Webinar Gratuito

Análisis Forense al Firewall de Windows

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 2 de Marzo del 2017

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, 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 e Instructor en PERUHACK2016NOT. 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 & 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

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

El Firewall de Windows

El Firewall de Windows es un firewall de estado basado en host incorporado en Windows Vista, Server 2008, Windows XP SP2, Windows Server 2003 SP 1 y posteriores.

El Firewall de Windows descarta tráfico entrando el cual no corresponde ya sea con tráfico enviando en respuesta a una petición de una computadora (tráfico solicitado), o tráfico no solicitado el cual ha sido especificado como permitido (tráfico exceptuado).

El Firewall de Windows ayuda a proporcionar protección de usuarios y programas maliciosos los cuales envían tráfico entrante no solicitado para atacar las computadoras.

En Vista y Server 2008, el Firewall de Windows también puede descartar tráfico saliente, y se configura utilizando el Firewall de Windows con Seguridad Avanzada, el cual integra reglas para el comportamiento del Firewall y para la protección de tráfico con IPsec.

* https://technet.microsoft.com/en-us/network/bb545423.aspx

Análisis al Registro del Firewall

Los “logs” o registro de sucesos si existen en la máquina, pueden proporcionar algunos datos interesantes sobre cuando se intentaron conexiones de red hacia la máquina. Una de las principales quejas sobre los registros del Firewall es el reto para mapear los paquetes con la aplicación propietaria quien inició la conexión. El archivo de registro no se configura por defecto. Cualquier investigador leyendo esto debe considerar ajustar una política de grupo para configurar los ajustes globales del registro del firewall, de tal manera este existirá en la mayoría de las máquinas en la red. Esto producirá un entorno enriquecido para el tema forense. Algunos puntos a examinar en el Firewall de Windows:

- ¿Qué ocurrió?
- ¿Fecha y hora?
- ¿Computadoras involucradas?
- ¿Puertos involucrados?
- ¿Tipos de paquetes?

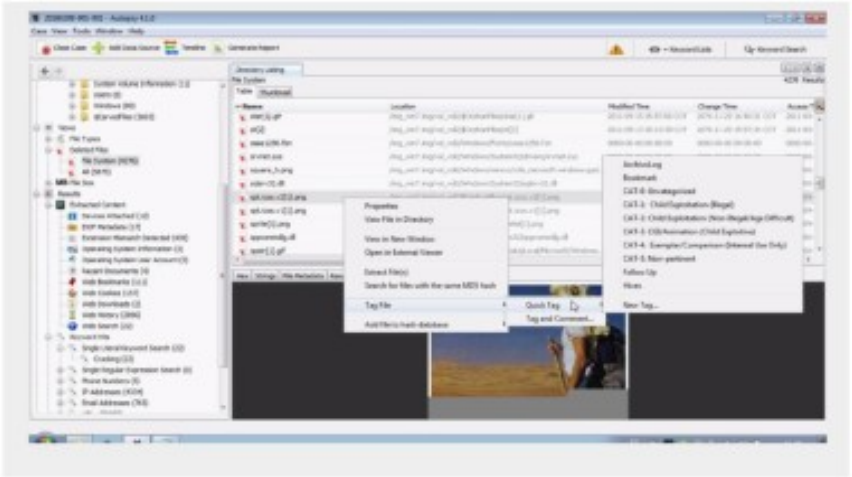
El registro del Firewall de Windows es útil si está activo, si es así se pueden correlacionar eventos con el registro de eventos de Windows.

Curso Virtual Fundamentos de Forense Digital

.

