

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 41

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab41- Export Malicious Redirection Packet Comments

Paso 1:

The image shows the Wireshark 'Open Capture File' dialog box. The 'Buscar en:' field is set to 'wireshark101v2files'. The file list contains various .pcapng files, with 'sec-suspicious101.pcapng' selected. The 'Nombre de archivo:' field also contains 'sec-suspicious101.pcapng'. The 'Tipo de archivo:' is set to 'All Files'. The 'Read filter:' is empty, and the 'Format:' is 'Wireshark/... - pcapng'. The 'Size:' is '120KB, 172 data records'. The 'Start / elapsed:' is '2011-07-13 01:31:34 / 00:00:17'. The 'Abrir' button is highlighted.

The background shows a packet capture of an HTTP 302 redirect. The packet list shows a packet of type 'HTTP' with status '302 Found'. The packet details show the 'Location' field set to 'http://www.artbrokerage.com'. The packet bytes show the raw data of the packet.

Nombre	Fecha de modificación	Tipo	Tamaño
mydns101_00019_20201201190250.pcapng	01/12/2020 19:03	Wireshark capture...	2 KB
mydns101_00020_20201201190300.pcapng	01/12/2020 19:03	Wireshark capture...	1 KB
net-lost-route.pcapng	08/05/2012 15:17	Wireshark capture...	87 KB
pantheon.jpg	05/12/2020 19:32	Archivo JPG	5.415 KB
sec-concern101.pcapng	14/11/2012 19:17	Wireshark capture...	157 KB
sec-nessus101.pcapng	03/11/2012 23:06	Wireshark capture...	249 KB
sec-suspicious101.pcapng	10/12/2012 17:30	Wireshark capture...	121 KB
smb-join101.pcapng	24/10/2012 13:55	Wireshark capture...	127 KB
split250_00000_20160704110754.pcapng	04/07/2016 12:11	Wireshark capture...	262 KB
split250_00001_20160704110759.pcapng	04/07/2016 12:11	Wireshark capture...	265 KB
split250_00002_20160704110759.pcapng	04/07/2016 12:11	Wireshark capture...	252 KB
split250_00003_20160704110759.pcapng	04/07/2016 12:11	Wireshark capture...	253 KB
split250_00004_20160704110759.pcapng	04/07/2016 12:11	Wireshark capture...	244 KB
split250_00005_20160704110804.pcapng	04/07/2016 12:11	Wireshark capture...	1 KB
stopproblem101_00027_20201201125630.pca...	01/12/2020 12:56	Wireshark capture...	1.566 KB
stopproblem101_00028_20201201125640.pca...	01/12/2020 12:56	Wireshark capture...	1.625 KB
stopproblem101_00029_20201201125650.pca...	01/12/2020 12:56	Wireshark capture...	517 KB
tcp-decodeas.pcapng	23/10/2012 14:01	Wireshark capture...	4.169 KB
tr-twohosts.pcapng	02/12/2013 14:07	Wireshark capture...	54.526 KB
tr-winsize.pcapng	02/12/2013 14:07	Wireshark capture...	7.252 KB
wlan-ipadstartstop101.pcapng	14/11/2012 11:01	Wireshark capture...	66 KB

Nombre de archivo: sec-suspicious101.pcapng
Tipo de archivo: All Files
Read filter:
Format: Wireshark/... - pcapng
Size: 120KB, 172 data records
Start / elapsed: 2011-07-13 01:31:34 / 00:00:17

Abrir
Cancelar
Ayuda

Formatted comment (frame.comment.expert) | Packets: 172 · Displayed: 172 (100.0%) · Comments: 19 | Profile: wireshark101

Paso 2:

The image shows the Wireshark network traffic analysis interface. The main pane displays a list of captured packets. The first packet is an HTTP GET request from 24.6.173.220 to 74.125.224.84. The subsequent packets are TCP acknowledgments (ACKs) from the destination to the source. The packet list pane shows the following details:

