
Sniffers

Captura de Informações

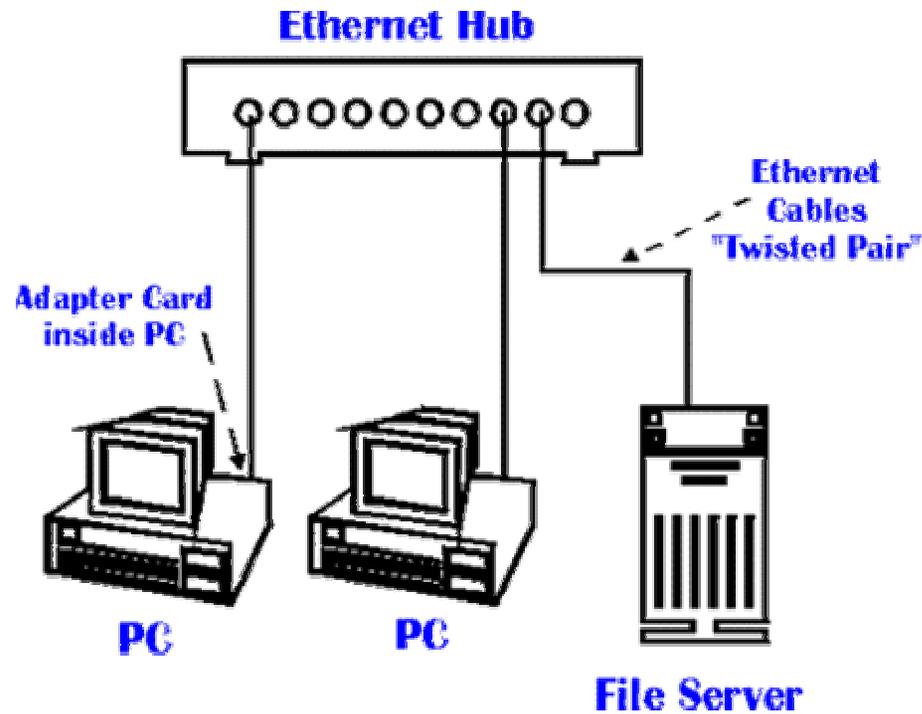
Sniffers

- Ferramenta de Apoio ao Administrador para análise de tráfego.
 - Ferramenta de Ataque para furto de informações dentro de uma rede.
-

Sniffers

- Ver pacotes transitando, capturá-los e verificar o conteúdo.
 - Fácil, em redes baseadas em Hubs.
 - Não é possível capturar dados em redes com switches, com sniffers “simples”. Mas, existe a possibilidade através de “ArpSpoofing”.
-

Sniffers



Sniffers

- Furto de informações:
 - nomes de usuários,
 - senhas,
 - conteúdo de emails,
 - conversas ICQ,
 - dados internos em uma empresa.
-

Sniffers

- Ataques internos (funcionários hostis).
 - Ataques remotos, via Internet, **com acesso privilegiado a um gateway** (roteador de perímetro), que fica entre a rede interna e a externa.
-

Alguns Sniffers

TCPDump e TCPshow

DSniff: mailsnarf, tcpkill, tcpnice, MSGSnarf

EtherDetect

ADMSniff

AResetter

HTTPCapture

Ngrep

Snif

TraceWolf Packet Sniffer

TCPDump

- Ferramenta de análise;
 - Para administradores *NIX.
 - Rede Ethernet
 - Tamanho máximo do pacote: 1500 bytes.
 - Tamanho máximo do quadro: 1518 bytes
-

TCPDump: capturando tráfego

Toda a rede:

```
>tcpdump -s 1518 -vv -l -n -w  
      /tmp/teste
```

Tráfego de FTP:

```
>tcpdump -s 1518 -vv -l -n port 21  
      -w /tmp/ftp.log
```

Tráfego de SMTP:

```
>tcpdump -s 1518 -vv -l -n port 25  
      -w /tmp/smtp.log
```

TCPDump: capturando tráfico

Tráfico de POP:

```
>tcpdump -s 1518 -vv -l -n port 110  
-w /tmp/pop.log
```

Tráfico de IMAP:

```
>tcpdump -s 1518 -vv -l -n port 143  
-w /tmp/imap.log
```

TCPDump: capturando tráfico

Todos os logs:

```
>tcpdump -s 1518 -vv -l -n port 21  
      or port 25 or port 110 or  
      port 143 -w  
      /tmp/todos_logs.log
```

TCPShow

- Converter o *log* apresentado em hexadecimal para o formato ASCII, usando TCPShow:

```
>tcpshow -pp -track  
      <todos_logs.log>  
      <todos_logs.result>
```

Ferramentas DSniff

- MailSnarf
 - TCPkill
 - TCPnice
 - MSGSnarf
-

EtherDetect

The screenshot shows the EtherDetect application window. The main window title is "EtherDetect" and it has a menu bar with "File", "View", "Sniffer", and "Help". Below the menu bar is a toolbar with various icons. The main area is divided into several panes:

- Connections Table:** A table listing network connections with columns for #, Start Time, Client IP, Server (IP:Port), Protocol, P., and Last Time. The table contains 11 rows of data.
- Packet Details Table:** A table showing details for a selected packet, with columns for Time Offset, P., D., and Data. It shows a list of 11 packets.
- Packet Structure Tree:** A tree view showing the structure of the selected packet (1506 bytes). It includes Ethernet Header (Dst Mac Address: 00.40..., Src Mac Address: 00.07..., Type: 2048) and IP Header (Header Length: 5, Version: 4, Service Type: 0, Total length: 1492, Identifier: 22708, Offset: 18384, TTL: 43, Protocol: 6, Check Sum: 62538).
- Raw Data:** A hex dump of the packet data, showing hexadecimal values and their corresponding ASCII characters.

At the bottom of the window, there is a status bar with the text "Ready" on the left and "Buffer: 9% Conns: 32 Packets: 1542" on the right.

ADMSniff

- Um sniffer simples baseado na biblioteca de captura de pacotes LibPcap.
- Utilizada em muitas ferramentas Open Source, tais como, TCPDump, Ethereal, Ettercap, ...
- ADMSniff funciona em background, gerando os arquivos de registro de cada conexão:

```
>admsniff -i eth0
```

AResetter

- Sniffer que utiliza a técnica de ***spoofing*** para cancelar conexões em uma rede, equivalente ao TCPkill nas ferramentas DSniff.

```
> . /aresetter
```

HTTPCapture

- Sniffer projetado para captura de:
 - HTTP Realm Authentication
 - Jabber Logins
 - FTP Logins
 - POP3 Logins
 - CVS Logins (pserver)

 - `>httpcapture -debug -interface eth0`
-

Ngrep

- Ngrep capturando senhas de POP3:

```
> ngrep -d eth0 'user|pass' tcp  
    port 110
```

- Ngrep capturando senhas de FTP:

```
> ngrep -d eth0 'user|pass' tcp  
    port 21
```

Snif

- Sniffer para Windows.
 - Intercepta e analisa pacotes transmitidos através de uma rede com switch.
 - Aceita plug-ins para trabalhar com diferentes protocolos, como, IP, TCP e UDP.
 - Shareware (<http://www.ufasoft.com/>)
-

TraceWolf Packet Sniffer

- Sniffer para Windows.
 - Captura, abre e mostra todos os pacotes que passam pelo seu modem ou placa de rede Ethernet, mostrando campos de cabeçalho e de dados.
 - Demo
-

Sniffer snoop em Telnet

```
# snoop -d qfe0 port telnet ganassi
  ganassi -> nomex-lab      TELNET R port=32835
\377\373\1\377\375\1login:
  nomex-lab -> ganassi      TELNET C port=32835 r
  ganassi -> nomex-lab     TELNET R port=32835 r
  nomex-lab -> ganassi      TELNET C port=32835 o
  ganassi -> nomex-lab     TELNET R port=32835 o
  nomex-lab -> ganassi      TELNET C port=32835
  nomex-lab -> ganassi      TELNET C port=32835 o
  ganassi -> nomex-lab     TELNET R port=32835 o
  nomex-lab -> ganassi      TELNET C port=32835
  nomex-lab -> ganassi      TELNET C port=32835 t
  ganassi -> nomex-lab     TELNET R port=32835 t
  nomex-lab -> ganassi      TELNET C port=32835
  ganassi -> nomex-lab     TELNET R port=32835 Password:
  nomex-lab -> ganassi      TELNET C port=32835
  nomex-lab -> ganassi      TELNET C port=32835 t
  ganassi -> nomex-lab     TELNET R port=32835
  nomex-lab -> ganassi      TELNET C port=32835 0
  ganassi -> nomex-lab     TELNET R port=32835
```

Sniffer snoop em IMAP

```
# snoop -d qfe0 port imap2 ganassi
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600
jordan -> ganassi IMAP C port=46600
ganassi -> jordan IMAP R port=46600 * OK ganassi SIMS (tm) 2.0p12
IMAP
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 1 capability\r\n
ganassi -> jordan IMAP R port=46600
ganassi -> jordan IMAP R port=46600 * CAPABILITY IMAP4 STATUS SCAN
IMAP4
jordan -> ganassi IMAP C port=46600
jordan -> ganassi IMAP C port=46600 2 login "hacked" "t00lklt"\r\n
ganassi -> jordan IMAP R port=46600 2 OK LOGIN completed
```

Contra medidas

- Ataques de sniffers podem ser evitados se a empresa tiver uma política quanto ao uso de suas máquinas de trabalho.
 - Políticas rígidas estendem-se a atividades via emails e Web com impossibilidade de download.
-

Contra-medidas

- Se o usuário não pode instalar, elimina-se a possibilidade de sniffers.
 - Escolher protocolos criptografados, sempre quando houver possibilidade de escolha entre não-criptografados e criptografados.
 - Utilizar switches no lugar de hubs, o que dificulta sniffers e melhora o desempenho da rede.
-