LATINOWARE 2018

SURICATA

IDS/IPS para a segurança em redes de computadores

João Eriberto Mota Filho

Foz do Iguaçu, PR, 19 de outubro de 2018

Sumário

- IDS e IPS
- Projeto Suricata
- Principais características
- Suricata como IDS
- Suricata como IPS no Linux
- Suricata + Fail2ban
- Personalização de regras
- Conclusão
- Referências

Sumário

IDS e IPS

- Sistemas de firewall são formados por diversos elementos como filtros de pacotes e de estados, proxies, IDS, IPS, verificadores de integridade etc.
- O Intrusion Detection System (IDS) é responsável por gerar logs a respeito de anomalias no tráfego e tentativas de invasão.
- Duas características comuns em IDS são a possibilidade de falsos positivos e o não bloqueio de tráfego.
- Geralmente, o IDS faz a remontagem de pacotes e de segmentos depois da passagem dos mesmos.

IDS e IPS

- O Intrusion Prevention System (IPS) tem um mecanismo interno similar a um IDS.
- A principal diferença é que o IPS faz o bloqueio de tráfego malicioso.
- Um IPS nunca deveria gerar falsos positivos, a fim de evitar o bloqueio de tráfego legítimo.
- O IPS deve fazer a remontagem de pacotes e de segmentos antes de liberar a entrada de tais elementos na rede. Isso requer maior poder computacional.
- Tanto o IDS quanto o IPS trabalham com heurísticas e expressões regulares (geralmente PCRE), ou outros métodos.

IDS e IPS

Quadro comparativo entre IDS e IPS

	Log	Bloqueio de anomalias	Falsos positivos	Remontagem retém tráfego
IDS	X		X	
IPS	X	X		X

Sumário

Projeto Suricata

- Suricata é um projeto de IDS/IPS sob a licença GPL-2, disponibilizado publicamente pela primeira vez em 2009.
- É mantido por uma organização sem fins lucrativos, a Open Information Security Foundation (OISF).
- O seu desenvolvimento é feito por membros da OISF, pela comunidade Open Source e por fabricantes de software e hardware. Atualmente, o core de desenvolvedores é formado por 13 pessoas*.

(*) https://oisf.net/team/

Projeto Suricata

- Em 2018 foi criado o Suricata Community Council, cujo objetivo é aproximar a comunidade dos desenvolvedores do projeto.
- Anualmente, desde 2015, ocorre em algum lugar do mundo a SuriCon. Trata-se de uma conferência que reúne pessoas do mundo inteiro, interessadas no Suricata e no seu desenvolvimento ou utilização.
- O site da SuriCon é https://suricon.net/
- O site do Projeto Suricata é o https://suricata-ids.org

Sumário

Principais características

- Uma lista completa das características do Suricata está disponível em https://suricata-ids.org/features/all-features/
- Algumas delas:
  * Pode atuar como IDS e IPS.
  * Multithread configurável, gerando uma alta performance de análise de tráfego.
  * Gravação de tráfego em formato pcap.
  * Integração com o Netfilter do Linux.
  * Suporte a Linux, FreeBSD, OpenBSD, Mac OS X e MS Windows.

Principais características

- Algumas características do Suricata (continuação):
  * Suporte pleno ao IPv6.
  * Decodificação de túneis como Teredo e GRE.
  * Suporte a uma ampla gama de protocolos de camadas 2, 3, 4 e 7 do Modelo OSI. Alguns exemplos: PPP, PPPoE, VLAN, MPLS, SCTP, HTTP, SMB, SMPT, DNS, NTP etc.
  * Diversas possibilidades para a aquisição de dados, incluindo os sockets de alta performance AF_PACKET, PF_RING e NETMAP.
  * Ampla possibilidade de saída de relatórios de dados.
  * Atualização de regras via Internet.
  * Possibilidade de regras personalizadas.

Principais características

- O Suricata já traz diversos conjuntos de regras prontas. Na versão 4.0.5, em 17 de outubro de 2018, foram listados 59 conjuntos*:

```
activex app-layer-events attack_response botcc
botcc.portgrouped chat ciarmy compromised current_events
decoder-events deleted dnp3-events dns dns-events dos drop
dshield exploit files ftp games http-events icmp icmp_info
imap inappropriate info malware misc mobile_malware
modbus-events netbios  nfs-events ntp-events p2p policy
pop3 rbn rbn-malvertisers rpc scada scan shellcode smtp
smtp-events snmp sql stream-events telnet tftp tls-events
tor trojan user_agents voip web_client web_server
web_specific_apps worm
```

(*) alguns devem ser buscados em https://rules.emergingthreats.net

Principais características

- Há um documento, criado pela Empresa proofpoint que define vários dos conjuntos de regras.

- Tal documento está disponível em http://tools.emergingthreats.net/docs/ETPro Rule Categories.pdf

- VISUALIZAÇÃO DO DOCUMENTO.

Sumário

Suricata como IDS

- Atuando como IDS, o Suricata apenas escutará o tráfego para gerar logs sobre atividades suspeitas (comprovadas ou não).
- Na condição mencionada, a sua instalação poderá ser feita sobre uma máquina que esteja atuando como roteador (level 3) ou como bridge (level 2).
- A bridge oferece algumas vantagens, como a invisibilidade e uma maior proteção contra ataques.
- Para saber como fazer uma bridge no Debian, consulte o link http://bit.ly/bridge_debian.