Fundamentos de Forense Digital

Curso Virtual - 2017



Único Curso del Año 2017

Fechas

Domingos 5, 12, 19 y 26 de Marzo del 2017

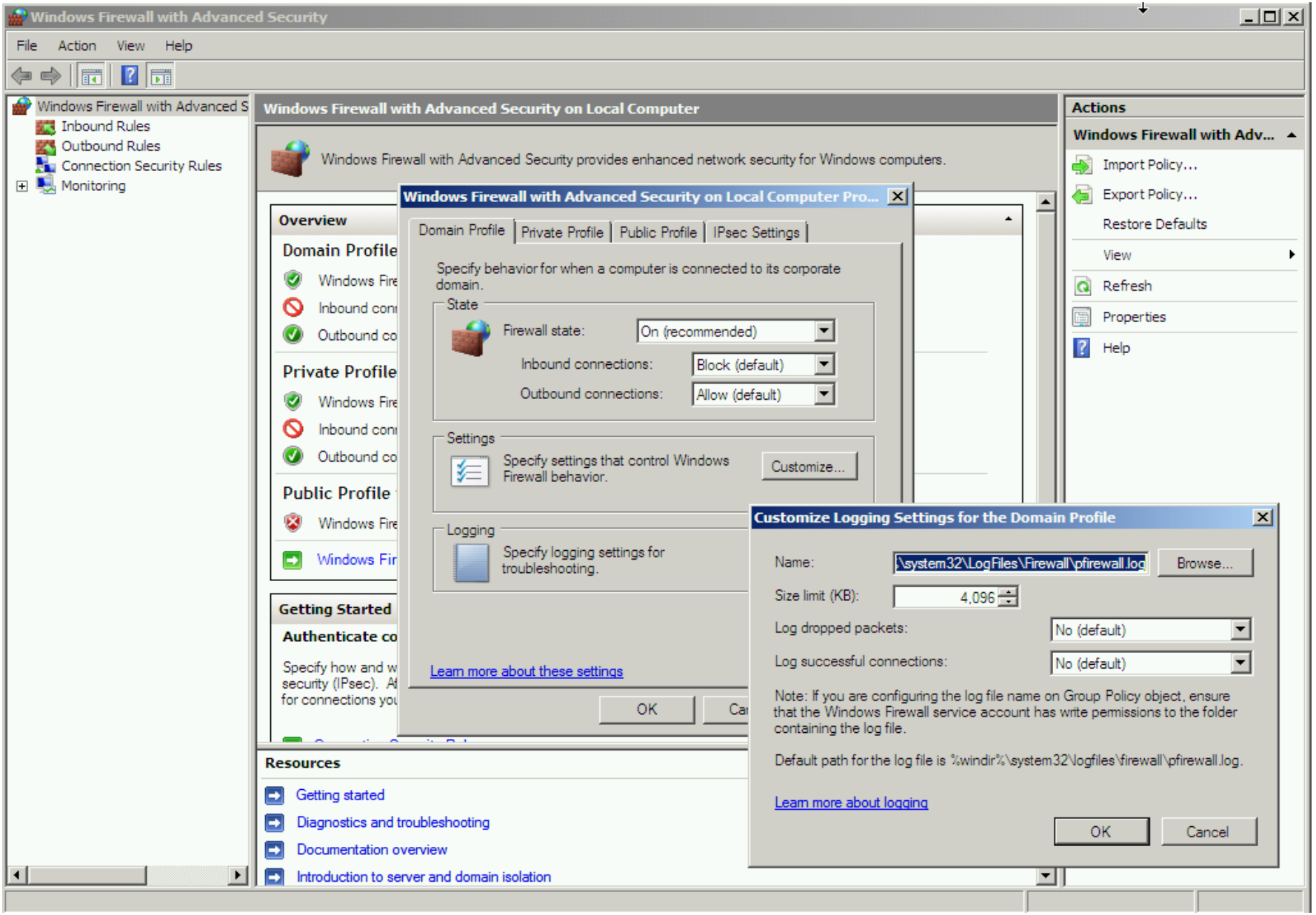
Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

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

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

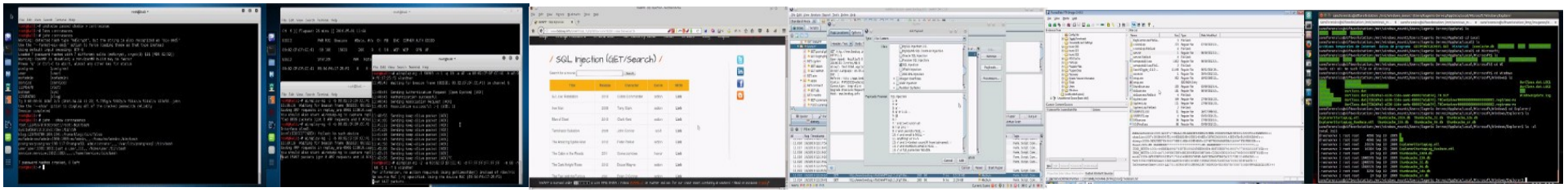
http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

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

Y todos los cursos virtuales:

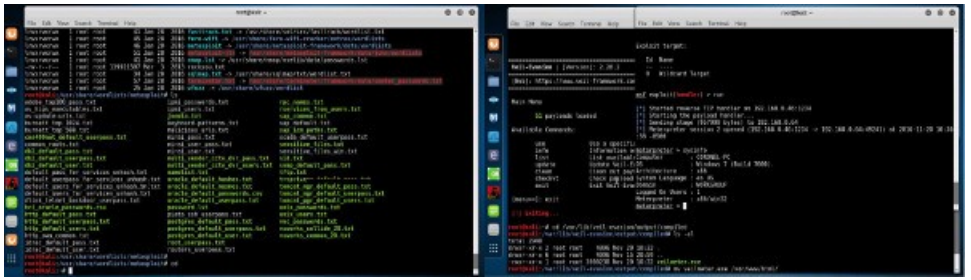
http://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 31 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 al Firewall de Windows

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 2 de Marzo del 2017