

sedian

Seguridad Digital
de Andalucía

Guía del usuario

Análisis de tráfico de red: Técnicas avanzadas de detección y análisis de red

V1.0



Junta de Andalucía

Algo sobre mí

- Responsable de negocio de seguridad en **SEMIC**
- Autor del blog **hacking-etico.com**
- Fundador de la comunidad **Hack&Beers**

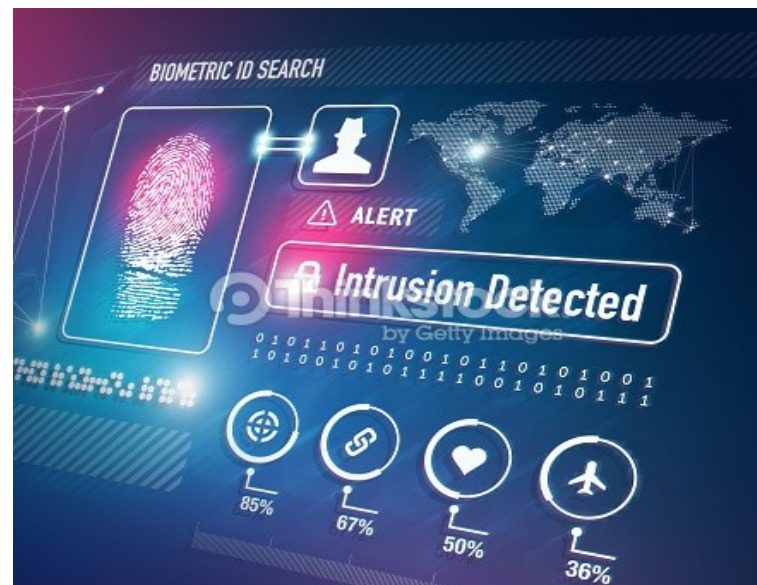


OBJETIVOS

- Entender la finalidad del análisis de tráfico de red.
- Aprender diferentes métodos de análisis de tráfico de red en función de la finalidad.
- Diferenciar entre *Life Analysis* vs *Death Analysis*.
- Aprender a utilizar herramientas de captura y análisis de tráfico.
- Aprender a utilizar IDS para la detección de amenazas.
- Aprender a recolectar información para facilitar su análisis.

Análisis de tráfico de red: ¿Para qué?

- Detección de problemas de **rendimiento**.
- Detección de posibles **amenazas**.
- Detección de **ataques**.
- Pruebas de seguridad ofensiva para mejorar la seguridad defensiva (**Red** vs **Blue**).
- Analizar un **incidente** de seguridad en su fase de detección, análisis, contención, erradicación, lecciones aprendidas...
- **Mediciones y métricas** de seguridad.
- **Mejora continua**.



Como respuesta a un incidente

- ***Life Analysis***

- Artefactos latentes en la red
- Análisis del tráfico
 - Analizadores / Sniffers
 - FW / IDS / IPS / NTA / UEBA

- ***Death Analysis***

- Posibles rastros en los sistemas
 - pcap / logs
- Análisis del tráfico
 - Analizadores / IDS / SIEM



Ataque, Detección, Respuesta y Análisis



Herramientas a utilizar

- Durante esta sesión se verán algunos ejemplos de usos de las siguientes herramientas de análisis, detección y recolección.
- **NetworkMiner** y **Wireshark** para el análisis de tráfico.
- **Snort** como IDS para la detección de amenazas / ataques.
- Stack de **ELK** para la recolección de logs y visualización amigable.



Ya tengo el arsenal, ¿y ahora qué analizo?

- ¿Atacante externo o interno?
- ¿Qué tácticas ha seguido el atacante?
- ¿Qué técnicas ha utilizado el atacante?
- **MITRE ATT&CK**
 - Desarrollado por MITRE.
 - Matriz de referencia de posibles procedimientos, tácticas y técnicas utilizadas.
 - Categorizados por Sistemas Operativos, Dispositivos Móviles, Entornos Cloud o ICS (Sistemas de Control Industrial)



Tácticas y técnicas de las APT

- **APT** (*Advanced Persistent Threat*)
- Diferentes grupos de operaciones APT
- MITRE tiene cerca de 100 operaciones APT identificadas y registradas en su ATT&CK
 - *Lazarus Group, Equation Group (Shadow Brokers), Fancy Bear (APT 28), Machete, Elfin (APT 33)...*
- Tácticas y técnicas en común.
- Nos puede servir para saber cuáles son las más usadas.



MITRE ATT&CK: Navigator

MITRE ATT&CK® Navigator

Lazarus x

FIN7 x

Equation x

layer by operation x

layer x

+

selection controls

layer controls

technique controls

Initial Access

9 techniques

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (1/3)

Replication Through Removable Media

Supply Chain Compromise (0/3)

Trusted Relationship

Valid Accounts (0/3)

Execution

10 techniques

Command and Scripting Interpreter (1/7)

Exploitation for Client Execution

Inter-Process Communication (0/2)

Native API

Scheduled Task/Job (0/5)

Shared Modules

Software Deployment Tools

System Services (0/2)

User Execution (1/2)

Windows Management Instrumentation

Persistence

17 techniques

Account Manipulation (0/2)

BITS Jobs

Boot or Logon Autostart Execution (2/11)

Boot or Logon Initialization Scripts (0/5)

Browser Extensions

Compromise Client Software Binary

Create Account (0/2)

Create or Modify System Process (1/4)

Event Triggered Execution (0/15)

External Remote Services

Hijack Execution Flow (0/11)

Office Application Startup (0/6)

Pre-OS Boot (1/3)

Scheduled Task/Job (0/5)

Server Software Component (0/3)

Privilege Escalation

12 techniques

Abuse Elevation Control Mechanism (0/4)

Access Token Manipulation (1/5)

Boot or Logon Autostart Execution (2/11)

Boot or Logon Initialization Scripts (0/5)

Create or Modify System Process (1/4)

Event Triggered Execution (0/15)

Exploitation for Privilege Escalation

Group Policy Modification

Hijack Execution Flow (0/11)

Process Injection (1/11)

Scheduled Task/Job (0/5)

Valid Accounts (0/3)

Defense Evasion

32 techniques

Abuse Elevation Control Mechanism (0/4)

Access Token Manipulation (1/5)

BITS Jobs

Deobfuscate/Decode Files or Information

Direct Volume Access

Execution Guardrails (0/1)

Exploitation for Defense Evasion

File and Directory Permissions Modification (0/2)

