

Procedimentos e Ferramentas para Manutenção de Honeypots de Alta Interatividade

Lucio Henrique Franco, Antonio Montes

{lucio,montes}@lac.inpe.br

**Laboratório Associado de Matemática
e Computação Aplicada
Instituto Nacional de Pesquisas Espaciais**

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



Roteiro

- Conceitos
- Taxonomia dos Honeypots
- Procedimentos desenvolvidos
- Instalação dos Honeypots
- Acompanhamento dos Honeypots
- Desativação dos Honeypots
- Ferramentas Desenvolvidas
- Trabalhos Relacionados
- Trabalhos Futuros
- Conclusão

Conceitos

- *Honeypots*
 - *São recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades*
- *Honeynets*
 - *São ferramentas de pesquisa que consistem de uma rede projetada especificamente para ser comprometida. Elas contêm mecanismos de captura, análise e contenção de tráfego e partem do princípio que todo este tráfego é considerado malicioso*

Finalidades dos Honeypots e Honeynets

- Coleta de códigos maliciosos
- Identificar varreduras e ataques automatizados
- Acompanhamento das vulnerabilidades
- Motivação dos atacantes
- Correlação de informações com outras fontes
- Auxílio aos sistemas de detecção de intrusão
- Manter atacantes afastados de sistemas importantes

Taxonomia dos Honeypots

Baixa Interatividade	Alta Interatividade
Emulam sistemas e serviços	Executam as versões reais
Simples. Fácil gerenciamento	Cuidados na instalação e configuração. Coleta de artefatos
Atacante não deve ter controle	Pode ter controle total
Ações limitadas, captura de tráfego e malware	Captura de mais informações, incluindo ferramentas e comandos
Difíceis de iludir atacantes avançados/determinados	Difícil de distinguir de um sistema de produção

Projeto HoneyNet.BR

- O Projeto HoneyNet.BR utiliza honeypots de alta interatividade sendo eles de várias arquiteturas e executando diversos sistemas operacionais
- Gerência complexa, não se deve deixar vestígios na sua preparação
- Deve possuir mecanismos de captura e preservação dos dados
- Desenvolvimento de procedimentos e pradronizações para administrar grande número de honeypots
- Documentação e histórico dos sistemas

Instalação dos Honeypots

- Padronização dos passos corretos a serem executados
 - Define-se o sistema operacional, os serviços e suas versões
 - Disco tem o seu conteúdo zerado
 - Instala-se o sistema operacional e configura-se os seus serviços
 - Execução de diversos scripts para criação de usuários, gerenciamento de logs, etc

