

Tugas UAS Keamanan Informasi
Telekomunikasi dan keamanan jaringan



Nama : Sugiono Heri Saputro

Nim : 1310651053

Kls: C

UNIVERSITAS MUHAMMADIYAH JEMBER
FAKULTAS TEKNIK INFOMATIKA

2014-2015

Perangkat telekomunikasi bertugas menghubungkan pemakainya dengan pemakai lain. Kedua pemakai ini bisa berdekatan tetapi bisa berjauhan. Kalau memiliki arti harfiah dari telekomunikasi (tele = jauh, komunikasi = hubungan dengan pertukaran informasi) memang teknik telekomunikasi dikembangkan manusia untuk menebus perbedaan jarak yang jauhnya bisa tak terbatas menjadi perbedaan waktu yang sekecil mungkin.

Telecommunications and Network Security atau telekomunikasi dan keamanan jaringan Model OSI, Dan Kemudian setelah Anda mendapatkan ke bawah dan Anda tahu perangkat jaringan yang beroperasi pada tingkat yang, Anda dapat beralih gigi dan pergi ke model TCP / IP. Model TCP / IP adalah NITA (Sekarang Ini Benar-benar hebat). Dalam itu bukan "butuh" (seperti dalam minuman) itu NITA atau Network, Internet, Transportasi dan Aplikasi. Jadi, inilah perbandingan: Dan ingat, Anda perlu tahu mana perangkat jaringan beroperasi pada lapisan yang,

Untuk TCP / IP Anda perlu memahami IPv4. Tahu Alamat Swasta, sudah ada tiga dari Mereka. Dan Anda harus tahu keuntungan dari IPv6. Jadi pertanyaan trik, karena rentang alamat dari oktet Dalam IPv4 skema pengalamatan adalah 0-254; 10.10.10.255 adalah alamat IP yang valid dan jika Anda mengatakan ya, maka apa yang akan dipergunakan untuk? Dalam IPv6 apa "::" mewakili. Jawabannya = apa-apa. Sebenarnya itu nol. Tapi perbedaan yang sama.

Anda seharusnya memahami perbedaan antara Analog dan Digital komunikasi; Asynchronous dan Synchronous antara; dan antara broadband dan baseband. Berbicara tentang komunikasi analog, apa kelemahan utama menggunakan modem yaitu Mereka dapat digunakan untuk menghindari firewall dan perangkat IDS / IPS.

Untuk percakapan wilayah jaringan, Anda perlu mengetahui istilah tradisional LAN, WAN, MAN, PAN, WLAN, PWLAN, dll Anda juga harus mengetahui konfigurasi BUS, STAR, RING, dan MESH. Sebuah pertanyaan yang baik adalah dalam konfigurasi yang akan Anda menemukan Hub Paling Mungkin.

Dan berbicara tentang hub, mari kita bicara sedikit tentang perangkat yang berbeda Anda boleh berada di berbicara berdamai dengan. Yaitu Mereka hub, switch, repeater, jembatan, gateway, PBX, firewall dan honeypots hanya untuk beberapa nama. Anda harus mencari di bulan Oktober Mana yang hanya maju semua lalu lintas; Mana yang penyaring lalu lintas berdasarkan alamat MAC dan yang mana yang paling mudah untuk hack.

