

Réseau - InterceptingImages - 50 points

Kévin DUVERGER

Table des matières

1	Résolution InterceptingImages :
----------	--

2

1 Résolution InterceptingImages :

Pour ce nouveau challenge, on nous donne un échange de données FTP et le but est de trouver l'image qui a été échangée entre un client et un serveur. La première chose que l'on peut faire est ouvrir la capture pour comprendre comment cela fonctionne :

118	9.251268	192.168.1.44	142.250.178.138	UDP	71	53235 → 443	Len=29
119	9.276965	142.250.178.138	192.168.1.44	UDP	67	443 → 53235	Len=25
120	10.657564	146.59.227.136	192.168.1.44	TCP	82	9876 → 28097	[PSH, ACK] Seq=57 Ack=1 Win=491 Len=28
121	10.702205	192.168.1.44	146.59.227.136	TCP	54	28097 → 9876	[ACK] Seq=1 Ack=85 Win=253 Len=0
122	11.147686	146.59.227.136	192.168.1.44	TCP	82	9876 → 17648	[PSH, ACK] Seq=57 Ack=1 Win=501 Len=28
123	11.200097	192.168.1.44	146.59.227.136	TCP	54	17648 → 9876	[ACK] Seq=1 Ack=85 Win=251 Len=0
124	11.805842	192.168.1.224	192.168.1.44	TCP	72	50940 → 2121	[PSH, ACK] Seq=76 Ack=607 Win=65536 Len=6 TSval=86900192 TSecr=155907344
125	11.806059	192.168.1.44	192.168.1.224	TCP	100	2121 → 50940	[PSH, ACK] Seq=607 Ack=82 Win=65280 Len=34 TSval=155914738 TSecr=86900192
126	11.810400	192.168.1.224	192.168.1.44	TCP	74	50940 → 2121	[PSH, ACK] Seq=82 Ack=641 Win=65536 Len=8 TSval=86900211 TSecr=155914738
127	11.810559	192.168.1.44	192.168.1.224	TCP	92	2121 → 50940	[PSH, ACK] Seq=641 Ack=90 Win=65280 Len=26 TSval=155914742 TSecr=86900211
128	11.822578	192.168.1.224	192.168.1.44	TCP	74	50940 → 2121	[PSH, ACK] Seq=90 Ack=667 Win=65536 Len=8 TSval=86900223 TSecr=155914742
129	11.822744	192.168.1.44	192.168.1.224	TCP	92	2121 → 50940	[PSH, ACK] Seq=667 Ack=98 Win=65280 Len=26 TSval=155914755 TSecr=86900223

Comme vous pouvez le voir on ne voit jamais de FTP dans ce fichier et c'est probablement car Wireshark s'est arrêté à TCP. De plus, à part quelques échanges parasites, vous pouvez voir que la majorité des communications a lieu entre les IP 192.168.1.44 et 192.168.1.224, et ces sur ces dernières que nous allons nous concentrer.

On peut donc aller sur la première trame échangée entre ces 2 machines, la 51, faire un clic droit et aller vers "suivre" :

The screenshot shows the Wireshark interface with packet 51 selected. A right-click context menu is open over the packet, with the 'Suivre' (Follow) option highlighted. The packet details pane shows TCP Stream data.

En faisant cela, nous obtenons la capture suivante :

The screenshot shows the 'Follow TCP Stream' window in Wireshark. The data is displayed in hexadecimal and ASCII format. The stream is identified as 'tcp.stream eq 2'.

Et comme vous pouvez le voir il n'y a qu'environ 1200 octets qui semble plus être un échange de commandes entre le client et le serveur qu'une image (d'ailleurs les données échangées ici ne commencent même pas par la signature d'une image PNG / JPG).

Pour comprendre pourquoi, il faut se souvenir du fonctionnement du protocole FTP : la connexion principale est utilisée pour l'échange de commandes entre le client et le serveur, et une autre connexion est créée pour échanger les données. La solution est donc de trouver l'autre stream TCP entre les 2 machines qui se produira probablement avec des ports différents de la première. En allant éplucher la capture réseau, vous devriez remarquer que le paquet 82 a bien de nouveaux ports :

