**Uruchamianie usług sieciowych**

**Usługi** w systemie Linux, to programy uruchomione przez cały czas działania systemu w celu wykonania określonych czynności. Programy uruchomione w tle (nie przyłączone do konkretnego terminalu) nazywane są **demonami**. Demon, jeśli nie wykonuje konkretnego zadania, to nadal zajmuje pewien fragment pamięci komputera.

Z kolei **demony** mogą być zarządzane przez **superdemona**. Przykładem **superdemona** w systemie Ubuntu jest xinetd, który zarządza uruchamianiem usług sieciowych. Na przykład, zamiast uruchamiać proces usługi bezpiecznej powłoki (**SSH**), który pracując jako demon będzie zajmował zasoby komputera nawet gdy nie będzie prób nawiązania połączenia, możemy uruchomić proces sshd pod nadzorem superdemona. Wówczas superdemon będzie kontrolował port 22 i – w przypadku nadejścia połączenia – uruchomi proces sshd. W analogiczny sposób można uruchomić procesy innych usług sieciowych: serwera WWW, FTP czy poczty elektronicznej.

Serwer udostępniający usługi sieciowe, ma jednocześnie otwarte porty odpowiadające tym usługom. Listę otwartych portów danego hosta można uzyskać poleceniem nmap adres\_ip.

**Sprawdzenie otwartych portów**

**UWAGA program netstat pochodzi z pakietu net-tools (należy doinstalować)**

netstat -ant |grep 22 usługa ssh

netstat -ant |grep 23 usługa telnet

nmap należy doinstalować sudo apt install nmap

nmap localhost

nmap 192.168.0.1

**Usługi zdalnego dostępu do terminala linuxa**

Programy dla Windows do nawiązania połączenia przez zdalny dostęp

* **Putty**
* **WinSCP**

1. Telnet

Usługa sieciowa **telnet** pozwala zalogować się zdalnie do komputera i wykonywać na nim polecenia. Dane w sesjach telnetu są przesyłane bez szyfrowania, co naraża użytkownika na przechwycenie haseł i innych poufnych danych. Z tego względu nie jest możliwe bezpośrednie logowanie się na konto użytkownika **root** w systemie Linux.

Telnet to usługa działająca na zasadzie klient–serwer, kontrolowana przez superdemona xinetd. Klient jest dołączony do każdej dystrybucji systemu Ubuntu. Z kolei oprogramowanie serwera należy zainstalować samodzielnie.

Polecenie, którym sprawdzamy czy usługa telnet jest zainstalowana na komputerze:

**sudo systemctl status inetd**.

Jeśli nie, to instalujemy ją poleceniem:

**sudo apt install telnetd -y**.

Po instalacji próbujemy się połączyć z komputerem, gdzie jest zainstalowana usługa telnet, np. **telnet 172.22.2.100**.

Po nawiązaniu połączenia z innym komputerem zostaniemy poproszeni o podanie loginu do konta na zdalnym komputerze. Po udanym zalogowaniu możemy wykonywać dowolne polecenia na zdalnym komputerze.

port 23 połączenie nieszyfrowane

Instalacja serwera telnet

sudo apt install telnetd

Klienta telnet na Windows należy włączyć w funkcjach systemu

Podłączenie się do telnet z terminala klienta linuks

 telnet -l użytkownik ip

1. SSH usługa zdalnego dostępu do terminala

Usługa **SSH** (*Secure Shell*) umożliwia połączenie się użytkownika ze zdalnym komputerem i wykonywanie na nim poleceń, ale, w odróżnieniu od telnet-u, sesja połączenia jest szyfrowana. Protokół SSH jest oparty na kryptografii klucza publicznego. W praktyce oznacza to, że do korzystania z SSH potrzebne są dwa klucze kryptograficzne: publiczny oraz prywatny. Dane przesyłane w czasie transmisji są szyfrowane za pomocą klucza publicznego, natomiast można je odszyfrować za pomocą klucza prywatnego. Klucz publiczny jest powszechnie dostępny, może być upubliczniony i przesyłany przez sieć. Z kolei klucz prywatny musi być dobrze chroniony i nigdy nie jest przesyłany przez sieć. Każda kombinacja klucz prywatny/publiczny jest niepowtarzalna.

