

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 40

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab40- Read Analysis Notes in a Malicious Redirection Trace File

Paso 1:

The screenshot shows a Windows desktop environment. In the foreground, a file selection dialog titled "Wireshark - Open Capture File" is open. The dialog shows a list of files in the "wireshark101v2files" folder. The file "sec-suspicious101.pcapng" is selected. The dialog also shows the file's size (121 KB) and the date it was modified (10/12/2012 17:30). The "Nombre de archivo" field contains "sec-suspicious101.pcapng" and the "Tipo de archivo" is set to "All Files". The "Read filter" is set to "Automatically detect file type" and the "Format" is "Wireshark/... - pcapng". The "Size" is "120KiB, 172 data records" and the "Start / elapsed" time is "2011-07-13 01:31:34 / 00:00:17".

In the background, the Wireshark interface is visible. The "Packets" pane shows a list of captured packets. The selected packet is packet 1, which is a TCP Reset (RST) packet. The packet details pane shows the following information:

- Frame 1: 120 bytes on wire (960 bits) captured (960 bits) on 0
- Ethernet II, Src: Intel (08:00:00:00:00:00), Dst: Intel (08:00:00:00:00:00)
- TCP, Seq=1111111111, Win=0, Len=0
- IP, Src=10.0.0.1, Dst=10.0.0.2
- Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
- Transmission Control Protocol, Seq=1111111111, Win=0, Len=0
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII. The ASCII data is:

```
..1... d...E..
.p.Q@... ..C..
x2...P.X...Q..P..
@)V...GE T /favic
on.ico?v =2 HTTP/
1.1..Hos t: www.c
ollegehu mor.com..
User-Ag ent: Moz
illa/5.0 (window
s NT 6.1 ; WOW64;
rv:16.0 ) Gecko/
20100101 Firefox
/16.0..A ccept: t
ext/html ,applica
tion/xht ml+xml,a
pplicati on/xml;q
=0.9,*/* ;q=0.8..
Accept-L anguage:
en-US,e n;q=0.5..
Accept- Encoding
```

Paso 2:

sec-suspicious101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	TCP
1	0.000000	0.0
2	0.054665	0.0
3	0.006804	0.0
4	0.001200	0.0
5	0.000003	0.0
6	0.000608	0.0
7	0.474442	0.0
8	0.017301	0.0
9	0.024975	0.0
10	0.001156	0.0
11	0.000008	0.0
12	0.000014	0.0
13	0.000647	0.0
14	0.024191	0.0
15	0.002104	0.0
16	0.102909	0.1
17	0.000121	0.0
18	0.000565	0.0

Details

Measurement Submeasured Displayed Filtered

Packets 172 172 (100.0%) —

Time span, s 17.217 17.217 —

Average pps 10.0 10.0 —

Average packet size, B 458 458 —

Bytes 78846 78846 (100.0%) 0

Average bytes/s 4579 4579 —

Average bits/s 36k 36k —

Section Comment

[Copyright 2012/2013 Chappell University]

While watching a Pawn Stars episode that featured a Peter Lik photograph, I decided to find out what that photograph sold for. From our lab machine, I did a google search for "Peter Lik for sale" and selected "images".

This trace includes the Google query for the images (frame 1), and the responses in a compressed list (frames 2-6) filled with images and the image links.

I clicked on one image which was linked to artbrokerage.com and ulisseide.org (frame 7).

See packet comments for more detail.

Packet Comments

Frame 1: This is the original search query for the "Peter Lik for sale" images.

Frame 5: In this response, the server sends numerous thumbnail images along with their image URL and HTTP URLs. This response mentions the image resolution URL (imgres?imgurl) as www.artbrokerage.com/artthumb/likp_35911_2/850x600//Peter_Lik_Beyond_Paradise.jpg with an image reference URL (imgrefurl) of www.ulisseide.org/stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale. We will ask for the image from artbrokerage and the page from www.ulisseide.org.

Frame 7: Now we clicked on the image load the expanded thumbnail from Google. We ask for the imgres and imgrefurl.

Frame 12: We get the expanded image through Google - there are a lot of web display parameters in this response. So far we are getting everything from Google.

Frame 14: We clicked on the web link associated with the expanded image. This launches our connections to the two websites we know of - artbrokerage.com and ulisseide.org. In this frame we begin to establish a connection to www.ulisseide.org at 77.93.251.49. The SYN/ACK is in frame 19. Right-click on this packet to colorize the conversation with Color 1.

