Informazioni su Snort 3: Valutazione delle firme stateful Byte_Jump

Sommario

Introduzione

Questo documento descrive le nuove tecniche aggiunte a Snort 3 a partire dalla 7.4.

Premesse

- Il modulo di rilevamento Snort 3 funziona in modalità blocco. Sebbene questo approccio offra un vantaggio in termini di prestazioni e una semplicità di implementazione (relativa), presenta alcune limitazioni nel rilevare le firme che si estendono su più blocchi di dati.
- Per semplificare l'esperienza dell'utente, in Snort sono già stati implementati alcuni miglioramenti, ovvero:
  1. I bit di flusso consentono al processo di scrittura delle regole di contrassegnare il flusso di rete con una proprietà definita dall'utente. Tale proprietà può essere impostata, cancellata e testata su qualsiasi pacchetto del flusso (consente di trarre conclusioni su una firma più grande rispetto ai pacchetti).
- Un modulo di flusso accumula pacchetti wire in un pacchetto ricostruito, che è un blocco più grande e più significativo di un pacchetto raw; valutare le regole IPS rispetto al pacchetto ricostruito dà più probabilità di vedere l'intera immagine e corrispondere a un modello più

grande (firma).
- In alcuni casi il pacchetto ricostruito presenta non solo dati nuovi, ma include anche una parte dei dati precedenti già elaborati dal rilevamento; anche in questo caso, il blocco di dati accumulati consente di rilevare firme che si estendono all'indietro nel flusso (in qualche misura).
- Uno splitter a flusso taglia il flusso in blocchi, ma il punto di taglio è potenzialmente un punto debole che l'attaccante potrebbe utilizzare per evitare il rilevamento di pattern; Snort ha quindi un meccanismo di tremolio implementato per rendere la divisione più imprevedibile. Questo complica ulteriormente l'analisi per l'aggressore.

Novità

La valutazione della firma con conservazione dello stato è una nuova tecnica che può essere aggiunta all'elenco. Estende le funzionalità di rilevamento abilitando la valutazione delle regole IPS su più blocchi. Pertanto, una regola non non corrisponde immediatamente se il blocco corrente è privo di dati, ma attende invece l'arrivo di un numero maggiore di dati.

Piattaforme supportate

Piattaforme software e hardware minime

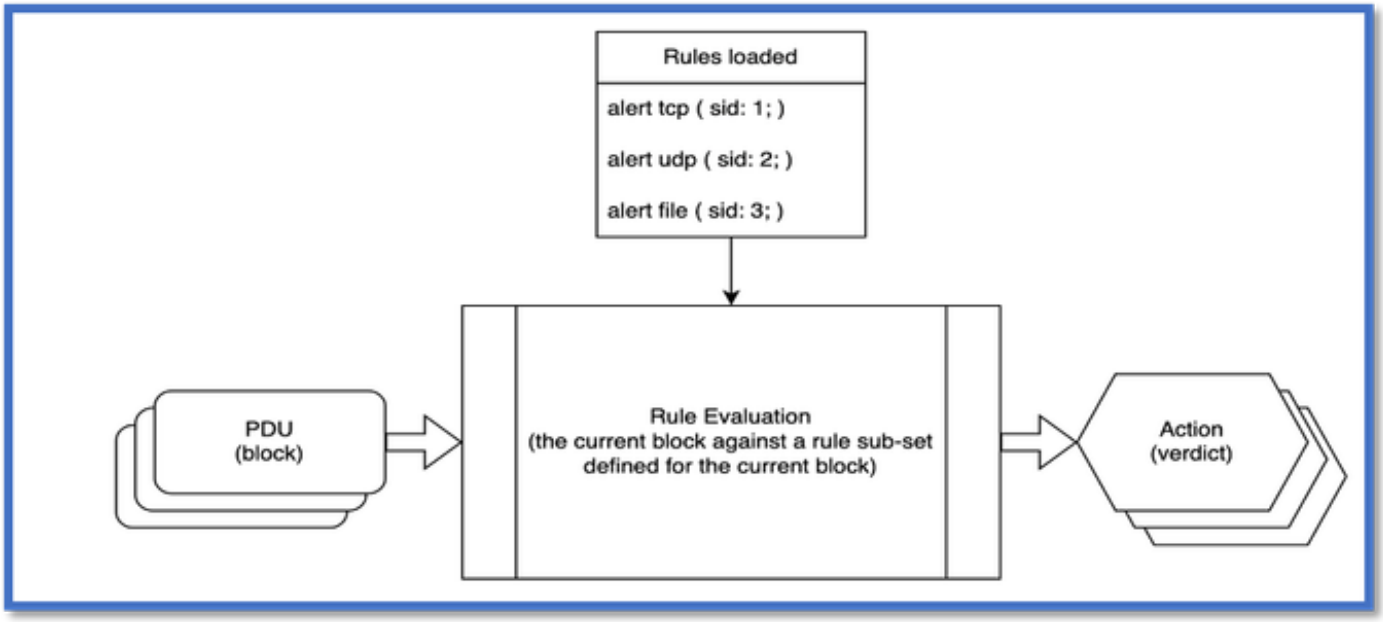
Versione minima di Gestione supportata	Dispositivi gestiti	Versione minima dispositivo gestito supportato richiesta	Note
Management Center 7.4.0	FTD	7.4.0	Solo snort 3
Device Manager 7.4.0	Qualsiasi FTD che supporta la gestione FDM	7.4.0	Solo snort 3

