5. Dump de memória

5.1 Kernel Linux anterior a 2.6.27

- Kernel sem restrição de acesso à memória. Executar:

```
# dd if=/dev/mem of=/mnt/memoria.dd
```

5.2 Kernel Linux 2.6.27 ou posterior

- Kernel com restrição de acesso à memória (CONFIG_STRICT_DEVMEM).
- Compilar e instalar o módulo *fmem*, disponível em *http://hysteria.sk/~niekt0/foriana*.
- Executar:

```
# dd if=/dev/fmem of=/mnt/memoria.dd
```

5.3 Máquina virtual Xen

- Executar na máquina real (Dom0):

```
# xm dump-core <resource> memoria.dd
```

6. Imagem da mídia a ser periciada

- **ATENÇÃO: deverá haver duas testemunhas durante todo o processo, inclusive no momento da abertura da máquina com HD a ser periciado.**
- Adicionar HD de maior capacidade do que o da mídia a ser periciada.
- Inicializar a máquina a ser periciada com um live CD ou pendrive com ferramentas forense (veja algumas opções no site *http://eriberto.pro.br/forense*).
- Montar a partição do HD adicional em */mnt*. NÃO monte qualquer partição da mídia a ser periciada.
- Com o comando *dd* ou com *dcfldd*, criar a imagem e, depois, calcular dois hashes da imagem, sendo um, obrigatoriamente, do tipo SHA2.
- Um exemplo de sintaxe do *dd*, considerando a mídia a ser periciada como sendo o HD SATA */dev/sda*:

```
# dd if=/dev/sda of=/mnt/sda.dd
# md5sum /mnt/sda.dd > /mnt/sda.dd.md5
# sha256sum /mnt/sda.dd > /mnt/sda.dd.sha256
```


- Prefira *dcfldd* (mais rápido e mostra andamento):

```
# dcfldd if=/dev/sda of=/mnt/sda.dd hash=md5,sha256
  md5log=/mnt/sda.dd.md5 sha256log=/mnt/sda.dd.sha256
```

- No caso de mídias danificadas (bad blocks, CDs com defeito etc), utilize *rdd*, *ddrescue* ou *gddrescue*.

7. Procedimentos finais

- Lacrar o a mídia original na presença de duas testemunhas, utilizando lacres numerados.
- Gerar um *certificado de integridade*, em três vias, referente às mídias (incluindo memória), com os dados:
  - nome e CPF do perito e das testemunhas;
  - número de série dos discos e pendrives a serem (colher em etiquetas ou no log */var/log/syslog*);
  - hashes obtidos (incluindo memória, se for o caso);
  - números dos lacres;
  - foto da mídia lacrada;
  - assinatura do perito e das testemunhas.
- Enviar as mídias lacradas e duas vias do certificado de integridade para a autoridade ou pessoa interessada.
- Capturar dados gerais da máquina com *lshw* e *hwinfo*.

8. Cuidados extras com as imagens

- Caso haja a necessidade de montar alguma imagem, faça-o somente no modo read-only.
- Sempre trabalhe em uma cópia de cada imagem.

9. Coleta de dados via rede

Algumas vezes será necessário enviar dados para outra máquina, via rede. Um exemplo disso é uma máquina virtual sem acesso a pendrive. Utilize *netcat*. Um exemplo de coleta do resultado do comando *free* via rede:

- Máquina destino: `# nc -l -p 53000 > free`
- Máquina periciada: `# free -m | nc <ip_dest> 53000`

Perícia Forense Computacional

"Guia de referência rápida"

PERÍCIA LINUX COM DEBIAN GNU/LINUX

Parte 1:
Procedimentos iniciais e coletas

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. Orientações aos gerentes de rede em casos de invasão

- Ao detectar uma invasão, não emita comandos na máquina comprometida.
- Desconecte imediatamente o cabo de rede.
- NUNCA desligue a máquina se o atacante não o tiver feito remotamente.
- Não ligue a máquina, caso tenha certeza da invasão e a mesma esteja desligada. Se ligoudo a máquina e detectou a invasão, não a desligue e não mexa mais.
- Chame imediatamente um perito forense.
- Acompanhe o trabalho do perito.