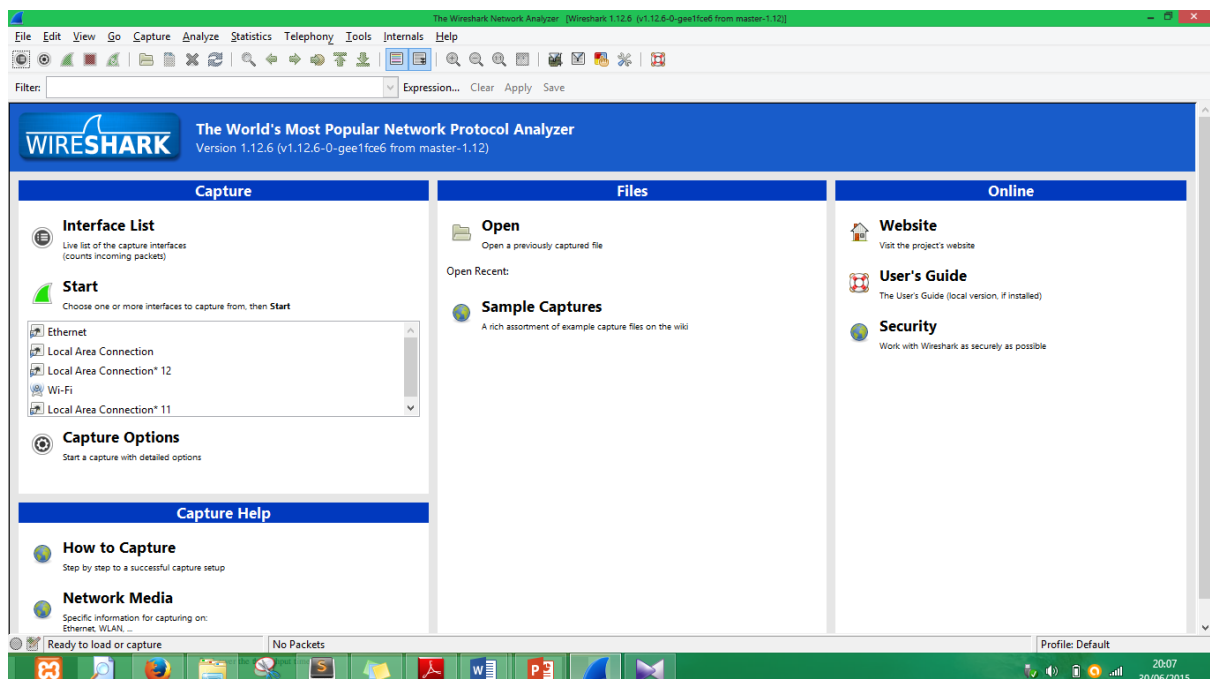
Dalam beberapa layanan dan protokol, memeriksa DNS, Terutama membaca rincian di belakang zona transfer dan Bagaimana Mereka bekerja. Kemudian melihat DHCP, layanan Active Directory, LDAP dan Kerberos. Bayar perhatian khusus untuk port yang dan menggunakan Kerberos Yang protokol yang digunakan untuk berkomunikasi antara klien dan Kerberos.

Remote akses semakin banyak perhatian dari (ISC) 2, sehingga membayar perhatian khusus pada bagaimana RADIUS mengotentikasi, mengapa ISDN (Ini masih tidak apa-apa) bukanlah pilihan yang baik, mengapa VPN dengan cepat Menjadi fakta bahwa standar untuk remote aman modem komunikasi dan mengapa tidak boleh pernah diizinkan di jaringan Anda.

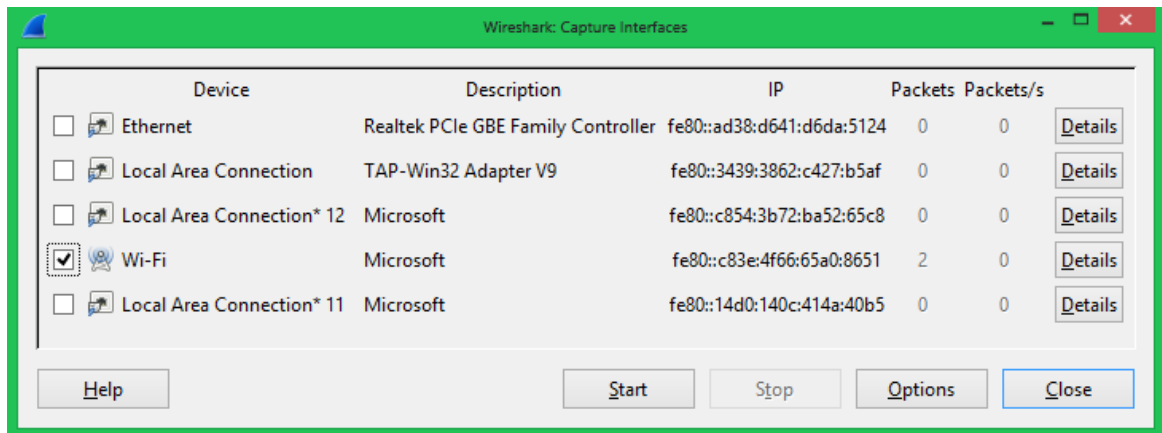
Wireless, ah nirkabel. Ini di mana-mana. Sebagian besar pendirian mengiklankan "GRATIS WIFI" Dan masing-masing tim profesional keamanan melihat que Mereka merasa ngeri, itu seperti menggantung tanda di leher Anda katakan di sini adalah userid dan password mandat. Tapi serius, mari kita lihat beberapa topik Anda harus Menjadi akrab dengan untuk ujian. Jadi untuk daftar cucian dari akronim, WEP, WPA, WPA2, 801.x (dan segala bentuk 801-802,11 termasuk A, B, G, N, I) dan jangan lupa SSID. Jangan SSID broadcast. Itu jawabannya, Anda hanya perlu ingat Ketika Anda sampai ke pertanyaan pada ujian. Anda juga harus memahami wardriving dan wardialing dan udara sniffing. Oh, dan sebelum aku lupa, biarkan aku menjawab dengan Blackberry dengan earphone remote menggunakan Bluetooth. Beberapa pertanyaan yang muncul di Bluetooth termasuk BlueScanner dan bluesniffer. Aku bahkan melihat beberapa pertanyaan pada versi terbaru yang lebih Yang menangani komunikasi nirkabel Apple untuk iPad dan lain lain.