Dettagli funzionalità

Descrizione funzionalità funzionale

Come funziona?

Il flusso di lavoro del modulo di rilevamento è illustrato nel diagramma. Nella fase di elaborazione del traffico, il modulo ha già caricato tutte le regole e accetta blocchi di dati uno per uno, valuta le regole e definisce le azioni da intraprendere per il blocco di valutazione della firma con conservazione dello stato del processo.



Note sullo schema:

1. Una volta definito un sottoinsieme di regole per il blocco di dati corrente, ogni regola da esso derivata viene valutata indipendentemente da altre regole.
2. Ogni blocco di dati viene valutato in modo indipendente dagli altri blocchi.
3. Il blocco di dati è un'astrazione per un set di buffer IPS che vengono valutati per il pacchetto corrente.
4. Action è un elenco di azioni valutate per il pacchetto corrente; il verdetto finale viene determinato in seguito.

Per informazioni sul funzionamento della valutazione delle firme con conservazione dello stato, vedere come viene valutata una regola IPS comune e come i blocchi di dati possono formare un flusso.

Valutazione regole comuni

Una regola IPS può essere presentata nel seguente formato:

```
action protocol source → destination ( option_1: parameters; option_2: parameters;
option_3: parameters; gid: 1; sid: 1; meta_option_1; meta_option_2; meta_option_3; )
```

Dove:

azione - Azione IPS sul pacchetto se la regola viene attivata

protocollo - protocollo da associare

origine, destinazione - indirizzo IP e porta

option_1, option_2, option_3 - Opzioni IPS che fanno parte della valutazione della regola

gid, sid - coppia univoca che identifica la regola (sono come opzioni di metadati)

meta_option_1, meta_option_2, meta_option3 - metadati di regole come un messaggio, un tipo di classe o un riferimento. Queste opzioni non partecipano alla valutazione delle regole.

