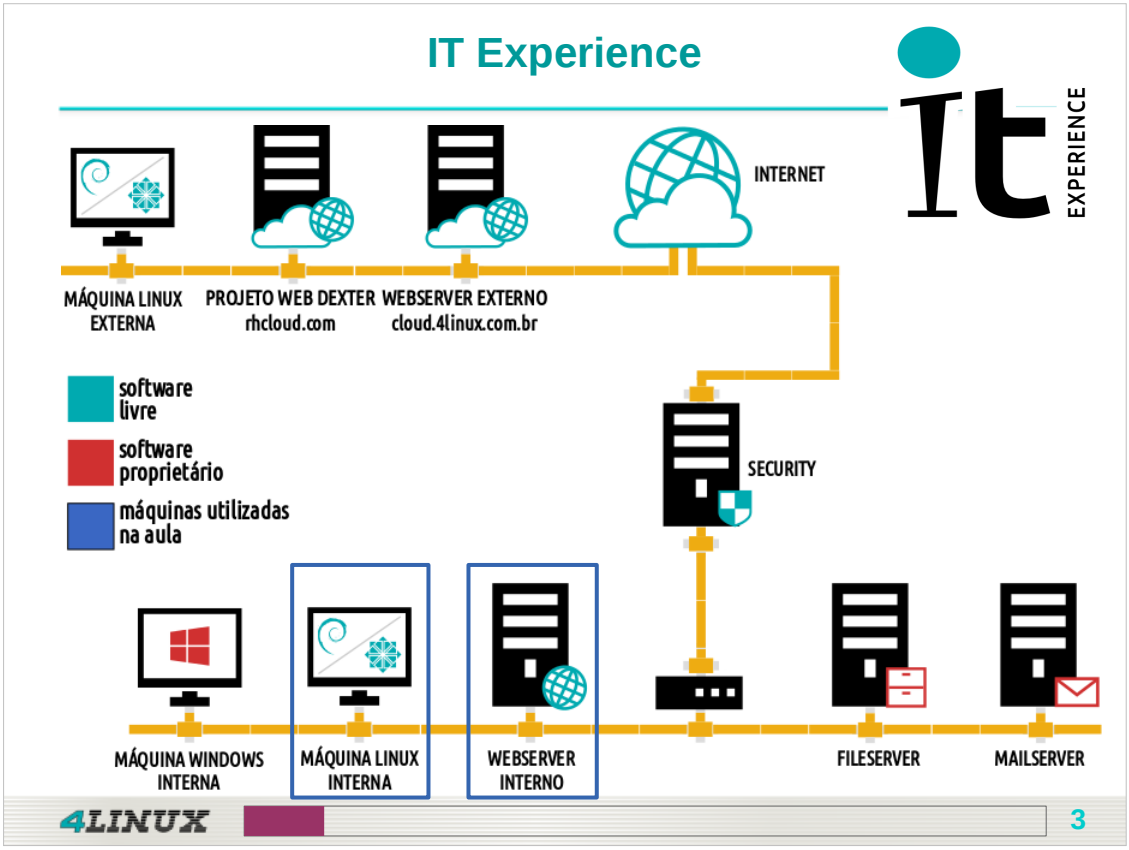
Introdução ao GPG

Anotações:


IT Experience
IT EXPERIENCE
INTERNET
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
software livre
software proprietário
máquinas utilizadas na aula
SECURITY
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
WEBSERVER INTERNO
FILESERVER
MAILSERVER
4LINUX
3

Anotações:

Objetivos da Aula

Aula 15

- Introdução a criptografia;
- Instalação do GNUPG;
- Gerenciar chaves com GPG;
- Encriptar e decriptar arquivos com GPG;
- Gerenciar assinaturas com GPG.

Anotações:

Introdução ao GPG

Criptografia:

Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado.

Anotações:

Introdução ao GPG

Tipos de criptografia:

Simétrica:

- Simples e útil;
- Cobre situações nas quais uma parte esteja envolvida;
- A pessoa que encripta é a mesma que decripta.

Assimétrica:

- Proporciona privacidade e autenticidade;
- Úteis na troca de e-mail;
- Seu uso exige que cada um dos lados possua um par chaves.

