

Protokoły zdalnego logowania Telnet i SSH

Krzysztof Maćkowiak

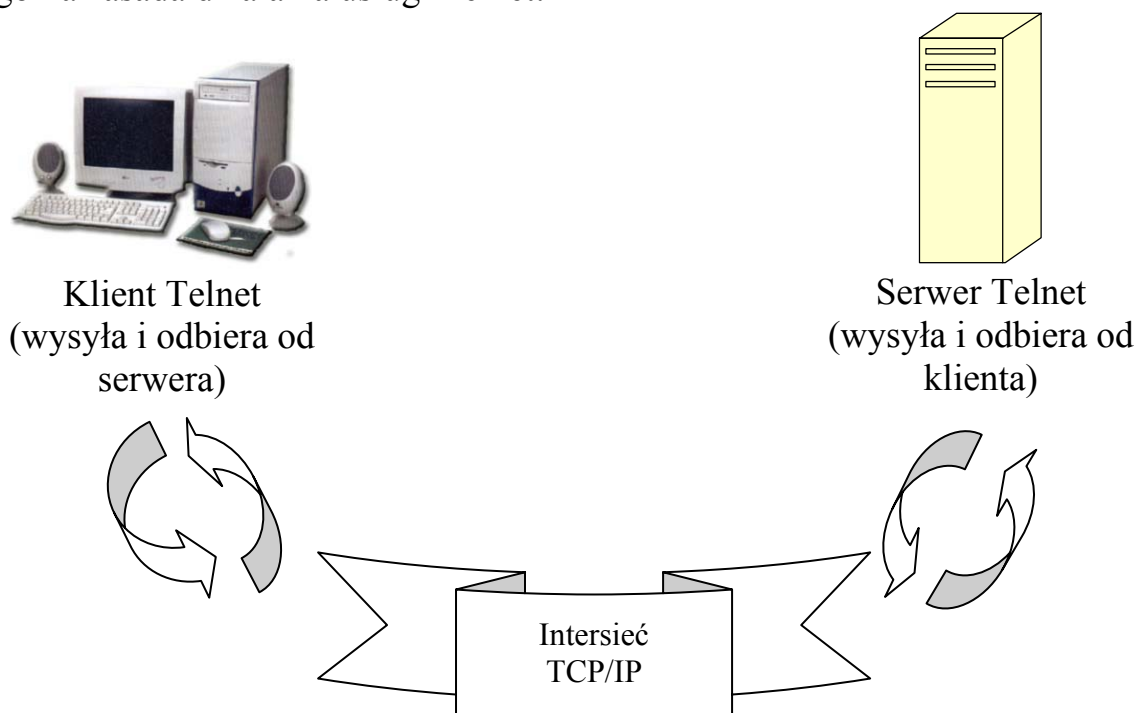
Wprowadzenie

Wykorzystując Internet mamy możliwość uzyskania dostępu do komputera w odległej sieci z wykorzystaniem swojego komputera, który spełnia w tym przypadku rolę wirtualnego terminala. Proces ten nosi nazwę zdalnego logowania. Po zalogowaniu się na odległy komputer mamy dostęp do zasobów – danych i aplikacji, znajdujących się na zdalnej maszynie.

Protokół Telnet

W celu terminalowego dostępu do komputerów i zasobów informatycznych możemy skorzystać z protokołu Telnet, należącego do warstwy aplikacyjnej i wykorzystującego protokół TCP. Protokół ten korzysta z portu 23 i jest oparty na modelu klient-serwer. Użytkownik chcący skorzystać z tej usługi musi posiadać program Telnet, będący klientem. Serwer świadczy usługi. Na serwerze wymagany jest specjalny proces nadzorujący. W systemach rodziny UNIX proces ten nosi najczęściej nazwę telnetd, w systemach Windows jest to Telnet server.

Ogólna zasada działania usługi Telnet:



Rys.5. Usługa Telnet – komunikacja pomiędzy klientem i serwerem.

Fazy korzystania z protokołu Telnet

Nawiązywanie połączenia.

