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。

内容

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 Security Appliance
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

解決方法

正規表現(regex)は、「grep」コマンドを使用してアクセスログ、プロキシログなどのアプライアンスで使用可能なログを検索する際に強力なツールとなります。CLIコマンド「grep」を使用すると、Webサイト、またはURLの任意の部分、またはユーザ名に基づいてログを検索し、いくつかの名前を付けることができます。

次に、正規表現とgrepを使用してトラブルシューティングを支援できる一般的なシナリオをいくつか示します。

シナリオ 1：アクセスログでの特定のWebサイトの検索

最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)のアクセスログでWebサイトに対する要求を見つけようとすることです。

例：
SSH経由でアプライアンスに接続します。プロンプトが表示されたら、「grep」コマンドを入力して、使用可能なログを一覧表示できます。

CLI > grep
grepするログの番号を入力します。 []> 1（アクセスログの場合は#を選択してください）
正規表現を「grep」に入力します。 []> website\.com

シナリオ 2：特定のファイル拡張子またはトップレベルドメインの検索の試行

「grep」コマンドを使用すると、URLまたはトップレベルドメイン(.com、.org)内の特定のファイル拡張子(.doc、.pptx)を検索できます。

例：
.crlで終わるすべてのURLを見つけるには、次の正規表現を使用できます。**\.crl$**

ファイル拡張子に.pptxを持つすべてのURLを検索するには、次の正規表現を使用できます。
\.pptx

シナリオ 3：Webサイトの特定のブロックを検索する

特定のWebサイトを検索する際に、特定のHTTP応答を検索する場合もあります。

例：
domain.comのすべてのTCP_DENIED/403メッセージを検索するには、次の正規表現を使用できます。**tcp_denied/403.*domain\.com**

シナリオ 4：アクセスログでのマシン名の検索

NTLMSSP認証スキームを使用すると、ユーザエージェント（Microsoft NCSIが最も一般的）が認証時にユーザクレデンシャルではなくマシンクレデンシャルを誤って送信するインスタンスが発生することがあります。これを引き起こすURL/ユーザエージェントを追跡するには、「grep」でregexを使用して、認証が発生したときに行われた要求を切り分けることができます。

使用されたマシン名がない場合は、「grep」を使用して、次の正規表現を使用して認証を行うときにユーザ名として使用されたすべてのマシン名を検索できます。**\$@**

これが発生する行が見つかったら、次の正規表現を使用して使用された特定のマシン名を「grep」できます。**machinename\$**

最初に表示されるエントリは、ユーザがユーザ名ではなくマシン名で認証されたときに行われた要求です。

シナリオ 5：アクセスログでの特定の期間の検索

デフォルトでは、アクセスログサブスクリプションには、人間が読み取り可能な日時を示すフィールドは含まれません。特定の期間のアクセスログを確認する場合は、次の手順に従います。

http://www.onlineconversion.com/unix_time.htmなどのサイトからUNIXタイムスタンプを検索します。タイムスタンプを取得したら、アクセスログ内で特定の時刻を検索できます。

例：
Unixのタイムスタンプ1325419200は、01/01/2012 12:00:00に相当します。

2012年1月1日の12:00前後に、次のregexエントリを使用してアクセスログを検索できます。
13254192

シナリオ 6：重大メッセージまたは警告メッセージの検索

正規表現を使用して、プロキシログやシステムログなど、利用可能なログで重要なメッセージや警告メッセージを検索できます。

以下に、いくつかの例を示します。
プロキシログで警告メッセージを検索するには、次の正規表現を入力します。

1. CLI > grep
2. grepするログの番号を入力します。
   []> 17（ここでプロキシログの#を選択）
3. 正規表現を「grep」に入力します。
   []> **警告**

その他の便利なリンク：

正規表現 – ユーザガイド