Webinar Gratuito

Capturar Tráfico de Red con Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Junio del 2021

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.reydes.com

reydes@gmail.com

+51 949 304 030

Forense de Redes

El Forense de redes es una de las ramas del forense digital, donde los datos a ser analizados están fluyendo en el tráfico de red, desde y hacia los sistemas bajo observación.

El propósito de este tipo de observación es recolectar información, obtener evidencia legalmente, establecer las causas de un evento, analizar el comportamiento de malware, entre otros.

Cuando un incidente se relaciona con un “cable” (inalámbrico), sea este exitoso o no, los artefactos dejados por este ayudan a entender y recrear no únicamente la intención sobre el incidente, sino también conocer las acciones realizadas.

* https://forensicswiki.xyz/wiki/index.php?title=Network_forensics

Captura de Evidencia en Red

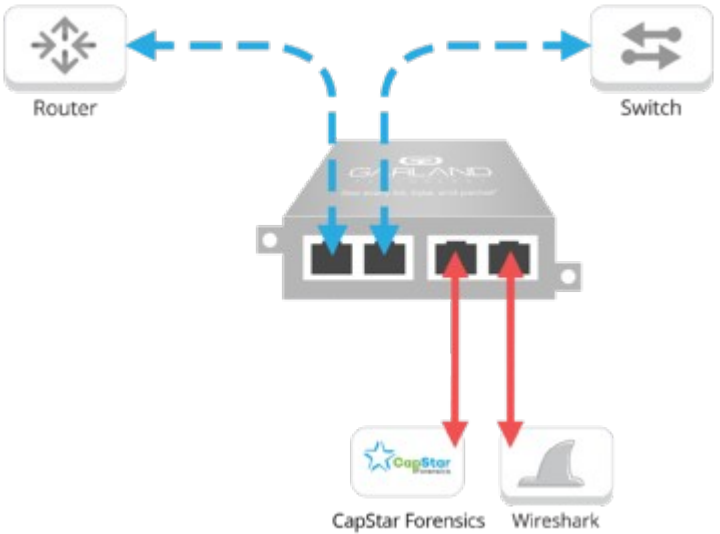
Primero es necesario tener una estrategia para luego planificar la adquisición de la evidencia.

Capturar evidencia requiere por si mismo documentar todos los sistemas accedidos y utilizados, capturar y guardar los flujos de datos, hacia las unidades de almacenamiento, además de recolectar los eventos (logs) desde los servidores, firewalls, etc. Existen algunas prácticas recomendadas para capturar evidencia:

- Crear copias de la evidencia con sus correspondientes hashes
- Nunca trabajar con la evidencia original
- Utilizar herramientas estándares
- Documentar todas las acciones realizadas

TAP (Derivación) de Red

Proporciona una manera de acceder hacia los datos fluyendo a través de la red. Se utiliza para un tercero vigile el tráfico entre dos puntos de la red. Tiene al menos tres puertos. Puerto A, Puerto B, y Puerto de Vigilancia. Un tap insertado entre A y B pasa todo el tráfico, pero también copia los mismos datos hacia el puerto de vigilancia.



Wireshark

Es un analizador para paquetes de red. Presenta los datos de paquetes capturados con tanto detalle como sea posible.

Se puede pensar en esta herramienta como en un dispositivo para examinar aquello suscitándose dentro de un cable de red, así como los electrónicos utilizan un voltímetro para examinar aquello suscitándose dentro de un cable electrónico, pero a un nivel más profundo.

En el pasado estas herramientas eran muy caras, propietarias o ambas. Con la llegada de Wireshark todo esto cambió. Pues es libre, de fuente abierta, y uno de los mejores analizadores de paquetes disponibles actualmente.

* https://www.wireshark.org

Wireshark (Cont.)

Capturar datos en vivo de la red es una de las principales características de Wireshark. El motor para captura de Wireshark proporciona lo siguiente:

- Capturar desde diferentes tipos de hardware de red, como Ethernet o 802.11
- Simultaneamente capturar desde múltiples interfaces de red
- Detener la captura basándose en diferentes eventos, como la cantidad de datos capturados, tiempo transcurrido, o el número de paquetes
- Simultaneamente decodificar paquetes mientras son capturados
- Filtrar paquetes, reduciendo la cantidad de datos a ser capturados
- Guardar los paquetes en múltiples archivos, opcionalmente rotándolosa un número fijo de archivos.

