

T: Testy pasywne i aktywne sieci komputerowych.

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 snifferami.

W testach pasywnych do analizy funkcjonowania sieci komputerowych można wykorzystać oprogramowanie typu sniffer. Sniffer to program komputerowy służący do przechwytywania i analizowania pakietów sieciowych.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat programów typu sniffery.

Sniffer – program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci.

Wspólną cechą wielu takich analizatorów jest przełączenie karty sieciowej w tryb mieszany (ang. promiscuous), w którym urządzenie odbiera wszystkie ramki z sieci, także te nieadresowane bezpośrednio do niego; sniffery mogą być uruchamiane także na routerze lub na komputerze będącym jedną ze stron komunikacji sieciowej – i w tych przypadkach tryb promiscuous nie jest konieczny.

Sniffer stanowi nieodzowne narzędzie diagnostyczne większości administratorów sieci, zwłaszcza podczas diagnostyki problemów z niezawodnością lub wydajnością połączeń. Może być również stosowany do monitorowania aktywności sieciowej osób trzecich, co jest w większości przypadków niezgodne z prawem. W celu ochrony przed takimi atakami, niektóre protokoły komunikacyjne stosują mechanizmy kryptograficzne.

Najczęściej używanymi programami tego typu są: tcpdump, sniffit, ettercap, dsniiff, wireshark (dawniej ethereal) oraz snort. Ten ostatni pełni także funkcję sieciowego systemu wykrywania intruzów. Istnieją także liczne bardziej specjalizowane narzędzia tego typu (np. komercyjne systemy przeznaczone na potrzeby organów ścigania i służb wywiadowczych).

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 -promisc
tcpdump -i enp0s3
tcpdump src or dst host 149.156.137.250
```

Zrzut ekranu prezentujący działanie programu tcpdump:

