Aula 05
Forense Computacional

Ferramentas Open Source

Agenda

- ✓ Script da última aula
- ✓ Dados não voláteis
- ✓ MACtimes
- ✓ Memória física
- ✓ Dump da Memória
- ✓ PTK

Script

- Ver scripts rodando

Informações Cronológicas

- ✓ Saber quando uma sequência de eventos ocorreu pode ser mais importante do que saber o que ocorreu.
- ✓ MACtimes - São atributos de tempo de um arquivo (mtime, atime e ctime).

- ➢ ***mtime*** (Modification time): mostra a última data e hora em que o arquivo foi modificado.
- ➢ **atime** (Access time): mostra a última data e hora em que um diretório ou arquivo foi acessado/lido.
- ➢ **ctime** (Creation time): mostra a data e hora em que arquivo foi criado.

- ➢ Comado touch???
- ➢ $ touch - m 0909141940 arquivo
- ➢ $ touch -c -t 191101100341.15 mem.dump

STAT

Análise de memória física

- ✓ A análise de memória física baseia-se em fazer um dump da memória física e virtual de um sistema.
- ✓ O que podemos conseguir através da memória física?
  - ➢ Arquivos com senhas em texto puro;
  - ➢ Arquivos com variáveis de ambiente ($HISTFILE)
  - ➢ O mapas de todos os serviços que se encontram em execução.
- ✓ Aplicações de terminal:
  - ➢ **memdump** (posix) http://www.porcupine.org/forensics/memdump-1.0.tar.gz
  - ➢ http://www.vivaolinux.com.br/dica/A-importancia-de-rastrear-comandos-com-o-HISTFILE

Análise de memória física

- ✓ **Configuração de memory dump do windows**
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\i8042prt\Parameters
  - Criar uma chave tipo DWORD chamada CrashOnCtrlScroll com valor 1;
  - Pressionar o Ctrl direito e scroll lock duas vezes;
  - C:\Windows\Minidump\memory.dmp;
  - W7 = C:\Windows\Minidump\032012-29203-01.dmp

Dump da memória

- ✓ Dump da memória é nome do processo de capturar as informações da memória, e pode ser feito através do comando **dd, dcfldd** entre outros.

 # dd < /dev/mem > mem.dump

 # dd < /dev/kmem > kmem.dump

- ✓ É possível realizar buscas por palavras-chave através dos comandos grep e strings

 # strings -a mem.dump | grep palavra-chave

Ex.

 # strings -a mem.dump | grep firefox

Dump da memória

- ✓ O diretório /proc é um pseudo-sistema de arquivos usado como uma interface para as estruturas de dados do kernel.
- ✓ A memória pode ser acessada pelo pseudo-arquivo /proc/kcore, que representa a memória física do sistema no formato de um core file.
- ✓ Buscando processos vinculados ao firefox:

 # strings -a /proc/kcore | grep firefox > kcore_firefox.dump

 # more kcore_firefox.dump

Dump da memória

- ✓ fmem

 # dcfldd if=/dev/fmem of=/home/fdtk/evidencias/memoria.img count=3072 bs=1M

 # strings -a /home/fdtk/evidencias/memoria.img | grep firefox

✓Abrir imagem no PTK

Dados Não-Voláteis

- ✓ As análises baseadas em dados armazenados em mídia de backup, pendrives, Cds, ou memória auxiliar como um HD, são chamadas de “Análise Post-Mortem”.

- ✓ Dados não voláteis, são dados que podem permanecer na máquina durante longos períodos de tempo e podem ser recuperados mesmo após a mesma ser desligada.

- ✓ Conteúdo de arquivos, logs (registro de atividades realizadas por algum programa) do sistema e MACtimes.

Dados Não-Voláteis

- ✓ A coleta dos dados, que pode ser executada de 2 maneiras, localmente ou através da rede e dividida em 3 formas que são:
  - Disco para Disco (clone);
  - Partição para Partição;
  - Disco/partição para arquivo (img.dd).
  - ✓ Algumas das ferramentas que podem ser utilizadas neste procedimento são:
  - dd;
  - sdd;
  - aimage;
  - air;
  - dd_rhelp
  - ...

Dados Não-Voláteis

- ✓ **dcfldd** - é uma versão melhorada do GNU dd com características úteis para Forense e segurança. Baseado no programa dd encontrado no pacote GNU Coreutils, dcfldd tem as seguintes características adicionais:

- ➢ **Hash On-the-fly** dos dados transmitidos.
- ➢ **Barra de progresso** da quantidade de dados que já foram tratados.
- ➢ **Wipe** - Limpeza de discos com padrões conhecidos.
- ➢ **Check** - Verificação se a copia gerada é idêntica a unidade original, bit por bit.
- ➢ **Destino duplo** - Saída simultânea para mais de um arquivo / disco é possível.
- ➢ **Split** - A saída pode ser dividido em vários arquivos.

Coleta de dados Não-Voláteis

- ✓ **Criando imagem de disco para disco (clone) pela rede**

  - ✓ A estação Forense será o server ou seja, receberá e gravará os dados vindos da estação suspeita. Para isso, você deve levantar o netcat em modo listening (ouvindo), desta forma todos os dados que chegarem a porta definida, serão processados por ele. A estação suspeita por sua vez terá seus dados copiados e enviados a estação Forense.

