

Monitoring Telnet

Ainul Fuad Farhan

inungf@ymail.com

http://inungandthenotes.blogspot.com

Lisensi Dokumen:

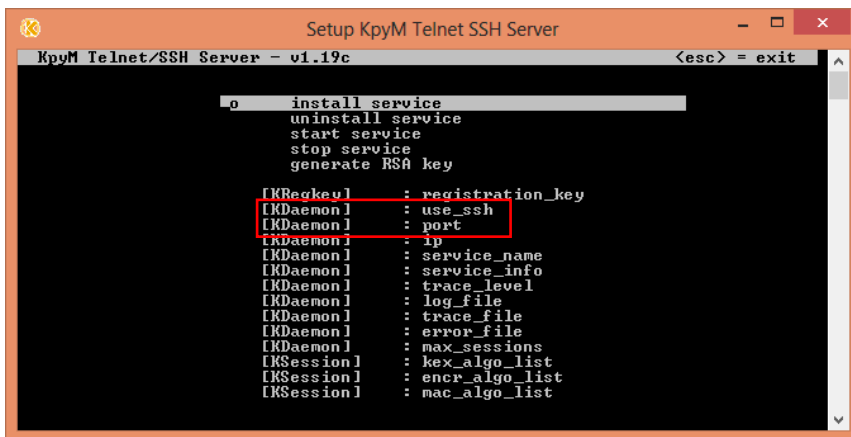
Copyright © 2003-2013 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

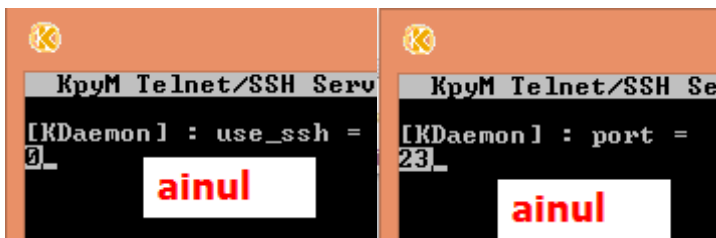
Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

Telnet berisikan perintah user yang berdasarkan protokol TCP/IP untuk mengakses komputer dari jarak jauh (remote). Melalui Telnet, administrator atau user lain dapat mengakses komputer dari jarak jauh. Pada Web, kita dapat menggunakan protokol HTTP dan FTP untuk mengakses komputer jarak jauh, tetapi hanya login seperti user biasa sesuai dengan hak akses yang telah di set pada komputer yang dituju.

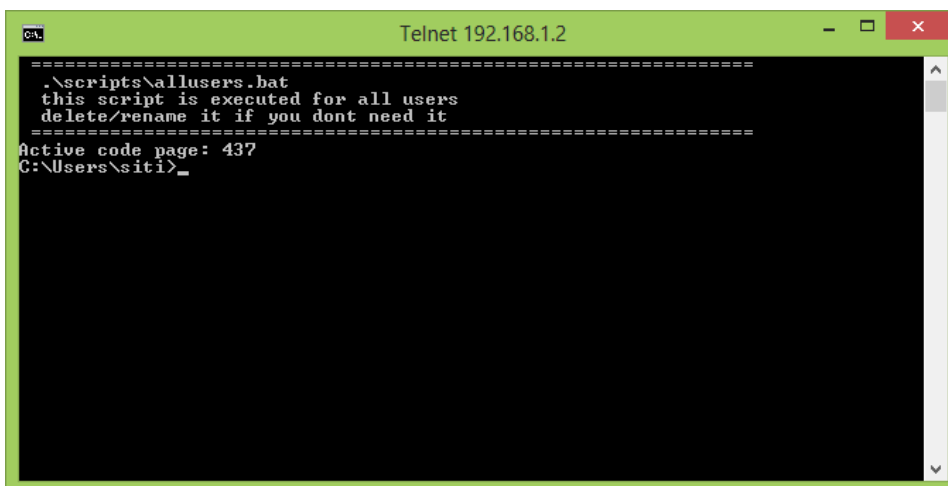
Dengan menggunakan telnet kita mampu melakukan *remote* ke *directory* komputer lain, tentunya dengan mengetahui *user* dan *password* dari komputer yang kita tuju tersebut. Namun pada perangkat seperti laptop dan komputer kita memerlukan bantuan dari aplikasi lain guna menjadikan port dari telnet itu berfungsi, salah satu aplikasi yang digunakan adalah **kts119c**.