* https://www.wireshark.org/docs/wsug_html_chunked/ChapterCapture.html

Curso

Curso Virtual Forense de Redes 2021

Domingos 6, 13, 20 y 27 de Junio del 2021. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

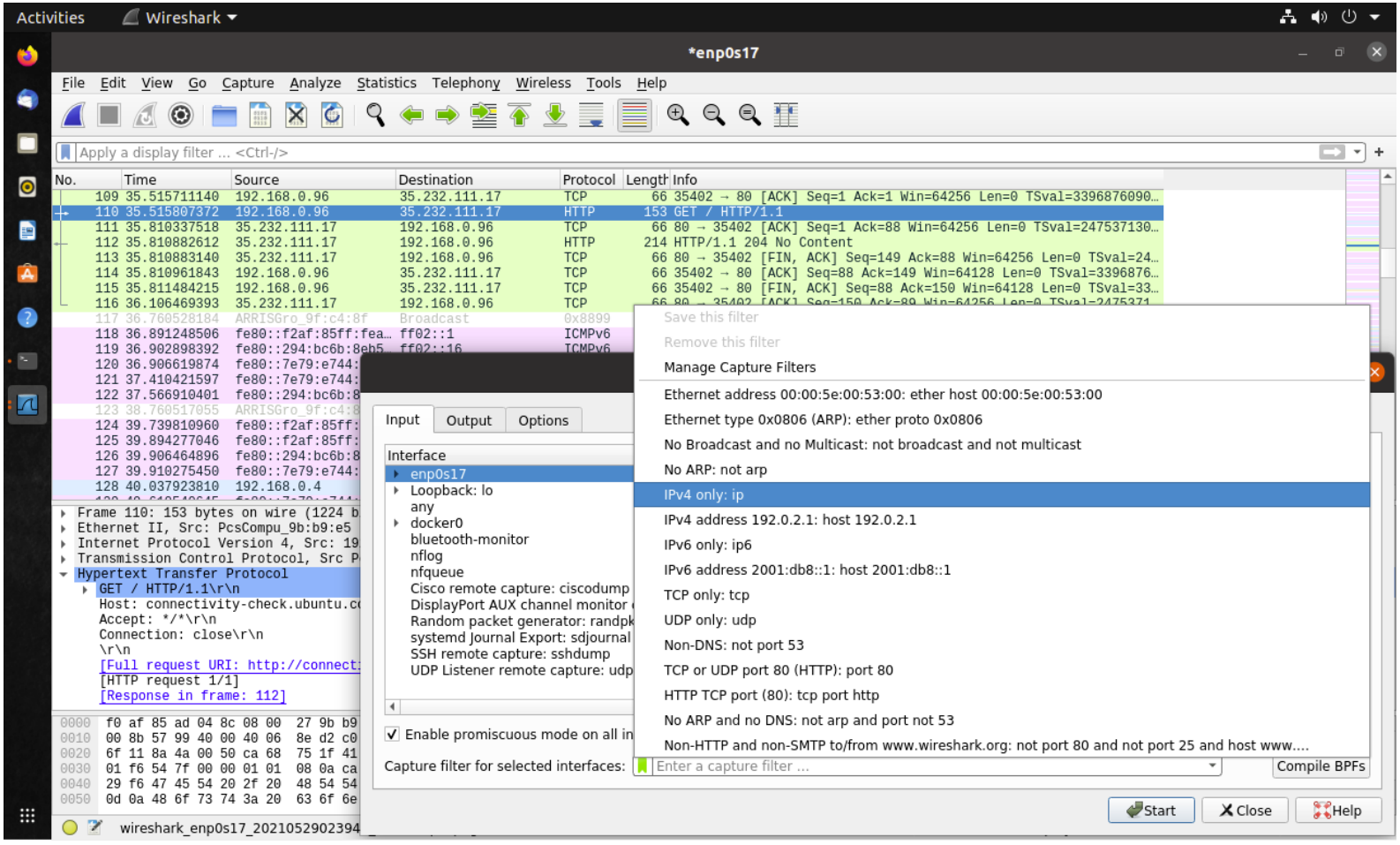
En la actualidad es muy común trabajar en cualquier investigación forense relacionada a un componente de red. El forense de computadoras siempre será un habilidad fundamental y crítica para esta profesión, pues obviar las comunicaciones de red, es similar a ignorar las imágenes proporcionadas por las cámaras de seguridad correspondientes a un crimen cometido. Ya sea se enfrente un incidente relacionado con una intrusión, un caso de robo de datos, uso indebido por parte de los empleados, o se esté involucrado en el descubrimiento pro activo del adversario, la red frecuentemente proporciona una vista incomparable del incidente. Esta evidencia puede proporcionar la prueba necesaria para mostrar intención, descubrir los atacantes han estado activos por meses o más, o incluso puede resultar útil para probar definitivamente la ocurrencia de un delito.