```
root@ubuntu: ~
16:37:29.357163 IP cluster010.ovh.net.http > 10.0.2.15.40028: Flags [P.], seq 10129:10460, ack 1483, win 65535, length 331
16:37:29.364042 IP cluster010.ovh.net.http > 10.0.2.15.40028: Flags [P.], seq 10460:13191, ack 1483, win 65535, length 2731
16:37:29.364079 IP 10.0.2.15.40028 > cluster010.ovh.net.http: Flags [.], ack 13191, win 62480, length 0
16:37:29.372510 IP cluster010.ovh.net.http > 10.0.2.15.40031: Flags [P.], seq 17615:19075, ack 1479, win 65535, length 1460
16:37:29.372554 IP 10.0.2.15.40031 > cluster010.ovh.net.http: Flags [.], ack 19075, win 65320, length 0
16:37:29.381985 IP cluster010.ovh.net.http > 10.0.2.15.40031: Flags [P.], seq 19075:20884, ack 1479, win 65535, length 1809
16:37:29.382030 IP 10.0.2.15.40031 > cluster010.ovh.net.http: Flags [.], ack 20884, win 65320, length 0
16:37:29.388054 IP cluster010.ovh.net.http > 10.0.2.15.40030: Flags [P.], seq 14948:18515, ack 1479, win 65535, length 3567
16:37:29.388090 IP 10.0.2.15.40030 > cluster010.ovh.net.http: Flags [.], ack 18515, win 65320, length 0
16:37:29.852565 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 1952:2283, ack 1043, win 65535, length 331
16:37:29.852617 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 2283, win 35394, length 0
16:37:29.860635 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 2283:4872, ack 1043, win 65535, length 2589
16:37:29.860696 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 4872, win 39760, length 0
16:37:30.104067 IP cluster010.ovh.net.http > 10.0.2.15.40027: Flags [P.], seq 4872:5241, ack 1043, win 65535, length 369
16:37:30.104105 IP 10.0.2.15.40027 > cluster010.ovh.net.http: Flags [.], ack 5241, win 42600, length 0
16:37:30.114204 IP 10.0.2.15.15176 > slb-cache-ns.tkk.net.pl.domain: 5036+ A? zs9elektronik.pl. (34)
16:37:30.114360 IP 10.0.2.15.61593 > slb-cache-ns.tkk.net.pl.domain: 33433+ AAAA? zs9elektronik.pl. (34)
16:37:30.153858 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.15176: 5036 1/0/0 A 79.96.95.47 (50)
16:37:30.168369 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.61593: 33433 0/1/0 (85)
16:37:30.172095 IP 10.0.2.15.22420 > slb-cache-ns.tkk.net.pl.domain: 50888+ A? www.greszata.pl. (33)
16:37:30.172237 IP 10.0.2.15.44859 > slb-cache-ns.tkk.net.pl.domain: 61642+ AAAA? www.greszata.pl. (33)
16:37:30.236472 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.22420: 50888 2/0/0 CNAME greszata.pl., A 87.98.239.19 (63)
16:37:30.376894 IP slb-cache-ns.tkk.net.pl.domain > 10.0.2.15.44859: 61642 1/1/0 CNAME greszata.pl. (101)
16:37:32.424071 IP 10.0.2.15.48878 > fra15s18-in-f14.1e100.net.https: Flags [.], ack 2748807, win 65535, length 0
16:37:32.431071 IP fra15s18-in-f14.1e100.net.https > 10.0.2.15.48878: Flags [.], ack 19098, win 65535, length 0
^C
952 packets captured
955 packets received by filter
0 packets dropped by kernel
root@ubuntu:~# tcpdump -i eth0
```

Zadanie3:

Odszukaj w serwisie internetowym dobreprogramy.pl informacje na temat programu Wireshark.

Wireshark jest jednym z popularniejszych programów wykorzystywanych do analizy ruchu sieciowego. W celu uniknięcia problemów z uprawnieniami do zarządzania kartami sieciowymi, program należy uruchomić z poziomu administratora systemu:

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Zapisz

No.	Time	Source	Destination	Protocol	Length	Info
30	4.259196000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [SYN, ACK] Seq=0 Ack=1
31	4.263547000	10.0.2.15	91.121.70.102	TCP	54	52542 > http [ACK] Seq=1 Ack=1 Win=2
32	4.268839000	10.0.2.15	91.121.70.102	HTTP	373	GET /sig/135.jpg HTTP/1.1
33	4.271871000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [ACK] Seq=1 Ack=320 Win
34	5.431637000	10.0.2.15	91.121.70.102	TCP	54	52542 > http [FIN, ACK] Seq=320 Ack=
35	5.431904000	10.0.2.15	87.98.239.19	HTTP	489	GET /psk/2 konfiguracja_i_obsługa_lo
36	5.434168000	91.121.70.102	10.0.2.15	TCP	60	http > 52542 [ACK] Seq=1 Ack=321 Win
37	5.434213000	87.98.239.19	10.0.2.15	TCP	60	http > 40034 [ACK] Seq=2083 Ack=1215