Dengan melakukan konfigurasi pada `use_ssh` dan `port` di atas kita memanfaatkan port 23 sebagai protokol Telnet.



Dengan melakukan konfigurasi seperti di atas pada kedua laptop/komputer, berlangsunglah Telnet antara kedua perangkat. Berikut merupakan contoh dari telnet yang dilakukan dari laptop yang memiliki IP Address 192.168.1.10 ke 19.168.1.2 (Siti).



Nah dari telnet yang telah berhasil tersebut, ada protokol-protokol yang berlalu lalang, seperti biasa kita menggunakan Wireshark guna melakukan *capture* protokol yang berlalu lalang tadi.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Fe80::2405:F348:6ad5:592	ff02::1:2	DHCPv6	137	solicit XID: 0x86f960 CID: 0001000114dfde75f0def110b650
2	1.00193600	Fe80::2405:F348:6ad5:592	ff02::1:2	DHCPv6	137	solicit XID: 0x86f960 CID: 0001000114dfde75f0def110b650
3	3.01595200	Fe80::2405:F348:6ad5:592	ff02::1:2	DHCPv6	137	solicit XID: 0x86f960 CID: 0001000114dfde75f0def110b650
4	7.02351200	Fe80::2405:F348:6ad5:592	ff02::1:2	DHCPv6	137	solicit XID: 0x86f960 CID: 0001000114dfde75f0def110b650
5	7.19075400	Asustekc_fd:85:f1	Broadcast	ARP	42	who has 192.168.1.2? Tell 192.168.1.10
6	7.19109100	WistronI_10:b6:50	Asustekc_fd:85:f1	ARP	60	192.168.1.2 is at f4:6d:04:fd:85:f1
7	7.19103600	192.168.1.10	192.168.1.2	TCP	74	mini-sql > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=234875
8	7.19161700	wistronI_10:b6:50	Broadcast	ARP	60	who has 192.168.1.10? Tell 192.168.1.2
9	7.19166900	Asustekc_fd:85:f1	wistronI_10:b6:50	ARP	42	192.168.1.10 is at f4:6d:04:fd:85:f1
10	7.19198100	192.168.1.2	192.168.1.10	TCP	74	telnet > mini-sql [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TS
11	7.19230700	192.168.1.10	192.168.1.2	TCP	66	mini-sql > telnet [ACK] Seq=1 Ack=1 Win=66560 Len=0 TSval=234875 TSecr=234512
12	9.31435500	192.168.1.2	192.168.1.10	TELNET	75	Telnet data ...
13	9.31509500	192.168.1.10	192.168.1.2	TELNET	69	Telnet data ...