No.	Time	TCP Delta	Source	Destination	Protocol	Info
1	0.000000	0.000000...	24.6.173.220	74.125.224.84	HTTP	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=firefox-a&as=N&rls=org.mozilla:en-US:official&biw=863&bih=53&tbm=isch&tbnid=FsTtm d2sv8mb6 :Yw97r eK1wMU70 :D89BG ZtHnidKt :fKQrH FFe1N-TO :LSVP3 QwK_SSS1 M:,XEbza g82V1D3S M:,NI8d- DZwgNye2 M:,fp9Mq H4E9dW45 M: HTTP/ 1.1 · · · Hos
2	0.054665	0.054665...	74.125.224.84	24.6.173.220	TCP	80 → 50263 [ACK] Seq=1 Ack=1044 Win=316 Len=0
3	0.006804	0.006804...	74.125.224.84	24.6.173.220	TCP	80 → 50263 [ACK] Seq=1 Ack=1044 Win=316 Len=14
4	0.001200	0.001200...	74.125.224.84	24.6.173.220	TCP	80 → 50263 [ACK] Seq=1431 Ack=1044 Win=316 Len=0
5	0.000003	0.000003...	74.125.224.84	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/javascript)
6	0.000608	0.000608...	24.6.173.220	74.125.224.84	TCP	50263 → 80 [ACK] Seq=1044 Ack=2926 Win=16445 Len=0
7	0.474442	0.000000...	24.6.173.220	74.125.224.84	HTTP	GET /imgres?imgurl=http://www.artbrokerage.com
8	0.017301	0.017301...	74.125.224.84	24.6.173.220	TCP	80 → 50220 [ACK] Seq=1 Ack=1404 Win=508 Len=0
9	0.024975	0.024975...	74.125.224.84	24.6.173.220	TCP	80 → 50220 [ACK] Seq=1 Ack=1404 Win=508 Len=14
10	0.001156	0.001156...	74.125.224.84	24.6.173.220	TCP	80 → 50220 [ACK] Seq=1431 Ack=1404 Win=508 Len=0
11	0.000008	0.000008...	74.125.224.84	24.6.173.220	TCP	80 → 50220 [PSH, ACK] Seq=2861 Ack=1404 Win=508 Len=0
12	0.000014	0.000014...	74.125.224.84	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/html)
13	0.000647	0.000647...	24.6.173.220	74.125.224.84	TCP	50220 → 80 [ACK] Seq=1404 Ack=4167 Win=16445 Len=0
14	0.024191	0.000000...	24.6.173.220	77.93.251.49	TCP	50316 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
15	0.002104	0.000000...	24.6.173.220	66.11.147.48	TCP	50317 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
16	0.102909	0.102909...	66.11.147.48	24.6.173.220	TCP	80 → 50317 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
17	0.000121	0.000121...	24.6.173.220	66.11.147.48	TCP	50317 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18	0.000565	0.000565...	24.6.173.220	66.11.147.48	HTTP	GET /artthumb/likp_35911_2/850x600/Peter_Lik_B

The packet details pane shows the selected packet (No. 1) with the following details:

- Frame 1: 1
- Ethernet II
- Internet Protocol Version 4
- Transmission Control Protocol
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the selected packet, starting with 0000 00 01 and ending with 0130 4d 3a 2c 58 45 62 7a 61 67 38 32 56 6c 44 33 53.

A context menu is open over the packet list, showing the following options:

- Expand Subtrees
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column (Ctrl+Shift+I)
- Apply as Filter (Ctrl+Shift+F) - **Selected**
- Prepare as Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes... (Ctrl+Shift+O)
- Export Packet Bytes... (Ctrl+Shift+X)
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As... (Ctrl+Shift+U)
- Go to Linked Packet
- Show Linked Packet in New Window

The status bar at the bottom shows: Packets: 172 · Displayed: 172 (100.0%) · Comments: 19 | Profile: wireshark101

Paso 3:

The image shows a Wireshark packet capture analysis of a file named `sec-suspicious101.pcapng`. The main packet list shows several HTTP requests and responses. The selected packet is packet 1, which is an HTTP GET request for `http://www.artbrokerage.com/artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Paradise.jpg`. The packet details pane shows the request structure, including the Host, User-Agent, and Referer fields. The packet bytes pane shows the raw data of the request.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	192.168.1.100	192.168.1.1	HTTP	1043	GET http://www.google.com/... HTTP/1.1
1	0.000000	192.168.1.1	192.168.1.100	HTTP	1043	200 OK
2	0.000000	192.168.1.100	192.168.1.1	HTTP	1043	GET http://www.google.com/... HTTP/1.1
3	0.000000	192.168.1.1	192.168.1.100	HTTP	1043	200 OK
4	0.000000	192.168.1.100	192.168.1.1	HTTP	1043	GET http://www.google.com/... HTTP/1.1
5	0.000000	192.168.1.1	192.168.1.100	HTTP	1043	200 OK

Packet Details (Packet 1):

- Frame 1: 1043 bytes on interface (8776 bits) on interface unknown, id 0
- Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: 08:00:00:00:00:00
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
- Transmission Control Protocol, Src Port: 80, Dst Port: 80, Seq: 1, Ack: 1, Len: 1043
- Hypertext Transfer Protocol

