Snoop Sniffer

Fernando Spencer
CAT / CBPF

spencer@cbpf.br

Tópicos Abordados

- Introdução
- Funcionalidades
- Modo de uso
- Exemplos
- Conclusão

Introdução

- Sniffers
- Objetivos
- Ethereal
- DSniff
- TCP Wrappers

Funcionalidades

- Binário
- Promiscuous Mode
- Capturar pacotes em tempo real
- Flexibilidade para analizar

Modo de Uso

```
# snoop |more
# snoop |grep "ICMP Time exceeded"
# snoop –o <nome_arquivo>
# snoop -o <nome_arquivo> -c 1000
# snoop -o <nome_arquivo>  port <número>
# snoop -i <nome_arquivo> -v -p10-32,56
# snoop –o <nome_arquivo> from marte or
to 8:0:20:f1:b3:51 or net 152.84.253.0
not 152.84.253.13
```

Exemplos

```
 w
12:06pm  up 32 day(s), 23:39,  0 users,  load average: 0.00, 0.00, 0.02
ser     tty           login@  idle   JCPU   PCPU  what
 who

 /usr/sbin/snoop | grep TELNET
sing device /dev/le (promiscuous mode)
o-tc0-tty407.iis.com.br -> davies.microbiology.ubc.ca TELNET C port=1112
avies.microbiology.ubc.ca -> rio-tc0-tty407.iis.com.br TELNET R port=1112
```

Conclusão

- Modo texto
- Limitação
- Flexibilidade
- Segurança