3. Orientações às autoridades ao apreender máquinas suspeitas

- Se a máquina estiver ligada no momento do flagrante e houver possibilidade, chame um perito forense para realizar um dump de memória. Isso ajudará muito nas investigações, pois há dados preciosos na memória, incluindo senhas.
- Para remover a máquina do local, lacre a mesma, dentro de uma caixa ou saco apropriado, na presença de duas testemunhas. Utilize lacres confiáveis, seguros e numerados.

4. Medidas iniciais nas forenses (somente para máquinas vivas)

A seguir, serão mostradas as medidas iniciais, a serem adotadas por peritos forenses, ao tomar o primeiro contato com a máquina comprometida, caso a mesma ainda esteja ligada. **Todos os procedimentos deverão ser realizados na presença de duas testemunhas.**

- Inserir uma mídia externa (pendrive ou HD) de maior capacidade do que a memória RAM para colher dados.
- Logar como root na máquina comprometida e montar o dispositivo USB em */mnt*, por exemplo.
- Executar, de imediato, um dump de memória, gravando-o na mídia externa (veja o item *5. Dump de memória*). Esta tem que ser a primeira ação.

Colher os seguintes dados:

- Os usuários logados no momento:
```
# w > /mnt/w
```
- Histórico de comandos na memória:
```
# history > /mnt/history
```
- Situação de uso de memória:
```
# free -m > /mnt/free
```
- Relação de processos ativos:
```
# ps aux > /mnt/ps
```
- Lista de possíveis processos ocultos*:
```
# unhide proc > /mnt/unhide.proc
# unhide sys > /mnt/unhide.sys
# unhide brute > /mnt/unhide.brute
```
- Lista de possíveis portas de rede ocultas*:
```
# unhide-tcp > /mnt/unhide.tcp
```
- Tempo de vida da máquina:
```
# uptime > /mnt/uptime
```

* Somente se esses comandos estiverem disponíveis. Nunca instale nada em uma máquina viva.

- Conexões e portas de rede abertas:
```
# netstat -tunap > /mnt/netstat
```
- Relação de pacotes instalados (Debian e derivados):
```
# COLUMNS=110 dpkg -l > /mnt/pacotes
```
- Relação de pacotes instalados (RedHat e derivados):
```
# rpm -qa > /mnt/pacotes
```
- Data e hora da máquina, tomando o cuidado de anotar a hora do seu relógio para comparação futura:
```
# date > /mnt/date
```
A defasagem de horário deverá constar no laudo.
- Utilização de discos:
```
# df -hT > /mnt/df
```
- Detalhes sobre dispositivos montados:
```
# mount > /mnt/mount
```
- Esquema de particionamento dos discos:
```
# fdisk -l > /mnt/fdisk
```
- Kernel utilizado:
```
# uname -a > /mnt/uname
```
- Dados básicos de rede:
```
# ifconfig > /mnt/ifconfig
```
- Rotas de rede:
```
# route -n > /mnt/route
```
- Módulos de kernel carregados:
```
# lsmod > /mnt/lsmod
```

Depois de colher os dados:

- Desmontar e remover o dispositivo externo, verificando, em outra máquina, se os dados foram gravados.
- Desligar a máquina, puxando o cabo da tomada.
- Em outra máquina, calcular dois ou mais hashes da imagem, sendo um, obrigatoriamente, do tipo SHA2. As duas testemunhas deverão estar atentas a este passo.
```
# md5sum memoria.dd > memoria.dd.md5
# sha256sum memoria.dd > memoria.dd.sha256
```
- Mostre os hashes obtidos às testemunhas (antes de calcular, explique e demonstre a elas o que é hash).