



Concurso Universitario de Software Libre

PROYECTOS

El Concurso Universitario de software libre, organizado por la Escuela Técnica Superior de Informática de la Universidad de Sevilla, entra en su recta final. Los proyectos se están desarrollando y ya falta poco para saber quién ganará en cada una de las categorías.

Entre los organizadores del concurso y Linux Magazine, hemos escogido unos cuantos proyectos para que sus artífices expliquen con sus propias palabras en qué consisten, cómo se lleva el desarrollo y los pormenores de su aplicación.

En esta entrega vemos una novedosa manera de mantener protegido el sistema frente a intrusiones, sin por ello cortar el acceso a usuarios legítimos, y un asistente para la descarga de subtítulos de películas guardadas en nuestro ordenador.

SharpKnocking

El proyecto consiste en una forma de mantener ocultos servicios que estén corriendo en una máquina conectada a Internet y permitir que sean accedidos en el momento en que el usuario de este sistema lo crea oportuno, de forma segura.

Esto se consigue modificando las reglas

del firewall iptables que viene incluido en el kernel de Linux (en realidad netfilter, del que iptables forma parte como herramienta de configuración), de manera que todos los puertos especificados en la configuración de SharpKnocking quedarían cerrados al exterior ocultando los servicios que hubiera tras ellos. Los paquetes entrantes, antes de ser bloqueados por el firewall, serán monitorizados por el demonio KnockingDaemon.

Esto ofrece dos ventajas fundamentales. La primera es que posibles atacantes que usen scripts automatizados para encontrar máquinas con servicios vulnerables (a una vulnerabilidad existente o una nueva) no encontrarían los servicios protegidos en la máquina, con lo cual el equipo quedaría a salvo hasta que el software pudiera ser actualizado.

La segunda ventaja es consecuencia de la primera. Un usuario con poca experiencia

puede permitir el acceso desde el exterior a multitud de servicios en su máquina de manera más segura. Simplemente tiene que proporcionar las secuencias de llamada (que actúan como llaves, o si se prefiere, como la clásica contraseña a base de golpes con el puño en una puerta, típica de las películas de mafiosos, y de la que se deriva el logo del proyecto) necesarias a las personas que tengan que accederlos.

El método de acceso a los servicios es sencillo, los usuarios deben utilizar la aplicación PortKnocker que realiza una «llamada» a la máquina en la que se encuentra el servicio. Esta llamada consiste en una secuencia de paquetes enviados a un cierto conjunto de puertos en la máquina en el orden especificado por el usuario. Estos paquetes son capturados por el demonio KnockingDaemon antes de ser bloqueados por iptables

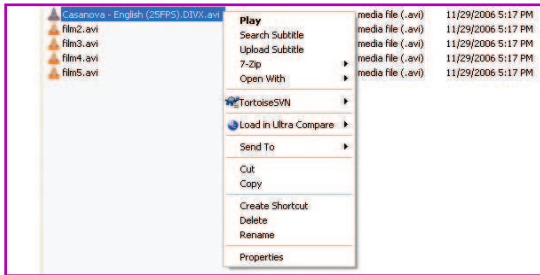


Figura 1: SubDownloader permitirá bajarse los subtítulos de la película de una manera sencilla y rápida.

para analizarlos. Si la llamada es correcta, el demonio abrirá el puerto correspondiente a la llamada sólo para la dirección IP de origen, permaneciendo oculto para el resto.

En el lado del servidor, para introducir las configuraciones a las que deberá atender KnockingDaemon se utilizará el programa Doorman, el cual, aparte de servir como configurador, permite exportar las llamadas definidas, de forma que podemos importarlas en PortKnocker, pudiendo transportar por tanto las «llaves» de nuestros servicios con nosotros de forma sencilla. También mientras Doorman se este ejecutando, al encontrar una llamada nos preguntará si queremos abrir el puerto especificado o no (si no corre se abrirá, para que pueda el sistema ser usado en modo desatendido). También permitirá desactivar temporalmente la reacción a la llegada de secuencias de llamadas, de forma que podamos «cerrar» el sistema incluso contra nuestras propias claves de entrada.

Este concepto de endurecimiento de la seguridad de un sistema no ha sido inventado por nosotros, es un concepto denominado «Port Knocking» y ya existen varias implementaciones del mismo. Cada implementación tiene una serie de características y funcionamiento distinto, pero todas coinciden en los preceptos básicos de comportamiento que hemos enunciado anteriormente.

