IPS com Software Livre

Snort INLINE

Alejandro Flores
http://www.triforsec.com.br

Quem sou eu?

- RHCE
- 14 anos trabalhando com Linux
- 13 anos trabalhando com Segurança da Informação
- 10 anos de experiência com Snort
- Desenvolvedor do Projeto B.A.S.E
- Criador e Desenvolvedor do projeto IDSRG
- Criador e Desenvolvedor do projeto Spyket Security System

Um pouco de SNORT

Criado por Martin Roesch em 1998

Inicialmente um Sniffer/Logger de pacotes que poderia ser utilizado como um leve sistema de detecção de intrusão de rede, com sistema de regras para procura/detecção no conteúdo dos pacotes.

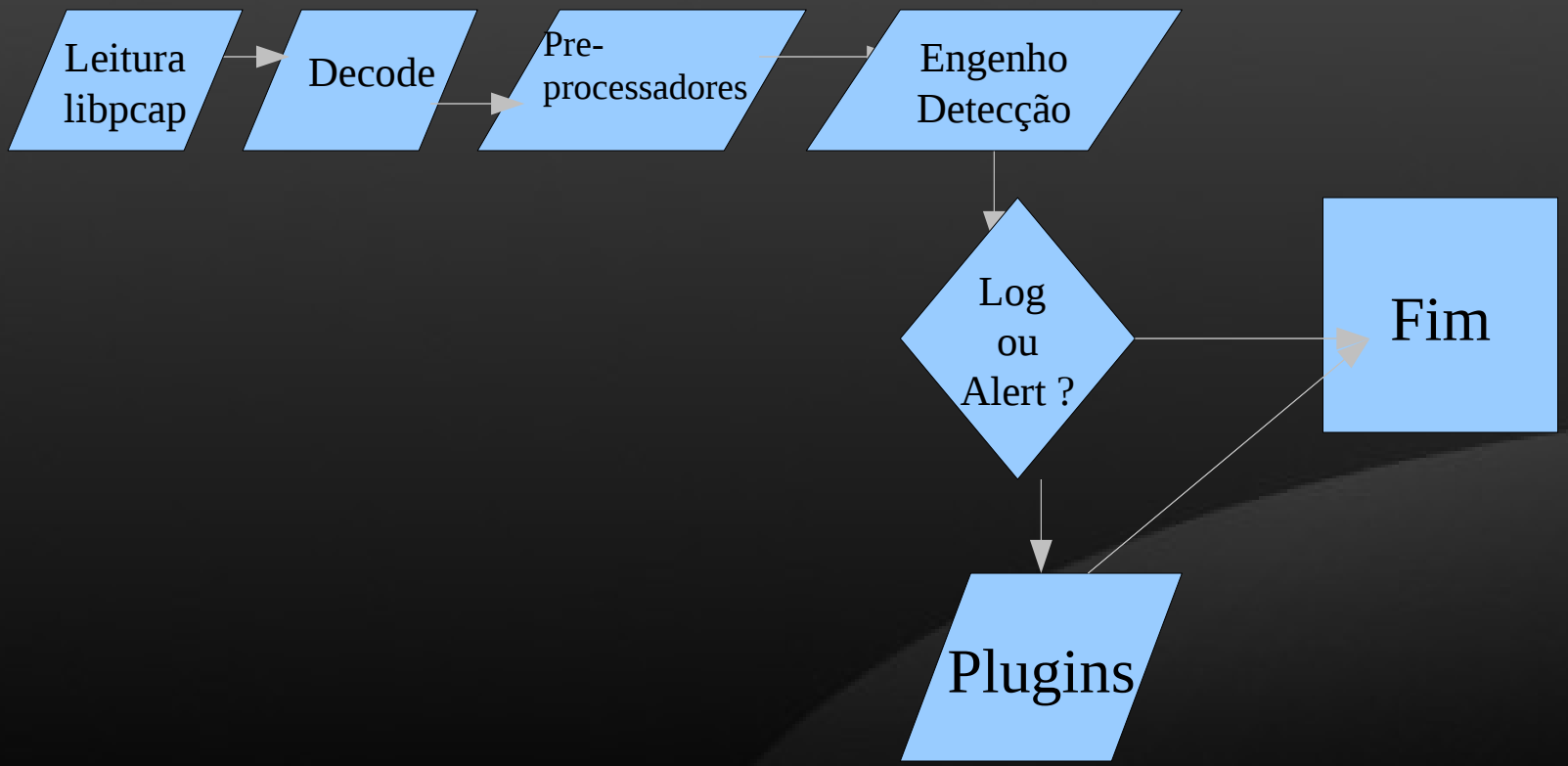
Um pouco de SNORT

Funcionamento:

- Captura de Pacotes
- Decoders
- Préprocessadores
- Engenho de detecção
- Output Plugins (Log, Alerta)

Um pouco de SNORT

Fluxo dos pacotes (modo nids):



IDS x IPS x Firewall

- Firewall: Controle de trafego
  - Trabalha no cabeçalho dos pacotes tcp/ip
  - Não analisa o conteúdo (payload) dos pacotes
  - Controle: origem, destino, portas, protocolos e flags
  - Análise de estado das conexões

IDS x IPS x Firewall

- IDS: Intrusion Detection System (snort)
  - Trabalha em qualquer parte do pacote
  - Regras para detecção de conteúdo malicioso
  - Passivo: Detecção, Alerta, Log
  - Le os pacotes diretamente via libpcap

IDS x IPS x Firewall

- IPS: Intrusion Prevention System (snort inline)
  - Um IDS com capacidades de Firewall
  - Ativos: Detecção, Bloqueio, Alerta, Log
  - Recebe os pacotes via libipq (netfilter)

Voltando ao SNORT

- Em modo NIDS o snort “abre” a(s) interface(s) de rede para leitura
- Cada pacote segue o fluxo mostrado no slide 5
- Pré-processadores ajudam na normalização do trafego, remontagem de fragmentos e analise de estado de conexões, entre outros

Snort inline = Snort + Iptables

- O IPTABLES manda os pacotes para o target QUEUE para serem processados por um programa externo, compilado utilizando a libipq, que deve responder ACCEPT ou DROP para cada pacote recebido.

Snort inline = Snort + Iptables

- Em modo '*inline*', o snort espera pelos pacotes enviados ao target QUEUE do iptables ao invés de ler via libpcap
- O netfilter aguarda o snort dizer o que fazer com o pacote
- Caso o pacote atinja alguma regra, este poderá ser descartado
- Se o pacote não atingir nenhuma regra, o snort manda ACCEPT para o netfilter

Regras para snort inline

Para responder o que fazer com os pacotes que disparam um alerta, as regras do snort devem ser modificadas para rejeitar o pacote em caso de um ataque.

Regras para snort inline

O snort inline tem as seguintes ações para as regras:

- **drop –** responde ao netfilter para descartar o pacote e faz log via snort
- **reject –** responde ao netfilter para descartar o pacote, log via snort e envia um TCP reset para protocolo TCP e ICMP Destination port Unreacheable para UDP
- **sdrop –** responde ao netfilter para descartar o pacote e nada é logado

Regras para snort inline

Exemplo de regra:

drop tcp any any -> any 80 (classtype:attempted-user; msg:"Tentativa de conexão porta 80"; sid:15001)

*Ação da regra

* Cabeçalho da regra

* Opções da regra

Preparando o ambiente

- Posicionando o seu IPS

Seu ips precisa estar posicionado de forma que o trafego a ser analisado tenha que passar por ele, seja de forma roteada (gateway) ou transparente (bridge), uma vez que é necessário bloquear o trafego malicioso.

Snort inline no gateway

- Todo trafego entre as redes roteadas passam obrigatoriamente por ele.
- É possível analisar todo o trafego que entra e sai, mas é melhor separar o que deve ser analisado.
- Através do iptables, criamos a regra que envia os pacotes para o target QUEUE

$ sudo iptables -A FORWARD -p tcp –dport 80 -j QUEUE

$ sudo snort -Qvc /etc/snort/snort.conf -l /var/log/snort

Snort inline transparente

Para funcionar transparente, o linux deve trabalhar em modo bridge, posicionado entre os segmentos de rede cujo trafego deve ser analisado.

$ sudo brctl addbr br0

$ sudo brctl addif br0 eth0

$ sudo brctl addif br0 eth1

$ sudo iptables -A FORWARD -p tcp –dport 80 -j QUEUE

$ sudo snort -Qvc /etc/snort/snort.conf -l /var/log/snort

Mercado atual

Os principais IPS (comercial) do mercado hoje são:

- Sourcefire (SNORT!)
- Escolhido como a melhor solução quase todos os anos.
- ISS Proventia
- TippingPoint

Mercado atual

Vantagens das 'caixas' IPS (comercial)

- Hardware
- Software enxuto
- Suporte

Mercado atual

Vantagens do IPS com software livre (snort)

- CUSTO!
- Flexibilidade e customização
- Não precisa comprar uma ferrari se seu limite de velocidade é 60 km/h

Agradecimentos!

Aldrey Galindo e a organização do evento!

 Ícones em Creative Commons http://icontexto.blogspot.com/ -- Bruno Maia

Contato


http://zroone.blogspot.com/


https://www.twitter.com/zroone


http://www.facebook.com/zroone


GMAIL: alejandrorflores@gmail.com

Alejandro Flores
http://www.triforsec.com.br