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

Detección de sniffers usando Linux (37020 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 23/11/2001 16:39 modificado el 23/11/2001 16:39

> Un **sniffer** es un programa que captura todo el tráfico que pasa por la red, de forma que ejecutado en una red local, permiten obtener pares (**usuario:contraseña**) rápidamente.
> Suele funcionar de forma pasiva, siendo muy dificiles de detectar, aunque existen algunas técnicas que nos permitiran averiguar si tenemos *espias* en nuestra red ...

Existen multitud de **sniffer's en Linux**, cada cual con sus peculiaridades y características, pero uno de los más potentes y que más me gusta, es **dsniff**, os recomiendo la lectura del artículo: Maxima seguridad con dsniff. El sniffer total.(1)

Advertencia: **Detectar un sniffer** es sumamente dificil, por no decir ,que si esta correctamente configurado y oculto usando otras técnicas, es **practicamente imposible** detectarlos. Aqui intentaré dar algunas ideas y consejos para que conozcais de que va el tema.

Se dan 2 situaciones distintas:

- Consulta directa de las interfaces de red.
- NO es posible la consulta directa de las interfaces de red.

Consulta directa de las interfaces de red.

En el primer caso lo que tendremos que hacer es mirar el estado de las diferentes interfaces de redes que tengamos en dicho equipo. La forma más habitual e utilizar el comando *ifconfig* (paquete net-tools), aunque podemos usar otros como *ifstatus* o *cpm* (check for network interfaces in promiscuous mode).

Aqui os muestro como el resultado del comando ifconfig antes y después de ejecutar el sniffer en una máquina **FreeBSD**:

```
$ ifconfig
fxp0: flags=8843<UP,BROADCAST,
      RUNNING,SIMPLEX,MULTICAST> mtu 1500
```

Estando el sniffer en ejecución, podemos ver en la primera línea la palabra "**PROMISC**", que nos revela el estado de la tarjeta de red:

```
$ ifconfig
fxp0: flags=8943<UP,BROADCAST,
      RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
```

Normalmente cuando la interface pasa a modo promiscuo, queda reflejado en el fichero de logs, tal y como podemos ver aqui.

```
# cat /var/log/messages
.
Nov 20 08:51:20 maquineta
         /kernel: fxp0: promiscuous mode enabled
.
```

Aunque es la forma más sencilla y directa de detectar un sniffer, tampoco es infalible, puesto que aun estando en marcha el sniffer puede que no aparezca la interfaz como *promiscuos* sobretodo si han crackeado la maquina y le han metido un LKM del estilo del **RhideS v1.0** (rhides.c en 7a69#12):
"Is usualy to install a sniffer when you hack some system, but if you do it, the net device is established to promisc mode and if the admin is inteligent must to discover the sniffer. Using RhideS you can to hide some promisc mode interface easily. Inserting the module you can specify magic words."

Otras posibles medidas para detectar el sniffer son:

- Controlar y detectar los **logs** que genera el sniffer.
- Controlar las **conexiones al exterior**, por ejemplo, el envío sospechoso de e-mail a cuentas extrañas.
- Utilizar la herramienta **lsof** (LiSt Open Files), de forma que tengamos monitorizados los programas que acceden al dispositivo de red.

NO es posible la consulta directa de las interfaces de red.

En caso de que no podamos acceder y consultar el estado de las interfaces de red, puesto que el sniffer no esta en nuestra máquina sino que se encuentra en alguna otra máquina de la red. Lo que tendremos que hacer, es utilizar algun defecto en la implementación concreta del protocolo TCP/IP por algun programa/comando (tal y como hace el programa **neped** respecto a el *arp*) o ingeniarnoslas para averiguar de alguna forma si tenemos algun sniffer corriendo en la red:

"Una de las posibles técnicas, consiste en enviar paquetes a una máquina inexistente y cuya dirección no está dada de alta en el servidor de nombres. Sabremos que tenemos un sniffer en nuestra red si posteriormente detectamos cualquier intento de acceso a la máquina ficticia".