80	4.399140	192.168.1.44	192.168.1.224	TCP	117 2121 → 50940 [PSH, ACK] Seq=478 Ack=70 Win=65280 Len=51 TSval=155907331 TSecr=86892798
81	4.403469	142.250.178.138	192.168.1.44	UDP	67 443 → 53235 Len=25
82	4.407037	192.168.1.224	192.168.1.44	TCP	74 43754 → 51096 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=86892807 TSecr=0 WS=1024
83	4.407152	192.168.1.44	192.168.1.224	TCP	74 51096 → 43754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=155907339 TSecr=
84	4.410308	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=86892811 TSecr=155907339
85	4.411690	192.168.1.224	192.168.1.44	TCP	72 50940 → 2121 [PSH, ACK] Seq=70 Ack=529 Win=65536 Len=6 TSval=86892812 TSecr=155907331
86	4.412342	192.168.1.44	192.168.1.224	TCP	120 2121 → 50940 [PSH, ACK] Seq=529 Ack=76 Win=65280 Len=54 TSval=155907344 TSecr=86892812
87	4.412725	192.168.1.44	192.168.1.224	TCP	209 51096 → 43754 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=143 TSval=155907344 TSecr=86892811
88	4.412823	192.168.1.44	192.168.1.224	TCP	66 51096 → 43754 [FIN, ACK] Seq=144 Ack=1 Win=65280 Len=0 TSval=155907344 TSecr=86892811
89	4.412851	192.168.1.44	192.168.1.224	TCP	90 2121 → 50940 [PSH, ACK] Seq=583 Ack=76 Win=65280 Len=24 TSval=155907345 TSecr=86892812
90	4.416071	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [ACK] Seq=1 Ack=144 Win=67584 Len=0 TSval=86892816 TSecr=155907344
91	4.417852	192.168.1.224	192.168.1.44	TCP	66 43754 → 51096 [FIN, ACK] Seq=1 Ack=145 Win=67584 Len=0 TSval=86892818 TSecr=155907344

> Frame 82: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 > Ethernet II, Src: c6:5b:40:f2:7b:4a (c6:5b:40:f2:7b:4a), Dst: Intel_ce:5b:03 (f0:9e:4a:ce:5b:03)
 > Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.44
 > Transmission Control Protocol, Src Port: 43754, Dst Port: 51096, Seq: 0, Len: 0

Nous pouvons une nouvelle fois suivre cette communication et voici ce que l'on obtient :

Wireshark - Suivre le flux TCP (tcp.stream eq 3) - capture.pcap

6d6f646966793d32303235303931313232323332343b7065726d3d723b73697a653d31343934313b747970653d66696c653b2062617365496d6167652e6a70670d0a6d6f646966793d32303235303931313232333233313b7065726d3d723b73697a653d3238373735373b747970653d66696c653b2066696e616c496d6167655f636f6d70757465722e706e670d0a

o client pkt(s), 1 server pkt(s), 0 turn(s).

Conversation entière (143 bytes) Afficher les données comme Brut Flux 3

Trouver : Trouver Suivant

Filtrer ce flux Imprimer Enregistrer sous... Retour Fermer Aide

Malheureusement, cela ressemble très peu à une image, il faut continuer à chercher.

Une autre connexion qui est différente des 2 autres commence au paquet 134 :

No.	Time	Source	Destination	Protocol	Length	Info
132	11.882081	192.168.1.44	192.168.1.224	TCP	117	2121 → 50940 [PSH, ACK] Seq=693 Ack=104 Win=65280 Len=51 TSval=155914814 TSecr=86900281
133	11.885688	192.168.1.224	192.168.1.44	TCP	66	50940 → 2121 [ACK] Seq=104 Ack=744 Win=65536 Len=0 TSval=86900286 TSecr=155914814
134	11.889819	192.168.1.224	192.168.1.44	TCP	74	55102 → 51097 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=86900290 TSecr=0 WS=1024
135	11.889931	192.168.1.44	192.168.1.224	TCP	74	51097 → 55102 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=155914822 TSecr=
136	11.893429	192.168.1.224	192.168.1.44	TCP	66	55102 → 51097 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=86900294 TSecr=155914822
137	11.897968	192.168.1.224	192.168.1.44	TCP	97	50940 → 2121 [PSH, ACK] Seq=104 Ack=744 Win=65536 Len=31 TSval=86900298 TSecr=155914814
138	11.898805	192.168.1.44	192.168.1.224	TCP	120	2121 → 50940 [PSH, ACK] Seq=744 Ack=135 Win=65280 Len=54 TSval=155914831 TSecr=86900298
139	11.899073	192.168.1.44	192.168.1.224	TCP	1514	51097 → 55102 [ACK] Seq=1 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294
140	11.899073	192.168.1.44	192.168.1.224	TCP	1514	51097 → 55102 [ACK] Seq=1449 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294
141	11.899073	192.168.1.44	192.168.1.224	TCP	1514	51097 → 55102 [ACK] Seq=2897 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294
142	11.899073	192.168.1.44	192.168.1.224	TCP	1514	51097 → 55102 [ACK] Seq=4345 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294
143	11.899073	192.168.1.44	192.168.1.224	TCP	1514	51097 → 55102 [ACK] Seq=5793 Ack=1 Win=65280 Len=1448 TSval=155914831 TSecr=86900294

