YDAYS

SURICATA

INTRODUCTION À SURICATA

Qu'est-ce que Suricata ?

Suricata est un moteur de détection d'intrusion en réseau (NIDS), de prévention d'intrusion (IPS) et un analyseur de paquets de haute performance. Il est open-source et conçu pour détecter et prévenir les attaques réseau en surveillant le trafic en temps réel.

INTRODUCTION À SURICATA

Détection d'intrusion (IDS/IPS)

Suricata peut être configuré pour fonctionner comme un système de détection d'intrusion (IDS) ou un système de prévention des intrusions (IPS). En mode IDS, il surveille le réseau et génère des alertes sur les événements suspects, tandis qu'en mode IPS, il peut bloquer automatiquement les attaques en temps réel.

INTRODUCTION À SURICATA

Détection d'intrusion (IDS/IPS)

Suricata peut être configuré pour fonctionner comme un système de détection d'intrusion (IDS) ou un système de prévention des intrusions (IPS). En mode IDS, il surveille le réseau et génère des alertes sur les événements suspects, tandis qu'en mode IPS, il peut bloquer automatiquement les attaques en temps réel.

INTRODUCTION À SURICATA

Journalisation et alertes

- Suricata peut générer des alertes en cas d'attaque détectée, et enregistrer des informations détaillées dans des fichiers de log.

- Il prend en charge des formats de journalisation comme JSON pour une analyse facile et l'intégration avec des outils externes comme ELK Stack (Elasticsearch, Logstash, Kibana).

INTRODUCTION À SURICATA

Détection de signature et anomalies

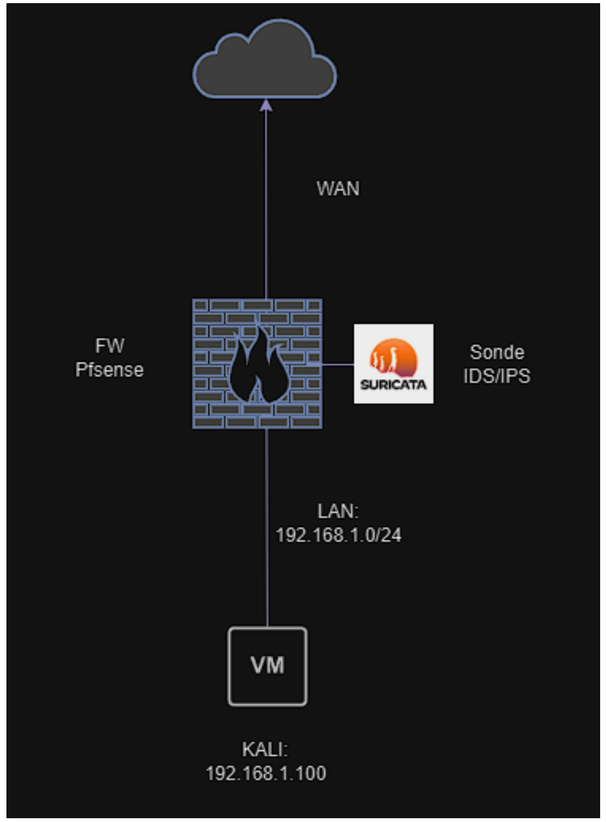
- Suricata utilise des règles de signature pour identifier les comportements malveillants, similaires à d'autres systèmes IDS/IPS.

- Il peut également détecter des comportements anormaux en utilisant des techniques comme l'analyse de flux et des heuristiques.

DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

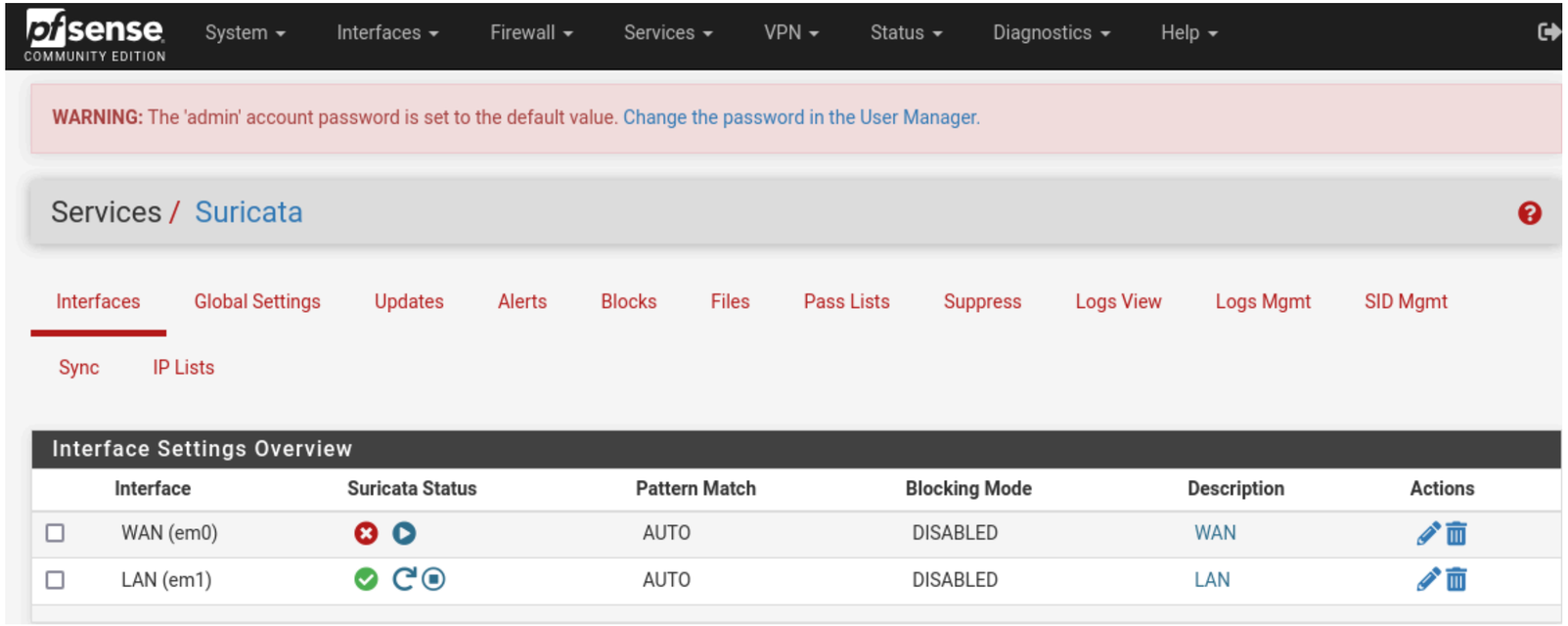
- **Topologie:**



DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

- **Configuration de suricata sur l'interface LAN pour la démo mais on peut également et surtout le faire sur l'interface WAN:**



DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

- **Configuration de suricata sur l'interface LAN pour la démo mais on peut également et surtout le faire sur l'interface WAN:**

J'ai effectué des règles personnalisées de détection:

alert tcp any any -> any any (msg:"SYN Scan Detected"; flags:S; threshold: type both, track by_src, count 20, seconds 3; sid:1000001; classtype:attempted-recon; rev:1;)

alert tcp any any -> any any (msg:"FIN Scan Detected"; flags:F; threshold: type both, track by_src, count 20, seconds 3; sid:1000002; classtype:attempted-recon; rev:1;)

alert icmp any any -> any any (msg:"Ping Echo Request Detected"; itype:8; threshold: type both, track by_src, count 5, seconds 10; sid:1000003; classtype:network-scan; rev:1;)

DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

1: règle pour détecter un scan SYN/FIN typique, ce qui est souvent utilisé par Nmap pour effectuer un scan furtif des ports ouverts

