es 2

Per creare una regola Suricata che scateni un alert quando il contenuto di un pacchetto MQTT contiene la stringa "flag", segui questi passaggi:

1. Abilitare la funzionalità `payload-printable`

Prima di creare la regola, assicurati di abilitare la funzionalità `payload-printable` nel file di configurazione di Suricata (`suricata.yaml`). Questo ti permetterà di vedere il contenuto dei pacchetti nei log di Suricata.

Apri il file `suricata.yaml` e cerca la sezione `alert-debug`. Dovrebbe apparire come segue:

```
outputs:
  - alert-debug:
      enabled: yes
      filename: alert-debug.log
      append: yes
      payload: yes             # enables dumping payload in
Base64
      payload-printable: yes   # enable dumping payload in
printable (lossy) format
      packet: yes              # enables dumping of packet
(without stream segments)
      http-body: yes           # requires the HTTP log deco
der be enabled and logging of bodies enabled in the HTTP co
nfig
```

Assicurati che `payload-printable` sia impostato su `yes`.

2. Creazione della regola Suricata

Ora crea una regola Suricata per rilevare il contenuto "flag" nei pacchetti MQTT. Di seguito un esempio di regola:

```
alert tcp any any -> any any (msg:"MQTT flag detected"; con
tent:"flag"; nocase; classtype:misc-activity; sid:1000002;
rev:1;)
```

Spiegazione della Regola:

- `alert tcp any any -> any any`: La regola si applica a tutto il traffico TCP indipendentemente dagli indirizzi IP e dalle porte.
- `msg:"MQTT flag detected"`: Messaggio che verrà visualizzato quando la regola viene attivata.
- `content:"flag"`: Cerca la stringa "flag" nel contenuto del pacchetto.
- `nocase`: Ignora le differenze tra maiuscole e minuscole.
- `classtype:misc-activity`: Categoria dell'allarme.
- `sid:1000002`: Identificatore univoco della regola.
- `rev:1`: Revisione della regola.

3. Aggiornamento delle regole di Suricata

Aggiungi la regola creata al file delle regole locali di Suricata (`local.rules`):

```
echo 'alert tcp any any -> any any (msg:"MQTT flag detecte
d"; content:"flag"; nocase; classtype:misc-activity; sid:10
00002; rev:1;)' >> /etc/suricata/rules/local.rules
```

4. Riavvio di Suricata

Riavvia Suricata per applicare le nuove regole:

```
sudo systemctl restart suricata
```

5. Verifica dei log di Suricata

Genera del traffico MQTT che contiene la stringa "flag" e controlla i log di Suricata per vedere se la regola viene attivata. I log si trovano di solito in `/var/log/suricata/alert-debug.log`.

```
cat /var/log/suricata/fast.log | grep "MQTT flag detected"
```

6. Ricostruzione della Flag

Controlla il contenuto dei pacchetti nei log di Suricata per trovare i "pezzi" della flag nel formato `SEC{qualcosa}` e ricostruiscila.

Conclusione

Seguendo questi passaggi, sarai in grado di creare una regola Suricata che rileva il contenuto "flag" nei pacchetti MQTT e visualizzare i log dei pacchetti. Assicurati di verificare e testare la regola con del traffico MQTT reale per garantire che funzioni correttamente.