Grep ESA, S A, e WSA com o Regex para procurar logs

Índice

[Introdução](#)
[Pré-requisitos](#)
[Grep com Regex](#)
[Cenário 1: Encontre um Web site particular nos logs do acesso](#)
[Cenário 2: Tentativa de encontrar uma extensão de arquivo ou um domínio de nível superior particular](#)
[Cenário 3: Tentativa de encontrar um bloco particular para um Web site](#)
[Encenação 4: Encontre um nome de máquina nos logs do acesso](#)
[Encenação 5: Encontre um período de tempo específico nos logs do acesso](#)
[Encenação 6: Busca para crítico ou mensagens de advertência](#)

Introdução

Este documento descreve como usar expressões regulares (regex) com o **comando grep** a fim procurar logs.

Pré-requisitos

As informações neste documento são baseadas nestas versões de software e hardware:

- Ferramenta de segurança da Web de Cisco (WSA)
- Cisco envia por correio eletrónico a ferramenta de segurança (o ESA)
- Dispositivo do Gerenciamento do Cisco Security (S A)

Grep com Regex

Regex pode ser uma ferramenta poderosa quando usado com o **comando grep** procurar através dos logs disponíveis no dispositivo, tal como logs do acesso, logs do proxy, e outro. Você pode procurar os logs baseados no Web site, ou parte de na URL, e em nomes de usuário com o comando CLI do **grep**.

Estão aqui alguns cenários comuns onde você pode usar o regex com o **comando grep** a fim ajudar com Troubleshooting.

Cenário 1: Encontre um Web site particular nos logs do acesso

A maioria de cenário comum é quando você tenta encontrar os pedidos que estão feitos a um Web site nos logs do acesso do WSA.

Aqui está um exemplo:

Conecte ao dispositivo através do Shell Seguro (ssh). Uma vez que você tem a alerta, inscreva o **comando grep** a fim alistar os logs disponíveis.

```
CLI> grep
```

Incorpore o número do log que você deseja ao **grep**.

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

Incorpore a expressão regular ao **grep**.

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

Cenário 2: Tentativa de encontrar uma extensão de arquivo ou um domínio de nível superior particular

Você pode usar o **comando grep** a fim encontrar uma extensão de arquivo particular (.doc, .pptx) em uma URL ou em um domínio de nível superior (.com, .org).

Aqui está um exemplo:

A fim encontrar todas as URL que terminam com .crl, use este regex:

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

A fim encontrar todas as URL que contêm a extensão de arquivo .pptx, use este regex:

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

Cenário 3: Tentativa de encontrar um bloco particular para um Web site

Quando você procura por um Web site particular, você pôde igualmente procurar por uma resposta HTTP particular.

Aqui está um exemplo:

Se você quer procurar por todas as mensagens TCP_DENIED/403 para domain.com, use este regex:

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

Encenação 4: Encontre um nome de máquina nos logs do acesso

Quando você usa o método de autenticação NTLMSSP, você pôde encontrar um exemplo onde

um agente de usuário (Microsoft NCSI é o mais comum) enviasse incorretamente credenciais da máquina em vez das credenciais do usuário quando autentica. A fim seguir para baixo o agente URL/User que causa esta edição, use o regex com **grep** a fim isolar o pedido feito quando a autenticação ocorreu.

Se você não tem o nome de máquina que esteve usado, use o **grep** e encontre todos os nomes de máquina que foram usados como nomes de usuário ao autenticar com este regex:

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

Uma vez que você tem a linha onde esta ocorre, grep para o nome de máquina específico que foi usado com este regex:

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

A primeira entrada que aparece deve ser o pedido que foi feito quando o usuário autenticado com o nome de máquina em vez do nome de usuário.

Encenação 5: Encontre um período de tempo específico nos logs do acesso

Àrevelia, as assinaturas do log do acesso não incluem o campo que mostra a data/hora compreensíveis para o utilizador. Se você quer verificar os logs do acesso para ver se há um período de tempo particular, termine estas etapas:

1. Olhe acima o timestamp de UNIX de um local tal como a conversão em linha.
2. Uma vez que você tem o timestamp, procure por umas horas específicas dentro dos logs do acesso.

Aqui está um exemplo:

Um timestamp de Unix de **1325419200** é equivalente a **01/01/2012 de 12:00:00**.

Você pode usar esta entrada do regex a fim procurar o 1º de janeiro os logs do acesso perto de 12:00, 2012:

13254192

Encenação 6: Busca para crítico ou mensagens de advertência

Você pode procurar por crítico ou por mensagens de advertência em todos os logs disponíveis, tais como logs do proxy ou log de sistema, com expressões regulares.

Aqui está um exemplo:

A fim procurar por mensagens de advertência nos logs do proxy, incorpore este regex:

```
CLI> grep
```

Incorpore o número do log que você deseja ao **grep**.

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

Incorpore a expressão regular ao **grep**.

```
[]> warning
```