Fase 7 della risoluzione dei problemi del percorso dei dati di Firepower: Policy anti-intrusione

Sommario

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi ai percorsi di dati, consultare l'articolo di panoramica.

In questo articolo viene illustrata la settima fase della risoluzione dei problemi relativi al percorso dati di Firepower, ovvero la funzionalità relativa ai criteri per le intrusioni.

Prerequisiti

- Questo articolo è applicabile a tutte le piattaforme Firepower che eseguono criteri di intrusione La funzione **trace** è disponibile solo nella versione 6.2 e successive per la piattaforma Firepower Threat Defense (FTD)
- Conoscenza di Snort open source è utile, anche se non richiesto Per informazioni su Snort open source, visitare il sito https://www.snort.org/

Risoluzione dei problemi relativi alla fase dei criteri per le intrusioni

Utilizzo dello strumento "trace" per rilevare le interruzioni dei criteri (solo FTD)

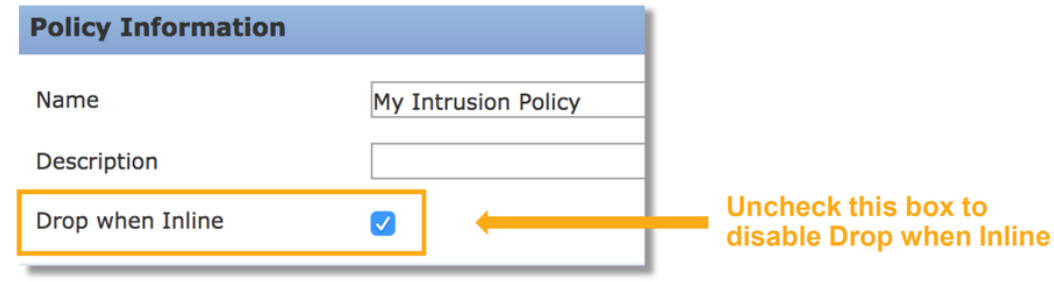
Lo strumento di traccia di supporto del sistema può essere eseguito dall'interfaccia della riga di comando FTD (CLI). Questa procedura è simile allo strumento **firewall-engine-debug** menzionato nell'articolo della fase Access Control Policy, con la differenza che consente di analizzare in modo più approfondito i meccanismi interni di Snort. Ciò può essere utile per verificare se sul traffico interessante vengono attivate regole dei criteri per le intrusioni.

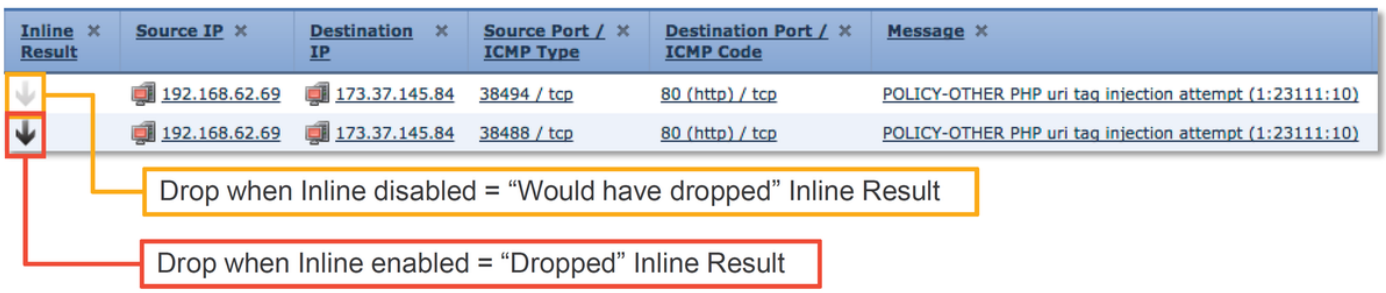
Nell'esempio seguente, il traffico proveniente dall'host con indirizzo IP 192.168.62.6 viene bloccato da una regola dei criteri per le intrusioni (in questo caso, **1:23111**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Notate che l'azione applicata da snort è **caduta**. Quando una perdita viene rilevata da snort, quella particolare sessione viene quindi inserita nella lista nera in modo che vengano scartati anche tutti i pacchetti aggiuntivi.