Group Policy Modification

Hide Artifacts (1/6)

Hijack Execution Flow (0/11)

Impair Defenses (2/5)

Indicator Removal on Host (2/6)

Indirect Command Execution

Masquerading (2/6)

Modify Authentication Process (0/3)

Credential Access

13 techniques

Brute Force (1/4)

Credentials from Password Stores (0/3)

Exploitation for Credential Access

Forced Authentication

Input Capture (1/4)

Man-in-the-Middle (0/1)

Modify Authentication Process (0/2)

Network Sniffing

OS Credential Dumping (1/8)

Steal or Forge Kerberos Tickets (0/3)

Steal Web Session Cookie

Two-Factor Authentication Interception

Unsecured Credentials (0/5)

Discovery

22 techniques

Account Discovery (0/3)

Application Window Discovery

Browser Bookmark Discovery

Domain Trust Discovery

File and Directory Discovery

Network Service Scanning

Network Share Discovery

Network Sniffing

Password Policy Discovery

Peripheral Device Discovery

Permission Groups Discovery (0/2)

Process Discovery

Query Registry

Remote System Discovery

Software Discovery (0/1)

System Information Discovery

System Network Configuration Discovery

Lateral Movement

9 techniques

Exploitation of Remote Services

Internal Spearphishing

Lateral Tool Transfer

Remote Service Session Hijacking (0/2)

Remote Services (2/6)

Replication Through Removable Media

Software Deployment Tools

Taint Shared Content

Use Alternate Authentication Material (0/2)

Collection

15 techniques

Archive Collected Data (2/2)

Audio Capture

Automated Collection

Clipboard Data

Data from Information Repositories (0/1)

Data from Local System

Data from Network Shared Drive

Data from Removable Media

Data Staged (1/2)

Email Collection (0/3)

Input Capture (1/4)

Man in the Browser

Man-in-the-Middle (0/1)

Screen Capture

Video Capture

Command and Control

16 techniques

Application Layer Protocol (1/4)

Communication Through Removable Media

Data Encoding (1/2)

Data Obfuscation (1/2)

Dynamic Resolution (0/3)

Encrypted Channel (1/2)

Fallback Channels

Ingress Tool Transfer

Multi-Stage Channels

Non-Application Layer Protocol

Non-Standard Port

Protocol Tunneling

Proxy (1/4)

Remote Access Software

Traffic Signaling (0/1)

Web Service (1/3)

Exfiltration

8 techniques

Automated Exfiltration

Data Transfer Size Limits

Exfiltration Over Alternative Protocol (1/2)

Exfiltration Over C2 Channel

Exfiltration Over Other Network Medium (0/1)

Exfiltration Over Physical Medium (0/1)

Exfiltration Over Web Service (0/2)

Scheduled Transfer

Impact

13 techniques

Account Access Removal

Data Destruction

Data Encrypted for Impact

Data Manipulation (0/3)

Defacement (1/2)

Disk Wipe (2/2)

Endpoint Denial of Service (0/4)

Firmware Corruption

Inhibit System Recovery

Network Denial of Service (0/2)

Resource Hijacking

Service Stop

System Shutdown/Reboot

Ahora sí, pasemos a analizar tráfico

 arp_spoof.pcap	06/01/2014 23:57	Wireshark capture...	27 KB
 heart.pcap	20/04/2014 20:49	Wireshark capture...	25 KB
 hydra_ftp.pcap	25/09/2012 21:27	Wireshark capture...	30 KB
 hydra_telnet.pcap	12/01/2014 12:50	Wireshark capture...	64 KB
 nmap.pcap	25/09/2012 21:27	Wireshark capture...	169 KB
 ntp.pcap	09/01/2014 16:35	Wireshark capture...	4 KB
 snmp.pcap	09/01/2014 16:36	Wireshark capture...	12 KB
 with_pdf.pcap	05/01/2014 20:27	Wireshark capture...	350 KB

contagio

malware dump

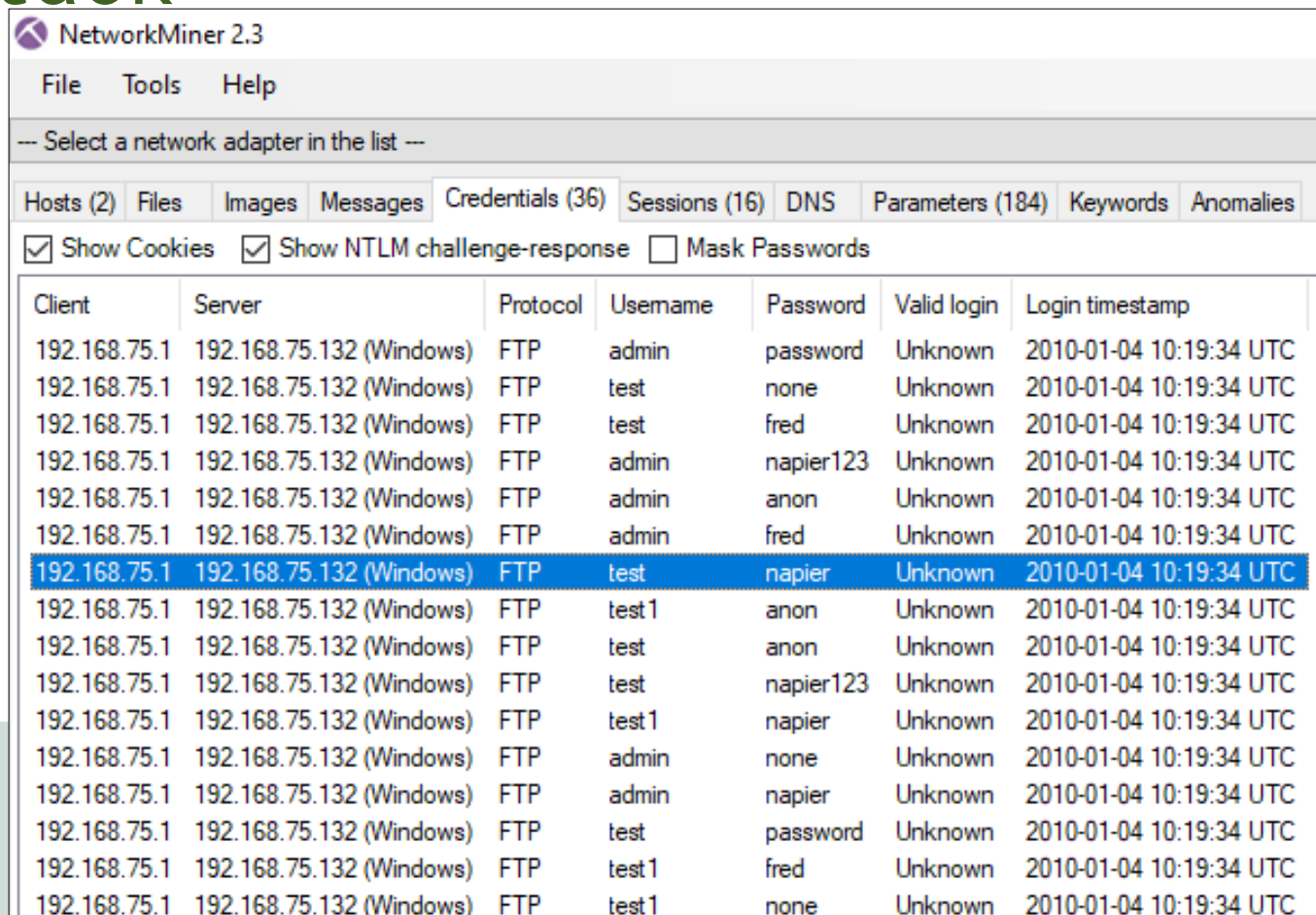
[Home](#) [Search the Interwebs](#)