No 2. Login ke elearning.unmuhjember.ac.id

Langkah pertama buka aplikasi wireshark seperti gambar di bawah ini



Pilih aplikasi wi-fi lalu pilih star seperti tampilan gambar di bawah ini



Buka web yang akan di coba seperti contoh : elearning.unmuhjember.ac.id

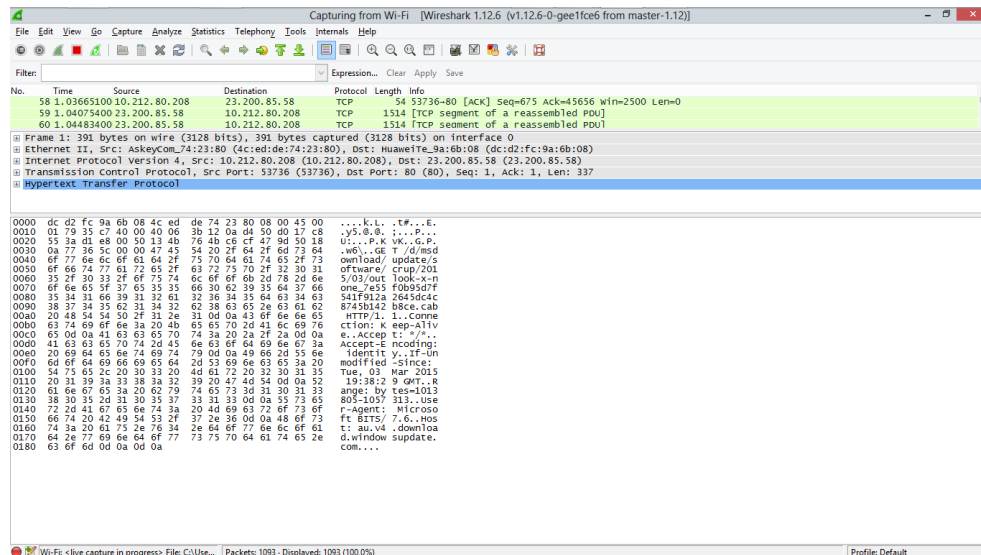


Tampilan seperti di bawah ini

Masukkan username dan kata sandi lalu login seperti biasa...

Ketika Selesai LOGIN, STOP Wreshark

Lihat Ipnnya melalui cmd



```
e'learning' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Fuad>ping e'learning.unmuhjember.ac.id
Ping request could not find host e'learning. Please check the name and try again.

C:\Users\Fuad>ping elearning.unmuhjember.ac.id
Ping request could not find host elearning. Please check the name and try again.

C:\Users\Fuad>ping elearning.unmuhjember.ac.id

Pinging elearning.unmuhjember.ac.id [118.97.237.109] with 32 bytes of data:
Reply from 118.97.237.109: bytes=32 time=28ms TTL=61
Reply from 118.97.237.109: bytes=32 time=15ms TTL=61
Reply from 118.97.237.109: bytes=32 time=17ms TTL=61
Reply from 118.97.237.109: bytes=32 time=10ms TTL=61

Ping statistics for 118.97.237.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 28ms, Average = 17ms

C:\Users\Fuad>
```

ip.dst=="118.97.237.109"

