

## **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], Analize/Follow TCP Stream).

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

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

Microsoft Internet Security and Acceleration Server 2004

Microsoft Internet Security & Acceleration Server 2004 Standard Edition

Monitoring SBS2005

Dashboard Alerts Sessions Services Reports Connectivity **Logging**

Filter By	Condition	Value
Log Record Type	Equals	Firewall or Web P...
Log Time	Live	
Action	Not Equal	Connection Status

Log Time	Destination IP	Destination P...	Protocol	Action	Rule	Client IP	Client Username	Source Networ
2014-09-16 16:10:50	212.77.100.127	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:50	212.77.100.127	80	HTTP	Closed Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	212.77.100.127	80	HTTP	Initiated Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	82.196.187.209	80	HTTP	Initiated Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	212.77.100.127	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:50	212.77.100.127	80	HTTP	Closed Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	82.196.187.209	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:50	82.196.187.209	80	HTTP	Closed Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	213.189.48.248	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:50	213.189.48.246	80	HTTP	Initiated Connection		192.168.11.150		Local Host
2014-09-16 16:10:50	213.189.48.246	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:50	213.189.48.248	80	http	Allowed Connection	tomek ulga wyjs...	192.168.19.29	SBSMENIS\student1...	Internal
2014-09-16 16:10:51	192.168.19.1	8080	proxy	Initiated Connection		192.168.19.29		Internal
2014-09-16 16:10:51	192.168.19.1	8080	proxy	Initiated Connection		192.168.19.29		Internal
2014-09-16 16:10:51	192.168.19.1	8080	proxy	Initiated Connection		192.168.19.29		Internal

132 items (Query is done)