Wie verwenden Sie reguläre Ausdrücke (Regex) mit grep, um Protokolle zu durchsuchen?

Inhalt

Frage

Wie verwenden Sie reguläre Ausdrücke (Regex) mit grep, um Protokolle zu durchsuchen?

Umgebung

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

Lösung

Reguläre Ausdrücke (Regex) können ein leistungsstarkes Tool sein, wenn Sie mit dem Befehl "grep" nach Protokollen suchen, die auf der Appliance verfügbar sind, z. B. Zugriffsprotokolle, Proxy-Protokolle und andere. Bei Verwendung des CLI-Befehls "grep" können wir anhand der Website oder eines beliebigen Teils der URL oder der Benutzernamen nach einigen Protokollen suchen.

Im Folgenden finden Sie einige gängige Szenarien, in denen Sie regex mit grep zur Fehlerbehebung verwenden können.

Szenario 1: Suchen einer bestimmten Website in den Zugriffsprotokollen

Das häufigste Szenario ist der Versuch, Anfragen zu einer Website in den Zugriffsprotokollen der

Cisco Web Security Appliance (WSA) zu finden.

Beispiel:
Stellen Sie über SSH eine Verbindung zur Appliance her. Sobald Sie die Eingabeaufforderung haben, können wir den Befehl "grep" eingeben, um die verfügbaren Protokolle aufzulisten.

CLI> grep
Geben Sie die Nummer des Protokolls ein, das Sie "grep" eingeben möchten. []> 1 (Wählen Sie hier die # für Zugriffsprotokolle aus)
Geben Sie den regulären Ausdruck als "grep" ein. []> **Website\.com**

Szenario 2: Versuch, eine bestimmte Dateierweiterung oder Domäne oberster Ebene zu finden

Mithilfe des Befehls "grep" können wir eine bestimmte Dateierweiterung (.doc, .pptx) in einer URL oder einer übergeordneten Domäne (.com, .org) finden.

Beispiel:
Um alle URLs zu finden, die mit .crl enden, können Sie den folgenden regulären Ausdruck verwenden: **\.crl$**

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

Szenario 3: Versuchen, einen bestimmten Block für eine Website zu finden

Bei der Suche nach einer bestimmten Website suchen wir möglicherweise auch nach einer bestimmten HTTP-Antwort.

Beispiel:
Wenn wir nach allen TCP_DENIED/403-Nachrichten für domain.com suchen möchten, können wir den folgenden regulären Ausdruck verwenden: **tcp_leugnen/403.*Domäne\.com**

Szenario 4: Suchen eines Maschinennamens in den Zugriffsprotokollen

Bei der Verwendung des NTLMSSP-Authentifizierungsschemas kann es vorkommen, dass ein Benutzer-Agent (Microsoft NCSI ist die häufigste) bei der Authentifizierung nicht die Anmeldeinformationen des Benutzers, sondern die Anmeldeinformationen des Computers falsch sendet. Um die URL/den Benutzer-Agent zu ermitteln, die dies verursacht, können wir regex mit "grep" verwenden, um die Anforderung zu isolieren, die bei der Authentifizierung gestellt wurde.

Wenn wir nicht den verwendeten Computernamen haben, können wir "grep" verwenden und alle Computernamen finden, die bei der Authentifizierung als Benutzernamen verwendet wurden, indem wir den folgenden regulären Ausdruck verwenden: **\$@**

Sobald die Zeile vorhanden ist, in der dies auftritt, können wir für den spezifischen

Computernamen, der mit dem folgenden regulären Ausdruck verwendet wurde, "grep" eingeben:
Maschinenname\$

Der erste 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

In der Standardeinstellung enthalten die Protokoll-Subscriptions nicht das Feld, in dem das von Menschen lesbare Datum/die Uhrzeit angezeigt wird. Wenn wir die Zugriffsprotokolle für einen bestimmten Zeitraum überprüfen möchten, können wir die folgenden Schritte ausführen:

Suchen Sie den UNIX-Zeitstempel von einer Website wie http://www.onlineconversion.com/unix_time.htm. Sobald der Zeitstempel vorhanden ist, können Sie in den Zugriffsprotokollen nach einer bestimmten Zeit suchen.

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

Mithilfe des folgenden regulären Eintrags können Sie die Zugriffsprotokolle zum 1. Januar 2012 um etwa 12:00 Uhr durchsuchen: 13254192

Szenario 6: Suchen nach kritischen oder Warnmeldungen

Mithilfe von regulären Ausdrücken können wir in allen verfügbaren Protokollen, z. B. in Proxy- oder Systemprotokollen, nach kritischen oder Warnmeldungen suchen.

Beispiel:
Um nach Warnmeldungen in den Proxyprotokollen zu suchen, können Sie den folgenden regulären Ausdruck eingeben:

1. **CLI>** grep
2. Geben Sie die Nummer des Protokolls ein, das Sie "grep" eingeben möchten.
   []> 17 (Wählen Sie hier die # für Proxy-Protokolle aus)
3. Geben Sie den regulären Ausdruck als "grep" ein.
   []> **Warnung**

Weitere nützliche Links:

Reguläre Ausdrücke - Benutzerhandbuch