Instalação dos Honeypots

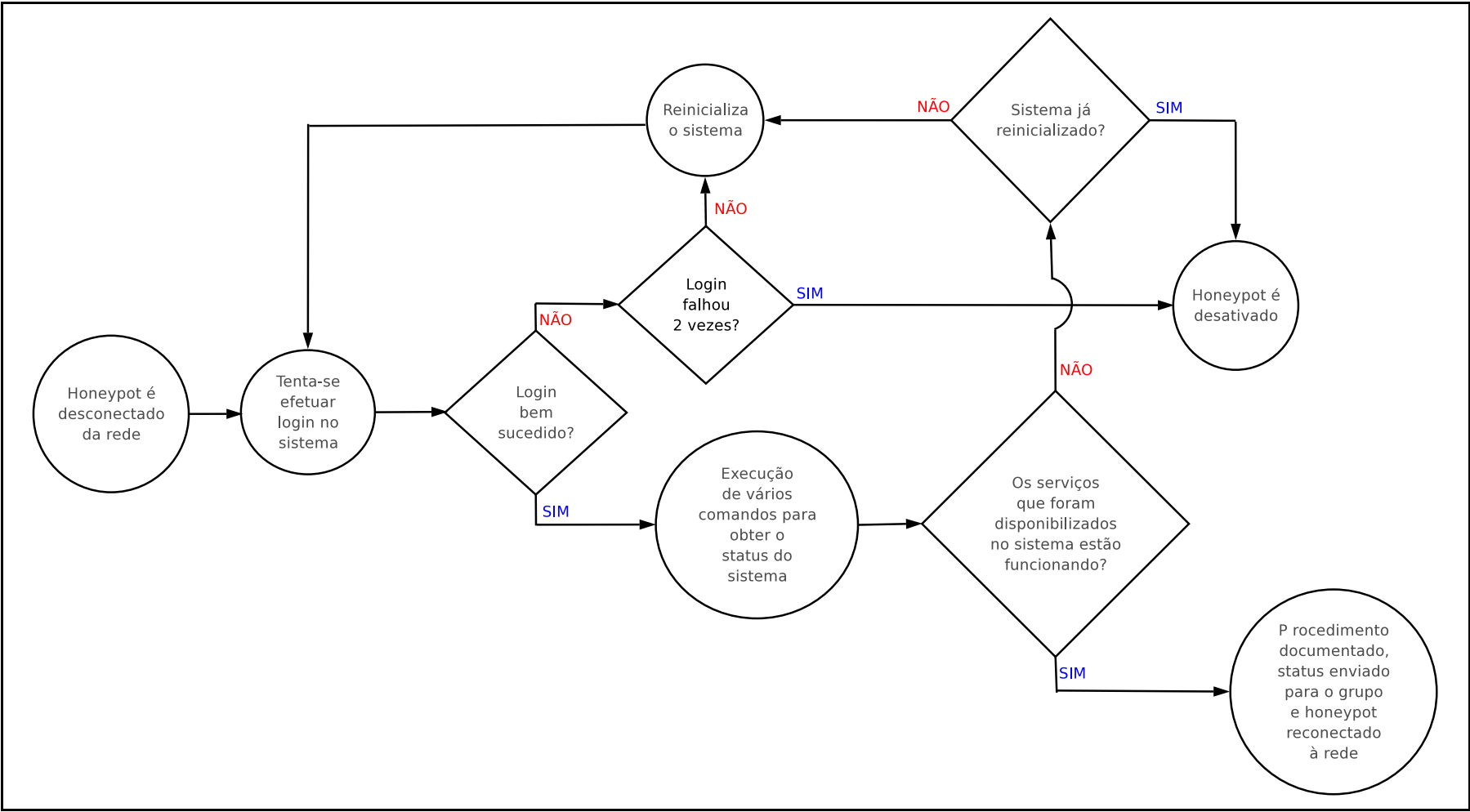
- Configura-se o sistema de captura de teclas
- Realiza a geração do hash MD5 de todos os arquivos e geração do status do sistema
- Gera-se a imagem do disco
- Documenta-se as atividades realizadas em um livro de registros

Padronizações na Instalação dos Honeypots

- As partições devem ser inferiores a 2GB e se possível utilizar, somente, a partição /
- Forma de armazenamento das imagens e status:

```
/foobar_windows2000server/  
  install1/  
    image_15_03_2004_foobar_orig/  
    image_15_04_2004_foobar_hack/  
    status_15_03_2004_foobar_orig/  
    status_15_04_2004_foobar_hack/  
  install2/  
    image_18_04_2004_foobar_orig/  
    status_19_04_2004_foobar_orig/
```

Acompanhamento dos Honeypots



Desativação dos Honeypots

- Login no console ou através de uma distribuição Linux ou pelo sistema operacional OpenBSD
- Realiza a coleta e análise do status do sistema comprometido
- É feita a imagem da máquina comprometida
- O host é liberado para ser preparado e configurado novamente como um honeypot
- São feitos estudos e análise forense sobre as imagens e sobre o tráfego de rede coletado referente a este honeypot

Ferramentas Desenvolvidas

- Forma de automatização dos procedimentos a serem seguidos
- Vem sendo desenvolvidas e empregadas para sistemas Unix, Windows e Linux
- São desenvolvidas em sua maioria em shell script