Antisniff, del que tenemos incluso el código fuentes en la version **Unix**, es una de las mejores herramientas de detección de sniffer de forma remota, aunque quizás este un poquitín obsoleto, sobretodo porque no contempla la nueva generación de sniffers.
AntiSniff is a new class of proactive security monitoring tool. It has the ability to scan a network and detect whether or not any computers are in promiscuous mode. This is often a sign that a computer has been compromised. With AntiSniff, administrators and security teams can finally get a handle on who is watching network traffic at their site. Antisniff was designed to detect compromized machines with IP stacks that a remote attacker could utilize to sniff network traffic. It was not designed to detect hardware based network probes or special purpose network analyzers which an attacker would need physical access to install.

Sentinel es otra interesante herramienta, cuyo objetivo principal es la detección remota de sniffers. Utiliza las librerias **libcap** y **libnet** y tenemos el código fuente disponible.
The sentinel project is an implementation of effective remote promiscuous detection techniques.For portability purposes, the sentinel application uses the libpcap and libnet libraries.

Por último comentar la existencia de una curiosa herramienta: **AntiAntiSniffer Sniffer**, cuyo objetivo es detectar la ejecución en la red del **Antisniff**, evitando ser detectado por el mismo.

Conclusión: Recordar (una vez más) la necesidad de usar encriptación a diario en **TODAS** nuestras comunicaciones: S/key, gpg, SSH, SSL, Firewall, VPNs, etc...

Enlaces:

- dsniff: http://www.monkey.org/~dugsong/dsniff/[2]
- sniffit: http://reptile.rug.ac.be/~coder/sniffit/sniffit.html[3]
- net-tools:http://www.tazenda.demon.co.uk/phil/net-tools/[4]
- neped.c:http://www.securityfocus.com/data/tools/neped.c[5]
- Ifstatus: http://www.ja.net/CERT/Software/ifstatus/ifstatus2.2.tar.gz[6]
- cpm, ifsolstat: http://www.ja.net/CERT/Software/sniffdetect/[7]
- 7a69ezine: http://www.7a69ezine.org/[8]
- lsof: http://freshmeat.net/redir/lsof/6029/url_changelog/[9]

- Antisniff: http://www.l0pht.com/antisniff/[10]
  http://www.securityfocus.com/data/tools/anti_sniff_researchv1-1-2.tar.gz[11]
- Sentinel: http://www.packetfactory.net/Projects/sentinel/[12]
- libnet: http://www.packetfactory.net/Projects/libnet[13]
- libpcap: http://www.tcpdump.org[14]
- Anti Antisniff: http://www.securityfocus.com/data/tools/aass.c[15]
- sniffing-faq: http://www.robertgraham.com/pubs/sniffing-faq.html[16]
- Sniffing (network wiretap, sniffer) FAQ: http://cs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm[17]

--
Carlos Cortes (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [18]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=928
2. http://www.monkey.org/~dugsong/dsniff/
3. http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
4. http://www.tazenda.demon.co.uk/phil/net-tools/
5. http://www.securityfocus.com/data/tools/neped.c
6. http://www.ja.net/CERT/Software/ifstatus/ifstatus2.2.tar.gz
7. http://www.ja.net/CERT/Software/sniffdetect/
8. http://www.7a69ezine.org/
9. http://freshmeat.net/redir/lsof/6029/url_changelog/
10. http://www.l0pht.com/antisniff/
11. http://www.securityfocus.com/data/tools/anti_sniff_researchv1-1-2.tar.gz
12. http://www.packetfactory.net/Projects/sentinel/
13. http://www.packetfactory.net/Projects/libnet
14. http://www.tcpdump.org
15. http://www.securityfocus.com/data/tools/aass.c
16. http://www.robertgraham.com/pubs/sniffing-faq.html
17. http://cs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm
18. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com