Microcurso:
Honeypots e Honeynets

Antonio Montes*
Cristine Hoepers†
Klaus Steding-Jessen†

*Instituto Nacional de Pesquisas Espaciais – INPE
Ministério da Ciência e Tecnologia

†NIC BR Security Office – NBSO
Comitê Gestor da Internet no Brasil

Roteiro

- Definições
- Histórico e aplicações
- Projetos em andamento
- Honeypots de baixa interatividade
- Honeynets

Definição

- 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.

Histórico

Primeiras publicações

- Clifford Stoll – *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (1989); Sistema não havia sido preparado para ser invadido. Discrepância de US$0,75 na contabilidade do sistema deu início à monitoração do invasor.

- Bill Cheswick – *An Evening with Berferd in Which a Cracker is Lured, Endured, and Studied* (1992); Sistema preparado para ser invadido, visando o aprendizado. Foram utilizados emuladores de serviços e ambientes chroot'd.

Histórico (cont.)

- Lance Spitzner – *Learning the Tools and the Tactics of the Enemy with Honeynets* (2000);
  Descrição de uma rede especialmente preparada para ser comprometida, início do Projeto Honeynet.

Outras Ferramentas

- Deception Toolkit (1997)
- CyberCop Sting (1998)
- NetFacade (1998)
- BackOfficer Friendly (1998)
- Honeynet Project (1999)
- Honeyd (2002)

Aplicações

- Honeynets de Pesquisa são ferramentas de pesquisa que podem ser utilizadas para observar o comportamento de invasores, permitindo análises detalhadas de suas motivações, das ferramentas utilizadas e vulnerabilidades exploradas.
- Honeypots de Produção podem ser utilizados em redes de produção como complemento ou no lugar de sistemas de detecção de intrusão.

Prós & Cons

- Tradicionalmente segurança sempre foi sinônimo de defesa passiva, honeypots e honeynet provocaram uma mudança de postura, permitindo maior pró-atividade por parte dos administradores;
- Grande vantagem: são instalados de maneira que todo tráfego destinado a um honeypot é anômalo ou malicioso, sem falsos-positivos, dados de alto valor;
- Grande desvantagem: só vê tráfego destinado a ele, introduz um risco adicional.

Tipos de Honeypots

- Alta ou baixa interatividade.
- Baixa interatividade:
  - Emula serviços;
  - Por serem relativamente seguros, são apropriados para redes de produção;
  - Excelentes complementos para SDI.

Tipos de Honeypots (cont.)

- Alta interatividade
  - Serviços legítimos;
  - 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.

Honeynet.BR

- Início do projeto em dezembro de 2001, entrou em operação em março de 2002;
- Arquitetura consiste numa rede administrativa, formada por um firewall (pf) operando em modo bridge e um sistema de detecção de intrusão on-line (hogwash). O firewall registra todo o tráfego e limita a banda de saída. A honeynet é composta de várias máquinas rodando diferentes sistemas operacionais e serviços.

Honeynet.BR (cont.)

- Desenvolvimento de Metodologias e Ferramentas para a Implantação, Controle e Monitoração de Honeynets;
- Desenvolvimento de Metodologias e Ferramentas para a Análise das Informações Colhidas em Honeynets e seu uso na Resposta a Incidentes de Segurança;
- Desenvolvimento de Metodologias e Ferramentas para o Registro de Atividades em Máquinas Invadidas;
- Desenvolvimento de Metodologias e Ferramentas para o Redirecionamento de Ataques;

Honeynet.BR (cont.)

- Artigo apresentado na *15th Annual Computer Security Incident Handling Conference* (FIRST), Ottawa, Canadá, June 22-27, 2003;
- Curso *hands-on* apresentado na Universidade Groningen, Holanda, Outubro, 6-10, 2003.
- Rede de Honeypots Distribuídos.

Honeypots Distribuídos

- Rede de honeypots de baixa interatividade com o objetivo de cobrir o maior número de AS da Internet brasileira;
- Atualmente em fase de implantação em diversas redes acadêmicas e de pesquisa do País:
  - 14 instituições, cobrindo mais de 1500 IPs;
- Usa o aplicativo Honeyd para emular diferentes sistemas operacionais e serviços de rede;
- Logging centralizado.

Honeypots Distribuídos (cont.)

- Além de servir como complemento do SDI (ataques internos, falsos positivos);
- Permite levantar tendências, coletar artefatos, fontes de ataques, etc;
- Apoio à atuação de grupos de resposta a incidentes.