Filter ip nya dengan kode "ip.dst=="alamat IP"

Cari di info yg ada login.phpnya

Lihat di HTML Form URL Decoded

Capturing from Wi-Fi [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.dst==118.97.237.109 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
20	7.881549000	192.168.43.179	118.97.237.109	TCP	65	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
21	7.771617000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57512-80 [ACK] Seq=1 Ack=1 Win=60
22	7.931632000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57510-80 [ACK] Seq=1 Ack=1 Win=60
43	18.754058000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
44	18.754352000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
45	18.764110000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57510-80 [ACK] Seq=1 Ack=1 Win=60
46	19.755065000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57512-80 [ACK] Seq=1 Ack=1 Win=60
47	19.755348000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
48	19.765045000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57510-80 [ACK] Seq=1 Ack=1 Win=60
49	20.755477000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57512-80 [ACK] Seq=1 Ack=1 Win=60
50	20.755670000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
51	20.765495000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57510-80 [ACK] Seq=1 Ack=1 Win=60
53	21.762602000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57512-80 [ACK] Seq=1 Ack=1 Win=60
54	21.762760000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
55	21.772602000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57510-80 [ACK] Seq=1 Ack=1 Win=60
72	29.422193000	192.168.43.179	118.97.237.109	HTTP	677	POST /login/index.php?authldap_skipntlmssw=1 HTTP/1.1
73	29.912166000	192.168.43.179	118.97.237.109	HTTP	677	TCP Retransmission) POST /login/index.php?authldap
76	30.744928000	192.168.43.179	118.97.237.109	HTTP	677	TCP Retransmission) POST /login/index.php?authldap
77	31.855123000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57512-80 [ACK] Seq=1 Ack=1 Win=60
78	31.855294000	192.168.43.179	118.97.237.109	TCP	55	[TCP Keep-Alive] 57511-80 [ACK] Seq=1 Ack=1 Win=60
79	31.855167000	192.168.43.179	118.97.237.109	TCP	55	[TCP Retransmission] 57510-80 [ACK] Seq=1 Ack=1 Win=60
84	32.000181000	192.168.43.179	118.97.237.109	TCP	66	57510-80 [ACK] Seq=613 Ack=1389 Win=64 Len=0 TSval=
87	32.130927000	192.168.43.179	118.97.237.109	TCP	66	57510-80 [ACK] Seq=613 Ack=4165 Win=64 Len=0 TSval=
88	32.208112000	192.168.43.179	118.97.237.109	HTTP	568	GET /user/plx.php?f11e=0/f1.jpg HTTP/1.1
89	32.247899000	192.168.43.179	118.97.237.109	HTTP	565	GET /theme/sawahid/images/menu/dategrad.png HTTP/1.1
90	32.267899000	192.168.43.179	118.97.237.109	HTTP	565	GET /theme/sawahid/images/menu/dategrad.png HTTP/1.1

< >

Frame 72: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface 0

- Ethernet II, Src: IntelCor_45:56:90 (00:1c:bf:45:56:90), Dst: SamsungE_27:3f:3a (3c:a1:0d:27:3f:3a)
- Internet Protocol Version 4, Src: 192.168.43.179 (192.168.43.179), Dst: 118.97.237.109 (118.97.237.109)
- Transmission Control Protocol, Src Port: 57510 (57510), Dst Port: 80 (80), Seq: 2, Ack: 1, Len: 611

```

0000  3c a1 0d 27 3f 3a 00 1c bf 45 56 90 08 00 45 00  <..?...EV...E.
0010  02 97 40 c0 40 00 00 06 47 80 c0 88 2b 02 76 61  .....GK...VA
0020  e0 e0 e0 a6 00 50 87 eb 8a 40 23 10 12 48 80 18  .m...P...@...
0030  00 3c 43 a4 00 00 01 01 08 0a 09 41 03 c7 1a 94  <C.....A...
0040  38 81 50 4f 53 54 20 2f 8c 8f 67 69 6e 2f 89 64  8.POP/ /login/in
0050  64 65 78 7e 70 68 70 3f 61 75 74 68 6c 64 61 70  dex.php?authldap

```

Wi-Fi - live capture in progress File C:\Use... Packets: 1033 - Displayed: 100 (5.4%) Profile Teruskan Unduh

Maka akan terlihat passwordnya

Inilah yg dinamakan sniffing....

ALHAMDULILAH,,