HVLinux V0.2.2 http://hvlinux.tsx.org
LabX - http://labx.tsx.org
DoctorX <d0ct0r_x@hven.com.ve>

Titulo: Anti-Sniff
Autor :DoctorX
Fecha : 01/02/99

Anti-Sniffer

¿Como detectar la Presencia de un sniffer en tu sistema?

Un sniffer puede ser un gran causante de problemas de seguridad, ya que daria a ciertas personas gran cantidad de claves de usuarios del sistema.

Esto seria una invitacion a violaciones de la seguridad del mismo por lo que parte de la labor de un administrador de un sistema o en nuestro caso, nosotros si tienes tu propia linux box, es la de velar por la seguridad de la misma. Por lo cual la deteccion de los sniffes es fundamental ya que estos podrian capturar email, claves y cualquier cosa que salga por un puerto.

Claro que existen sniffers como el sniffit que son doblemente letales, pero eso sera tema de otro articulo.

Un sniffer coloca las interface a trabajar en modo promiscuo, o sea que acepte todos los paquetes. Aunque tambien se puede ejecutar un sniffer sin utilizar el modo promiscuo que seria mas facil de detectar, pero el problema es que un sniffer que funciona en modo promiscuo puede capturar todos los paquetes que viajen a traves de una interface ethernet, mientras que el otro solo en las sesiones tty (asi como el tty watcher).

Una manera de detectar un sniffer seria utilizar este comando:

"ifconfig -a"

Hay que chequear si existen interfaces en modo promiscuo. Otra forma seria el utilizar este comando:

"netstat -r"

y te dara cierta informacion de interes como esta:

Routing tables
Internet:

Destination	Gateway	Flags	Refs	Use	Interface
Default	hackven.org	UG	1	32949	eth0
Localhost	localhost	UH	2	73	eth1

el uso de la interface eth0 te puede crear la sospecha y ejecutando "ifconfig eth0" puedes darte cuenta si en realidad esta siendo utilizada por un sniffer: Ejemplo :

```
#ifconfig eth0
    le0:
flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,MULTICAST>
          inet 127.0.0.1 netmask 0xffffff00 broadcast 255.0.0.1
```

o si no otra forma seria la de ejecutar un programa que te ayude a realizar la deteccion como en nosniff.c . El codigo C esta a continuacion :

```
#include <stdio.h>
#include <sys/socket.h>
#include <sys/ioctl.h>
#include <errno.h>
#if defined (__linux__)
#include <linux/if.h>
#else
#include <net/if.h>
#endif
#define size(p) (sizeof(p))
int dev_flags=0,
   device_flags=0,
   set_look_all=0;
int
main(int argc, char **argv) {
 struct ifreq ifreq, *ifr;
 struct ifconf ifc;
 char buf[BUFSIZ], *cp, *cplim;
 if(argc <= 1)
       set_look_all++;
 if((dev_flags = socket(PF_INET, SOCK_DGRAM, 0)) < 0) {
       fprintf(stderr, "Error \n");
       perror("socket");
       exit(1);
 }
 ifc.ifc_len = sizeof(buf);
 ifc.ifc_buf = buf;
 if(ioctl(dev_flags, SIOCGIFCONF, (char *)&ifc) < 0) {
       perror("SIOCGIFCONF");
       exit(1);
 }
```

```
 ifr = ifc.ifc_req;
 cplim=buf+ifc.ifc_len;
 for(cp = buf; cp < cplim;
            cp += sizeof (ifr->ifr_name) + size(ifr->ifr_addr))
{
            ifr = (struct ifreq *)cp;
            if(argv[1])
                  if(strcmp(ifr->ifr_name, argv[1]) && !set_look_all)
                        continue;
            ifreq = *ifr;
            if(ioctl(dev_flags, SIOCGIFFLAGS, (char *)&ifreq) < 0)
            {
                  fprintf(stderr, "SIOCGIFFLAGS: %s (get interface flags):
%s\n", ifr->ifr_name,strerror(errno));
                  continue;
            }
            device_flags=0; device_flags = ifreq.ifr_flags;
            fprintf(stdout, "%s: ", ifreq.ifr_name);
            if((device_flags & IFF_PROMISC) != 0)
                  fprintf(stdout, "Dispositivo en modo Promiscuo: Sniffer
detectado.\n");
             else
                  fprintf(stdout, "No en modo Promiscuo: Ningun Sniffer
detectado.\n");
            if(!set_look_all)
                  exit(0); // finalizado
             else
                  continue; //siguiente dispositivo
 }
 if(!set_look_all)
       fprintf(stdout, "%s: Dsipositivo desconocido.\n", argv[1]);
                              // dispositivo no encontrado
}
```

para compilarlo :

```
gcc -o nosniff  nosniff.c
```

este programa no puede ser compilado en SunOS

Atte

DoctorX
<d0ct0r_x@hven.com.ve>