Packet Bytes:

Offset	Hex	ASCII
0000	00 01 5c	
0010	04 3b 73	
0020	e0 54 c4	
0030	40 12 f4	
0040	3d 70 65	
0050	61 6c 65	
0060	6c 69 65	
0070	73 61 3d	
0080	69 6c 6c	
0090	69 61 6c	
00a0	35 35 33	
00b0	69 64 3d	
00c0	4d 3a 2c	
00d0	4d 3a 2c	
00e0	4d 3a 2c	
00f0	4d 3a 2c	
0100	4d 3a 2c	
0110	4d 3a 2c 4e 49 38 64 2d 44 5a 77 67 4e 79 65 32	M:,NI8d-DZwgNye2
0120	4d 3a 2c 66 70 39 4d 71 48 34 45 39 64 57 34 35	M:,fp9Mq H4E9dW45
0130	4d 3a 2c 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73	M: HTTP/ 1.1 · Hos

Packet Comments:

- This is the original search query for the "Peter Lik for sale" images.

Wireshark Interface:

- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
- pkts_comment
- Host
- www.google.com
- www.artbrokerage.com
- www.ulisseide.org
- 3xsd5p828s.cz.cc

Wireshark Status Bar:

- Packets: 172 · Displayed: 19 (11.0%) · Comments: 19
- Profile: wireshark101

Paso 4 y 5:

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The File menu is open, displaying options like Open, Open Recent, Merge..., Import from Hex Dump..., Close, Save, Save As..., File Set, Export Specified Packets..., Export Packet Dissections, Export Packet Bytes..., Export PDUs to File..., Export TLS Session Keys..., Export Objects, Print..., and Quit. The 'Export Packet Dissections' option is selected, opening a submenu with 'As Plain Text...', 'As CSV...', 'As "C" Arrays...', 'As PSMML XML...', 'As PDML XML...', and 'As JSON...'. The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
220	74.125.224.84	74.125.224.84	24.6.173.220	HTTP	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&clien
220	74.125.224.84	74.125.224.84	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/javascript)
220	74.125.224.84	74.125.224.84	24.6.173.220	HTTP	GET /imgres?imgurl=http://www.artbrokerage.com
220	74.125.224.84	74.125.224.84	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/html)
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50316 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
220	66.11.147.48	66.11.147.48	24.6.173.220	TCP	50317 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
220	66.11.147.48	66.11.147.48	24.6.173.220	HTTP	GET /arthumb/likp_35911_2/850x600/Peter_Lik_B
220	77.93.251.49	77.93.251.49	24.6.173.220	HTTP	GET /stat/gthyu/index.php?p=peter-lik-inner-pe
48	24.6.173.220	24.6.173.220	77.93.251.49	TCP	80 → 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1
220	77.93.251.49	77.93.251.49	24.6.173.220	HTTP	HTTP/1.1 302 Found
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50319 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
220	77.93.251.49	77.93.251.49	24.6.173.220	HTTP	HTTP/1.1 302 Found
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50320 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
220	77.93.251.49	77.93.251.49	24.6.173.220	HTTP	GET /in.cgi?8&seoref=http%3A%2F%2Fwww.google.c
220	77.93.251.49	77.93.251.49	24.6.173.220	HTTP	HTTP/1.1 200 OK (text/html)
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50321 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50324 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	77.93.251.49	77.93.251.49	24.6.173.220	TCP	50326 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Packet comments

- Well that didn't go so well for them... our Symantec software terminated the connection and wouldn't run the script.
 - [Expert Info (Comment/Comment): Well that didn't go so well for them... our Symantec software terminated the connection and wouldn't run the script.]
 - [Severity level: Comment]
 - [Group: Comment]

> Frame 96: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface unknown, id 0

> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 78.41.203.19

> Transmission Control Protocol, Src Port: 50321, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Comment (frame.comment)

Packets: 172 · Displayed: 19 (11.0%) · Comments: 19 | Profile: wireshark101

sec-suspicious101.pcapng

Wireshark · Export Packet Dissections

Guardar en: wireshark101v2files

Nombre

Fecha de modificación

Tipo

Tamaño

hostinformation.csv

02/12/2020 22:50

Archivo de valores...

