Segurança e Auditoria em Sistemas

Criptografia
Linux
Windows

Professor: Jiyan Yari

Criptografia no Linux e no Windows

A criptografia tem se tornado relativamente fácil de ser usada nos principais sistemas operacionais modernos de computadores pessoais, assim como também em smartphones, principalmente porque este último equipamento tem sido alvo preferido de tentativas de roubo de dados.

Criptografia no Linux e no Windows

Neste contexto serão apresentadas algumas ferramentas que possibilitam realizar a criptografia de arquivos, pastas (diretórios), partições de disco e até mesmo de discos inteiros de forma fácil e descomplicada.

Em alguns há soluções nativas, como no caso do Windows (BitLocker), e do Android (criptografia e credenciais).

Em outros, como no caso do Linux, com ferramentas de terceiros (ccrypt).

Criptografia de arquivos no Linux - ccrypt

ccrypt

Ccrypt é mais usado para criptografia de arquivos.

Usa o algoritmo “Rijndael cipher”, que é a mesma usada no padrão AES.

O AES usa um tamanho de bloco de 128 bits, enquanto ccrypt usa um tamanho de bloco de 256 bits.

O ccrypt normalmente gera arquivos de extensão “cpt”.

Criptografia de arquivos no Linux - ccrypt

Instalação

Distribuições Debian Like (Debian, Ubuntu, Mint, etc):

```
# apt-get install ccrypt
```

ou

```
$ sudo apt-get install ccrypt
```

Criptografia de arquivos no Linux - ccrypt

Opções:

-e, –encrypt: criptografa;

-d, –decrypt: descriptografa;

-c, –cat: descriptografa um ou mais arquivos;

-x, –keychange: muda a chave dos dados criptografados.

Criptografia de arquivos no Linux - ccrypt

Criptografando arquivos:

```
$ ccrypt -e nome_arquivo
```

ou

```
$ ccrypt nome_arquivo
```

ou

```
$ ccrypt nome_arquivos
```

Criptografia de arquivos no Linux - ccrypt

Exemplos:

```
$ ccrypt compras.xlsx
Enter encryption key:
Enter encryption key: (repeat)

$ ls
compras.xlsx.cpt
$cat compras.xlsx.cpt
ůPj□L□□na□Nh□ى□z□□□稷□M□v□□$□d□
u□□□ +
          □Yc□□3□□O□pZ□Q□S□□□□y
```

Criptografia de arquivos no Linux - ccrypt

Exemplos:

```
$ crypt *.xlsx
Enter encryption key:
Enter encryption key: (repeat)

$ ls
compras.xlsx.cpt  dados_temp.xlsx.cpt  dados.xlsx.cpt
compra.xlsx.cpt   dadostemp.xlsx.cpt   notas.xlsx.cpt
```

Criptografia de arquivos no Linux - ccrypt

Descriptografando:

```
$ ccrypt -d nome_arquivo
```

ou

```
$ ccrypt -d nome_arquivos
```

Criptografia de arquivos no Linux - ccrypt

Exemplos:

```
$ ccrypt -d compras.xlsx.cpt
Enter decryption key:

$ ls
compras.xlsx
```

Criptografia de arquivos no Linux - ccrypt

Exemplos:

```
$ ccrypt -d *.cpt
Enter decryption key:

$ ls
compras.xlsx        compra.xlsx     dados_temp.xlsx
dadostemp.xlsx      dados.xlsx      notas.xlsx
```

Criptografia de partições e dispositivos no Linux

O Linux, por padrão, torna fácil criptografar uma partição já na instalação da distribuição.

A maioria das distribuições possui um passo-a-passo que guia o usuário no processo todo, no entanto, depois de instalado também é possível, e de forma fácil, criptografar uma partição ou discos removíveis no Linux.

Criptografia de partições e dispositivos no Linux

A maioria das distribuições Linux oferece opção de criptografar uma partição na instalação da distribuição.

A maioria das distribuições possui um passo-a-passo que guia o usuário no processo todo, no entanto, depois de instalado também é possível, e de forma fácil, criptografar uma partição ou discos removíveis no Linux.

Criptografia de partições e dispositivos no Linux

Neste contexto, o Linux permite criptografar também de forma bastante rápida e fácil criptografar rapidamente dispositivos flash USB e discos rígidos externos.

A ferramenta mais usada é o LUKS (Linux Unified Key Setup).

Criptografia de partições e dispositivos no Linux

Instalação:

Nas distribuições Debian Like:

```
$ apt install cryptsetup
```

Criptografia de partições no Linux - dm-crypt

Cuidados:

A criptografia de partições sobrescreve todos os dados existentes, dessa forma, caso ocorra erro no nome do dispositivo, certamente haverá perda irreprável de dados.

Criptografia de partições no Linux - dm-crypt

Cuidados:

Qualquer operação de criptografia em dispositivos e ou partições requer que se faça um backup de todos os arquivos no dispositivo de armazenamento removível antes de criptografá-lo.

No LUKS, em específico, a criptografia formatará a unidade, excluindo todos os dados nela.

Criptografia de partições no Linux - dm-crypt

Cuidados:

Dessa forma, uma sugestão é se certificar dos nomes das partições utilizando ferramentas de visualização de partições como o:

- sblk;
- cfdisl.
- fdisk.

Criptografia de partições no Linux - dm-crypt

```
$ sblk

NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0 931,5G  0 disk
├─sda1   8:1    0   100M  0 part
├─sda2   8:2    0    16M  0 part
├─sda3   8:3    0 195,4G  0 part
├─sda4   8:4    0     1G  0 part
└─sda5   8:5    0   735G  0 part
sdb      8:16   0   477G  0 disk
├─sdb1   8:17   0   100M  0 part /boot/efi
├─sdb2   8:18   0    16M  0 part
├─sdb3   8:19   0 244,1G  0 part
├─sdb4   8:20   0     1K  0 part
└─sdb5   8:21   0 232,8G  0 part /
```

Criptografia de partições no Linux - dm-crypt

```
$ sudo cfdisk
```

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	206847	204800	100M	EFI System
/dev/sda2	206848	239615	32768	16M	Microsoft reserved
/dev/sda3	239616	409989119	409749504	195,4G	Microsoft basic data
/dev/sda4	1951426560	1953523711	2097152	1G	Windows recovery environment
/dev/sda5	409989120	1951426559	1541437440	735G	Microsoft basic data

Criptografia de partições no Linux - dm-crypt

```
$ sudo fdisk -l /dev/sda
```

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	206847	204800	100M	EFI System
/dev/sda2	206848	239615	32768	16M	Microsoft reserved
/dev/sda3	239616	409989119	409749504	195,4G	Microsoft basic data
/dev/sda4	1951426560	1953523711	2097152	1G	Windows recovery environment
/dev/sda5	409989120	1951426559	1541437440	735G	Microsoft basic data

Criptografia de partições no Linux - dm-crypt

```
$ sudo fdisk -l
```

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	206847	204800	100M	EFI System
/dev/sda2	206848	239615	32768	16M	Microsoft reserved
/dev/sda3	239616	409989119	409749504	195,4G	Microsoft basic data
/dev/sda4	1951426560	1953523711	2097152	1G	Windows recovery environment
/dev/sda5	409989120	1951426559	1541437440	735G	Microsoft basic data