



CESoL
2008

IPS HLBR: aprimorando a segurança da sua rede



João Eriberto Mota Filho
Pedro Arthur Pinheiro Rosa Duarte

Fortaleza, CE, 20 de agosto de 2008

Sumário

- ✓ Breve histórico
- ✓ IPS X IDS
- ✓ Por que utilizar um IPS?
- ✓ Por que utilizar um IDS em conjunto com um IPS?
- ✓ Funcionamento do HLBR
- ✓ Exemplo de regra no HLBR
- ✓ Demonstração do HLBR
- ✓ Consumo de recursos computacionais
- ✓ A palavra de um desenvolvedor
- ✓ Conclusão



HLBR

Quem conhece?

Quem usa?



Breve histórico do HLBR

- ✓ Hogwash Light BR. Criado a partir do Hogwash, um projeto de Jason Larsen, desenvolvido em 1996;
- ✓ Encontra-se na versão 1.6 (8ª versão);
- ✓ A versão 1.0 introduziu a possibilidade de uso de expressões regulares POSIX nas regras de detecção;
- ✓ A versão 1.6 passou a utilizar expressões regulares PERL e trouxe diversas melhorias no código;
- ✓ IPS, instalado na camada 2 do modelo OSI (enlace), entendendo as camadas 2, 3 e 4 e atuando na 7, tudo no modelo OSI;
- ✓ Projeto mantido, atualmente, por 03 desenvolvedores e 16 tradutores / testers;
- ✓ Disponível em <http://hlbr.sf.net> e no Debian GNU/Linux.



IDS x IPS

- ✓ IDS (Intrusion Detection System): detecta e registra ações maliciosas e tráfego anômalo nas redes de computadores. Os IDS são passivos. Os HIDS atuam em hosts.
- ✓ IPS (Intrusion Prevention System): detecta, registra e trata ações maliciosas e tráfego anômalo nas redes de computadores. Os IPS são ativos. Alguns são reativos (desaconselhável). Atuam in-line na topologia.
- ✓ Os IDS são minuciosos, causando alto consumo de recursos e falsos positivos em demasia. No entanto, são indispensáveis na análise de tráfego.
- ✓ Os IPS são generalistas, provendo baixo consumo de recursos, velocidade e altíssimas taxas de acertos.



Por que utilizar um IPS?

- ✓ Tanto o IPS quanto o IDS analisam os dados que trafegam no payload dos pacotes IP.
- ✓ Os IPS são responsáveis por proverem a segurança de conteúdo para a rede.
- ✓ O IPS é parte integrante do sistema de firewall da rede.



Por que utilizar um IDS em conjunto com um IPS?

- ✓ IPS bloqueiam tráfego e não podem gerar falsos positivos.
- ✓ IDS logam tráfego, podendo e devendo gerar falsos positivos.
- ✓ O IDS devem ser utilizados logo após os IPS para mostrar tráfego anômalo não detectado.



