Come si utilizzano le espressioni regolari (regex) con grep per cercare i log?

Sommario

Domanda

Come si utilizzano le espressioni regolari (regex) con grep per cercare i log?

Ambiente

Cisco Web Security Appliance
Cisco Email Security Appliance
Cisco Security Management Appliance

Soluzione

Le espressioni regolari (regex) possono essere uno strumento efficace se utilizzato con il comando "grep" per eseguire ricerche nei log disponibili nell'accessorio, ad esempio nei log degli accessi, nei log proxy e in altri log. Possiamo cercare nei log basati sul sito web, o su qualsiasi parte dell'URL, o sui nomi utente, per citarne alcuni, quando usiamo il comando CLI "grep".

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

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

Lo scenario più comune è il tentativo di trovare le richieste inviate a un sito Web nei log degli accessi di Cisco Web Security Appliance (WSA).

Ad esempio:
Collegare l'accessorio tramite SSH. Una volta visualizzato il prompt, è possibile digitare il comando "grep" per elencare i log disponibili.

CLI> grep
Immettere il numero del registro che si desidera "grep". []> 1 (scegliere il numero per i log degli accessi qui)
Immettere l'espressione regolare "grep". []> **sito Web\.com**

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

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

Ad esempio:
Per trovare tutti gli URL che terminano con .crl è possibile utilizzare il seguente regex: **\.crl$**

Per trovare tutti gli URL che contengono l'estensione file .pptx, possiamo usare il seguente regex: **\.pptx**

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

Quando si cerca un sito Web specifico, è possibile che venga cercata anche una determinata risposta HTTP.

Ad esempio:
Se si desidera cercare tutti i messaggi TCP_DENIED/403 per domain.com, è possibile utilizzare il seguente regex: **tcp_negato/403.*dominio\.com**

Scenario 4: Ricerca di un nome di 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 rintracciare l'URL/agente utente che causa questo, possiamo usare regex con "grep" per isolare la richiesta fatta quando si è verificata l'autenticazione.

Se non si dispone del nome computer utilizzato, è possibile utilizzare "grep" e trovare tutti i nomi computer utilizzati come nomi utente durante l'autenticazione con il seguente regex: **\$@**

Una volta che abbiamo la linea in cui questo si verifica, possiamo "grep" per il nome macchina specifico che è stato utilizzato utilizzando il seguente regex: **nomecomputer\$**

La prima voce che viene visualizzata deve 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, è possibile eseguire la procedura seguente:

Cercare il timestamp UNIX da un sito quale http://www.onlineconversion.com/unix_time.htm. Una volta ottenuto l'indicatore orario, è possibile cercare un orario specifico all'interno dei log degli accessi.

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

La seguente voce regex può essere utilizzata per eseguire una ricerca nei log degli accessi all'ora 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 nei log proxy o nei log di sistema, utilizzando espressioni regolari.

Ad esempio:
Per cercare i messaggi di avviso nei log proxy, è possibile immettere il seguente regex:

1. **CLI>** grep
2. Immettere il numero del registro che si desidera "grep".
   []> 17 (scegliere il numero per i log proxy qui)
3. Immettere l'espressione regolare "grep".
   []> **avviso**

Altri collegamenti utili:

Espressioni regolari - Guida per l'utente