

es 1

→ soluzione github:

Prima di tutto, dobbiamo andare su wireshark e collegarci su netflix.com, ed inserire l'opzione `resolve names` nelle impostazioni di wireshark, in modo da catturare l'url delle CDN di netflix e ricevere gli alert quando abbiamo un video stream.

A questo punto, prendiamo alcuni degli url di queste CDN, ed inseriamole in una regola in un files `seclab.rules`, sottoforma di regola di suricata.

```
alert tls any any -> any any (msg:"Netflix video stream 1";  
tls_sni; content:"oca.nflxso.net"; isdataat:!1,relative; fl  
ow:to_server,established; flowbits: set,traffic/id/netflix;  
flowbits:set,traffic/label/social-network; sid:303080301; r  
ev:1;)
```

RICORDA: devi cambiare il `sid` di ogni regola in modo che non ci siano due regole con lo stesso `sid` !! In questo modo, ci dovrebbe avvisare ogni volta che si fa una chiamata a `oca.nflxso.net`, che il suffisso di uno degli hostname del CDN.

Dunque, testiamo il tutto. Carichiamo il file di configurazione e il file delle regole su suricata in questo modo (NOTA: l'interfaccia di rete potrebbe essere diversa sul tuo pc):

```
suricata -c suricata.yaml -l logs -s seclab.rules -i enp0s3  
1f6
```

I log compariranno nella cartella `logs`.

→ soluzione chatgpt:

Per identificare il traffico in uscita verso il portale `netflix.com` utilizzando Suricata, è necessario scrivere una regola che monitori il traffico di rete diretto a quell'indirizzo. Suricata è un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS) che può analizzare il traffico di rete in tempo reale.

Ecco come creare e validare una regola Suricata per identificare il traffico verso `netflix.com`:

1. Identificazione degli IP di Netflix

Per creare una regola efficace, è necessario conoscere gli indirizzi IP che corrispondono a `netflix.com`. Netflix utilizza una rete di Content Delivery Network (CDN) con molti IP distribuiti geograficamente. Un approccio è ottenere una lista di questi IP tramite DNS.

2. Creazione della Regola Suricata

Dopo aver ottenuto una lista di IP associati a `netflix.com`, si può scrivere una regola Suricata. Di seguito un esempio di regola che può essere utilizzata:

```
alert http $HOME_NET any -> [IP1, IP2, IP3, ...] any (msg:"Access to Netflix"; flow:to_server,established; content:"netflix.com"; http_host; nocase; classtype:policy-violation; sid:1000001; rev:1;)
```

Oppure si può usare il dominio:

```
alert http $HOME_NET any -> netflix.com any (msg:"Access to Netflix"; flow:to_server,established; content:"nextlix.com"; http_host; nocase; classtype:policy-violation; sid:100001; rev:1;)
```

Spiegazione della Regola:

- `alert http`: La regola genera un allarme per il protocollo HTTP.
- `$HOME_NET any -> [IP1, IP2, IP3, ...] any`: Monitorizza il traffico in uscita dal network locale (`$HOME_NET`) verso gli IP di Netflix su qualsiasi porta.
- `msg:"Access to Netflix"`: Messaggio che verrà visualizzato quando la regola viene attivata.
- `flow:to_server,established`: Considera solo il traffico in direzione del server (uscita) con connessione stabilita.
- `content:"netflix.com"; http_host; nocase`: Cerca la stringa `netflix.com` nell'header `Host` delle richieste HTTP, ignorando la differenza tra maiuscole e minuscole.

- `classtype:policy-violation` : Categoria dell'allarme.
- `sid:1000001` : Identificatore univoco della regola.
- `rev:1` : Revisione della regola.

3. Validazione della Regola

Per validare la regola, è necessario eseguire Suricata in modalità IDS e verificare che la regola generi allarmi quando si accede a `netflix.com`.

Passi per la Validazione:

1. Aggiornare il file delle regole di Suricata:

Aggiungere la regola sopra descritta nel file delle regole di Suricata (di solito

`local.rules`).

2. Riavviare Suricata:

Riavviare il servizio Suricata per applicare le nuove regole:

```
sudo systemctl restart suricata
```

3. Generare il traffico verso Netflix:

Accedere al portale

`netflix.com` tramite un browser o altri strumenti di rete.

4. Verificare i log di Suricata:

Controllare i log di Suricata (di solito in

`/var/log/suricata/alerts.log`) per vedere se la regola è stata attivata:

```
cat /var/log/suricata/alerts.log | grep "Access to Netfl
ix"
//se non funziona allora usare fast.log
```

4. Aggiornamenti Dinamici

Dato che gli IP di `netflix.com` possono cambiare, potrebbe essere utile implementare uno script che aggiorna periodicamente gli IP e aggiorna la regola di conseguenza.

Esempio di Script per Aggiornare IP:

Ecco un esempio di come potrebbe essere uno script per aggiornare gli IP:

```
#!/bin/bash

# File delle regole di Suricata
RULES_FILE="/etc/suricata/rules/local.rules"

# Ottenere gli IP di netflix.com
IPS=$(dig +short netflix.com)

# Generare la nuova regola
RULE="alert http \\$HOME_NET any -> [$(echo $IPS | tr ' '
',')] any (msg:\\\\"Access to Netflix\\"; flow:to_server,established; content:\\\\"netflix.com\\"; http_host; nocase; clas
stype:policy-violation; sid:1000001; rev:2;)"

# Aggiornare il file delle regole
echo "$RULE" > $RULES_FILE

# Riavviare Suricata
sudo systemctl restart suricata
```

Conclusione

Seguendo questi passi, si può creare e validare una regola Suricata per identificare il traffico in uscita verso `netflix.com`. È importante mantenere aggiornate le liste degli IP per garantire l'efficacia della regola.