3	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
4	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
5	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
6	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
7	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
8	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
9	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
10	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0

No	Start	End	Protocol	Length	Info
1	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
2	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
3	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
4	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
5	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
6	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
7	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
8	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
9	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0
10	0.000000	0.000000	Telnet	100	192.168.1.100 → 192.168.1.100:23 [RST] Seq=123456789 Win=0 Len=0

Gambar: Kredensial Telnet Tercapture