Informazioni sulle regole Snort3

Sommario

Introduzione

Questo documento descrive le regole per **Snort3** nel Cisco **Secure Firewall Threat Defense (FTD)**.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Licenze

Nessuna licenza specifica richiesta, la licenza di base è sufficiente e le funzionalità menzionate sono incluse nel motore **Snort** all'interno dell'FTD e nelle versioni open source **Snort3**.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco **Secure Firewall Threat Defense (FTD)**, Cisco **Secure Firewall Management Center (FMC)** versione 7.0+ con **Snort3**.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Snort è il motore Cisco IPS in grado di analizzare il traffico in tempo reale e di registrare i pacchetti.

Snort può eseguire l'analisi dei protocolli, la ricerca dei contenuti e il rilevamento di attacchi.

Snort3 è una versione aggiornata dell'IPS Snort2 con una nuova architettura software che migliora le prestazioni, il rilevamento, la scalabilità e la fruibilità.

Regole Snort3

Utilizzano il formato LUA per creare **Snort3** regole più facili da leggere, scrivere e verificare.

Azioni regola

Questa nuova versione modifica le azioni della regola. Le nuove definizioni sono:

- **Pass**: Interrompe la valutazione delle regole successive rispetto al pacchetto
- **Alert**: Genera solo evento
- **Block**: Elimina pacchetto, blocca sessione rimanente
- **Drop**: Elimina solo il pacchetto
- **Rewrite**: Obbligatorio se viene utilizzata l'opzione sostituisci
- **React**: Pagina di risposta blocco HTML
- **Reject**: inserimento di TCP RST o ICMP non raggiungibile

Anatomia delle regole

L'anatomia è:

L'intestazione della regola contiene l'azione, il protocollo, le reti di origine e di destinazione e le porte.

Dentro **Snort3**, l'intestazione della regola può essere una delle opzioni seguenti:

- Intestazione regola del servizio

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

- Intestazione regola file

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

- Intestazione regola convenzionale

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

Caratteristiche delle regole

Alcune delle nuove funzioni sono:

- Spazi vuoti arbitrari (ogni opzione in una riga distinta)

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

- l'uso coerente di , e ;

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

- Reti e porte sono opzionali

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

- Aggiunge altri buffer permanenti (elenco non completo)

```
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
```

- C Commenti sullo stile

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

- Parola chiave Note (rem)

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

- appids, parole chiave

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

- sd_pattern per il filtro dei dati sensibili
- Parola chiave Regex con l'utilizzo della tecnologia hyperflex
- La parola chiave Service sostituisce i metadati

Esempi

Esempio con intestazione del servizio http e buffer sticky http_uri

Attività: scrittura di una regola per il rilevamento della parola **malicious** nell'URI HTTP.

Soluzione:

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

Esempio con intestazione servizio file

Attività: consente di scrivere una regola per il rilevamento dei file PDF.

Soluzione:

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

Collegamenti correlati

Scaricare software Snort Rules e IDS

Github

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).