  Na estação Forense, que receberá os dados da estação suspeita faça:

$ nc -v -l 12345 > /dev/sdb

nc --> netcat

-v -->> verbose

-l --> parâmetro informando ao nc que ele será o ouvinte (listening)

12345 --> porta tcp na qual o netcat estará aguardando os dados

> --> sinal de maior indica saída para

/dev/sdb --> arquivo que será gerado a partir dos dados recebidos pelo netcat na porta 12345

Coleta de dados Não-Voláteis

Na estação suspeita e que terá seus dados copiados, faça:

$ sudo dd if=/dev/sdb conv=noerror,sync bs=128k | nc -vn 10.1.1.10 12345 -q 5

dd --> disk dump, copia os dados
if=/dev/sdb --> informa qual a origem dos dados
conv=noerror,sync --> informa ao dd que não pare a copia caso ocorra algum erro.
bs=128k --> informando ao dd que envie blocos de 128k de dados por fez
| --> pipe = informa que a saída dos dados de um comando serão entrada em outro.
nc --> netcat
-vn --> verbose + ip numérico
10.1.1.10 --> ip de destino
12345 --> porta de destino
-q 5 --> desconectar em 5 segundos após a conclusão da operação

Coleta de dados Não-Voláteis

- ✓ **Criando imagem de partição para partição pela rede + hash sha256sum**
  - ➢ **Cópia dos dados**

✓ Na estação forense faça:

$ nc -v -l 12345 > /dev/sdb1

✓ Na estação suspeita faça:

$ sudo dd if=/dev/sdb1 conv=noerror,sync bs=128k | nc -vn 10.1.1.10 12345 -q 5

  - ➢ **Hash dos dados**

✓ Na estação forense faça:

$ nc -v -l 12345 > /home/fdtk/evidencias/sha256.txt

✓ Na estação suspeita faça:

$ sudo sha256sum dev/sdb1 | nc -vn 10.1.1.10 12345 -q 5

Coleta de dados Não-Voláteis

✓ **Criando imagem de disco para arquivo pela rede**

➢ **Na estação Forense faça:**

$ nc -v -l 12345 > hd1-caso1.dd

nc --> netcat
-v --> verbose
-l --> parametro informando ao nc que ele será o ouvinte
12345 --> porta tcp na qual o netcat estara aguardando os dados
> --> sinal de maior indica saída
hd1-caso1.dd --> arquivo que será gerado a partir dos dados recebidos pelo necat na porta 12345

➢ **Na estação suspeita faça:**

$ sudo dd if=/dev/sdb conv=noerror,sync bs=128k | nc -vn 10.1.1.10 12345 -q 5

dd --> disk dump, copia os dados
if=/dev/sdb --> informa qual a origem dos dados
conv=noerror,sync --> informa ao dd que nao pare a copia caso ocorra algum erro.
bs=128k --> informando ao dd que envie blocos de 128k de dados por fez
| --> pipe = informa que a saída dos dados de um comando serão entrada em outro.
nc --> netcat
-vn --> verbose + ip numérico
10.1.1.10 --> ip de destino
12345 --> porta de destino
-q 5 --> desconectar em 5 segundos após a conclusão da operação

Coleta de dados Não-Voláteis

- ✓ **Criando imagem de disco para arquivo pela rede com dcfldd e alguns paramentros a mais**

➢ **Na estação Forense faça:**

$ nc -v -l 12345 > hd1-caso1.dd

nc --> netcat
-v --> verbose
-l --> parametro informando ao nc que ele será o ouvinte
12345 --> porta tcp na qual o netcat estara aguardando os dados
> --> sinal de maior indica saída
hd1-caso1.dd --> arquivo que será gerado a partir dos dados recebidos pelo necat na porta 12345

Coleta de dados Não-Voláteis

- ✓ **Criando imagem de disco para arquivo pela rede com dcfldd e alguns paramentros a mais**

  - ➢ **Na estação suspeita faça:**

$ sudo dcfldd if=/dev/sdb hash=sha256,sha512 sha256log=/home/fdtk/evidencias/sha256.txt sha512log=/home/fdtk/evidencias/sha512.txt hashconv=after conv=noerror,sync bs=128k | nc -vn 10.1.1.10 12345 -q 5

dcfldd --> disk dump, copia os dados
if=/dev/sdb --> informa qual a origem dos dados
hash256,hash512 --> Calcula um hash256sum + um hash 512 on-the-fly
sha256log=/home/fdtk/evidencias/sha256.txt --> Local e arquivo de hash criado on-the-fly de 256-bits
sha256log=/home/fdtk/evidencias/sha512.txt --> Local e arquivo de hash criado on-the-fly de 512-bits
hashconv=after --> gerar o hash apos a cópia
conv=noerror,sync --> informa ao dcfldd que não pare a copia caso ocorra algum erro.
bs=128k --> informando ao dcfldd que envie blocos de 128k de dados por fez
| --> pipe = informa que a saída dos dados de um comando serão entrada em outro.
nc --> netcat
-vn --> verbose + ip numérico
10.1.1.10 --> ip de destino
12345 --> porta de destino
-q 5 --> desconectar em 5 segundos após a conclusão da operação

Coleta de dados Não-Voláteis

- ✓ **Efetuando a coleta das evidências localmente**

```
$ sudo dcfldd if=/dev/sdb hash=sha256,sha512 sha256log=/home/fdtk/evidencias/sha256.txt
sha512log=/home/fdtk/evidencias/sha512.txt hashconv=after conv=noerror,sync
of=/home/fdtk/evidencias/caso01/hd1-caso1.dd
```

Atividade

✓Hands-on

- ✓ Create images of your pendrives.

- ✓ **Utilizando o material e os exemplos mostrados durante a aula, gerar uma imagem do seu pendrive, abrí-lo no PTK e recuperar 5 arquivos deletados.**

Leitura complementar

http://augustocampos.net/revista-do-linux/030/seguranca.html