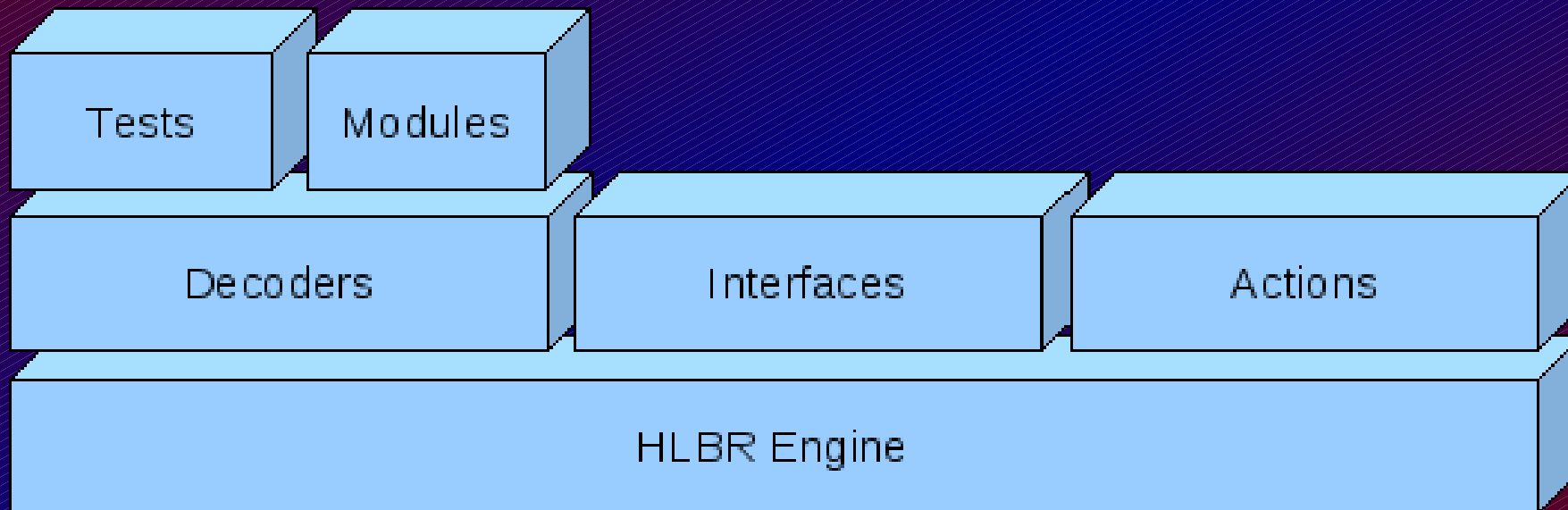
Funcionamento do HLBR

- ✓ Deve ser posicionado nas extremidades do sistema de firewall (externa e internamente);
- ✓ Não altera o cabeçalho IP dos pacotes pois é uma bridge (**invisível!!!**);
- ✓ Não utiliza endereço IP para operar pois é uma bridge (**invisível!!!**);
- ✓ Não “reseta” ou finaliza a conexão (não reativo). Apenas descarta os pacotes maliciosos (**invisível!!!**);
- ✓ Fornece logs de conteúdo em formato tcpdump;
- ✓ É muito difícil um ataque ao HLBR, uma vez que o mesmo não possui IP (não há como direcionar um shellcode, inviabilizando um buffer overflow remoto).