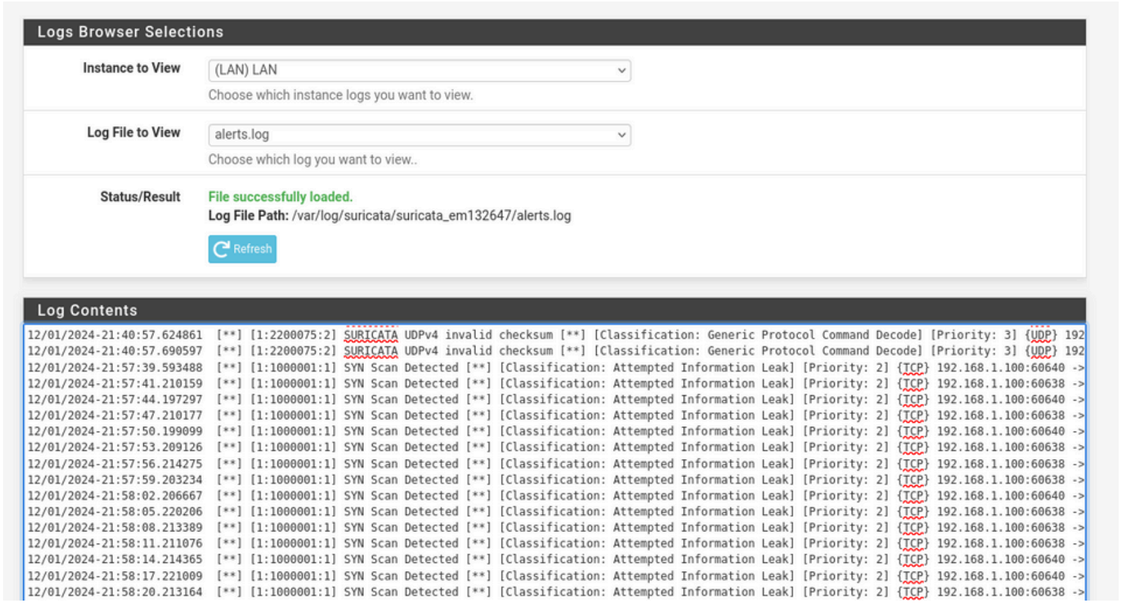
2: Règle pour détecter un ping (ICMP Echo Request)

DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

```
┌──(florent㉿kali)-[~]
└─$ nmap -v -sS -p 1-65535 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 22:48 CET
Initiating ARP Ping Scan at 22:48
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 22:48, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:48
Completed Parallel DNS resolution of 1 host. at 22:48, 0.00s elapsed
Initiating SYN Stealth Scan at 22:48
Scanning pfSense.home.arpa (192.168.1.1) [65535 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
SYN Stealth Scan Timing: About 16.23% done; ETC: 22:51 (0:02:40 remaining)
SYN Stealth Scan Timing: About 34.03% done; ETC: 22:51 (0:01:58 remaining)
SYN Stealth Scan Timing: About 57.70% done; ETC: 22:51 (0:01:07 remaining)
Completed SYN Stealth Scan at 22:50, 130.65s elapsed (65535 total ports)
Nmap scan report for pfSense.home.arpa (192.168.1.1)
Host is up (0.00052s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:E7:DB:7F (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 130.86 seconds
           Raw packets sent: 131171 (5.772MB) | Rcvd: 305 (30.344KB)
```




```
12/01/2024-21:57:39.593488  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60640 -> 192.168.1.1:1723
12/01/2024-21:57:41.210159  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60638 -> 192.168.1.1:17288
12/01/2024-21:57:44.197297  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60640 -> 192.168.1.1:32947
12/01/2024-21:57:47.210177  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60638 -> 192.168.1.1:7027
12/01/2024-21:57:50.199099  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60640 -> 192.168.1.1:37892
12/01/2024-21:57:53.209126  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60638 -> 192.168.1.1:33503
12/01/2024-21:57:56.214275  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60638 -> 192.168.1.1:61991
12/01/2024-21:57:59.203234  [**] [1:1000001:1] SYN Scan Detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.1.100:60638 -> 192.168.1.1:17777
```

DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

```
┌──(florent㉿kali)-[~]
└─$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.594 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.674 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.418 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.481 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.545 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.413 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=0.472 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=0.390 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=0.376 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=0.564 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=0.617 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=0.491 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=64 time=2.77 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=0.546 ms
```

```
12/01/2024-21:58:27.465530  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:58:37.712217  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:58:47.851179  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:58:58.058194  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:08.305985  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:18.474512  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:28.692173  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:38.868891  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:49.066651  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-21:59:59.278853  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
12/01/2024-22:00:09.450914  [**] [1:1000003:1] Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3]
{ICMP} 192.168.1.100:8 -> 192.168.1.1:0
```

DÉMONSTRATION AVEC UN FW PFSENSE

Démonstration

```
┌──(florent㉿kali)-[~]
└─$ sudo hping3 --flood --icmp 192.168.1.1
[sudo] password for florent:
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.1 hping statistic ---
1582794 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
DDoS ICMP Ping Flood Detected [**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
DDoS ICMP Ping Flood Detected [**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
DDoS ICMP Ping Flood Detected [**] [Classification: Attempted Denial of Service] [Priority: 2] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
Ping Echo Request Detected [**] [Classification: Detection of a Network Scan] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.1:0
```

QUESTIONS