ESA, SMA e WSA Grep con Regex per cercare i log

Sommario

Introduzione

In questo documento viene descritto come usare le espressioni regolari (regex) con il comando **grep** per cercare nei log.

Prerequisiti

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

- Cisco Web Security Appliance (WSA)
- Cisco Email Security Appliance (ESA)
- Cisco Security Management Appliance (SMA)

Grep con Regex

Regex può essere uno strumento efficace se utilizzato con il comando **grep** per eseguire ricerche nei log disponibili sull'accessorio, ad esempio i log degli accessi, i log proxy e altri ancora. È possibile eseguire la ricerca nei log basati sul sito Web o su qualsiasi parte dell'URL e nei nomi utente con il comando **grep** CLI.

Di seguito sono riportati alcuni scenari comuni in cui è possibile utilizzare regex con il comando **grep** per semplificare la risoluzione dei problemi.

Scenario 1: Ricerca di un sito Web specifico nei log degli accessi

Lo scenario più comune si verifica quando si cerca di trovare le richieste inviate a un sito Web nei log degli accessi del WSA.

Di seguito è riportato un esempio:

Collegare l'accessorio tramite SSH (Secure Shell). Una volta visualizzato il prompt, immettere il comando **grep** per elencare i log disponibili.

```
CLI> grep
```

Immettere il numero del registro che si desidera **conservare**.

```
[]> 1 (Choose the # for access logs here)
```

Immettere l'espressione regolare **grep**.

```
[]> website\.com
```

Scenario 2: Tentativo di trovare una particolare estensione di file o un dominio di primo livello

Èpossibile utilizzare il comando **grep** per trovare una particolare estensione di file (doc, pptx) in un URL o in un dominio di primo livello (com, org).

Di seguito è riportato un esempio:

Per trovare tutti gli URL che terminano con .crl, utilizzare questo regex:

```
\.crl$
```

Per trovare tutti gli URL con estensione pptx, utilizzare questo regex:

```
\.pptx
```

Scenario 3: Tentativo di trovare un blocco particolare per un sito Web

Quando si cerca un particolare sito Web, è possibile cercare anche una particolare risposta HTTP.

Di seguito è riportato un esempio:

Se si desidera cercare tutti i messaggi TCP_DENIED/403 per domain.com, utilizzare questo regex:

```
tcp_denied/403.*domain\.com
```

Scenario 4: Trova nome computer nei log degli accessi

Quando si utilizza lo schema di autenticazione NTLMSSP, è possibile che si verifichi un'istanza in cui un agente utente (Microsoft NCSI è il più comune) invia in modo non corretto le credenziali del

computer anziché quelle dell'utente durante l'autenticazione. Per individuare l'URL/agente utente che causa il problema, usare regex con **grep** per isolare la richiesta effettuata al momento dell'autenticazione.

Se non si dispone del nome computer utilizzato, utilizzare **grep** e cercare tutti i nomi computer utilizzati come nomi utente durante l'autenticazione con questo regex:

```
\$@
```

Una volta individuata la riga in cui si verifica questa condizione, utilizzare il comando grep per il nome di macchina specifico utilizzato con questo regex:

```
machinename\$
```

La prima voce visualizzata dovrebbe essere la richiesta effettuata quando l'utente ha eseguito l'autenticazione con il nome del computer anziché con il nome utente.

Scenario 5: Ricerca di un periodo di tempo specifico nei log degli accessi

Per impostazione predefinita, le sottoscrizioni dei log degli accessi non includono il campo che mostra la data e l'ora leggibili. Se si desidera controllare i log degli accessi per un determinato periodo di tempo, attenersi alla seguente procedura:

1. Cercare il timestamp UNIX da un sito quale Conversione online.
2. Una volta ottenuto l'indicatore orario, cercare un orario specifico all'interno dei log degli accessi.

Di seguito è riportato un esempio:

Un timestamp Unix di **1325419200** equivale a **01/01/2012 12:00:00**.

Èpossibile utilizzare questa voce regex per cercare nei log degli accessi vicini alle 12:00 del 1 gennaio 2012:

13254192

Scenario 6: Ricerca di messaggi critici o di avviso

Èpossibile cercare messaggi critici o di avviso in qualsiasi log disponibile, ad esempio i log proxy o i log di sistema, con espressioni regolari.

Di seguito è riportato un esempio:

Per cercare i messaggi di avviso nei log proxy, immettere questo regex:

```
CLI> grep
```

Immettere il numero del registro che si desidera **conservare**.

```
[]> 17 (Choose the # for proxy logs here)
```

Immettere l'espressione regolare **grep**.

```
[]> warning
```