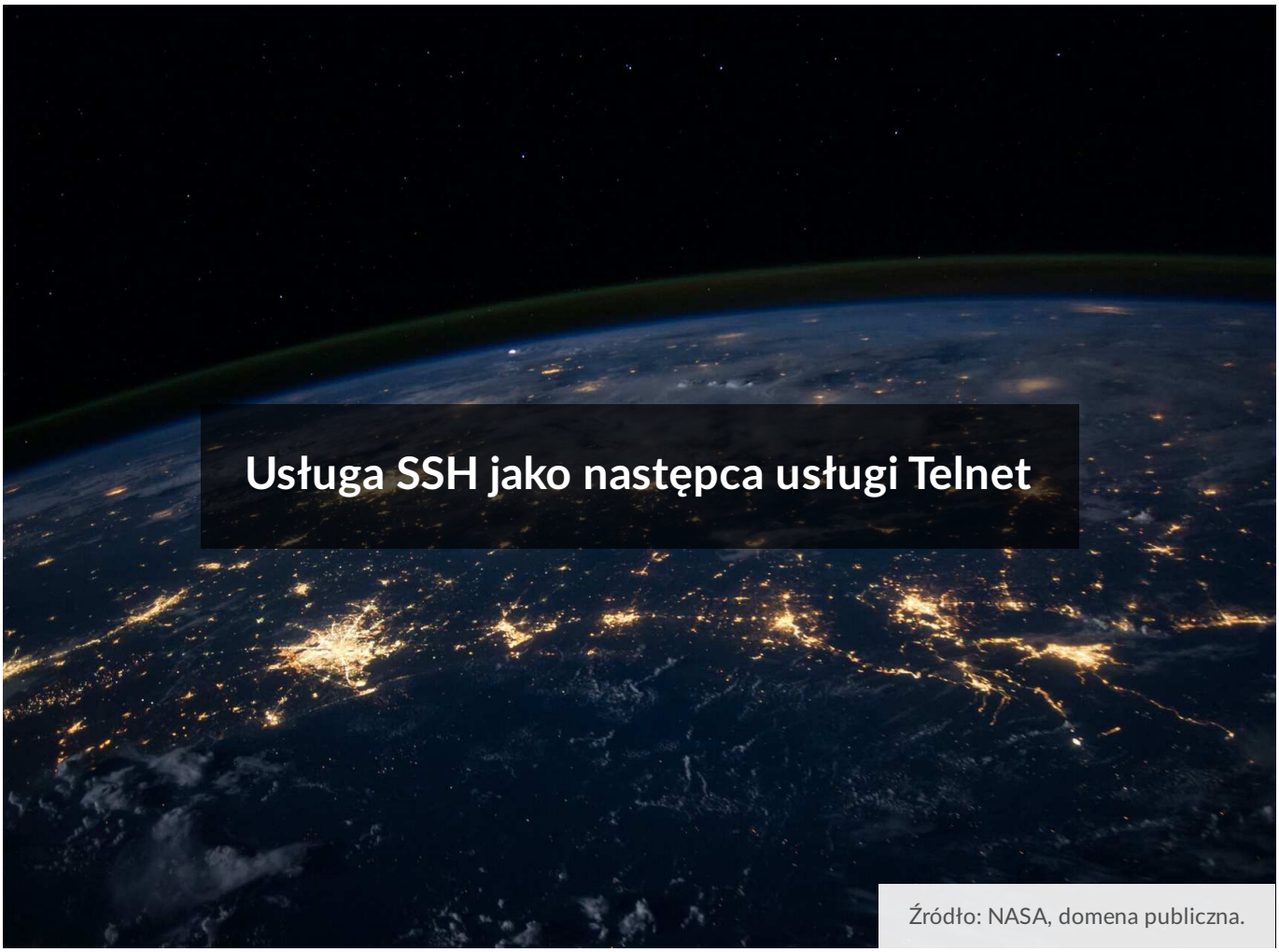
Usługa SSH jako następca usługi Telnet



Źródło: NASA, domena publiczna.