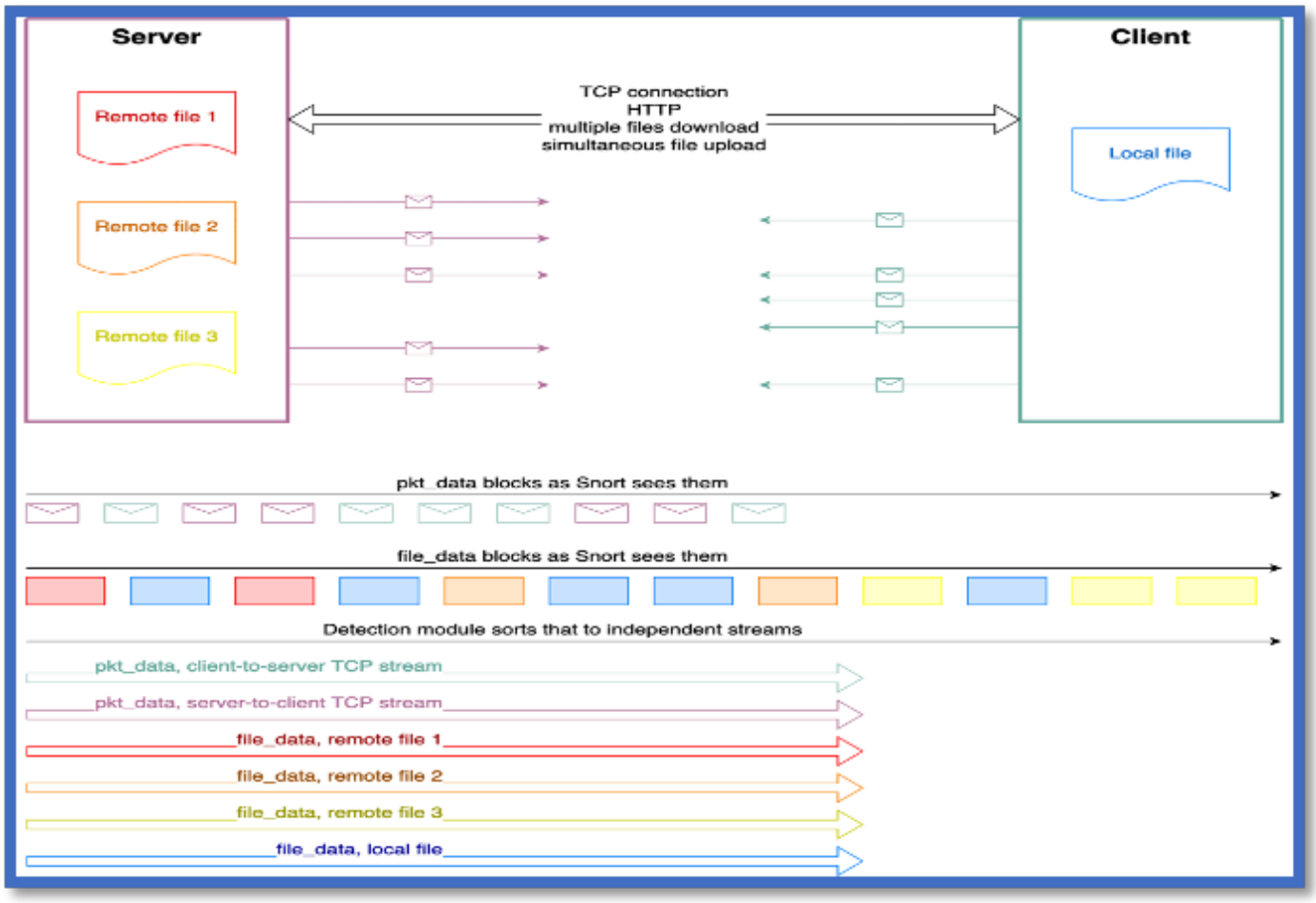
- Il protocollo, l'origine e la destinazione formano un'intestazione di regola. Funziona come un filtro per un flusso di rete (che viene accettato per la valutazione). Tutto tra parentesi è un corpo di regola. Le opzioni IPS (ad eccezione dei metadati della regola) del corpo della regola sono quelle valutate per il blocco di dati. Essi si conformano alle seguenti indicazioni:
- Le opzioni vengono valutate in base all'ordine da sinistra a destra.
    1. può essere uno dei due tipi principali.
    2. buffer setter, l'opzione seleziona il buffer IPS per il pacchetto corrente.
- altri (ricerca di pattern, operazioni matematiche, manipolazione del cursore, operazioni di flow bit)
- viene utilizzato un cursore per tenere traccia della posizione nel buffer IPS selezionato.

