DESVIO DE TRÁFEGO MALICIOSO DESTINADO A REDES DE PRODUÇÃO PARA UMA HONEYNET

Lucio Henrique Franco
lucio@lac.inpe.br

Antonio Montes
montes@lac.inpe.br

Laboratório Associado de Computação e Matemática Aplicada

Instituto Nacional de Pesquisas Espaciais

Av. dos Astronautas, 1758 – 122270-010 – São José dos Campos, SP - Brasil

Apresentação

- Mecanismos de Proteção em Camadas
- Motivação do Trabalho
- *Honeypots* e *Honeynets*
- Propósito do Trabalho
- Descrição do Sistema Proposto
- Arquitetura do Sistema
- Considerações Finais

Mecanismos de Proteção em Camadas

- A segurança de um sistema **não** pode ser garantida por um único mecanismo de defesa
- Política de segurança, senhas e backup, coleta e monitoração de *logs*, utilização de *firewall*, sistemas de detecção de intrusão
- *Firewalls* não bloqueam tentativa de intrusão a serviços de rede para os quais o tráfego é permitido

Mecanismos de Proteção em Camadas

- Intrusão é qualquer ação que tenta comprometer a integridade, a confidencialidade ou a disponibilidade de um recurso computacional
- Comportamento do atacante difere do comportamento de um usuário legítimo

Motivação do Trabalho

- Aplicações geram grande quantidade de registros
- Ataques passam a ser difíceis de serem descobertos
- Não se pode quantificar quantos sistemas foram invadidos e os ataques passam a não serem reportados
- Difícil identificação da origem e motivação dos atacantes

Honeypots e Honeynets

- *Honeypots*
  - Um recurso de segurança preparado especificamente para ser sondado, atacado ou comprometido e para registrar essas atividades
- *Honeynets*
  - São redes compostas de uma sub-rede de administração e de uma sub-rede de honeypots.

Honeypots e Honeynets

Baixa Interatividade	**Alta Interatividade**
Emulam sistemas e serviços	Executam as versões reais
Simples. Fácil gerenciamento	Cuidados na instalação e confi - guração. Coleta de artefatos
Mínimo risco ao ambiente, atacante não tem controle	Alto risco, pode ser usado para disparar ataques
Ações limitadas, captura somente o tráfego	Podem capturar mais informações, incluindo ferramentas, comunicação e comandos

Honeypots e Honeynets

- Coleta de ferramentas
- Acompanhamento das vulnerabilidades
- Troca de informações entre os invasores
- Motivação dos atacantes
- Correlação de informações com outras fontes

Propósito do Trabalho

- Arquitetura de segurança em camadas, o uso de sistemas de detecção de intrusão, *firewall*, uma *honeynet* e um sistema de reconstrução de sessões
- Identificação e desvio de ataques sem interrupção da sessão hostil
- Monitoração dos passos dos atacantes

Propósito do Trabalho

- Desvio de tráfego destinado a portas não disponíveis na rede monitorada
- Provê meios para permitir que o atacante retorne ao sistema comprometido
- Desvio de tráfego de conexões destinadas a portas que não estão disponíveis na rede monitorada.