38	5.555374000	87.98.239.19	10.0.2.15	TCP	317	[TCP segment of a reassembled PDU]
39	5.555417000	10.0.2.15	87.98.239.19	TCP	54	40034 > http [ACK] Seq=1215 Ack=2346

▶ Frame 35: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0

▶ Ethernet II, Src: CadmusCo_1f:b4:e6 (08:00:27:1f:b4:e6), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 87.98.239.19 (87.98.239.19)

▶ Transmission Control Protocol, Src Port: 40034 (40034), Dst Port: http (80), Seq: 780, Ack: 2083, Len: 435

▼ Hypertext Transfer Protocol

▶ GET /psk/2 konfiguracja_i_obsługa_lokalnych_sieci_komputerowych/ HTTP/1.1\r\n

Host: greszata.pl\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: pl,en-US;q=0.7,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://greszata.pl/psk/\r\n

Cookie: 60gpBAK=R1224225179; 60gp=R477089669\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://greszata.pl/psk/2_konfiguracja_i_obsługa_lokalnych_sieci_komputerowych/]

0030 87 70 54 52 00 00 47 45 54 20 2f 70 73 6b 2f 32 .PTR..GET /psk/2

0040 5f 6b 6f 6e 66 69 67 75 72 61 63 6a 61 5f 69 5f konfiguracja_i

0050 6f 62 73 6c 75 67 61 5f 6c 6f 6b 61 6c 6e 79 63 obsługa_lokalnyc

0060 68 5f 73 69 65 63 69 5f 6b 6f 6d 70 75 74 65 72 h_sieci_komputer

Text item (text), 75 bytes Packets: 48 · Displayed: 48 (100,0%) Profile: Default

W celu wykorzystania programu Wireshark do analizy sieci wykonaj następujące czynności:

- uruchom program,
- wybierz polecenie Interfaces z menu Capture i wskaż kartę sieciową, z której będą przechwytywane dane,
- uruchom nasłuchiwanie ruchu sieciowego klikając przycisk Start,
- można wymusić ruch sieciowy poprzez połączenie z komputerem skanującym z innej stacji sieciowej dowolnym klientem sieciowym,
- po zarejestrowaniu danych sieciowych wyłączyć skanowanie klikając przycisk Stop z menu Capture.

Po zarejestrowaniu danych należy dokonać analizy przechwyconych pakietów. Do tego celu pomocne może być polecenie Follow TCP Stream dostępne w menu Analyze. Wcześniej należy zaznaczyć pakiet, dla którego chcemy przeprowadzić analizę.

Zadanie4:

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.

Wykonując testy aktywne administrator wprowadza do sieci dodatkowe dane, które ułatwiają monitorowanie ruchu pakietów sieciowych między urządzeniami. Pomiary aktywne przeprowadza się w celu sprawdzenia jakości usług sieciowych (QoS, ang. Quality of Service).

Testy aktywne pozwalają określić jakość usług sieciowych (Quality of Service, QoS).

Podczas testów aktywnych dokonuje się pomiarów następujących parametrów:

- dostępność usługi,
- opóźnienie w jednym kierunku (One Way Delay Minimum, OWD),
- zmienność opóźnienia przekazu pakietów (IP Packet Delay Variation, IPDV),
- opóźnienie pakietów w pętli (Round Trip Delay, RTD),
- straty pakietów (One Way Loss, OWL),
- poziom strat pakietów (IP Packet Loss Ratio, IPLR).

Parametry diagnozowane podczas pomiarów aktywnych:

- przepustowość sieci – możliwość przesyłania danych między źródłem a celem,
- opóźnienie przesyłanych danych – np. minimalne opóźnienie, średnie opóźnienie, sprawdzane w jednym kierunku lub w obu kierunkach,
- straty pakietów danych – np. ilość zagubionych danych przesyłanych w sieci.

Zadanie5:

Odszukaj w serwisie internetowym Wikipedii informacje na temat protokołu ICMP oraz programów ping i traceroute. Zwróć uwagę na różnicę w działaniu programów tracert i mtr.

ICMP (ang. Internet Control Message Protocol, internetowy protokół komunikatów kontrolnych) – jest to protokół warstwy sieciowej modelu OSI, wykorzystywany w diagnostyce sieci oraz trasowaniu.

Programy przeznaczone do testów aktywnych:

- ping,
- tracert/traceroute.

Ping – polecenie służące do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami, zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami. Opóźnienie to czas wymagany, aby wysłany pakiet danych dotarł do odbiorcy, a odpowiedź zwrotna trafiła z powrotem do nadawcy. Ping korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply.

Zadanie6:

Przeprowadź diagnozę ruchu sieciowego za pomocą programu ping.