Po uruchomieniu program Telnet przechodzi w tryb przyjmowania poleceń. W celu nawiązania połączenia z odległą maszyną należy podać jej adres IP lub odpowiadającą mu nazwę mnemoniczną: `telnet 232.152.12.1`. Po nawiązaniu połączenia na ekranie widzimy komunikat potwierdzający nawiązanie połączenia: `Connected to tpsa` (W zależności od programu klienta komunikat może się trochę różnić). Kiedy zostanie ustanowione połączenie, tworzony jest wirtualny terminal sieciowy (NVT) na obydwu końcach połączenia. Eliminuje to potrzebę zapamiętywania wzajemnych właściwości terminali klienta i serwera. Wszystkie hosty odwzorowują właściwości i konwencje swoich urządzeń lokalnych, aby wydawało się, że uzyskują dostęp do NVT przez sieć.

Autoryzacja użytkownika.

Po nawiązaniu połączenie następuje etap autoryzacji użytkownika. Odbywa się on w podobny sposób, w jaki użytkownik uzyskuje prawa do zasobów logując się lokalnie. W pierwszej kolejności użytkownik podaje nazwę użytkownika(login), następnie podaje hasło.

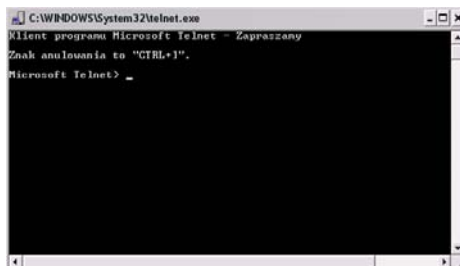
Praca na zdalnym serwerze.

Użytkownik po zalogowaniu może swobodnie pracować na odległej maszynie, tak jakby siedział przy jej terminalu. Może wydawać wszystkie polecenia, które odnoszą się do serwera. Wydawane polecenia mogą zmieniać konfigurację zdalnego serwera. Wszystkie dane zawarte są na serwerze. Gdy użytkownik wykona jakąś operację np. zmieni jakieś dane – zostaną zmienione dane na serwerze zdalnym.

Zakończenie połączenia.

W celu zakończenia połączenia należy wydać polecenie `logout`.

Standardowy klient usługi Telnet w systemie Windows:



Rys.6. Okna terminala programu Telnet.

Inne aplikacje typu klient usługi Telnet dla systemu Windows to: CRT 2.0, NetTerm 4.03.

Specyfikacja protokołu Telnet zawarta jest w dokumencie RFC854 [3].

Największą wadą usługi Telnet jest przesyłanie hasła podczas autoryzacji w formie niezaszyfrowanej. Hasło takie może zostać przechwycone w trakcie przesyłania przez osobę korzystającą z programu podsłuchującego (*Sniffer*). Z tego powodu zaleca się stosowanie SSH (*Secure Shell*) umożliwiającego komunikację pomiędzy klientem a serwerem za pomocą szyfrowanego połączenia. Korzystając z SSH zaleca się wyłączenie usługi Telnet w systemie.

Protokół SSH (Secure Shell)

Jest usługą odpowiadającą usłudze Telnet, dodatkowo rozszerzoną o możliwość szyfrowania połączenia pomiędzy klientem a serwerem. Podobnie jak usługa Telnet jest ona oparta na modelu klient-serwer. Po stronie użytkownika musi być włączony klient SSH, natomiast po drugiej stronie serwer SSH. Standardowy numer portu protokołu SSH to 22.

Protokół SSH [1] składa się z trzech głównych komponentów:

- protokół warstwy transportu (uwierzytelnienie serwerów, poufność, integralność, tajność przekierowania, opcjonalna kompresja),
- protokół uwierzytelniania użytkownika,
- protokół połączenia, który zwielokrotnia zaszyfrowany tunel w kilka logicznych kanałów.

Integralność danych chroniona jest poprzez dołączanie do każdego pakietu kodu uwierzytelniającego komunikat (MAC), obliczonego na podstawie wspólnego zakodowanego hasła, numeru kolejnego pakietu oraz zawartości tego pakietu.

