Servidores Web e Protocolos de Computação Remota

Módulo/Unidade 0840 Servidores web

João Silva (Autoria do Manual)

Curso Técnico/a de Informática Instalação e Gestão de Redes (Duração 2045 Horas)

Carga Horária: 50 Horas | Pontos de Crédito: 4.5

Objetivos da Unidade 0840

- Aprender o que são servidores web, como funcionam e seus tipos (estáticos e dinâmicos).
- **Instalar e configurar o servidor Web**.
- Fornecer conhecimentos para utilizar os **principais protocolos e serviços de computação remota** de forma eficiente e segura.

1. TELNET, RLOGIN, SSH e FTP.
2. Servidor Web - computação remota, TALK e NFS.

Destinatários e Pré-requisitos

- **Destinatários**: Formandos de **nível médio** que desejam ampliar seus conhecimentos sobre servidores web e suas funcionalidades.
- **Pré-requisitos Técnicos**:
  - Ter um **Virtualbox com Ubuntu** instalado e configurado.
  - Ter acesso à Internet e a um navegador web.
  - Saber usar o **terminal do Ubuntu** e os comandos básicos de linux.
- O manual não requer conhecimentos prévios sobre servidores web.

Protocolos Legados: TELNET e RLOGIN

- **Login Remoto**: Permite aceder ao sistema ou servidor à distância, como se estivesse localmente.
- **TELNET** (Teletype Network):
  - Protocolo de acesso remoto (cliente Telnet) para interagir via terminal virtual.
  - **INSEGURO**: Transmite todas as informações (incluindo senhas e comandos) em **texto simples**.
  - **Recomendação**: Evitar o uso em ambientes de produção e desabilitá-lo.
- **RLOGIN** (Remote Login):
  - Semelhante ao Telnet, também **não é seguro** (dados em texto simples).
  - **Diferença**: Permite armazenar credenciais num arquivo `rhosts` local.
  - **Desabilitação**: Altere a linha "disable = no" para "disable = yes" no arquivo de configuração (`/etc/xinetd.d/rlogin`).

SSH: O Padrão de Segurança

- **Conceito**: Protocolo que permite conexão a um servidor remoto pela internet, de maneira **segura e criptografada**.
- **Portas**: Usa a porta **TCP 22** por padrão (Telnet usa 23, RLOGIN usa 513).
- **Logon Remoto**: Requer um **par de chaves SSH** (privada, protegida por senha, e pública, copiada para o servidor no arquivo `~/.ssh/authorized_keys`).
- **Comando**: `ssh utilizador@endereco_ip`.
- **Vantagem**: Usa criptografia para proteger os dados enviados e recebidos, evitando a interceção e leitura em texto simples.

SCP: Cópia de Ficheiros Segura

- **SCP (Secure Copy)**: Utilitário para copiar ficheiros entre cliente e servidor remotamente de forma **segura**.
- **Sintaxe Geral**: `scp [opções] origem destino`
- **Opções Comuns**:
  - `-r`: Copiar **recursivamente** (necessário para diretórios).
  - `-P`: Especificar uma porta diferente da padrão (22).
  - `-i`: Especificar o arquivo de **chave privada SSH** para autenticação.
  - `user@host:/caminho`: Forma do caminho remoto.
- **Exemplo** (Local para Remoto):

```
scp relatorio.pdf
user@192.168.0.10:/home/user/documentos
```

Recursos Avançados e Segurança SSH

- **Execução de Programas Remotos**: Use `ssh user@servidor comando`.
- **Clientes X Localmente**: Use a opção `-X` para redirecionamento X11 de aplicativos gráficos remotos para a máquina local.
- **Túneis SSH**:
  - Encaminhamento de tráfego seguro (`-L` para local; `-R` para remoto).
- **Desabilitação do Acesso Root Remoto**:
  - **Prática Recomendada**: Desabilitar o acesso direto à conta `root` para reduzir riscos de ataques.
  - **Configuração**: No arquivo `/etc/ssh/sshd_config`, mude `PermitRootLogin` para **"no"**.

FTP: Protocolo e Insegurança

- **Definição**: Protocolo muito utilizado (desde 1970) para **transferência de ficheiros** entre cliente e servidor remoto via conexão TCP/IP.
- **Funcionalidade**: Permite enviar, baixar, editar e excluir ficheiros num servidor remoto.
- **Insegurança**: O FTP padrão **não é seguro**, pois as informações são transmitidas em **texto simples**.
- **Alternativas Seguras**:
  - **FTPS** (FTP com SSL/TLS).
  - **SFTP** (SSH File Transfer Protocol).
- **Modos de Conexão**:
  - **Ativo**: Servidor FTP cria a conexão de dados com o cliente.
  - **Passivo**: Cliente FTP cria a conexão de dados com o servidor.

