



IRISTM Network Traffic Analyzer

Control y reconstrucción gráficos de datos

Su empresa le ha confiado la tarea de garantizar que el funcionamiento de los sistemas sea correcto y seguro en todo momento. Desgraciadamente, el origen de la mayoría de los problemas de seguridad o rendimiento, tanto si se trata de actos malintencionados, falta de cumplimiento del usuario o simplemente asignación errónea de ancho de banda, suele encontrarse dentro de su propia red.

Creado por eEye Digital Security, uno de los principales desarrolladores de productos de seguridad de red, Iris es un analizador de tráfico de red muy sofisticado y fácil de utilizar. Iris permite examinar el funcionamiento interno de la red, realizando el trabajo de investigación necesario para detectar las violaciones de seguridad y resolver los problemas de rendimiento de forma rápida y sin esfuerzo.

Decodificación rápida de los datos sin procesar

En vez de ver los datos sin procesar en paquetes e intentar comprender lo que representan, Iris convierte el tráfico de la red a su formato original con un simple clic. Con Iris, podrá leer el texto real de un mensaje de correo electrónico, así como de cualquier archivo adjunto, tal y como se envió. Iris reconstruirá las páginas html que hayan visitado los usuarios y simulará cookies para obtener acceso a sitios web protegidos por contraseña. Además, puede mostrar los mensajes instantáneos enviados por las dos partes de una conversación.

Grabación y reproducción del tráfico de red

Iris funciona de forma similar a un aparato de vídeo, graba los datos de comunicación que viajan por la red y los reproduce en tiempo real o posteriormente. Iris le permite tomar el tráfico capturado en una zona de la red y reproducirlo en otra con el fin de realizar tareas como comprobar la carga de la red, verificar los niveles de servicio y supervisar aplicaciones cuyo desarrollo esté en curso. Asimismo, permite reproducir los archivos de captura creados por otro analizador de tráfico de red y realizar funciones de data mining como buscar palabras clave y revisar las estadísticas del tráfico para obtener un análisis completo del tráfico almacenado.

Estadísticas detalladas

Iris proporciona una variedad de datos estadísticos superior a cualquier otro analizador de tráfico disponible, aporta información sobre distribución de protocolos, equipos host principales, distribución de paquetes por tamaño y utilización del ancho de banda. Mediante el análisis frecuente de la utilización de los sistemas, se pueden identificar y eliminar de forma proactiva los problemas antes de que éstos deriven en largos períodos de inactividad para los usuarios. También es posible maximizar el ancho de banda en la red, reasignar recursos y planificar de forma más efectiva el crecimiento futuro.

Características principales

- Funciona con Windows 95/98/NT/2000/XP
- Herramienta de captura instantánea de datos de red que permite descodificar el tráfico en tiempo real
- Graba y reproduce el tráfico con el fin de obtener un registro completo de actividades sospechosas en la red
- Identifica los problemas de rendimiento antes de que generen períodos de inactividad en la red
- Potentes funciones de programación, alertas y elaboración de informes estadísticos



