5. O que buscar na análise (continuação)

Em casos de invasão por rede ou comprometimento local do SO

- Analise diretórios relevantes.
- Busque rastros do oponente em outros diretórios.
- Busque por rootkits e backdoors.
- Verifique se o sistema operacional estava atualizado. Inicie a verificação pelos pacotes mais relevantes. Exemplo: Apache, PHP e Java em um defacement.

6. Alguns comandos e ferramentas

- Instale o Sleuth Kit.
- ls -lta: mostra a data e a hora de criação ou modificação de arquivos e diretórios.
- ls -lua: mostra a data e a hora de acesso a arquivos e diretórios.
- stat: mostra dados gerais de um arquivo. Ex: MACtimes.
- strings + grep: faz chover no Nordeste.
- chkrootkit e rkhunter: procuram por rootkits. Exemplos:

```
# chkrootkit -r /mnt
# rkhunter --update; rkhunter -c -r /mnt
```

- clamav: procura por worms e vírus. Exemplo:

```
# freshclam; clamscan -r /mnt
```

- fls + mactime: estabelece uma linha de tempo (timeline).
- find: dentre outras coisas, pode procurar por arquivos em diversas situações. Exemplo de busca para arquivos modificados nos últimos 2 dias:

```
# find /mnt/ -mtime -2 print
```

- foremost: busca por arquivos, apagados ou não, em imagens de disco e memória. É interessante utilizá-lo como usuário comum para poder abrir arquivos encontrados. Ou use sux para se tornar root. Exemplo:

```
$ foremost -T memoria.dd
```

Com *-a* recupera arq. danificados mas dá falsos positivos.

- magicrescue: idêntico ao foremost. No entanto, pode produzir resultados diferentes. Usa recipes. Veja-os em */usr/share/magicrescue/recipes*. Exemplo:

```
$ mkdir mr; magicrescue -r msoffice -d mr
  imagem.dd
```

- hexedit: mostra e edita conteúdos em hexadecimal e ASCII. É um ambiente. Para linha de comando simples utilize hexdump.
- mcview: mostra e edita conteúdos em ASCII.
- file: mostra características de arquivos. Útil com imagens, fotos, documentos office e executáveis.
- okular (KDE) e evince (Gnome) para conteúdos diversos.
- gwenview, pornview e gimp podem ser utilizados para ver fotos (inclusive danificadas).
- mmls ou fdisk -lu: mostra dados sobre a arquitetura de um disco a partir da análise de uma imagem.
- metacam: mostra dados exif de imagens JPG.
- Mais? *apt-cache search forensic* ou *http://bit.ly/forense* (veja o item "Páginas com ferramentas e tutoriais").

7. Laudo

- O laudo de perícia forense, em 3 vias, deverá conter:
  - nome, CPF e contatos do perito;
  - período de realização da forense;
  - breve relato do ocorrido (inclui notícias iniciais);
  - dados gerais sobre o hardware periciado;
  - detalhamento dos procedimentos realizados (um segundo perito deverá ter condições de refazer todos os procedimentos, caso alguma autoridade requeira);
  - dados, fatos e indícios relevantes encontrados;
  - conclusão e recomendações;
  - apêndices (inclui certificado de integridade) e anexos.

Obs: apêndices contêm material produzido pelo perito. Anexos contêm material colhido pelo perito.

Perícia Forense Computacional

"Guia de referência rápida"

PERÍCIA LINUX COM DEBIAN GNU/LINUX

Parte 2:

Análise de evidências e laudo

Versão 1.1 - 03 de setembro de 2010

debian

http://www.eriberto.pro.br/forense
eriberto@eriberto.pro.br

2048R/2DF0491F: 1D75 E212 B34C F4BF A9E0 D0D8 DE6D E039 C1CF C265

1. Preâmbulo

Este guia de referência foi criado com o intuito de servir como orientação e checklist para profissionais que realizam perícias forenses computacionais.

Assim, este documento resume e complementa a palestra *Forense computacional em Linux for dummies*, disponível em *http://www.eriberto.pro.br/palestras* e o artigo de wiki *Forense computacional*, disponível no endereço *http://www.eriberto.pro.br/forense*.

