Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

# Hacking en redes conmutadas y SSL. (26214 lectures)

Per **Miguel Angel Coll**, ***cuoyot*** (www.cuoyot.net)

Creado el 15/02/2002 21:55 modificado el 15/02/2002 22:10

*Mucha gente cree que no sirve de nada montar un sniffer en una red conmutada. Otros piensan que el SSL es 100% seguro. Todos ellos aun no han leido este artículo.*

Quien no ha oído decir: "En las redes conmutadas no sirve de nada meter un sniffer", o "Es imposible capturar una sesión SSL o SSH". Hasta yo creo haberlo dicho alguna vez.

Pues bien, como se suele decir "Hecha la ley, hecha la trampa".

## Como Sniffear en redes conmutadas:

Las técnicas utilizadas para sniffear en redes conmutadas se basan en el conocido "ARP poison" (envenenamiento ARP). Este sencillo ataque consiste en mandar un paquete del tipo "REPLY ARP" en el que otorgamos a una IP una MAC distinta de la real. La mayoría de los S.O (excepto Linux 2.4 y Solaris 8) no implementan estados en el protocolo ARP y por tanto aceptan el REPLY aún sin haber realizado ninguna petición.

Usando esta técnica para sniffear las conexiones entre dos equipos "A" y "B", mandaremos al equipo "A" un "ARP REPLY" diciéndole que la MAC correspondiente a la ip de "B" es la del equipo donde está el sniffer. Seguidamente haremos la operación inversa con B y haremos un _mini_proxy entre A y B. De esta forma todas las comunicaciones entre A y B pasarán por nuestra máquina. Seguro que los más avispados pensaréis: "Pero si los switch's no soportan una MAC por dos puertos distintos". Eso es cierto, los switch's guardan una tabla con las MAC's visibles desde cada una de sus bocas. Pero esa caché tiene un tamaño limitado, ¿qué pasa si la llenamos de entradas falsas? por lo general se vuelve a generar con la nueva información. También he oído comentar que los servidores DNS pueden envenenarse, esto nos daría la posibilidad de sniffear a través de Internet.

## Como capturar una sesión SSL:

Leyendo el apartado anterior ya podemos suponer por donde viene el problema. La técnica utilizada se conoce como "Man in The middle".Esta técnica consiste en capturar el establecimiento de la conexión por parte del cliente "A"; acto seguido enviamos otra petición igual que la capturada hacia el servidor "B" con origen la ip del sniffer. A la vez, enviamos un certificado Falso (más o menos currado) hacia el cliente y realizamos un _mini_proxy entre las 2 conexiones establecidas. De esta manera en el sniffer tenemos la comunicación desencriptada. El gran fallo de este ataque es que si el cliente no es tonto (demasiado suponer), no aceptará el certificado falso.

La mayor dificultad estriba en la captura inicial que se deberá realizar por envenenamiento de "ARP" o de "DNS".

## La manera fácil de hacer todo esto:

http://ettercap.sourceforge.net[1]
http://www.monkey.org/~dugsong/dsniff/[2]

## Conclusiones generales

Sospecha de las tablas ARP con entradas MAC repetidas. No deposites toda tu confianza en el switch. Si sospechas, instala un detector de intrusión (http://www.snort.org[3]) . Nunca aceptes certificados en conexiones SSL( sobretodo de bancos en los que tengas más de 100 pts.).

Miguel Ángel Coll
Agradecimientos: Ignacio Pérez.

---

**Lista de enlaces de este artículo:**

1. http://ettercap.sourceforge.net
2. http://www.monkey.org/~dugsong/dsniff/
3. http://www.snort.org

---

E-mail del autor: cuoyot _ARROBA_ cuoyot.net
**Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1193**