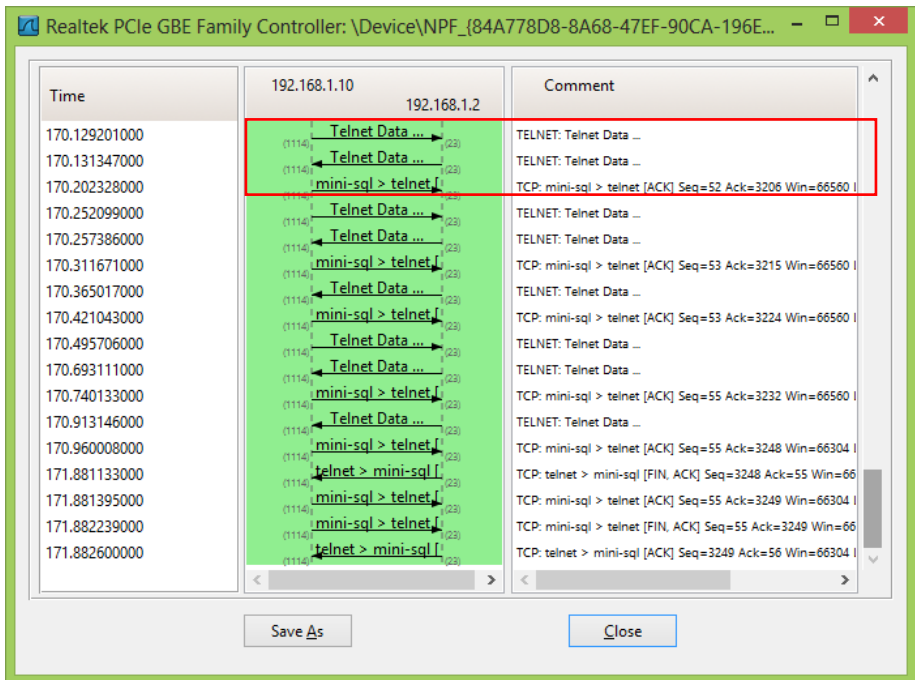
Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: WistronI_10:b6:50 (f0:de:f1:10:b6:50), Dst: Asustekc_fd:85:f1 (f4:6d:04:fd:85:f1)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IP (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 Sender MAC address: wistronI_10:b6:50 (f0:de:f1:10:b6:50)
 Sender IP address: 192.168.1.2 (192.168.1.2)
 Target MAC address: Asustekc_fd:85:f1 (f4:6d:04:fd:85:f1)
 Target IP address: 192.168.1.10 (192.168.1.10)

ainul

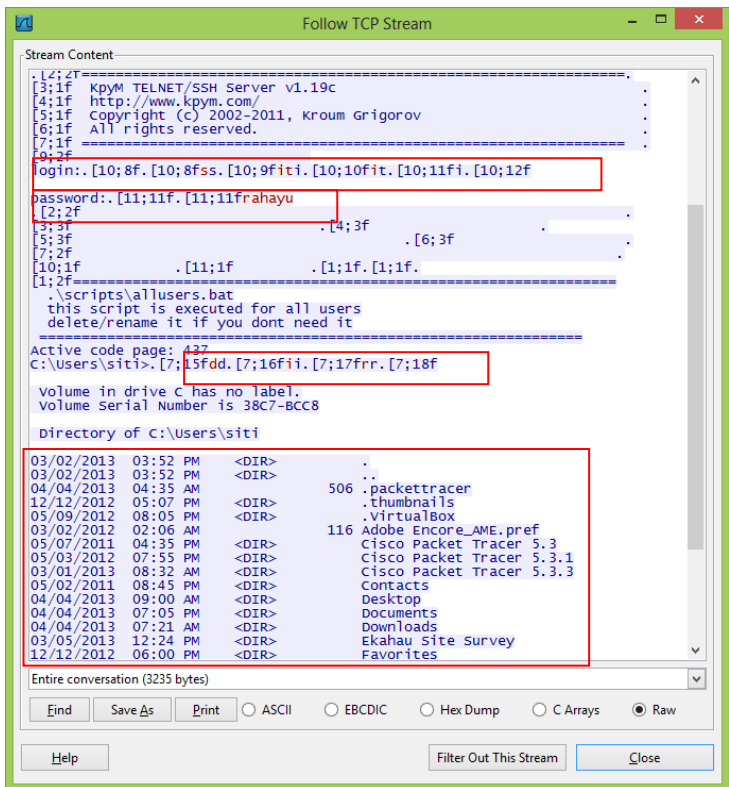
Dari beberapa protokol frame di atas terlihat bahwa Laptop dengan IP Add 192.168.1.10 sedang mengirim ARP dulu untuk melakukan **3Ways Handshaking** ketika akan melakukan *log in* ke laptop dengan IP Add 192.168.1.2, yang berisi [SYN], [SYN ACK], dan [ACK].