Il motivo per cui snort è in grado di eseguire l'azione **drop** è che l'opzione "Drop when Inline" è abilitata all'interno della policy sulle intrusioni. È possibile verificare questa condizione nella pagina iniziale all'interno della politica sulle intrusioni. In Firepower Management Center (FMC), selezionare **Policies > Access Control > Intrusion** (Policy > Controllo di accesso > Intrusione), quindi fare clic sull'icona di modifica accanto al criterio in questione.





Se l'opzione "Drop When Inline" è disattivata, snort non elimina più i pacchetti in conflitto, ma avvisa comunque con il **risultato in linea** di "Will Have Dropped" (Rilascio in linea) negli eventi di intrusione.

Se l'opzione "Drop When Inline" è disabilitata, l'output di traccia mostra un'azione **che potrebbe essere interrotta** per la sessione di traffico in questione.

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

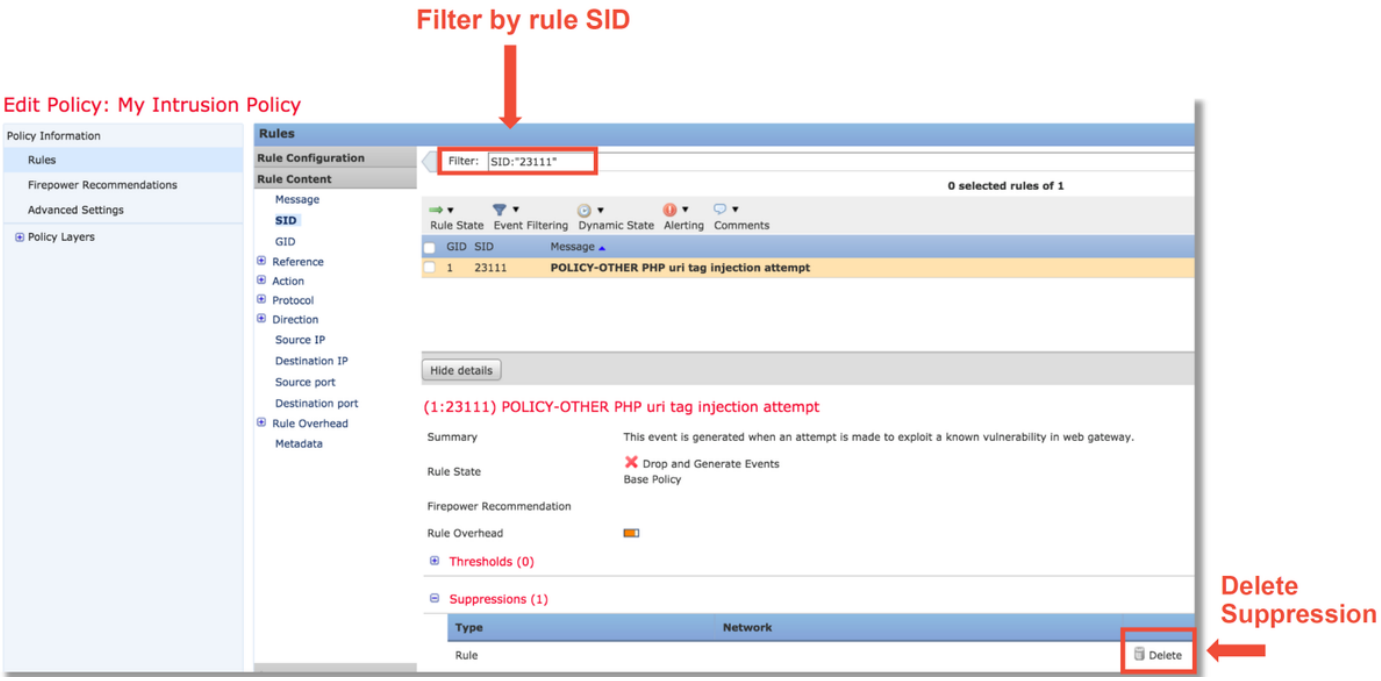
Verifica eliminazioni nei criteri per le intrusioni

Èpossibile che lo snort blocchi il traffico senza inviare eventi di intrusione al FMC (caduta silenziosa). A tale scopo, è necessario configurare le **eliminazioni.** Per verificare se è stata configurata una soppressione in un criterio di intrusione, è possibile controllare la shell degli esperti sul back-end, come illustrato di seguito.

