LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Pertemuan 2

Disusun oleh

Nama: Rafli Rajendra Permana

NIM: 21/473999/SV/18868

SARJANA SAINS TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

I. Tujuan

1. Merekam dan menganalisis trafik HTTP
2. Merekam dan menganalisis trafik HTTPS

II. Dasar Teori

HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi. Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan arti sebenarnya dari data yang sedang dipertukarkan. Hal ini dilakukan melalui penggunaan sertifikat yang dapat dilihat nanti di lab ini. Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

III. Alat dan Bahan

1. Perangkat Komputer
2. Sambungan Internet
3. VM Cyberops Workstation

IV. Hasil

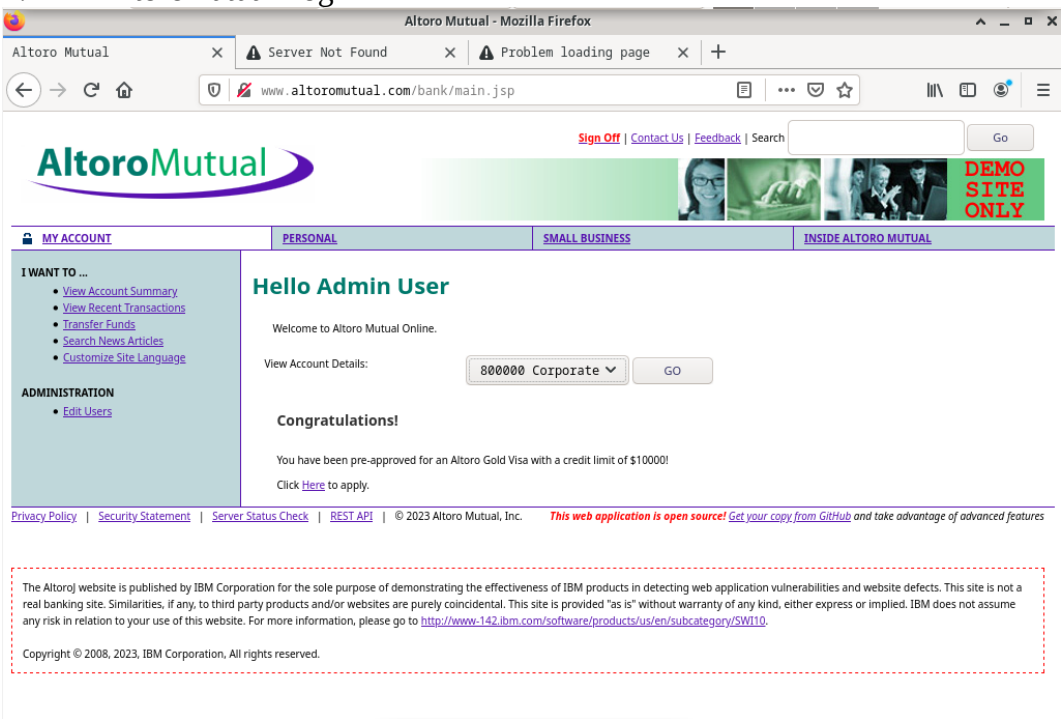
HTTP Scanning

1. IP Address, TCP Dump

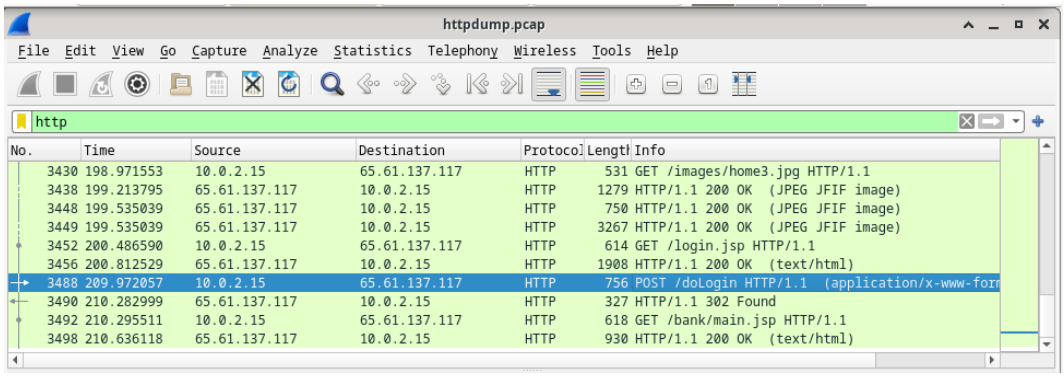