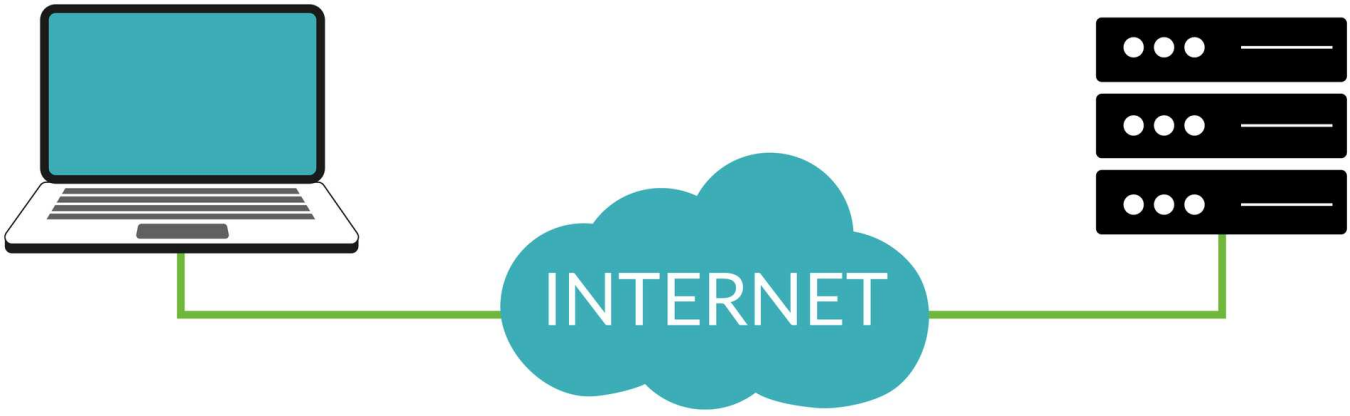
Korzystając z komputera czy innego urządzenia elektronicznego, przywykliśmy do stylowych i estetycznych pod względem graficznym interfejsów użytkownika. Jednak na długo przed pojawianiem się tego rodzaju interfejsów użytkownicy komputerów porozumiewali się z nimi za pomocą tekstowych terminali, wydając im polecenia wpisywane z klawiatury. Kiedy do gry wkroczyły sieci komputerowe, zastanawiano się, jak można połączyć ze sobą komputery znajdujące się w różnych lokalizacjach i zarządzać nimi tak, jakbyśmy znajdowali się bezpośrednio przy nich. Na bazie tych rozważań powstał jeden z pierwszych protokołów komunikacyjnych warstwy aplikacji, czyli Telnet, a później jego następca, czyli protokół SSH.

> **Twoje cele**
>
> - Scharakteryzujesz działanie połączenia terminalowego.
> - Przeanalizujesz dwa protokoły realizujące połączenia terminalowe.
> - Wskażesz różnice pomiędzy protokołem Telent a protokołem SSH.

Przeczytaj

Protokoły komunikacyjne warstwy aplikacji, takie jak HTTP, HTTPS czy FTP, są powszechnie znane i najczęściej wykorzystywane przez użytkowników sieci komputerowych. Istnieją również działające w tej warstwie protokoły, które nie są tak popularne, ale równie często stosowane. Zaliczamy do nich protokoły zdalnego połączenia terminalowego, a mianowicie **TELNET** i **SSH**.

> **Ciekawostka**
>
> Załóżmy, że jesteśmy administratorami sieci komputerowej. Nasza sieć jest bardzo duża, a biura znajdują się w kilku różnych lokalizacjach. Powstaje pytanie: jak administrować taką siecią, w której urządzenia, takie jak rutery, przełączniki sieciowe, a przede wszystkim obsługujące ją serwery, są od nas oddalone o wiele kilometrów? W tej sytuacji mamy dwa wyjścia: możemy za każdym razem, kiedy zaistnieje potrzeba zmiany konfiguracji, jechać do biura, w którym akurat znajduje się serwer wymagający takich zmian, lub też połączyć się z nim zdalnie, nie wychodząc zza biurka. Oczywiście pierwsza opcja nie jest optymalna - musimy przecież dojechać do biura, a to strata czasu i pieniędzy. Wybieramy zatem drugą opcję, czyli połączenie zdalne.



