3.1 - Criptografia - Prática

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

Criptografia - Prática

Criptografia - Prática

- **GnuPG - GPG**
  - É uma implementação gratuita do padrão OpenPGP definido pela RFC 4880.
  - Permite criptografar e assinar seus dados e comunicação. Apresenta um sistema de gerenciamento de chave versátil, bem como módulos de acesso para todos os tipos de diretórios de chave pública.
  - Ferramenta de linha de comando com recursos para integração com outras aplicações.

- **GPG - Criptografando - Simétrico**
  - **gpg** −−**version** (é possível verificar quais algoritmos de criptografia são suportados)
  - **gpg** −−**symmetric** <**arquivo**> (criptografa arquivo usando chave simétrica)
  - **gpg** −−**symmetric** −−**cipher-algo** <**nome do algoritmo**> <**arquivo**> (criptografa arquivo utilizando algoritmo simétrico definido pelo usuário. Por padrão, o arquivo de saída gerado adicionará ".gpg" ao nome do arquivo criptografado).
  - **gpg** −−**output** <**arquivo**> −−**symetric** −−**cipher-algo** <**nome do algoritmo**> (−−output (ou -o) define o nome do arquivo de saída.)

Criptografia - Simétrica

- **GPG - Descriptografando - Simétrico**
  - **gpg** −−**output** <**arquivo de saída**> −−**decrypt** <**arquivo**> (Descriptografa arquivo. −−decrypt pode ser substituído por -d).

- **GPG - Criando um par de chaves pública/privada**
  - Para gerar um par de chaves pessoais use o comando **gpg** −−**gen-key**. Ele executará os seguintes passos:
    - Chave criptográfica - Selecione DSA e ELGamal a não ser que tenha necessidades específicas.
    - Tamanho da chave - 1024 bits traz uma boa combinação de proteção/velocidade.
    - Validade da chave - 0 a chave não expira. Um número positivo tem o valor de dias, que pode ser seguido das letras w (semanas), m (meses) ou y (anos). Por exemplo, "7m", "2y", "60".

Criptografia - Assimétrica

- Para Criptografia Assimétrica, consulte:
  - https://pt.wikibooks.org/wiki/Guia_do_Linux/Avan%C3%A7ado/Introdu%C3%A7%C3%A3o_ao_uso_de_criptografia_para_transmiss%C3%A3o/armazenamento_de_dados/Usando_pgp_(gpg)para_criptografia_de_arquivos ou
  - Guia GPG.pdf

Tarefa

1. Criptografe um arquivo e o decripte utilizando criptografia simétrica.
2. Crie um par de chaves pública/privada.
   - No moodle, busque por "Link para repositório de atividade da Aula 3.1". Deposite neste repositório, em seu respectivo diretório, sua chave pública.
   - Selecione dois colegas presentes em sala de aula e envie mensagens confidenciais. As mensagens devem ser colocadas em um arquivo de texto (.txt) e depositadas no respectivo diretório do usuário de destino.
   - Descriptografe e leia as mensagens confidenciais recebidas por você.
   - Em seu diretório deposite um arquivo, de qualquer tipo, assinador por você.
   - Verifique os arquivos assinados por alguns de seus colegas.
   - Assine a chave pública de um colega e deposite no diretório deste colega.
   - Cheque as assinaturas dos colegas que assinaram sua chave pública.

Criptografia - Hash

- **Gerando Hash**
  - md5sum <nomedoarquivo> > md5.txt
  - sha1sum <nomedoarquivo> > sha.txt
- **Verificando Hash**
  - md5sum -c md5.txt
  - sha1sum -c sha.txt

Criptografia - Hash

- Ferramentas para quebra de hash:
  - Hashcat: suporta vários algoritmos de hash, incluindo MD5, SHA-1, SHA-256 e outros.
  - Cain & Abel: ferramenta de segurança que pode ser usada para quebrar senhas e realizar outras tarefas de segurança, como escanear portas, realizar ataques de força bruta e sniffing de rede. Ele suporta vários algoritmos de hash, incluindo MD5, SHA-1 e outros.
  - Hydra: ferramenta de força bruta de linha de comando que pode ser usada para quebrar senhas, bem como realizar outros tipos de ataques de força bruta em sistemas e serviços.
  - RainbowCrack: usa técnicas de tabela arco-íris para quebrar senhas mais rapidamente do que outras ferramentas de quebra de senha convencionais. Ele suporta vários algoritmos de hash, incluindo MD5, SHA-1 e outros.
  - Ophcrack: usada principalmente para quebrar senhas do Windows. Ele usa tabelas de pré-computação para quebrar senhas mais rapidamente do que outras ferramentas convencionais de quebra de senha.

Criptografia - Hash

- John the ripper.
  - Ferramenta de segurança de código aberto que pode ser usada para testes de penetração e análise forense, mas seu uso deve estar dentro dos limites legais e éticos.

```
fabio@ubuntu:~$ sudo apt install john
```

  - Existem três modos de operação principais no John the Ripper. Os modos são apresentados a seguir.

Criptografia - Hash

- Modo de Dicionário: usa uma lista de palavras comuns para tentar adivinhar a senha. É necessário ter uma lista de palavras comuns em um arquivo de texto. Então, basta executar o John the Ripper com o arquivo de hash e o arquivo de dicionário como entrada, como no exemplo a seguir:

```
fabio@ubuntu:~$ john --wordlist=dicionario.txt arquivo_hash
```

Criptografia - Hash

- Modo Incremental: tenta todas as combinações possíveis de caracteres, começando com uma determinada cadeia de caracteres e avançando incrementalmente em direção a senhas mais longas e complexas. É necessário especificar uma cadeia de caracteres inicial para começar a gerar as senhas a partir dela.

```
fabio@ubuntu:~$ $ john --incremental=Aa1 arquivo_hash
```

Criptografia - Hash

- Modo Híbrido: combina o modo de dicionário e o modo incremental para tentar adivinhar a senha. É necessário especificar um arquivo de dicionário e uma cadeia de caracteres inicial.

```
fabio@ubuntu:~$
    $ john --wordlist=dicionario.txt --rules --incremental=Aa1 arquivo_hash
```

Criptografia - Hash

- Existem diversos dicionários disponíveis na internet que podem ser utilizados com o John the Ripper. Alguns exemplos de dicionários comuns incluem:
  - RockYou: um dicionário de senhas muito conhecido e usado em diversos ataques de segurança. Pode ser encontrado em:
    `https://wiki.skullsecurity.org/index.php?title=Passwords#Rockyou`
  - CrackStation: um dicionário de senhas que inclui senhas vazadas de grandes violações de dados e outras fontes. Pode ser encontrado em:
    `https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm`
  - Probable-Wordlists: uma coleção de dicionários de palavras comuns e senhas que podem ser usados com o John the Ripper. Pode ser encontrado em:
    `https://github.com/berzerk0/Probable-Wordlists`
  - SecLists: uma coleção de várias listas de palavras e senhas, incluindo dicionários, lista de nomes de usuários, senhas comuns e muito mais. Pode ser encontrado em:
    `https://github.com/danielmiessler/SecLists`

Referências

- https://pt.wikibooks.org/wiki/Guia_do_Linux/Avan%C3%A7ado/Introdu%C3%A7%C3%A3o_ao_uso_de_criptografia_para_transmiss%C3%A3o/armazenamento_de_dados/Usando_pgp_(gpg)para_criptografia_de_arquivos
- http://www.tutonics.com/2012/11/gpg-encryption-guide-part-4-symmetric.html
- https://www.guiafoca.org/guiaonline/seguranca/ch07s11.html