Tipos de Acesso e Servidores FTP

- **Servidores Comuns**: Wu-FTPd (com arquivo de configuração `/etc/ftpaccess`) e **vsftpd** (Very Secure FTP Daemon).
- **FTP Público (Anonymous)**:
  - Não requer credenciais, usando o nome de utilizador **"anonymous"**.
  - Acede tipicamente ao **diretório** `pub`.
  - Configuração no `vsftpd.conf`: `anonymous_enable=YES`.
- **FTP de Utilizadores**:
  - Requer **autenticação** com conta e senha válida do sistema operacional ou contas virtuais.
  - Pode-se usar `chroot_local_user=YES` para **limitar o utilizador à sua pasta raiz** (ChangeRoot).
- **Limitação de Utilizadores**: O `vsftpd` permite limitar o número total (`max_clients`) e por IP (`max_per_ip`).

TALK e VNC

- **Computação Remota**: Capacidade de aceder e controlar um computador à distância por meio de rede.
- **TALK**:
  - Ferramenta de comunicação em **tempo real** via interface de texto dividida.
  - Requer: Instalação mútua, nome de utilizador e endereço IP do outro.
  - **Serviços Necessários**: `daemon talkd` (para convites/mensagens) e `inetd` ou `xinetd` (inicia `talkd` nas portas 517 ou 518).
  - **Limitações**: Falta de criptografia dos dados.
- **VNC (Virtual Network Computing)**:
  - Permite aceder e controlar a **interface gráfica** de um computador à distância.
  - Ferramenta versátil **multiplataforma**.
  - Requer: Servidor VNC (remoto) e Cliente VNC (local).

NFS: Partilha de Arquivos em Rede

- **Conceito**: Sistema de arquivos distribuídos (Sun Microsystems, anos 80) que permite a **montagem de sistemas de arquivos remotos** numa rede TCP/IP.
- **Utilidades**:
  - Acesso centralizado a arquivos como se estivessem localmente.
  - Facilita a partilha e o **backup centralizado** de dados.
  - Permite **configurar um único site em múltiplos servidores** (distribuição de carga).
- **Daemons Essenciais**:
  - `rpcd`: Fornece serviços básicos de Chamada Remota de Procedimento (RPC).
  - `mountd`: Atende a solicitações de montagem, verificando permissões.
  - `nfsd`: Atende a solicitações de leitura e escrita.

NFS: Configuração, Permissões e Montagem

- **Arquivo Exports** (`/etc/exports`):
  - Define o sistema de arquivos exportado, clientes e opções.
  - Ex. opções: `rw` (leitura/escrita), `ro` (somente leitura), `sync` (sincronização).
- **Acesso Root**:
  - Por padrão, o root cliente tem acesso restrito (`root_squash`).
  - `no_root_squash`: Permite que o utilizador `root` do cliente tenha **acesso total** à pasta exportada.
- **Montagem** (Importação de Pastas):
  - **Temporária**: Comando `mount -t nfs servidor:/dir /ponto_montagem`.
  - **Permanente**: Configuração no arquivo `/etc/fstab`.
- **Verificação**: Comando `showmount -e servidor` lista as pastas exportadas.

RPC: Chamada Remota de Procedimento

- **Conceito**: Protocolo que permite a um programa **executar uma função em outro computador** na rede sem conhecer os detalhes desse computador.
- **Funcionamento**: O computador remoto usa o **`portmapper`** ou **`rpcbind`** para descobrir qual programa é responsável e qual porta está a utilizar.
- **Ligação ao NFS**: O NFS utiliza o RPC para permitir que os programas executem funções nos sistemas de arquivos remotos, fazendo com que cliente e servidor comuniquem como se as funções estivessem a ser executadas localmente.
- **Verificação RPC (rpcinfo)**:
  - O comando `rpcinfo -p servidor` lista todos os programas registados.
  - A presença do **programa 100003** indica que o servidor está a executar o NFS.

Sumário e Recomendações de Segurança

- Priorize protocolos **seguros** (SSH, SCP, SFTP/FTPS) e desabilite protocolos inseguros (TELNET, RLOGIN, FTP padrão).
- A **criptografia** é a chave para a proteção de dados e credenciais em computação remota.
- Utilize **autenticação baseada em chaves SSH** sempre que possível.
- **NFS e RPC** são essenciais para a partilha de recursos e centralização do armazenamento em ambientes de rede.
- Siga as melhores práticas de segurança, como **desabilitar o acesso root remoto** ('PermitRootLogin no').