Frame 15: Here we begin connecting to www.artbrokerage.com at 66.11.147.48. The SYN/ACK is in frame 16. Right-click on this packet to colorize the conversation with Color 2.

Frame 18: We request an 850x600 size of a Peter Lik photo.

Frame 21: Now we are making a request to www.ulisseide.org.

Frame 23: This TCP connection is used to get the image file from artbrokerage.com. Check out File | Export Objects | HTTP.

Frame 67: Here's the redirection to the malicious site. See the Location line. We are being redirected to <http://3xsd5p828s.cz.cc>. Consider making a coloring rule for all HTTP redirections - `http.response.code > 299 && http.response.code < 400`.

Frame 68: We removed the DNS queries from the trace file - we must have looked up the IP address and now we're making a connection to the 3xsd5p828s.cz.cc site. Set this TCP conversation to use color 4 (we skipped 3 because it's too close to 2).

Capture file comments

[Copyright 2012/2013 Chappell University]

While watching a Pawn Stars episode that featured a Peter Lik photograph, I decided to find out what that photograph sold for. From our lab machine, I did a google search for "Peter Lik for sale" and selected "images".

This trace includes the Google query for the images (frame 1), and the responses in a compressed list (frames 2-6) filled with images and the image links.

sec-suspicious101.pcapng

Profile: wireshark101

Paso 3 y 4:

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture file named 'sec-suspicious101.pcapng'. The packet list on the left shows packets 6 through 23. The packet details pane on the left shows the selected packet (23) with its structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

The 'Expert Information' pane on the right shows a list of packets with their summary, group, and protocol. The list includes:

- Packet 6: Error, Bad checksum [should be 0x9254], Checksum, IPv4
- Packet 7: Warning, Connection reset (RST), Sequence, TCP
- Packet 8: Note, This frame is a (suspected) retransmission, Sequence, TCP
- Packet 9: Chat, Connection finish (FIN), Sequence, TCP
- Packet 10: Chat, Connection establish acknowledge (SYN+ACK): server port..., Sequence, TCP
- Packet 11: Chat, Connection establish request (SYN): server port 80, Sequence, TCP
- Packet 12: Chat, GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir..., Sequence, HTTP
- Packet 13: Comment, Packet comments listed below., Comment, Frame
- Packet 14: Comment, This is the original search query for the "Peter Lik for sale" i..., Comment, Frame
- Packet 15: Comment, In this response, the server sends numerous thumbnail im..., Comment, Frame
- Packet 16: Comment, Now we clicked on the image load the expanded thumbna..., Comment, Frame
- Packet 17: Comment, We get the expanded image through Google - there are a l..., Comment, Frame
- Packet 18: Comment, We clicked on the web link associated with the expanded i..., Comment, Frame
- Packet 19: Comment, Here we begin connecting to www.artbrokerage.com at 66..., Comment, Frame
- Packet 20: Comment, We request an 850x600 size of a Peter Lik photo., Comment, Frame
- Packet 21: Comment, Now we are making a request to www.ulisseide.org., Comment, Frame
- Packet 22: Comment, This TCP connection is used to get the image file from artb..., Comment, Frame
- Packet 23: Comment, Here's the redirection to the malicious site. See the Locatio..., Comment, Frame
- Packet 24: Comment, We removed the DNS queries from the trace file - we must..., Comment, Frame
- Packet 25: Comment, Our malicious host is redirecting us to run a CGI script (in..., Comment, Frame
- Packet 26: Comment, And here we go... this is the ugly connection., Comment, Frame
- Packet 27: Comment, Please oh please hit us over the head with a baseball bat! ..., Comment, Frame
- Packet 28: Comment, They're dropping a cookie on our drive and giving us a link..., Comment, Frame
- Packet 29: Comment, Well that didn't go so well for them... our Symantec softwa..., Comment, Frame
- Packet 30: Comment, And another termination triggered by Symantec., Comment, Frame
- Packet 31: Comment, Yes, Symantec is screaming with messages on our system..., Comment, Frame
- Packet 32: Comment, We're just returning to Google after a little sidetrack to the ..., Comment, Frame

The bottom of the interface shows the Windows taskbar with various application icons.