ログを grep 検索するときに正規表現（regex）をどのように使用しますか。

目次

質問

ログを grep 検索するときに正規表現（regex）をどのように使用しますか。

環境

Cisco Web セキュリティ アプライアンス
Cisco E メール セキュリティ アプライアンス
Ciscoセキュリティ管理アプライアンス

解決策

アクセス ログ、プロキシ ログ、および他のようなアプライアンスで、利用可能なログを検索する「グレップ」コマンドで使用されたとき正規表現（regex）は強力なツールである場合もあります。 CLI コマンド「グレップ」を使用するとき少数を指名するために Webサイトに、か URL 基づいて、ログまたはユーザネームの部分を、検索できます。

グレップとトラブルシューティングと助けるのに 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下記にあります。

シナリオ 1： アクセス ログの特定の Webサイトを見つけること

もっとも一般的なシナリオは Cisco Web セキュリティ アプライアンス（WSA）のアクセス ログの Webサイトに作られる Find 要求に試みています。

例：
SSH によるアプライアンスへの接続応答。 プロンプトがあれば、利用可能なログをリストする「グレップ」コマンドを入力できます。

CLI> グレップ
「グレップに」希望するログの数を入力して下さい。 [] > 1（アクセス ログのための#ここに選択して下さい）
「グレップ」に正規表現を入力して下さい。 [] > Webサイト\ .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ように試み

.org）で特定のファイル 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「グレップ」コマンドを使用できます。

例：
.crl で私達を終了するすべての URL を見つけることは次の regex を使用する可能性があります: \ .crl$

へファイル拡張子 .pptx が含まれているすべての URL を見つけるために、次の regex を使用する可能性があります: \ .pptx

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ように試み

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。

例：
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った場合次の regex を使用する可能性があります: tcp_denied/403.*domain\.com

シナリオ 4： アクセス ログのマシン名を検索すこと

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 例に出くわすかもしれません。 認証が行われたときにへこれを引き起こす URL/User エージェントを見つけ出すために、「グレップ」となされる要求を隔離するのに regex を使用できます。

使用したマシン名を持たなければ、「グレップ」を使用し、次の regex を使用して認証するときユーザネームとして使用したすべてのマシン名を検索すことができます: \ $@

これが発生する行があれば、次の regex の使用によって使用した特定のマシン名のための「グレップ」できます: machinename \ $

アップす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ること

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下記のようにステップに従うことができます:

http://www.onlineconversion.com/unix_time.htm 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。 タイムスタンプがあれば、アクセス ログ内の特定時を捜すことができます。

例：
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 日の 12:00 の時のまわりにアクセス ログを検索するのに次の 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を捜すこと

正規表現を使用してあらゆる利用可能なログの重要か警告メッセージを、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。
ヘプロキシ ログの警告メッセージを捜すために、次の regex を入力することができます:

1. **CLI>** グレップ
2. 「グレップに」希望するログの数を入力して下さい。
   [] > 17 （プロキシ ログのための#ここに選択して下さい）
3. 「グレップ」に正規表現を入力して下さい。
   [] > **警告します**

他の有用なリンク:

正規表現-ユーザガイド