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name       : My Intrusion Policy
```

Si noti che il criterio intrusione denominato "Criterio intrusione" contiene una soppressione per la regola 1:23111. Pertanto, il traffico può essere eliminato a causa di questa regola, senza alcun evento. Questo è un altro motivo per cui l'utilità di traccia può essere utile, poiché mostra ancora le cadute che si verificano.

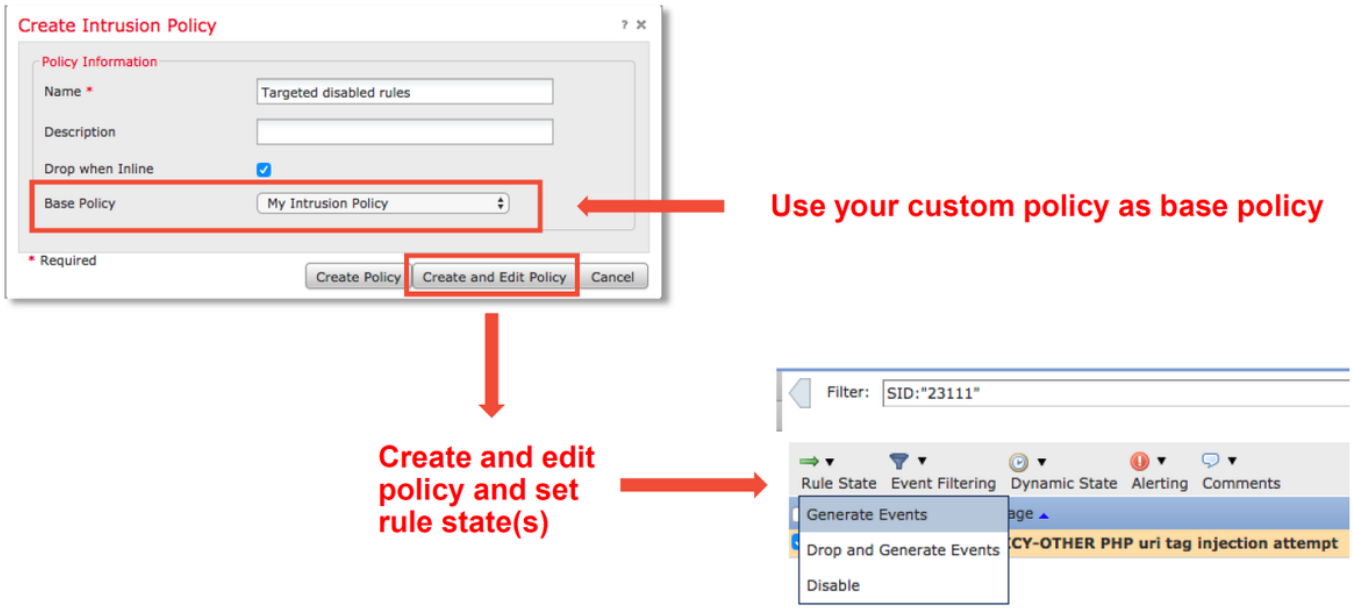
Per eliminare l'eliminazione, la regola in questione può essere filtrata all'interno della visualizzazione **Regole** dei criteri di intrusione. Viene visualizzata un'opzione per eliminare la soppressione, come illustrato di seguito.



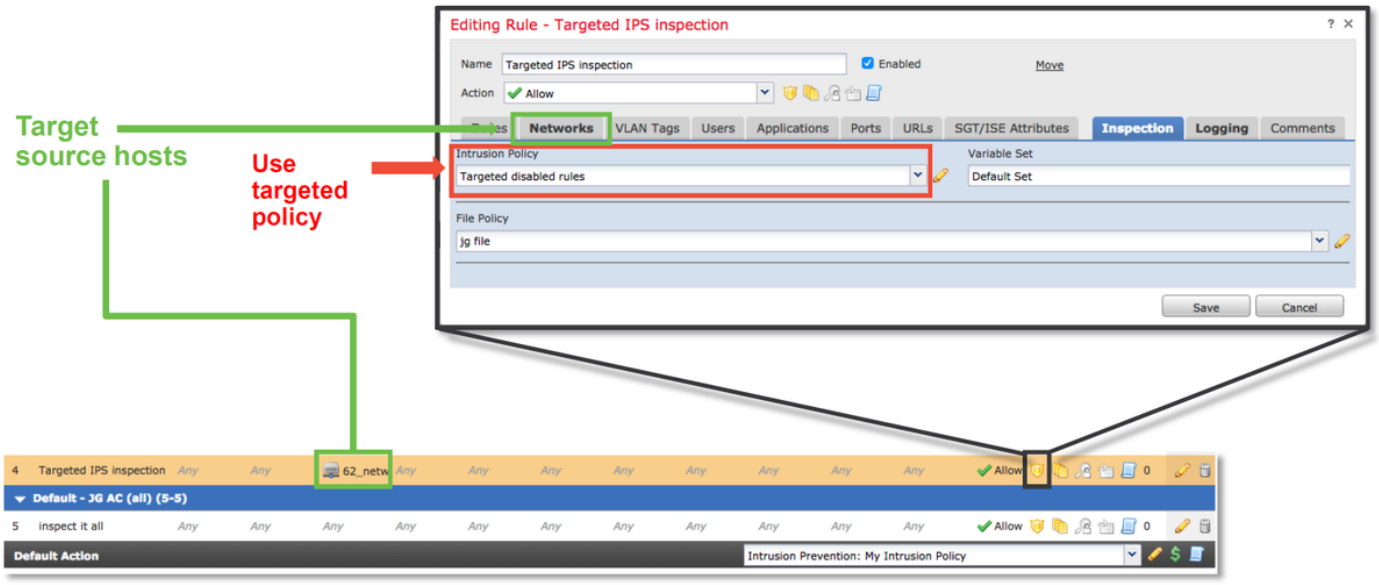
Creare un criterio per l'intrusione mirata

Se il traffico viene interrotto da una determinata regola dei criteri per le intrusioni, è possibile decidere di non interromperlo e di non disattivare la regola. La soluzione consiste nel creare un nuovo criterio di intrusione con le regole in conflitto disattivate e quindi fare in modo che valuti il traffico proveniente dagli host di destinazione.

Di seguito è riportata un'illustrazione su come creare la nuova policy di intrusione (in **Policy > Controllo di accesso > Intrusione**).



Dopo aver creato il nuovo criterio di intrusione, è possibile utilizzarlo all'interno di una nuova regola dei criteri di controllo dell'accesso, destinata agli host in questione, il cui traffico era stato precedentemente eliminato dal criterio di intrusione originale.



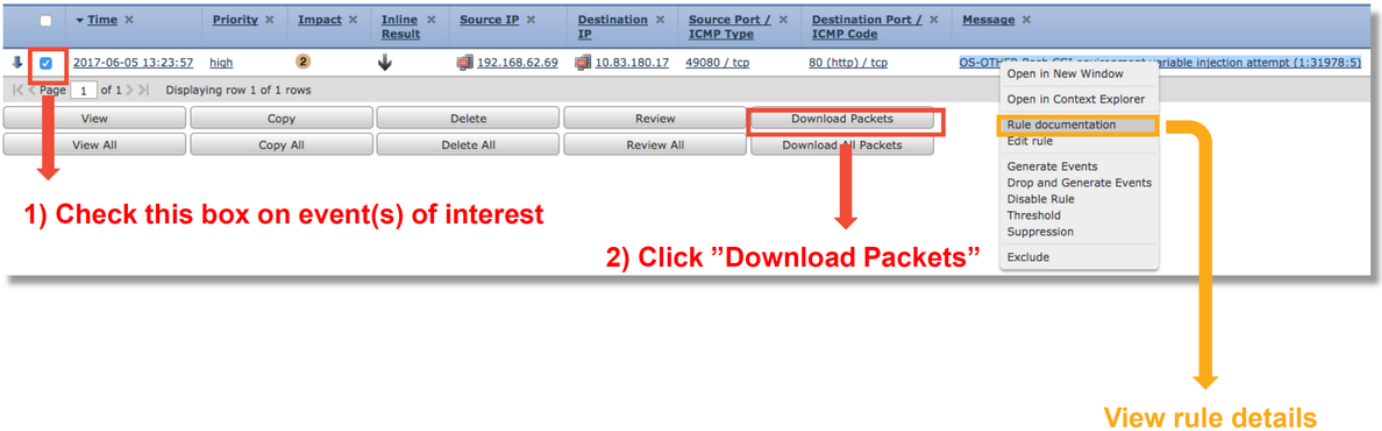
Risoluzione dei problemi di falso positivo