```
ping localhost
ping -n 2 s27st01
ping -t wp.pl
ping -l 1500 -f wp.pl
```

Jakie dane zostały przekazane przez program ping?

```

C:\>ping 192.168.100.1
Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time=4ms TTL=63
Reply from 192.168.100.1: bytes=32 time=3ms TTL=63
Reply from 192.168.100.1: bytes=32 time=9ms TTL=63
Reply from 192.168.100.1: bytes=32 time=15ms TTL=63

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 15ms, Average = 7ms

C:\>ping wp.pl
Pinging wp.pl [212.77.100.101] with 32 bytes of data:
Reply from 212.77.100.101: bytes=32 time=24ms TTL=250
Reply from 212.77.100.101: bytes=32 time=31ms TTL=250
Reply from 212.77.100.101: bytes=32 time=26ms TTL=250
Reply from 212.77.100.101: bytes=32 time=23ms TTL=250

Ping statistics for 212.77.100.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 31ms, Average = 26ms

C:\>_

C:\>ping -l 1473 -f wp.pl
Pinging wp.pl [212.77.100.101] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 212.77.100.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping -l 1472 -f wp.pl
Pinging wp.pl [212.77.100.101] with 1472 bytes of data:
Reply from 212.77.100.101: bytes=1472 time=58ms TTL=250
Reply from 212.77.100.101: bytes=1472 time=33ms TTL=250
Reply from 212.77.100.101: bytes=1472 time=30ms TTL=250
Reply from 212.77.100.101: bytes=1472 time=32ms TTL=250

Ping statistics for 212.77.100.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 58ms, Average = 38ms

C:\>_

```

Traceroute - program służący do badania trasy pakietów w sieci IP. Działanie traceroute opiera się na protokołach komunikacyjnych UDP oraz ICMP.

Zadanie7:

Przeprowadź diagnozę ruchu sieciowego za pomocą programu traceroute.

tracert hostname

tracert wp.pl

tracert wp.pl

mtr wp.pl (<https://ubuntix.pl/jak-korzysta-z-komendy-linux-mtr-my-traceroute>)

gnome-nettool

```

C:\>tracert wp.pl
Tracing route to wp.pl [212.77.100.101]
over a maximum of 30 hops:

  0  4 ms    1 ms    3 ms   192.168.10.17
  1  9 ms    16 ms   16 ms   10.1.10.1
  2  24 ms   23 ms   14 ms   83.145.140.25
  3  27 ms   27 ms   27 ms   wp.plix.pl [195.182.218.204]
  4  26 ms   29 ms   32 ms   rtr-2.rtr-int-1.adm.wp.sa.pl
  5  24 ms   23 ms   23 ms   www.wp.pl [212.77.100.101]

Trace complete.

C:\>_

```

```

Administrator: Wiersz polecenia
C:\>tracert wp.pl
Tracing route to wp.pl [212.77.98.9]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  s27wifi [192.168.27.1]
  2  <1 ms  <1 ms  <1 ms  192.168.11.1
  3  7 ms   13 ms  3 ms   85.16.97.176.in-addr.arpa [176.97.16.85]
  4  7 ms   5 ms   5 ms   74.16.97.176.in-addr.arpa [176.97.16.74]
  5  1 ms   1 ms   1 ms   core17.184.kosman.pl [62.108.184.17]
  6  2 ms   1 ms   1 ms   lt-1-2-0v12.z-kosman-com-gw.kosman-gw.man.koszal
in.pl [62.108.160.1]
  7  5 ms   4 ms   4 ms   koszalin-jra.10ge.task.gda.pl [153.19.0.97]
  8  4 ms   4 ms   4 ms   wp-jro4.10ge.task.gda.pl [153.19.102.6]
  9  11 ms  19 ms  11 ms  rtr-int-1.rtr1.adm.wp-sa.pl [212.77.96.42]
 10  11 ms  11 ms  10 ms  www.wp.pl [212.77.98.9]

Trace complete.

C:\>_

```