Honeypots de Baixa Interatividade

Características

- Emulam algumas partes de serviços e sistemas
  - não existe serviço real a ser atacado
  - sucesso depende da qualidade do emulador
- O atacante não tem acesso ao sistema operacional real
- O atacante não pode comprometer o honeypot (em tese)
- Adequados para redes de produção

Riscos

- Ocorrer o comprometimento
  - do sistema operacional
  - do software do honeypot
- Atrair atacantes para a rede onde está o honeypot

Quando Usar

- Não há pessoal e/ou hardware disponível para manter uma honeynet
- O risco de um honeypot de alta interatividade não é aceitável
- Detecção de ataques internos

Quando Usar (cont.)

Tem-se o propósito de:

- identificar varreduras e ataques automatizados
- identificar tendências
- manter atacantes afastados de sistemas importantes
- coletar assinaturas de ataques
- coletar código malicioso

Listeners

- Propósito:
  - fechar o *three-way handshake*
  - registrar as atividades
- Basicamente dois tipos:
  - apenas estabelecem a conexão
  - entendem o protocolo (http, ftp, etc)
- Podem ser executados *standalone* ou via honeyd

Honeyd

"A framework for virtual honeypots, that simulates virtual computer systems at the network level."

Niels Provos,

Honeyd: A Virtual Honeypot Daemon

Características do Honeyd

- Simula sistemas, executando em espaços de endereçamento não alocados
- Simula diversos hosts virtuais ao mesmo tempo
- Permite a configuração de serviços arbitrários
- Simula um SO no nível de pilha do TCP/IP
  - Engana o `nmap` e o `xprobe`
- Suporta redirecionamento de um serviço

Características do Honeyd (cont.)

- Suporta somente os protocolos TCP, UDP e ICMP
- Recebe o tráfego de rede:
  - Utilizando proxy ARP (`arpd`)
  - Através de roteamento específico para os endereços IP virtuais

Onde Obter o Honeyd

- Honeyd

  http://www.honeyd.org/

  http://www.citi.umich.edu/u/provos/honeyd/

- Honeyd: A Virtual Honeypot Daemon (Extended Abstract)

  http://niels.xtdnet.nl/papers/honeyd-eabstract.pdf

Honeynets

Definição de Honeynets (1)

"Honeynets são ferramentas de pesquisa que consistem de uma rede projetada especificamente para ser comprometida, com mecanismos de controle que impedem que esta rede seja usada como base para lançar ataques contra outras redes."

Cristine Hoepers, Klaus Steding-Jessen, Antonio Montes,
Honeynets Applied to the CSIRT Scenario

Características

- Redes com múltiplos sistemas e aplicações
- Possuem mecanismos robustos de contenção
- Possuem mecanismos de captura de dados e geração de alertas
- Não haver poluição de dados
  - somente tráfego gerado por "*blackhats*", sem testes ou tráfego gerado pelos administradores

Requisitos

Mecanismos de Contenção:

- Devem conter ataques partindo da honeynet para outras redes
- Precisam ser transparentes para o atacante
  - nem sempre iludem atacantes avançados
- Precisam deixar o atacante trabalhar
  - fazer download de ferramentas, conectar no IRC, etc
- Deve ter múltiplas camadas de contenção para prevenir falhas

Requisitos (cont.)

Captura de dados:

- Deve-se capturar o maior número possível de dados
- Prover redundância
- Coleta deve ser feita em diferentes pontos
  - firewall, IDS, honeypots, loghost, etc
- Considerar utilizar um formato conhecido
  - permite o uso de ferramentas populares
  - facilita o desenvolvimento de ferramentas

Requisitos (cont.)

Centralização de dados:

- Necessário em um ambiente distribuído
- Centralizar dados em um único ponto facilita a análise e o armazenamento
- Devem ter mecanismo seguro de transferência de dados

Requisitos (cont.)