Uno scenario comune è rappresentato da un'analisi falsa positiva degli eventi di intrusione. Prima di aprire un caso falso positivo, è possibile verificare diversi aspetti.

1. Nella pagina **Visualizzazione tabella degli eventi intrusione**, fare clic sulla casella di controllo relativa all'evento in questione

2. Fare clic su **Download Packets** per ottenere i pacchetti acquisiti da Snort quando è stato attivato l'evento Intrusion.

3. Fare clic con il pulsante destro del mouse sul nome della regola nella colonna **Messaggio**, quindi su **Documentazione regola** per visualizzare la sintassi della regola e altre informazioni importanti.



Di seguito è riportata la sintassi della regola che ha attivato l'evento nell'esempio precedente. Le parti della regola che è possibile verificare in base a un file di acquisizione pacchetti (PCAP) scaricato dal FMC per questa regola sono in grassetto.

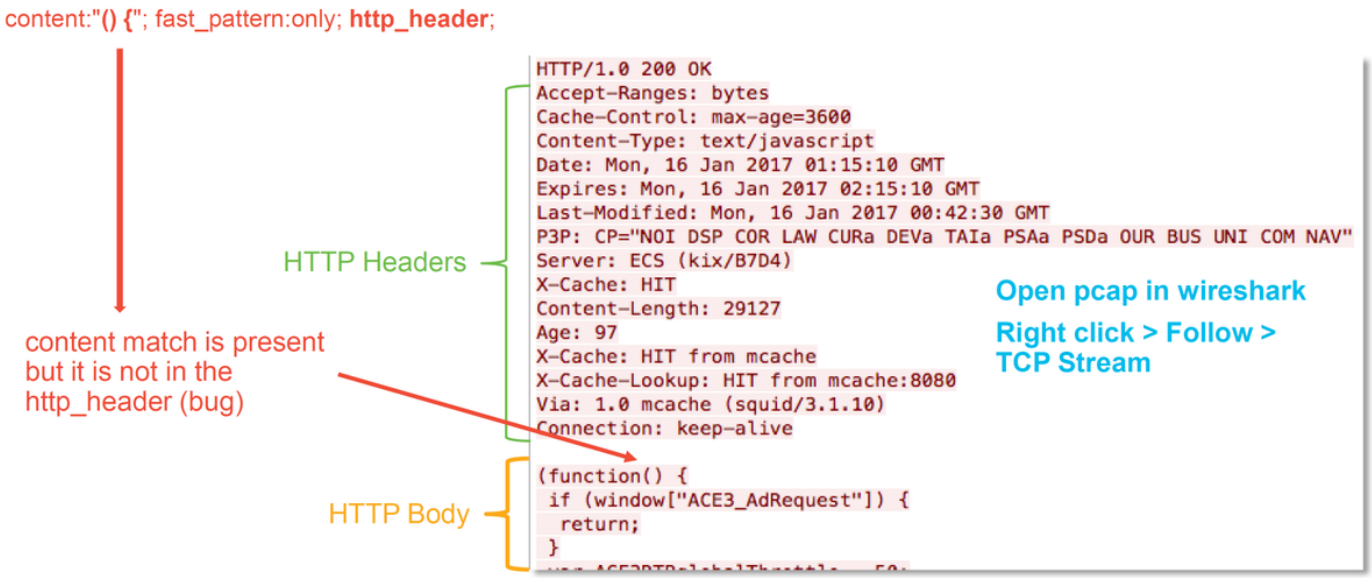
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"Tentativo di inserimento di variabili d'ambiente CGI OS-OTHER Bash"; \
flusso:a_server,stabilito; \

contenuto:"() {"; fast_pattern:solo; http_header; \
metadati:policybalance-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, ruleset community, **service http**; \
riferimento:cve,2014-6271; riferimento:cve,2014-6277; riferimento:cve,2014-6278; riferimento:cve,2014-7169; \
classtype:tentato-admin; \
sid:31978; rev. 5;)

Èquindi possibile eseguire i passaggi iniziali per eseguire il processo di analisi e verificare se il traffico ha soddisfatto la regola attivata.

1. Controllare la regola di controllo di accesso a cui corrisponde il traffico. Queste informazioni sono disponibili nelle colonne della scheda Eventi intrusione.
