Introdução

Os *sniffers* explodiram em popularidade nos últimos anos, vindo de monitoração de redes privadas até as ferramentas públicas que existem hoje como o Snoop ou ethereal. Estas ferramentas são usadas por diversas razões, incluindo problemas na rede, analisar o tráfego, descobrir nós, etc.

Aqui será coberto um dos mais comuns e efetivos *sniffers*, o snoop. De todos os sniffers, o snoop sempre será encontrado no Solaris.

O que é Snoop?

Snoop é um binário executável o qual põe sua interface de rede em modo promiscuo. Estando neste modo, snoop pode capturar todos os pacotes que trafegam pela sua rede em tempo real ou em gravado em arquivo. Assim, os detalhes das informações fazem do snoop uma ferramenta poderosa e flexível.

Como usar o Snoop?

A primeira decisão deve ser o que vai ser feito, capturar pacotes em tempo real ou gravar em arquivo. Na maioria das vezes será optado por gravar em arquivo, pois em tempo real, os pacotes atravessam a tela rápido demais para serem lidos. Neste caso o único benefício é uma curta análise de como o tráfego está se movendo pela rede. Para sérias análises, provavelmente será feita a captura de pacotes para arquivo, sendo analisados com mais calma a qualquer momento.

Modos de uso

```
snoop |more  
# executa o snoop e faz a paginação dos resultados na tela.
```

```
snoop |grep "ICMP Time exceeded"  
# mostra os pacotes que contem a mensagem.
```

```
snoop -o <nome_arquivo>  
# captura os pacotes da rede e gera (opção -o) um arquivo
```

```
snoop -o <nome_arquivo> -c 1000  
# captura limitada (opção -c) de 1000 pacotes da rede.
```

```
snoop -o <nome_arquivo> port <número>  
# captura pacotes em uma porta especificada
```

```
snoop -i <nome_arquivo> -p10-32,56  
# filtra os pacotes 10 ao 32 e 56 do arquivo gerado no item anterior
```

```
snoop -o <nome_arquivo> from zeus or to 8:0:20:f1:b3:51 or net  
192.168.3.0 not 192.168.3.58  
# gera arquivo com opções por host name, Mac e network com uma  
exclusão de um IP.
```

Poder do Snoop

Agora será abrangido o poder desta ferramenta, o snoop tem uma variedades de filtros, permitindo focar em algum tipo de pacote, seja por origem, destino, protocolo, etc. De qualquer forma, para uma informação mais completa verifique os manuais do snoop.

A principio, podemos seleccionar MAC, IP ou *host* que será *snooped*. Com isto, são limitados os pacotes que serão capturados pela interface. Caso queira analisar apenas um nó, coloque seu ip, caso sejam muitos, pode-se utilizar as expressões "and" ou "or" entre os nós. É possível também qualificar melhor o focus usando o "from" ou "to", que estão relacionados com a origem e destino respectivamente. O "!" ou "not" fazem a operação lógica NOT. Por último, a expressão "net" captura todos os pacotes que pertencem a uma rede específica.

Como nós podemos qualificar endereços ou redes específicas nas camadas 2 ou 3, também é possível limitar a captura de pacotes nas camadas 4, 5, 6, e 7. Na camada 4, podemos qualificar "tcp", "udp" ou "icmp" (atualmente RCF 792 trata o icmp na camada 3, mas foi tratado aqui em camada 4 em reflexão ao manual do snoop).

Para as camadas 5, 6 e 7 são usados "port" e "rpc" (baseados no /etc/services e /etc/rpc). O comando abaixo captura todos os pacotes DNS ou NFS.

```
snoop -o filename -V port domain or rpc nfs
```

Segurança

Após ter sido coberto a flexibilidade do snoop, agora será aplicada a sua segurança. O snoop senta silenciosamente em sua rede e captura todos

os dados. Diferente de ferramentas comuns que utilizam icmp, snoop não alerta a ninguém a sua presença. Isto permite que a rede seja analisada com segurança. Além disso, o snoop pode ser executado por um longo período.

Snoop possui duas fazes críticas de segurança, ele nos diz quem esta na rede e o que estão fazendo.

O que o snoop não pode fazer?

Snoop não pode operar em redes *switched*, ele somente é capaz de de capturar pacotes que atravessam uma interface designada. *Switches* bloqueiam e redirecionam pacotes baseados no endereço MAC, camada 2. Caso hka um *switch*, o snoop só irá capturar os pacotes que colidirem neste domínio.

Caso seja desejado capturar todo o tráfego da rede, o snoop precisa operar no mesmo segmento do roteador.

Entretanto esta limitação pode ser usada ao seu favor, uma tática comum de hackers é utilizar sniffers para interceptar o tráfego da rede.