

DAFTAR ISI

| | |
|---|------|
| PRAKATA | vi |
| DAFTAR ISI..... | viii |
| DAFTAR TABEL | x |
| DAFTAR GAMBAR..... | xi |
| INTISARI..... | xiii |
| ABSTRACT..... | xiv |
| BAB I | 1 |
| PENDAHULUAN | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 3 |
| 1.3 Batasan Masalah | 3 |
| 1.4 Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian..... | 3 |
| 1.6 Metodologi Penelitian..... | 4 |
| BAB II | 5 |
| TINJAUAN PUSTAKA..... | 5 |
| BAB III | 9 |
| LANDASAN TEORI..... | 9 |
| 3.1 Hacking..... | 9 |
| 3.2 Packet Analyzer/Sniffer..... | 10 |
| 3.3 Cara Kerja Packet Sniffer..... | 11 |
| 3.4 ARP Chace Poisoning/Spoofing..... | 12 |
| 3.5 Packet Data | 13 |
| 3.6 SSL (Security Sockets Layer) | 18 |
| BAB IV..... | 21 |
| METODE PENELITIAN | 21 |
| 4.1 Alat dan Bahan | 21 |

| | | |
|----------------------|---|----|
| 4.2 | Skema Sistem dan Flowchart | 21 |
| 4.2.1 | Flowchart Serangan Packet Sniffer | 21 |
| 4.2.1 | Skema SSL, ARP Poisoning/MitM dan Simulasi Penyerangan..... | 22 |
| 4.3 | Rancangan Pengujian | 25 |
| 4.4 | Instalasi dan Konfigurasi Software..... | 25 |
| 4.4.1 | Instalasi dan Konfigurasi Ettercap..... | 25 |
| 4.4.2 | Instalasi Drifnet | 27 |
| 4.5 | Pengujian Packet Sniffing | 28 |
| 4.5.1 | Uji Coba Sniffing dengan Ettercap | 28 |
| 4.5.2 | Uji Coba Sniffing Data Image dengan Driftnet | 33 |
| BAB V | | 35 |
| HASIL DAN PEMBAHASAN | | 35 |
| 5.1 | Hasil dan Pembahasan Packet Sniffing | 35 |
| 5.1.1 | Hasil Pengujian Packet sniffing dengan ettercap..... | 35 |
| 5.1.2 | Hasil Pengujian Packet sniffing dengan driftnet | 45 |
| BAB VI | | 49 |
| PENUTUP | | 49 |
| 6.1 | Kesimpulan..... | 49 |
| 6.1 | Saran | 49 |
| DAFTAR PUSTAKA | | 51 |

DAFTAR TABEL

| | |
|---|----|
| Tabel 5.1 Daftar hasil percobaan yang diperoleh | 36 |
| Tabel 5.2 Daftar Status Preload pada Website | 45 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 3.1 Gambar format paket TCP (Tanenbaum 2011) | 15 |
| Gambar 3.2 langkah yang dilalui sebuah packet sebelum meninggalkan host | 16 |
| Gambar 4.1 Flowchart aktivitas penyerangan dengan packet sniffer | 21 |
| Gambar 4.2 Skema simulasi serangan | 22 |
| Gambar 4.3 Skema cara kerja SSL | 23 |
| Gambar 4.4 Skema penyerangan dengan ARP Poison/MitM | 24 |
| Gambar 4.5 Tampilan awal aplikasi ettercap | 26 |
| Gambar 4.7 Bagian konfigurasi ettercap value di ganti menjadi 0 | 26 |
| Gambar 4.9 Modifikasi pada perintah IP Table | 27 |
| Gambar 4.10 Tampilan awal aplikasi Driftnet | 27 |
| Gambar 4.11 Tampilan langkah awal memulai sniffing | 28 |
| Gambar 4.12 Tampilan pemilihan input jaringan | 29 |
| Gambar 4.13 Tampilan scan hosts | 29 |
| Gambar 4.14 Tampilan perintah hosts-list | 30 |
| Gambar 4.15 Tampilan daftar host yang terdeteksi | 30 |
| Gambar 4.16 Tampilan adding target 1 | 31 |
| Gambar 4.17 Tampilan adding target 2 | 32 |
| Gambar 4.18 Perintah MitM | 32 |
| Gambar 4.19 Tampilan perintah start sniffing | 33 |
| Gambar 4.20 Tampilan aplikasi driftnet | 34 |
| Gambar 5.1 Hasil percobaan dengan ettercap pada website BBC dan Path | 36 |
| Gambar 5.2 Hasil percobaan dengan ettercap pada web Steam dan Warframe | 37 |
| Gambar 5.3 Hasil percobaan pada web Palawa UGM, Indorelawan dan SSO UGM | 37 |
| Gambar 5.4 Hasil percobaan pada web Kaskus | 38 |
| Gambar 5.5 Contoh struktur data yang diperoleh dari web BBC | 39 |
| Gambar 5.6 Hasil yang diperoleh dengan PASS berformat md5. Kotak merah menunjukkan barisan kata yang merupakan password dalam format md5 | 40 |
| Gambar 5.6a Hasil pengecekan status preload pada website facebook | 43 |
| Gambar 5.6a hasil pengecekan status preload pada website kaskus | 43 |
| Gambar 5.7a Tampilan browser ketika mengakses koneksi yang unsecure | 44 |



| | |
|---|----|
| Gambar 5.7b Tampilan pilihan untuk melanjutkan akses atau tidak..... | 44 |
| Gambar 5.8 Hasil Sniffing dengan driftnet pada Google Image..... | 46 |
| Gambar 5.9 Hasil Sniffing pada fanpage di web Facebook..... | 47 |
| Gambar 5.11 Beberapa data gambar yang berhasil disadap oleh driftnet..... | 48 |