Descrição do Sistema Proposto

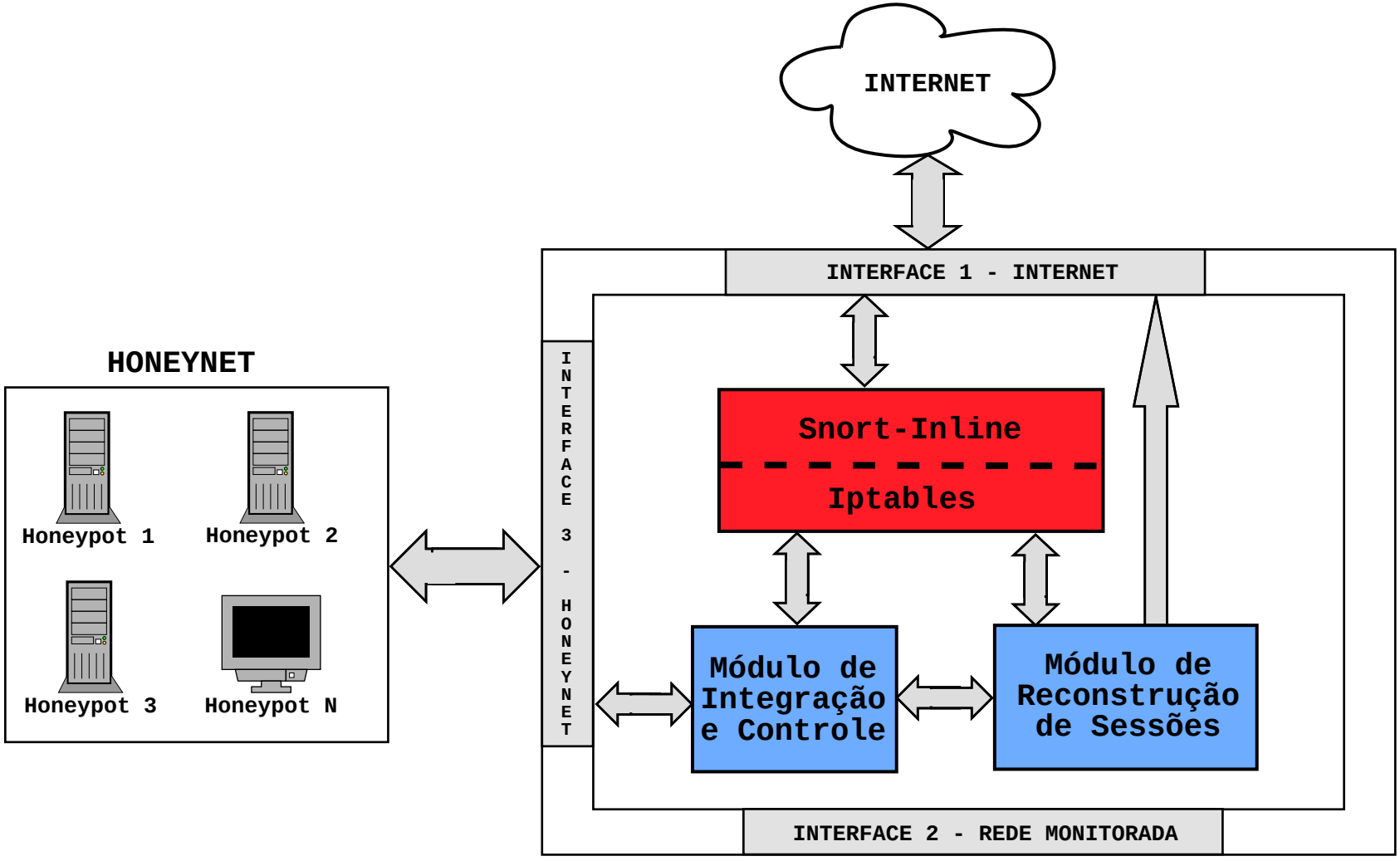


Diagrama de blocos do sistema proposto.

