



TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“LABORATORIO 40”

UNIDAD 3

1)

sec-suspicious101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización... <Ctrl>F

GET POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx

No.	Time	Source	Destination	Protocol	Info
157	15.268...	24.6.173.220			
8	0.555823	74.125.224.84			
9	0.579998	74.125.224.84			
10	0.581154	74.125.224.84			
164	16.015...	74.125.224.84			
165	16.016...	74.125.224.84			
11	0.581162	74.125.224.84			
2	0.054665	74.125.224.84			
3	0.051160	74.125.224.84			

< Frame 157: 66 bytes on wire (528 bits) captured on interface eth0 (0 bytes captured on interface eth0, 0 bytes discarded)
> Ethernet II, Src: HewlettP_07:8F:6D:8E:02:02, Dst: 08:00:27:00:00:00
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.84
> Transmission Control Protocol, Src Port: 50353, Dst Port: 80, Seq: 1401, Win: 0, Len: 0
[Stream index: 20]
[TCP Segment Len: 0]
Sequence Number: 0 (retransmission)
Sequence Number (raw): 1401
Next Sequence Number: 1

0000 00 01 5c 31 bb c1 d4 85 6
0010 00 34 74 59 40 00 80 06 0
0020 be d9 c4 b1 00 50 53 8a 7
0030 20 00 e4 8b 00 00 02 04 0
0040 04 02

Wireshark - Información especializada - sec-suspicious101.pcapng

Gravedad	Resumen	Grupo	Protocolo	Recuento
Warning	Connection reset (RST)	Sequence	TCP	12
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	9
Chat	Connection establish acknowledge (SYN+ACK): server port...	Sequence	TCP	20
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	19
Chat	GET /sbd?lq=peter+lik+for+sale&um=1&hl=en&client=firefox-a	Sequence	HTTP	22
Comment	Packet comments listed below.	Comment	Frame	19

1 This is the original search query for the "Peter Lik for sale" i... Comment Frame
5 In this response, the server sends numerous thumbnail im... Comment Frame
7 Now we clicked on the image load the expanded thumbna... Comment Frame
12 We get the expanded image through Google - there are a l... Comment Frame
14 We clicked on the web link associated with the expanded i... Comment Frame
15 Here we begin connecting to www.artbrokerage.com at 66... Comment Frame
18 We request an 850x600 size of a Peter Lik photo. Comment Frame
21 Now we are making a request to www.uliseide.org. Comment Frame
23 This TCP connection is used to get the image file from artb... Comment Frame
67 Here's the redirection to the malicious site. See the Locatio... Comment Frame
68 We removed the DNS queries from the trace file - we must... Comment Frame
75 Our malicious host is redirecting us to run a CGI script (in... Comment Frame
79 And here we go... this is the ugly connection. Comment Frame
84 Please oh please hit us over the head with a baseball bat! ... Comment Frame
87 They're dropping a cookie on our drive and giving us a link... Comment Frame
96 Well that didn't go so well for them... our Symantec softwa... Comment Frame
104 And another termination triggered by Symantec. Comment Frame
117 Yes, Symantec is screaming with messages on our system... Comment Frame
159 We're just returning to Google after a little sidetrack to the ... Comment Frame

No hay conjunto de filtro de visualización.

☐ Limitar filtro de visualización ☒ Agrupar por resumen Buscar:

sec-suspicious101.pcapng

Comentarios: 19 Perfi: wireshark101

12:39 p. m. 07/12/2020