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

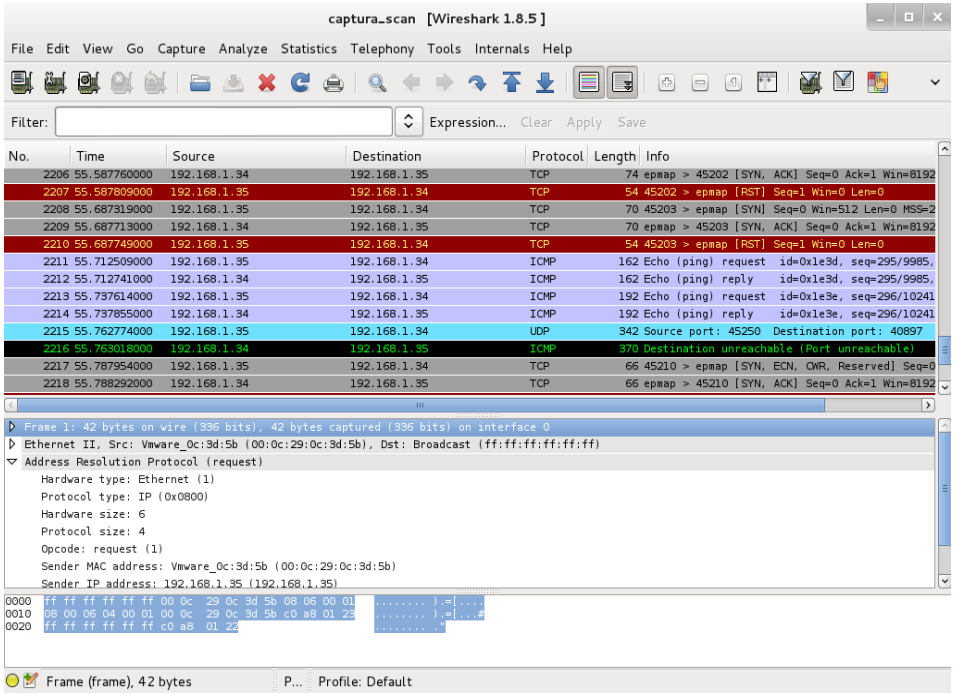
¿Quién Soy?

- 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.



Wireshark - http://www.wireshark.org

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.

Documentación - http://www.wireshark.org/docs/

¿Como funciona Wireshark?

El proceso de sniffing con Wireshark puede ser divido 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

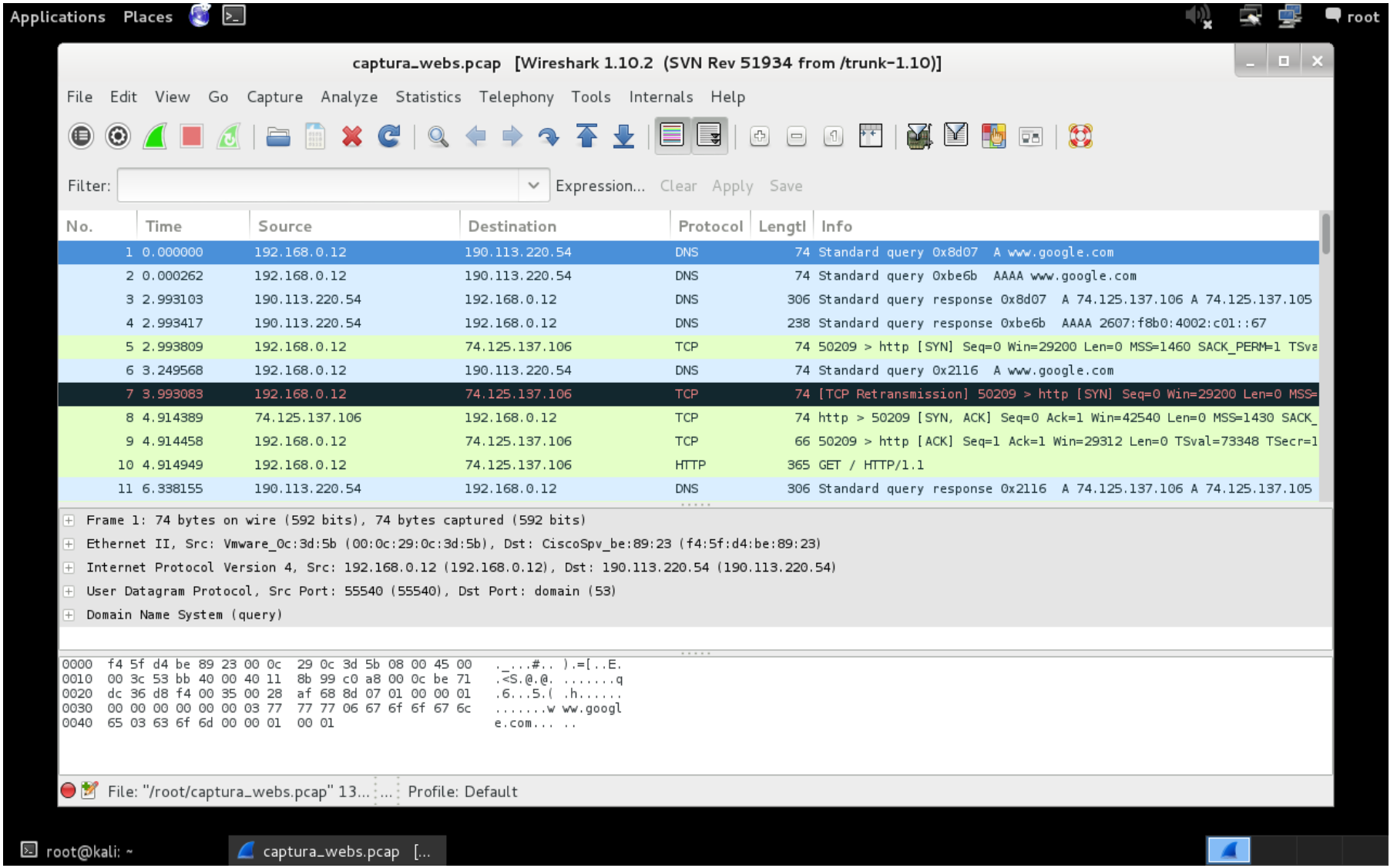
@Alonso_ReYDeS 


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


ReYDeS


http://www.reydes.com

Demostraciones



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