Snort3-regels begrijpen

Inhoud

Inleiding

In dit document worden regels beschreven voor het **Snort3** Engine in Cisco **Secure Firewall Threat Defense (FTD)**.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco-software **Secure Firewall Threat Defense (FTD)**
- **Intrusion Prevention System (IPS)**
- **Snort2** syntaxis

Licentie

Geen specifieke vergunningsvereiste, de basisvergunning is toereikend en de vermelde kenmerken zijn opgenomen in de **Snort**-motor binnen het FTD en in de open source-versies van **Snort3**.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco-software **Secure Firewall Threat Defense (FTD)**, Cisco **Secure Firewall Management Center (FMC)** versie

7.0+ met **Snort3**.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Snort is de Cisco IPS-engine die realtime verkeersanalyse en pakketvastlegging kan uitvoeren.

Snort U kunt protocolanalyse, contentzoeken uitvoeren en aanvallen detecteren.

Snort3 is een bijgewerkte versie van de Snort2 IPS met een nieuwe softwarearchitectuur die de prestaties, detectie, schaalbaarheid en bruikbaarheid verbetert.

Snort3-regels

Ze gebruiken dat LUA-formaat om de **Snort3** regels gemakkelijker te lezen, te schrijven en te verifiëren.

Regelgevende acties

Deze nieuwe versie wijzigt de regelacties, de nieuwe definities zijn:

- **Pass**: Stop de evaluatie van volgende regels tegen pakket
- **Alert**: alleen gebeurtenis genereren
- **Block**: Drop-pakket, blokrestant-sessie
- **Drop**: alleen drop-pakket
- **Rewrite**: Vereist als de vervangingsoptie wordt gebruikt
- **React**: Verzend de pagina met reacties op HTML-blokken
- **Reject**: Injecteer TCP/RST of ICMP onbereikbaar

Regel-anatomie

De anatomie is:

De regelkop bevat de actie-, protocol-, bron- en doelnetwerk(en) en poort(en).

In **Snort3**Kan de regelkop een van de volgende opties zijn:

- Kop voor serviceregel

```
<iline" lang="lua">alert http ( msg:"Alert HTTP rule"; flow:to_client,established;
content:"evil", nocase; sid:1000001; )
```

- Kop voor bestandsregel

```
alert file ( msg: “Alert File example”; file_data; content:”malicious_stuff”; sid:1000006; )
```

- Koptekst voor conventionele regels

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert HTTP rule";
flow:to_client,established; content:"evil", nocase; sid:1000001; )
```

Regelkenmerken

Enkele nieuwe functies zijn:

- Willekeurig 'whitespace' (elke optie op zijn eigen regel)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert TCP rule";
flow:to_client,established; content:"evil", nocase; sid:1000000; )
```

- het consequente gebruik van en ;

```
content:"evil", offset 5, depth 4, nocase;
```

- Netwerken en poorten zijn optioneel

```
alert http ( Rule body )
```

- Voegt meer kleverige buffers toe (Dit is niet de volledige lijst)

```
http_uri http_raw_uri http_header http_raw_header http_trailer http_raw_trailer http_cookie
http_raw_cookie http_true_ip http_client_body http_raw_body http_method http_stat_code
http_stat_msg http_version http2_frama_header script_data raw_data
```

- Opmerkingen C-stijl

```
alert http ( msg:"Alert HTTP rule"; /* I can write a comment here */ ... )
```

- Trefwoord voor opmerking (opmerking)

```
alert http ( msg:"Alert HTTP rule"; flow:to_client,established; rem:"Put comments in the rule
anywhere"; content:"evil", nocase; sid:1000001; )
```

- trefwoorden toevoegen

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Alert on apps"; appids:"Google, Google
Drive"; content:"evil", nocase; sid:1000000; )
```

- sd_patterns voor het filteren van gevoelige gegevens
- Regex-trefwoord met behulp van hyperflex-technologie
- Service-trefwoord vervangt metagegevens

Voorbeelden

Voorbeeld met http service header en sticky buffer http_uri

Taak: Schrijf een regel die het woord detecteert **malicious** in de HTTP-URI.

Oplossing:

```
alert http ( msg:"Snort 3 http_uri sticky buffer"; flow:to_server,established; http_uri;
content:"malicious", within 20; sid:1000010; )
```

Voorbeeld met header bestandsservice

Taak: Schrijf een regel waarmee PDF-bestanden worden gedetecteerd.

Oplossing:

```
alert file ( msg:"PDF File Detected"; file_type: "PDF"; sid:1000008; )
```

Verwante links

Snelheidsregels en IDS-softwaredownloads

Github

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.