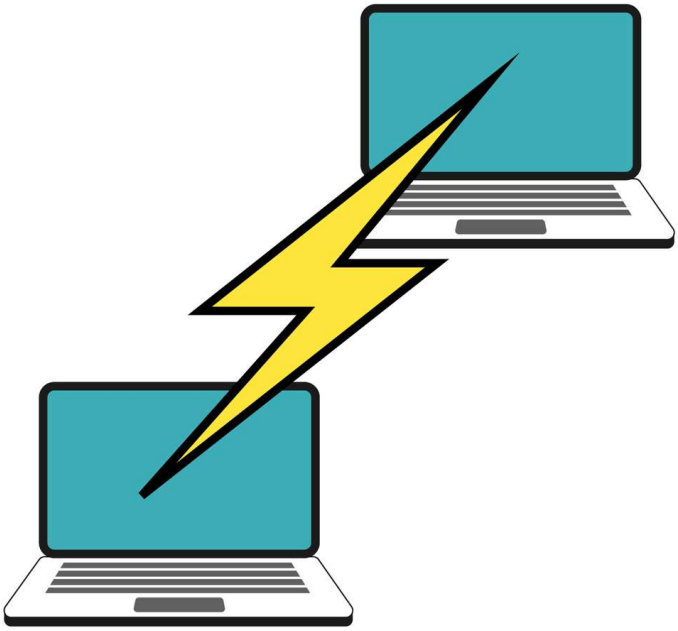
Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

> **Ważne!**
>
> Zdalne połączenie pozwala administratorom sieci na łączenie się ze wszystkimi urządzeniami sieciowymi oraz serwerami, które mają taką usługę uruchomioną.
> W trakcie połączenia zdalnego możemy konfigurować urządzenia i serwery tak, jakbyśmy pracowali bezpośrednio z nimi.

Takie rozwiązanie bardzo ułatwia pracę administratorom, gdyż często zdarza się, że odpowiadają oni za prawidłową pracę urządzeń znajdujących się w lokalizacjach oddalonych od siebie o dziesiątki, setki, a nawet tysiące kilometrów. A zatem bez możliwości fizycznego do nich dostępu.

Jednym z pierwszych protokołów warstwy aplikacji, jaki w ogóle powstał, był właśnie protokół zdalnego połączenia, czyli **Telnet**. Telnet to zarówno nazwa protokołu komunikacyjnego działającego w architekturze klient-serwer, jak i usługi systemu operacyjnego umożliwiające takie połączenie.

Podobnie jak w przypadku usługi FTP, również tutaj obsługa połączenia TELNET może realizować zewnętrzne oprogramowanie, np. **PUTTY**.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

> **Ważne!**
>
> Protokół TELNET ma jednak wadę, która spowodowała, że obecnie praktycznie przestał być używany i rekomenduje się jego wyłączenie na wszystkich urządzeniach, które do tej pory go stosowały.