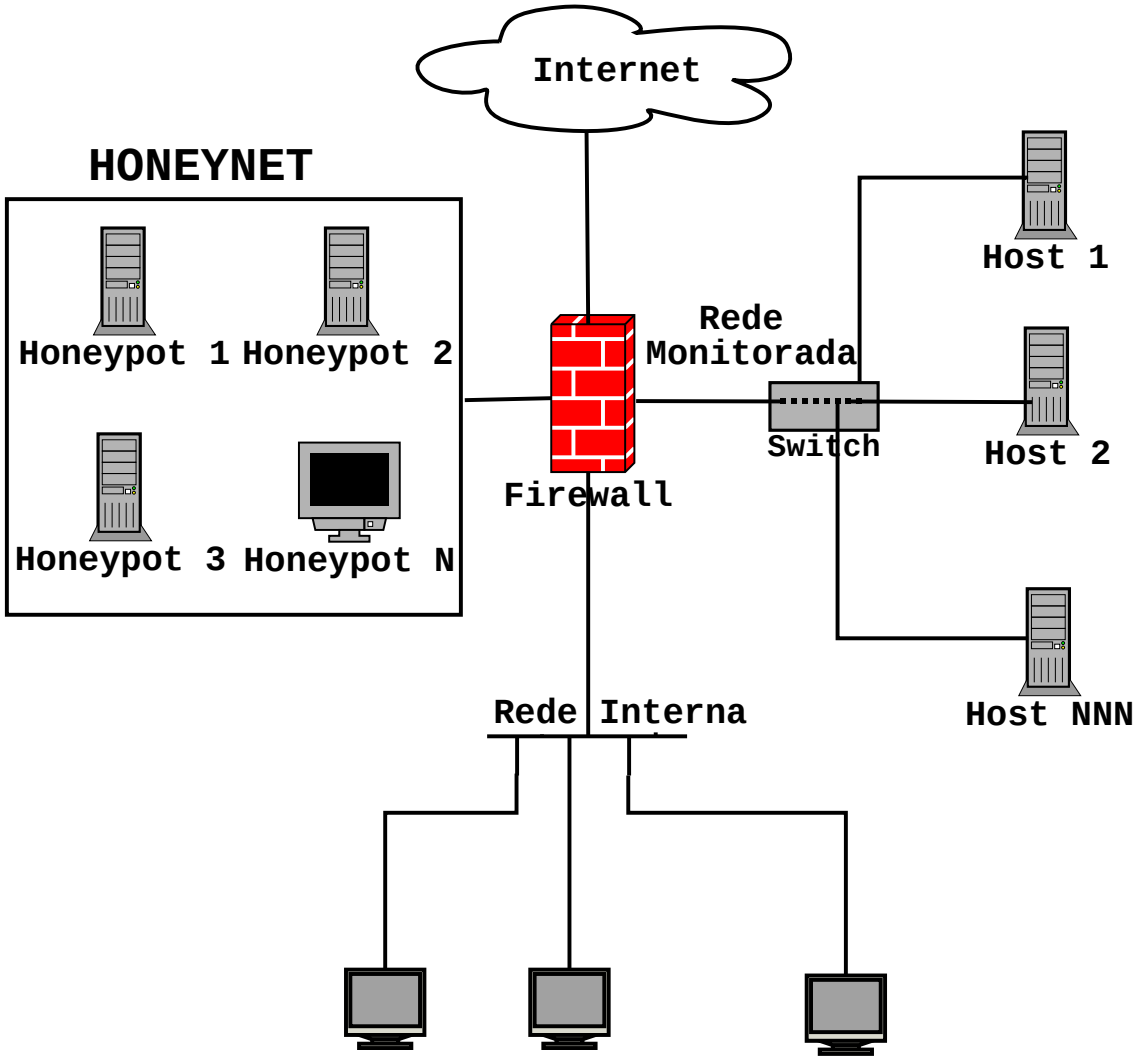
Descrição do Sistema Proposto

- *iptables*: *firewall stateful* utilizado nos *kernels* do sistema GNU/Linux versões 2.4.x e 2.5.x
- `Snort-inline`: interromperá a sessão entre o sistema atacante e o sistema alvo
- Terá como base o RECON e trabalhará com análise de dados em tempo-real
- Armazenamento de todas as sessões ativas
- *Honeynet* baseada na criada pelo Projeto Honeynet.BR e isolada da rede monitorada

Descrição do Sistema Proposto

- Módulo de Integração e Controle:
  - Responsável pela interação do sistema de detecção de intrusão, com o módulo de reconstrução de sessões, e o controle do desvio das sessões hostis para o *honeypot*
  - Desvio de forma transparente para o atacante
  - Armazenamento de todas as sessões ativas (destino)
  - Geração de alertas e *logs*

Arquitetura do Sistema



Arquitetura da rede para qual o sistema proposto foi projetado.

