Como você usa expressões regulares (regex) com grep para procurar logs?

Índice

Pergunta

Como você usa expressões regulares (regex) com grep para procurar logs?

Ambiente

Ferramenta de segurança da Web de Cisco
Cisco envia por correio eletrónico a ferramenta de segurança
Dispositivo do Gerenciamento do Cisco Security

Solução

As expressões regulares (regex) podem ser uma ferramenta poderosa quando usadas com o comando do “grep” procurar através dos logs disponíveis no dispositivo, tal como logs do acesso, logs do proxy, e outro. Nós podemos procurar os logs baseados no Web site, ou parte de na URL, ou em nomes de usuário, para nomear alguns, ao usar o comando CLI “grep”.

Estão abaixo alguns cenários comuns onde você pode usar o regex com grep para ajudar com Troubleshooting.

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

A maioria de cenário comum está tentando encontrar os pedidos que estão sendo feitos a um

Web site nos logs do acesso da ferramenta de segurança da Web de Cisco (WSA).

por exemplo:
Conecte ao dispositivo através do SSH. Uma vez que você tem a alerta, nós podemos datilografar o comando do “grep” alistar os logs disponíveis.

Grep **CLI>**
Incorpore o número do log que você deseja ao “grep”. []> 1 (escolha # para logs do acesso aqui)
Incorpore a expressão regular ao “grep”. []> **Web site \ .com**

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

Nós podemos usar o comando do “grep” encontrar uma extensão de arquivo particular (.doc, .pptx) em uma URL ou em um domínio de nível superior (.com, .org).

por exemplo:
Para encontrar todas as URL que nos terminam com .crl poderia usar o seguinte regex: **\ .crl$**

Para encontrar todas as URL que contêm a extensão de arquivo .pptx, nós poderíamos usar o seguinte regex: **\ .pptx**

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

Ao procurar por um Web site particular, nós pudemos igualmente procurar por uma resposta HTTP particular.

por exemplo:
Se nós quisemos procurar por todas as mensagens TCP_DENIED/403 para domain.com, nós poderíamos usar o seguinte regex: **tcp_denied/403.*domain\.com**

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

Ao usar o método de autenticação NTLMSSP, nós podemos vir através de um exemplo onde um agente de usuário (Microsoft NCSI é o mais comum) envie incorretamente credenciais da máquina em vez das credenciais do usuário ao autenticar. Para seguir para baixo o agente URL/User que causa este, nós podemos usar o regex com o “grep” para isolar o pedido feito quando a autenticação ocorreu.

Se nós não temos o nome de máquina que esteve usado, nós podemos usar o “grep” e encontrar todos os nomes de máquina que foram usados como nomes de usuário ao autenticar usando o seguinte regex: **\ $@**

Uma vez que nós temos a linha onde esta ocorre, nós podemos “grep” para o nome de máquina específico que foi usado usando o seguinte regex: **machinename \ $**

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

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

Àrevelia, as assinaturas do log do acesso não incluirão o campo que mostra a data/hora compreensíveis para o utilizador. Se nós queremos verificar os logs do acesso para ver se há um período de tempo particular, nós podemos seguir as etapas abaixo:

Olhe acima o timestamp de UNIX de um local tal como http://www.onlineconversion.com/unix_time.htm. Uma vez que você tem o timestamp, você pode procurar por umas horas específicas dentro dos logs do acesso.

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

Nós podemos usar a seguinte entrada do regex para procurar o 1º de janeiro os logs do acesso em torno da época de 12:00, 2012: 13254192

Encenação 6: Pesquisa por crítico ou por mensagens de advertência

Nós podemos procurar por crítico ou por mensagens de advertência em todos os logs disponíveis, tais como logs do proxy ou log de sistema, usando expressões regulares.

Por exemplo:
Para procurar por mensagens de advertência nos logs do proxy, nós podemos incorporar o seguinte regex:

1. Grep **CLI>**
2. Incorpore o número do log que você deseja ao “grep”.
   []> 17 (escolha # para logs do proxy aqui)
3. Incorpore a expressão regular ao “grep”.
   []> **advertindo**

Outros links úteis:

Expressões regulares - Guia do Usuário