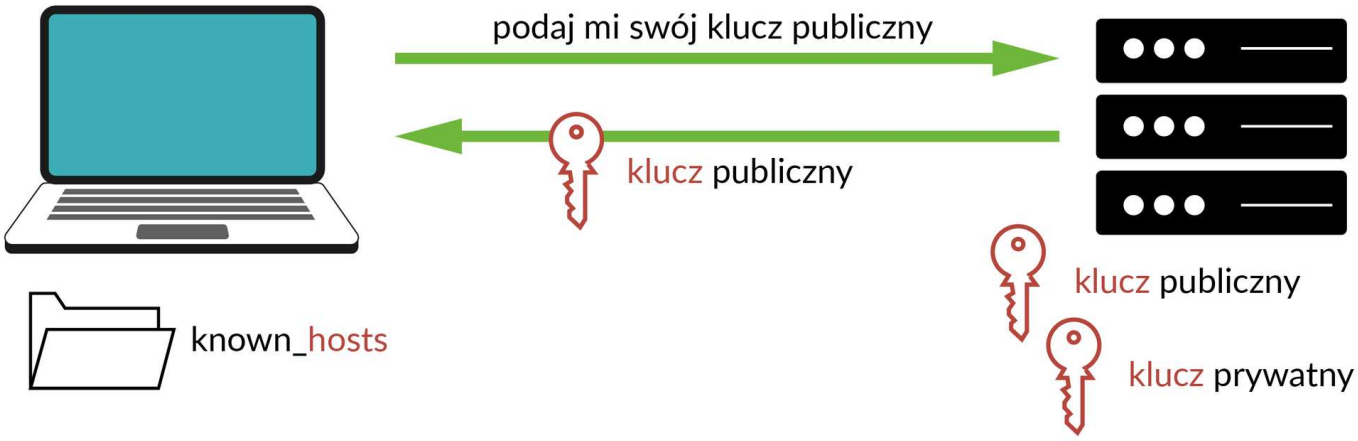
Niestety **TELNET nie oferuje szyfrowania komunikacji.** Wszelkie polecenia, a nawet loginy i hasła w sesji TELNET przesyłane są pomiędzy klientem a serwerem poprzez tekst jawny. Stanowi to ogromne zagrożenie - jeśli bowiem ktoś „podsłucha" taką komunikację, uzyska dostęp do wszystkich danych i poleceń, które administrator przesyła do serwera, czy urządzenia sieciowego.

Szyfrowany TELNET, czyli SSH

Następcą protokołu TELNET oferującym szyfrowanie komunikacji jest protokół zdalnego połączenia **SSH** (ang. *Secure Shell*). Szyfrowanie danych odbywa się najczęściej z wykorzystaniem metod AES.

Podczas instalacji usługi SSH na serwerze czy też na urządzeniu sieciowym tworzona jest para kluczy – **klucz publiczny i klucz prywatny** usługi SSH. Służą one do szyfrowania i deszyfrowania komunikacji z klientem.

Podczas pierwszego połączenia z serwerem SSH **klient zapisuje klucz publiczny** tego serwera na swoim dysku, w pliku `known_hosts`.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Następnie klient tworzy tzw. **klucz sesji**, który będzie stosowany do **szyfrowania całej komunikacji**. Klucz sesji zostaje zaszyfrowany kluczem publicznym otrzymanym wcześniej od serwera i jest do niego odsyłany. Od tego momentu cała komunikacja szyfrowana jest **kluczem sesji**.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Etap praktyczny nawiązywania sesji ze zdalnym serwerem Linux poprzez protokół **SSH** z wykorzystaniem programu **PUTTY** zademonstrowany został w poniższym filmie:

Film dostępny pod adresem /preview/resource/R1OebC92cEApT

Lekcja o sposobie nawiązania zdalnego połączenia z systemem Linux przez serwer SSH.

Słownik

> **AES**
>
> (ang. *Advanced Encryption Standard*) standard kryptograficzny wykorzystujący symetryczny szyfr blokowy

Prezentacja multimedialna

Polecenie 1

Zapoznaj się z prezentacją i wykonaj ćwiczenia.

Krótka historia internetu

1

Logo ARPA
Źródło: HistoryofInformation.com, domena publiczna.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1958
Powołanie ARPA (Advanced Research Projects Agency) - jej zadaniem było opracowywanie nowych technologii teleinformatycznych i adaptowanie ich do celów militarnych).

2

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1962
Paul Baran z firmy Rand Corporation wpada na pomysł sieci komputerowej opartej na wymianie

pakietów.

3

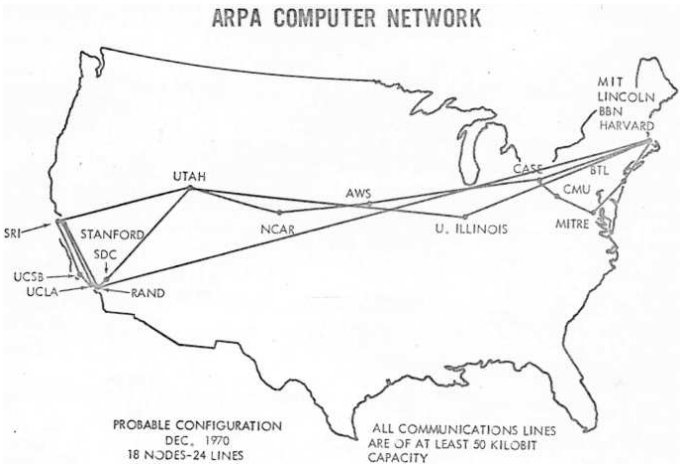
Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1967

