Prof. Marcos Monteiro

http://www.marcosmonteiro.com.br
contato@marcosmonteiro.com.br

https://www.snort.org

snort.org

Documents Downloads Products Community Store VRT

Get started with the world's most powerful detection software

Get Started

Download Snort and the rules you need to stay ahead of the latest threats

Download Rules

Keep up-to-date with the latest changes and documentation

Documents

SNORT®

snort.org.br

Snort.Org | SNORT Brasil

SNORT Brasil

Snort

The Open Source Network Intrusion Detection System

HOME | O que é e como funciona uma ferramenta IDS ? | A necessidade de um IDS | O SNORT | A arquitetura e o funcionamento do SNORT | Principais Comandos

Recursos

Palestra Open Source Security no

Marcos Monteiro

Pra Instalar:

- Pacotes necessários para a instalação do Snort:
- libpcap
- libpcre
- tcpdump
- openssl
- libdnet
- mysql (para gravação de logs no banco de dados MySQL)
- postgresql (para gravação de logs no banco de dados PostgreSQL)
- gcc
- g77
- libpcre3-dev
- libnet0-dev

Pra Instalar:

- Mais fácil, usa ai um Debian ou baseado
  - # apt-get install snort

Para iniciar o serviço do Snort devemos executar o seguinte comando:

  - # snort -c /etc/snort/snort.conf -u snort -g snort

Configurando

vi /etc/snort/snort.conf

– Devemos mudar os valores de algumas variáveis. Procure pelas seguintes linhas:

var RULE_PATH ../rules
var PREPROC_RULE_PATH ../preproc_rules

– E mude para:

var RULE_PATH /etc/snort/rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

output alert_fast: alert_quick

Ou:

output alert_full: alert_detailed

- No modo "alert_fast: alert_quick" o Snort funciona mais rápido, pois gera logs com o mínimo de detalhes possível. No modo "alert_full: alert_detailed" o Snort trabalha um pouco mais lento que no modo anterior, porque ele irá gerar alertas com o máximo de detalhamento possível, além disso, os logs utilizarão mais espaço em disco.

- Também temos que inserir a linha que indica a pasta de logs do snort. Adicionaremos essa opção no snort.conf da seguinte maneira:

  config logdir: /var/log/snort

- Existem mais duas variáveis importantes na configuração do arquivo snort.conf: HOME_NET e EXTERNAL_NET. Devemos localizar essas variáveis, que estarão dispostas no arquivo snort.conf da seguinte maneira:

- var HOME_NET any
- var EXTERNAL_NET any

- HOME_NET

  Esta é a rede da qual quer proteger

- EXTERNAL_NET

  Esta é sua rede de entrada, dela que você quer proteger (normalmente pode ser a Internet)

- var DNS_SERVERS $HOME_NET
- var SMTP_SERVERS $HOME_NET
- var HTTP_SERVERS $HOME_NET
- var SQL_SERVERS $HOME_NET
- var TELNET_SERVERS $HOME_NET
- var SNMP_SERVERS $HOME_NET

Identifique estes caras da sua rede!

Por exemplo

- var DNS_SERVERS [192.168.1.200/32]
- var SMTP_SERVERS [192.168.1.201/32]
- var HTTP_SERVERS [192.168.1.202/32]
- var SQL_SERVERS [192.168.1.203/32]
- var TELNET_SERVERS[192.168.1.204/32]
- var SNMP_SERVERS [192.168.1.205/32]

A virgula para aceitar mais de um.

