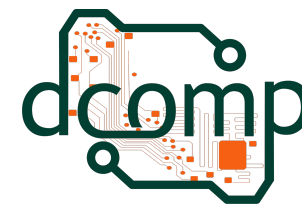




Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCA UFES
Departamento de Computação



Técnicas Anti-Forenses

Nome da Disciplina

Site: <http://jeiks.net>

E-mail: jacsonrcsilva@gmail.com

Técnicas Anti-Forenses

- As técnicas anti-forenses podem deixar uma busca ainda mais complicada ou impossível de ser realizada.
- As técnicas anti-forenses podem ser utilizadas
 - Para esconder algo que foi ou está sendo realizado; ou
 - Para apagar dados de forma irrecuperável.
- Métodos já estudados na disciplina:
 - Wipe;
 - Esteganografia;
 - Slack Space; e
 - Modificação de TimeStamps.

Criptografia

- Do Grego *kryptós*, "escondido", e *gráphein*, "escrita";
- Consiste no ato de transformar uma mensagem original em uma mensagem ilegível;
- Somente quem conhece o segredo que pode ver as informações ocultas.
- É um dos métodos mais antigos para esconder informações.
- Desde arquivos simples à sistemas de arquivos completos podem utilizar criptografia.



Trabalhando com sistemas de arquivos criptografados

Criando uma imagem:

```
dd if=/dev/zero of=imagem.img bs=1024 count=$((1024*10))
```

Escrevendo dados aleatórios na imagem criada:

```
shred imagem.img
```

Criptografando a partição:

```
cryptsetup -y --cipher serpent-cbc-essiv:sha256 \  
--key-size 256 luksFormat imagem.img
```

Montando a partição:

```
cryptsetup luksOpen imagem.img imagem  
mkfs.vfat /dev/mapper/imagem #somente uma vez, para formatar  
mkdir pasta  
mount /dev/mapper/imagem pasta
```

Desmontando:

```
umount /dev/mapper/imagem  
Cryptsetup luksClose imagem
```



Descriptografando senhas

Criando senhas digest (comum para o apache2):

```
htdigest -c arquivo.txt "Jacson Rodrigues" jeiks  
cat arquivo.txt
```

```
jeiks:Jacson Rodrigues:157dbd359942a88b2bdbe3bc2d2e6378
```

Descriptografando a senha:

```
john arquivo.txt
```

```
...
```

```
jeiks (test)
```

```
...
```



Outra forma de esconder arquivos

Suponha que tenhamos os dois arquivos:

- *imagem.jpg* # *Arquivo simples de imagem*
- *arquivo.rar* # *Arquivo compactado com senha*

Unindo o conteúdo dos dois arquivos:

```
cat imagem.jpg arquivo.rar > nova_imagem.jpg
```

Verifique se há problemas ao ver a imagem.

Agora, tente extrair o arquivo no Windows e no Linux.

Rootkits

- Um *rootkit* é um conjunto de programas
 - utilizados para impedir a detecção de atividades maliciosas no sistema.
- São utilizados por invasores de sistemas para manterem acesso após um ataque bem sucedido, sem que precisem subverter o sistema novamente.
- Cada *rootkit* possui diferentes características, como:
 - Esconder informações sobre os processos referentes;
 - Esconder seus arquivos;
 - Esconder *sockets* criados para comunicação em rede;
 - Modificar ou restringir o acesso aos arquivos de *log*.
- O termo “rootkit” vem da junção de:
 - “root”: representa o chamado super-usuário, ou usuário root.
 - “kit”: conjunto de programas que compõem o *rootkit*.

Atividade Avaliativa

1. Acessar o link:
jeiks.net/wp-content/uploads/2013/10/rootkits.pdf
2. Escrever uma descrição do que é *rootkit* e onde ele pode ser utilizado no sistema.
3. Escolher um *rootkit* dentre os citados no artigo e fazer uma análise do aplicativo.