

# 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](mailto:ReYDeS@gmail.com)

# 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 Instructor 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/ 

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](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](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](mailto: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](http://www.reydes.com/d/?q=Curso_de_Informatica_Forense)

E-mail: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com) / Sitio Web: <http://www.reydes.com>

# Demostraciones

The screenshot displays the Internet Information Services (IIS) Manager interface. The main window is titled "Logging" and shows the configuration for the "Default Web Site". The left-hand pane shows the "Connections" tree with the following structure:

- Start Page
- WIN-IQV4NET85GV (WIN-IQV4NET85GV)
- Application Pools
- FTP Sites
- Sites
  - Default Web Site
    - aspnet\_client
    - system\_web
    - 2\_0\_50727

The main content area is titled "Logging" and contains the following configuration options:

- Use this feature to configure how IIS logs requests on the Web server.
- One log file per:
- Log File
  - Format:  [Select Fields](#)
  - Directory:  [Browse...](#)
  - Encoding:
- Log File Rollover
  - Select the method that IIS uses to create a new log file.
  - Schedule:
    -
  - Maximum file size (in bytes):
  - Do not create new log files
  - Use local time for file naming and rollover

The right-hand pane shows the "Actions" section with the following options:

- Apply
- Cancel
- Disable
- View Log Files...
- Help
- Online Help

At the bottom of the window, the status bar shows: Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">



# Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](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](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](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](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Etico)

Curso Virtual Fundamentos de Hacking Web

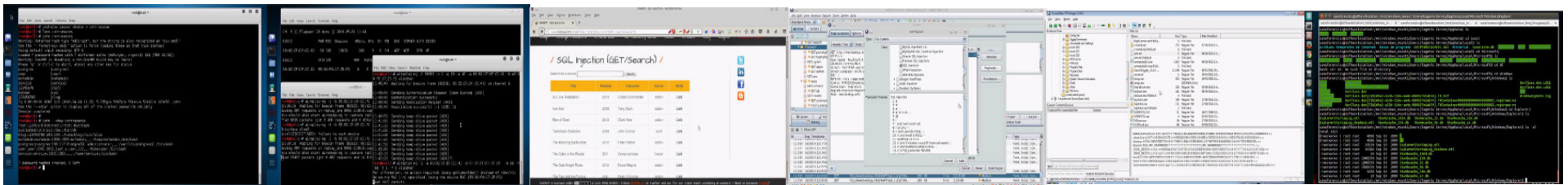
[http://www.reydes.com/d/?q=Curso\\_Fundamentos\\_de\\_Hacking\\_Web](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Hacking_Web)

Curso Virtual Fundamentos de Forense Digital

[http://www.reydes.com/d/?q=Curso\\_Fundamentos\\_de\\_Forense\\_Digital](http://www.reydes.com/d/?q=Curso_Fundamentos_de_Forense_Digital)

**Y todos los cursos virtuales:**

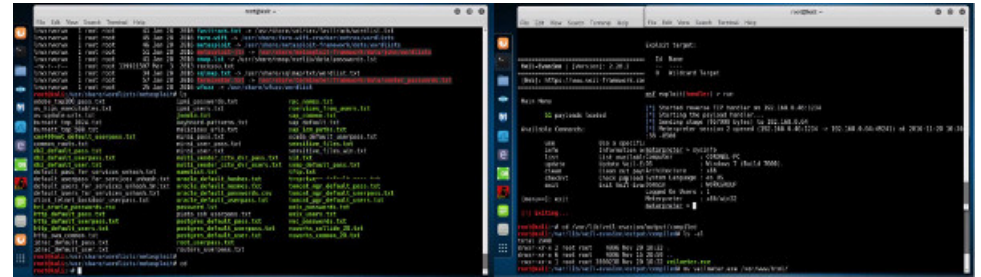
<http://www.reydes.com/d/?q=cursos>



# 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>

Alonso Caballero Quezada / ReYDeS Cursos Videos Blog Eventos Contacto



Servicio Independiente de Hacking Ético

Presentación



Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident

Cursos

- Curso de Informática Forense
- Curso de Hacking Windows
- Curso OWASP TOP 10
- Curso de Hacking Linux
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de Hacking con Kali Linux 2.0
- Curso Forense de Autopsy 4
- Curso de Metasploit Framework
- Curso de Nmap
- Curso Forense de Windows XP



# 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](mailto:ReYDeS@gmail.com)