Grupo de Resposta a Incidentes de Segurança

Introdução a Honeypots

O que são Honeypots?

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."
Lance Spitzner

- Honeypots são recursos que não tem qualquer valor de produção.

- Em tese, como não tem atividades legítimas não deve ter tráfego e, por isso, qualquer interação pode ser considerada não autorizada ou maliciosa.

O que são Honeypots?

Quais as vantagens de um honeypot?

- Pequena quantidade de informação com grande valor e facilidade de análise. Grandes honeypots bem configurados geram 1MB de dados e 10 alertas por dia.

- São preparados para capturar qualquer coisa que passe por eles, sejam ferramentas ou taticas inovadoras.

- Requerem recursos mínimos de hardware. Um velho Pentiun 233 com 128MB suporta uma rede de classe B inteira com facilidade.

- Simplicidade. Não precisam de algoritmos sofisticados, manutenção de tabelas ou atualização de assinaturas.

O que são Honeypots?

Por outro lado, só podem capturar as informações enviadas diretamente à eles. O tráfego precisa passar pelo honeypot para que seja possível extrair alguma informação.

São suscetíveis a falhas, mais específicamente, podem ser comprometidos e subvertidos. Como em qualquer tecnologia de segurança existem riscos, é possível que um atacante anule as proteções e subverta o honeypot.

Tipos de Honeypots

Existem três tipos básicos de honeypot

- baixa interatividade
- alta interatividade
- média interatividade

A interação define que nível de atividade é passível de utilização.

Tipos de Honeypots

Honeypots de baixa interatividade são ferramentas instaladas para emular sistemas e serviços. Por isso, o sistema operacional real deve ser instalado e configurado de forma segura para diminuir os seus riscos.

Características
- Fácil implementação e manutenção
- Baixo risco de comprometimento
- Informações capturadas são muito limitadas
- Capturam apenas atividades conhecidas
- Sua detecção é relativamente fácil

Exemplos de ferramentas: Specter, Honeyd, KFSensor

Tipos de Honeypots

Como funciona o Honeyd?

- Quando detecta uma tentativa de conexão a um IP não utilizado, o honeyd intercepta a conexão e interage com o atacante como se fosse a vítima.

- Por padrão qualquer conexão em portas TCP ou UDP é detectada e é gerado um log.

- Além disso, é possível configurar o monitoramento de portas específicas. Desta forma, toda a interação com o serviço emulado é capturada.

- Pode se fazer passar, por exemplo, por um roteador CISCO, um XP Server ou um Linux DNS Server.

Tipos de Honeypots

Exemplo de log do Honeyd

```
Microsoft Windows XP Professional SP1
or Windows 2000 SP3
        ( / 10.0.0.72 / )
        139/tcp
        137/tcp
        135/tcp
        445/tcp
        593/tcp
        6129/tcp
        4444/tcp
        137/udp
        135/udp
        445/udp

------------------------------------
Connection Counter
------------------------------------
Total:         10
  TCP:          4
  UDP:          2
 ICMP:          4
------------------------------------
```

```
------------------------
Honeypot: 10.0.0.71
------------------------------------
Source IP        Resource  Connections
192.168.100.130     21/tcp       1
192.168.131.157    11/icmp       1
192.168.139.133    11/icmp       1
------------------------------------
IPs              Resources  Connections
3                      2        3
------------------------------------
------------------------------------
Honeypot: 10.0.0.72
------------------------------------
Source IP        Resource  Connections
192.168.100.130     21/tcp       1
192.168.207.84      53/udp       1
192.168.217.41      53/udp       1
------------------------------------
IPs              Resources  Connections
3                      2        3
------------------------------------
```

Tipos de Honeypots

Exemplo de log do Honeyd

Top 10 Source Hosts

Rank	Source IP	Connections
1	192.168.100.130	3
2	192.168.139.133	2
3	192.168.50.20	1
4	192.168.131.157	1
5	192.168.217.41	1
6	192.168.207.84	1
7	192.168.177.253	1

Top 10 Accessed Resources

Rank	Resource	Connections
1	21/tcp	4
2	11/icmp	4
3	53/udp	2

Top 10 ICMP > 40 bytes Senders

Rank	Source IP	Connections
1	192.168.139.133	2
2	192.168.131.157	1
3	192.168.177.253	1

Connections per Hour

Hour	Connections
00:00	1
01:00	1
02:00	3
03:00	0
04:00	0
05:00	0
06:00	0
07:00	4
08:00	0
09:00	0
10:00	0
11:00	0
12:00	0
13:00	0
14:00	0
15:00	0
16:00	1
17:00	0
18:00	0
19:00	0
20:00	0
21:00	0
22:00	0
23:00	0

Tipos de Honeypots

Os honeypots de alta interatividade são sistemas reais, com aplicações e serviços reais onde o atacante interage diretamente com eles.