[Mobile and print friendly view |](#)

THURSDAY, FEBRUARY 19, 2015

Collection of Pcap files from malware analysis

NetworkMiner: FTP Brute Force Attack



NetworkMiner 2.3

File Tools Help

-- Select a network adapter in the list --

Hosts (2) Files Images Messages Credentials (36) Sessions (16) DNS Parameters (184) Keywords Anomalies

☒ Show Cookies ☒ Show NTLM challenge-response ☐ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	password	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	none	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	fred	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	napier123	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	anon	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	fred	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	napier	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test1	anon	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	anon	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	napier123	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test1	napier	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	none	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	admin	napier	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test	password	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test1	fred	Unknown	2010-01-04 10:19:34 UTC
192.168.75.1	192.168.75.132 (Windows)	FTP	test1	none	Unknown	2010-01-04 10:19:34 UTC

NetworkMiner: Extracción de ficheros

NetworkMiner 2.3

File Tools Help

--- Select a network adapter in the list ---

Hosts (5) Files (7) Images Messages Credentials (3) Sessions (4) DNS (4) Parameters (143) Keywords Anomalies

Filter keyword:

Frame nr.	Filename	Extension	Size	Source host	S. port
4	url.C4823F33[1].html	html	413 B	173.194.34.88 [www.google.co.uk]	TCP 80
32	favicon[1].ico	ico	261 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80
36	pdf[5].pdf	pdf	65 536 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80
116	pdf[6].pdf	pdf	10 778 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80
165	pdf[7].pdf	pdf	10 778 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80
166	pdf[8].pdf	pdf	10 778 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80
306	pdf[9].pdf	pdf	10 778 B	98.139.134.174 [p9p.geo.asbs.yahoodns.net] [www.pdf99...	TCP 80

Open file

Open folder

Calculate MD5 / SHA1 / SHA256 hash

Auto-resize all columns

OSINT hash lookup isn't available in the f

Sample submission isn't available in the fr

samples

Archivo Inicio Compartir Vista

Anclar al Acceso rápido Copiar Pegar

Portapapeles Organizar

Nueva carpeta Nuevo

Propiedades Abrir

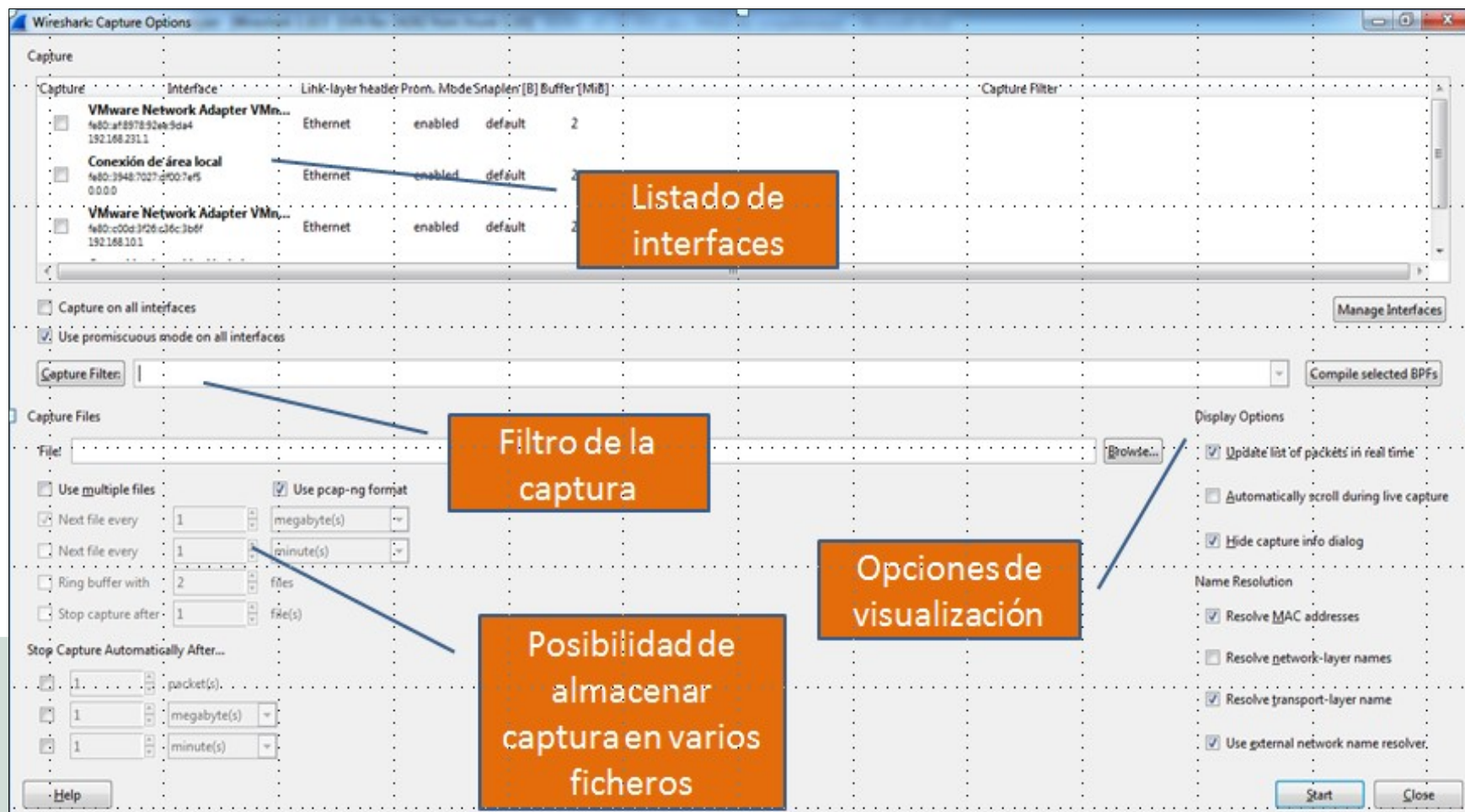
Seleccionar

← → ↑ << 98.139.134.174 > TCP-80 > samples

Buscar en ...

