

Praktikum 13

ANALISA PAKET DENGAN WIRESHARK & TCPDUMP

A. TUJUAN PEMBELAJARAN

1. Siswa mampu melakukan sniffing dengan wireshark dan tcpdump dan tahu keuntungan dan kelemahan kedua software tersebut
2. Siswa mampu melakukan analisa paket layer transport OSI (TCP dan UDP)
3. Siswa mampu melakukan analisa paket layer aplikasi Telnet dan SSH

B. DASAR TEORI

1. Sniffing

Menangkap atau mengendus(sniffing) trafik jaringan sangat berguna bagi administrator untuk menyelesaikan masalah-masalah yang muncul di jaringan, termasuk masalah keamanan. Hal ini berdasarkan fakta bahwa sejumlah penyerangan dimulai dengan penggunaan penyadap untuk melihat trafik jaringan dengan harapan melihat data-data penting yang ditransmisikan oleh user. Karena itu mempelajari kapabilitas dan keterbatasan software-software packet sniffing menjadi bagian yang penting dari kemampuan admin.

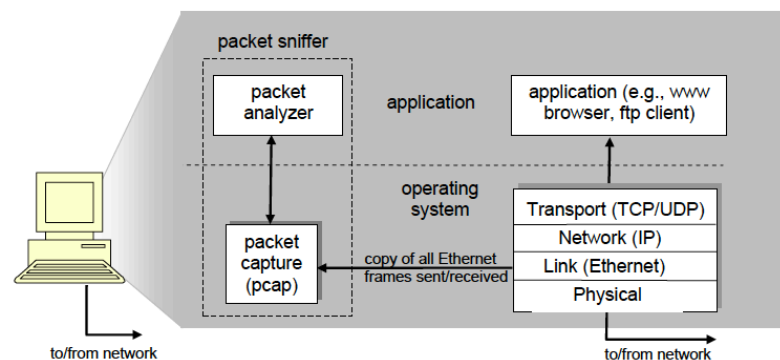


Gambar 13.1 Sniffing pada jaringan antara router 1 dan 2

Software Open Source Sniffing

Beberapa software open source yang digunakan untuk melakukan sniffing adalah :

1. TCP dump adalah tools UNIX/Linux yang banyak digunakan untuk merekam trafik jaringan berdasarkan kriteria user dan mampu menyimpan trafik dalam berbagai format yang berbeda. TCPdump umumnya digunakan pada kebanyakan distribusi linux dan dapat diperoleh di <http://www.tcpdump.org>.
2. Wireshark adalah aplikasi grafis yang banyak digunakan untuk monitoring dan analisis. Wireshark adalah opensource dan berjalan pada banyak platform OS termasuk Windows, Linux dan UNIX. Wireshark dapat didownload di <http://www.wireshark.org>.



Gambar 13.2 Blok Diagram Paket Sniffer

Bagaimana Sniffing Bekerja ?

Dalam menentukan bagaimana menyetting sniffer, topologi dan tipe jaringan harus menjadi pertimbangan. Secara lebih detail, perbedaan antara jaringan berbasis switch dan hub menjadi penentu trafik yang visible ketika sniffing dilakukan.

Ketika satu host butuh untuk berkomunikasi dengan host lain, host tersebut akan mengirim ARP request secara broadcast ke seluruh host dalam jaringan baik switch dan hub. Hanya host yang dicari akan menjawab dengan ARP reply yang berisi MAC address host tersebut. Pada jaringan berbasis switch, ketika komunikasi berjalan antara dua host, trafik diantaranya akan diisolasi oleh switch pada link fisik. Namun, pada jaringan berbasis hub, komunikasi antara kedua host dapat didengar oleh semua host yang lain pada jaringan tersebut, walaupun tidak diperhatikan.

Pasif dan Aktif Sniffing

Passive sniffing menempatkan NIC host pada mode promiscuous mode, yang artinya menangkap semua trafik yang dapat dilihat, termasuk trafik antara host yang berbeda terutama pada jaringan berbasis hub. Pada jaringan berbasis switch, passive sniffing dapat dilakukan pada switch yang melakukan SPAN atau mirror port dimana trafik secara dapat dikopikan dengan meletakkan sniffer pada port yang dimirror. Jika yang diinginkan adalah trafik yang masuk dan keluar jaringan, maka sniffer dapat diletakkan pada gateway.

Active Sniffing adalah alternative metode sniffing. Aktif sniffer mencoba mencari celah dari protocol ARP dengan melakukan ARP spoofing dengan menjawab request ARP dari host. Aktif sniffing secara aktif akan berusaha agar pemilik MAC address asli diabaikan atau dibuang dalam proses komunikasi antara host dan sniffer. Salah satu metode yang digunakan untuk active sniffing adalah MAC flooding.