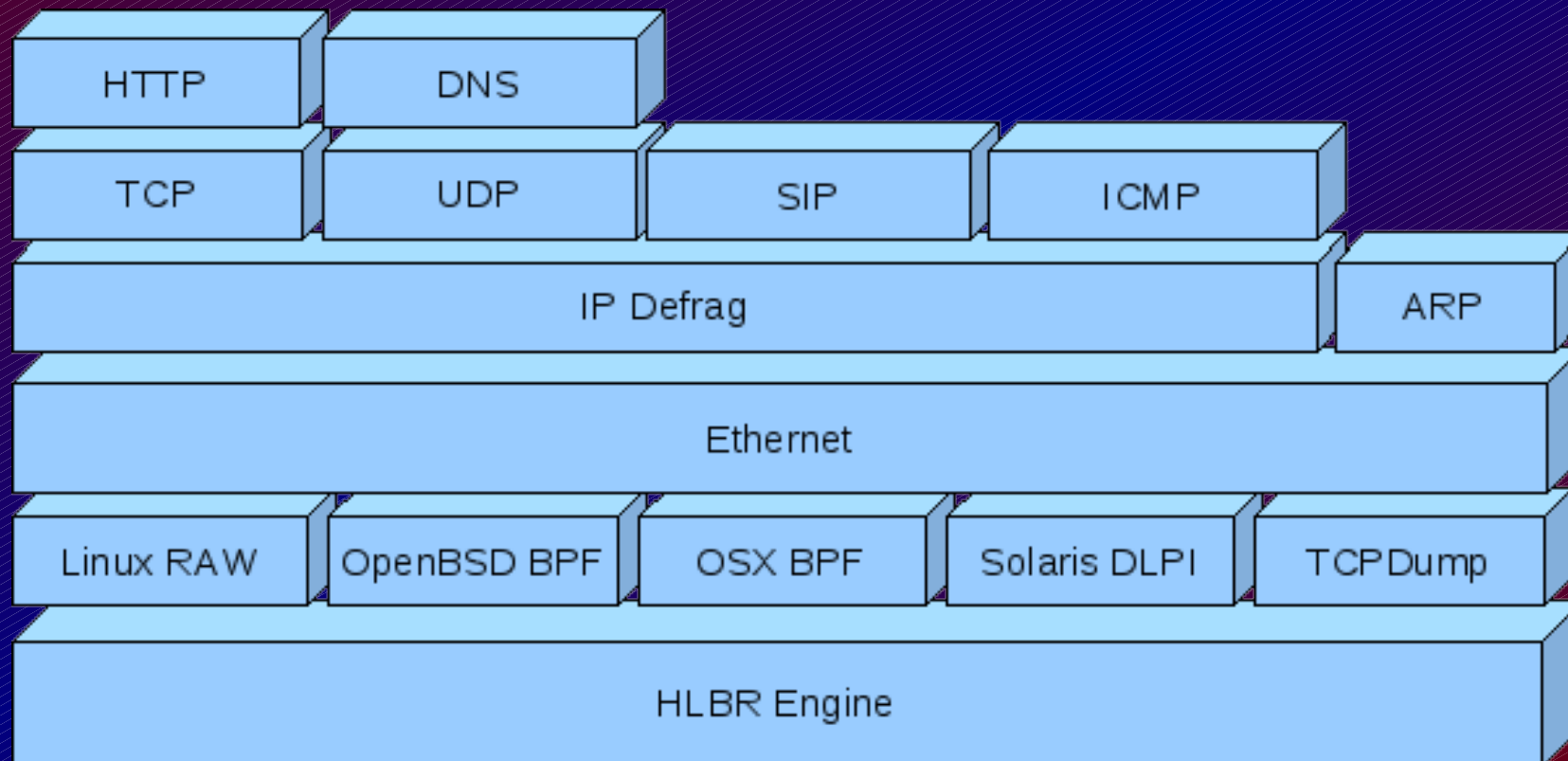
Funcionamento do HLBR

A arquitetura do HLBR



Funcionamento do HLBR

A arquitetura de decodificadores



Exemplo de regra no HLBR

Exemplo de uma regra com expressão regular:

```
<rule>  
ip dst(www)  
tcp dst(80)  
http regex((/|\.)+\.\.+(/|\.)+)  
message=(webattacks-1-re) directory change attempt (unicode,asc,plain)  
action=action1  
</rule>
```



Demonstração do HLBR

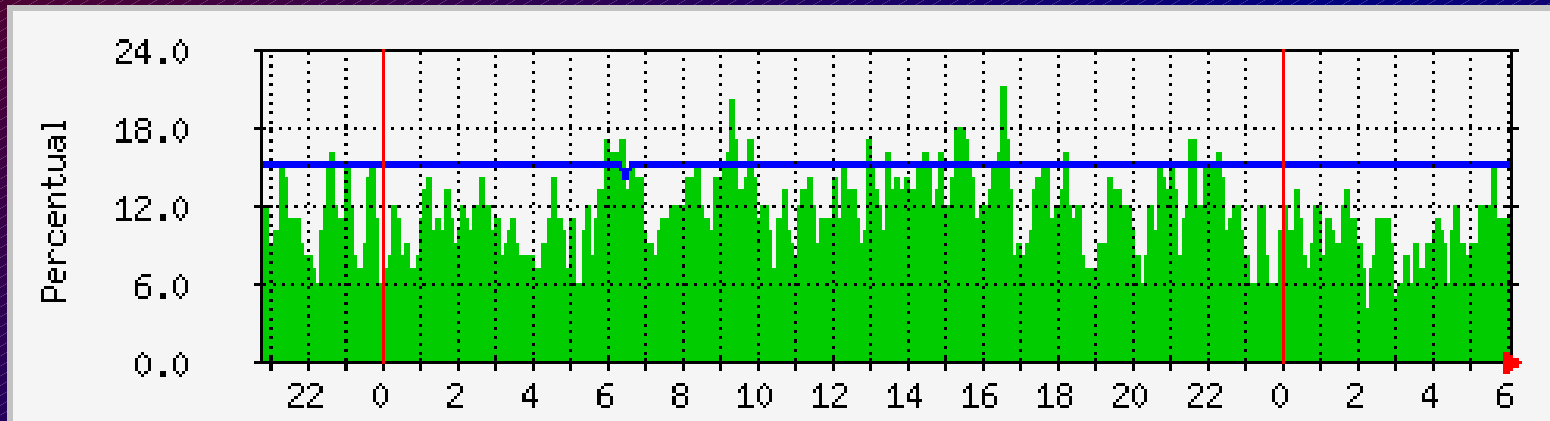
Topologia a ser utilizada:



(Visualização de filme)

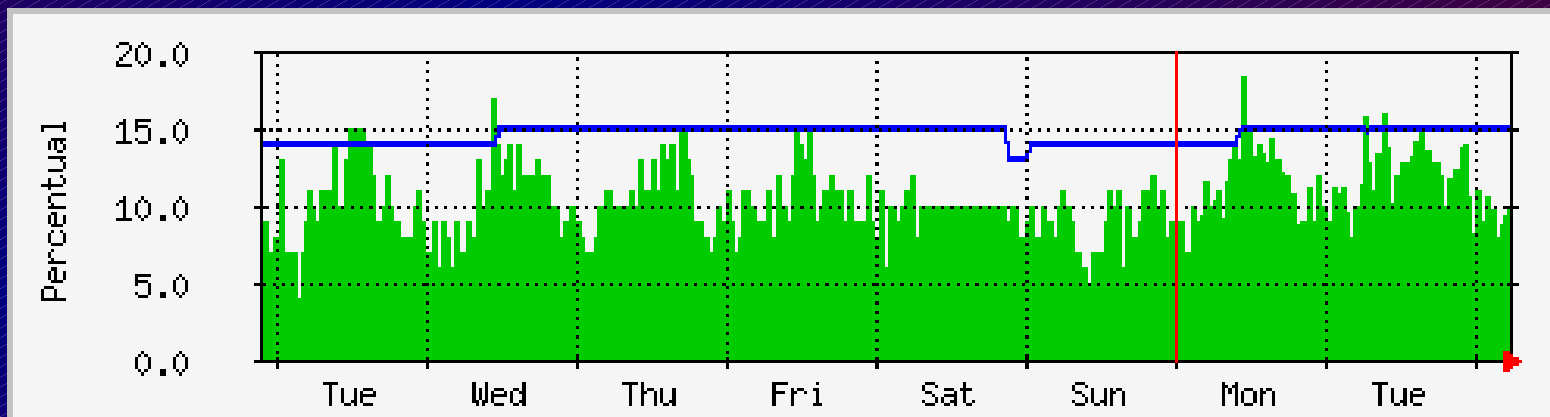
Consumo de recursos computacionais

Máquina Pentium4 single, com 256 MB RAM, conectada em um link dedicado de 4 Mb/s. Possui um HLBR com 139 regras.



Legenda:

- Processador
- Memória



A palavra de um desenvolvedor

ZZZZZZZ.....



O HLBR:

- ✓ É Software Livre;
- ✓ Atua na camada de enlace, trazendo diversas vantagens;
- ✓ Fornece logs em formato tcpdump;
- ✓ Não “reseta” ou finaliza. Apenas descarta!
- ✓ Ainda: ebttables é filtro de pacotes e não de conteúdo.





Esta palestra está disponível em:

<http://www.eriberto.pro.br>