### Korzystanie z serwera SSH

Usługa SSH działa w architekturze klient-serwer. W systemie Ubuntu klient jest instalowany domyślnie. Serwer zaś można zainstalować poleceniem:

**sudo apt install ssh**

lub

**sudo apt install openssh-server**.

Do uruchomienia/zatrzymania/restartu serwera służy komenda

**sudo /etc/init.d/ssh** z odpowiednim parametrem dodanym na końcu.

Z kolei poleceniem

**sudo systemctl status ssh** sprawdzamy czy w systemie jest zainstalowany i uruchomiony serwer SSH.

Ze zdalnym komputerem łączymy się za pomocą polecenia:

**ssh witek@komp1**, gdzie witek to nazwa użytkownika, a komp1 to nazwa komputera, do którego będziemy się łączyć.

Zamiast nazwy hosta można również użyć adresu IP:

**ssh witek@172.22.2.100**. Jeśli pracujemy w systemie Windows, to najpopularniejszym klientem SSH dla Windowsów jest program [PuTTY](https://www.putty.org/" \o "https://www.putty.org/).

Jeśli okaże się, że połączenie przez usługę SSH nie udaje się, to należy zwrócić uwagę na dwie kwestie. Po pierwsze: upewnić się, że serwer SSH jest zainstalowany i uruchomiony: **sudo systemctl enable ssh**, **sudo systemctl start ssh**. Po drugie: połączenia z serwerem SSH mogą być blokowane przez firewall po stronie serwera.

* **sudo ufw allow ssh** – zezwól na połączenia na porcie 22 przez firewall
* **sudo ufw enable** – aktywuj firewall
* **sudo ufw status** – pokaż status zapory

Jeśli ktoś nawiązał połączenie z naszym komputerem, ale zachowuje się nieprofesjonalnie i chcemy zakończyć jego wizytę, to możemy to zrobić w następujący sposób. Sprawdzamy poleceniem **who** lub **w** czy poza nami jest jeszcze ktoś zalogowany na komputerze. Następnie szukamy procesów związanych z połączeniami SSH: **ps faux | grep sshd**. Druga kolumna wyników działania tego polecenia będzie zawierała identyfikatory procesów, które musimy wyłączyć. Robimy to komendą **kill -9 PID**, gdzie PID to liczbowy identyfikator procesu.

Dodatkowo warto również profilaktycznie zatrzymać działanie serwera SSH i zmienić hasło (**passwd**) lub całkowicie zablokować (**usermod -L login**) konto, na które ktoś się zalogował. Polecenie **usermod** powinno być wykonane z uprawnieniami administratora i tylko wtedy jeżeli posiadamy więcej niż jedno konto w systemie. W przeciwnym wypadku możemy zablokować sobie możliwość logowania się na własne konto.

### Polecenie scp

Polecenie **scp** (*OpenSSH secure file coppy*) jest przydatnym narzędziem do kopiowania z oraz na zdalny komputer. Warunkiem koniecznym jego użycia jest oczywiście posiadanie konta (dokładniej: danych autoryzacyjnych do konta) na zdalnym komputerze.

Składnia plecenia **scp** kiedy chcemy pobrać plik ze zdalnego serwera:

**scp użytkownik@host:ścieżka\_do\_pliku\_zdalnego nazwa\_pliku\_lokalnego**

Składnia plecenia **scp** do wysłania pliku lokalnego na zdalny serwer:

**scp nazwa\_pliku\_lokalnego użytkownik@host:ścieżka\_do\_pliku\_zdalnego**

Oczywiście przy użyciu polecenia **scp** można również przesłać plik pomiędzy dwoma zdalnymi komputerami będąc zalogowanym na trzecim komputerze.

Pracuje na porcie 22

Usługa klient serwer

Połączenie jest szyfrowane

Zdalne kopiowanie plików

**scp plik użytkownik@nasze\_ip**

Instalacja serwera ssh

sudo apt install openssh-server

Instalacja klienta ssh (uwaga klient może być już zainstalowany domyślnie na linuxie). Jako klienta w Windows używamy programu putty (należy zainstalować)

sudo apt install openssh-client

Uruchomienie serwera ssh

$ systemctl status ssh

$ sudo systemctl restart ssh

Sprawdzenie listy otwartych portów

netstat -tlpn

nmap (trzeba doinstalować)

Odblokowanie portów na zaporze ufw dla usługi ssh

$ sudo ufw allow ssh

Włączenie ssh podczas startu systemu

$ sudo systemctl enable ssh

Połączenie z serwerem ssh z klienta linuksowego

$ ssh [linuxconfig@192.168.1.112](mailto:linuxconfig@192.168.1.112)

ssh użytkownik@adres\_IP\_serwera

KONFIGURACJA SERWERA SSH

Plik konfiguracyjny sshd\_config

/etc/ssh/sshd\_config

Zmiana domyślnego portu

Linia

port 2823

Ustawienie przepuszczenia portu na ufw

$ sudo ufw allow 8282/tcp

Restart serwera aby wprowadzić zmiany

$ sudo systemctl restart ssh

Logowanie się na kliencie do usługi SSH na innym porcie niż domyślny

$ ssh -p 8282 linuxconfig@192.168.1.112