
Sniffers

Captura de Informações

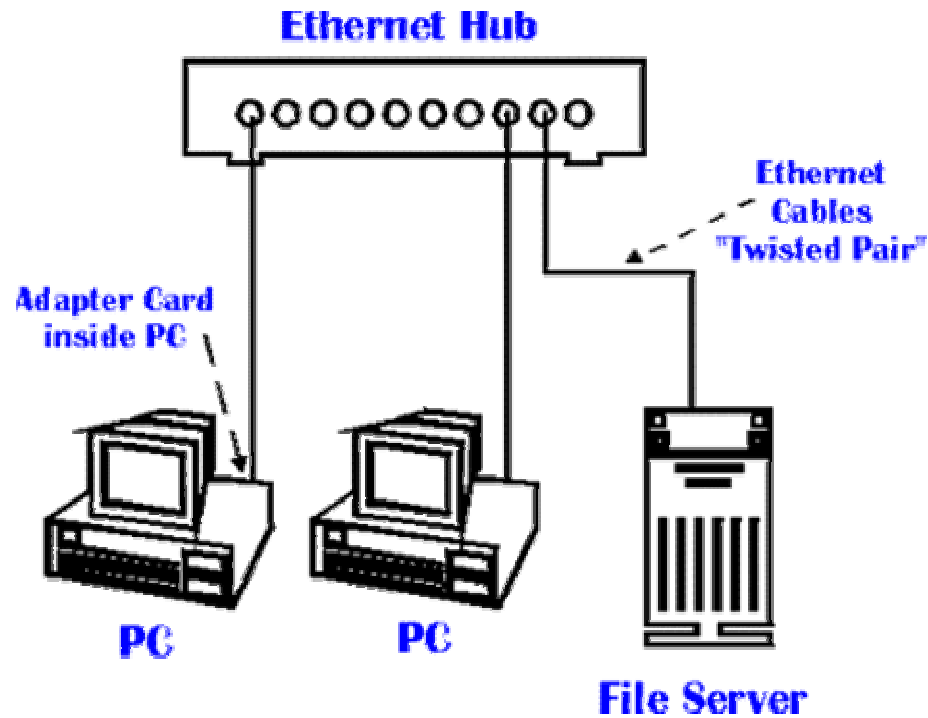
Sniffers

- 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 has a menu bar (File, View, Sniffer, Help) and a toolbar. The central pane is divided into two sections: a 'Connections' table and a 'Packets in Connection No.1' table.

#	Start Time	Client ...	Server (IP:Port)	Protocol	P...	Last Time
0	21:37:0...	192.168...	216.92.99.29:80	TCP:http	1	21:37:02
1	21:37:2...	192.168...	216.92.99.29:80	TCP:http	34	21:37:40
2	21:37:3...	192.168...	216.92.99.29:80	TCP:http	11	21:37:50
3	21:37:3...	192.168...	192.168.1.1:1900	UDP	4	21:38:00
4	21:37:3...	192.168...	192.168.1.255...	UDP	4	21:49:43
5	21:37:3...	192.168...	192.168.1.255...	UDP:n...	9	21:51:51
6	21:38:3...	192.168...	192.168.1.1:53	UDP:D...	20	21:48:42
7	21:38:3...	192.168...	202.107.60.39...	TCP:pop3	13	21:38:34
8	21:38:3...	192.168...	202.107.60.39...	TCP:pop3	28	21:38:38
9	21:40:5...	192.168...	207.68.171.24...	TCP:http	49	21:41:17
10	21:40:5...	192.168...	66.35.229.240:80	TCP:http	15	21:41:58
11	21:40:5...	192.168...	66.35.229.237:80	TCP:http	35	21:42:14

Time Offset	P...	D...	Data
21:37:20.813	62	0	
21:37:23.860	60	0	
21:37:23.860	54	0	
21:37:23.860	482	428	GET /sniffer/ 1
21:37:26.891	1506	1452	HTTP/1.1 200 O
21:37:26.891	1506	1452	ng="0" cellpad
21:37:26.891	54	0	
21:37:29.922	1506	1452	able> </td
21:37:29.922	1506	1452	indow external

The bottom section shows the details of a selected packet (1506 bytes):

- Ethernet Header
 - Dst Mac Address: 00.40...
 - Src Mac Address: 00.07...
 - Type: 2048
- IP Header
 - Header Length: 5
 - Version: 4
 - Service Type: 0
 - Total length: 1492
 - Identifier: 22706
 - Offset: 18384
 - TTL: 43
 - Protocol: 6
 - Check Sum: 62538

The data field shows the raw packet bytes in hexadecimal and their corresponding ASCII representation:

```
0000 00 40 B8 50 A5 AC 00 07 53 02 17 D1 08 00 45 00 .@.P....S.....E.
0010 05 D4 58 B4 40 00 2B 06 F4 4A D8 5C 63 1D C0 A8 ..X.B.+..J.\c...
0020 01 03 00 50 0B F6 9E FC 46 4A AB DB A4 F8 50 10 ...P....FJ....P.
0030 FF FF ED B5 00 00 48 54 54 50 2F 31 2E 31 20 32 .....HTTP/1.1 2
0040 30 30 20 4F 4B 0D 0A 44 61 74 65 3A 20 53 61 74 00 OK..Date: Sat
0050 2C 20 30 37 20 4A 75 6E 20 32 30 30 33 20 31 33 , 07 Jun 2003 13
0060 3A 33 37 3A 32 34 20 47 4D 54 0D 0A 53 65 72 76 :37:24 GMT..Serv
0070 65 72 3A 20 41 70 61 63 68 65 2F 31 2E 33 2E 32 er: Apache/1.3.2
0080 37 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 64 7..Last-Modified
0090 3A 20 53 61 74 2C 20 33 31 20 4D 61 79 20 32 30 : Sat, 31 May 20
00A0 30 33 20 30 38 3A 32 34 3A 30 39 20 47 4D 54 0D 03 08:24:09 GMT.
00B0 0A 45 54 61 67 3A 20 22 36 30 38 36 34 32 2D 35 .ETag: "608642-5
00C0 39 32 37 2D 33 65 64 38 36 36 61 39 22 0D 0A 41 927-3ed866a9"...A
00D0 63 63 65 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 ccept-Ranges: by
00E0 74 65 73 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E tes..Content-Len
00F0 67 74 68 3A 20 32 32 38 32 33 0D 0A 4B 65 65 70 gth: 22823..Keep
```

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.
-