

# Vzdálená konfigurace (TELNET, SSH) a souborové služby (FTP, TFTP, NFS)

Prezentace se zaměřuje na různé protokoly aplikační vrstvy TCP/IP modelu, které podporují komunikaci a sdílení dat v počítačových sítích. Podrobně rozebíráme protokoly jako TELNET, FTP, TFTP, NFS a RPC, jejich funkce, vlastnosti a možnosti využití. Výklad zahrnuje výhody a nevýhody každého protokolu a ukazuje jejich konkrétní použití v různých síťových aplikacích. Důraz je kladen na autentizaci, bezpečnost a efektivitu každého protokolu.

# Aplikační vrstva TCP/IP

## Charakteristika aplikační vrstvy

- Nejvyšší vrstva TCP/IP, poskytuje uživatelsky orientované služby, zajišťuje přístup k síťovým zdrojům.
- Umožňuje komunikaci a sdílení dat mezi aplikacemi na různých systémech.

## Role aplikačních protokolů

- Protokoly umožňují přístup k souborům, sdílení zdrojů, vzdálený přístup a další síťové služby.

# TELNET - Vzdálený terminál

## Účel a funkce TELNET

- Protokol pro vzdálený přístup, emuluje přímé připojení k terminálu vzdáleného počítače.
- Poskytuje prostředí virtuálního terminálu (NVT) - jednotné rozhraní pro přístup.

## Bezpečnostní rizika

- Data, včetně uživatelského jména a hesla, jsou přenášena v otevřeném formátu.

## Port a standard

- Používá TCP port 23, standardizováno v RFC 854 a následujících.

# Implementace TELNET - Klient a server

## TELNET klient

- Poskytuje rozhraní pro uživatele, který se připojuje k vzdálenému systému, přenáší vstupy z klávesnice.

## TELNET server

- Přijímá data od klienta a odesílá odpovědi zpět, simuluje práci přímo na vzdáleném zařízení.

# Základní vlastnosti TELNET

## Síťový virtuální terminál (NVT)

- Umožňuje jednotnou komunikaci bez ohledu na typ systému.

## Možnost vyjednávání režimů

- Klient a server si mohou vyjednat specifické režimy, jako je počet bitů na znak.

## Symetrické spojení

- TELNET nerozlišuje mezi terminály a procesy, což umožňuje jakékoliv aplikaci stát se klientem.

# FTP - File Transfer Protocol

## Účel FTP

- Přenos souborů mezi klientem a serverem v rámci sítě.

## Řídicí a datové spojení

- Používá dva kanály (port 21 pro řídicí spojení a port 20 pro datové spojení).

## Režimy přenosu

- ASCII pro textové soubory, BINARY pro ostatní typy souborů (např. binární, obrazové).

# Režimy FTP - Aktivní a Pasivní

## Aktivní režim

- Server otevírá datové spojení na portu 20, může způsobovat problémy s firewally.

## Pasivní režim (PASV)

- Klient otevírá jak řídicí, tak datové spojení, což je vhodné pro procházení firewally.

# Komunikace přes FTP

## Přístup k FTP serveru

- Uživatelé se přihlašují pomocí uživatelského jména a hesla.

## Základní příkazy FTP

- Například `open`, `get`, `put`, `mget`, `mput`.

## Anonymní FTP

- Přístup bez hesla pro volně dostupné soubory, často s použitím uživatelského jména „anonymous”.



# TFTP - Trivial File Transfer Protocol

## Charakteristika TFTP

- Jednoduchý protokol pro přenos souborů, využívá UDP, nevyžaduje autentizaci.

## Omezení a použití TFTP

- Nespolehlivý přenos, vhodný pro jednoduché přenosy a inicializaci zařízení.

## Port a standard

- Používá UDP port 69, specifikováno v RFC 1350.

# NFS - Network File System

## Účel NFS

- Umožňuje transparentní přístup k souborům na vzdálených systémech.

## Klient-server architektura

- Server poskytuje souborový systém pro sdílení, klient jej používá, jako by byl lokální.

## Bezpečnost a řízení přístupu

- Historicky omezená bezpečnost, novější verze NFS 4 (RFC 3530) podporuje zabezpečení a uzamykání souborů.

# RPC - Remote Procedure Call

## Úloha RPC

- Umožňuje volání vzdálených procedur mezi různými systémy.

## Práce s UDP a TCP

- Může běžet nad oběma protokoly, zajišťuje spolehlivost při použití UDP.

## Portmapper a autentizace

- Portmapper zajišťuje přístup k RPC službám, možnost autentizace pomocí DES nebo Kerberos.

# XDR - External Data Representation

## Charakteristika XDR

- Definuje formát nezávislý na platformě, umožňuje kompatibilitu mezi systémy.

## Použití XDR v NFS a RPC

- Podporuje formátování dat v NFS a RPC pro přenos po síti.

# Výhody a nevýhody aplikačních protokolů

## Výhody

- Široká škála služeb a aplikací, efektivní správa a sdílení dat.

## Nevýhody

- Některé protokoly (TELNET, FTP) mají nízké zabezpečení, přenáší data v otevřené podobě.

# Souhrn vlastností aplikačních protokolů

## Přehled protokolů

- TELNET, FTP, TFTP, NFS, RPC, XDR – každý nabízí specifickou funkcionalitu pro různé potřeby.

## Podpora bezpečnosti

- Moderní implementace mohou přidat šifrování nebo podporu protokolů SSL/TLS.

# Shrnutí

## Hlavní funkce aplikační vrstvy TCP/IP

- Podporuje komunikaci mezi aplikacemi a sdílení zdrojů v síťovém prostředí.

## Specifika jednotlivých protokolů

- Každý protokol je optimalizován pro různé účely – přenos dat, vzdálený přístup, sdílení souborů.

# Kontrolní otázky

1. Jaké jsou hlavní rozdíly mezi TELNET a SSH?
2. Jak funguje pasivní režim v FTP?
3. Jaký je hlavní účel XDR v RPC?
4. Proč je NFS výhodné pro sdílení souborů v LAN?
5. Jaké jsou bezpečnostní slabiny protokolu TELNET?



# Doporučená literatura

1. **RFC 854** – Telnet Protocol Specification.
2. **RFC 959** – File Transfer Protocol (FTP).
3. **RFC 1350** – The TFTP Protocol (Revision 2).
4. **Computer Networks** – Andrew S. Tanenbaum: Základy síťových protokolů.
5. **TCP/IP Illustrated, Volume 1** – W. Richard Stevens: Praktický průvodce TCP/IP.