Uruchomienie pierwszego węzła sieci na uniwersytecie w Los Angeles. Wtedy odbyło się pierwsze zdalne logowanie. Grupa ludzi skupiona przy odległym terminalu wpisywała kolejne litery, a druga grupa obserwowała monitor dołączony do hosta. To, czy wciskane klawisze odpowiadały znakom pojawiającym się na monitorze, potwierdzano telefonicznie.

4



Mapa ARPANET-u w grudniu 1970 r.

Źródło: UCLA and BBN, commons.wikimedia.org, CC BY-SA 4.0.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1969

Do sieci dołączono trzy kolejne węzły – jeden w stanie Utah i dwa w Kalifornii. Sieć przyjmuje oficjalną nazwę ARPANET (komputery miały 12

KB pamięci operacyjnej. Osiągnięto szybkość transferu 50 kbps).

5

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1971

Wprowadzenie systemu poczty elektronicznej i opracowanie protokołów FTP i Telnet. W sieci pracują już 23 serwery. Larry Roberts przeprowadza publiczną demonstrację sieci.

6

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1973

Pierwsze międzynarodowe połączenie Anglia – Norwegia.

7

Vint Cerf, 2007 r.

Źródło: Joi Ito, flickr.com, CC BY 2.0.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1974

Bob Khan i Vinton Cerf z ARPA podają szczegóły projektu nowego protokołu sieciowego TCP/IP.

Po raz pierwszy pojawia się słowo Internet, w opracowaniu badawczym dotyczącym protokołu TCP, napisanym przez Vintona Cerfa. W uznaniu za tę i inne zasługi Cerf znany jest jako „ojciec Internetu".

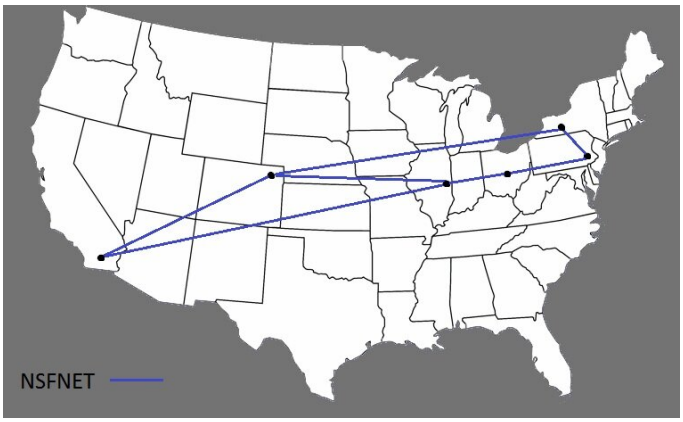
8

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1980

Sieć osiąga liczbę ~400 serwerów i ok. 10 tys. użytkowników.



9

Zasięg NSFNET-u w 1986 r.
Źródło: fandao1500, commons.wikimedia.org, CC0.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1984

Do rozwoju Internetu włącza się National Science Foundation, tworząc NSFNET – sieć coraz szybszych superkomputerów wykorzystywanych do celów naukowych.

Na potrzeby Internetu opracowano hierarchiczny system unikatowych nazw domenowych i protokołów DNS (*Domain Name System*). Od tej pory każda domena adresowa musi być zarejestrowana na jednym z tzw. *name serwers* (serwerów nazw).

10

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1985

William Gibson wydaje powieść s.f. „Neuromancer", w której po raz pierwszy pada słowo „cyberprzestrzeń". Od tej pory wszelkie wyrazy z przedrostkiem „cyber" robią szybką karierę. Powstaje też wtedy pierwsza domena komercyjna (adres zakończony na .com). Założyła ją firma Symbolics, producent sprzętu i oprogramowania. Swoją działalność rozpoczyna też America OnLine (AOL), obecnie największy komercyjny usługodawca internetowy na świecie.