2. Wireshark

Wireshark, atau dulunya dikenal sebagai Ethereal, adalah salah satu tool yang sangat ampuh untuk senjata para analis keamanan jaringan. Sebagai analyzer packet jaringan, Wireshark dapat berlaku sebagai peer di jaringan dan mengamati trafik secara detail dalam berbagai level, mulai dari header packet hingga bit yang menyusun suatu paket. Karena wireshark menggunakan GUI, banyak pengguna memperoleh kemudahan grafis dalam menggunakan informasi yang terkandung di dalamnya.

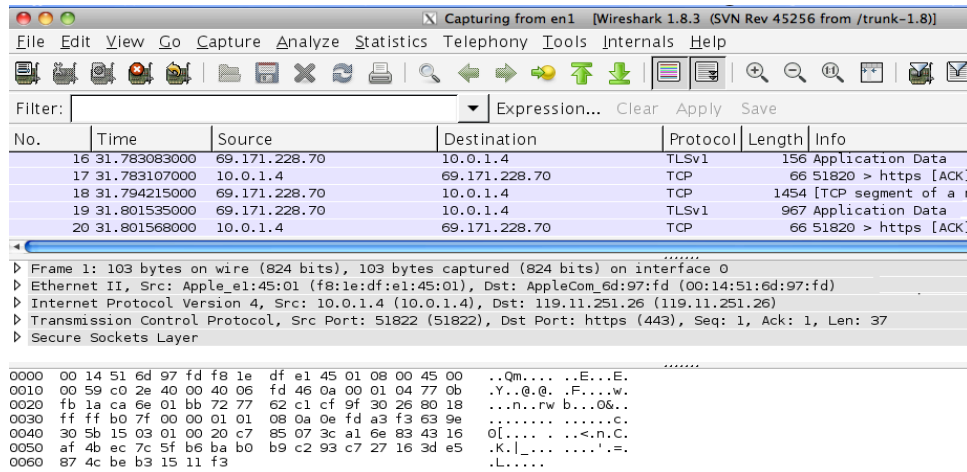
Pemakaian warna

Salah satu fitur dari wireshark adalah penggunaan warna. Untuk jenis-jenis paket yang berbeda Paket-paket di wireshark diberi highlight warna hijau, biru dan hitam. Secara default, hijau adalah warna yang digunakan untuk trafik TCP, biru muda adalah warna yang digunakan untuk trafik UDP dan hitam menunjukkan paket TCP yang bermasalah (misalnya karena dikirim secara tidak berurutan)

Menggunakan hasil capture Wireshark

Bila tidak ada paket yang menarik untuk diamati, Wireshark memiliki sejumlah file hasil

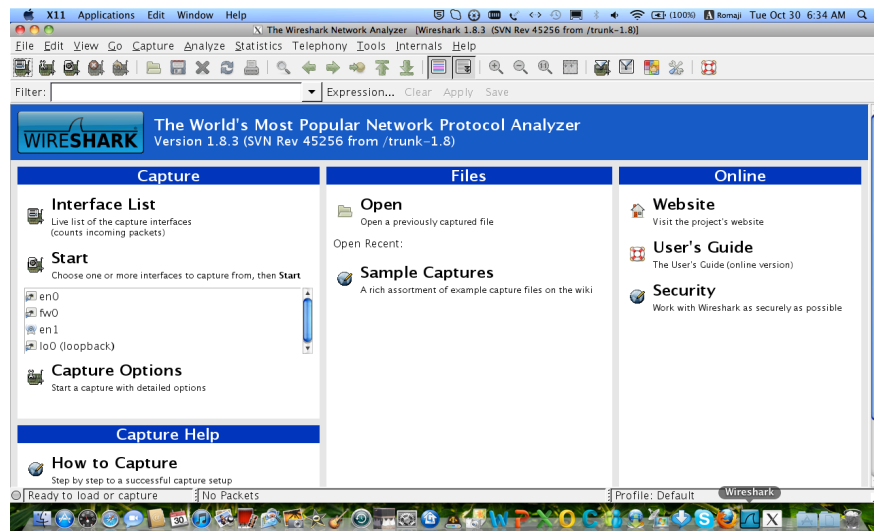
capture yang dapat di-load dan di-inspeksi oleh user. Untuk membuka filenya mudah. Buka menu utama dan browse file yang diinginkan.



