Wnioski ucznia – CW5: Testowanie połączenia sieciowego w Ubuntu

Dokument zawiera zwięzłe wnioski do wpisania do zeszytu, opracowane na podstawie instrukcji ćwiczenia.

Wniosek ogólny

- Potrafię testować i analizować połączenia sieciowe w Ubuntu przy użyciu poleceń: ping, host, traceroute, whois, dig, netstat, ss, tcpdump i nmap.
- Rozumiem podstawy działania protokołów ICMP, IP, DNS, TCP i UDP oraz umiem diagnozować typowe problemy sieciowe.
- Umiem podsłuchiwać ruch sieciowy w czasie rzeczywistym i z pliku PCAP, a także interpretować podstawowe parametry pomiarów (opóźnienia, straty, MTU).

Ping – kluczowe obserwacje

- Ping działa w oparciu o ICMP (poziom IP), dlatego TCP/UDP nie wpływają na wyniki.
- Wyniki pingu zawierają: liczbę wysłanych/odebranych pakietów, straty (%) oraz min/avg/max/mdev czasu odpowiedzi.
- Ping do nazwy hosta wymaga poprawnej rezolucji (plik /etc/hosts lub DNS).
- Ping do localhost (127.0.0.1) sprawdza stos sieciowy i interfejs loopback – zwykle brak strat.
- Wiele serwerów (np. instytucji publicznych) może blokować ICMP – brak odpowiedzi nie musi oznaczać awarii usługi.
- Większa liczba pakietów (-c 30) lepiej pokazuje stabilność łącza; TTL=1 pozwala zlokalizować miejsce odrzucenia; rozmiar -s i flaga -M do pozwalają testować MTU i fragmentację.

host / dig – DNS

- Pozwalają poznać adresy IP domen, aliasy i nazwy kanoniczne oraz sprawdzić odpowiedź serwera DNS.
- Wiele adresów IP dla jednej domeny wynika z równoważenia obciążenia (load balancing).

traceroute – trasa pakietów

- Pokazuje kolejne przeskoki (routery) do celu; gwiazdki (*) oznaczają brak odpowiedzi/filtrację/opóźnienia.
- Liczba hopów zależy od lokalizacji i topologii sieci.

whois – informacje rejestrowe

- Ujawnia właściciela domeny/adresu IP, daty utworzenia/aktualizacji, zakres (inetnum), kraj, adres oraz kontakt abuse.

- Dane domen rządowych bywa, że są częściowo ukryte.

netstat vs ss

- netstat pokazuje połączenia, porty nasłuchujące, trasę i statystyki, ale jest przestarzały (pakiet net-tools).
- ss jest szybsze i dokładniejsze: stany TCP/UDP, procesy używające portów, timery – zalecane zamiast netstat.

nmap – skanowanie

- Umożliwia wykrywanie otwartych portów i usług (TCP -sT, UDP -sU), systemu operacyjnego (-O) oraz hostów odpowiadających na ping (np. -sP).
- Skanowanie zakresów portów pomaga w audycie konfiguracji i bezpieczeństwa.

ip neighbour / ip route

- ip neighbour pokazuje mapowanie IP→MAC (tablica ARP) w sieci lokalnej.
- ip route show wyświetla tablicę routingu i bramę domyślną.

tcpdump – podgląd ruchu (część d)

- tcpdump -i <interfejs> przechwytuje pakiety; przy pingach widać ICMP echo request/reply.
- Każdy wpis zawiera timestamp, źródło→cel, protokół, id/seq/ttl/length; zwykle pokazywane są nagłówki.

tcpdump – zapis/odczyt PCAP (część e)

- -w zapisuje surowe pakiety do pliku PCAP (analiza offline, np. w Wireshark).
- -r odczytuje plik PCAP i wyświetla pakiety jak na żywo; zapisane pakiety odpowiadają temu, co zarejestrowano w części d.