11

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1989

Liczba serwerów w Internecie przekracza 100 000. Ilość hostów jest tak duża, że poważnym

problemem staje się znalezienie zadanych informacji. Remedium na to staje się pierwszy katalog zasobów sieciowych ARCHIE – program przeglądał znane serwery FTP i tworzył indeks ich zawartości z możliwością wyszukiwania plików.

12

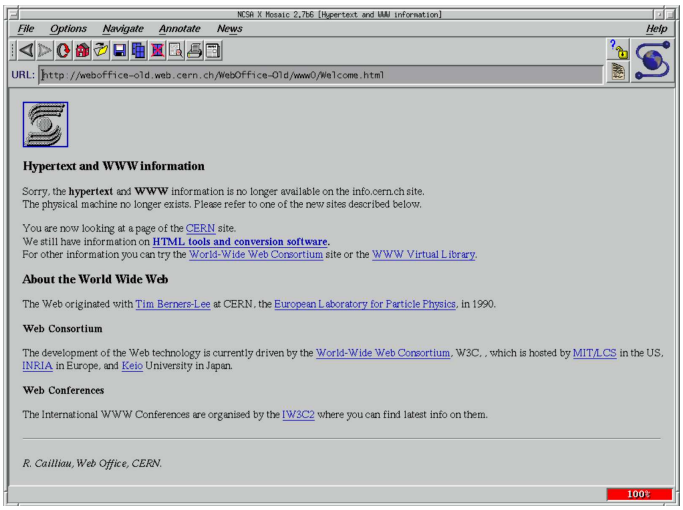
Tim Berners-Lee, 2014 r.
Źródło: Paul Clarke, commons.wikimedia.org, CC BY-SA 4.0.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1990

Tim Berners-Lee wpada na pomysł powiązania ze sobą dokumentów znajdujących się na serwerach WWW przy pomocy łączy hipertekstowych, co umożliwiło połączenie tekstu, grafiki oraz dźwięku. W 1991 roku stworzył on pierwszą przeglądarkę tekstową do WWW.



Zrzut ekranu strony otwartej w przeglądarce Mosaic

Źródło: Programm: National Center for Supercomputing Applications, pl.wikipedia.org, domena publiczna.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1994

Marc Andreessen wraz z zespołem NCSA (*National Center for Supercomputing Applications*) tworzą Mosaic – pierwszą przeglądarkę graficzną do odczytywania stron WWW. W sieci pojawia się strona internetowa Białego Domu. Rozpoczyna się wielka kariera stron internetowych – serwerów WWW jest już pięć razy więcej niż rok wcześniej. Pierwsza międzynarodowa konferencja poświęcona WWW („Woodstock of the Web") odbyła się w 1994 roku w instytucie CERN i zainteresowała ponad 600 potencjalnych uczestników, jednakże tylko 400 osób mogło wziąć w niej udział. Od tego samego roku można przez Internet słuchać radia oraz zamówić pizzę z Pizza Hut, w sieci pojawia się także pierwszy bank.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

1995

Powstaje projekt pierwszej wersji protokołu. Celem SSH było zastąpienie wcześniejszych protokołów rlogin, Telnet, FTP i rsh, które nie zapewniały silnego uwierzytelnienia ani gwarancji poufności.

Materiał audio dostępny pod adresem:

https://zpe.gov.pl/b/P5T0gGnGU

15

2006

Druga wersja protokołu SSH zostaje przyjęta jako standard.

Oprac. na podst.: *INTERNET - HISTORIA, WIEDZA PODSTAWOWA*, miroslawzelent.pl, dostęp 17.05.2021 r.

Ćwiczenie 1

Wyjśnij, z jakiego powodu powstał protokół SSH.

