ESA, SMA 및 WSA Grep with Regex to Search 로그

목차

소개

이 문서에서는 로그를 검색하기 위해 grep 명령과 함께 정규식(regex)을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco WSA(Web Security Appliance)
- Cisco ESA(Email Security Appliance)
- Cisco SMA(Security Management Appliance)

Grep with Regex

Regex는 **grep** 명령과 함께 사용하여 어플라이언스에서 사용 가능한 로그(예: 액세스 로그, 프록시 로그 등)를 검색하는 강력한 툴이 될 수 있습니다.grep CLI 명령을 사용하여 웹 사이트 또는 URL의 일부 및 사용자 이름을 기반으로 로그를 검색할 수 **있습니다**.

다음은 트러블슈팅을 지원하기 위해 regex를 grep 명령과 함께 사용할 수 **있는** 몇 가지 일반적인 시나리오입니다.

시나리오 1:액세스 로그에서 특정 웹 사이트 찾기

가장 일반적인 시나리오는 WSA의 액세스 로그에서 웹 사이트에 대한 요청을 찾으려고 할 때 발생

합니다.

예를 들면 다음과 같습니다.

SSH(Secure Shell)를 통해 어플라이언스에 연결합니다. 프롬프트가 표시되면 grep 명령을 입력하여 사용 가능한 로그를 나열합니다.

```
CLI> grep
```

그리려는 로그 번호를 **입력합니다**.

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

grep할 정규식을 **입력합니다**.

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

시나리오 2:특정 파일 확장명 또는 최상위 도메인을 찾습니다.

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

예를 들면 다음과 같습니다.

.crl로 끝나는 모든 URL을 찾으려면 다음 regex를 사용합니다.

```
\.crl$
```

파일 확장명 .pptx가 포함된 모든 URL을 찾으려면 다음 regex를 사용합니다.

```
\.pptx
```

시나리오 3:웹 사이트에 대한 특정 블록 찾기 시도

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 사용합니다.

```
tcp_denied/403.*domain\.com
```

시나리오 4:액세스 로그에서 머신 이름 찾기

NTLMSSP 인증 체계를 사용할 때 사용자 에이전트(Microsoft NCSI가 가장 일반적임)가 사용자 자격 증명 대신 머신 자격 증명을 잘못 전송하는 인스턴스가 발생할 수 있습니다.이 문제를 일으키는 URL/User Agent를 추적하려면 인증이 발생했을 때 요청된 요청을 격리하기 위해 grep와 regex를 사용합니다.

사용된 머신 이름이 없는 경우 grep를 사용하여 이 regex로 인증할 때 사용자 이름으로 사용된 모든 머신 이름을 찾습니다.

```
\$@
```

이러한 현상이 발생하는 줄이 있으면 이 regex와 함께 사용된 특정 머신 이름에 grep를 입력합니다.

```
machinename\$
```

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

시나리오 5:액세스 로그에서 특정 기간 찾기

기본적으로 액세스 로그 서브스크립션에는 사용자가 읽을 수 있는 날짜/시간을 표시하는 필드가 포함되지 않습니다.특정 기간 동안 액세스 로그를 확인하려면 다음 단계를 완료하십시오.

1. 온라인 변환과 같은 사이트에서 UNIX 타임스탬프를 찾습니다.
2. 타임스탬프가 있으면 액세스 로그 내에서 특정 시간을 검색합니다.

예를 들면 다음과 같습니다.

Unix 타임스탬프의 **1325419200**은 **01/01/2012 12:00:00과** 같습니다.

2012년 1월 1일에 12:00에 가까운 액세스 로그를 검색하려면 이 regex 항목을 사용할 수 있습니다.

13254192

시나리오 6:위험 또는 경고 메시지 검색

프록시 로그 또는 시스템 로그와 같은 사용 가능한 로그에서 정규식을 사용하여 위험 또는 경고 메시지를 검색할 수 있습니다.

예를 들면 다음과 같습니다.

프록시 로그에서 경고 메시지를 검색하려면 다음 regex를 입력합니다.

```
CLI> grep
```

그리려는 로그 번호를 **입력합니다**.

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

grep할 정규식을 **입력합니다**.

```
[]> warning
```