Mecanismos de Alerta:

- Devem ser confiáveis
- Podem usar meios diferentes
  - email, pager, celular, etc
- Necessitam de um mecanismo de priorização
- Arquivamento é importante para análise de tendências

Riscos

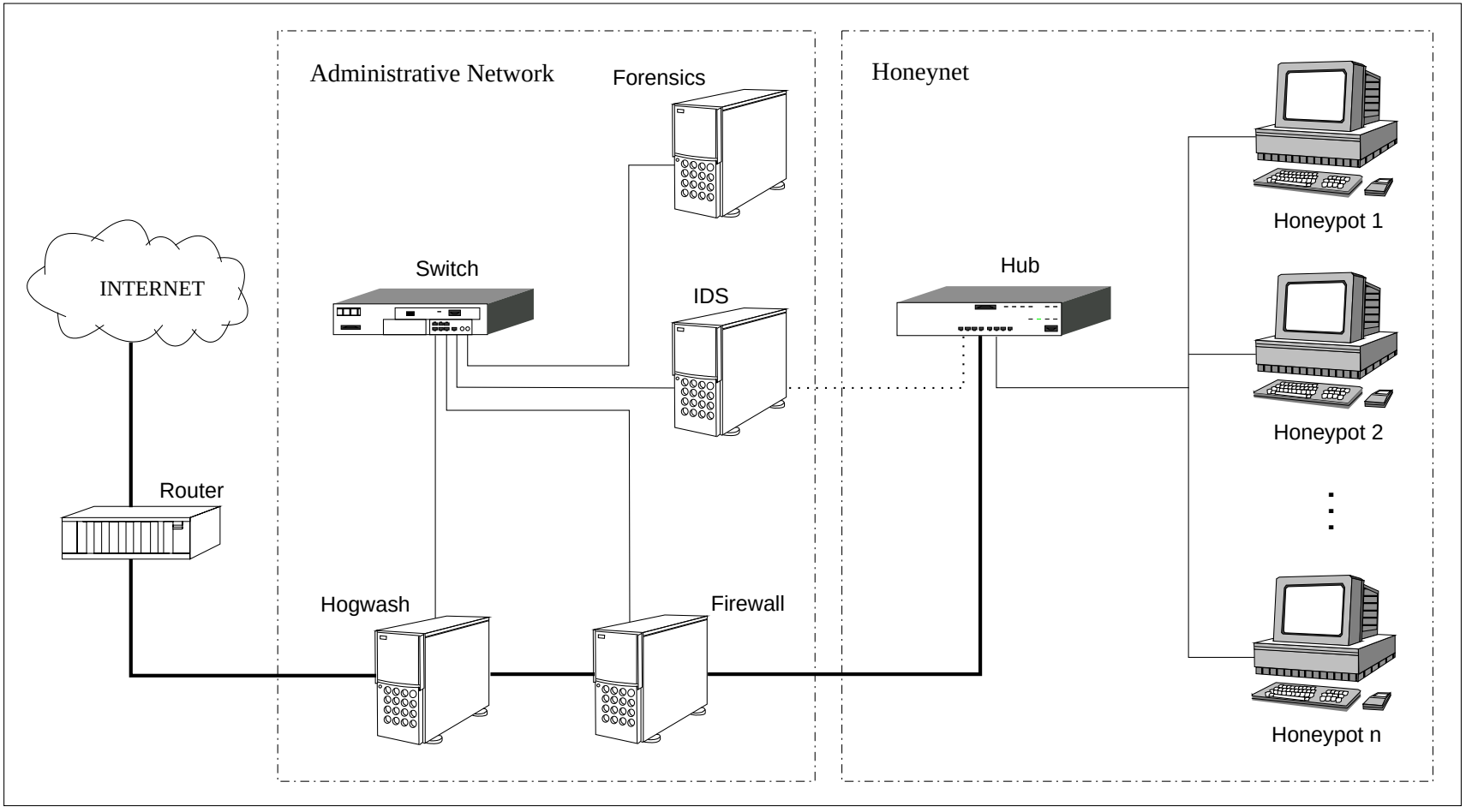
- Um engano na configuração da contenção pode:
  - permitir que a honeynet seja usada para prejudicar outras redes
  - abrir uma porta para a rede de sua organização
- Um comprometimento associado com a organização pode afetar a imagem
- Sua honeynet ser identificada

Riscos (cont.)

Por que é tão arriscado usá-las?

- Nível de interação – o atacante tem controle total da máquina
- São complexas de desenvolver e manter
  - diversas tecnologias atuando em conjunto
  - múltiplos pontos de falha
- Novos ataques e ameaças podem não ser contidos ou sequer vistos

Topologia da Honeynet.BR



Referências

- Honeynet.BR Project

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

- Honeynet Research Alliance

  http://www.honeynet.org/alliance/

- Authors:
  - Cristine Hoepers <cristine@nic.br>
  - Klaus Steding-Jessen <jessen@nic.br>
  - Antonio Montes <montes@lac.inpe.br>