Time	192.168.1.10	192.168.1.2	Comment
7.191036000	mini-sql > telnet		TCP: mini-sql > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=
7.191941000	telnet > mini-sql		TCP: telnet > mini-sql [SYN, ACK] Seq=0 Ack=1 Win=8192 L
7.192307000	mini-sql > telnet		TCP: mini-sql > telnet [ACK] Seq=1 Ack=1 Win=66560 Len=
9.314355000	telnet Data ...		TELNET: Telnet Data ...
9.315095000	Telnet Data ...		TELNET: Telnet Data ...
9.315881000	Telnet Data ...		TELNET: Telnet Data ...
9.316095000	Telnet Data ...		TELNET: Telnet Data ...
9.316361000	Telnet Data ...		TELNET: Telnet Data ...
9.316361000	mini-sql > telnet		TCP: mini-sql > telnet [ACK] Seq=19 Ack=45 Win=66560 Len=
9.411793000	Telnet Data ...		TELNET: Telnet Data ...
9.412429000	Telnet Data ...		TELNET: Telnet Data ...
9.521155000	Telnet Data ...		TELNET: Telnet Data ...
9.581639000	mini-sql > telnet		TCP: mini-sql > telnet [ACK] Seq=28 Ack=63 Win=66304 Len=
10.395871000	Telnet Data ...		TELNET: Telnet Data ...
10.440443000	mini-sql > telnet		TCP: mini-sql > telnet [ACK] Seq=28 Ack=481 Win=66048 L
11.379346000	Telnet Data ...		TELNET: Telnet Data ...
11.439118000	mini-sql > telnet		TCP: mini-sql > telnet [ACK] Seq=28 Ack=503 Win=66048 L

Ketika laptop akan *log out* dari Telnet maka akan ditutup dengan **3Ways Handshaking** yang berisi seperti berikut.



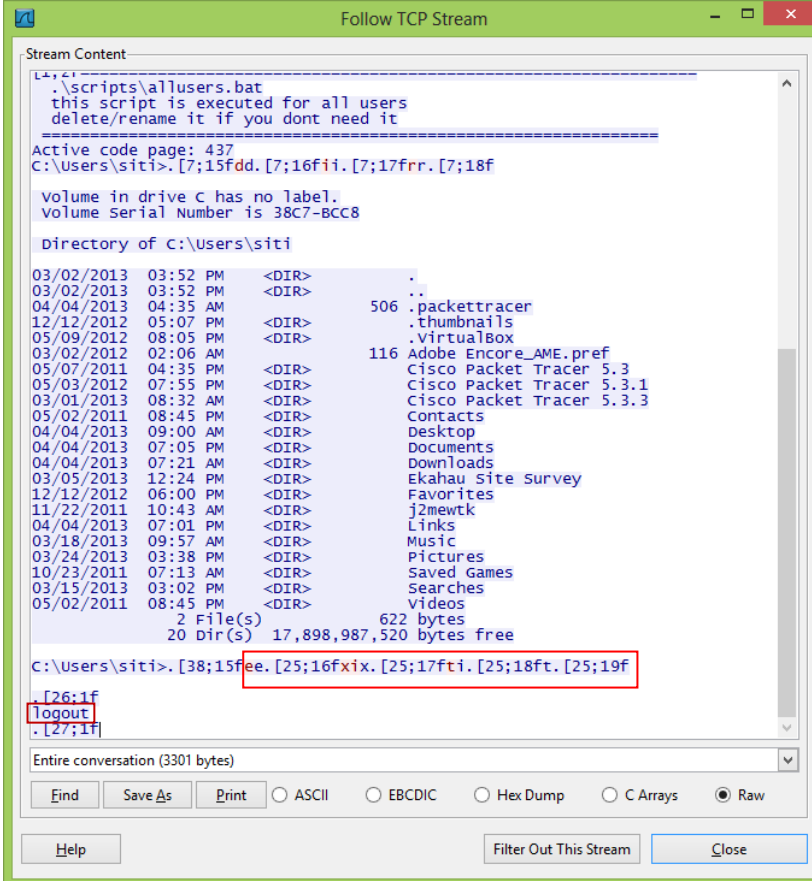
Itu tadi merupakan *capture* bagaimana 3ways handshaking ketika Laptop melakukan *log in* dan *log out*. Nah, ada lagi yang tercapture, yaitu *user* dan *password* dari laptop yang ditelnet beserta isi direktori. Dengan kita melakukan “Follow TCP Stream” pada salah satu protokol TCP yang ada pada frame yang tercapture Wireshark. Hasilnya adalah sebagai berikut.