Nombre	Fecha de modificación
pcaps	
Videos	
OneDrive - Personal	
Datos adjuntos	
Documentos	
Favoritos	
Favoritos compartidos	
Imágenes	
pdf.pdf	05/01/2014 20:16
pdf[1].pdf	05/01/2014 20:16
pdf[2].pdf	05/01/2014 20:16
pdf[3].pdf	05/01/2014 20:16
pdf[4].pdf	05/01/2014 20:16
pdf[5].pdf	05/01/2014 20:16
pdf[6].pdf	05/01/2014 20:16
pdf[7].pdf	05/01/2014 20:16

Wireshark: Opciones de captura



Wireshark: Filtro de captura

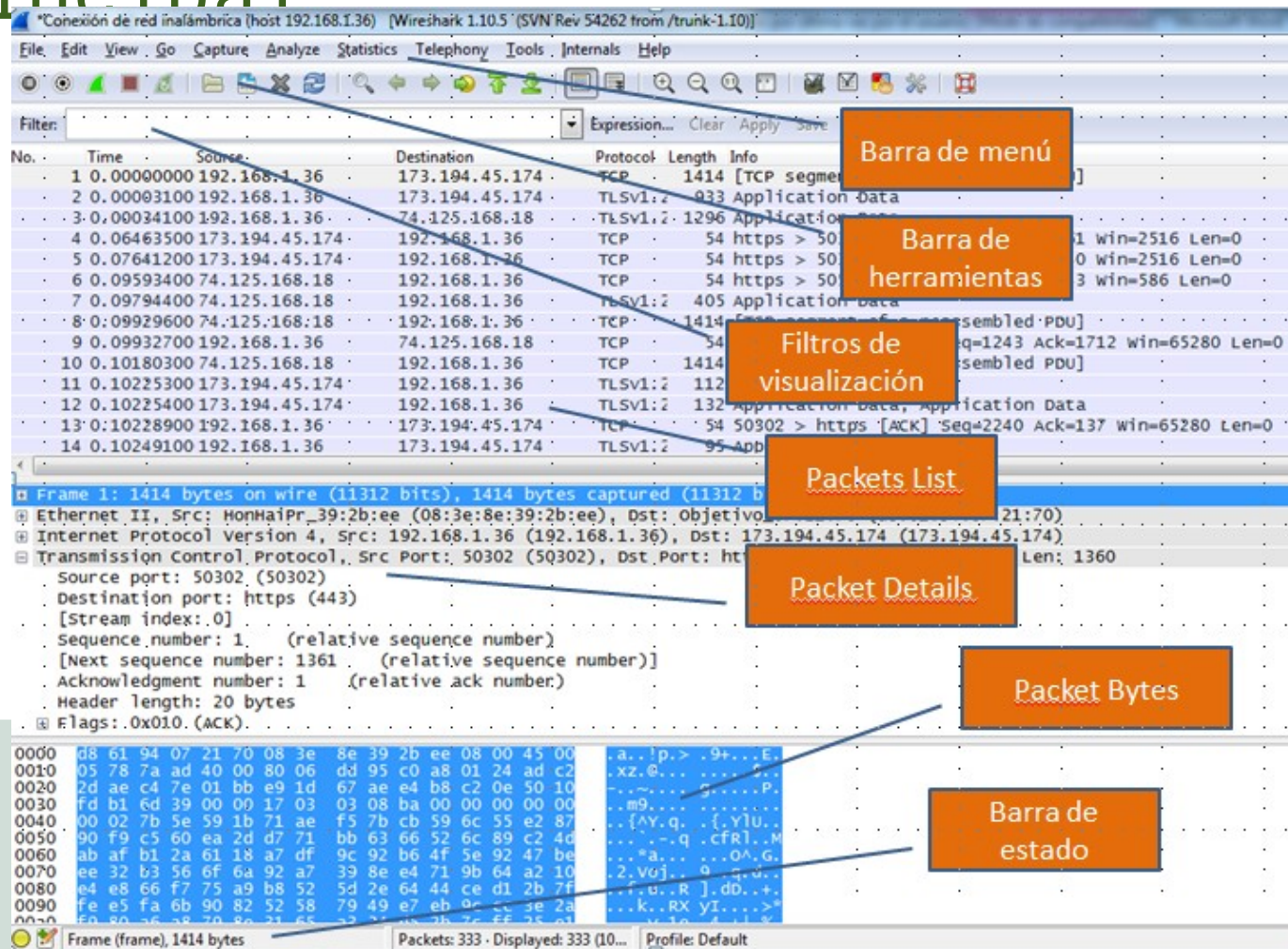
*Conexión de red inalámbrica (host 192.168.1.36) [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.36	173.194.45.174	TCP	1414	[TCP segment of a reassembled PDU]
2	0.00003100	192.168.1.36	173.194.45.174	TLSv1.2	933	Application Data
3	0.00034100	192.168.1.36	74.125.168.18	TLSv1.2	1296	Application Data
4	0.06463500	173.194.45.174	192.168.1.36	TCP	54	https > 50302 [ACK] Seq=1 Ack=1361 win=2516 Len=0
5	0.07641200	173.194.45.174	192.168.1.36	TCP	54	https > 50302 [ACK] Seq=1 Ack=2240 win=2516 Len=0
6	0.09593400	74.125.168.18	192.168.1.36	TCP	54	https > 50532 [ACK] Seq=1 Ack=1243 win=586 Len=0
7	0.09794400	74.125.168.18	192.168.1.36	TLSv1.2	405	Application Data
8	0.09929600	74.125.168.18	192.168.1.36	TCP	1414	[TCP segment of a reassembled PDU]
9	0.09932700	192.168.1.36	74.125.168.18	TCP	54	50532 > https [ACK] Seq=1243 Ack=1712 win=65280 Len=0
10	0.10180300	74.125.168.18	192.168.1.36	TCP	1414	[TCP segment of a reassembled PDU]
11	0.10225300	173.194.45.174	192.168.1.36	TLSv1.2	112	Application Data
12	0.10225400	173.194.45.174	192.168.1.36	TLSv1.2	132	Application Data, Application Data
13	0.10228900	192.168.1.36	173.194.45.174	TCP	54	50302 > https [ACK] Seq=2240 Ack=137 win=65280 Len=0
14	0.10249100	192.168.1.36	173.194.45.174	TLSv1.2	95	Application Data
15	0.10358300	74.125.168.18	192.168.1.36	TCP	1414	[TCP segment of a reassembled PDU]
16	0.10361400	192.168.1.36	74.125.168.18	TCP	54	50532 > https [ACK] Seq=1243 Ack=4432 win=65280 Len=0

