Lekcja

Temat: Zapoznanie z programem nauczania i warunkiem zaliczenia

1. Rozkład materiału:
   1. Korzystanie z wybranych usług oferowanych przez sieciowe systemy operacyjne
   2. Sieciowy system operacyjny – Windows serwer
   3. Bezpieczeństwo danych
   4. Sieciowy system operacyjny – linux
   5. Administrowanie systemem linux
   6. Usługi sieciowe w systemie linux
   7. Sieciowy system operacyjny – Novell NetWare
2. Warunki zaliczenia – warunkiem zaliczenia sieci komputerowych jest:
   1. Posiadanie na bieżąco uzupełnianego zeszytu (data, temat, zagadnienia)
   2. Pozytywne oceny ze wszystkich sprawdzianów
3. 2 sprawdziany na semestr
4. Jest możliwość poprawy w ciągu 2 tygodni od oddania sprawdzianu
5. Pytania, odpowiedź usta, kartkówka wagi 3, po min. 1 w semestrze
6. Kartkówki są niezapowiedziane
7. Jest jedno nieprzygotowanie
8. Aktywność na lekcji: plusy i minusy – ocena wagi 3, trzykrotność to albo 5 albo 1

DZIAŁ 1 Sieciowe systemy operacyjne

Lekcja

Temat: Sieciowe systemy operacyjne

1. Typy sieci komputerowych:
   1. P2P – udostępnianie plików i drukarek w Windowsie
   2. Klient – serwer – praca pod domeną
2. Historia i rodzaje sieciowych systemów operacyjnych:
   1. Arpanet – koniec lat 70
   2. Podział na MILNET i Internet (nowy ARPANET) – 1983
   3. Lata 90 – początek sieciowych systemów operacyjnych
   4. Rodzaje SSO:
      1. W pełni serwerowy – z usługami w jądrze systemu
      2. Z uruchamianymi usługami
      3. Tylko dla urządzeń (iOS, routerOS)
3. Przykłady SSO:
   1. Windows NT / Windows 2000 / Windows serwer:
      1. NT 40 Server – 1996 – NT 40 Workstation:
         1. Po raz pierwszy pojawił się NTFS
   2. Windows 2000 Serwer – Windows 2000 Pro:
      1. Active directory
   3. Windows Server 2003 – Windows XP pro:
      1. SBS -small business serwer
   4. Windows server 2003 R2 – XPSP3 Pro
   5. Windows server 2008 – Vista:
      1. Role I funkcje
      2. Wersja core – domyślnie bez środowiska graficznego
      3. Zmniejszone jądro systemu
      4. Menadżer okien przeniesiony z jądra
      5. Power Shell
   6. Windows server 2008 r2 – windows 7
   7. Windows server 2012 – windows 8:
      1. Nie wspiera Intanium
      2. Miał 4 edycje
   8. Windows 2012 R2 – windows 8.1:
      1. Hyper-V
      2. Możliwość doinstalowania graficzny do core’a
      3. Rozszerzono Power Shell’a
      4. Współpraca z Office 365
   9. Windows server 2016 – Windows 10 Pro:
   10. UNIX /Linux (unix zgodny z posix a linux niekoniecznie):
       1. Red Hat Enterprise Linux – RHEL 7.5
       2. S.U.S.E. linux enterprice server (SLES):
          1. Połączyli się z Novell Netware
          2. Płaci się za subskrypcje
       3. Oracle Linux (Oracle enterprice linux):
          1. Oparta na RHEL – wersja 7.5
       4. Novell Netware:
          1. Pierwsze SSO
          2. Powstał system NDS (Netware/Novell Directory System) 🡪 eDirectory – działa podobnie do Active Directory
          3. NFS – Netware File System
          4. Ograniczone działanie
       5. MacOsXServer 🡪 OS X 🡪 macOS:
          1. Dedykowana maszyna serwerowa
          2. Tylko serwery plików obecnie
4. Zadania administratora sieci komputerowych:
   1. Zadania pielęgnacyjne:
      1. Kontrola zajętości zasobów:
         1. Czy miejsce na dysku się nie kończy\
         2. Czy nie za mało RAM-u
      2. Archiwizacja systemu plików:
         1. Tworzenie kopii zapasowej
      3. Kontrola atrybutów związanych z utrzymaniem bezpieczeństwa systemu:
         1. Kontrola uprawnień
      4. Podejmowanie działań dla utrzymania pożądanego poziomu bezpieczeństwa:
         1. Aktualizacje
         2. Zmiany haseł
         3. Zasady bezpieczeństwa
   2. Obsługa żądań użytkowników:
      1. Reset hasła
      2. Dodawanie/usuwanie użytkowników
      3. Wyłączanie kont użytkowników
      4. Ustalanie zezwoleń dla użytkowników
      5. Powiadamianie użytkowników o zmianach w systemie
      6. Przydzielanie adresów IP oraz współpraca użytkownika z siecią
   3. Zadania wynikające z potrzeb bieżących:
      1. Wyłączanie i włączanie maszyn
      2. Konfigurowanie usług na bieżąco
      3. Usuwanie awarii
   4. Usuwanie awarii:
      1. Sprzętowych
      2. Zdiagnozowanie poważniejszych awarii przed oddaniem do serwisu
      3. Rekonstrukcja systemu plików – odzyskiwanie utraconych danych
   5. Działania w ramach ochrony systemu:
      1. Zarządzanie hasłami – ustalanie polityki haseł (długość, składnia)
      2. Ochrona plików systemowych
      3. Ochrona przed złośliwym oprogramowaniem – firewall, antywirus
   6. Inne zadania:
      1. Współpraca z webmasterem – instalowanie np.. konkretnej wersji PHP
      2. Współpraca z działem bezpieczeństwa -VPN, kontrola przepływu w sieci
      3. Współudział w przetargach i zakupach urządzeń sieciowych
      4. Kontakt z firmami gwarancyjnymi
      5. Kontrola legalności zainstalowanych systemów operacyjnych i innego oprogramowania

