Aula 07
Forense Computacional

Caso I

Agenda

- ✓ Ler documento;
- ✓ Aplicar os conhecimentos;
- ✓ Responder as questões do caso;

Sistema Linux comprometido

- ✓ O sistema em questão era um honeypot de alta interatividade, que foi comprometido por um atacante, visando ganhar o controle total do sistema através da escalada de privilégios.

- ✓ Inicialmente, vamos entender um pouco mais sobre o sistema comprometido:

  - ✓ O sistema executava uma instalação padrão do Linux Red Hat Server 6.2.
  - ✓ A time zone do sistema estava configurada para GMT-0600 (CST).
  - ✓ Algumas informações foram detectadas e logadas pelo IDS instalado.

Sistema Linux comprometido

- ✓ Para descompactar o arquivo com as imagens:
  # tar xvf challenge-images.tar

- ✓ Para descompactar as imagens coletada:
  # for i in 1 5 6 7 8 9
  > do
  > gunzip honeypot.hda$i.dd.gz
  > done

- ✓ Para montar as imagens precisamos criar os pontos de montagem:
  # mkdir /d1
  # mkdir /d1/boot
  # mkdir /d1/home
  # mkdir /d1/usr
  # mkdir /d1/var

Sistema Linux comprometido

- ✓ Montagem das imagens:

```
# mount -o ro,loop,nodev,noexec honeypot.hda8.dd /d1
# mount -o ro,loop,nodev,noexec honeypot.hda1.dd /d1/boot
# mount -o ro,loop,nodev,noexec honeypot.hda6.dd /d1/home
# mount -o ro,loop,nodev,noexec honeypot.hda5.dd /d1/usr
# mount -o ro,loop,nodev,noexec honeypot.hda7.dd /d1/var
```

Sistema Linux comprometido

- ✓ "ils" e "ils2mac" foram usados para obter os horário de MAC de exclusão dos inodes nas partições 1, 5, 6, 7 e 8. Os arquivos resultantes foram então combinados com os valores obtidos através da execução do "grave-robber“ contra o sistema de arquivos raiz em "/d1", para incluir os inodes excluídos juntamente com os inodes ativos.

```
# grave-robber -c /d1 -m -d . -o LINUX2
# for i in 1 5 6 7 8
> do
> ils honeypot.hda$i.dd | ils2mac > hda$i.ilsbody
> done
# ls -l *body
```

Sistema Linux comprometido

- ✓ "ils" e "ils2mac" foram usados para obter os horário de MAC de exclusão dos inodes nas partições 1, 5, 6, 7 e 8. Os arquivos resultantes foram então combinados com os valores obtidos através da execução do "grave-robber" contra o sistema de arquivos raiz em "/d1", para incluir os inodes excluídos juntamente com os inodes ativos.

```
# grave-robber -c /d1 -m -d . -o LINUX2
# for i in 1 5 6 7 8
> do
> ils honeypot.hda$i | ils2mac > hda$i.ilsbody
> done
# ls -l *body
```

Sistema Linux comprometido

Depois que visualizamos os arquivos gerados, vamos organizá-los melhor:

```
# for i in 1 5 6 7 8
> do
> cat hda$i.ilsbody >> body-deleted
> done
# cat body body-deleted > body-full
# mactime -p /d1/etc/passwd -g /d1/etc/group -b body-full \11/06/2000 >
mactime.txt
# pico mactime.txt
```

- ✓ Recuperação, verificação e visualização de arquivo apagado:

```
# icat honeypot.hda8.dd 8133 > foo
# file foo
# tar -tvf foo
# tar -xvf foo
```

<Analisar os arquivos recuperados>

Sistema Linux comprometido

- ✓ O script de instalação para o bot eggdrop foi encontrado, enquanto buscando por arquivos deletados:

  # grep -i " tpack " *
  # less `grep -i " tpack " * | awk '{print $3;}'`

- ✓ Após o carregamento do arquivo .tar, o invasor parece desempacotar outro arquivo tar no diretório “/d1/usr/man/.Ci”. Isso é possível verificar no mactimes.txt.

- ✓ Há, inclusive uma cópia do “inetd” encontrada no diretório .Ci, que difere do utilizado pelo sistema real da máquina comprometida:

  # md5sum /d1/usr/sbin/inetd /t/usr/man/.Ci/inetd

Sistema Linux comprometido

- ✓ Logo em seguida, o invasor cria um link do .bash_history tanto do "/" quanto do "/root" para o "/dev/null", numa tentativa de desabilitar o log history.

- ✓ Seguindo adiante, podemos encontrar uma lista os arquivos em /d1/usr/man/.Ci que foram criados ou executados pelo invasor.

- ✓ Isso mostra a substituição dos seguintes arquivos do sistema operacional, pelas versões de um rootkit com cavalo de tróia: ls, ps, netstat, tcpd e top.

- ✓ Executando o comando "strings" no arquivo "/d1/bin/ls", é exibido o nome do arquivo e configuração do rootkit "/usr/man/r".

<Analisar arquivo>

Sistema Linux comprometido

- ✓ Já o programa "snif" que podemos ver pelo mactimes.txt dentro do "./Ci" é o sniffer linsniff. O mesmo foi executado, mas o sniffer não conseguiu logar nenhuma conexão.

- ✓ De acordo com o mactimes, as *06:53:06*, o invasor instalou um servidor SSH, gerou um novo par de chaves pública/privada, e modificou o arquivo *"/d1/etc/rc.d/rc.local"* finalizando-o com a linha *"/usr/local/sbin/sshd1"* (iniciando o daemon em cada reboot). E finalmente podemos ver o daemon do ssh1 iniciado.

- ✓ O inode deletado com a propriedade *1010/users* suspeito.

Após recuperado, encontramos o script de instalação do sshd:

 # icat honeypot.hda5.dd-dead-109802 > 1010_users
 # file 1010_users
 # cat 1010_users