Wireshark: Partes de la pantalla principal



Wireshark: Empezar por las estadísticas

Wireshark · Endpoints · wireshark_E24003AF-EBD7-4EAE-848F-266D9EE03348_20200709181605_a42664.pcapng

Ethernet · 7		IPv4 · 20		IPv6 · 2		TCP · 54		UDP			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
	355	239 k	117	24 k	238	215 k	—	—	—	—	
	150	174 k	131	172 k	19	2409	—	—	—	—	
	5	91	54 k	59	38 k	32	16 k	—	—	—	
		36	2268	18	1080	18	1188	—	—	—	
	31	16	1298	10	779	6	519	—	—	—	
	0	13	858	0	0	13	858	—	—	—	
	1	9	1003	5	775	4	228	—	—	—	
	50	8	1196	4	673	4	523	—	—	—	
	6	6	544	2	220	4	324	—	—	—	
	4	6	480	2	186	4	294	—	—	—	
	37	5	712	3	529	2	183	—	—	—	
	2	3	381	1	229	2	152	—	—	—	
		3	381	1	229	2	152	—	—	—	
	6	3	240	1	93	2	147	—	—	—	
	4	3	240	1	93	2	147	—	—	—	
		2	132	0	0	2	132	—	—	—	
	89	2	161	1	107	1	54	—	—	—	
		1	46	1	46	0	0	—	—	—	
		1	60	0	0	1	60	—	—	—	
		1	46	0	0	1	46	—	—	—	

Wireshark: Identificando tráfico cryptolocker

Wireshark · Conversations **cryptolocker.pcap**

Ethernet · 5	IPv4 · 8	IPv6	TCP · 2	UDP · 7							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
4.2.2.2	192.168.248.165	262	30 k	131	20 k	131	10 k	0.296619	168.1672	954	
8.8.8.8	192.168.248.165	262	30 k	131	20 k	131	10 k	0.296552	168.1339	954	
176.119.0.216	192.168.248.165	24	2155	12	1582	12	1574	168.436223	47.3661	267	
192.168.248.174	239.255.255.250							15700	6.0255	3003	
192.168.248.165	224.0.0.22							0000	16.4852	157	
192.168.248.165	192.168.248.254							8419	10.8493	0	
65.55.21.21	192.168.248.165							5440	6.1616	0	
65.55.56.206	192.168.248.165							0273	0.1042	6911	

Apply as Filter ▶ Selected ▶ A ↔ B

Prepare a Filter ▶ Not Selected ▶ A → B

Find ▶ ...and Selected ▶ B → A

Colorize ▶ ...or Selected ▶ A ↔ Any

...and not Selected ▶ A → Any

...or not Selected ▶ Any → A

Any → B

Any → B

B → Any

Wireshark: Filtro por host y protocolo

Filter: ip.addr == 192.168.1.36							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
710	8.542759000	195.57.81.97	192.168.1.36	TCP	1414	[TCP segment of a reassembled PDU]				
711	8.542761000	195.57.81.97	192.168.1.36	HTTP	289	HTTP/1.1 200 OK (PNG)				
712	8.542825000	192.168.1.36	195.57.81.97	TCP	54	50811 > http [ACK] Seq=590 Ack=1596 win=66640 Len=0				
713	8.543304000	80.58.61.250	192.168.1.36	DNS	97	Standard query response 0x8352 A 82.194.88.23				
714	8.543948000	192.168.1.36	80.58.61.250	DNS	70	Standard query 0xcab3 A ethack.com				
715	8.544759000	80.58.61.250	192.168.1.36	DNS	89	Standard query response 0xb835 A 195.53.165.3				
716	8.545299000	192.168.1.36	80.58.61.250	DNS	78	Standard query 0xe4e7 A hacklabcordoba.com				
717	8.545329000	195.57.81.97	192.168.1.36	TCP	1414	[TCP segment of a reassembled PDU]				
Filter: ip.addr == 192.168.1.36 && http							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
711	8.542761000	195.57.81.97	192.168.1.36	HTTP	289	HTTP/1.1 200 OK (PNG)				
718	8.549879000	195.57.81.97	192.168.1.36	HTTP	226	HTTP/1.1 200 OK (PNG)				
1512	75.850007000	192.168.1.36	95.130.49.13	HTTP	540	GET / HTTP/1.1				
1523	76.356153000	95.130.49.13	192.168.1.36	HTTP	97	HTTP/1.1 200 OK (text/html)				
1525	76.394862000	192.168.1.36	95.130.49.13	HTTP	594	GET /portal_css/THEME%20svt/base-c				
1531	76.396788000	192.168.1.36	74.125.71.95	HTTP	383	GET /css?family=Maven+Pro:500 HTTP				
1538	76.474173000	192.168.1.36	95.130.49.13	HTTP	601	GET /portal_css/THEME%20svt/ploneC				
1540	76.485102000	74.125.71.95	192.168.1.36	HTTP	655	HTTP/1.1 200 OK (text/css)				
1552	76.493984000	192.168.1.36	95.130.49.13	HTTP	588	GET /portal_javascripts/THEME%20sv				
1553	76.493989000	192.168.1.36	95.130.49.13	HTTP	617	GET /portal_javascripts/THEME%20sv				
1556	76.494235000	192.168.1.36	95.130.49.13	HTTP	604	GET /portal_javascripts/THEME%20sv				
1559	76.496069000	192.168.1.36	95.130.49.13	HTTP	554	GET /jquery.tools.min.js HTTP/1.1				

Wireshark: Filtro y exportación de objetos

with_pdf.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.content_type == "application/pdf"