Lekcja

Temat: Korzystanie z usług sieciowych

1. Pojęcie usług sieciowych:
   1. http: 80
   2. https: 443
   3. usługa sieciowa jest to mechanizm udostępniający proces serwera na konkretnym porcie
   4. 2^16 portów
   5. Do 1023 takie bardzo znane
   6. Porty bardzo wysokie
   7. Z punktu widzenia użytkownika sieć komputerowa umożliwia prawidłowe funkcjonowanie aplikacji sieciowych. Każda z aplikacji korzysta z protokołu wymiany danych z inną aplikacją sieciowa, zlokalizowaną po stronie zdalnej. Protokół aplikacji określa sposób wymiany informacji między procesami w odległych hostach, a w szczególności składnię wiadomości, scenariusze wymiany, wiadomości, sposób kodowania, szyfrowania (jeśli wymagane). Jeśli aplikacja nie korzysta z protokołu transportowego TCP konieczna jest także realizacja sterowania przepływem oraz zapewnienie niezawodności transmisji.
   8. Protokoły aplikacji można podzielić na dwie grupy:
      1. Protokoły standardowe, dobrze znane i zestandarozywane w dokumentach RFC
      2. Protokoły autorskie – zwykle implementowane przez jednego producenta który nie publikuje specyfikacji protokołu
2. Serwis stron www
3. Usługi transferu plików
4. Poczta elektroniczna
5. Pojęcie usług sieciowych
6. Serwis stron www
7. Usługi transferu plików
8. Poczta elektroniczna

Ad1

Ilość portów to 2^16

Usługa sieciowa jest to mechanizm udostępniający proces serwera na konkretnym porcie w sieci.

