SURICATA

Il sistema di rilevamento delle intrusioni Suricata ci consente di monitorare costantemente l'attività di rete su ogni singolo dispositivo.

Iniziamo il processo di implementazione di Suricata procedendo con la sua installazione sull'endpoint con i seguenti comandi:

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
```

Analogamente ad un firewall, durante l'installazione di Suricata è fondamentale definire un set di regole precise che determineranno i tipi di traffico da monitorare e gli eventi da segnalare come allarmi.

```
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```

Per adattare Suricata alle specifiche esigenze di monitoraggio del server, è necessario modificare il file di configurazione "suricata.yaml". In particolare, all'interno della sezione 'external net', andrà specificato l'indirizzo IP esatto del server oggetto di analisi, precedentemente inserito nella voce "home_net". Impostando il valore 'any' per questo parametro, si garantirà il monitoraggio di tutto il traffico in entrata e in uscita dal dispositivo.

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.1.11]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    #EXTERNAL_NET: "!$HOME_NET"
    EXTERNAL_NET: "any"
```

Per garantire un monitoraggio completo e aggiornato del traffico di rete, abbiamo configurato Suricata indicando nel file di configurazione il percorso della directory contenente i rule set. Utilizzando il parametro '*.rules', abbiamo attivato l'utilizzo di tutte le regole disponibili, assicurandoci così di essere protetti dalle ultime minacce conosciute

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - *.rules
```

Per concentrare l'analisi del traffico sulla interfaccia di rete desiderata, ne specifichiamo il nome o l'indirizzo all'interno della configurazione di Suricata.

```
# Linux high speed capture support
af-packet:
  - interface: enp0s3
    # Number of receive threads. "
    #threads: auto
    # Default clusterid. AF_PACKET
    cluster-id: 99
```

Procediamo al riavvio del servizio per rendere effettive le modifiche di Suricata.

```
root@ecommerceserver:/etc/suricata# systemctl restart suricata
root@ecommerceserver:/etc/suricata# systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Sun 2024-10-27 12:14:33 UTC; 13s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 6113 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 12 (limit: 9386)
     Memory: 63.6M
        CPU: 196ms
     CGroup: /system.slice/suricata.service
             └─6122 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run

Oct 27 12:14:33 ecommerceserver systemd[1]: Starting LSB: Next Generation IDS/IPS...
Oct 27 12:14:33 ecommerceserver suricata[6113]: Likely stale PID 5949 with /var/run/sur
Oct 27 12:14:33 ecommerceserver suricata[6113]: Removing stale PID file /var/run/surica
Oct 27 12:14:33 ecommerceserver suricata[6113]: Starting suricata in IDS (af-packet) mo
Oct 27 12:14:33 ecommerceserver systemd[1]: Started LSB: Next Generation IDS/IPS.
lines 1-16/16 (END)
```

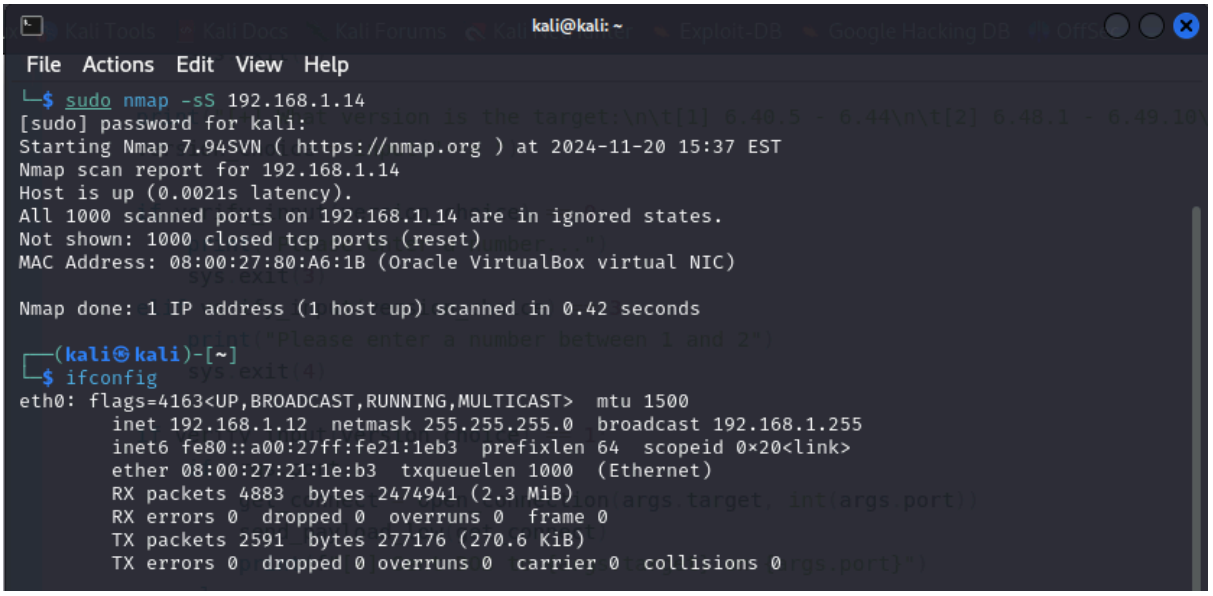
Accediamo a /var/ossec/etc per modificare il file di configurazione di Wazuh, in modo tale che i log generati da Suricata vengano inoltrati alla dashboard di Wazuh aggiungendo i seguenti parametri:

```
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

Procediamo al riavvio dell’agent di Wazuh per rendere efficaci tali modifiche.

Rilevazione Minacce

Da una macchina Kali sulla stessa rete lancio una scansione nmap sul server dove abbiamo installato Suricata



Possiamo notare su Wazuh come grazie a Suricata riusciamo a rilevare tali eventi di rete sull'endpoint, da notare i campi 'agent-ip'(macchina ubuntu dove ho installato Suricata) e src_ip(macchina kali da cui lancio nmap) nei log.