Gambar 13.3 GUI dari wireshark

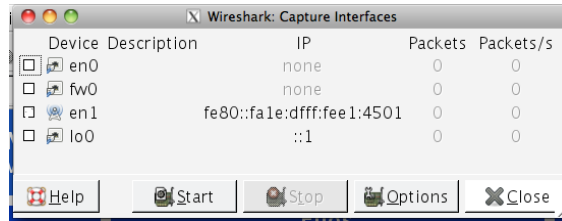
Cara Menjalankan Wireshark

1. Bukalah Wireshark



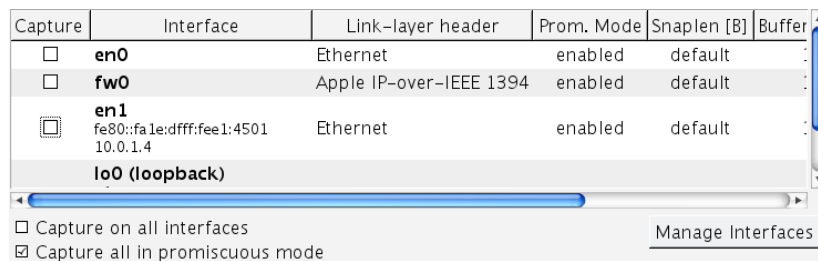
Gambar 13.4 Tampilan awal wireshark

2. Tentukan di interface mana wireshark berjalan. Pilih icon . Setelah itu akan muncul tampilan berikut :



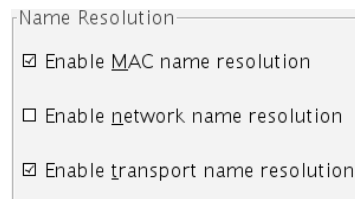
Gambar 13.5 Tampilan pilihan interface dimana wireshark beroperasi

- a. Pilih interface dimana anda melakukan sniffing.
- b. Pilih Option. Pilih Capture All in Promiscuous Mode



Gambar 13.6 Tampilan opsi capture

- c. Pada Name resolution, pilih dua opsi dari tiga, yaitu opsi enable MAC name resolution dan enable transport name resolution



Gambar 13.7 Tampilan Capture

3. Mulailah melakukan penangkapan packet. Pilih Start, pada tampilan Wireshark Capture Options
4. Akan muncul window seperti pada gambar 13.3 yang menunjukkan paket-paket yang ditangkap oleh wireshark pada subnet anda. Bagian yang paling atas, dibawah filter, disebut sebagai packet listing window. Bagian ini menunjukkan semua paket yang berhasil ditangkap oleh wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
16	31.783083000	69.171.228.70	10.0.1.4	TLSv1	156	Applicati
17	31.783107000	10.0.1.4	69.171.228.70	TCP	66	51820 > h
18	31.794215000	69.171.228.70	10.0.1.4	TCP	1454	[TCP segm
19	31.801535000	69.171.228.70	10.0.1.4	TLSv1	967	Applicati
20	31.801568000	10.0.1.4	69.171.228.70	TCP	66	51820 > h

Gambar 13.8 Packet Listing Window

Bagian kedua adalah packet detail window, yang menunjukkan informasi paket secara detail. Detail packet window ini membedah paket dan menunjukkan field-field dari tiap layer, mulai dari Frame 1, Ethernet II, IPv4, TCP/UDP, dan aplikasi layer (SSH, Telnet, HTTP, dll)

```

*****
> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
> Ethernet II, Src: Apple_e1:45:01 (f8:1e:df:e1:45:01), Dst: AppleCom_6d:97:fd (00:14:51:6d:97:fd)
> Internet Protocol Version 4, Src: 10.0.1.4 (10.0.1.4), Dst: 119.11.251.26 (119.11.251.26)
> Transmission Control Protocol, Src Port: 51822 (51822), Dst Port: https (443), Seq: 1, Ack: 1, Len: 37
> Secure Sockets Layer

```

Gambar 13.9 Packet Detail Window

Bagian terakhir adalah packet content window yang berisi isi dari paket tersebut. Biasanya ditulis dalam hexa dan ascii.

```

0000  00 14 51 6d 97 fd f8 1e df e1 45 01 08 00 45 00  ..Qm.... ..E...E.
0010  00 59 c0 2e 40 00 40 06 fd 46 0a 00 01 04 77 0b  .Y..@.@. .F....w.
0020  fb 1a ca 6e 01 bb 72 77 62 c1 cf 9f 30 26 80 18  ...n...rw b...0&..
0030  ff ff b0 7f 00 00 01 01 08 0a 0e fd a3 f3 63 9e  .....C.
0040  30 5b 15 03 01 00 20 c7 85 07 3c a1 6e 83 43 16  0[.... . .<.n.C.

```

Gambar 13.10 Packet Content Window

5. Stoplah penangkapan paket bila anda telah mendapatkan paket yang dibutuhkan

dengan memilih

