



Sniffery

- ▶ Wiele różnych programów dostępnych jest zarówno w środowisku UNIX jak i MS-Windows.
 - ▶ Solaris: `snoop`
 - ▶ Linux, *BSD: `tcpdump`, `wireshark`
 - ▶ Wszystkie systemy UNIX: specyficzne sniffery ukierunkowane na zbieranie haseł z nawiązywanych połączeń FTP, POP3 i innych protokołów.
- ▶ Wiele z nich można znaleźć pod adresem <http://freshmeat.net/> lub <http://sourceforge.net/>
- ▶ Niektóre nazwy: `snort`, `IPgrab`, `ettercap`, `One Way Network Sniffer`, etc.

Przykładowy wynik działania:

```
49 asic ts/pub/src# snoop cyber
   asic -> cyber    TELNET C port=53218
   cyber -> asic     TELNET R port=53218 login:
   asic -> cyber    TELNET C port=53218
   asic -> cyber    TELNET C port=53218 t
   cyber -> asic     TELNET R port=53218 t
   asic -> cyber    TELNET C port=53218
   asic -> cyber    TELNET C port=53218 s
   cyber -> asic     TELNET R port=53218 s
   asic -> cyber    TELNET C port=53218
   cyber -> asic     TELNET R port=53218 s/key 90
                                cy11009\r\n
   asic -> cyber    TELNET C port=53218
   cyber -> asic     TELNET R port=53218 PASSCODE
                                or Password
   asic -> cyber    TELNET C port=53218
   asic -> cyber    TELNET C port=53218 a
   cyber -> asic     TELNET R port=53218
   asic -> cyber    TELNET C port=53218 b
   cyber -> asic     TELNET R port=53218
   asic -> cyber    TELNET C port=53218 c
   cyber -> asic     TELNET R port=53218
   asic -> cyber    TELNET C port=53218
```