Ćwiczenie 2

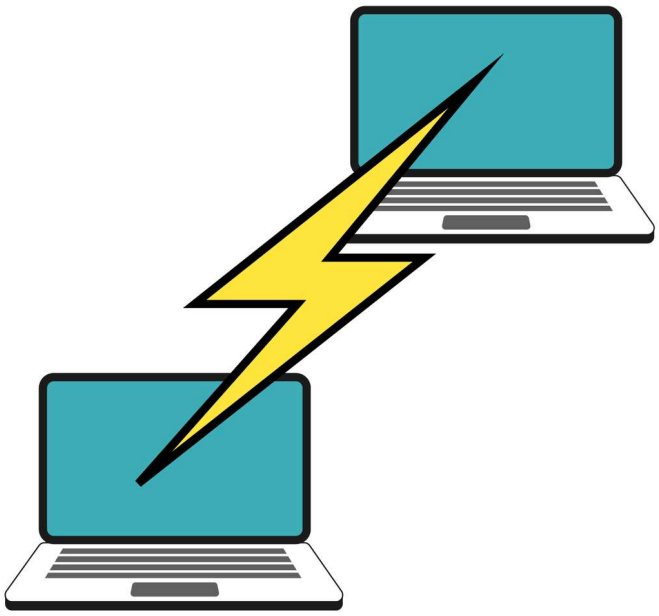
Porównaj ze sobą protokoły Telnet oraz SSH.

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Rysunek przedstawia ikonę programu do zdalnego połączenia. Wskaż, jaka jest nazwa tego programu.



- WinSCP
- HyperTerminal
- PUTTY
- CoreFTP

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Ćwiczenie 2

Wskaż, do czego używa się protokołów zdalnego połączenia. Zaznacz wszystkie poprawne odpowiedzi.

- [ ] tworzenie zasobów i plików na zdalnym serwerze
- [ ] konfiguracja urządzeń sieciowych
- [ ] wysyłanie poczty elektronicznej
- [ ] żądanie stron WWW
- [ ] zamiana nazw mnemonicznych na adresy IP
- [ ] zarządzanie serwerami

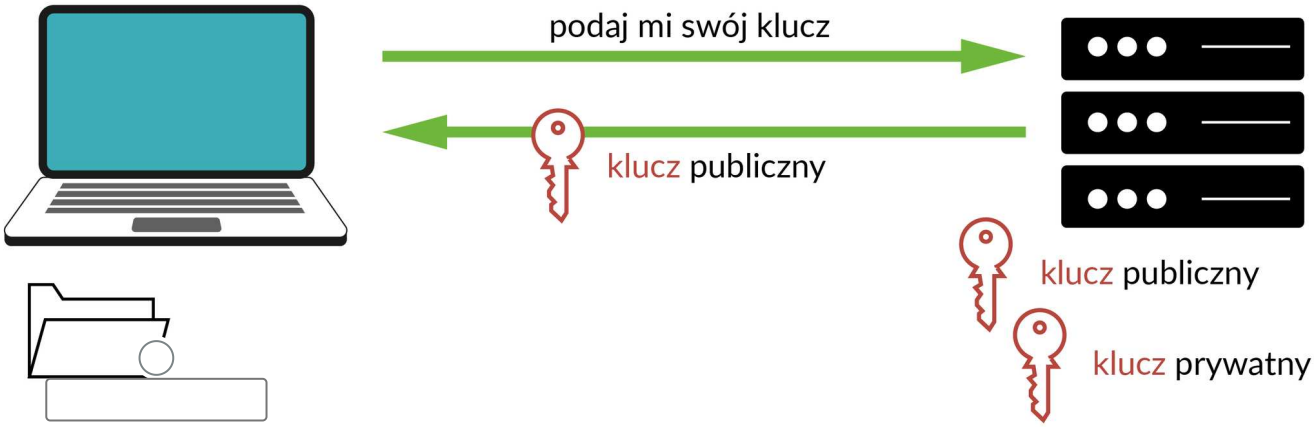
Ćwiczenie 3

Wskaż, jakim kluczem szyfrowana jest komunikacja klienta z serwerem podczas połączenia SSH.