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP

Más Información: https://www.reydes.com/d/?q=Curso_Forense_de_Redes

e-mail: reydes@gmail.com Sitio Web: https://www.reydes.com

Demostraciones



Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

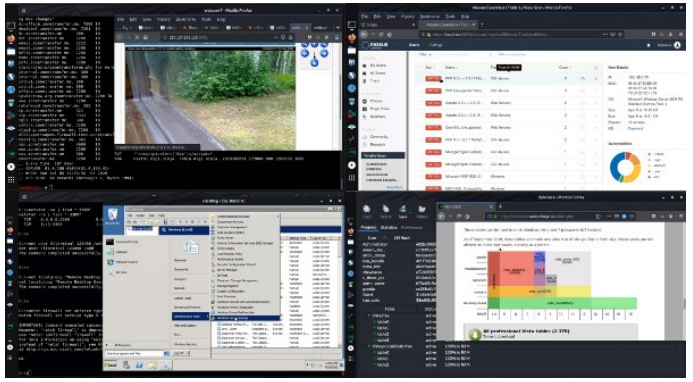
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

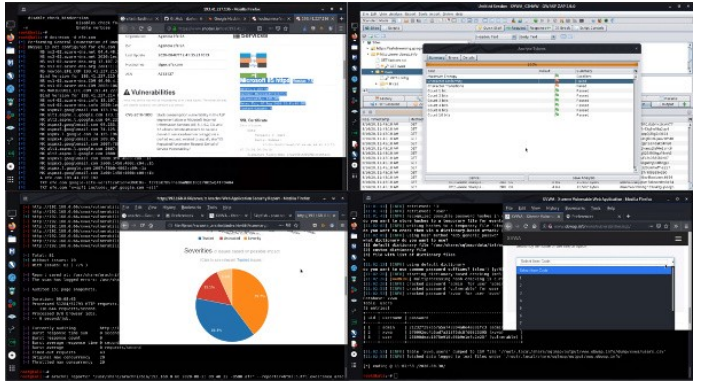
Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos





Más Contenidos

Videos de 66 webinars gratuitos

https://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

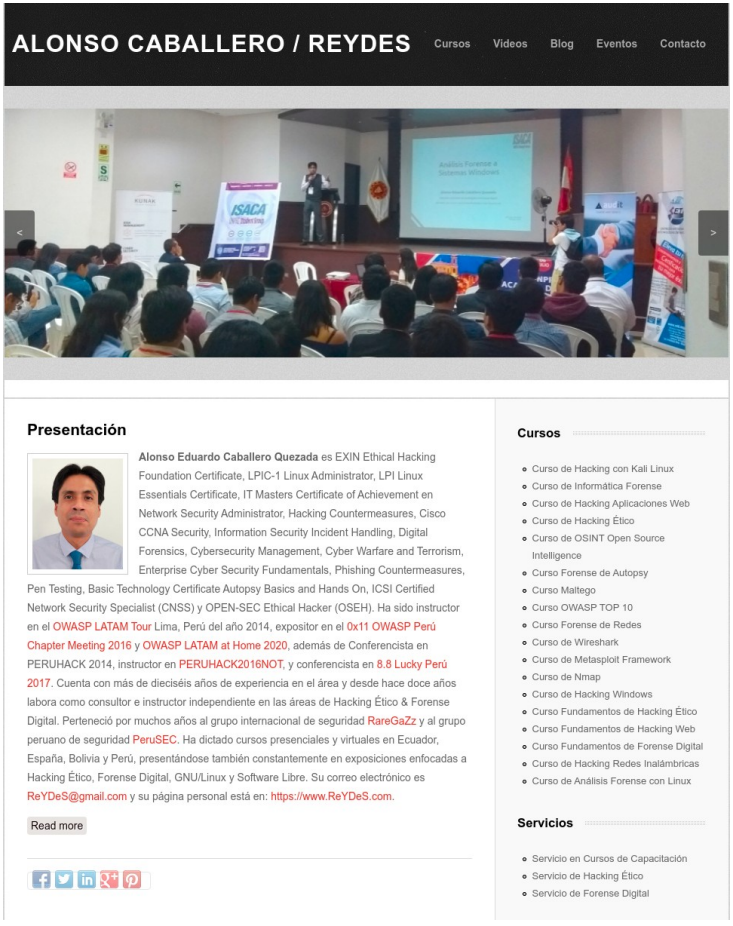
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

https://www.reydes.com/d/?q=blog/1



Webinar Gratuito

Capturar Tráfico de Red con Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Junio del 2021