Hoe gebruik je reguliere expressies (regex) met grep om te zoeken naar logs?

Inhoud

vraag

Hoe gebruik je reguliere expressies (regex) met grep om te zoeken naar logs?

Omgeving

Cisco web security applicatie
Cisco e-mail security applicatie
Cisco Security Management-applicatie

Oplossing

Reguliere expressies (regex) kunnen een krachtig gereedschap zijn wanneer ze worden gebruikt met de opdracht "grep" om door middel van logs op het apparaat te zoeken, zoals Access Logs, Proxy Logs, en anderen. We kunnen de logs doorzoeken op basis van de website, of een deel van de URL of gebruikersnamen, om er een paar te noemen, bij gebruik van de CLI-opdracht "grep".

Hieronder staan enkele gebruikelijke scenario's waar u regex met grep kunt gebruiken om te helpen bij het oplossen van problemen.

Scenario 1: Een bepaalde website vinden in de toegangslijsten

Het meest gebruikelijke scenario is het proberen om verzoeken te vinden die aan een website in de toegangslogs van de Cisco Web Security Appliance (WSA) worden gemaakt.

Bijvoorbeeld:
Sluit de stekker aan op het apparaat via SSH. Zodra u de melding hebt, kunnen we de opdracht "grep" typen om een lijst van de beschikbare logbestanden op te nemen.

CLI> grep
Voer het nummer in van het logbestand dat u wilt "invoegen". []> 1 (kies hier # voor toegangslogbestanden)
Geef de reguliere expressie op naar "grep". []> **website\.com**

Scenario 2: Probeer een bepaalde bestandsuitbreiding of een topniveaudomein te zoeken

We kunnen de opdracht "grep" gebruiken om een bepaalde bestandsuitbreiding (.doc,.pptx) te vinden in een URL of een top-level domein (.com,.org).

Bijvoorbeeld:
Om alle URL's te vinden die eindigen met .crl kunnen we de volgende regex gebruiken: **\.crl$**

Om alle URL's te vinden die de bestandsextensie .pptx bevatten, kunnen we de volgende regex gebruiken: **\.pptx**

Scenario 3: Proberen een specifiek blok voor een website te vinden

Bij het zoeken naar een bepaalde website zouden we ook op zoek kunnen gaan naar een bepaalde HTTP-respons.

Bijvoorbeeld:
Als we naar alle TCP_DENIED/403-berichten voor domein.com wilden zoeken, konden we de volgende regex gebruiken: **tcp_ont/403.*domein\.com**

Scenario 4: Een machinenaam zoeken in de toegangslijsten

Wanneer u NTLMSSP-verificatieregeling gebruikt, kunnen we een instantie tegenkomen waar een gebruikersagent (Microsoft NCSI is het meest gebruikelijk) bij het authentificeren van machines in plaats van gebruikersreferenties onjuist zal verzenden. Om de URL/User Agent op te sporen die dit veroorzaakt, kunnen we regex met "grep" gebruiken om het verzoek te isoleren dat is gedaan toen de authenticatie plaatsvond.

Als de gebruikte machinenaam niet bestaat, kunnen we "grep" gebruiken en alle machinenamen zoeken die als gebruikersnamen werden gebruikt bij het echtheidsonderzoek met behulp van de volgende regex: **\$@**

Zodra we de regel hebben waar dit voorkomt, kunnen we "grep" voor de specifieke machinenaam gebruiken die gebruikt werd door de volgende regex te gebruiken: **machinenaam\$**

Het eerste bericht dat verschijnt, is het verzoek dat is ingediend toen de gebruiker gewaarmerkt is met de machinenaam in plaats van de gebruikersnaam.

Scenario 5: Een specifieke tijdsperiode in de toegangslijsten vinden

Standaard zullen de abonnementen op het toegangslogboek het veld niet omvatten dat de datum/tijd toont die door de mens kan worden gelezen. Als we de toegangsbestanden voor een bepaalde periode willen controleren, kunnen we de onderstaande stappen volgen:

Zoek de UNIX tijdstempel op van een site zoals http://www.onlineconversion.com/unix_time.htm. Zodra u de tijdstempel hebt, kunt u binnen de toegangslijsten naar een specifieke tijd zoeken.

Bijvoorbeeld:
Een Unix timestamp van 1325419200 is gelijk aan 01/01/2012 12:00:00.

We kunnen de volgende regex-ingang gebruiken om de toegangsbestanden rond de tijd van 12:00 uur te zoeken op 1 januari ^{2012}: 13254192

Scenario 6: Zoeken naar kritische of waarschuwingsberichten

We kunnen kritieke of waarschuwingsberichten in elke beschikbare logbestanden zoeken, zoals proxy-logs of systeemlogs, met behulp van reguliere expressies.

Bijvoorbeeld:
Als u waarschuwingsberichten in de proxy-bestanden wilt zoeken, kunnen we de volgende regex invoeren:

1. **CLI>** grep
2. Voer het nummer in van het logbestand dat u wilt "invoegen".
   []> 17 (kies # voor proxy-logbestanden hier)
3. Geef de reguliere expressie op naar "grep".
   []> **waarschuwing**

Andere nuttige links:

Reguliere expressies - gebruikershandleiding