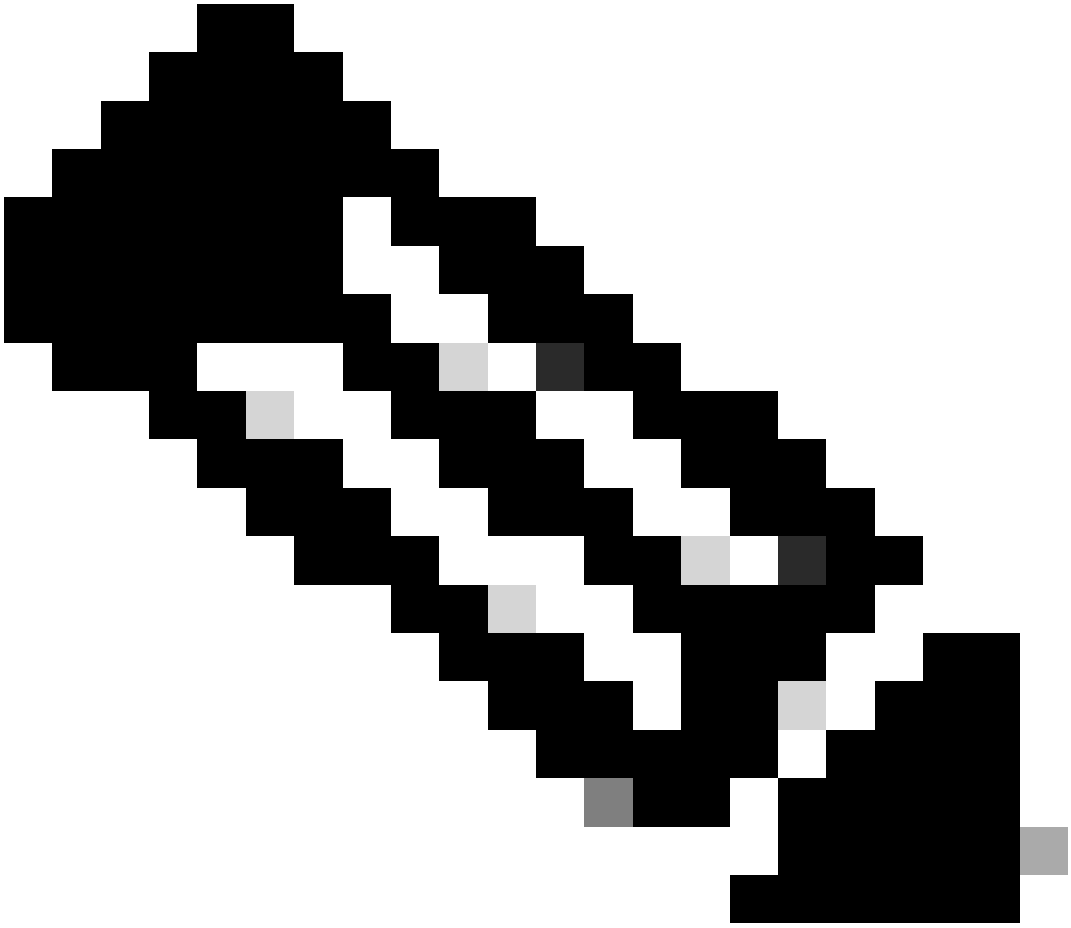
- un'opzione può essere:
    1. 'absolute', ovvero non dipende dalla posizione del cursore
    2. 'relative', ovvero inizia la valutazione dalla posizione del cursore
- se un'opzione tenta di impostare il cursore all'esterno del buffer IPS selezionato, l'operazione non riesce e l'intera regola non corrisponde (per mancanza di dati)
- L'ultimo punto è una limitazione del modulo di rilevamento. Se Snort può disporre di risorse illimitate, memorizza nella cache tutti i dati visualizzati per valutare le regole più e più volte quando i dati diventano disponibili (arrivano più pacchetti wire).