Arquitetura do Sistema

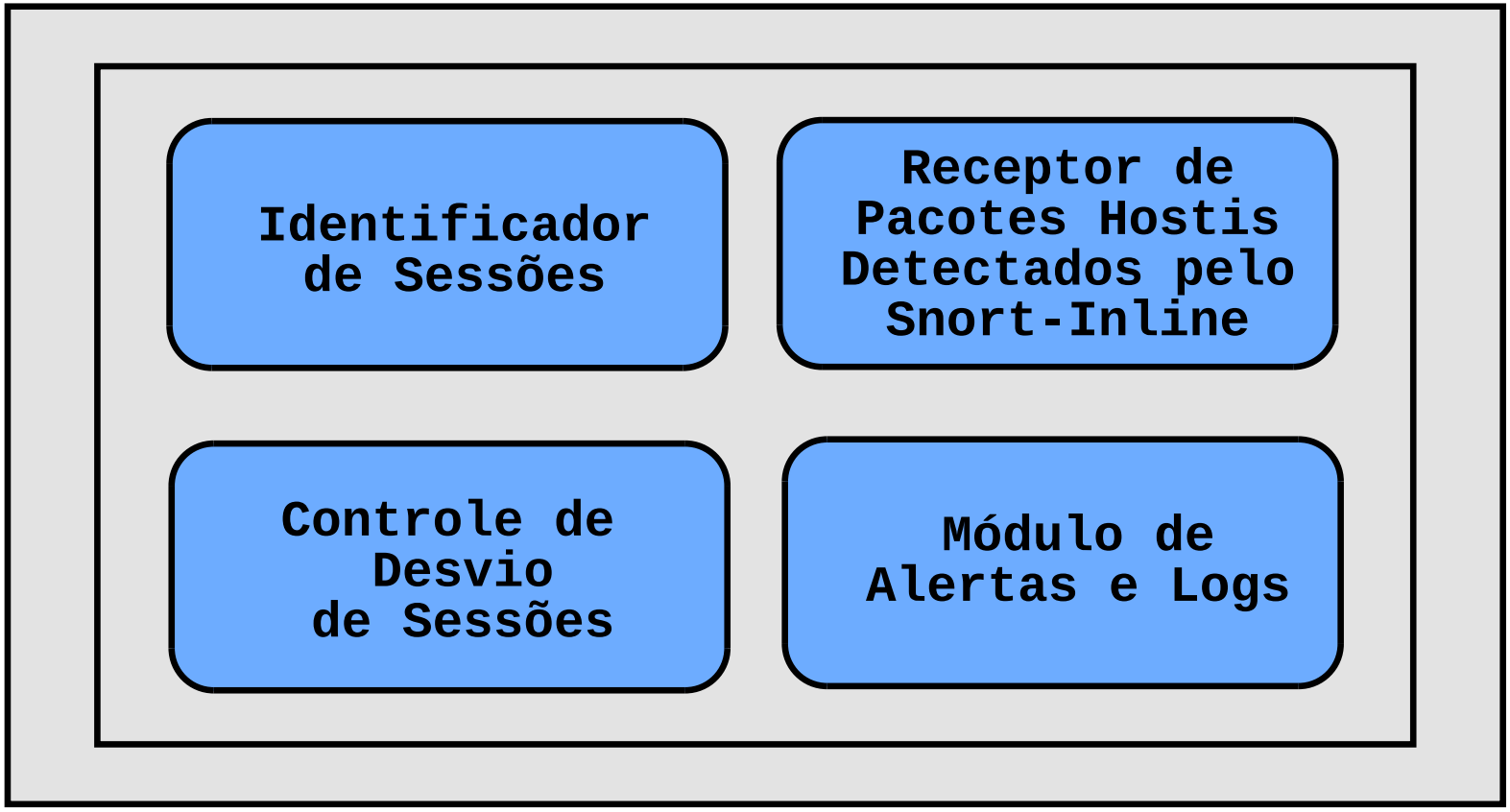


Diagrama de blocos do módulo de integração e controle.

Mapeamento da Rede

- Exemplo do arq. de configuração:

```
BPFFILTER "dst net 10.0.0.0/24"

NETMAP-10.0.0.5-255.255.255.0-80-TCP-10.0.1.1- \\
255.255.255.0-80-TCP-30*-20**-31***-300****-25*****

*      MAXSESSION
**     SESSIONTIMEOUTALL
***    SESSIONTIMEOUTB2INPKT
****   TAMSESSIONBYTES
*****  TAMSESSIONPKT
```

Mecanismos de Controle

- Captura do tráfego somente destinado a rede monitorada
- Número máximo de sessões TCP/IP
- *Timeout* da sessão em segundos
- *Timeout* da sessão entre três pacotes consecutivos pertencentes a ela em segundos
- Tamanho máximo da sessão em *bytes*
- Tamanho máximo da sessão em pacotes

Trabalhos Futuros

- Testes exaustivos antes de ser disponibilizado em ambientes reais de produção
- Refinamento do conjunto de regras para melhor desempenho
- Software complementar ao sistema que auxiliar a criação do arquivo de configuração
- Desenvolvimento de metodologias para tratar sessões criptografadas

Considerações Finais

- Outros sistemas semelhantes não apresentam as funcionalidades necessárias
- Baseia-se no conceito de arquiteturas de segurança em camadas
- Ferramenta capaz de identificar uma sessão hostil e desviá-la para um *honeypot* sem ser interrompida e, que possa ser empregada de modo funcional em qualquer rede de produção