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1a:19:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 84801sec preferred_lft 84801sec
    inet6 fe80::a00:27ff:fe1a:19b2/64 scope link
       valid_lft forever preferred_lft forever
```

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

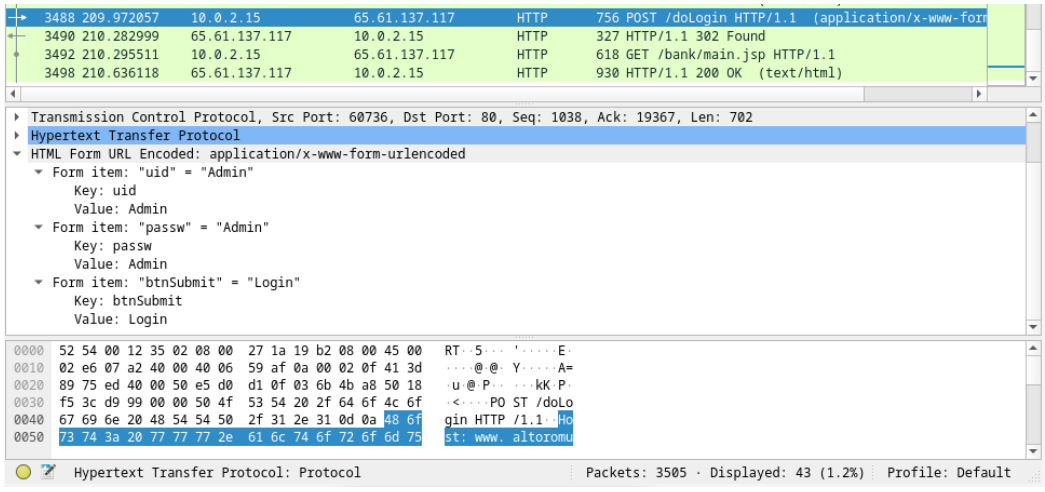
2. Altoromutual Login



3. HTTP Filter on Wireshark

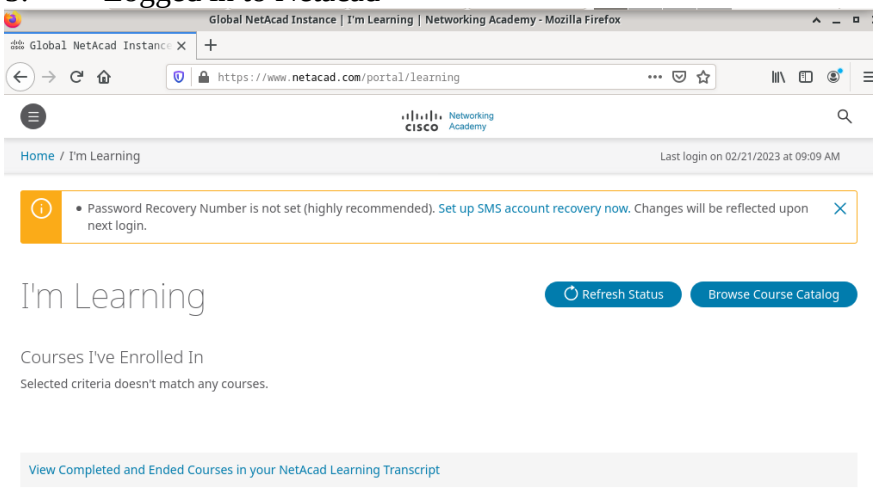


4. Altoromutual UID and Password

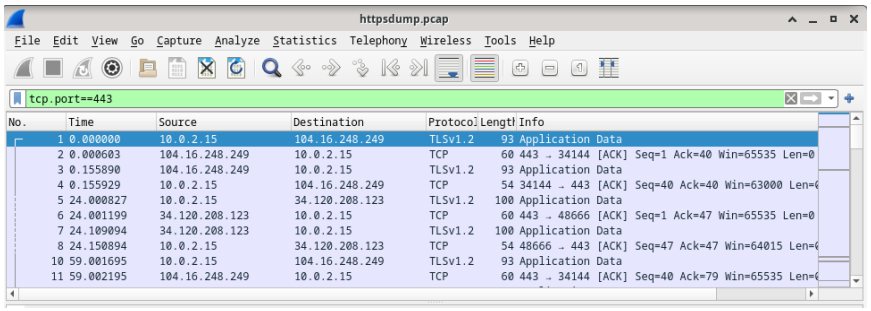


HTTPS Scanning

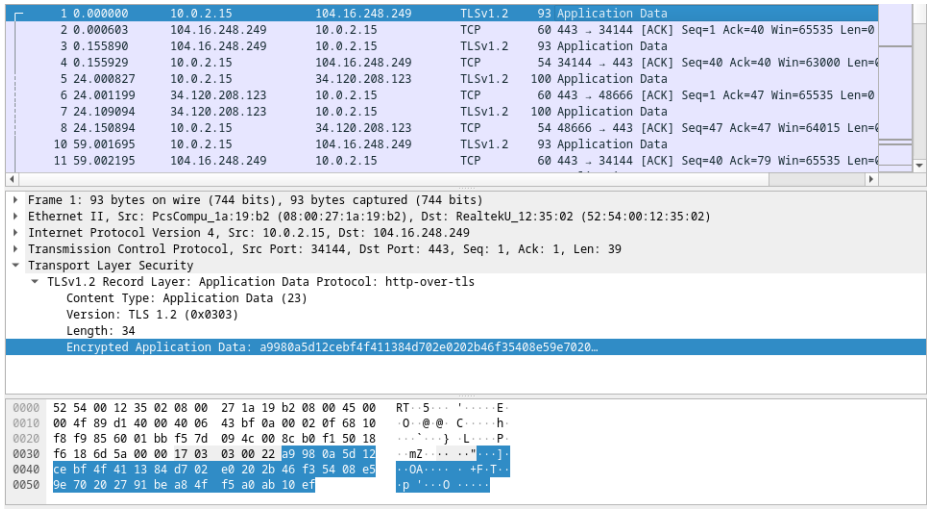
5. Logged in to Netacad



6. Filter TCP Port



7. Filter Result



V. Pembahasan

Pada praktikum ini dilakukan perekaman aktivitas HTTP dan HTTPS dan juga menganalisisnya. Menggunakan command tcpdump, dapat dibuat file pcap yang bisa dibuka menggunakan Wireshark. Untuk file hasil rekam HTTP yaitu httpdump.pcap, dapat dilihat pada POST bahwa UID dan password yang digunakan untuk login pada website HTTP tidak terenkripsi atau terproteksi.

Pada file hasil rekam HTTPS yaitu httpsdump.pcap, terdapat beberapa application data dalam port tcp 443, namun di dalamnya tidak terdapat informasi tentang UID dan password, dan hanya terdapat encrypted application data.

Melihat hasil praktikum di atas, terlihat jelas perbedaan antara HTTP dan HTTPS. HTTPS mengamankan koneksi dengan protokol keamanan digital menggunakan kunci kriptografik untuk mengenkripsi dan memvalidasi data. Untuk menggunakan HTTPS dan mengamankan domain, diperlukan sertifikat SSL/TLS. Oleh karena itu, pada website yang memiliki credentials akun-akun pengguna, HTTPS merupakan pilihan yang wajib untuk digunakan.