- ◯ kluczem `known_hosts`
- ◯ kluczem sesji
- ◯ kluczem prywatnym serwera
- ◯ kluczem publicznym serwera

Ćwiczenie 4

Uzupełnij grafikę, wskazując poprawną nazwę pliku, w którym klient przechowuje publiczne klucze serwerów SSH.



known_ssh_public_key | known_host | known_ssh_host | known_servers

Ćwiczenie 5

Pogrupuj odpowiednio stwierdzenia dotyczące protokołów TELNET oraz SSH.

TELNET

SSH

- działa na porcie 23
- szyfruje komunikację
- działa na porcie 22
- wymaga kluczy prywatnych i publicznych do poprawnej komunikacji
- nie szyfruje komunikacji
- obecnie rzadko stosowany
- jeden z pierwszych protokołów warstwy aplikacji

Ćwiczenie 6

Wskaż wszystkie typy kluczy tworzone podczas instalacji usługi SSH na serwerze lub urządzeniu sieciowym.

- [ ] sesji
- [ ] zmienny
- [ ] prywatny
- [ ] szyfrujący
- [ ] publiczny

Ćwiczenie 7

Uzupełnij zdanie właściwymi elementami.

Aby ustanowić [ ] sesję z serwerem poprzez [ ] wymagany jest adres [ ] lub [ ], numer [ ] aplikacji, a także [ ] i hasło [ ] serwera.

identyfikacyjny | IP | MAC | lokalną | użytkownika | portu | SSH | zdalną | nazwa domenowa | administratora | login

Ćwiczenie 8

Wskaż, na jakich portach nie działają usługi SSH i TELNET.

- [ ] 21 i 22
- [ ] 22 i 23
- [ ] 23 i 24
- [ ] 20 i 21

Dla nauczyciela

Autor: Damian Stelmach
Przedmiot: Informatyka

Temat: Usługa SSH jako następca usługi Telnet

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres rozszerzony

Podstawa programowa:

Cele kształcenia – wymagania ogólne

> III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

Treści nauczania – wymagania szczegółowe

> III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.
>
> Zakres podstawowy. Uczeń:
>
> > 4) charakteryzuje sieć internet, jej ogólną budowę i usługi, opisuje podstawowe topologie sieci komputerowej, przedstawia i porównuje zasady działania i funkcjonowania sieci komputerowej typu klient-serwer, peer-to-peer, opisuje sposoby identyfikowania komputerów w sieci.
>
> Zakres rozszerzony. Uczeń spełnia wymagania określone dla zakresu podstawowego, a ponadto:
>
> > 3) opisuje warstwowy model sieci komputerowej oraz model sieci internet, opisuje podstawowe funkcje urządzeń i protokoły stosowane w przepływie informacji i w zarządzaniu siecią;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Scharakteryzujesz działanie połączenia terminalowego.
- Przeanalizujesz dwa protokoły realizujące połączenia terminalowe.
- Wskażesz różnice pomiędzy protokołem Telent a protokołem SSH.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- ćwiczenia praktyczne.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Usługa SSH jako następca usługi Telnet". Uczniowie zapoznają się z treściami w sekcji „Przeczytaj".
2. Chętny lub wybrany uczeń przygotowuje rozwiązanie polecenia nr 1 z sekcji „Prezentacja multimedialna". Będzie pełnił rolę eksperta podczas zajęć.

Faza wstępna:

1. Nauczyciel wyświetla i odczytuje temat lekcji oraz cele zajęć. Prosi uczniów o sformułowanie kryteriów sukcesu.
2. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z multimedium**. Nauczyciel wyświetla zawartość sekcji „Prezentacja multimedialana". Uczniowie zapoznają się z prezentacją i wykonają ćwiczenie nr 1, po czym następuje dyskusja na temat porównania protokołu Telnet z innymi protokołami.
2. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-5 z sekcji „Sprawdź się". Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel ponownie wyświetla na tablicy temat lekcji zawarty w sekcji „Wprowadzenie" i inicjuje krótką rozmowę na temat zrealizowanych celów (czego uczniowie się nauczyli).

Praca domowa:

1. Uczniowie wykonują ćwiczenia 6-8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Uczniowie mogą wykorzystać multimedium w sekcji „Prezentacja multimedialna" do przygotowania się do lekcji powtórkowej.