



## **Sobre o Snort**

O Snort é um [software livre](#) de detecção de intrusão para rede (NIDS) desenvolvido inicialmente por Martin Roesch, capaz de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP. Executa análise de protocolo, busca/associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques, tais como buffer overflows, stealth port scans, ataques CGI, SMB probes, OS fingerprinting, entre outras. Esta ferramenta é suportada em arquiteturas RISC e CISC e em plataformas das mais diversas, como os vários sabores de Linux (RedHat, Debian, Slackware, Mandrake, etc.), OpenBSD, FreeBSD, NetBSD, Solaris, SunOS, HP-UX, AIX, IRIX, Tru64, MacOS X.

## **Sobre a comunidade Snort BR**

O grupo snort-br foi iniciado em janeiro de 2005 por André (si0ux) e Rodrigo Montoro (Sp0oKeR) . Abaixo algumas informações atuais do grupo:

Membros

- Atualmente mais de 500 membros cadastrado na lista de discussão

Lista de E-mail / Lista de Discussão

O projeto CIPSGA nos cedeu um espaço para a criação de uma lista de discussão para resolução de dúvidas (sobre o Snort e sistemas IDS) para os usuários brasileiros, comentários sobre o projeto e envio e notícias relacionadas.

Para se cadastrar visite o seguinte endereço: <http://listas.cipsga.org.br/cgi-bin/mailman/listinfo/snort-ids>

Para postar uma mensagem a todos os membros da lista, envie um email para [snort-ids@listas.cipsga.org.br](mailto:snort-ids@listas.cipsga.org.br). This e-mail address is being protected from spam bots, you need JavaScript enabled to view it

Canal de IRC

Foi criado um canal de IRC chamado #snort-br no servidor [irc.freenode.net](http://irc.freenode.net). Lá você poderá encontrar muita gente boa pra te ajudar.

## **Métodos de Search do Engine de Detecção do Snort**

por Rodrigo Montoro (Sp0oKeR)

<[spooker@gmail.com](mailto:spooker@gmail.com)>

O snort possui diversos mecanismos de search , ou seja, como ele faz o pattern match das tentativas de ataques. Baseado na sua necessidade e hardware, você pode selecionar o method de search que deseja, sendo para maior performance e/ou menor consumo de memória.

Para configurar essa opção basta modificar o `snort.conf` com a seguinte diretiva:

`config detection: search-method METODO_UTILIZADO` , onde o método utilizado podem ser os seguintes abaixo:

- `ac` Aho-Corasick Full (alta memória, melhor performance)
- `ac-std` Aho-Corasick Standard (memória moderada, alta performance)
- `ac-bnfa` Aho-Corasick NFA (pouca memória, alta performance)
- `acs` Aho-Corasick Sparse (baixa memory, média performance)
- `ac-banded` Aho-Corasick Banded (baixa memória, média performance)
- `ac-sparsebands` Aho-Corasick Sparse-Banded (baixa memória, alta performance)
- `lowmem` Low Memory Keyword Trie (baixa memória , baixa performance)

Por exemplo se quiser alto consumo de memória com alta performance usaria no

snort.conf :  
config detection: search-method ac

Sobre o algoritmo de search Aho-Corasick:

[http://en.wikipedia.org/wiki/Aho-Corasick\\_algorithm](http://en.wikipedia.org/wiki/Aho-Corasick_algorithm)

Em um artigo futuro falaremos mais informações sobre o search-method e resultados de benchmarks.

Mais info: <http://www.snort.org/docs/> na parte de Directives.

## **Overview Snort 3 alpha**

Por Cleber Brandao (CleBeer)

<[clebeer@gmail.com](mailto:clebeer@gmail.com)>

O objetivo Snort 3,0 alfa é testar os subsistemas do Snort 3.0 à medida que forem desenvolvidos.

Esta primeira versão alpha destina-se a testar a nova "fonte de dados" no módulo Snort, que contém o módulo de aquisição de dados, o decodificador e o gerenciador de fluxo.

Também mostra um pouco do novo Command Line Interface (CLI) para Snort, que é apoiado por uma linguagem de programação chamada Lua.

Instalação

Dependências:

\* Lua 5.1.1 - <http://www.lua.org>.

\* Libdnet >= 1.10 - <http://libdnet.sf.net>

\* Libpcap recente

\* Lib UUID.

Dependendo do seu sistema operacional você pode precisar carregá-la como uma dependência externa.

Por exemplo, no OpenBSD 3,9 precisa de ter o pacote instalado da árvore do ports.

Se seu sistema não incluir uma lib UUID ou você não conseguir encontrar uma para o seu SO Sugiro instalar o software e2fsprogs

<http://e2fsprogs.sf.net>.

Começando:

Faça o download em:

<http://www.snort.org/users/roesch/code/snort-03.0.0.a1.4.tar.gz>

Você precisará instalar o Lua 5.1 +, a Libdnet 1,10 + e a libpcap para compilar o Snort 3,0.

Após instalar as dependências você pode compilar o Snort 3,0 utilizando o classico

"/configure && make" dentro do diretório snort-03.0.0.a1.4

Assim que terminar vc pode digitar "snort" e será exibido o shell do snort CLI.

```
.._  -*> Snort! <*-
```

```
o" )~ Version 3.0 (Build 3) [PRE-ALPHA]
```

```
"" By Martin Roesch & The Snort Team: http://www.snort.org/team.html
```

```
1. Copyright 2006 Sourcefire Inc.
```

```
>
```

O processador de comandos do CLI é um script Lua chamado snort.lua ele pode ser encontrado

no diretório de compilação do snort em etc/snort.lua

para carrega-lo digite no prompt do CLI:

```
dofile("etc/snort.lua")
```

e o prompt ficará assim:

```
snort>
```

Agora você pode utilizar o snort 3 como um sniffer utilizando o comando sniff mais a interface que vc deseja escutar.

