Webinar Gratuito

Forense a Sistemas Windows

Alonso Eduardo Caballero Quezada

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

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

e-mail: ReYDeS@gmail.com

Jueves 1 de Marzo del 2018

Presentación

Alonso Eduardo Caballero Quezada es 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 y Cyber Warfare and Terrorism.

Ha sido instructor y expositor en OWASP Perú Chapter, instructor y expositor en PERUHACK, además de expositor en 8.8 Lucky Perú. Cuenta con más de catorce años de experiencia y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo Peruano PeruSEC. 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.

https://twitter.com/Alonso_ReYDeS

http://www.reydes.com

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

reydes@gmail.com

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

Sistemas de Archivos Windows

El sistema operativo Windows tiene principalmente dos generaciones de sistemas de archivos disponibles para los usuarios.

El primer sistema de archivos, FAT (File Allocation Table), fue utilizado en versiones anteriores de los sistemas Windows / MS-DOS, y creció desde sistemas de archivos de 12 bits denominado FAT12, hasta sistemas de archivos de 32 bits denominado FAT32.

El segundo sistema de archivos, NTFS (New Technology File System) fue introducido con Windows NT, y es utilizado hasta las versiones más recientes de Windows.

Master Boot Record
Sistema de Archivos FAT
Recuperar Particiones FAT
Recuperar Particiones NTFS

* https://technet.microsoft.com/en-us/library/cc938438.aspx
* https://technet.microsoft.com/en-us/library/cc776720(v=ws.10).aspx
* https://technet.microsoft.com/en-us/library/cc778410(v=ws.10).aspx
* https://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx

Recuperar Archivos Borrados

Una de las tareas más comunes requeridas en cualquier investigación forense, es encontrar y recuperar archivos, los cuales han sido borrados desde el sistema.

Si se encontrase borrados masivos antes de realizada la imagen forense, esto frecuentemente es un indicador principal, de el sospechoso a intentando ocultar algo.

El recuperar archivos borrados con las herramientas forenses modernas, no es una tarea compleja, dependiendo del lapso de tiempo entre cuando los archivos fueron borrados, y cuando estos empezaron a ser recuperados. Muchas herramientas para la recuperación, permiten visualizar, examinar, y recuperar archivos borrados desde un sistema.

Recuperar archivos borrados
Espacio sin asignar
Recuperar datos del espacio sin asignar

* https://www.cgsecurity.org/wiki/PhotoRec
* http://www.forensicswiki.org/wiki/Tools:Data_Recovery

Artefactos Windows

En el proceso de utilizar un sistema operativo Windows, muchos archivos son creados, borrados, modificados, y accedidos. Algunos de estos patrones o tipos específicos de cambios, son lo suficientemente únicos,para permitir exponer sin duda, una cierta acción fue realizada.

Si se fallase en determinar si existen o no estos artefactos, se podría bosquejar conclusiones incorrectas, o no ser capaz de sustentar los argumentos para un caso.

Los artefactos en Windows se convierten en puntos clave para una investigación, y frecuentemente conducen a la investigación de evidencia clave.

Papelera de reciclaje
Archivos LNK
Dispositivos USB extraíbles
Metadatos en documentos Office.
UserAssist, etc.

* https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf

Curso Virtual de Informática Forense 2018

Curso Virtual de Informática Forense 2018

Domingos 4, 11, 18 y 25 de Marzo del 2018. 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:

Todas las organizaciones deben prepararse para crímenes cibernéticos ocurriendo en sus sistemas de cómputo y dentro de sus redes. Actualmente se ha incrementado la demanda de analistas quienes puedan investigar crímenes como fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones de computadoras. Las agencias del gobierno también requieren personal debidamente entrenado para analizar sistemas Windows.