> Frame 134: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: c6:5b:40:f2:7b:4a (c6:5b:40:f2:7b:4a), Dst: Intel ce:5b:03 (f0:9e:4a:ce:5b:03)

> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.44

> Transmission Control Protocol, Src Port: 55102, Dst Port: 51097, Seq: 0, Len: 0

0000 f0 9e 4a ce 5b 03 c6 5b 40 f2 7b 4a 08 00 45 00 ····[···]@···E·

0010 00 3c 87 62 40 00 00 06 2e fd 0c a8 01 e0 c0 a8 <···@··· ······

0020 01 2c d7 3c c7 99 8b e9 05 1d 00 a0 00 00 a0 02 ···· ······ ······

0030 ff ff 95 59 00 00 02 04 05 b4 04 02 08 0a 05 2d ···· ······ ······

0040 fe 42 00 00 00 01 03 03 0a ······ ······ ······

Nous pouvons encore suivre cette communication, ce qui nous donne :

Wireshark - Suivre le flux TCP (tcp.stream eq 8) - capture.pcap

89504e470d0a1a0a000000d49484452000002e4000001ec0802000000157d2fc2000000017352474200aee1ce90000000467414d410000b18f0bfc610500000097048597300000b1201d2dd7efc0000ffa549444154785eefcde9b365c9712788b97bc4b9ef65561536126c8058898d0048701134da39ed148d66c2ecd5dd336632d37c2541109c31fd33fa20b3f943e68bcc6426d9d86864dde490204190e0da008895580ab567be7b22dcf5e1e7ee27eeb9cbbefbdcac2c30bd6ebdb374eac1e71223c7ee1eec1ffe9fff17f2532ed9db4699bb5377cc8d44c998ca5925429b5d4a9d42a50a13999999aa9a19111313334b9d482a6131111313130238e4586ae6a69b59936522535121611169152b0808b3033310b13919129999a2aa919a33c611696c2525022b3104b166d664c46645e136623c23373527f2acc222c2524a922524a8902f8f5575f1bf3f19a101b7156406a455ad4c34cd4bbcd57d7ed8aeae6edc33e5f5b6755e21266a5e8ad449cad20aafb9a9f597b2753afb1416e1329114a9139789bd9ec26c0916937edd6bb6a27533223262e2c22e09848616112722ea99a76ed5d35786b6826338b119139364f78a08090b15222152d566d6d5667092b9b0542e93d42a752365421ba3459dac8bb687afbfc7db6beb53ef779464f90089749ca24d346c012ec42579de7bb3365b9f7b6f664a2c2422b291b229b578122946ad6ad77ebb3b62b6adbd6ba44d8d8c98a5729dbca052590a09786ebdc3afbe037ed464c2ccc941fb4d18c98c55b2a134b65a9cc85c89889848999944b8081531b3663a9b1a19919219111532f45a89118bc632311319b19162b4f7de9b6933ed4466a6181d4c42c468113a8b88554d9d8c88c88a207c9d88cc4481fd83b5e7c78b1edf460abaf3de8af3dd4371eb075b9b97afffbdb43348ef99def84f171e2e7418aa1b5228e97f2193d15744a9b9c4e3f3d18613f6445abc1732cfe4dc341fb4ff7438e05828e8ded1349f2d1b1b44946a4c7f339874e5403746d84bb91bfbbfa564c88dbelcfc

o client pkt(s), 201 server pkt(s), 0 turn(s).

Conversation entière (287 kB) Afficher les données comme Brut Flux 8

Trouver : Trouver Suivant

Filtrer ce flux Imprimer Enregistrer sous... Retour Fermer Aide

Et en cliquant sur "enregistrer" vers une image png, vous devriez obtenir ce que vous attendez :

