Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Segurança e Preservação de Dados

Criptografia e Autenticação com GPG e Keyservers
Atividade Prática em Laboratório (Roteiro)

Ao final desta aula, o aluno será capaz de:

1. Gerar um par de chaves GPG (pública e privada).
2. Publicar a chave pública em um Keyserver (keys.openpgp.org).
3. Importar a chave pública de um colega usando o Keyserver.
4. Criptografar uma mensagem para um colega (Garantia de Confidencialidade).
5. Assinar uma mensagem com sua chave privada (Garantia de Autenticidade/Integridade).
6. Descriptografar e verificar a assinatura de uma mensagem recebida.

1. Procedimentos Iniciais

Passo	Ação do Aluno	Comandos e Notas
1	Abrir o Terminal	
2	Verificar a instalação do GPG	`gpg --version`
3	Configurar o Keyserver Padrão	Editar o arquivo `~/.gnupg/gpg.conf` e adicionar a linha: `keyserver hkps://keys.openpgp.org`
4	Criar um diretório para a prática	`mkdir aula-gpg && cd aula-gpg`

2. Geração do Par de Chaves

Passo	Ação do Aluno	Comandos e Notas
1	Gerar o par de chaves GPG	`gpg --full-generate-key`
2	Selecionar o tipo de chave	Escolher `(1) RSA and RSA (default)` e `4096 bits`
3	Definir validade	Sugerir 1 ano `(1y)` ou `0` (não expira)
4	Inserir as informações de ID (Identificação única de sua chave)	Nome completo | E-mail (válido) | Comentário (algo que ajude a identificar a ID) [Confirmar ou fazer alterações antes de gerar]
5	Criar uma senha para acessar sua chave.	Importante não esquecer!!!

3. Verificando Chaves Locais, Exportando Chave para texto (ascii) e Publicando em um Keyserver

Passo	Ação do Aluno	Comandos e Notas
1	Listar a chave gerada e obter o ID e a Fingerprint (Impressão Digital)	`gpg --list-keys --keyid-format=long`
2	Identificar: O ID da chave (últimos 16 dígitos) e o e-mail	
3	Exportar a chave pública (formato ASCII)	`gpg --export --armor SEU_EMAIL > minha_chave.asc`
4	Publicar a Chave no Keyserver (keys.openpgp.org).	A forma mais fácil é fazer upload via web: Acessar: `https://keys.openpgp.org/upload`
5	Fazer o upload do arquivo `minha_chave.asc.`	O keyserver enviará um link de confirmação para o e-mail registrado. Verificar o e-mail e clicar no link de verificação!

Antes de seguir consulte se sua chave pública já está disponível em **keys.openpgp.org**

A consulta pode ser feita pelo E-Mail, Key ID ou Fingerprint

4. Baixando e Importando Chaves Públicas

Passo	Ação do Aluno	Comandos e Notas
1	Identifique e-mails e/ou IDs de chaves de alguns colegas de sala	
2	Faça a busca e importe as chaves públicas desses colegas	`gpg --recv-keys --keyserver hkps://keys.openpgp.org EMAIL_DO_COLEGA`
3	Solicite que os colegas que você baixou as chaves públicas também baixem sua chave pública	
4	Liste seu 'chaveiro local' para verificar o resultado da importação	`gpg --list-keys` (ou `gpg --list-keys EMAIL` para ver uma chave específica)

5. Criptografando e enviando mensagens 'secretas' (Confidencialidade)

Passo	Ação do Aluno	Comandos e Notas
1	Crie uma mensagem 'secreta'	`echo "Olá, esta é uma mensagem secreta para você" > segredo.txt`
2	Criptografe de modo que só um colega possa ler	`gpg --output segredo.gpg --encrypt segredo.txt --recipient EMAIL_DO_COLEGA`
3	Envie o arquivo `segredo.gpg` para o seu colega	Pode ser via e-mail, ou compartilhamento local, simulando a transmissão.

6. Descriptografando a mensagem 'secreta'

Passo	Ação do Aluno	Comandos e Notas
1	Descriptografe as mensagens que seus colegas lhe enviaram	`gpg --decrypt segredo.gpg`
2	Informe sua senha para usar sua chave privada para abrir e ler a mensagem enviada para você.	O conteúdo do arquivo será disponibilizado sem criptografia para você.

7. Experimente agora assinar as mensagens que você envia (Autenticidade)

Utilize o parâmetro `--sign` para isso.

Ex:

- `echo "Resposta criptografada e assinada" > resposta.txt`
- `gpg --output resposta.asc --encrypt --sign resposta.txt --recipient EMAIL_DO_COLEGA`

Ao receber uma mensagem criptografada e assinada e digitar `gpg --decrypt resposta.asc`
O GPG pedirá sua senha para descriptografar e verificará a assinatura do remetente (se a chave pública dele estiver em seu chaveiro local) informando se a assinatura é "verdadeira" (Autenticidade)