Conteúdos

0. Introdução ao Linux (5 horas)

Antes de explorarmos os serviços de rede, é fundamental entender a filosofia e as ferramentas básicas do Linux.

- **O que é o Linux?** (1 hora)
  Explicação simples do sistema operativo, suas principais características (código aberto, seguro, personalizável) e a diferença entre o kernel e uma distribuição (Debian, Ubuntu, Fedora).
- **A Magia da Linha de Comando** (2 horas)
  Apresentar o terminal como a principal ferramenta de trabalho.

```
# Navegação básica
ls -l          # Lista ficheiros e pastas (o -l mostra mais detalhes)
cd /home       # Navega para a pasta "home"
pwd            # Mostra o seu diretório atual

# Criar e apagar ficheiros
touch ficheiro.txt
rm ficheiro.txt
```

- **O Conceito de Ficheiros e Diretórios** (2 horas)
  Explicação da estrutura hierárquica do Linux (‘/‘, ‘/home‘, ‘/etc‘, ‘/var/log‘).
- **Exercício de Consolidação**
  1. Crie uma nova pasta chamada `treino` na sua pasta pessoal. 2. Dentro da pasta `treino`, crie um ficheiro de texto chamado `notas.txt`. 3. Use o comando `ls -l` para confirmar que o ficheiro foi criado. 4. Apague o ficheiro e, em seguida, a pasta que criou.

—

1. Serviços de rede (10 horas)

Nesta secção, vamos explorar como os serviços de rede são geridos no Linux, desde o seu início até ao encerramento, e os principais ficheiros e diretórios envolvidos neste processo.

- **O Gestor de Tarefas: O Papel do `systemd`** (3 horas)
  Pense no `systemd` como o "gerente de todas as tarefas"do seu computador. Ele garante que tudo (serviços de rede, servidores web, etc.) comece a funcionar na ordem certa quando o sistema é ligado.
- **Controlar Serviços com `systemctl`** (5 horas)
  O comando `systemctl` é como a "lista de comandos"para o gestor de tarefas.

```
# Ver o estado de um serviço (Exemplo: SSH)
systemctl status sshd

# Ligar, desligar e reiniciar um serviço
systemctl start sshd
systemctl stop sshd
systemctl restart sshd

# "Ativar" e "desativar" um serviço para iniciar no arranque
systemctl enable sshd
systemctl disable sshd
```

- **Exercício de Consolidação** (2 horas) 1. Instale um servidor web simples (como o Nginx) no seu sistema. 2. Use `systemctl status nginx` para verificar se ele está a funcionar. 3. Desligue-o com `systemctl stop nginx` e verifique o estado novamente. 4. Crie um ficheiro de unidade ‘.service‘ básico para uma aplicação simples, como um script de "Olá, mundo!"e ative-o para que inicie no próximo arranque.

—

Figura 1: Exemplo da saída do comando `systemctl status sshd`. *Fonte: Imagem encontrada via Google Images.*

2. XINET.d (4 horas)

O `xinetd` é como um "rececionista"que só acorda um funcionário (serviço) quando alguém aparece para o ver. Isso economiza energia! É usado para serviços que não precisam estar sempre a funcionar.

- **Configuração e Gestão** (2 horas)
  As configurações do `xinetd` estão nos ficheiros do diretório `/etc/xinet.d/`. Cada serviço tem o seu próprio "cartão de identificação".

  ```
  service telnet
  {
  disable         = yes # Para ativar, mude para "no"
  ...
  }
  ```

- **Exercício de Consolidação** (2 horas)
  1. Encontre o ficheiro de configuração do serviço `ftp` no diretório `/etc/xinet.d/`. 2. Altere o valor da opção `disable` para habilitá-lo. 3. Reinicie o serviço `xinetd` para que as alterações entrem em vigor: ‘systemctl restart xinetd‘. 4. Use um cliente FTP para tentar ligar-se à sua máquina e confirme que o serviço foi ativado.

—

3. TCPWrappers (4 horas)

Pense nos `TCPWrappers` como um porteiro. Ele decide quem pode entrar (permitir) e quem não pode (negar) num serviço, com base no endereço IP.

- **As Duas Listas: ‘hosts.allow‘ e ‘hosts.deny‘** (2 horas)
  - `hosts.allow`: A "lista de convidados". Se alguém estiver aqui, entra. - `hosts.deny`: A "lista negra". Se alguém não estiver na lista de convidados e estiver aqui, é barrado.

- **Sintaxe e Exemplos Avançados** (1 hora)
  Pode usar ‘ALL‘ para todos e ‘EXCEPT‘ para criar exceções.

  ```
  # No ficheiro /etc/hosts.allow
  sshd: 192.168.1.100 EXCEPT 192.168.1.101

  # No ficheiro /etc/hosts.deny
  sshd: ALL
  ```

  Neste exemplo, todos podem aceder ao SSH, exceto o IP ‘192.168.1.101‘.

- **Exercício de Consolidação** (1 hora)
  1. Configure o seu ficheiro `hosts.deny` para negar o acesso SSH a todos. 2. No ficheiro `hosts.allow`, adicione o IP do seu computador para poder aceder. 3. Tente ligar-se a partir de outro computador para confirmar que o acesso é negado.

—

4. NIS (6 horas)

O NIS é como ter uma única "identidade"para toda uma rede de computadores. Em vez de ter uma conta de utilizador em cada máquina, você tem uma conta num servidor central que funciona em todas as máquinas NIS.

- **Arquitetura NIS (Servidor Mestre e Cliente)** (3 horas)
  - **Servidor Mestre**: Tem a lista principal de utilizadores e grupos. - **Cliente NIS**: Pede ao servidor as informações de utilizadores. O 'ypbind' é o serviço que o cliente usa para encontrar o servidor.

- **Configuração do Cliente** (2 horas)
  Os clientes precisam de saber a que servidor NIS ligar. Isso é definido no ficheiro '/etc/nsswitch.conf', onde se indica ao sistema para procurar utilizadores e grupos no NIS, além dos ficheiros locais.

- **Exercício de Consolidação** (1 hora)
  1. Numa máquina cliente, use o comando `ypwhich` para ver qual é o servidor NIS. 2. Use `ypcat passwd` para listar as contas de utilizador. 3. Crie uma nova conta de utilizador no servidor NIS (o instrutor deve mostrar como) e verifique se consegue iniciar sessão com essa conta a partir do computador cliente.

—

5. DHCP (9 horas)

O DHCP é um protocolo que automaticamente dá um "endereço de rua"(o endereço IP) a cada dispositivo que se liga à sua rede.

- **O Processo DORA: Como funciona?** (4 horas)
  Pense no processo DORA como uma conversa entre um novo dispositivo e o servidor DHCP:

  1. **D**iscover: "Olá, estou aqui! Há algum servidor DHCP disponível?"
  2. **O**ffer: "Sim, eu sou um servidor! Aqui está um endereço IP que pode usar."
  3. **R**equest: "OK, obrigado! Quero usar este endereço."
  4. **A**cknowledge: "Certo, é todo seu! Divirta-se na rede!"

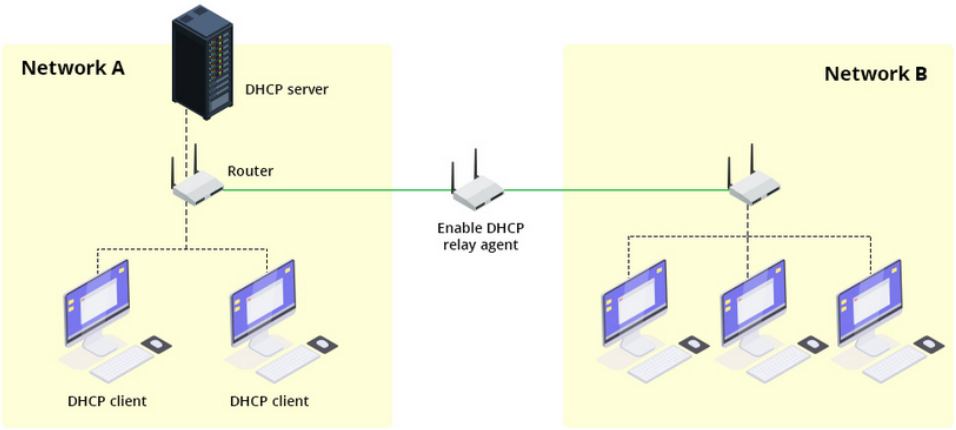

Figura 2: Diagrama do processo DORA. *Fonte: Imagem encontrada via Google Images.*

- **Configuração e Atribuição de Endereços** (3 horas)
  O ficheiro de configuração principal é o `/etc/dhcp/dhcpd.conf`. - `subnet`: Define a rede que o servidor vai gerir. - `range`: A lista de IPs que serão atribuídos dinamicamente. - `option routers`: Define o endereço do router/gateway. - `host`: Para dar um IP fixo a um computador específico (com base no endereço MAC).