2. Individuare la serie di variabili utilizzata nella regola di controllo d'accesso. L'insieme di variabili può quindi essere esaminato in **Oggetti > Gestione oggetti > Insiemi di variabili**
3. Assicurarsi che gli indirizzi IP nel file PCAP corrispondano alle variabili (in questo caso, un host incluso nella variabile **$EXTERNAL_NET** che si connette a un host incluso nella configurazione della variabile **$HOME_NET**)
4. Per il **flusso**, potrebbe essere necessario acquisire una sessione/connessione completa. Snort non acquisisce il flusso completo per motivi di prestazioni. Nella maggior parte dei casi, tuttavia, è possibile supporre che se una regola con flow:fixed è stata attivata, la sessione è stata stabilita al momento dell'attivazione della regola, quindi non è necessario un file PCAP completo per verificare questa opzione in una regola snort. Ma può essere utile capire meglio il motivo per cui è stata attivata.
5. Per il **servizio http**, esaminare il file PCAP in Wireshark per verificare se assomiglia al traffico HTTP. Se l'individuazione della rete è abilitata per l'host e in precedenza l'applicazione ha rilevato il protocollo "HTTP", è possibile che il servizio corrisponda in una sessione.

Tenendo presenti queste informazioni, i pacchetti scaricati dal FMC possono essere ulteriormente esaminati in Wireshark. Il file PCAP può essere valutato per determinare se l'evento attivato è un falso positivo.



Nella figura precedente, il contenuto rilevato dalla regola era presente nel file PCAP - **"() {"**

Tuttavia, la regola specifica che il contenuto deve essere rilevato nell'intestazione HTTP del pacchetto - **http_header**