No.	Time	Source	Destination	Protocol	Length	Info
114	3.236365	98.139.134.174	192.168.47.171	HTTP	391	HTTP/1.1 206 Partial Content (application/pdf)
163	4.133397	98.139.134.174	192.168.47.171	HTTP	459	HTTP/1.1 206 Partial Content (application/pdf)
241	4.596883	98.139.134.174	192.168.47.171	HTTP	1350	HTTP/1.1 206 Partial Content (application/pdf)
305	5.764174	98.139.134.174	192.168.47.171	HTTP	650	HTTP/1.1 206 Partial Content (application/pdf)
378	6.817552	98.139.134.174	192.168.47.171	HTTP	269	HTTP/1.1 206 Partial Content (application/pdf)

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
7	www.google.co.uk	text/html	413 bytes	url?sa=t&rct=j&q=
39	www.pdf995.com	image/x-icon	261 bytes	favicon.ico
114	www.pdf995.com	application/pdf	65 kB	pdf.pdf
163	www.pdf995.com	application/pdf	40 kB	pdf.pdf
241	www.pdf995.com	application/pdf	65 kB	pdf.pdf
305	www.pdf995.com	application/pdf	65 kB	pdf.pdf
378	www.pdf995.com	application/pdf	65 kB	pdf.pdf

Wireshark: Analizando APT Taidoor

Wireshark · Conversations · Taidoor_APT.pcap

Ethernet · 9 IPv4 · 5 IPv6 TCP · 34 UDP · 4											
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.253.132	211.234.117.141	263	21 k	142	14 k	121	7260	82.873730	83.7390	1370	
172.16.253.1	172.16.253.255	9	2648	9	2648	0	0	0.000000	157.9341	134	
172.16.253.132	224.0.0.22	7	378	7	378	0	0	73.500396	15.8920	190	
172.16.253.132	172.16.253.254	4	808	0	0	4	808	69.079289	1.0034	0	
0.0.0.0	255.255.255.255	2	697	2	697	0	0	69.078588	1.0017	5566	

ip.addr==172.16.253.132 && ip.addr==211.234.117.141

No.	Time	Source	Destination	Protocol	Length	Info
23	82.873730	172.16.253.132	211.234.117.141	TCP	62	1229 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
24	83.139209	211.234.117.141	172.16.253.132	TCP	60	443 → 1229 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
25	83.139293	172.16.253.132	211.234.117.141	TCP	54	1229 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
26	83.139466	172.16.253.132	211.234.117.141	HTTP	248	GET /gmzlk.php?id=031870111D309GE67E HTTP/1.1
27	83.139619	211.234.117.141	172.16.253.132	TCP	60	443 → 1229 [ACK] Seq=1 Ack=195 Win=64240 Len=0
28	83.414936	211.234.117.141	172.16.253.132	TCP	60	443 → 1229 [FIN, PSH, ACK] Seq=1 Ack=195 Win=64240 Len=0
29	83.415014	172.16.253.132	211.234.117.141	TCP	54	1229 → 443 [ACK] Seq=195 Ack=2 Win=64240 Len=0
30	83.415295	172.16.253.132	211.234.117.141	TCP	54	1229 → 443 [FIN, ACK] Seq=195 Ack=2 Win=64240 Len=0
31	83.415426	211.234.117.141	172.16.253.132	TCP	60	443 → 1229 [ACK] Seq=2 Ack=196 Win=64239 Len=0
32	85.404991	172.16.253.132	211.234.117.141	TCP	62	1230 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
33	85.638192	211.234.117.141	172.16.253.132	TCP	60	443 → 1230 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
34	85.638231	172.16.253.132	211.234.117.141	TCP	54	1230 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
35	85.638395	172.16.253.132	211.234.117.141	HTTP	248	GET /viswi.php?id=001090111D309GE67E HTTP/1.1
36	85.638544	211.234.117.141	172.16.253.132	TCP	60	443 → 1230 [ACK] Seq=1 Ack=195 Win=64240 Len=0
37	85.912159	211.234.117.141	172.16.253.132	TCP	60	443 → 1230 [FIN, PSH, ACK] Seq=1 Ack=195 Win=64240 Len=0

Wireshark: Analizando APT Taidoor

ip.addr==172.16.253.132 && ip.addr==211.234.117.141 && http						
No.	Time	Source	Destination	Protocol	Length	Info
26	83.139466	172.16.253.132	211.234.117.141	HTTP	248	GET /gmzlk.php?id=031870111D309GE67E HTTP/1.1
35	85.638395	172.16.253.132	211.234.117.141	HTTP	248	GET /viswi.php?id=001090111D309GE67E HTTP/1.1
44	88.148314	172.16.253.132	211.234.117.141	HTTP	248	GET /obeaa.php?id=021655111D309GE67E HTTP/1.1
58	90.654033	172.16.253.132	211.234.117.141	HTTP	248	GET /vrjffj.php?id=007090111D309GE67E HTTP/1.1
64	93.157641	172.16.253.132	211.234.117.141	HTTP	248	GET /zqmse.php?id=013197111D309GE67E HTTP/1.1
73	95.600532	172.16.253.132	211.234.117.141	HTTP	248	GET /ivzdi.php?id=010093111D309GE67E HTTP/1.1
83	98.097168	172.16.253.132	211.234.117.141	HTTP	248	GET /ipubv.php?id=008698111D309GE67E HTTP/1.1
89	100.577374	172.16.253.132	211.234.117.141	HTTP	248	GET /zeyys.php?id=027858111D309GE67E HTTP/1.1
98	103.061175	172.16.253.132	211.234.117.141	HTTP	248	GET /gpaqi.php?id=027619111D309GE67E HTTP/1.1
107	105.519200	172.16.253.132	211.234.117.141	HTTP	248	GET /hgsht.php?id=019957111D309GE67E HTTP/1.1
113	108.051386	172.16.253.132	211.234.117.141	HTTP	248	GET /gftqr.php?id=022816111D309GE67E HTTP/1.1
119	110.518423	172.16.253.132	211.234.117.141	HTTP	248	GET /tyrae.php?id=005421111D309GE67E HTTP/1.1
128	112.989890	172.16.253.132	211.234.117.141	HTTP	248	GET /cidso.php?id=028428111D309GE67E HTTP/1.1
137	115.473787	172.16.253.132	211.234.117.141	HTTP	248	GET /xmeqb.php?id=006115111D309GE67E HTTP/1.1
146	117.952542	172.16.253.132	211.234.117.141	HTTP	248	GET /gauhx.php?id=010093111D309GE67E HTTP/1.1
155	120.430136	172.16.253.132	211.234.117.141	HTTP	248	GET /wwekz.php?id=015513111D309GE67E HTTP/1.1
165	122.018026	172.16.253.132	211.234.117.141	HTTP	248	GET /aufsa.php?id=018508111D309GE67E HTTP/1.1

