grep와 정규식(regex)을 사용하여 로그를 검색하는 방법은 무엇입니까?

목차

[질문](#)
[환경](#)
[솔루션](#)
[시나리오 1:액세스 로그에서 특정 웹 사이트 찾기](#)
[시나리오 2:특정 파일 확장명 또는 최상위 도메인을 찾는 중](#)
[시나리오 3:웹 사이트에 대한 특정 블록을 찾는 중](#)
[시나리오 4:액세스 로그에서 머신 이름 찾기](#)
[시나리오 5:액세스 로그에서 특정 기간 찾기](#)
[시나리오 6:위험 또는 경고 메시지 검색](#)

질문

grep와 정규식(regex)을 사용하여 로그를 검색하는 방법은 무엇입니까?

환경

Cisco Web Security Appliance
Cisco Email Security Appliance
Cisco Security Management Appliance

솔루션

정규식(regex)은 어플라이언스에서 사용 가능한 로그(예: 액세스 로그, 프록시 로그 등)를 검색하는 데 "grep" 명령과 함께 사용할 경우 강력한 툴이 될 수 있습니다.CLI 명령 "grep"를 사용할 때 웹 사이트 또는 URL의 일부 또는 사용자 이름을 기반으로 로그를 검색할 수 있습니다.

다음은 문제 해결을 지원하기 위해 regex와 grep를 함께 사용할 수 있는 몇 가지 일반적인 시나리오입니다.

시나리오 1:액세스 로그에서 특정 웹 사이트 찾기

가장 일반적인 시나리오는 Cisco WSA(Web Security Appliance)의 액세스 로그에서 웹 사이트에 대한 요청을 찾는 것입니다.

예를 들면 다음과 같습니다.
SSH를 통해 어플라이언스에 연결합니다.프롬프트가 표시되면 "grep" 명령을 입력하여 사용 가능한 로그를 나열할 수 있습니다.

CLI> grep
"grep"할 로그 번호를 입력합니다. []> 1(액세스 로그의 # 선택)
"grep"에 정규식을 입력합니다. []> **웹 사이트\.com**

시나리오 2:특정 파일 확장명 또는 최상위 도메인을 찾는 중

"grep" 명령을 사용하여 URL 또는 최상위 도메인(.com, .org)에서 특정 파일 확장명(.doc, .pptx)을 찾을 수 있습니다.

예를 들면 다음과 같습니다.
.crl로 끝나는 모든 URL을 찾으려면 다음 regex를 사용할 수 있습니다.**\.crl$**

파일 확장명 .pptx가 포함된 모든 URL을 찾으려면 다음 regex를 사용할 수 있습니다.\.pptx

시나리오 3:웹 사이트에 대한 특정 블록을 찾는 중

특정 웹 사이트를 검색할 때 특정 HTTP 응답을 검색할 수도 있습니다.

예를 들면 다음과 같습니다.
domain.com에 대한 모든 TCP_DENIED/403 메시지를 검색하려면 다음 regex를 사용할 수 있습니다.**tcp_denied/403.*domain\.com**

시나리오 4:액세스 로그에서 머신 이름 찾기

NTLMSSP 인증 체계를 사용할 때 사용자 에이전트(Microsoft NCSI가 가장 일반적임)가 인증할 때 사용자 자격 증명 대신 머신 자격 증명을 잘못 전송하는 인스턴스가 나타날 수 있습니다.이러한 원인이 되는 URL/사용자 에이전트를 추적하려면 regex와 "grep"를 함께 사용하여 인증이 발생했을 때 수행된 요청을 격리할 수 있습니다.

사용된 머신 이름이 없는 경우 "grep"를 사용하여 다음 regex를 사용하여 인증할 때 사용자 이름으로 사용된 모든 머신 이름을 찾을 수 있습니다.**\$@**

이러한 현상이 발생하는 선이 있으면 다음 regex를 사용하여 사용한 특정 머신 이름에 대해 "grep"를 수행할 수 있습니다.**컴퓨터 이름\$**

첫 번째 항목은 사용자가 사용자 이름 대신 시스템 이름으로 인증할 때 만들어진 요청이어야 합니다.

시나리오 5:액세스 로그에서 특정 기간 찾기

기본적으로 액세스 로그 서브스크립션에는 사용자가 읽을 수 있는 날짜/시간을 표시하는 필드가 포

함되지 않습니다.특정 기간 동안 액세스 로그를 확인하려면 다음 단계를 수행하십시오.

http://www.onlineconversion.com/unix_time.htm과 같은 사이트에서 UNIX 타임스탬프를 찾습니다 .타임스탬프가 있으면 액세스 로그 내에서 특정 시간을 검색할 수 있습니다.

예를 들면 다음과 같습니다.
Unix 타임스탬프 1325419200은 01/01/2012 12:00:00과 같습니다.

2012년 1월 1일 12:00을 기준으로 다음 regex 항목을 사용하여 액세스 로그를 검색할 수 있습니다 .13254192

시나리오 6:위험 또는 경고 메시지 검색

사용 가능한 모든 로그(예: 프록시 로그 또는 시스템 로그)에서 정규식을 사용하여 위험 또는 경고 메시지를 검색할 수 있습니다.

예를 들면 다음과 같습니다.
프록시 로그에서 경고 메시지를 검색하려면 다음 regex를 입력할 수 있습니다.

1. **CLI>** grep
2. "grep"할 로그 번호를 입력합니다.
   []> 17(여기에서 프록시 로그의 # 선택)
3. "grep"에 정규식을 입력합니다.
   []> **경고**

기타 유용한 링크:

정규식 - 사용 설명서