Configurazione della variabile SNORT_BPF su un centro difesa

Sommario

Introduzione

È possibile utilizzare Berkeley Packet Filter (BPF) per escludere un host o una rete dall'ispezione da parte di un centro difesa. Snort utilizza la variabile **Snort_BPF** per escludere il traffico da un criterio di intrusione. In questo documento viene spiegato come utilizzare la variabile **Snort_BPF** in diversi scenari.

> **Suggerimento**: è consigliabile utilizzare una regola di attendibilità in un criterio di controllo dell'accesso per determinare il traffico da ispezionare o meno, anziché un BPF nel criterio di intrusione. La variabile **`Snort_BPF`** è disponibile nella versione 5.2 del software ed è deprecata nella versione 5.3 o successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti: Defense Center, Intrusion Policy, Berkeley Packet Filter e Snort Rules.

Componenti usati

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

- Centro difesa
- Software versione 5.2

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.

Procedura di configurazione

Per configurare la variabile **Snort_BPF**, attenersi alla seguente procedura:

1. Accedere all'interfaccia utente Web del Centro difesa.
2. Passare a **Criteri > Intrusione > Criteri intrusione**.
3. Fare clic sull'icona a forma di *matita* per modificare il criterio di intrusione.
4. Fare clic su **Variabili** dal menu a sinistra.
5. Una volta configurate le variabili, sarà necessario salvare le modifiche e riapplicare il criterio di intrusione affinché diventi effettivo.

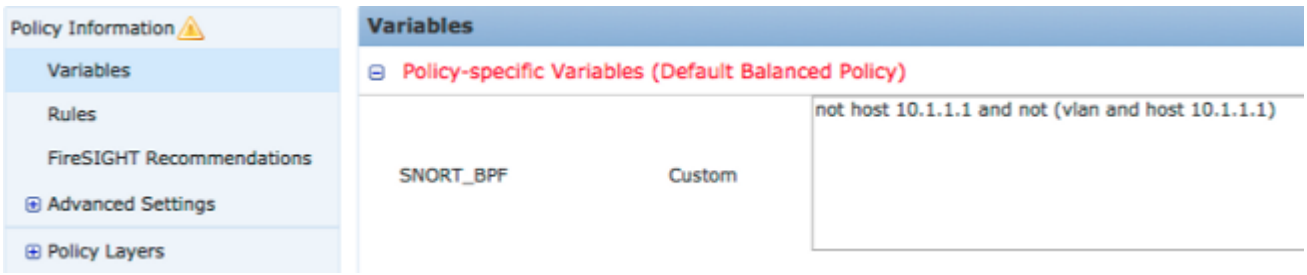

Figura: schermata della pagina di configurazione della variabile Snort_BPF

Esempi di configurazione

Di seguito sono riportati alcuni esempi di base da utilizzare come riferimento:

Scenario 1: ignorare tutto il traffico, DA e VERSO uno scanner di vulnerabilità

1. Abbiamo uno scanner di vulnerabilità all'indirizzo IP 10.1.1.1
2. Si desidera ignorare tutto il traffico DA e VERSO lo scanner
3. Il traffico può avere o meno un tag 802.1q (vlan)

La tabella **SNORT_BPF** è la seguente:

```
not host 10.1.1.1 and not (vlan and host 10.1.1.1)
```

CONFRONTO: il traffico *non* ha il tag VLAN, ma i punti 1 e 2 rimangono veri e sono:

```
not host 10.1.1.1
```

In inglese semplice, questo comando ignora il traffico in cui uno degli endpoint è 10.1.1.1 (lo scanner).

Scenario 2: Ignora tutto il traffico, DA e VERSO due scanner di vulnerabilità

1. Abbiamo uno scanner di vulnerabilità all'indirizzo IP 10.1.1.1
2. Abbiamo un secondo scanner di vulnerabilità all'indirizzo IP 10.2.1.1
3. Si desidera ignorare tutto il traffico DA e VERSO lo scanner
4. Il traffico può avere o meno un tag 802.11 (vlan)

La tabella **SNORT_BPF** è la seguente:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1))
```

Confronto: il traffico *non* è contrassegnato con VLAN, ma i punti 1 e 2 rimangono veri e sono:

```
not (host 10.1.1.1 or host 10.2.1.1)
```

In sintesi, questo comando ignora il traffico in cui uno degli endpoint è 10.1.1.1 O 10.2.1.1.

> **Nota**: è importante notare che il tag vlan deve, in quasi tutti i casi, comparire solo una volta in un determinato BPF. Le uniche situazioni in cui dovrebbe essere visualizzata più di una volta sono quelle in cui la rete utilizza tag VLAN annidati (talvolta denominati 'QinQ').

Scenario 3: Ignora traffico con tag VLAN, DA e VERSO due scanner di vulnerabilità

1. Abbiamo uno scanner di vulnerabilità all'indirizzo IP 10.1.1.1
2. Abbiamo un secondo scanner di vulnerabilità all'indirizzo IP 10.2.1.1
3. Si desidera ignorare tutto il traffico DA e VERSO lo scanner
4. Il traffico è contrassegnato come 802.11 (vlan) e si desidera utilizzare un tag (vlan) specifico, come nella vlan 101

La tabella **SNORT_BPF** è la seguente:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))
```

Scenario 4: Ignorare il traffico proveniente da un server di backup

1. Abbiamo un server di backup di rete all'indirizzo IP 10.1.1.1
2. I computer della rete si connettono a questo server sulla porta 8080 per eseguire il backup notturno
3. Si desidera ignorare questo traffico di backup, in quanto crittografato e con volumi elevati

La tabella **SNORT_BPF** è la seguente:

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
```

```
and dst port 8080))
```

Confronto: il traffico *non* è contrassegnato con VLAN, ma i punti 1 e 2 rimangono veri e sono:

```
not (dst host 10.1.1.1 and dst port 8080)
```

Tradotto, questo significa che il traffico verso la 10.1.1.1 (il nostro ipotetico server di backup) sulla porta 8080 (porta di ascolto) non deve essere ispezionato dal motore di rilevamento IPS.

Inoltre, è possibile usare net al posto dell'host per specificare un blocco di rete, piuttosto che un singolo host. Ad esempio:

```
not net 10.1.1.0/24
```

In generale, è buona norma rendere il BPF il più specifico possibile, escludendo il traffico da ispezione che deve essere escluso, senza escludere alcun traffico non correlato che possa contenere tentativi di exploit.

Scenario 5: per utilizzare intervalli di rete anziché singoli host

È possibile specificare intervalli di rete nella variabile BPF anziché negli host per ridurre la lunghezza della variabile. A tale scopo, utilizzare la parola chiave net al posto di host e specificare un intervallo CIDR. Di seguito è riportato un esempio:

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> Nota: assicurarsi di immettere l'indirizzo di rete utilizzando la notazione CIDR e un indirizzo utilizzabile all'interno dello spazio degli indirizzi del blocco CIDR. Ad esempio, utilizzare net 10.8.0.0/16 anziché net 10.8.2.16/16.

OSPF (Open Shortest Path First) **SNORT_BPF** Questa variabile viene utilizzata per impedire che determinati traffici vengano ispezionati da un motore di rilevamento IPS, spesso per motivi di prestazioni. Questa variabile utilizza il formato standard BPF (Berkeley Pack Filters). Il traffico corrisponde al **SNORT_BPF** variabile verrà ispezionata; mentre il traffico NON corrisponde alla **SNORT_BPF** La variabile NON verrà ispezionata dal motore di rilevamento 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).