Webinar Gratuito

Análisis Forense a IIS

Alonso Eduardo Caballero Quezada

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

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

e-mail: ReYDeS@gmail.com

Jueves 1 de Junio del 2017

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 y Cybersecurity Management.

Ha sido Instructor en el OWASP LATAM Tour Lima Perú y expositor en el 0x11 OWASP Perú Chapter Meeting, además de Conferencista e Intructor en PERUHACK. 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 e Informática Forense. 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, Informática Forense, GNU/Linux.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

IIS

Internet Information Services (IIS), formalmente conocido como Internet Information Server, es un servidor web ampliable creado por Microsoft para ser utilizado con el sistema operativo Windows.

IIS soporta HTTP, HTTPS, FTP, FTPS, SMTP y NNTP. Ha sido una parte integral de la familia Windows desde hace muchos años.

IIS tiene diferentes funcionalidades y características; gestión remota delegada, poderosas herramientas de administración, infraestructura web escalable, cacheo y compresión dinámica, herramientas de diagnóstico, protección mejorada del servidor, publicación segura de contenido, protección de acceso, soporte PHP y ASP.NET, ser un servidor web modular y ampliable, plataforma integrada de medios, entre otros.

Por todo esto, Internet Information Services (IIS) es un servidor web flexible para Windows, seguro y manejable para hospedar cualquier cosa en la web.

* https://www.iis.net/
* https://en.wikipedia.org/wiki/Internet_Information_Services

Formato del Registro de Eventos de IIS

W3C Extended Log File Format o Formato extendido W3C para archivos de registros de eventos, contiene una secuencia de líneas conteniendo caracteres ASCII terminados ya sea por una secuencia LF o CRLF.

Los generadores de archivos de eventos deben seguir las convenciones para la terminación de línea correspondiente a la plataforma sobre la cual se ejecutan. Los analizadores deben aceptar ambas formas. Y cada línea puede contener ya sea una directiva o una entrada.

Las entradas están constituida de una secuencia de campos relacionados a una única transacción HTTP. Los campos están separados por espacios en blanco, se fomenta el uso de caracteres ”tab” para este propósito. Si un campo no es utilizado en una entrada particular, el “-” omite el campo. Las directivas registran información sobre el proceso de “logging” por si mismo.

Las líneas iniciando con “#” contienen directivas.

* https://www.w3.org/TR/WD-logfile.html
* https://msdn.microsoft.com/en-us/library/windows/desktop/aa814385(v=vs.85).aspx

Curso Virtual de Informática Forense

Curso Virtual de Informática Forense 2017

Domingos 4, 11, 18 y 25 de Junio del 2017. 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.

