LAPORAN PRAKTIKUM NETWORK SECURITY

Nama: M Fahri marfiansyah

Kelas: 5B

Nim: 105841105823

1. Kesimpulan Hasil Praktikum

Berdasarkan hasil praktikum Network Security yang meliputi Sniffing, ARP Spoofing, Session Hijacking, dan IP Spoofing, dapat disimpulkan bahwa sebagian besar serangan jaringan klasik tidak lagi efektif pada sistem dan jaringan modern. Hal ini disebabkan oleh peningkatan mekanisme keamanan seperti enkripsi komunikasi, proteksi ARP, dan filtering paket jaringan.

Percobaan ARP spoofing menunjukkan bahwa serangan tidak berhasil secara stabil sehingga attacker tidak dapat berada pada posisi Man-In-The-Middle. Akibatnya, session hijacking tidak dapat dilakukan. Percobaan IP spoofing juga menunjukkan bahwa sistem target mampu bertahan dari serangan Ping of Death, SYN Flood, Land Attack, dan Teardrop karena adanya perlindungan pada kernel modern.

2. Perbedaan Metode pada Percobaan IP Spoofing

Ping of Death bertujuan mengirim paket ICMP berukuran besar untuk menyebabkan crash sistem. SYN Flood memanfaatkan kelemahan three-way handshake TCP. Land Attack menggunakan IP sumber dan tujuan yang sama, sedangkan Teardrop memanfaatkan fragmentasi paket IP. Keempat metode ini sudah tidak efektif pada sistem modern.

3. Tipe Transport Layer pada IP Spoofing

IP spoofing umumnya menggunakan protokol TCP dan ICMP. TCP digunakan karena

sifatnya yang connection-oriented dan dapat dieksploitasi pada proses handshake. ICMP digunakan karena tidak memerlukan koneksi dan mudah dimanipulasi.

4. Metode Penanggulangan ARP Spoofing dan IP Spoofing

ARP spoofing dapat ditangkal dengan static ARP, Dynamic ARP Inspection, ARP monitoring, dan penggunaan protokol terenkripsi seperti SSH. IP spoofing dapat dicegah dengan ingress-egress filtering, firewall, IDS/IPS, SYN cookies, dan rate limiting.