Objetivos:

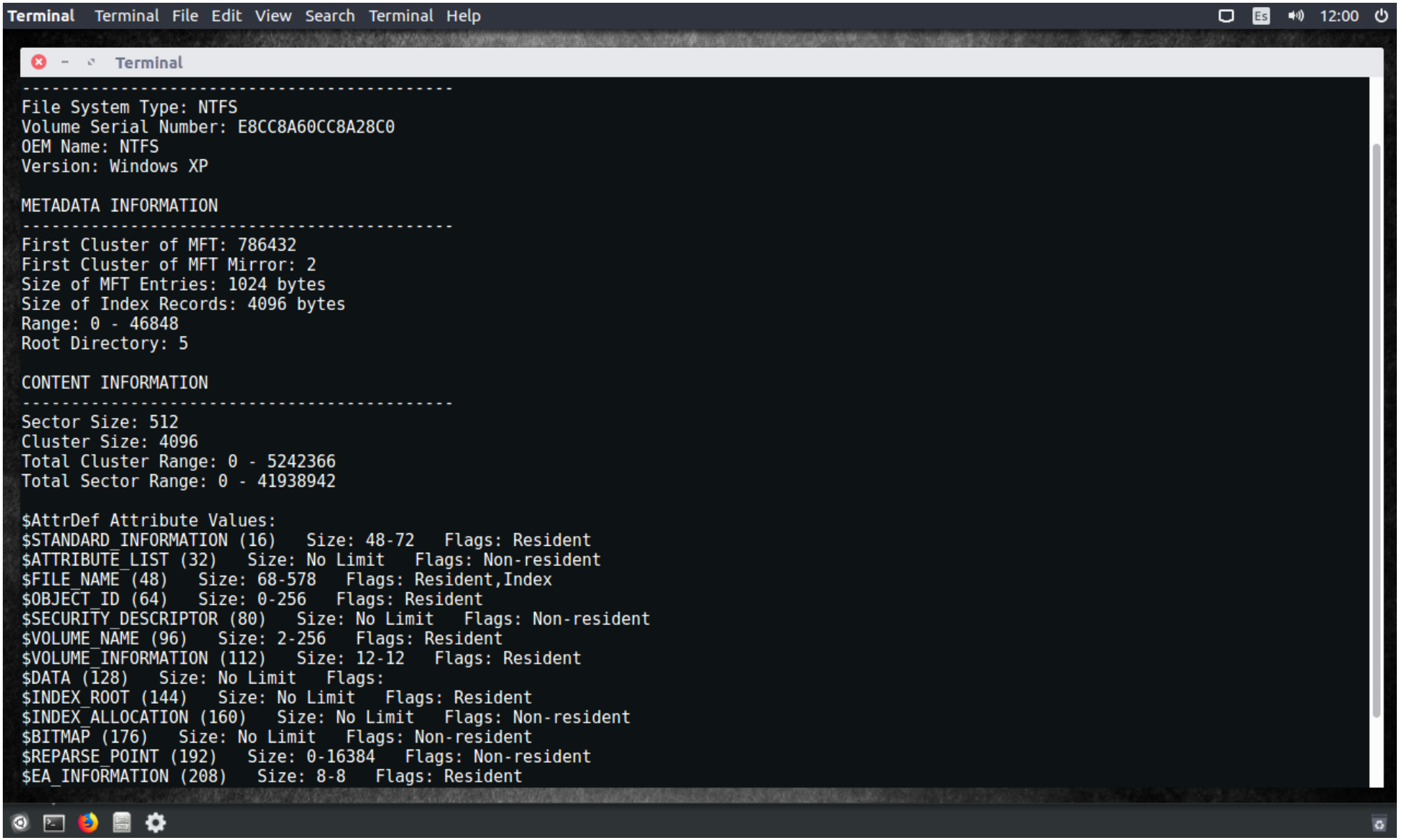
Este curso se enfoca en construir un profundo conocimiento en forense digital del sistema operativo Microsoft Windows. Pues no se puede proteger aquello desconocido, por lo tanto entender las capacidades forenses y artefactos es un componente clave en la seguridad de la información. Aprender a recuperar, analizar y autenticar datos forenses sobre sistemas Windows. Entender como rastrear actividad detallada del usuario sobre la red, y como organizar sus hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas y litigios civiles o penales. Utilizar los nuevos conocimientos adquiridos para validar las herramientas de seguridad mejorando las evaluaciones de seguridad, identificar amenazas internas, rastrear atacantes, y mejorar las políticas de seguridad. Aunque se conozca o no, Windows silenciosamente registra una cantidad inimaginable de datos sobre los usuarios. Este curso enseña la manera de obtener y analizar toda esta ingente cantidad de datos.

