

Webinar Gratuito

WireShark

V. 2

Alonso Eduardo Caballero Quezada



Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: ReYDeS@gmail.com

Sábado 18 de Octubre del 2014

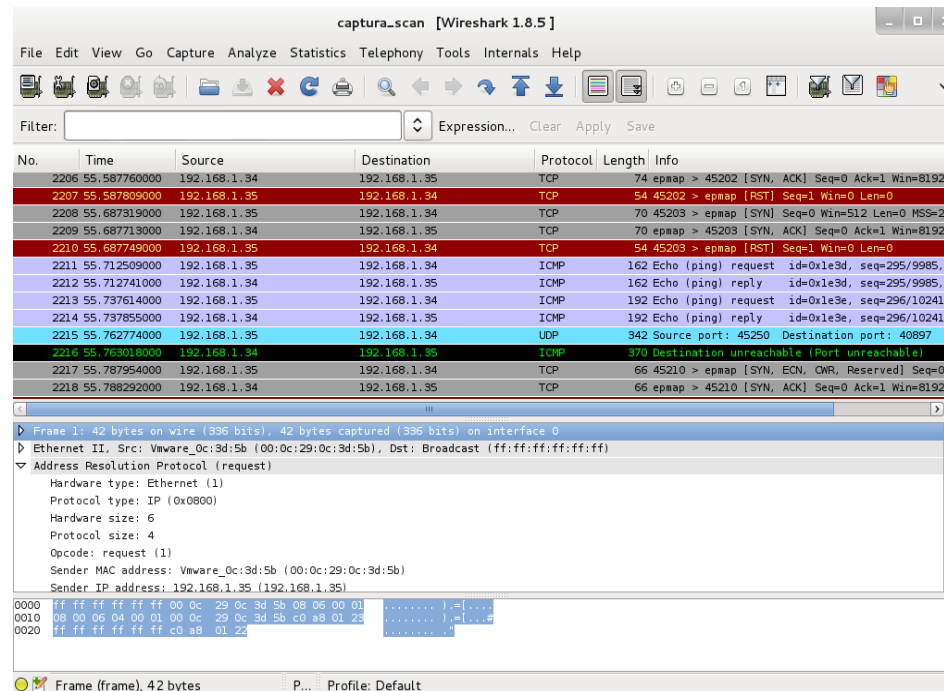
¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
-  @Alonso_ReYDeS
-  pe.linkedin.com/in/alonsocaballeroquezada/

¿Qué es Wireshark?

Wireshark es una herramienta open source que permite analizar paquetes de red, la cual permite capturar los paquetes de datos fluyendo a través de la red, para presentarlas de forma sencilla y comprensible.

Wireshark puede ser considerada como una cuchilla suiza, dado que puede ser utilizada en diferentes circunstancias como diagnosticar problemas de red, operaciones de seguridad, y aprendizaje de protocolos.



Beneficios de Wireshark

1. Soporte para varios protocolos.

Soporta una amplia variedad de protocolos desde TCP, UDP, HTTP, hasta GSM, MSN, BitTorrent, etc.

2. Interfaz de usuario amigable.

Interfaz gráfica interactiva que ayuda a analizar los paquetes capturados. Además de muchas opciones avanzadas de filtrado o exportación de paquetes.

3. Análisis de tráfico en “vivo”.

Puede capturar datos en “vivo” fluyendo por el cable de red y generar un reporte de la información sobre estos protocolos.

4. Proyecto open source.

Tiene la contribución de alrededor de 500 desarrolladores.

¿Como funciona Wireshark?

El proceso de sniffing con Wireshark puede ser dividido en tres fases.

1. Recolección.

Define la interfaz de red a modo promiscuo y de esta manera capturar los datos binarios en bruto fluyendo en la red.

2. Conversión.

Los trozos de datos binarios recolectados son luego convertidos en una forma “comprensible”. Los paquetes también pueden ser reemsamblados en base a su secuencia.

3. Análisis.

Implica el análisis de los datos capturados y reemsamblados. Involucra identificar el tipo de protocolo, el canal de comunicación, número de puerto, etc. A un nivel más avanzado también se puede analizar las cabeceras de los protocolos para mejor comprensión.

Curso Virtuales

Todos los Cursos están disponibles en Video.

Curso Virtual de Hacking Ético

http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Más Información:



caballero.alonso@gmail.com



<http://pe.linkedin.com/in/alonsocaballeroquezada/>



<http://www.reydes.com>

@Alonso_ReYDeS 

 ReYDeS

Demostraciones

Applications Places >_ root

captura_webs.pcap [Wireshark 1.10.2 (SVN Rev 51934 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	0.000000	192.168.0.12	190.113.220.54	DNS	74	Standard query 0x8d07 A www.google.com
2	0.000262	192.168.0.12	190.113.220.54	DNS	74	Standard query 0xbe6b AAAA www.google.com
3	2.993103	190.113.220.54	192.168.0.12	DNS	306	Standard query response 0x8d07 A 74.125.137.106 A 74.125.137.105
4	2.993417	190.113.220.54	192.168.0.12	DNS	238	Standard query response 0xbe6b AAAA 2607:f8b0:4002:c01::67
5	2.993809	192.168.0.12	74.125.137.106	TCP	74	50209 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva
6	3.249568	192.168.0.12	190.113.220.54	DNS	74	Standard query 0x2116 A www.google.com
7	3.993083	192.168.0.12	74.125.137.106	TCP	74	[TCP Retransmission] 50209 > http [SYN] Seq=0 Win=29200 Len=0 MSS=
8	4.914389	74.125.137.106	192.168.0.12	TCP	74	http > 50209 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_
9	4.914458	192.168.0.12	74.125.137.106	TCP	66	50209 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSva=73348 TSecr=1
10	4.914949	192.168.0.12	74.125.137.106	HTTP	365	GET / HTTP/1.1
11	6.338155	190.113.220.54	192.168.0.12	DNS	306	Standard query response 0x2116 A 74.125.137.106 A 74.125.137.105

.....

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- Ethernet II, Src: Vmware_0c:3d:5b (00:0c:29:0c:3d:5b), Dst: CiscoSpv_be:89:23 (f4:5f:d4:be:89:23)
- Internet Protocol Version 4, Src: 192.168.0.12 (192.168.0.12), Dst: 190.113.220.54 (190.113.220.54)
- User Datagram Protocol, Src Port: 55540 (55540), Dst Port: domain (53)
- Domain Name System (query)

.....

```
0000 f4 5f d4 be 89 23 00 0c 29 0c 3d 5b 08 00 45 00  . . . # . . ) . = [ . . E .
0010 00 3c 53 bb 40 00 40 11 8b 99 c0 a8 00 0c be 71  . < S . @ . @ . . . . . q
0020 dc 36 d8 f4 00 35 00 28 af 68 8d 07 01 00 00 01  . 6 . . 5 . ( . h . . . . .
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  . . . . . w w w . g o o g l
0040 65 03 63 6f 6d 00 00 01 00 01  . . . . . e . c o m . . . . .
```

File: "/root/captura_webs.pcap" 13... Profile: Default

root@kali: ~ captura_webs.pcap [...]

Más Material

Videos de 22 Webinars Gratuitos que he dictado sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

<http://www.reydes.com/d/?q=videos>

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

<http://www.reydes.com/d/?q=node/3>

Todos los artículos y documentos que he publicado.

<http://www.reydes.com/d/?q=node/2>

Mi Blog sobre temas de mi interés.

<http://www.reydes.com/d/?q=blog/1>

¡Muchas Gracias!

WireShark

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: ReYDeS@gmail.com

Sábado 18 de Octubre del 2014