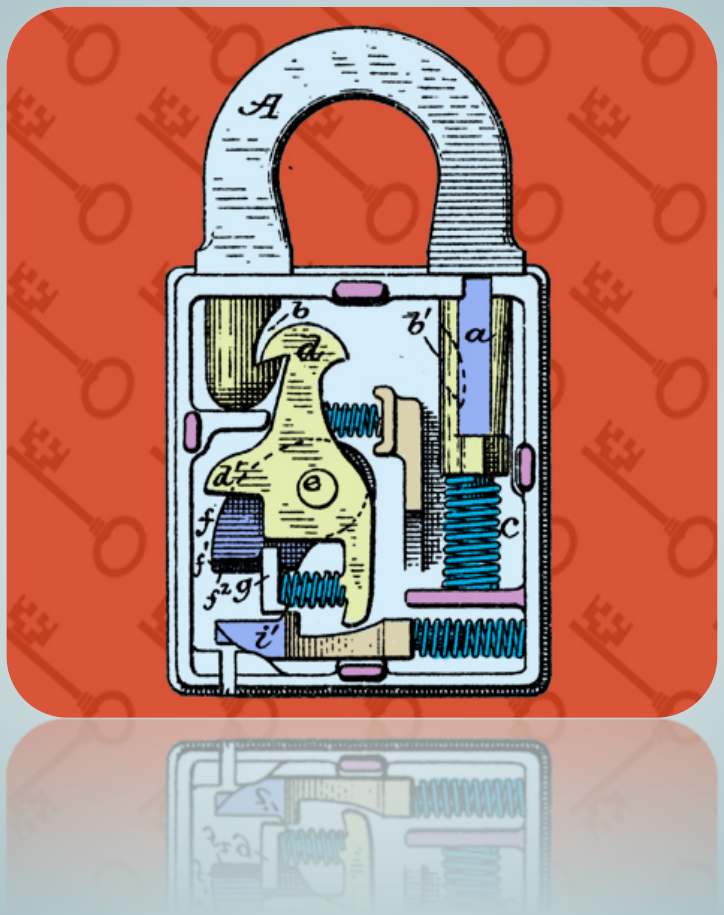
Garantía y Seguridad en Sistemas y Redes

Práctica 10. Proxy Transparente



Esteban Stafford

Departamento de Ingeniería
Informática y Electrónica

Este tema se publica bajo Licencia:
Creative Commons BY-NC-SA 4.0

Práctica 10

Proxy transparente

1. Introducción

Además de los cortafuegos, que suelen operar a nivel de red, existen otros dispositivos para mejorar la seguridad de entidades o empresas. Esta práctica se centra en el uso de un proxy para reducir la granularidad del control de acceso, tanto entrante como saliente, de las conexiones HTTP.

2. Objetivos

El objetivo fundamental que persigue esta práctica es aprender a manejar el proxy `squid` como herramienta de control de red.

3. Material

En esta práctica se usará fundamentalmente el proxy `squid` para el que existe una gran cantidad de información y ejemplos de uso en Internet.

4. Desarrollo

4.1. Creación de un entorno de trabajo

En esta práctica utilzaremos el entorno de trabajo propuesto en la práctica anterior.

- Servidor GSSR
  - Es la máquina que hemos usado en otras prácticas. Asegúrate de que no está activado el IDS.
  - El primer interfaz de red está configurado como NAT.
  - El segundo esta conectado a `vboxnet0`.
- Cortafuegos
  - Clon del servidor GSSR, también con el IDS desactivado.
  - Es conveniente cambiar el nombre de la máquina para no confundirla con el servidor.
  - El primer interfaz de red debe ponerse en modo *bridge*.
  - El segundo esta conectado a `vboxnet0`.

- Equipo de sobremesa
  - Máquina sin disco que arranca con una distribución live de Linux. Por ejemplo: http://cdimage.kali.org/kali-2.0/kali-linux-light-2.0-i386.iso
  - El interfaz de red debe estar conectado a `vboxnet0`.

De esta manera tenemos un equipo que hace de puente entre la red física de nuestra máquina y una red virtual interna, con un equipo servidor y otro de sobremesa.

4.2. Instalación de `squid`

El proxy `squid` es un programa muy conocido y lleva muchos años formando parte de las principales distribuciones de Linux. En Ubuntu se instala trivialmente con el comando `apt-get`. La configuración del proxy se encuentra en `/etc/squid3/squid.conf`. Errores e información de estado pueden encontrarse en `/var/log/squid3`. El servicio se maneja a través de `initctl`, con los comandos `start`, `stop`, etc. Revisa la configuración del proxy y trata de que el navegador del equipo de sobremesa pueda navegar a través de él. ¿Qué directiva se utiliza para definir el puerto de escucha del servicio?

¿Para qué sirve la siguiente regla?

```
http_access deny to_localhost
```

4.3. Control de acceso

Escribe un conjunto de reglas que eviten que la máquina cliente acceda a sitios relacionados con el java.

4.4. Autentificación

Crea una pequeña base de datos de usuarios con el comando `htpasswd` del paquete `apache2-utils`.

```
htpasswd -c -d /etc/squeid3/users boss
htpasswd -d /etc/squeid3/users coder
...
```

Configura `squid` para que utilice este fichero para autentificar a los usuarios del proxy. De manera que si no se puede autentificar al usuario no permita hacer la conexión. Luego, que no permita al usuario `boss` acceder a `stackoverflow`, e impida al usuario `coder` navegar por `reddit`.

4.5. Proxy transparente

Alternativamente a configurar todos los navegadores de una entidad para que usen un proxy, se puede configurar el cortafuegos para que redirija todo el tráfico HTTP al proxy. Configura el proxy en modo permisivo, comentando todas las reglas escritas en apartados anteriores y configura el cortafuegos para que utilice el proxy en modo transparente.

Una vez que funcione el proxy en modo transparente, añade las reglas anteriores y comprueba que funcionan correctamente.

4.6. Conexiones SSL

Configura el navegador del equipo de sobremesa para que use el proxy con conexiones SSL. Investiga cómo se pueden realizar estas conexiones sin violar la privacidad de las mismas. ¿Se puede hacer con en proxy en modo transparente?