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 y Cybersecurity Management. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. 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 y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal esta en: http://www.ReYDeS.com.

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

e-mail: reydes@gmail.com **Sitio web:** http://www.reydes.com

Demostraciones



Cursos Virtuales 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

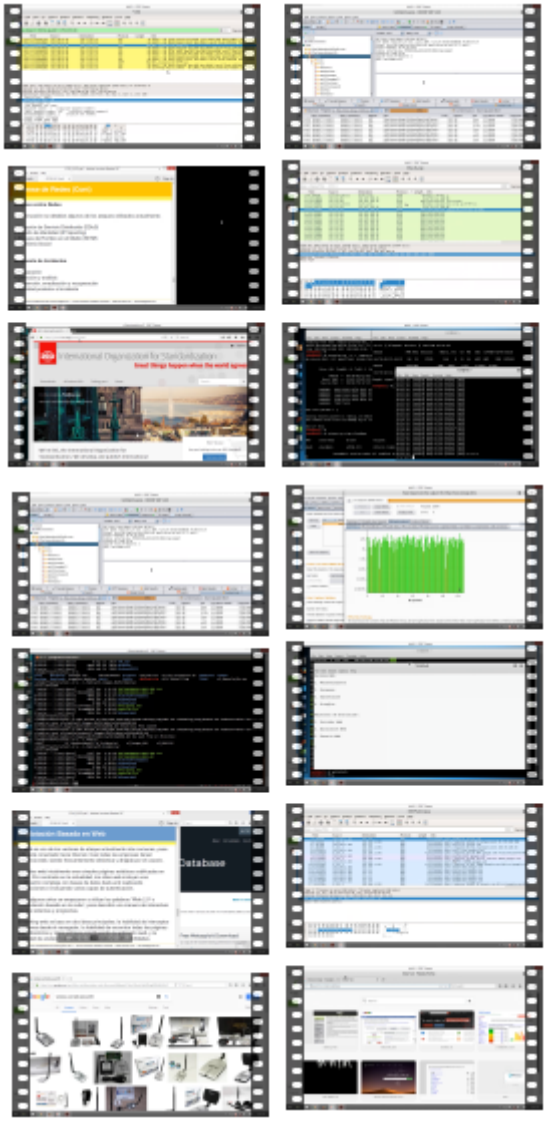
Curso Virtual Fundamentos de Hacking Ético
http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico

Curso Virtual Fundamentos de Hacking Web
http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Web

Curso Virtual Fundamentos de Forense Digital
http://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital

Y todos los cursos virtuales:

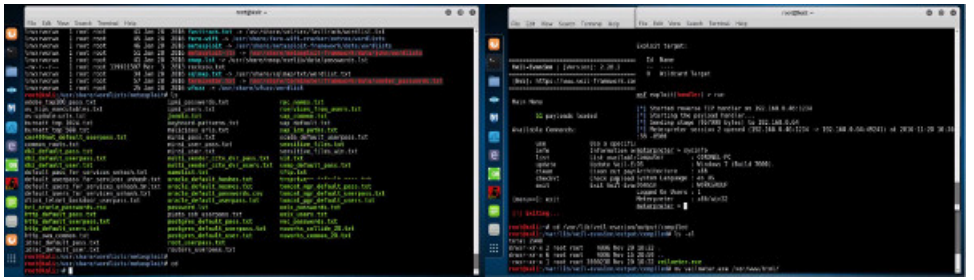
http://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 38 webinars gratuitos

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



Diapositivas utilizadas en los webinars gratuitos

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

Artículos y documentos publicados

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

Mi Blog sobre temas de mi interés.

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

Webinar Gratuito

Forense a Sistemas Windows

Alonso Eduardo Caballero Quezada

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

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

e-mail: ReYDeS@gmail.com

Jueves 1 de Marzo del 2018