Gerador de Hash MD5

- Gera o hash MD5 de todos os arquivos num dado diretório; incluindo arquivos de subdiretórios com a compressão do arquivo final gerado
- Exemplo de uma possível adaptação da ferramenta:

```
#!/bin/bash
ARGS="$1"0
if [ $ARGS == "0" ]; then
    echo "usage: $0 directory"; exit 1;
fi
RESULT=`uname -n`_${1}_md5;
RESULT=`echo $RESULT | sed -e 's/\\//_/g' `
find $1 -type f -exec md5sum {} \; >> $RESULT
gzip $RESULT
```

Ferramenta para Remoção Segura

```
#!/bin/bash
ARGS="$1"0
if [ $ARGS == "0" ];
then
    echo "usage: $0 directory"; exit 1;
fi
for i in `find $1 -type f`; do
    tam=`ls -l ${i} | awk -F' ' '{print $5}'`;
    dd if=/dev/zero of=${i} bs=1 count=$tam;
    rm -f ${i};
done
rm -rf $1
```

Configurações Gerais dos Honeypots

- Framework de todos os procedimentos descritos
- Desenvolvido em módulos e permite a seleção de comandos a serem executados
- Executa os principais passos, como:
 - **Criação das contas e senhas dos usuários**
 - **Instalação dos mecanismos de coleta de logs**
 - **Instalação do mecanismo de sincronização de tempo**
 - **Remoção segura dos arquivos fontes instalados**
 - **Geração do hash MD5 do sistema**
 - **Geração do status do sistema**
 - **Geração da imagem do disco e compressão das partições**

Configurações Gerais dos Honeypots



Acompanhamento dos Honeypots

- Visa manter os honeypots o menor tempo possível inativo
- Faz uso de um CD que contém binários estáticos de diversos sistemas
- Executa-se os comandos definidos no próprio script, dentre eles:
 - `hostname, df -h, w, last, netstat -na, ps -auwx, vmstat, rpcinfo -p 0, lsof, socklist, uptime, printenv`
- É criado um diretório que conterá a saída desses comandos

Acompanhamento dos Honeypots

- **Resumo da saída do arquivo gerado:**

```
$cat /mnt/floppy/15_03_2004/hp1
```

```
### STATIC BINS ###
```

```
### hostname ###
```

```
hp1
```

```
### df -h ###
```

```
Filesystem  Size  Used Avail Capacity  Mounted on  
/dev/hda1  1.4G  0.8G  0.6G    75%    /
```

```
### w ###
```

```
11:07:24 up 3 days, 21:05, 1 user, load average: 0.00, 0.04, 0.36
```

```
USER  TTY  FROM  LOGIN@  IDLE   JCPU   PCPU   WHAT  
root  tty1  -     8:47am  2:19m  0.35s  0.02s  /bin/sh
```

Trabalhos Relacionados

- Há diversas ferramentas como, por exemplo, a `md5deep` ^{*a*}, a `shred` pertencente ao pacote `fileutils` ^{*b*} ou o comando `rm -P` que podem auxiliar na geração do hash MD5 ou na remoção segura de arquivos, porém, elas não oferecem a mesma portabilidade e integração com outros sistemas e/ou scripts

^{*a*}<http://md5deep.sourceforge.net/>

^{*b*}<ftp://ftp.gnu.org/gnu/fileutils/>

Trabalhos Futuros

- Revisões e aprimoramentos constantes
- Desenvolvimento para outros sistemas operacionais
- Migração do MD5 para SHA1
- Nos sistemas Windows, substituição do `cygwin` para o conjunto de ferramentas GNU ^a de mesma funcionalidade
- Desenvolvimento de um comando `rm` adaptado
- Caso haja necessidade, criação ou migração dos scripts para outras linguagens

^a<http://unxutils.sourceforge.net/>

Conclusão

- A criação de metodologias, procedimentos e o desenvolvimento de ferramentas para a configuração de um honeypot de alta interatividade é de grande relevância porque automatizam processos e auxiliam na coleta de informações
- Os padrões passam a ser conhecidos e seguidos por todos do grupo na tentativa de evitar erros
- As ferramentas vem sendo desenvolvidas e empregadas ao longo do tempo e o acompanhamento das honeynets, desde então, mostrou a utilidade do desenvolvimento dessas para automatizar a configuração de um honeypot, seus ajustes e refinamentos