ESA, SMA und WSA Grep mit Regex to Search Logs

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mit dem Befehl **grep** reguläre Ausdrücke (Regex) verwenden, um Protokolle zu durchsuchen.

Voraussetzungen

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Web Security Appliance (WSA)
- Cisco E-Mail Security Appliance (ESA)
- Cisco Security Management Appliance (SMA)

Greg mit Regex

Regex kann ein leistungsstarkes Tool sein, wenn es mit dem Befehl **grep** verwendet wird, um nach Protokollen zu suchen, die auf der Appliance verfügbar sind, z. B. Zugriffsprotokolle, Proxy-Protokolle usw. Sie können die Protokolle anhand der Website oder eines beliebigen Teils der URL und der Benutzernamen mit dem Befehl **grep** CLI durchsuchen.

Hier sind einige gängige Szenarien, in denen Sie regex mit dem Befehl **grep** verwenden können, um die Fehlerbehebung zu unterstützen.

Szenario 1: Suchen einer bestimmten Website in den Zugriffsprotokollen

Das häufigste Szenario ist, wenn Sie versuchen, Anfragen zu finden, die an eine Website in den Zugriffsprotokollen der WSA gesendet werden.

Hier ein Beispiel:

Stellen Sie über Secure Shell (SSH) eine Verbindung zur Appliance her. Geben Sie nach der Eingabeaufforderung den Befehl **grep ein**, um die verfügbaren Protokolle aufzulisten.

```
CLI> grep
```

Geben Sie die Nummer des Protokolls ein, das Sie **grep** verwenden möchten.

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

Geben Sie den regulären Ausdruck in **grep ein**.

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

Szenario 2: Versuchen Sie, eine bestimmte Dateierweiterung oder Domäne der obersten Ebene zu finden.

Sie können den Befehl **grep** verwenden, um eine bestimmte Dateierweiterung (.doc, .pptx) in einer URL oder einer Domäne der obersten Ebene (.com, .org) zu finden.

Hier ein Beispiel:

Um alle URLs zu finden, die mit .crl enden, verwenden Sie den folgenden regulären Ausdruck:

```
\.crl$
```

Um alle URLs zu finden, die die Dateierweiterung .pptx enthalten, verwenden Sie den folgenden regulären Ausdruck:

```
\.pptx
```

Szenario 3: Versuchen Sie, einen bestimmten Block für eine Website zu suchen.

Wenn Sie nach einer bestimmten Website suchen, können Sie auch nach einer bestimmten HTTP-Antwort suchen.

Hier ein Beispiel:

Wenn Sie nach allen TCP_DENIED/403-Nachrichten für domain.com suchen möchten, verwenden Sie den folgenden Regex:

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

Szenario 4: Suchen eines Maschinennamens in den Zugriffsprotokollen

Wenn Sie das NTLMSSP-Authentifizierungsschema verwenden, können Sie auf eine Instanz stoßen, in der ein User Agent (Microsoft NCSI ist die häufigste) bei der Authentifizierung fälschlicherweise Anmeldeinformationen an einen Computer anstatt Benutzeranmeldeinformationen sendet. Um die URL/den Benutzer-Agent zu ermitteln, die dieses Problem verursacht, verwenden Sie regex mit **grep**, um die Anforderung zu isolieren, die bei der Authentifizierung gestellt wurde.

Wenn Sie nicht den verwendeten Computernamen haben, verwenden Sie **grep** und suchen Sie alle Computernamen, die bei der Authentifizierung mit diesem regulären Ausdruck als Benutzernamen verwendet wurden:

```
\$@
```

Wenn Sie die Zeile haben, in der dies auftritt, sollten Sie für den spezifischen Computernamen, der mit diesem regulären Ausdruck verwendet wurde, die folgende Zeile verwenden:

```
machinename\$
```

Der erste angezeigte Eintrag sollte die Anforderung sein, die bei der Authentifizierung des Benutzers mit dem Computernamen anstelle des Benutzernamens erstellt wurde.

Szenario 5: Suchen eines bestimmten Zeitraums in den Zugriffsprotokollen

Standardmäßig enthalten die Zugriffsprotokollabonnements nicht das Feld, das das für den Benutzer lesbare Datum/die Uhrzeit anzeigt. Wenn Sie die Zugriffsprotokolle für einen bestimmten Zeitraum überprüfen möchten, führen Sie die folgenden Schritte aus:

1. Suchen Sie den UNIX-Zeitstempel von einer Website aus, z. B. Online Conversion.
2. Wenn Sie den Zeitstempel eingegeben haben, suchen Sie in den Zugriffsprotokollen nach einer bestimmten Uhrzeit.

Hier ein Beispiel:

Ein Unix-Zeitstempel von **1325419200** entspricht dem **01.01.2012 12:00:00**.

Sie können diesen regulären Eintrag verwenden, um am 1. Januar 2012 um fast 12:00 Uhr die Zugriffsprotokolle zu durchsuchen:

13254192

Szenario 6: Suchen nach kritischen oder Warnmeldungen

Sie können in allen verfügbaren Protokollen (z. B. Proxy-Protokolle oder Systemprotokolle) mit regulären Ausdrücken nach kritischen oder Warnmeldungen suchen.

Hier ein Beispiel:

Um nach Warnmeldungen in den Proxyprotokollen zu suchen, geben Sie den folgenden regulären Ausdruck ein:

```
CLI> grep
```

Geben Sie die Nummer des Protokolls ein, das Sie **grep** verwenden möchten.

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

Geben Sie den regulären Ausdruck in **grep ein**.

```
[]> warning
```