

PROJETO INTERDISCIPLINAR I

Linux e LPI

www.lpi.org

João Bosco Teixeira Junior

boscojr@gmail.com

Certificação LPIC-1

- Prova 102
 - 105 – Shell, Scripting, e Gerenciamento de Dados
 - 106 – Interface com usuário e desktop
 - 107 – Tarefas Administrativas
 - 108 – Serviços Essenciais
 - 109 – Fundamentos de rede
 - **110 - Segurança**

Referências Bibliográficas

- Internet
 - IBM developerWorks Brasil
 - <http://www.ibm.com/developerworks/br/linux/>
 - Procurar por Learn Linux
- Livros
 - Certificação Linux
 - Autor: Uirá Ribeiro
 - LPI Linux Certification In a Nutshell
 - Editora: O'Reilly

110 – Segurança

Três Conceitos

- 110.1 Segurança do Sistema
- 110.2 Segurança do Host
- 110.3 Segurança da informação (Cifragem - ssh)

110 – Segurança

110.1 – Segurança do Sistema

- Procurar por arquivos com `suid/sgid` bits ligado
 - # `find -perm`
- Mudar informações de expiração de senha
 - # `chage -M dias usuario`
- Usar `netstat` e `nmap` para verificar se existe portas abertas
- Limites de uso de processos e memória
 - `Ulimits`, `/etc/security/limits.conf`
- Configuração básica do `sudo`
 - `Sudo`, `/etc/sudoers`

110 – Segurança

110.2 – Segurança do Host

- Impedindo logins
 - Criar o arquivo /etc/nologin
- SuperServer
 - Inetd
 - Xinetd
- Impedindo acesso a serviços
 - tcp_wrappers
 - /etc/hosts.allow
 - /etc/hosts.deny

110 – Segurança

110.3 – Criptografia - SSH

- Secure Shell
 - Criptografa a comunicação
 - Detecta “spoofing”
- Permite a cópia de arquivos entre hosts
- Permite autenticação por senha e por chave
- Permite a criação de túneis e redirecionamento de portas.

110 – Segurança

110.3 – Criptografia - SSH

- Configurações
 - Cliente: `/etc/ssh/ssh_config`
 - Servidor: `/etc/ssh/sshd_config`
- Iniciando o serviço
 - `/etc/init.d/ssh start`
- Acessando um servidor
 - `ssh usuario@[ip ou hostname]`

110 – Segurança

110.3 – SSH

- Copiando um arquivo/pasta (-r)
 - Destino remoto

```
scp -r pasta_local usuario@ip:/pasta_destino
```

- Destino Local

```
scp -r usuario@ip:/pasta_origem pasta_destino
```

110 – Segurança

110.3 – SSH

- Autenticação por chave
 - Passo 1: Gerar chaves publica e privada

```
# ssh-keygen -t rsa
```

- Passo 2: Copiar a chave pública para o host remoto

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub login@servidor
```

- Passo 3: Fazer login sem senha

```
# ssh usuario@host
```

110 – Segurança

110.3 – SSH

- Fazendo o redirecionamento de portas
- EX: Cliente por trás de um firewall precisa ser acessado por alguém na internet

```
# ssh usuario@host -R 2222:127.0.0.1:22
```

Por hoje é só!