Flusso di dati e buffer IPS

- Il flusso di dati è un flusso di byte in un modulo contiguo dalla stessa origine. Si tratta di un nuovo concetto presentato a sostegno della valutazione stateful. La valutazione delle regole tra blocchi deve essere eseguita all'interno degli stessi dati logici (sia che si tratti di un file, di un puro flusso TCP o di testo JavaScript).

- In generale, un blocco di dati ricevuto dal modulo di rilevamento potrebbe:
    - Provenire da un buffer IPS diverso (ad esempio, pkt_data e file_data non sono uguali)
    - Appartiene a un altro flusso
    - Non da un flusso (buffer generati da un pacchetto non elaborato)
    - Non forma un flusso contiguo (ICMP, UDP)
    - Non essere in ordine (Risposta parziale HTTP)
    - Contengono dati ripetuti (un blocco accumulato, come in http_inspect.script_detection o HTTP Chunked Response)
- Il modulo di rilevamento può ordinare le cose per concatenare solo i blocchi dallo stesso flusso, altrimenti il processo di valutazione vedrebbe interferenze indesiderate dai blocchi di interfoliazione.


Server
Remote file 1
Remote file 2
Remote file 3
TCP connection
HTTP
multiple files download
simultaneous file upload
Client
Local file
pkt_data blocks as Snort sees them
file_data blocks as Snort sees them
Detection module sorts that to independent streams
pkt_data, client-to-server TCP stream
pkt_data, server-to-client TCP stream
file_data, remote file 1
file_data, remote file 2
file_data, remote file 3
file_data, local file



Nota: nell'esempio viene illustrato un caso in cui un client HTTP carica e scarica più file contemporaneamente.

- Al momento, solo due buffer IPS possono rappresentare un flusso: pkt_data e file_data, dove:
    1. pkt_data da due flussi per il protocollo TCP (direzioni client-server e server-client)
    2. file_data deve formare flussi per file, allegati MIME e altri dati di protocollo (come la pagina HTML HTTP e/o altri tipi di contenuto)
- La valutazione stateful viene eseguita esclusivamente all'interno del flusso di dati.

Continuazione regola

- La sezione termina con un'istruzione che indica che l'opzione IPS non corrisponde se il cursore viene impostato fuori dal buffer IPS corrente. Quando invece il buffer IPS forma un flusso di dati, la funzione di valutazione delle firme con conservazione dello stato interviene e salva il contesto di valutazione della regola nell'oggetto flusso di dati Snort. Il contesto di valutazione salvato (stato) è denominato continuazione delle regole. La valutazione della

firma con conservazione dello stato posticipa il verdetto finale della regola finché non saranno disponibili ulteriori dati.

- La continuazione della regola è composta da tre parti principali: nome del buffer IPS, origine del buffer e posizione del cursore di destinazione (l'origine del buffer è un identificatore univoco per il flusso di dati).
- Quando un blocco di dati viene elaborato dal modulo di rilevamento, vengono eseguite le azioni successive:-
  - La valutazione della firma con conservazione dello stato crea una continuazione della regola e la associa al flusso se:
    - L'opzione IPS (byte_jump, content, pcre o qualsiasi altro elemento che aggiorna la posizione del cursore) imposta il cursore dopo il buffer IPS corrente
    - Il buffer IPS corrente supporta il flusso di dati.
    - Il buffer IPS corrente forma attualmente un flusso di dati.
- La valutazione della firma con conservazione dello stato ritira la continuazione della regola appena creata e la rimuove dal flusso se:
  - La regola IPS è stata attivata sul blocco di dati corrente (la regola corrisponde su altre posizioni del blocco)
- La valutazione della firma con conservazione dello stato rifiuta le continuazioni della regola in sospeso e le rimuove dal flusso se:
  - Il buffer IPS non forma un flusso contiguo (ad esempio, i blocchi contengono dati ripetuti o è presente uno spazio (parte dei dati è stata persa o il blocco non è in ordine).
- La valutazione delle firme stateful aggiorna la posizione del cursore di destinazione con nuovi dati disponibili quando:
  - L'origine buffer dalla continuazione regola è uguale all'origine buffer selezionata
  - Il buffer IPS forma un flusso contiguo
- La valutazione della firma con conservazione dello stato invia la continuazione della regola al motore delle regole IPS quando:
  1. Punti di posizione del cursore di destinazione all'interno del buffer IPS selezionato (ovvero, ha ricevuto tutti i dati necessari per completare la valutazione della regola).

