ログを検索する Regex での ESA、SMA、WSA の Grep

目次

概要

この文書にログを検索するために **grep コマンド**で正規表現（regex）を使用する方法を記述されています。

前提条件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Web セキュリティ アプライアンス（WSA）
- Cisco E メール セキュリティ アプライアンス（ESA）
- Cisco セキュリティ管理アプライアンス（SMA）

Regex のグレップ

Regex はアクセス ログ、プロキシ ログ、および他のような機器で、利用可能なログを検索する **grep コマンド**で使用されたとき強力なツールである場合もあります。 Webサイトに、か**グレップ** CLI コマンドで URL 基づいてログおよびユーザネームの部分を検索できます。

grep コマンドでトラブルシューティングと助けるために regex を使用できるところにいくつかの一般的なシナリオはここにあります。

シナリオ 1： アクセス ログの特定の Webサイトを見つけて下さい

もっとも一般的なシナリオは WSA のアクセス ログの Webサイトになされる Find 要求に試みる

ときあります。

次に例を示します。

セキュア シェル（SSH）によるアプライアンスへの接続応答。 プロンプトがあったら、利用可能なログをリストするために **grep コマンドを**入力して下さい。

```
CLI> grep
```

グレップに希望するログの数を入力して下さい。

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

グレップに正規表現を入力して下さい。

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

シナリオ 2： 特定のファイル ファイル拡張子かトップレベル ドメインを見つける試み

.org）で特定のファイル拡張子（.doc、.pptx）を URL またはトップレベル ドメイン（.com 見つけるために **grep コマンドを**使用できます。

次に例を示します。

.crl で終了するすべての URL を見つけるために、この regex を使用して下さい:

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

ファイル拡張子 .pptx が含まれているすべての URL を見つけるために、この regex を使用して下さい:

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

シナリオ 3： Webサイトのための特定のブロックを見つける試み

特定の Webサイトを捜すとき、また特定の HTTP応答を捜すかもしれません。

次に例を示します。

domain.com のためのすべての TCP_DENIED/403 メッセージを捜したいと思う場合この regex を使用して下さい:

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

シナリオ 4： アクセス ログのマシン名を検索して下さい

NTLMSSP 認証機構を使用するとき、認証するときユーザ エージェントがユーザーの資格情報の代りに（Microsoft NCSI はもっとも一般的なです）不正確にマシン信任状を送信 する 例に出会う

かもしれません。 認証が行われたときにこの問題を引き起こしている URL/User エージェントを見つけ出すために、なされる要求を隔離するために**グレップ**と regex を使用して下さい。

使用したマシン名を持たなかったら、**グレップを**使用し、この regex と認証した場合ユーザネームとして使用したすべてのマシン名を検索して下さい:

```
[]> website\.com
```
これが発生する行があれば、この regex と使用した特定のマシン名のためのグレップ:

```
[]> website\.com
```
現われる最初のエントリはときにユーザネームの代りにマシン名と認証されたユーザなされた要求であるはずです。

シナリオ 5： アクセス ログの特定の期間を見つけて下さい

デフォルトで、アクセス ログ サブスクリプションは人が読み取り可能な日付/時間を示すフィールドが含まれていません。 特定の時間があるようにアクセス ログを確認したいと思う場合これらのステップを完了して下さい:

1. オンライン変換のようなサイトからの UNIX タイムスタンプを調べて下さい。
2. タイムスタンプがあったら、アクセス ログ内の特定時を捜して下さい。

次に例を示します。

1325419200 の Unix タイムスタンプは 01/01/2012 12:00:00 と同等です。

2012 年 1月 1 日 12:00 の近くのアクセス ログを検索するためにこの regex エントリを使用できます:

13254192

シナリオ 6： 重要か警告メッセージのための検索

あらゆる利用可能なログの重要か警告メッセージを、正規表現のプロキシ ログまたはシステムログのような、捜すことができます。

次に例を示します。

プロキシ ログの警告メッセージを捜すために、この regex を入力して下さい:

```
CLI> grep
```
グレップに希望するログの数を入力して下さい。

```
[]> 17 (Choose the # for proxy logs here)
```
グレップに正規表現を入力して下さい。

[]> **warning**