Tshark: Muy útil para scripting

```
tshark -r test.pcap -R "http && tcp.dstport==80" -Tfields -e ip.dst
```

```
root@kali:/home/miguel/python/scripts# tshark -r test.pcap -R "http && tcp.dstport==80" -Tfields -e ip.dst
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser
up/CapturePrivileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
95.130.50.121
95.130.50.121
95.130.50.121
95.130.50.121
95.130.50.121
95.130.50.121
95.130.50.121
95.130.50.121
195.57.153.40
173.194.67.95
95.130.50.121
94.23.81.104
93.184.220.111
68.232.35.121
95.130.50.121
192.0.76.3
95.130.50.121
95.130.50.121
95.130.50.121
```

The background of the terminal window features the Kali Linux logo, which is a stylized blue dragon. Below the dragon, the text "KALI LINUX" is written in a bold, blue, blocky font. Underneath that, in a smaller, lighter blue font, is the tagline "The quieter you become, the more you are able to hear."

Tshark: Ejemplo de script de geolocalización

```
GNU nano 2.2.6 File: localiza2.py

#!/usr/bin/env python

import pygeoip
import sys

geo = pygeoip.GeoIP('GeoLiteCity.dat')

for line in sys.stdin:
    sys.stdout.write(line)
    print geo.record_by_addr(line)
```

```
tshark -r test.pcap -R "http && tcp.dstport==80" -Tfields -e ip.dst | sort -u | python localiza2.py
```

```
192.0.76.3
{'city': u'San Francisco', 'region_code': u'CA', 'area_code': 415, 'time_zone': 'America/Los_
CA', 'country_code3': 'USA', 'latitude': 37.7484000000000004, 'postal_code': u'94110', 'longit
nited States', 'continent': 'NA'}
195.57.153.40
{'city': None, 'region_code': None, 'area_code': 0, 'time_zone': None, 'dma_code': 0, 'metro
ostal_code': None, 'longitude': -4.0, 'country_code': 'ES', 'country_name': 'Spain', 'contine
195.57.81.80
{'city': None, 'region_code': None, 'area_code': 0, 'time_zone': None, 'dma_code': 0, 'metro
ostal_code': None, 'longitude': -4.0, 'country_code': 'ES', 'country_name': 'Spain', 'contine
23.214.148.124
{'city': u'Amsterdam', 'region_code': u'07', 'area_code': 0, 'time_zone': 'Europe/Amsterdam',
, 'latitude': 52.349999999999994, 'postal_code': None, 'longitude': 4.916699999999992, 'coun
t': 'EU'}
54.209.104.176
{'city': u'Ashburn', 'region_code': u'VA', 'area_code': 703, 'time_zone': 'America/New_York',
```

Snort: Detección off-line de ataques

- Utilización del IDS en modo off-line (packet dump [pcap])
- Uso de las reglas *community* de **Snort**
- Posibilidad de añadir reglas ET (**Emerging Threat**)
- Alertas en consola
- Para facilitar análisis, alertas a ficheros logs
- Posibilidad de explotación posterior de los ficheros logs



Snort: Detección off-line de ataques

```
ubuntu@ip-172-26-0-74:~$ nmap -v -sT 172.26.6.119 -A
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-09 19:47 UTC
```

```
NSE: Loaded 146 scripts for scanning.
```

```
NSE: Script Pre-scanning.
```

```
Initiating NSE at 19:47
```

```
Completed NSE at 19:47
```

```
07/09-19:47:46.691300 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:8087 -> 172.26.0.74:32986
Initiating NSE at 07/09-19:47:46.691319 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:47828 -> 172.26.6.119:1095
07/09-19:47:46.691326 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:1095 -> 172.26.0.74:47828
Completed NSE at 07/09-19:47:46.691351 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:36400 -> 172.26.6.119:541
07/09-19:47:46.691359 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:541 -> 172.26.0.74:36400
Initiating Ping S 07/09-19:47:46.691393 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:51826 -> 172.26.6.119:41511
07/09-19:47:46.691401 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:41511 -> 172.26.0.74:51826
Scanning 172.26.6 07/09-19:47:46.691418 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:32788 -> 172.26.6.119:3390
07/09-19:47:46.691425 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:3390 -> 172.26.0.74:32788
Completed Ping Sc 07/09-19:47:46.691453 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:41512 -> 172.26.6.119:8500
Initiating Paralle 07/09-19:47:46.691462 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:8500 -> 172.26.0.74:41512
07/09-19:47:46.691488 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:50422 -> 172.26.6.119:9099
Completed Paralle 07/09-19:47:46.691495 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:9099 -> 172.26.0.74:50422
Initiating Connec 07/09-19:47:46.691521 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:50712 -> 172.26.6.119:65129
07/09-19:47:46.691528 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:65129 -> 172.26.0.74:50712
07/09-19:47:46.691551 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:34830 -> 172.26.6.119:60443
07/09-19:47:46.691557 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:60443 -> 172.26.0.74:34830
07/09-19:47:46.691590 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:55480 -> 172.26.6.119:49176
07/09-19:47:46.691598 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:49176 -> 172.26.0.74:55480
07/09-19:47:46.691617 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:48816 -> 172.26.6.119:4321
07/09-19:47:46.691623 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:4321 -> 172.26.0.74:48816
07/09-19:47:46.691654 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:45746 -> 172.26.6.119:1090
07/09-19:47:46.691662 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.6.119:1090 -> 172.26.0.74:45746
07/09-19:47:46.691686 [**] [1:1000006:2] "Escaneo de puertos TCP" [**] [Priority: 0] {TCP} 172.26.0.74:49394 -> 172.26.6.119:3945
```

Snort: Análisis del log (/var/log/alert)