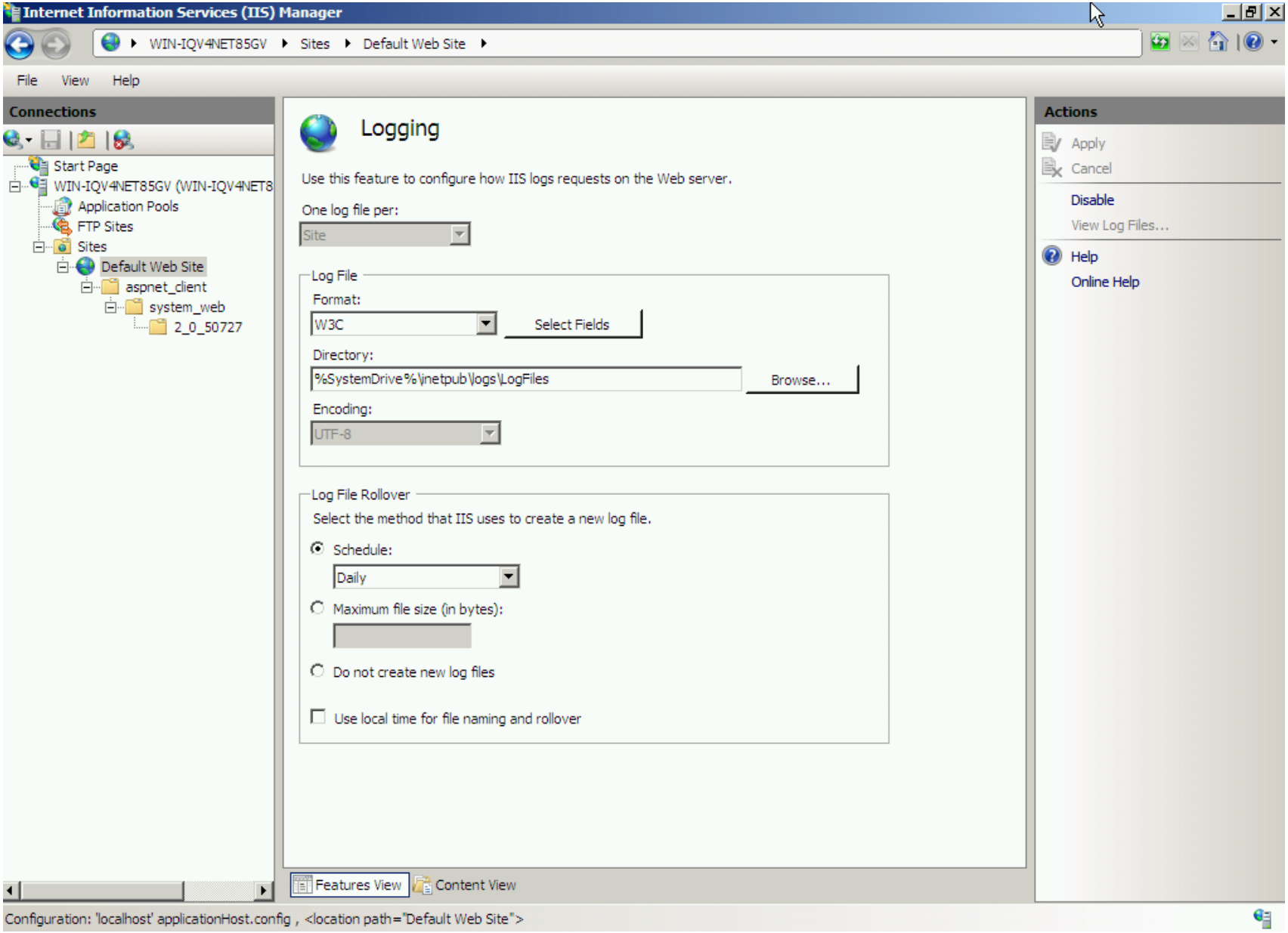
Objetivos:

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 y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. 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, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.

Más Información: http://www.reydes.com/d/?q=Curso_de_Informatica_Forense
E-mail: **caballero.alonso@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

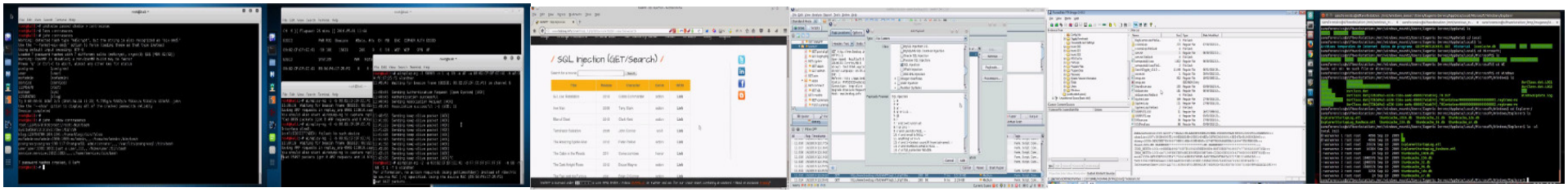
Curso Virtual Fundamentos de Hacking Ético
http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico

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:

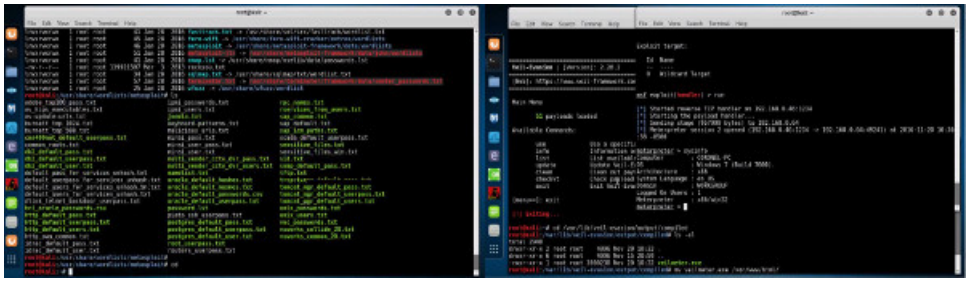
http://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 33 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

Análisis Forense a IIS

Alonso Eduardo Caballero Quezada

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

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

e-mail: ReYDeS@gmail.com

Jueves 1 de Junio del 2017