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

GNUPG:

Instalação na Linux Interna:

 # apt-get install gnupg

Verificar versão do GNUPG:

$ gpg --version

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

GNUPG:

1 – Para começar gere uma chave privada para trabalharmos com o gpg. Atenção as respostas em negrito (usuário suporte):

$ gpg --gen-key

Sua opção? **2**

What keysize do you want? (2048) **1024**

A chave é valida por? (0) **1y**

Is this correct? (y/N) **y**

Nome completo: **Suporte Máquina Interna**

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

GNUPG:

Endereço de correio eletrônico: **suporte-maqinterna@dexter.com.br**

Comentário: **Usuário Máquina Interna**

Muda (N)ome, (C)omentário, (E)ndereço ou (O)k/(S)air? **O**

Você precisa de uma frase secreta para proteger sua chave. **(Digite sua frase secreta)**

NOTA: Execute em outro terminal, diversos comandos para conseguir gerar entropia suficiente.

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

Gerenciamento de chaves:

Exportar chave para arquivo:

$ gpg --armor --output "chave_publica_suporte-maqinterna.txt" --export "suporte-maqinterna@dexter.com.br"

Envie o arquivo para a máquina Webserver Interno:

$ scp chave_publica_suporte-maqinterna.txt suporte@192.168.200.20:

Anotações:

Introdução ao GPG

Servidor: Webserver Interno

GNUPG:

Instalação no CentOS:

 # yum install gnupg

Verificar versão do GNUPG:

$ gpg --version

Importar chave de arquivo:

$ gpg --import chave_publica_suporte-maqinterna.txt

Anotações:

Introdução ao GPG

Servidor: Webserver Interno

Gerenciamento de chaves:

Listar chaves importadas:

$ gpg --list-keys

Editar chaves importadas:

$ gpg --edit-key "Suporte Máquina Interna"

Comando para definir o grau de confiança:

gpg> trust

Sua decisão? 5

Do you really want to set this key to ultimate trust? (y/N) y

Anotações:

Introdução ao GPG

Servidor: Webserver Interno

GNUPG:

1 – Para começar gere uma chave privada para trabalharmos com o gpg. Atenção as respostas em negrito:

 # gpg --gen-key

Sua opção? **2**

What keysize do you want? (2048) **1024**

A chave é valida por? (0) **1y**

Is this correct? (y/N) **y**

Nome completo: **Administrador WebServer Interno**

Anotações:

Introdução ao GPG

Servidor: Webserver Interno

GNUPG:

Endereço de correio eletrônico: **admin@dexter.com.br**

Comentário: **Servidor Webserver Interno**

Muda (N)ome, (C)omentário, (E)ndereço ou (O)k/(S)air? **O**

Você precisa de uma frase secreta para proteger sua chave. **(Digite sua frase secreta)**

NOTA: Execute em outro terminal, diversos comandos para conseguir gerar entropia suficiente.

Anotações:

Introdução ao GPG

Servidor: Webserver Interno

Encriptar:

Encriptar arquivo "fstab" na maquina WebServer Interno:

$ cp /etc/fstab .

$ gpg --recipient "Suporte Máquina Interna" --output "fstab.gpg" --encrypt "fstab"

Envie o arquivo para a máquina Linux Interna:

$ scp fstab.gpg suporte@192.168.200.10:

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

Decriptar arquivos:

Decriptar arquivo "fstab.gpg" na máquina Linux Interna:

$ gpg --decrypt-files fstab.gpg

Anotações:

Introdução ao GPG

Servidor: Máquina Linux Interna

Gerenciamento de assinaturas:

Assinar um arquivo com GPG:

$ echo "Assinatura com GPG" > carta.txt

$ gpg --clearsign carta.txt

Verificar assinatura de um arquivo com GPG:

$ gpg --verify carta.txt

Anotações:

Pergunta LPI

Qual opção do comando gpp você deve executar para listar chaves importadas?

a. `--list-keys`
b. `--show-keys`
c. `--edit-key`
d. `--keys-list`
e. `--keys-show`

Anotações:

Pergunta LPI

Qual opção do comando gpp você deve executar para listar chaves importadas?

a. `--list-keys`
b. `--show-keys`
c. `--edit-key`
d. `--keys-list`
e. `--keys-show`

Resposta: a

Anotações:

Próximos passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!

Anotações: