T: Rodzaje testów i pomiarów pasywnych.

Podział pomiarów i testów sieci komputerowych:
- testy parametrów fizycznych (okablowanie strukturalne),
- testy i pomiary pasywne (obserwacja funkcjonowania sieci),
- testy i pomiary aktywne (wykorzystanie dodatkowych danych testowych).

Wykonując testy pasywne administrator zbiera informacje dotyczące funkcjonowania sieci poprzez monitorowanie ruchu pakietów sieciowych między urządzeniami. Do testów pasywnych wykorzystywane są programy nazywane sniferami.

Zadanie1:

Wykorzystując serwis internetowy Wikipedii wyjaśnij pojęcie `sniffer`.

Do najpopularniejszych programów do analizy ruchu sieciowego należą:
- tcpdump,
- wireshark (https://www.wireshark.org/),
- snort.

Zadanie2:

Przeprowadź diagnozę ruchu sieciowego w systemie Linux za pomocą programu `tcpdump`.

Jakie dane zostały przechwycone przez komputer stacjonarny?

```
ifconfig eth0 promisc
ifconfig eth0 nopromisc
tcpdump -i eth0
tcpdump src or dst host 149.156.137.250
```

Zadanie3:

Przeprowadź diagnozę ruchu sieciowego za pomocą programu `wireshark`. Ogranicz nasłuchiwanie programu do usługi ftp i przeprowadź nasłuch połączenia do serwera (TCP – ftp [SYN], Analyze/Follow TCP Stream).

```
/etc/init.d/vsftpd status
netstat -ant | grep :21
ftp admin3tib2@hostname
```

Do przeprowadzania monitoringu ruchu sieciowego w systemach Windows Serwer można wykorzystać oprogramowanie Microsoft Internet and Security Acceleration Server.