eEye[®] Digital Security

Prestaciones y ventajas adicionales

- **Estadísticas e informes**
Suministra más datos estadísticos que cualquier otro analizador de tráfico. Los datos se pueden mostrar en varios formatos gráficos (por ejemplo, diagramas de barras, gráficos circulares, etc.) e incluyen:
 - Datos de distribución de protocolos
Informa sobre el uso de la red en función de los protocolos MAC, IP e IPX.
 - Estadísticas sobre equipos host
Proporciona un análisis de los datos de tráfico de la capa IP recopilados para cada equipo host en tiempo real y ordenados según el nivel de actividad.
 - Datos de distribución por tamaño
Muestra el número de paquetes y su tamaño, clasificados en seis categorías.
 - Uso de ancho de banda
Muestra de forma gráfica el número de paquetes por segundo y bytes por segundo que fluyen por la red en tiempo real.
 - Informes de tráfico
Estos informes se muestran en una ventana del explorador desde la que se puede guardar, imprimir o copiar a otro programa el informe.
- **Reconstrucción de datos**
Utiliza los datos de los paquetes sin procesar y los convierte en sesiones HTTP, SMTP y POP3 completas en su formato original. Los paquetes que se pueden visualizar son los siguientes:
 - Mensajes de correo electrónico tanto de salida como de entrada
Es posible leer el texto del mensaje, el asunto y el destinatario. Iris inicia un cliente de correo electrónico para abrir el mensaje, así como cualquier archivo adjunto, tal y como se envió.
 - Sesiones de navegación por Internet
Reconstruye las páginas html reales en su formato original de modo que pueda verse la página que visitó el usuario.
 - Intercambio de mensajes instantáneos
Iris reconstruye todos los mensajes instantáneos enviados por las dos partes de una conversación.
 - Correo electrónico basado en web no cifrado
 - Transferencias de FTP
- **Vídeo de red**
Graba los datos de comunicación que viajan por la red y los reproduce en tiempo real o posteriormente.
- **Manipulación o forjado de paquetes**
Capaz de crear paquetes personalizados para enviarlos por la red.
- **Opciones de filtro múltiples**
Captura datos concretos mediante filtros de paquetes, basados en capas de protocolo o hardware, palabras clave, direcciones IP o MAC, puerto de origen y destino, datos personalizados y tamaño de paquete.
- **Análisis de datos capturados**
Data Miner puede procesar cualquier cantidad de datos, desde un solo archivo de tráfico a grandes cantidades de datos capturados de una sola vez. Data Miner está preparado para realizar análisis exhaustivos de tráfico almacenado.
- **Descodificación de protocolos**
Organiza los paquetes capturados y los clasifica en función del protocolo, como HTTP o SNMP, con lo que proporciona una lista de todas las sesiones de navegación, todos los mensajes de correo electrónico agrupados por mensajes entrantes y salientes, etc.
- **Potente motor de sniffing y de spoofing**
Puede gestionar tanto tráfico como genere la red, crear registros y descodificar el tráfico en tiempo real. Iris posee un motor de gestión de paquetes de gran velocidad que puede gestionar hasta 9.000 paquetes por segundo.
- **Función de programación**
Se configura fácilmente con el fin de ejecutar y capturar paquetes en determinados intervalos de tiempo. Puede capturar datos automáticamente en todo momento durante los intervalos de tiempo especificados por semana.
- **Funciones de alerta**
El módulo Guard supervisa todas las conexiones de su equipo y puede emitir un aviso al detectar una conexión concreta.

Requisitos del sistema

Windows 95/98/Me/NT/2000/XP

Internet Explorer 4.01 con comctl32.dll v 5.0+ -o- Internet Explorer 5.0+

Sistema mínimo: Pentium 166, 32 MB de RAM, unidad de disco duro de 1 GB

Sistema recomendado: Pentium 400, 128 MB de RAM, unidad de disco duro de 10 GB

Acerca de eEye Digital Security

eEye Digital Security es uno de los principales desarrolladores de productos de seguridad de redes. Los productos de eEye ofrecen niveles excepcionales de protección frente a ataques malintencionados y vulnerabilidades no detectadas. eEye es una empresa global con oficinas en los Estados Unidos y Europa, que ayuda a proteger los activos digitales de grandes empresas y entidades gubernamentales de más de 40 países.



Cra. 55 No. 40A - 20, Of. 506
PBX. (57)(4) 261 23 93, Fax. Ext. 22
Medellín, Colombia
info@techno-partners.com
www.techno-partners.com

eEye Digital Security
www.eEye.com

U.S. Tel: 1.866.339.3732
N. America: 1.949.349.9062
Geneva: +41 22.787.2282
London: +44 (0)20.7470.5630
Paris: +33 1.58.71.40.31



eEye® Digital Security

N. America: sales@eeye.com
International: sales.eu@eeye.com