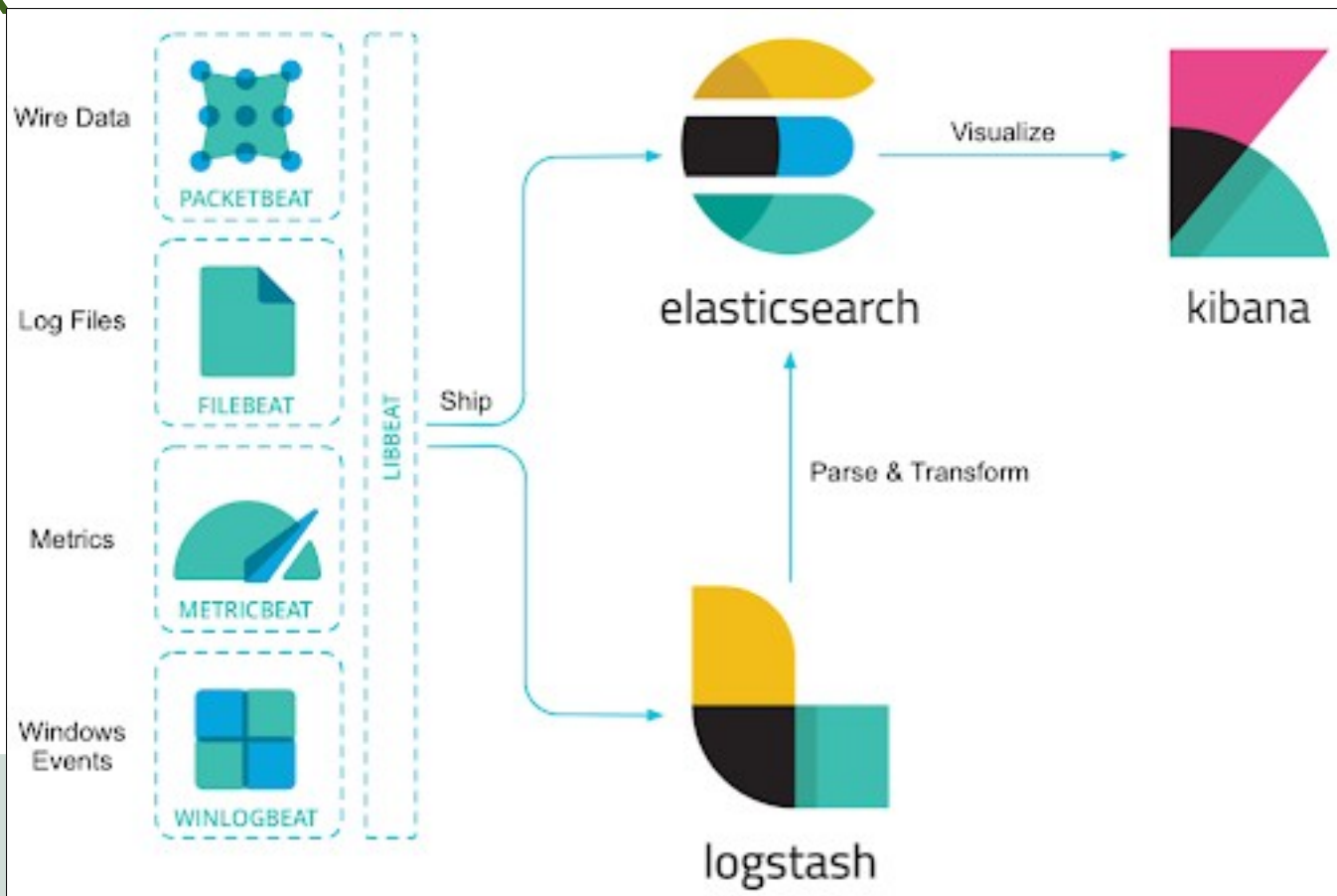
```
[Priority: 0]
07/09-17:52:24.004036 [REDACTED]:14731 -> 172.26.6.119:22
TCP TTL:99 TOS:0x0 ID:15776 IpLen:20 DgmLen:40 DF
***A*** Seq: 0x3B71AE0D Ack: 0xA1D865BD Win: 0x201 TcpLen: 20

[**] [1:1000006:2] "Escaneo de puertos TCP" [**]
[Priority: 0]
07/09-17:52:30.096057 [REDACTED]:15093 -> 172.26.6.119:22
TCP TTL:99 TOS:0x0 ID:15777 IpLen:20 DgmLen:40 DF
***A*** Seq: 0x4E9AC40B Ack: 0x612FF9B Win: 0x1171 TcpLen: 20

[**] [1:1000006:2] "Escaneo de puertos TCP" [**]
[Priority: 0]
07/09-17:52:33.393265 [REDACTED]:15093 -> 172.26.6.119:22
TCP TTL:99 TOS:0x0 ID:15778 IpLen:20 DgmLen:104 DF
***AP*** Seq: 0x4E9AC40B Ack: 0x612FF9B Win: 0x1171 TcpLen: 20

[**] [1:254:4] DNS SPOOF query response with TTL of 1 min. and no authority [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/09-17:54:27.797113 172.26.0.2:53 -> 172.26.6.119:46203
UDP TTL:255 TOS:0x0 ID:38732 IpLen:20 DgmLen:107
Len: 79
```

ELK: Facilitar análisis con stack ELK



ELK: Facilitar análisis con stack ELK

The screenshot displays the ELK Stack Discover interface. At the top, the 'Discover' tab is active. Below the navigation bar, the search query '"escaneo de puertos"' is entered in the search bar, with a 'KQL' button and a 'Refresh' button to its right. The left sidebar shows the 'file*' filter selected, with a search field for field names and a 'Filter by type' button. Under 'Selected fields', '@timestamp', 'host.ip', and 'message' are listed. Under 'Available fields', '_id', '_index', '_score', and '_type' are listed. The main panel shows 17 hits for the search query. The results are displayed in a table with columns for 'message', 'host.ip', and '@timestamp'. The 'message' column contains log entries for a port scan, with the phrase 'Escaneo de puertos' highlighted in yellow. The 'host.ip' column shows the IP address 172.26.6.119 and the source IP 172.17.0.1. The '@timestamp' column shows the date and time of the event.

message	host.ip	@timestamp
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:38.316
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:31.314
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:24.313
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:24.313
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:24.313
> [**] [1:1000006:2] "Escaneo de puertos TCP" [**]	172.26.6.119, fe80::c9:bfff:fec3:d208, 172.17.0.1, fe80::42:baff:fe81:6a97, fe80::9ca2:f4ff:fe7a:4b2e	Jul 9, 2020 @ 19:52:23.312

Gracias



<https://es.linkedin.com/in/miguel-angel-arroyo-moreno>



@miguel_arroyo76



marroyomo@gmail.com

avante
¿hasta dónde quieres llegar?

sedian Seguridad Digital
de Andalucía