

Cuestiones seminario 1

por: Arturo Cortés Sánchez

Actividad 1: Hacer capturas de telnet y ssh con wireshark entre las dos máquinas virtuales ¿podemos sacar información de los paquetes telnet?

eth0 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
80	2.926777	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
81	2.926785	10.0.2.5	10.0.2.4	TELNET	67	Telnet Data ...
82	2.926792	10.0.2.4	10.0.2.5	TCP	66	53390 > telnet [ACK] Seq=126 Ack=103 Win=14720 Len=0 TSval=...
83	3.158686	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
84	3.158964	10.0.2.5	10.0.2.4	TELNET	67	Telnet Data ...
85	3.158973	10.0.2.4	10.0.2.5	TCP	66	53390 > telnet [ACK] Seq=127 Ack=104 Win=14720 Len=0 TSval=...
86	3.398793	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
87	3.398987	10.0.2.5	10.0.2.4	TELNET	67	Telnet Data ...
88	3.398994	10.0.2.4	10.0.2.5	TCP	66	53390 > telnet [ACK] Seq=128 Ack=105 Win=14720 Len=0 TSval=...
89	3.704482	10.0.2.4	10.0.2.5	TELNET	68	Telnet Data ...
90	3.706162	10.0.2.5	10.0.2.4	TELNET	78	Telnet Data ...
91	3.706186	10.0.2.4	10.0.2.5	TCP	66	53390 > telnet [ACK] Seq=130 Ack=117 Win=14720 Len=0 TSval=...
92	5.064245	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
93	5.103533	10.0.2.5	10.0.2.4	TCP	66	telnet > 53390 [ACK] Seq=117 Ack=131 Win=14592 Len=0 TSval=...
94	5.240216	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
95	5.240695	10.0.2.5	10.0.2.4	TCP	66	telnet > 53390 [ACK] Seq=117 Ack=132 Win=14592 Len=0 TSval=...
96	5.519318	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
97	5.519450	10.0.2.5	10.0.2.4	TCP	66	telnet > 53390 [ACK] Seq=117 Ack=133 Win=14592 Len=0 TSval=...
98	5.687253	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
99	5.687435	10.0.2.5	10.0.2.4	TCP	66	telnet > 53390 [ACK] Seq=117 Ack=134 Win=14592 Len=0 TSval=...

Frame 83: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)

Ethernet II, Src: CadmusCo_e5:97:03 (08:00:27:e5:97:03), Dst: CadmusCo_17:b6:43 (08:00:27:17:b6:43)

Internet Protocol Version 4, Src: 10.0.2.4 (10.0.2.4), Dst: 10.0.2.5 (10.0.2.5)

Transmission Control Protocol, Src Port: 53390 (53390), Dst Port: telnet (23), Seq: 126, Ack: 103, Len: 1

Telnet

Data: n

```
0000 08 00 27 17 b6 43 08 00 27 e5 97 03 08 00 45 10  ..'.C.. '.....E.
0010 00 35 3e 2f 40 00 40 06 e4 7b 0a 00 02 04 0a 00  .5>/@.@. {. ....
0020 02 05 d0 8e 00 17 e4 e4 59 16 9f 23 9d 27 80 18  .....Y..#.'..
0030 00 73 18 30 00 00 01 01 08 0a 00 04 69 9b 00 04  .s. ....i...
0040 63 5b 6e                                     c[n
```

File: "/tmp/wireshark_eth0_20170... Packets: 196 Displayed: 196 Marked: 0 Dropped: 0 Profile: Default

Si, se puede ver el usuario, la contraseña y cualquier comando que se envíe, así como la respuesta.

En la captura se puede ver un ejemplo de carácter perteneciente al login introducido.