Z punktu widzenia użytkownika, sieć komputerowa umożliwia prawidłowe funkcjonowanie aplikacji sieciowych. Każda z aplikacji korzysta z protokołu wymiany danych z inną aplikacją sieciową, zlokalizowaną po stronie zdalnej. Protokół aplikacji określa sposób wymiany informacji między procesami w odległych hostach, a w szczególności: składnię wiadomości, scenariusze wymiany wiadomości, sposób kodowania, szyfrowania (jeśli wymagane). Jeśli aplikacja nie korzysta z protokołu transportowego TCP, konieczna jest także realizacja sterowania przepływem oraz zapewnienie niezawodności transmisji.

Protokoły aplikacji można podzielić na:

* Protokoły standardowe, dobrze znane i zestandaryzowane w RFC (Request For Comments)
* Protokoły autorskie, zwykle implementowane przez jednego producenta, który nie publikuje specyfikacji protokołu

Ad2

Serwis stron www – obsługuje protokół HTTP na porcie 80 oraz HTTPS na 443. Jest to program działający na serwerze obsługujący żądania protokołu aplikacji HTTP i HTTPS. Z serwerem łączy się klient (przeglądarka) aby pobrać wskazaną stronę www. Może korzystać z usług innego równolegle działającego oprogramowania udostępniając wynikowe, dynamicznie utworzone strony www często wzbogacone danymi z baz danych.

Serwer WWW - program działający na serwerze, obsługujący żądania protokołu aplikacji HTTP i HTTPS. Z serwerem WWW łączy się, poprzez się, poprzez sieć komputerową, przeglądarka internetowa będąca jego klientem, aby pobrać wskazaną stronę WWW. Protokół http działa domyślnie na porcie 80, a https na porcie 443. Serwer WWW może też korzystać z usług innego, równolegle działającego oprogramowania(np. PHP, ASP itp.), udostępniając wynikowe, dynamiczne utworzone strony WWW często wzbogacone danymi z bazy danych.

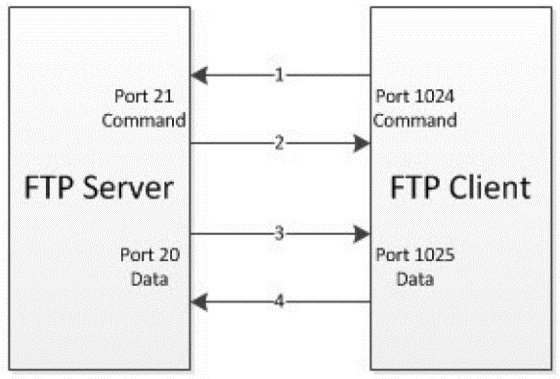
Serwer może pracować w 3 trybach:

* wysyłanie czystych plików HTML, które po przetworzeniu pobierają niezbędne pliki wskazane w pliku indeksującym
* przetwarzanie skryptów po stronie serwera, plik nie jest od razu wysyłany do klienta, tylko jest kompilowany na serwerze i dopiero wysyłany do klienta
* przetwarzane skrypty komunikujące się z serwerem baz danych - CMS - Content Management system

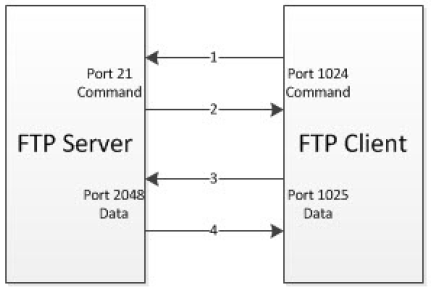
Ad3

Protokół FTP (file transfer protocol) przeznaczony jest do transferu plików miedzy hostami. Jest dość nietypowy, ponieważ używa dwóch dwukierunkowych połączeń TCP do poprawnej realizacji zadania. Połączenie sterujące (control) zawiązywane jest z serwerem FTP na porcie 21, natomiast połączenie do transmisji danych użytkownika (data) używa portu zależnego od trybu pracy.

W trybie aktywnym host klienta losuje numer lokalnego, wolnego portu N (z puli tzw. portów wysokich, czyli powyżej 1024).