Ex.:

```
snort> sniff ("eth0")
```

Se você quiser executar um tipo de filtro você pode fazê-lo utilizando o comando fsniff (<interface>, <filtro>)

Ex.:

```
snort> fsniff("eth0", "tcp and port 22")
```

Espero que aproveitem assim que possível colocarei mais detalhes em [www.snort.org.br](http://www.snort.org.br)

## **Snort Drinking Game**

Por Cleber Brandao (CleBeer)

[<clebeer@gmail.com>](mailto:clebeer@gmail.com)

Instruções: fique sem ler os emails da lista de usuários snort durante um mês. Ou ao invés disso você pode utilizar os arquivos antigos da lista. Leia o email e se ele possuir algum item da lista a seguir você deve beber o "Penalty drink" caso contrário passe para o próximo email. Repita isso até que você não consiga mais ler ou a garrafa esteja vazia.

Tome uma dose se...

- A resposta da questão esta na documentação
- A resposta da questão esta no FAQ.
- O remetente não sabe usar o google
- A resposta é "RTFM" (Read th fucking manual)
- O remetente esta usando a pcap bugada da Red Hat
- O remetente possui uma assinatura com mais de 4 linhas
- O remetente postou um log de captura de pacote e substituiu o numero IP por XXX porem não alterou o IP exibido em hexa.

Tome duas doses se...

O remetente obviamente nunca leu a documentação do snort

- A assinatura do remetente possui "O conteúdo deste email é..."
- O conteúdo da mensagem possui "Por favor me descadastre da lista"
- O remetente disse que não achou a resposta no google e a resposta
- esta nos primeiros 10 resultados do google

E o "Big Penalty Drink"

Se você perceber que esta bebendo por cause de um email que vovê enviou dobre a dose. E tome seis (sim seis doses) se você tiver enviado algum email em HTML pra lista.

Happy Snort Drink...

Fonte: <http://www.joelesler.net/2008/02/snort-drinking-game-by-erek-adams.html>

## **Sistemas de Detecção de Intrusão (IDS)**

Por André Luiz R. Ferreira (si0ux)  
<[andreirf@gmail.com](mailto:andreirf@gmail.com)>

Talvez a melhor maneira de garantir a segurança de um sistema seja fazer com que ele informe sobre certas alterações de seu estado . É provável que a sua casa ou seu local de trabalho possua um sistema de alarme. O alarme residencial é um tipo de dispositivo de detecção de intrusão.

Na computação um Sistema de Detecção de Intrusão (comumente chamado de IDS ,em inglês, Intrusion Detection System) é uma ferramenta com recursos para detectar alterações no status do seu sistema ou de sua rede. Um IDS deve ser suficientemente inteligente para detectar tentativas de invasão em tempo real, podendo disparar alertas ou tomar as providências apropriadas predefinidas para ajudar na proteção de uma rede de computadores ou um host em especial.

É comum encontrarmos dois tipos de estratégias para detecção dos possíveis incidentes de segurança:

- *IDS baseados em regras ou assinaturas*: este é o tipo mais comum de IDS, principalmente por ser mais fácil de instalar. O desafio é fazer com que as assinaturas permaneçam atualizadas. Da mesma forma que acontece com programas anti-vírus, se as assinaturas estiverem desatualizadas, o IDS não será capaz de detectar os ataques mais recentes, como por exemplo a tentativa de exploração de uma nova vulnerabilidade.
- *IDS baseados em anomalias*: inicialmente, este tipo de IDS passa algum tempo reunindo amostras da atividade ou comportamento normal e aceitável da rede ou do computador, armazenando estas informações em uma base de dados e, em seguida, alarma a qualquer comportamento que estiver fora dos parâmetros capturados.

Embora existam muitos fornecedores diferentes, há apenas dois tipos de IDS:

- *Baseados em host (HIDS)*: analisam arquivos de logs, programas e conexões abertas de rede, analisam o disco rígido e memória e depois emitem alertas caso ocorra algum evento.
- *Baseados em rede (NIDS)*: ouvem o tráfego à medida que este atravessa a rede.

Um dos IDS mais utilizados e populares no momento é o Snort. O Snort é um IDS baseado em rede, que é desenvolvido pela empresa Sourcefire e a comunidade open-source. Ele pode ser executado em qualquer sistema UNIX e até em sistemas Windows.

Talvez o elemento mais importante de um IDS baseado em rede seja a possibilidade de informar todos os detalhes de um pacote que entra ou sai da rede. Ele pode identificar o tipo de protocolo, os endereços IPS e as portas de origem e destino, além de exibir o payload (campo de dados). O Snort cumpre este papel, colocando a placa de rede em modo promíscuo, podendo até reagir aos ataques, interagindo com ferramentas de firewalls, gravando seus registros em banco de dados, disponibilizando-os para consulta pela Web, além de poder atuar também como um IPS (Intrusion Prevention System) e outros recursos. Mas estes são assuntos para um próximo artigo... :-D

Sinta-se livre para acessar o material disponível em nosso site e enviar suas dúvidas em nossa lista de discussão. Abraços!