eth0 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
81	6.359924	fe80::a00:27ff:fe17:b1ff02::fb	10.0.2.5	MDNS	99	Standard query A FR-VirtualBox.local, "QM" question
82	6.359969	10.0.2.5	224.0.0.251	MDNS	79	Standard query A FR-VirtualBox.local, "QM" question
83	6.360377	10.0.2.4	224.0.0.251	MDNS	89	Standard query response A, cache flush 10.0.2.4
84	6.546097	10.0.2.5	10.0.2.4	TELNET	118	Telnet Data ...
85	6.546110	10.0.2.4	10.0.2.5	TCP	66	53418 > telnet [ACK] Seq=142 Ack=972 Win=16768 Len=0 TSval=
86	7.361607	10.0.2.4	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
87	7.361914	10.0.2.5	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
88	7.362231	192.168.1.1	10.0.2.4	DNS	108	Standard query response A 162.213.33.133 A 162.213.33.164
89	7.362428	192.168.1.1	10.0.2.5	DNS	108	Standard query response A 162.213.33.133 A 162.213.33.164
90	7.596512	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
91	7.596921	10.0.2.5	10.0.2.4	TELNET	67	Telnet Data ...
92	7.596935	10.0.2.4	10.0.2.5	TCP	66	53418 > telnet [ACK] Seq=143 Ack=973 Win=16768 Len=0 TSval=
93	7.843329	10.0.2.4	10.0.2.5	TELNET	67	Telnet Data ...
94	7.843506	10.0.2.5	10.0.2.4	TELNET	67	Telnet Data ...
95	7.843515	10.0.2.4	10.0.2.5	TCP	66	53418 > telnet [ACK] Seq=144 Ack=974 Win=16768 Len=0 TSval=
96	8.459927	10.0.2.4	10.0.2.5	TELNET	68	Telnet Data ...

Frame 97: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits)

Ethernet II, Src: CadmusCo_17:b6:43 (08:00:27:17:b6:43), Dst: CadmusCo_e5:97:03 (08:00:27:e5:97:03)

Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)

Transmission Control Protocol, Src Port: telnet (23), Dst Port: 53418 (53418), Seq: 974, Ack: 146, Len: 241

Telnet

Data: \r\n

Data: \033[0m\033[01;34mDescargas\033[0m \033[01;34mEscritorio\033[0m hola \033[01;34mImágenes\033[0m original \033[01;34mMúsica\033[0m \033[01;34mPlantillas\033[0m \033[01;34mVideos\033[0m

Data: \033[01;34mDocumentos\033[0m examples.desktop hola2 \033[01;34mMúsica\033[0m \033[01;34mPlantillas\033[0m \033[01;34mVideos\033[0m

File: "/tmp/wireshark_eth0_20170..." Packets: 100 Displayed: 100 Marked: 0 Dropped: 0 Profile: Default

Ejemplo de respuesta a ls en
/home/alumno

eth0 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
157	15.823910	10.0.2.4	10.0.2.4	TLSv1.2	1502	Server Hello
158	15.823931	10.0.2.4	162.213.33.48	TCP	54	37498 > https [ACK] Seq=149 Ack=1449 Win=17376 Len=0
159	15.826056	162.213.33.48	10.0.2.4	TLSv1.2	1502	Certificate
160	15.826064	10.0.2.4	162.213.33.48	TCP	54	37498 > https [ACK] Seq=149 Ack=2897 Win=20272 Len=0
161	15.826464	162.213.33.48	10.0.2.4	TLSv1.2	559	Server Key Exchange, Server Hello Done
162	15.826469	10.0.2.4	162.213.33.48	TCP	54	37498 > https [ACK] Seq=149 Ack=3402 Win=23168 Len=0
163	15.868226	10.0.2.4	162.213.33.48	TLSv1.2	321	Client Key Exchange
164	15.929803	10.0.2.4	10.0.2.5	TCP	114	[TCP segment of a reassembled PDU]
165	15.930130	10.0.2.4	10.0.2.5	TCP	114	[TCP segment of a reassembled PDU]
166	15.930140	10.0.2.4	10.0.2.5	TCP	66	33426 > ssh [ACK] Seq=2819 Ack=3467 Win=22528 Len=0 TSval=
167	15.962114	162.213.33.48	10.0.2.4	TCP	60	https > 37498 [ACK] Seq=3402 Ack=416 Win=32353 Len=0
168	15.962125	10.0.2.4	162.213.33.48	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
169	16.058355	10.0.2.4	10.0.2.5	TCP	114	[TCP segment of a reassembled PDU]
170	16.058705	10.0.2.5	10.0.2.4	TCP	114	[TCP segment of a reassembled PDU]
171	16.058717	10.0.2.4	10.0.2.5	TCP	66	33426 > ssh [ACK] Seq=2867 Ack=3515 Win=22528 Len=0 TSval=
172	16.132844	162.213.33.48	10.0.2.4	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
173	16.132864	10.0.2.4	162.213.33.48	TCP	54	37498 > https [ACK] Seq=507 Ack=3493 Win=23168 Len=0
174	16.141628	10.0.2.4	162.213.33.48	TLSv1.2	251	Application Data
175	16.212549	162.213.33.48	10.0.2.4	TCP	60	https > 37498 [ACK] Seq=3493 Ack=704 Win=32065 Len=0
176	16.263199	162.213.33.48	10.0.2.4	TLSv1.2	512	Application Data, Application Data

