ESA, SMA en WSA Grep met Regex naar zoeklogs

Inhoud

Inleiding

Dit document beschrijft hoe u reguliere expressies (regex) kunt gebruiken met de opdracht grep om in logbestanden te zoeken.

Voorwaarden

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Web Security applicatie (WSA)
- Cisco e-mail security applicatie (ESA)
- Cisco Security Management-applicatie (SMA)

Grep met Regex

Regex kan een krachtig hulpmiddel zijn wanneer het wordt gebruikt met de grep-opdracht om te zoeken in logboeken die op het apparaat beschikbaar zijn, zoals toegangslogboeken, proxylogboeken en andere. U kunt de logboeken op de website, of om het even welk deel van de URL, en gebruikersnamen met de grep CLI bevel zoeken.

Hier zijn een aantal veelvoorkomende scenario's waarin u regex kunt gebruiken met de grep opdracht om te helpen met probleemoplossing.

Scenario 1: Vind een bepaalde website in de Toegangslijsten

Het meest voorkomende scenario is wanneer u probeert om verzoeken te vinden die aan een website in de toegangslogboeken van de WSA worden gemaakt.

Hierna volgt een voorbeeld:

Sluit het apparaat aan via Secure Shell (SSH). Zodra u de prompt hebt, voert u de grep-opdracht in om een lijst van de beschikbare logbestanden op te maken.

```
<#root>

CLI>

grep
```

Voer het nummer in van het logbestand dat u wilt laten groeien.

```
<#root>

[]>

1

 (Choose the # for access logs here)
```

Voer de reguliere expressie in die moet worden gegrepen.

```
<#root>

[]>

website\.com
```

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

U kunt de grep opdracht gebruiken om een bepaalde bestandsextensie (.doc, .pptx) te vinden in een URL of een topleveldomein (.com, .org).

Hierna volgt een voorbeeld:

Om alle URL's te vinden die eindigen met .crl, gebruik deze regex:

```
\.crl$
```

Om alle URL's te vinden die de bestandsextensie .pptx bevatten, gebruikt u deze regex:

```
\.pptx
```

Scenario 3: Poging tot het vinden van een bepaald blok voor een website

Wanneer u naar een bepaalde website zoekt, kunt u ook zoeken naar een bepaalde HTTP-respons.

Hierna volgt een voorbeeld:

Als u wilt zoeken naar alle TCP_DENIED/403 berichten voor domain.com, gebruik deze regex:

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

Scenario 4: Zoek een machinenaam in de toegangslogboeken

Wanneer u de NTLMSSP-verificatieregeling gebruikt, kunt u een instantie tegenkomen waarbij een User Agent (Microsoft NCSI is de meest gebruikelijke) machinereferenties in plaats van gebruikersreferenties onjuist verstuurt wanneer deze worden geverifieerd. Om de URL/User Agent die dit probleem veroorzaakt op te sporen, gebruikt u regex met grep om het verzoek te isoleren dat is ingediend toen de verificatie plaatsvond.

Als u niet de machinenaam hebt die werd gebruikt, gebruik grep en vind alle machinenamen die als gebruikersnamen werden gebruikt bij het verifiëren met deze regex:

```
\$@
```

Zodra u de lijn hebt waar dit voorkomt, grep voor de specifieke machinenaam die met deze regex werd gebruikt:

```
machinename\$
```

De eerste ingang die verschijnt zou het verzoek moeten zijn dat werd ingediend toen de gebruiker met de machinenaam in plaats van de gebruikersnaam voor authentiek verklaarde.

Scenario 5: Vind een specifieke tijdsperiode in de toegangslijsten

In de standaardinstellingen voor toegangslogabonnementen is niet het veld opgenomen dat de menselijk leesbare datum/tijd toont. Als u de toegangslogboeken voor een bepaalde tijdspanne wilt controleren, voltooi deze stappen:

1. Zoek de Unix tijdstempel op vanaf een site zoals Online Conversion.
2. Zodra u de tijdstempel hebt, zoekt u naar een specifieke tijd binnen de toegangslogboeken.

Hierna volgt een voorbeeld:

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

U kunt deze regex-vermelding gebruiken om de toegangslogboeken rond 12:00 op 1 januari 2012 te doorzoeken:

13254192

Scenario 6: Zoeken naar kritische of waarschuwingsberichten

U kunt kritieke of waarschuwingsberichten zoeken in alle beschikbare logboeken, zoals proxylogboeken of systeemlogboeken, met reguliere expressies.

Hierna volgt een voorbeeld:

Om naar waarschuwingsberichten in de volmachtslogboeken te zoeken, ga dit regex in:

<#root>

CLI>

grep

Voer het nummer in van het logbestand dat u wilt laten groeien.

<#root>

[]>

1

7 (Choose the # for proxy logs here)

Voer de reguliere expressie in die moet worden gegrepen.

<#root>

[]>

warning

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.