10 KB

Acceso rápido

Escritorio

Bibliotecas

Este equipo

Red

Nombre de archivo: suspicious101.csv

Tipo: CSV (Comma Separated Values summary) (*.csv)

Guardar

Cancelar

Ayuda

Packet Range

☒ All packets

☐ Selected packet

☐ Marked packets

☐ First to last marked

☐ Range:

☐ Remove Ignored packets

Captured

172

Displayed

19

Packet Format

☒ Packet summary line

☒ Include column headings

☐ Packet details: As displayed

☐ Packet Bytes

☐ Each packet on a new page

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d...E.

0010 00 28 73 ea 40 00 80 06 00 00 18 06 ad dc 4e 29 ..(s:@...N)

0020 cb 13 c4 91 00 50 1c ac c9 17 c5 9e 84 21 50 14P...!P.

0030 00 00 df 39 00 00g...

Comment (frame.comment)

Packets: 172 · Displayed: 19 (11.0%) · Comments: 19

Profile: wireshark101

Windows Taskbar

Paso 6:

suspicious101.csv - Excel Omar Vazquez Canto

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Ayuda ¿Qué desea hacer? Compartir

Portapapeles Fuente Alineación Número Estilos Celdas Edición Confidencialidad

F21

No.	Time	TCP Delta	Source	Destination	Protocol	Info	Host	Comment
1	"0.000000"	"0.000000000"	"24.6.173.220"	"74.125.224.84"	"HTTP"	"GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=firefox-a&sa=N&rls=org.m"		
5	"0.062672"	"0.000003000"	"74.125.224.84"	"24.6.173.220"	"HTTP"	"HTTP/1.1 200 OK (text/javascript)"		"In this response, the server sends numero"
7	"0.475050"	"0.000000000"	"24.6.173.220"	"74.125.224.84"	"HTTP"	"GET /imgres?imgurl=http://www.artbrokerage.com/artthumb/likp_35911_2/850x"		
12	"0.043454"	"0.000014000"	"74.125.224.84"	"24.6.173.220"	"HTTP"	"HTTP/1.1 200 OK (text/html)"		"We get the expanded image through Google -"
14	"0.024838"	"0.000000000"	"24.6.173.220"	"77.93.251.49"	"TCP"	"50316 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1"		"We cl"
15	"0.002104"	"0.000000000"	"24.6.173.220"	"66.11.147.48"	"TCP"	"50317 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1"		"Here"
18	"0.103595"	"0.000565000"	"24.6.173.220"	"66.11.147.48"	"HTTP"	"GET /artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Paradise.jpg HTTP/1.1"		
21	"0.086025"	"0.000709000"	"24.6.173.220"	"77.93.251.49"	"HTTP"	"GET /stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale HTTP/1.1"		"www.u"
23	"0.161477"	"0.146588000"	"66.11.147.48"	"24.6.173.220"	"TCP"	"80 > 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassemb"		
67	"0.580651"	"0.547913000"	"77.93.251.49"	"24.6.173.220"	"HTTP"	"HTTP/1.1 302 Found"		"Here's the redirection to the malicious site. See the Loc"
68	"0.002170"	"0.000000000"	"24.6.173.220"	"95.169.190.217"	"TCP"	"50319 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1"		"We"
75	"0.382179"	"0.002074000"	"95.169.190.217"	"24.6.173.220"	"HTTP"	"HTTP/1.1 302 Found"		"Our malicious host is redirecting us to run a CGI script"
79	"0.003645"	"0.000000000"	"24.6.173.220"	"95.169.190.217"	"TCP"	"50320 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1"		"And"
84	"0.196512"	"0.000015000"	"24.6.173.220"	"95.169.190.217"	"HTTP"	"GET /in.cgi?8&seoref=http%3A%2F%2Fwww.google.com%2Fimgres%3Fimgurl"		
87	"0.210788"	"0.011399000"	"95.169.190.217"	"24.6.173.220"	"HTTP"	"HTTP/1.1 200 OK (text/html)"		"They're dropping a cookie on our drive and g"
96	"0.244080"	"0.002946000"	"24.6.173.220"	"78.41.203.19"	"TCP"	"50321 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"		"Well that didn't go so well fo"
104	"0.181295"	"0.001678000"	"24.6.173.220"	"78.41.203.19"	"TCP"	"50324 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"		"And another termination tri"
117	"0.283123"	"0.001682000"	"24.6.173.220"	"78.41.203.19"	"TCP"	"50326 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0"		"Yes, Symantec is screaming"
159	"12.732243"	"15.712621000"	"24.6.173.220"	"74.125.224.84"	"HTTP"	"GET /gen_204?atyp=i&ct=backbutton&cad=&ei=ejsdTsWPN4OmsQOf9W6D"		
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								

suspicious101

Listo

100%