Incluir Regra

- include $RULE_PATH

  include $RULE_PATH/local.rule
  include $RULE_PATH/backdoor.rules
  include $RULE_PATH/bad-traffic.rules
  include $RULE_PATH/chat.rules
  include $RULE_PATH/ddos.rules
  include $RULE_PATH/dns.rules
  include $RULE_PATH/dos.rules
  include $RULE_PATH/exploit.rules

alert tcp 192.168.1.50 any -> 192.168.1.1
1:1024 (msg:"tentativa ou acesso, porta <
1025"; sid:1; rev:0;);

Na criação de regras para o Snort podemos definir intervalos de portas ou IP's

Para verificar o tráfego da rede com o snort em modo sniffer de rede, devemos utilizar o seguinte comando:

- # snort -v

05/07-18:57:48.321440 192.168.2.50:4358 -> 192.168.2.80:53 UDP TTL:127 TOS:0×0 ID:6873 IpLen:20 DgmLen:70 Len: 42

Mais detalhes em:

- # snort -vd

05/07-19:00:02.941503 192.168.0.2.1:137 -> 192.168.255.255:137 UDP TTL:128 TOS:0×0 ID:51302 IpLen:20 DgmLen:78 Len: 50 AC 6D 01 10 00 01 00 00 00 00 00 00 20 45 45 45 .m..... EEE 46 45 4D 46 45 45 42 44 43 43 41 43 41 43 41 43 FEMFEEBDCCACACAC 41 43 41 43 41 43 41 43 41 43 41 43 41 00 00 20 ACACACACACACA.. 00 01 ..

Entendendo as Regras

As regras no Snort também obedecem a um modelo. O modelo está descrito abaixo:

<tipo_de_alerta> <protocolo> <rede_origem> <porta_origem> → <rede_destino> <porta_destino> (Cabeçalho da Regra; Opções; sid:X;...);

alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mountd access";sid:11)

Para tipo_de_alerta, nós temos:

- alert
  - Gera um alerta usando um método selecionado e então loga o pacote;
- log
  - loga o pacote;
- pass
  - ignora o pacote;
- Activate
  - alerta e então ativa outra regra dinâmica;
- dynamic
  - permanece inativa até ser ativado por uma regra activate, então atua como uma regra de log.

Entendendo as Regras

- Para Protocolos, nós temos:

1. tcp;
2. udp;
3. icmp;

Para Opções de Regras, temos quatro categorias principais:

- 1. meta-data
  - Essas opções provêem informação sobre a regra, mas não tem qualquer efeito durante a detecção;
- 2. payload
  - Todas essas opções procuram por dados dentro do payload(seção DATA) do pacote e podem ser inter-relacionadas;
- 3. non-payload
  - Essas opções procuram por dados fora do payload;
- 4. post-detection
  - Essas opções são regras específicas que acontecem após uma regra ter sido detectada.

Opções de Regra de Meta-Data

- msg

A opção msg informa a ferramenta de log e alerta qual a mensagem que deve ser imprimida quando o alerta for dado.

Formato:

msg ”<mensagem texto aqui>”;

Entendendo as Regras

reference

A opção reference permite as regras incluírem referências externas ao ataque. Essas referências possuem maiores informações sobre o ataque. Atualmente o Snort suporta apenas alguns sistemas específicos com URLs únicas. Abaixo uma lista deles:

Sistema	PrefixoURL
bugtraq	http://www.securityfocus.com/bid/
cve	http://cve.mitre.org/cgi-bin/cvename.cgi?name=
nessus	http://cgi.nessus.org/plugins/dump.php3?id=
arachnids (inativo)	http://www.whitehats.com/info/IDS
mcafee	http://vil.nai.com/vil/dispVirus.asp?virus k=

EXEMPLO

reference: <id system>,<id>; [reference: <id system>,<id>;]

Vejamos alguns exemplos abaixo:

alert tcp any any -> any 7070 (msg:"IDS411/dos-realaudio"; \ flags:AP; content:"|fff4 fffd 06|"; reference:arachnids,IDS411;)

alert tcp any any -> any 21 (msg:"IDS287/ftp-wuftp260-venglin-linux"; \ flags:AP; content:"|31c031db 31c9b046 cd80 31c031db|"; \ reference:arachnids,IDS287; reference:bugtraq,1387; \ reference:cve,CAN-2000-1574;)

Entendendo as Regras

- sid

A opção sid é usada unicamente para identificar regras do Snort. Esta informação permite aos plugins que interagem com o snort identificar regras facilmente. Esta opção deve ser usada com a opção “rev”, que veremos mais abaixo.