▶ Frame 163: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits)

▶ Ethernet II, Src: CadmusCo e5:97:03 (08:00:27:e5:97:03), Dst: RealtekU 12:35:00 (52:54:00:12:35:00)

▶ Internet Protocol Version 4, Src: 10.0.2.4 (10.0.2.4), Dst: 162.213.33.48 (162.213.33.48)

▶ Transmission Control Protocol, Src Port: 37498 (37498), Dst Port: https (443), Seq: 149, Ack: 3402, Len: 267

▼ Secure Sockets Layer

▶ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange

```

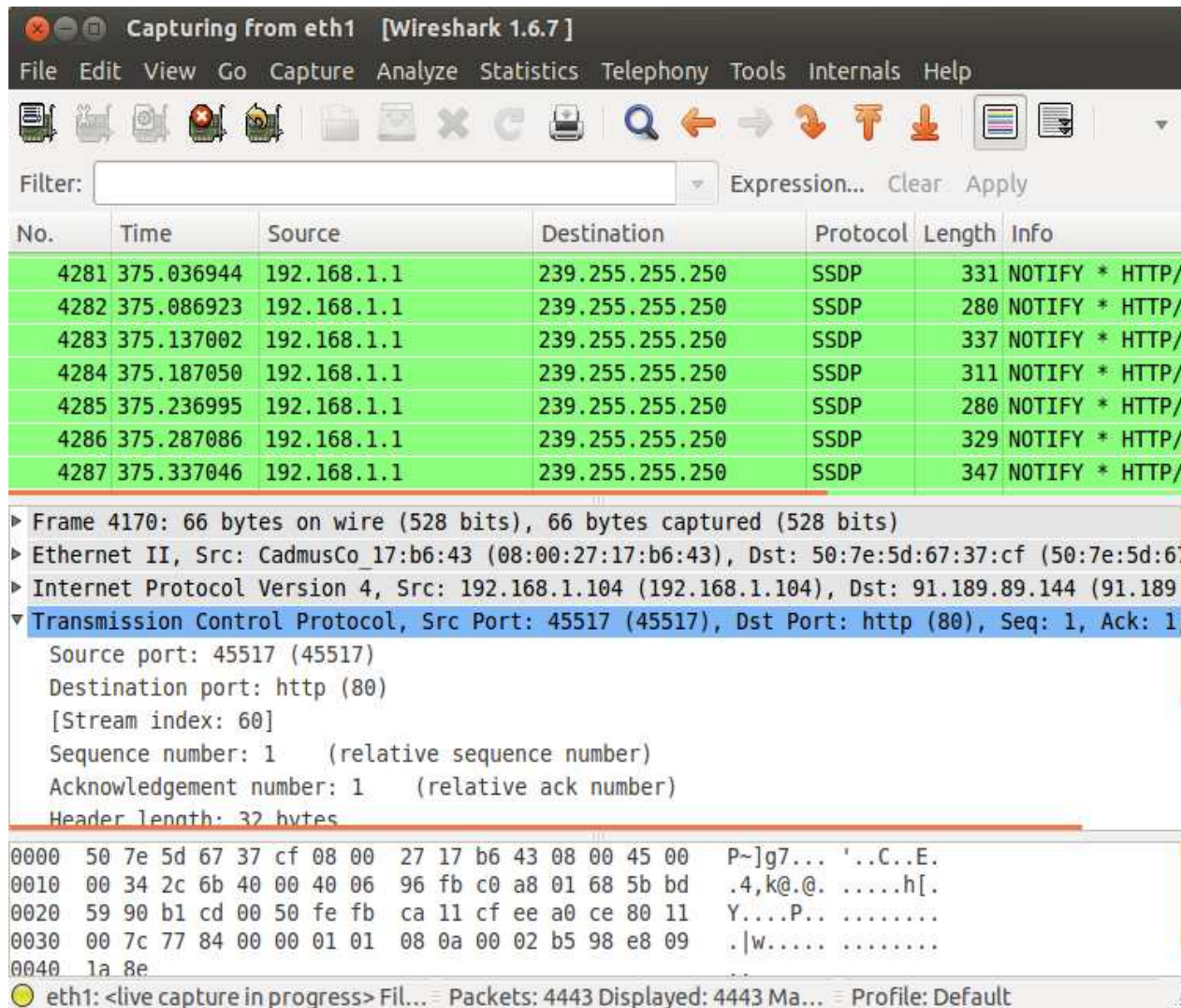
0000 52 54 00 12 35 00 08 00 27 e5 97 03 08 00 45 00 RT..5... '.....E.
0010 01 33 32 d0 40 00 40 06 36 ec 0a 00 02 04 a2 d5 .32.@.@. 6.....
0020 21 30 92 7a 01 bb 95 a6 b3 4b 00 04 a1 1c 50 18 !0.z.... .K...P.
0030 5a 80 d1 2e 00 00 16 03 03 01 06 10 00 01 02 01 Z.....
0040 00 1b 23 f2 f5 71 32 17 0f 2a 08 e4 1f 13 c9 2c ..#.q2. .*.....,
0050 52 b8 7e 6e d3 39 46 b4 18 a4 49 3d 38 7c 93 17 R.-n.9F. .I=B|..
0060 1b ba 2e f9 98 d5 39 98 1f 58 2e 51 45 e8 aa d2 .....9. .X.QE...
0070 ff f1 1e 2b 6f 21 6e 4f 30 4a 39 47 87 d2 7f a4 ...+o!n0 0J9G....
0080 3e 0b 77 0f 1d 86 88 b3 7b 1a 2f d0 ee f3 34 78 >.w.... {./...4x
0090 d9 db b1 7a d5 4f a3 01 11 a4 f5 9f 11 5c 39 96 ...z.0. ....\9.
00a0 70 c0 a3 79 02 65 d7 a7 e0 92 9e f3 48 aa f2 ea p..y.e. ....H...
00b0 38 11 00 85 c2 50 31 ef 0b 04 84 1b c6 7f 78 00 8A V1. K v