Pasywny tryb FTP polega na zmianie kierunku komunikacyjnego. Połączenia są otwierane przez klienta. Pierwsze między wysokim a portem 21 serwera. Następnie klient wysyła.



serwer otwiera port Y zamiast portu 20 i to serwer czeka na inicjacje ze strony klienta do przesyłania plików. strzałki data są na odwrót i zamiast :20 jest :Y (port wysoki).

w sumie oba polaczenia są inicjowane przez klienta.

SFTP – protokół SFTP nie wymaga obecności serwera FTP, a przesyłane dane są szyfrowane z wykorzystaniem klucza szyfrującego. Domyślny port to 22 (jak w SSH). Przesyłając plik przy użyciu protokołu FTP uzyskujemy dobre przepływności ale nie zyskujemy bezpieczeństwa – nasze hasła i dane nie są szyfrowane podczas przesyłania co potencjalnie stwarza zagrożenie ich kradzieży

SCP jest to rozwiązanie wysyłające tylko pliki przy wykorzystaniu SSH (port 22)

FTPS – protokół, który jest rozszerzeniem protokoły FTP wykorzystującym SSL/TLS. FTPS używa portu 990 TCP dla kontroli przepływu oraz 989 TCP dla transferu danych (RFC 2228 i 4217). FTPS nie powinien być mylony z protokołem SFTP.

RCP – port 469 wysyła w postaci niezaszyfrowanej i został zastąpiony przez SCP – stosowany w systemach UNIX

FISH – wykorzystuje SSH (port 22) lub Remote Shell (RSH – port 514) do transferu i zarządzania plików oraz folderów

TFP (trivial file transfer protocol) – port 69 i działa na protokole UDP; używany do ściągania firmwarów do urządzeń sieciowych

Ad4 – poczta elektroniczna

Poczta elektroniczna – najbardziej popularna usługa sieciowa zrewolucjonizowała komunikację między ludźmi dzięki swojej prostocie i szybkości. Do poprawnego działania poczty elektronicznej na komputerze lub innym urządzeniu końcowym (PDA, telefon komórkowy, konsola) wymagane jest kilka aplikacji i usług

Protokoły warstwy aplikacji:

* do dostarczania poczty:
  + pop (post office protocol)
  + IMAP (Internet messafe access protocol)
* Do wysyłania poczty:
  + SMTP (Simple mail transfer protocol)

|  |  |  |
| --- | --- | --- |
| Protokół | Porty bez SSL | Porty z SSL |
| SMTP | 587, 25 (zdeprecjonowany) | 465 (SMTPS) |
| POP3 | 110 | 995 (POP3S) |
| IMAP | 143 | 993 (IMAPS) |

Rekordy DNS dla maila – MX

Serwer:

* A.pl:
  + A:
    - Inbox
    - Outbox
    - Sentbox
    - Draftbox
    - Trashbox
    - \*\*spambox (opcjonalny)

MTA – (mail transfer agent) – ściśle związany z SMTP, sprawdza czy w outboxie są maile do wysłania

MDA (mail deliver agent) – może skanować w poszukiwaniu wirusów,

MUA (mail user agent)

POP3 – protokół odpowiedzialny za przechowywanie poczty offline, umożliwia pobranie wszystkich wiadomości i używania tych wiadomości offline. Pobieramy i rozłączmy się i usuwa wiadomości z serwera (ale w opcjach można pozostawić wiadomości na serwerze). Wszytkie wiadomości są pobierane w całości,

IMAP – pobiera tylko nagłówki (część wiadomości) po kliknięciu jest wiadomość dopobierana. Przeczytana na jednym urządzeniu pokazuje że jest przeczytana na drugim urządzeniu. Działanie w czasie rzeczywistym – usunięcie wiadomości to usunięcie na serwerze. Potrafi tworzyć katalogi inne niż standardowe.

IMAP do zarządzania w czasie rzeczywistym, a POP3 offline.

Zadanie domowe – podejrzenie wiadomości po nagłówkach