Formato:

sid <snort_rule_id>

Deve-se atentar a numeração de id que precisa ser obedecida para se formar um padrão. Ela é a seguinte:

- < 100 – Reservada para uso Futuro;
- 100 – 1000000 – Regras incluídas com a distribuição do Snort;
- > 1000000 – Regras usadas localmente;

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Entendendo as Regras

- rev

Esta opção é usada unicamente para identificar revisões em regras do Snort. Revisões permitem demonstrar uma melhora na escrita das assinaturas de ataques. Esta opção deve ser usada em conjunto com a opção “sid”.

Formato:

rev <inteiro da revisão>

Exemplo:

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Entendendo as Regras

- **classtype**Serve para orientar a categoria de ataque que se está sendo detectado. Trabalha em cima de uma tabela com nome, descrição e prioridade. O usuário pode então especificar qual a prioridade que determinado tipo de ataque tem ao ser detectado.

Formato:

classtype: <nome da classe>;

As classificações de regras são definidas num arquivos chamado classification.config. Este arquivo utiliza a seguinte sintaxe:

config classification: <nome da classe>,<descrição>,<prioridade>

Marcos Monteiro

Entendendo as Regras

- priority

A opção priority emite um nível de alerta para a regra. Formato:

priority: <inteiro para prioridade>;

Exemplo:

alert TCP any any -> any 80 (msg: "WEB-MISC phf attempt"; flags:A+;content: "/cgi- bin/phf"; priority:10;)

Essa opção é importante na definição de alertas críticos no SNOC

Respondendo

- reset_dest:
  - Envia pacotes TCP para o destino do ataque, fechando a conexão;
- reset_source:
  - Envia pacotes TCP para a origem do ataque, fechando a conexão;
- reset_both:
  - Envia pacotes TCP para ambos, origem e destino, fechando a conexão;

Respondendo

- icmp_net:
  - Envia um pacote ICMP network unreachable para a origem do ataque;
- icmp_host:
  - Envia um pacote ICMP host unreachable para a origem do ataque;
- icmp_port:
  - Envia um pacote ICMP port unreachable para a origem do ataque;
- icmp_all:
  - Envia pacotes ICMP host unreachable e ICMP network unreachable para a origem do ataque.

EXEMPLO

alert icmp any any -> any any (msg:"Ping suspeito"; sid:1; resp:icmp_all;)

Com a regra acima o Snort gerará um alerta de qualquer pacote ICMP que estiver passando de qualquer máquina para qualquer máquina e enviará pacotes ICMP para a máquina de origem com as seguintes mensagens:

host unreachable;

network unreachable.

Antes

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DDOS TFN Probe"; icmp_id:678; itype:8; content:"1234"; reference:arachnids,443; classtype:attempted-recon; sid:221; rev:4;)

alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"DDOS shaft synflood"; flow:stateless; flags:S,12; seq:674711609; reference:arachnids,253; reference:cve,2000-0138; classtype:attempted-dos; sid:241; rev:10;)

Depois

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DDOS TFN Probe"; icmp_id:678; itype:8; content:"1234"; reference:arachnids,443; classtype:attempted-recon; sid:221; rev:4; **resp:icmp_host;**)

alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"DDOS shaft synflood"; flow:stateless; flags:S,12; seq:674711609; reference:arachnids,253; reference:cve,2000-0138; classtype:attempted-dos; sid:241; rev:10; **resp:reset_both;**)

Não esquece que precisa:

service snort restart

Obrigado pela atenção!!

Prof. Marcos Monteiro

http://www.marcosmonteiro.com.br

Fontes:

http://www.vivaolinux.com.br

CRIANDO REGRAS PARA O SNORT - Glaudson Ocampos