Características
- Grande quantidade de informação capturada
- Pode detectar tecnicas não conhecidas
- Captura todas as interações, previstas ou não
- Alto risco de comprometimento
- Dificil implementação e manutenção
- Precisa de mecanismos de contenção

Exemplos de ferramentas: Symantec Decoy Server e Honeynets

Tipos de Honeypots

Como funciona o Honeynets?

- É uma arquitetura de rede desenhada para controlar todas as interações usando maquinas reais como vítimas.

- São capturados desde sessões SSH até e-mails e arquivos baixados apenas com a instalação de módulos do kernel nas vítimas.

- Usa o Honeywall Gateway, que permite o inbound mas controla o outbound

Tipos de Honeypots

Honeypots de media interação são o meio termo entre baixa e alta. Eles continuam emulando os sistemas e serviços mas a quantidade de dados extraídos, sem que se tenha a exposição da alta interatividade, é substancialmente maior.

Em contra partida, seus riscos são um pouco mais elevados do que em um de baixa interação

Por que usar um Honeypot?

Os honeypots são usados, basicamente, com duas finalidades:

- produção
- pesquisa

Em geral, honeypots de baixa interação são usados para produção e os de alta interação para pesquisa.

Honeypots servindo ao propósito de pesquisa são usados para coletar informações como tendências ou novas trends.

Um exemplo de honeypot de pesquisa é o Honeynet Project

Por que usar um Honeypot?

Os honeypots com propósito de produção podem ser divididos em três áreas distintas:

- prevenção
- detecção
- resposta

Para as funções de prevenção e detecção é mais comum utilizar honeypots de baixa interação enquanto um de alta interação é mais usado para resposta. Isso se deve ao fato de que são necessárias informações mais detalhadas para responder a um incidente.

Por que usar um Honeypot?

Honeypots para Prevenção:

- Focado em ataques automáticos como worms e port scan.
- Podem confundir o atacante e restringir suas ações apenas ao honeypot.
- Monitoram uma faixa de IP não utilizada, quando detectam atividade interagem e retardam o atacante. Em alguns casos é possível parar o ataque.
- Um exemplo de ferramenta para esse fim é o LaBrea Tarpit e Deception Toolkit

Por que usar um Honeypot?

Honeypots para Detecção:

- Uma vez detectado o ataque, é possível reagir a ele impedindo que prossiga ou, pelo menos, mitigando os danos.

- As quantidades de falsos positivos são reduzidas devido à qualidade das informações geradas.

- São capazes de trabalhar com encriptação e em ambientes IPv6

Por que usar um Honeypot?

Honeypots para Resposta:

- Podem ser retirados da rede para sofrem analise forense de forma rápida e fácil.

- São muito fáceis de analizar, visto que toda interação pode ser considerada maliciosa.

- Produz as informações necessárias para responder ao incidente de forma rápida e eficiente.

Honeypots dinâmicas

- Honeypot dinâmica é um “sistema” que automaticamente determina quantos honeypots são necessários, como serão implementados e com que sistemas se parecerão.

- Se adaptam às características da rede em que estão “plugados”

- Utilizam fingerprint para detecção de sistemas

Honeytokens

- São recursos cujo valor está no seu uso não autorizado.

- Ao contrário dos honeypots, eles não são computadores. São qualquer tipo de entidade digital, como um número de cartão, um apresentação powerpoint, uma base de dados ou um login.

- Um honeytoken trabalha de forma exatamente igual ao honeypot. Qualquer acesso pode ser considerado não autorizado ou malicioso.

- Não precisa de algoritmos sofisticados, assinaturas atualizadas ou regras para configurar.

Honeyclients

- Honeyclient se passa por um cliente normal e interage com o servidor para analizar as suas ações

- É comum encontrarmos honeyclients na forma de navegadores, entretanto, qualquer tipo de cliente que interage com o servidor pode ser utilizado.

- Exemplos de honeyclient são MITRE HoneyClient, Shelia, Honeymonkey e CaptureHPC

Como detectar Honeypots

- Qualquer honeypot pode, eventualmente, ser detectado.
- Existem algoritmos que testam se o sistema está em máquina virtual.
- Versões antigas do Honeyd, por exemplo, respondiam a um pacote SYN com um SYN/ACK sem nenhuma opção.

Projeto Milhouse

Referências

- Honeypots – por Lance Spitzner
http://www.tracking-hackers.com/papers/honeypots.html

Honeypots – A Segurança Através do Disfarce
http://gris.dcc.ufrj.br/artigos/GRIS-2006-A-001.pdf

- Dynamic Honeypots
http://www.securityfocus.com/infocus/1731

- Honeytokens: The Other Honeypot
http://www.securityfocus.com/infocus/1713

- A Guide to Diferent Kinds of Honeypots
http://www.securityfocus.com/print/infocus/1897

Dúvidas?

Obrigado!