Configurazioni utente

- Poiché le continuazioni delle regole richiedono memoria, Snort non è in grado di archiviarne un numero illimitato. Per controllare il limite, è disponibile un'opzione di configurazione:
  1. Detection.max_continuations_per_flow = 1024: numero massimo di continuazioni memorizzate contemporaneamente nel flusso { 0:65535 }
- Quando la valutazione della firma con conservazione dello stato raggiunge il limite, sostituisce la continuazione della regola meno recente con una nuova.
- La continuazione della regola meno recente che risiede nel flusso è presente per troppo tempo, ovvero non soddisfa ancora una condizione per riprendere la valutazione della regola.
- Inoltre, sono disponibili numerosi conteggi di peg per ottimizzare le regole IPS (che devono essere l'obiettivo principale) e il limite (se necessario):
  1. detection.cont_creations: numero totale di continuazioni create (somma)
  2. detection.cont_returns: numero totale di continuazioni richiamate (somma)

3. detection.cont_flows: numero totale di flussi utilizzando la continuazione (somma)
4. detection.cont_evals: numero totale di continuazioni soddisfatte dalla condizione (somma)
5. detection.cont_matching: numero totale di continuazioni associate (somma)
6. detection.cont_mismatch: numero totale di continuazioni non corrispondenti (somma)
7. detection.cont_max_num: numero massimo di continuazioni simultanee per flusso (max)
8. detection.cont_match_distance: numero totale di byte passati dalle continuazioni corrispondenti (somma)
9. detection.cont_mismatch_distance: numero totale di byte saltati da continuazioni non corrispondenti (somma)

Risoluzione dei problemi

Questa funzionalità è un miglioramento del processo di rilevamento esistente, pertanto non è possibile risolvere il problema in modo esplicito. In caso di guasti nel rilevamento, le regole, la configurazione o il traffico devono essere esaminati.

Problema

Problema: descrizione

- Diciamo che una firma deve controllare contemporaneamente l'inizio del file e la coda.
- Ad esempio, in un file di destinazione di questa struttura (intestazione, corpo, metadati) è necessario verificare se uno dei relativi metadati ha un valore 0.

- Byte dei file: e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 dove

    - e1 f3 22 03 - 4 byte per il numero magico, che identifica il tipo di file
    - 7f ff - 2 byte per le dimensioni del corpo
    - xx xx ... xx - 32 kb di alcuni dati
    - 01 00 02 00 - 4 byte di metadati, in formato tag-value (1 byte per ciascuno)
- La regola IPS ha il seguente aspetto: alert file (file_data; contenuto:"|e1f32203|",fast_pattern; byte_jump:2,0,relative; contenuto:"00",within:4, relative; sid: 1;)

    - Dove

        - Il protocollo di file garantisce che la regola accetti solo pacchetti ricostruiti (i pacchetti non elaborati non partecipano alla valutazione della firma con stato)
        - L'opzione ‘file_data’ seleziona un buffer di dati che può formare un flusso
        - La prima opzione di contenuto è un pattern veloce e verifica la presenza del numero magico (se si tratta del tipo di file desiderato)
        - l'opzione byte_jump legge le dimensioni del corpo del file e passa al corpo del file
        - La seconda opzione di contenuto esegue il controllo finale dei valori dei metadati, entro i limiti dei parametri, e rende l'opzione relativa.