Dari “Flow Graph” tersebut terlihat *user login* yang digunakan adalah *siti* dan *password login*

yang digunakan adalah **rahayu**. Perintah cmd yang digunakan adalah **dir**. Terlihat bahwa directory dari laptop tersebut berisi packettracer, virtualbox, cisco packet tracer, dsb.

Beda lagi “Flow Graph” yang ditampilkan ketika melakukan *logout*.



```
Follow TCP Stream
Stream Content
L4, L4
.\scripts\allusers.bat
this script is executed for all users
delete/rename it if you dont need it
-----
Active code page: 437
C:\Users\siti>. [7;15fdd. [7;16fii. [7;17frr. [7;18f
Volume in drive C has no label.
Volume Serial Number is 38C7-BCC8

Directory of C:\Users\siti

03/02/2013 03:52 PM <DIR> .
03/02/2013 03:52 PM <DIR> ..
04/04/2013 04:35 AM <DIR> 506 .packettracer
12/12/2012 05:07 PM <DIR> .thumbnails
05/09/2012 08:05 PM <DIR> .virtualBox
03/02/2012 02:06 AM <DIR> 116 Adobe Encore_AME.pref
05/07/2011 04:35 PM <DIR> Cisco Packet Tracer 5.3
05/03/2012 07:55 PM <DIR> Cisco Packet Tracer 5.3.1
03/01/2013 08:32 AM <DIR> Cisco Packet Tracer 5.3.3
05/02/2011 08:45 PM <DIR> Contacts
04/04/2013 09:00 AM <DIR> Desktop
04/04/2013 07:05 PM <DIR> Documents
04/04/2013 07:21 AM <DIR> Downloads
03/05/2013 12:24 PM <DIR> Ekahau Site Survey
12/12/2012 06:00 PM <DIR> Favorites
11/22/2011 10:43 AM <DIR> j2mewtk
04/04/2013 07:01 PM <DIR> Links
03/18/2013 09:57 AM <DIR> Music
03/24/2013 03:38 PM <DIR> Pictures
10/23/2011 07:13 AM <DIR> Saved Games
03/15/2013 03:02 PM <DIR> Searches
05/02/2011 08:45 PM <DIR> Videos
                2 File(s)          622 bytes
                20 Dir(s)      17,898,987,520 bytes free

C:\Users\siti>. [38;15fee. [25;16fix. [25;17fti. [25;18ft. [25;19f
. [26;1f
logout
. [27;1f

Entire conversation (3301 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

Perintah yang dilakukan untuk *logout* adalah **exit**.

Nah begitulah monitoring pada Telnet menggunakan Wireshark.

Terimakasih, semoga bermanfaat.

Referensi:

- http://www.dq-online.com/index.php?option=com_content&view=article&id=68:telnet&catid=50:network&Itemid=64
- <http://id.wikipedia.org/wiki/Telnet>



Biografi Penulis

Ainul Fuad Farhan. Mahasiswa Politeknik Negeri Semarang Jurusan Teknik Elektro, Prodi D4 Telekomunikasi. Alumni SMA N 1 JUWANA tahun 2010.

Contact Person :

Blog : <http://inungandthenotes.blogspot.com>

Facebook : lukazkazx@yahoo.com

Twitter : @inungf