Algunos de estos proyectos existentes pueden ser encontrados en la página [1]. Hemos solicitado la inclusión de nuestro proyecto en la lista de enlaces de dicha página para conocimiento de las personas interesadas en esta técnica.

Los interesados en nuestro proyecto pueden visitar nuestro blog (que se encuentra agregado en el planet del concurso) o descargar la última versión desde la forja en [2] y [3].

Autores

Los responsables de este proyecto somos Luis Roman Guitiérrez y Miguel Ángel Pérez Valencia, ambos estudiantes de la Universidad de Sevilla que estamos terminando la carrera este año.

Inicialmente, más que la idea de sobre qué realizar el proyecto, lo que teníamos eran ganas de aportar algo al software libre. Ambos hemos sido usuarios de software libre y distribuciones Linux desde hace bastante tiempo y sabemos bien que para que esto continúe funcionando requiere de un poco de esfuerzo por parte de todos los que se consideren dentro de la comunidad.

El tema del port knocking lo conocimos por casualidad tras leer sobre él en algún blog que ahora mismo no recordamos, pero que nos llevó hasta una página web con más información y que más tarde nos serviría de inspiración y de base para el proyecto.

Otro aliciente adicional de nuestro proyecto es el uso del lenguaje C# y de la plataforma Mono para hacerlo correr en Linux.

Mono es una implementación libre desarrollada inicialmente por Novell de la plataforma .Net creada por Microsoft hace unos años. El proyecto Mono comenzó con la idea de ofrecer al software libre todas las ventajas que ofrecía la nueva plataforma de Microsoft aprovechando que las especificaciones de los lenguajes que corren en la plataforma fueron estandarizadas y que la documentación de la librería de clases estaba disponible vía web.

Por tanto, realizando nuestro proyecto en Mono, estamos utilizando una tecnología relativamente nueva y estamos apoyando al proyecto en sí. De hecho colaboramos en ocasiones enviando reportes de bugs desconocidos que nos vamos encontrando.

SubDownloader

Autor

Iván García (Universidad de Valencia)

El Proyecto

La idea de SubDownloader es totalmente nueva e interesante: Surge para ahorrar tiempo y esfuerzo a esa gente cinéfila que

prefiere las películas en Versión Original pero le cuesta encontrar subtítulos por internet. Muchas veces el subtítulo no existe o está mal sincronizado con nuestro AVI.

Apoyándose con una base de datos de más de 240.000 subtítulos (opensubtitles.org), SubDownloader busca y descarga automáticamente el subtítulo en el idioma que prefieras. La seguridad de que ese subtítulo funcione para tu vídeo AVI es del 100% ya que el que lo puso en la Base de Datos tenía el mismo fichero de vídeo.

La identificación única de cada fichero AVI se realiza mediante un rápido algoritmo de HASH sobre los AVI's (27Gb's en 7 segundos).

El programa también se va a ir enriqueciendo con la colaboración de los usuarios, una especie de wikipedia de subtítulos donde la gente puede Subir subtítulos, Votar, Reportar fallos, etc.

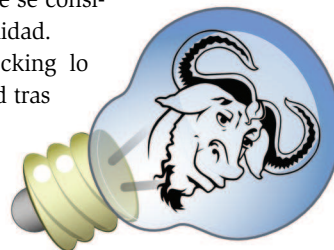
Hasta la fecha, más de 35.000 subtítulos han sido subidos con el programa y ya cuenta con 30.000 descargas desde su salida hace varios meses.

El programa está programado en Python sobre la interfaz WxPython, es multiplataforma y también contará con una versión línea de comandos para ser usado por terceros programas.

Funcionamiento Básico

Busca la película AVI en tu disco duro y pulsando el botón derecho del ratón aparecerá un menú con la opción "Search Subtitle" o "Upload Subtitle" (ver Figura 1).

La opción "Search Subtitle" buscará automáticamente los subtítulos disponibles para tu AVI listado por idiomas (ni siquiera tienes que introducir el título de la película).



RECURSOS

- [1] Proyectos de portknocking: <http://www.portknocking.org>
- [2] Forja de SharpKnocking: <http://projects.iikecoffee.net/sharpknocking>, <https://forja.rediris.es/projects/csl-csknocking>.
- [3] Blog de SubDownloader: <http://subdownloader.wordpress.com/>
- [4] Repositorio de SubDownloader: https://forja.rediris.es/scm/?group_id=161