Fazy korzystania z protokołu SSH

Nawiązywanie połączenia.

Połączenie SSH inicjowane jest po stronie programu-klienta. W celu nawiązania połączenia użytkownik wydaje polecenie: `ssh -l uzytkownik nasz_system.pl`.

Autoryzacja użytkownika może przebiegać w dwojaki sposób:

1. Na podstawie podanej nazwy użytkownika i hasła.
2. W celu zwiększenia bezpieczeństwa można zastosować technikę klucza publicznego z wykorzystaniem algorytmu szyfrowania asymetrycznego RSA. W pierwszej kolejności klient generuje parę kluczy (polecenie `ssh-`

keygen). Następnie łączy się z serwerem i otrzymuje od niego jego klucz publiczny. Klucz ten porównywany jest z zachowanym w wewnętrznej bazie danych klienta, z poprzednich połączeń. W przypadku wykrycia niezgodności kluczy wyświetlane jest specjalne ostrzeżenie umożliwiające przerwanie połączenia. Następnie, klient przekazuje serwerowi swój klucz publiczny, generuje losową 256 bitową liczbę, szyfruje ją przy pomocy swojego klucza prywatnego oraz klucza publicznego serwera. Serwer po otrzymaniu tak zakodowanej liczby rozszyfrowuje ją przy pomocy swojego klucza prywatnego i klucza publicznego klienta. Tak otrzymana liczba jest losowa a ponadto znana tylko klientowi i serwerowi. Jest ona używana jako klucz do szyfrowania dalszej komunikacji, z wykorzystaniem między innymi takich algorytmów symetrycznych jak: IDEA, DES, 3DES, Blowfish. Korzystanie z takiego rozwiązania jest bezpieczniejsze i mniej uciążliwe w eksploatacji – nie trzeba za każdym razem podawać nazwy użytkownika i hasła.

Dodatkowe możliwości protokołu SSH

Przydatną opcją protokołu SSH jest tzw. *Port Forwarding* [2]. Mechanizm ten pozwala na kierowanie poprzez bezpieczny kanał komunikacyjny SSH danych przeznaczonych dla innych, niechronionych portów, co gwarantuje równie wysoki poziom bezpieczeństwa, jak w przypadku dostępu do konsoli systemu poprzez SSH. W ten sposób można np. szyfrować pocztę przekazywaną poprzez protokół POP3, chociaż sam POP3 zapewnia zupełnie jawną transmisję danych i umożliwia swobodny dostęp do przesyłanych tekstów. Z uwagi na fakt, że mechanizm *Port Forwarding* działa równolegle do samego shella, istnieje więc także możliwość jednoczesnego wydawania poleceń oraz odbierania w tle poczty elektronicznej (lub korzystania z innej usługi). Zakładając, że zdalny komputer nosi nazwę *webs*, program *ssh* należy uruchomić w następujący sposób: `ssh -L 110:webs:110`. Po prawidłowym zalogowaniu port 110 lokalnego systemu zostanie połączony z takim samym portem zdalnego komputera. Komunikacja będzie odbywać się poprzez bezpieczny kanał transmisyjny.

Rozszerzeniem protokołu SSH jest protokół *scp* (secure copy), umożliwiający bezpieczne przesyłanie plików.

Przykładowe darmowe narzędzia służące do obsługi tego protokołu to: PuTTY, Tera Term Pro/TTssh.

Zastosowanie protokołów Telnet i SSH

Protokoły Telnet oraz SSH mogą być wykorzystywane do:

- pracy na zdalnej maszynie,

- korzystania ze zdalnych baz danych,
- konfigurowania odległego serwera lub routera,
- korzystania z poczty e-mail,
- eksploatacji serwera WWW,
- itp.

Literatura

1. Kaeo Merike, *Tworzenie bezpiecznych sieci*. MIKOM 2000.
2. Pawlak Marcin, *Bezpieczna komunikacja*. CHIP, Grudzień 1999.
3. Postel J., Reynolds J.K., *Telnet Protocol Specification*. RFC 854, Maj 1983.