```

File: "/tmp/wireshark_eth0_20170..." Packets: 187 Displayed: 187 Marked: 0 Dropped: 0 Profile: Default

Por otro lado, en las capturas ssh no se puede visualizar ningún dato de los introducidos

Actividad 2: Poner la red de una MV en adaptador puente e intentar capturar tráfico del dispositivo host.



Capturing from eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
4281	375.036944	192.168.1.1	239.255.255.250	SSDP	331	NOTIFY * HTTP/
4282	375.086923	192.168.1.1	239.255.255.250	SSDP	280	NOTIFY * HTTP/
4283	375.137002	192.168.1.1	239.255.255.250	SSDP	337	NOTIFY * HTTP/
4284	375.187050	192.168.1.1	239.255.255.250	SSDP	311	NOTIFY * HTTP/
4285	375.236995	192.168.1.1	239.255.255.250	SSDP	280	NOTIFY * HTTP/
4286	375.287086	192.168.1.1	239.255.255.250	SSDP	329	NOTIFY * HTTP/
4287	375.337046	192.168.1.1	239.255.255.250	SSDP	347	NOTIFY * HTTP/

Frame 4170: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: CadmusCo_17:b6:43 (08:00:27:17:b6:43), Dst: 50:7e:5d:67:37:cf (50:7e:5d:67:37:cf)

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 91.189.89.144 (91.189.89.144)

Transmission Control Protocol, Src Port: 45517 (45517), Dst Port: http (80), Seq: 1, Ack: 1

Source port: 45517 (45517)

Destination port: http (80)

[Stream index: 60]

Sequence number: 1 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 32 bytes

0000 50 7e 5d 67 37 cf 08 00 27 17 b6 43 08 00 45 00 P~]g7... '..C..E.

0010 00 34 2c 6b 40 00 40 06 96 fb c0 a8 01 68 5b bd .4,k@. @.h[.

0020 59 90 b1 cd 00 50 fe fb ca 11 cf ee a0 ce 80 11 Y....P..

0030 00 7c 77 84 00 00 01 01 08 0a 00 02 b5 98 e8 09 .|w.....

0040 1a 8e

eth1: <live capture in progress> Fil... Packets: 4443 Displayed: 4443 Ma... Profile: Default

Se intercepta gran cantidad de tráfico HTTP y no se puede conectar a la otra maquina virtual por telnet o ssh.

Si en la configuración de ambas maquinas se pone la red en adaptador puente si se pueden conectar