Problema: soluzione

La regola verrebbe valutata nel modo seguente:

Sul primo pacchetto (di dimensioni 8kB), che contiene un'intestazione di file e una parte del corpo:

1. È stato selezionato il buffer dati_file IPS. Il cursore punta allo 0° byte e1.
2. L'opzione di pattern veloce corrisponde e imposta la posizione del cursore subito dopo il numero magico, puntando al byte 7f.
3. L'opzione byte_jump legge due byte di dimensioni del corpo del file. Il cursore viene aggiornato da questi due byte. Quindi byte_jump calcola un collegamento per oltre 32768 byte.
4. la valutazione della firma con conservazione dello stato crea una continuazione della regola, dove sono necessari altri 24578 byte (32768 - (8 kB - 4 byte di intestazione - 2 byte di dimensioni del corpo)).
5. L'intera regola non corrisponde, poiché l'opzione byte_jump non riesce a impostare la posizione del cursore in tale punto.

Sul secondo pacchetto (di dimensioni 16kB), che trasporta la parte del corpo del file:

1. durante la valutazione della firma con conservazione dello stato viene rilevata la continuazione della regola in sospeso.
2. Il buffer viene selezionato in base al nome e viene verificato che file_data sia disponibile e che la nuova dimensione dei dati sia 16384.
3. Il cursore aggiornato indica che sono ancora necessari 8194 byte (24578 - 16384)
4. La regola non viene ripresa.

Al terzo pacchetto (di dimensioni 8198), che trasporta la parte del corpo del file e i metadati:

1. durante la valutazione della firma con conservazione dello stato viene rilevata la continuazione della regola in sospeso.
2. Il buffer viene selezionato in base al nome e viene verificato che file_data sia disponibile e che la nuova dimensione dei dati sia 8198.
3. Il cursore aggiornato mostra che il buffer contiene dati sufficienti. La posizione del cursore è 8194.
4. la valutazione della firma con stato elimina la continuazione della regola.
5. la valutazione della firma con conservazione dello stato riprende la valutazione della regola dalla seconda opzione di contenuto con il cursore posizionato sul byte 01.
6. L'opzione di contenuto trova una corrispondenza nel secondo byte cercato.
7. Tutta la regola finalmente spara.

Dettagli limitazioni e problemi comuni

Limitazioni E Altre Considerazioni

- A causa dell'implementazione della valutazione delle firme con conservazione dello stato, Snort elimina tutte le continuazioni delle regole in sospeso quando ricarica la configurazione.

Si noti che le continuazioni delle regole, nonostante siano state eliminate, occupano comunque la memoria Snort finché il blocco di dati successivo non viene inviato al modulo di rilevamento.

- La funzionalità di latenza delle regole per la regola IPS nella valutazione con conservazione dello stato ha lo stesso effetto di una valutazione comune delle regole. Viene riepilogato il tempo di valutazione per le parti della regola in blocchi di dati diversi. Se il tempo supera il limite, la valutazione della regola esegue un cortocircuito, chiudendo prima.
- Le operazioni Flowbits mantengono il loro significato, anche se vengono comunque eseguite come opzioni "statiche".
  Un'operazione di impostazione/cancellazione/test del bit di flusso viene eseguita in un contesto attualmente noto. Pertanto, se l'opzione flowbit viene valutata in una continuazione di regola, prenderà in considerazione l'ambiente corrente (set di flowbit), non quello in cui la regola ha iniziato la valutazione.

Inoltre, un processo di scrittura delle regole deve prestare attenzione alla posizione dello schema veloce.

Anche se può trovarsi in qualsiasi parte della regola, l'opzione di scelta rapida viene valutata prima dell'intera regola. Viene attivata la valutazione delle regole. Per la regola basata sulla valutazione della firma con conservazione dello stato, il punto di continuazione della regola deve trovarsi dopo l'opzione di pattern rapido.
Inoltre, la regola IPS può avere più continuazioni di regola nella valutazione (una dopo l'altra, non contemporaneamente). Poiché qualsiasi opzione del corpo della regola può avere la propria continuazione, il processo di scrittura della regola consente di eseguire controlli aggiuntivi in posizioni diverse del flusso di dati con la stessa regola IPS.

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).