Содержание

Вопрос

Как вы используете регулярные выражения (regex) с grep для поиска журналов?

Среда

Cisco Web Security Appliance
Устройство безопасности электронной почты Cisco
Устройство менеджмента Cisco Security

Решение

Регулярные выражения (regex) могут быть мощным программным средством, когда используется с командой "grep" перерыть журналы, доступные на устройстве, такие как Журналы Доступа, Журналы Прокси и другие. Мы можем искать журналы на основе веб-сайта, или любую часть URL, или имена пользователей, для именования некоторых, при использовании команды CLI "grep".

Ниже некоторые общие сценарии, где можно использовать regex с grep для помощи с устранением проблем.

Сценарий 1: Обнаружение определенного веб-сайта в журналах доступа

Наиболее распространенный сценарий пытается найти запросы сделанными к веб-сайту в журналах доступа Cisco Web Security Appliance (WSA).

Пример:
Соединитесь с устройством через SSH. Как только у вас есть приглашение, мы можем ввести команду "grep" для распечатки доступных журналов.

CLI> grep
Введите номер журнала, которого вы желаете к "grep". []> 1 (Выбирают # для журналов доступа здесь),
Введите регулярное выражение в "grep". []> **website\.com**

Сценарий 2: Попытка найти определенное расширение файла или домен верхнего уровня

Мы можем использовать команду "grep" для обнаружения определенного расширения файла (.doc, .pptx) в URL или домене верхнего уровня (.com, .org).

Пример:
Найти все URL, которые заканчиваются .crl, мы могли использовать следующий regex: **\.crl$**

Для обнаружения всех URL, которые содержат расширение файла .pptx мы могли использовать следующий regex: **\.pptx**

Ситуация 3: Попытка найти определенный блок для веб-сайта

При поиске определенного веб-сайта мы могли бы также искать определенный Ответ HTTP.

Пример:
Если бы мы хотели искать все сообщения TCP_DENIED/403 для domain.com, то мы могли бы использовать следующий regex: **tcp_denied/403. *domain\.com**

Сценарий 4: обнаружение имени машины в журналах доступа

При использовании схемы проверки подлинности NTLMSSP мы можем столкнуться с экземпляром, куда Клиент User Agent (Microsoft NCSI наиболее распространена) неправильно передаст учетные данные машины вместо учетных данных пользователя при аутентификации. Для разыскивания URL/клиента User Agent, который вызывает это мы можем использовать regex с "grep" для изоляции запроса, выполненного, когда произошла аутентификация.

Если у нас нет имени машины, которое использовалось, мы можем использовать "grep" и найти все имена машины, которые использовались в качестве имен пользователей при аутентификации использования следующего regex: **\$**

Как только у нас есть линия, где это происходит, мы можем "grep" для определенного имени машины, которое использовалось при помощи следующего regex: **$ machinename**

Первая запись, которая подходит, должна быть запросом, который был выполнен, когда пользователь аутентифицировался с именем машины вместо имени пользователя.

Сценарий 5: обнаружение определенного периода времени в журналах

доступа

По умолчанию подписки журнала доступа не будут включать поле, которое показывает человекочитаемую дату/время. Если мы хотим проверить журналы доступа в течение периода определенного времени, мы можем выполнить действия ниже:

Поиск метка времени UNIX от узла, такого как http://www.onlineconversion.com/unix_time.htm. Как только у вас есть метка времени, можно искать специфическое время в Журналах Доступа.

Пример:
Метка времени Unix 1325419200 эквивалентна 01.01.2012 12:00:00.

Мы можем использовать следующую запись regex для поиска журналов доступа примерно во время 12:00 1-го января 2012: 13254192

Сценарий 6: поиск критических или предупреждающих сообщений

Мы можем искать критические или предупреждающие сообщения в любых доступных журналах, таких как журналы прокси или системные журналы, с помощью регулярных выражений.

Пример:
Для поиска предупреждающих сообщений в журналах прокси мы можем ввести следующий regex:

1. **CLI>** grep
2. Введите номер журнала, которого вы желаете к "grep".
   []> 17 (Выбирают # для журналов прокси здесь),
3. Введите регулярное выражение в "grep".
   []> **предупреждение**

Другие полезные ссылки:

Регулярные выражения - руководство пользователя