2. Ambiente de análise forense

- Uma vez colhidos os dados iniciais e imagens (veja o guia que contém a parte 1), a perícia deverá ser realizada em ambiente próprio.
- O ambiente deverá ter, por exemplo, o The Sleuth Kit (TSK) instalado (no Debian, # *apt-get install sleuthkit*).
- O TSK é o sucessor do TCT (The Coroner's Toolkit).
- O Autopsy é um front-end web para o Sleuth Kit.
- Há ferramentas prontas em Live CD/DVD, caso você não queira construir um ambiente manualmente. Veja *http://eriberto.pro.br/forense*.

3. Ações iniciais na perícia

A história e os fatos

- A primeira ação será ouvir a história contada por quem solicitou a perícia de uma determinada máquina.
- O perito deve anotar a história e fazer perguntas que esclareçam pontos obscuros.
- Das anotações surgirá uma linha de investigação e palavras-chave a serem utilizadas na análise.
- Buscar dados complementares usando engenharia social ou outros métodos.
- Criar uma lista de palavras-chave com base na história contada e nos dados levantados com engenharia social.

Ordenação cronológica (timeline)

- Utilizada em máquinas invadidas remotamente ou quando se quer buscar manipulações em arquivos, ocorridas dentro de uma determinada faixa de tempo.
- Nem sempre será necessário trabalhar com timelines.
- Feita sobre os MACtimes (**M**odify / read **A**ccess / status **C**hange).
- Timeline de filesystem com Sleuth Kit (ainda não suporta plenamente o Ext4):

```
# fls -r -m / imagem.dd > imagem.dd.timeline
# mactime -b imagem.dd.timeline
```

- Caso seja necessário ver eventos desde 10 ago. 2010:

```
# mactime -b imagem.dd.timeline 2010-08-10
```

- Caso seja necessário ver eventos entre 10 ago. 2010 e 15 ago. 2010:

```
# mactime -b imagem.dd.timeline 2010-08-
10..2010-08-15
```

Criação de lista de strings

- A lista de strings deve ser criada para diminuir o espaço a ser varrido durante a busca por uma palavra ou expressão.
- Por default, o comando strings considera qualquer sequência de 4 caracteres imprimíveis. Isso pode ser mudado com a opção *-n*.
- Criar a lista a partir das imagens de disco e memória.

```
# strings memoria.dd > memoria.dd.strings
```

- Para fazer uma busca, use *grep*, *egrep* ou *fgrep*. Exemplo:

```
# cat memoria.dd.strings | grep -i bras.lia
```

- No caso anterior, como *grep* entende expressões regulares, o caractere ponto foi utilizado no lugar de um possível "i" acentuado.
- Se você precisa de um guia rápido sobre expressões regulares, consulte *http://bit.ly/wp-er*. Para diversos guias, consulte *http://aurelio.net/er*.

4. Cuidados com as imagens

- Caso haja a necessidade de montar alguma imagem de disco, faça-o somente no modo read-only. Exemplos:

```
# mount -o loop,ro imagem.dd /mnt
# mount -o loop,ro,offset=32256 imagem.dd /mnt
```

- Lembre-se que só se pode montar imagens de partições de HD ou mídias removíveis. Imagens de memória (incluindo o swap) devem ser analisadas diretamente.
- Sempre trabalhe em uma cópia de cada imagem. Isso permitirá que você tenha uma imagem original caso ocorra algum acidente ou operação indevida.

5. O que buscar na análise

Em qualquer caso

- Verifique os arquivos modificados dentro de determinada faixa de tempo (timeline).
- Busque por palavras-chave relevantes nas imagens.
- Analise logs (dentro da memória ou no filesystem com strings, por exemplo).
- Analise a memória e o swap. Busque, dentre outras coisas, por senhas e arquivos. Para senhas, utilize palavras-chave e dicionários.
- Se puder montar alguma imagem de disco, analise:
  - */tmp*
  - */var/tmp*
  - */home*
  - outros diretórios de interesse.
- Analise as propriedades de arquivos do tipo office, PDF, imagens JPG (dados exif) e outros.
- Figuras podem conter esteganografia.
- Arquivos criptografados possuem senha e a mesma pode estar na memória.

Continua...