- **Exercício de Consolidação** (2 horas)
  1. Configure um servidor DHCP para a sua rede de treino com um ‘range‘ de IPs para os alunos. 2. Adicione uma entrada estática para o computador do instrutor, garantindo que ele tenha sempre o mesmo IP. 3. Reinicie o serviço DHCP e peça aos alunos para testarem se estão a receber os IPs da forma correta.

—

6. DNS (10 horas)

O DNS é como a "lista telefónica"da internet. Ele traduz nomes fáceis de lembrar (como ‘google.com‘) em endereços IP que os computadores entendem (como ‘142.250.187.110‘).

- **Como a Lista Telefónica Funciona: A Hierarquia** (5 horas)
  A consulta de DNS é um processo de "perguntas e respostas": 1. O seu computador pergunta ao servidor DNS local: "Qual o IP de ‘google.com‘?"2. Se o servidor não souber, ele pergunta ao "servidor de raiz": "Onde encontro o ‘.com‘?"3. O servidor de raiz responde: "Vá ao servidor ‘.com‘."4. O servidor DNS local pergunta ao servidor ‘.com‘: "Onde encontro o ‘google‘?"5. O servidor ‘.com‘ responde: "Vá ao servidor autoritativo de ‘google.com‘."6. O servidor DNS local pergunta ao servidor de ‘google.com‘: "Qual o IP de ‘google.com‘?"7. O servidor responde com o endereço IP.

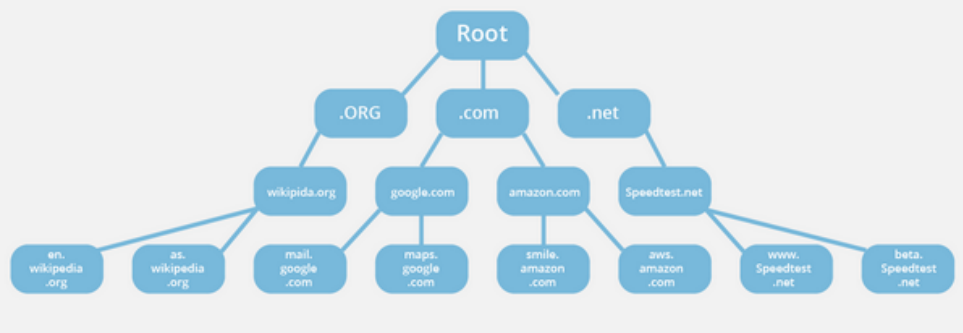

Figura 3: Fluxo de uma consulta DNS típica, mostrando a hierarquia de servidores. *Fonte: Imagem encontrada via Google Images.*

- **Tipos de Registos DNS (A, CNAME, MX)** (3 horas)
  - `A`: É a entrada principal, que diz ‘google.com‘ -> ‘142.250.187.110‘. - `CNAME`: Cria um "apelido". Exemplo: ‘www‘ é um apelido para o servidor principal. - `MX`: Diz qual servidor de email é responsável por um domínio.
- **Exercício de Consolidação** (2 horas)
  1. Use o comando ‘dig google.com‘ para ver a resposta DNS. 2. Use ‘dig www.google.com‘ para ver como o ‘CNAME‘ funciona. 3. Use ‘dig google.com MX‘ para encontrar o servidor de e-mail. 4. Crie um ficheiro de zona simples para um domínio ‘minhaescola.com‘ e adicione os registos A, CNAME e MX.

—

7. LOGS (2 horas)

Os logs são como um "diário de bordo"do seu computador. Eles registam tudo o que acontece e são essenciais para encontrar erros e problemas.

- **Onde Encontrar o Diário** (1 hora)
  A maioria dos logs está em `/var/log`. Os ficheiros mais importantes são: - `syslog` ou `messages`: Mensagens gerais do sistema. - `auth.log`: Registos de login e autenticação.
- **Como Ler o Diário: Comandos Úteis** (1 hora)
  - `tail -f /var/log/syslog`: Mostra as últimas linhas do ficheiro e acompanha as novas linhas em tempo real. - `grep "erro"/var/log/syslog`: Procura por uma palavra-chave como "erro".

- **Exercício de Consolidação**
  1. Tente iniciar um serviço com a sintaxe errada (o instrutor deve mostrar). 2. Use o comando `tail` ou `grep` para encontrar a mensagem de erro no ficheiro de log e identifique o motivo do erro. 3. Filtre os logs de autenticação para encontrar todas as tentativas de login falhadas na sua máquina.