Suricata como IDS

- A instalação do Suricata no Debian pode ser feita com:

```
# apt-get install suricata
```

Para outras distribuições, veja antes se a versão disponível é a mais atual em https://repology.org/metapackage/suricata/versions

- O próximo passo será configurar o arquivo /etc/suricata/suricata.yaml. Há diversos tutoriais na Internet, inclusive no site oficial do Suricata.

- O Suricata possui uma integração com o Oinkmaster para atualizar regras. O Oinkmaster é o atualizador de regras para o Snort. Para isso, execute:

```
# apt-get install suricata-oinkmaster
# suricata-oinkmaster-updater
# suricatasc -c reload-rules
```

Suricata como IDS

- Além de atualizar o Suricata, o comando suricata-oinkmaster-updater já faz o download das regras existentes em https://rules.emergingthreats.net.
- Ao ser inicializado, o Suricata começará a observar o tráfego e a gerar logs.
- O log mais comum será o /var/log/suricata/fast.log
- DEMONSTRAÇÃO

Sumário

Suricata como IPS no Linux

- Normalmente, a implementação da pilha de rede em um SO é feita totalmente dentro do kernel.
- SO's trabalham com o conceito de kernel space e user space.
- Implementações de IPS em user space não alcançam boa velocidade de análise e de throughput.
- Uma solução seria criar um IPS como módulo de kernel. Mas isso seria enorme, pesado e de difícil manutenção.
- Programas grandes e pesados devem trabalhar em user space!

Suricata como IPS no Linux

- O Netfilter, é implementado pelo kernel (kernel space) e gerenciado pelo comando iptables (além de ebtables e arptables).
- Ele provê uma API de comunicação com o user space.
- Então, o Suricata poderá conectar-se com o Netfilter e solicitar bloqueios de tráfego.

RESOLVIDO!!!

Suricata como IPS no Linux

- A nfnetlink_queue, presente no Kernel Linux desde a versão 2.6.14, coloca pacotes de rede em uma fila, enviando informações dos mesmos para o user space, por intermédio do alvo NFQUEUE . Exemplo:

```
# iptables -A FORWARD -o eth0 -p tcp --dport 22 -j NFQUEUE
  --queue-num 5
```

- As informações enviadas são: ID, cabeçalho e payload.
- Um programa em user space pode inspecionar ou modificar o pacote, se desejar. A seguir, tal programa DEVE descartar ou reinjetar o pacote no kernel.
- Se a fila (buffer) lotar, os novos pacotes serão descartados ou aceitos por default, dependendo da configuração adotada.

Suricata como IPS no Linux

- O kernel space é rápido. O programa em user space também deverá ser!
- É lógico que a velocidade total dependerá da disponibilidade de processador e memória.
- Como IPS, o Suricata deverá ser colocado in-line, referenciando a fila designada pelo NFQUEUE:

```
# suricata -c /etc/suricata/suricata.yaml -q 5
```

- No Debian, o número da fila poderá ser configurado em /etc/default/suricata.
- É recomendável ter sempre um IDS logo após um IPS.

Suricata como IPS no Linux

- Em virtude da possibilidade de bloqueios via comando da NFQUEUE, o Suricata poderá ser instalado em máquinas finalísticas (HIPS).

Sumário

Suricata + Fail2ban

- O Fail2ban é um analisador de logs, em tempo real, com capacidade de bloqueio com base em eventos de log.
- O endereço IP do infrator será bloqueado por tempo determinado pelo administrador da rede.
- Nesse caso, o Fail2ban deverá aliar-se ao Suricata em modo IDS.
- A diferença é que o Suricata, como IPS, descartará pacotes maliciosos. Já a sua associação com o Fail2ban bloqueará totalmente o atacante por um período de tempo.
- Para detalhes, veja a minha palestra “Controle de anomalias e bloqueio de ataques em redes em tempo real”.

Sumário

Personalização de regras

- É possível desabilitar regras, modificar regras existentes e criar regras novas.
- O manual oficial do Suricata possui mais de 90 páginas que explicam, de forma simples e direta, como funcionam as regras.
- Você também poderá estudar as regras existentes. Elas estão em /etc/suricata/rules/.
- Para desabilitar uma regra, basta comentá-la com ‘#'.
- É necessário ter cuidado com o Oinkmaster, pois atualizações poderão reverter algum trabalho feito anteriormente.

Personalização de regras

- Para evitar que o Oinkmaster reative uma regra comentada, basta editar o arquivo /etc/oinkmaster.conf e inserir uma linha 'disablesid' com o número 'sid' da regra. Exemplo:

```
disablesid 2102011
```

- No mesmo arquivo é possível fazer uma série de operações com regras, incluindo alterações automáticas após cada atualização.
- Além disso, você poderá ter as suas próprias regras. O arquivo é bem comentado, bastando ler para aprender.

Sumário

Conclusão

- O Suricata é um IDS/IPS versátil e com muitas características interessantes.
- A sua boa performance como IPS é facilitada pelo uso de NFQ.
- Há diversas regras prontas, atualizadas constantemente.
- É possível ter regras personalizadas.
- Participações especiais nesta palestra: Suricata Léo e Samoieda Lua.

Sumário

Referências

- Suricata. https://suricata-ids.org
- Suricata no Debian. https://wiki.debian.org/suricata
- NFQUEUE. https://home.regit.org/netfilter-en/using-nfqueue-and-libnetfilter_queue/
- man iptables-extensions
- Sistemas de firewall, disponível em http://eriberto.pro.br/palestras
- Controle de anomalias e bloqueio de ataques em redes em tempo real, disponível em http://eriberto.pro.br/palestras

Esta palestra está disponível em:

http://eriberto.pro.br

Siga-me no Twitter @eribertomota