In questo caso, il contenuto è stato trovato nel corpo HTTP. Questo è un falso positivo. Tuttavia, non è un falso positivo nel senso che la regola è scritta in modo errato. La regola è corretta e in questo caso non può essere migliorata. Nell'esempio viene probabilmente rilevato un bug Snort che causa confusione nel buffer. Ciò significa che Snort ha identificato le intestazioni http in modo non corretto.

In questo caso, è possibile verificare la presenza di eventuali bug relativi al motore Snort/IPS nella versione in uso sul dispositivo e, in assenza di bug, aprire una richiesta in Cisco Technical Assistance Center (TAC). Le clip delle sessioni complete sono necessarie per indagare su un problema del genere, in quanto il team Cisco deve esaminare come Snort è entrato in quello stato, cosa che non può essere fatta con un singolo pacchetto.

Vero esempio positivo

La figura seguente mostra l'analisi del pacchetto per lo stesso evento Intrusion. Questa volta, l'evento è un vero positivo perché il contenuto non viene visualizzato nell'intestazione HTTP.

Dati da fornire a TAC

Dati	Istruzioni
Risoluzione dei problemi relativi al file dal dispositivo Firepower per il controllo del traffico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techno
Acquisizioni di pacchetti scaricate dal FMC	Per istruzioni, vedere questo articolo
Qualsiasi output CLI rilevante raccolto, ad esempio **trace**output	Per istruzioni, vedere questo articolo

Fasi successive

Se è stato determinato che il componente Criteri per le intrusioni non è la causa del problema, il passaggio successivo consiste nella risoluzione dei problemi relativi alla funzionalità Criteri di analisi della rete.

Fare clic qui per passare all'ultimo articolo.