Het First Responder Program (Secure Firewall Edition) begrijpen

Inhoud

Inleiding

Dit document beschrijft het gebruik en de implementatie van het Eerste Responder-programma voor Cisco Secure Firewall.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is gebaseerd op Cisco Secure Firewall-producten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het First Responder-programma is gemaakt door TAC om het gemakkelijker en sneller te maken om diagnostische gegevens te leveren voor de open cases. Het programma bestaat uit twee hoofdonderdelen:

Geautomatiseerde e-mail

Deze e-mail wordt aan het begin van de case verzonden met instructies over het verzamelen en uploaden van diagnostische gegevens voor TAC-analyse. Er zijn meerdere technologieën die gebruikmaken van dit systeem, en elke e-mail wordt toegewezen aan de "Technologie" en "Subtechnologie" die worden gekozen wanneer de case wordt aangemaakt.

Script/opdrachten

Elke implementatie van het First Responder-programma heeft zijn eigen unieke manier om gegevensverzameling en -levering te verwerken. De Secure Firewall-implementatie maakt gebruik van het TAC-authored FirePOWER.py Python-script om dit te realiseren. Het geautomatiseerde e-mailproces genereert een opdracht met één regel, die uniek is voor deze specifieke case, die kan worden gekopieerd en geplakt naar de CLI van beveiligde firewallapparaten die moeten worden uitgevoerd.

Reden voor deze e-mail

Er zijn bepaalde technologieën die zijn ingeschakeld voor het eerste antwoordprogramma. Dit betekent dat elke keer dat een case wordt geopend tegen een van deze enabled-technologieën, een eerste antwoordbericht wordt verstuurd. Als u een eerste antwoordbericht per e-mail ontvangt en gelooft niet dat de gegevensaanvraag relevant is, kunt u de communicatie negeren.

Voor de gebruikscase van Secure Firewall is het eerste antwoordprogramma beperkt tot de FTD-software (Firepower Threat Defence). Als u een ASA-code (Adaptive Security Appliance) gebruikt, moet u deze e-mail negeren. Aangezien deze twee producten op dezelfde hardware draaien, wordt algemeen opgemerkt dat ASA-cases worden gemaakt in de Secure Firewall-technologieruimte, die de eerste e-mail van de antwoordpersoon genereert.

Geautomatiseerde e-mail

Hier is een voorbeeld van de geautomatiseerde e-mail die als deel van dit programma wordt verzonden:

```
From: first-responder@cisco.com <first-responder@cisco.com>
Sent: Thursday, September 1, 2022 12:11 PM
To: John Doe <john.doe@cisco.com>
Cc: attach@cisco.com
Subject: SR 666666666 - First Responder Automated E-mail

Dear John,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution and the steps to collect them:

*** Troubleshoot File ***

* Connect to the device using SSH
* Issue the command expert, skip this step for FMC version 6.4.x and earlier
* Issue the command sudo su
* When prompted for the password, enter your password.
* For FMC 6.4 or FTD 6.7 and later issue the command
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

* For FMC 6.3 or FTD 6.6 and earlier issue the command
curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

For more information on what this command does, or to understand why you are receiving this e-
mail - please refer to
<LINK_TO_THIS_ARTICLE>

For 6.3 and earlier versions we recommend confirming cxd.cisco.com resolves to <CURRENT_CXD_IP1>
or
<CURRENT_CXD_IP2>. Furthermore, we recommend validating the SHA checksum of the file by running
url -s -k https://cxd.cisco.com/public/ctfr/firepower.py | shasum which should output
<CURRENT_SHA>.

If you are unable to upload troubleshooting files (or would prefer not to), please let us know
what
hardware and software version ou are running if you have not already.

Sincerely, First Responder Team
```

De geautomatiseerde e-mails voor het eerste antwoordprogramma zijn opgesplitst in twee delen, bekend als het introductieblok en het gegevensverzoekblok.

Inleiding Blok

Het introductieblok is een statische string die wordt opgenomen in elke eerste antwoordbericht e-mail. Deze inleidende zin dient alleen om de context van het (de) gegevensaanvraagblok(ken) aan te geven. Hier is een voorbeeld van een introductieblok:

```
Dear <NAME>,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
```

```
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution
and the steps to collect them:
```

Blok van gegevensaanvraag

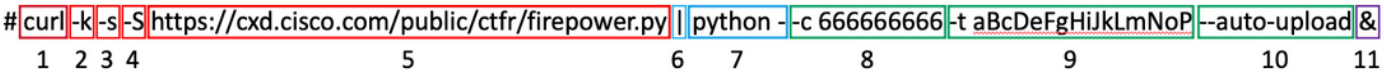
De gegevensaanvraagblokken vormen de kern van het eerste antwoordprogramma. Elk blok is een vooraf gedefinieerde set stappen om gegevens te verzamelen voor een bepaalde technologie. Zoals vermeld in de sectie **Achtergrondinformatie**, wordt elk gegevensaanvraagblok aan een specifieke technologie in kaart gebracht. Dit is dezelfde technologie die gekozen is om een ondersteuningscase te openen. Gewoonlijk bevat de geautomatiseerde e-mail één gegevensaanvraagblok. Als de gekozen technologie echter meer dan één gegevensaanvraagblok heeft toegewezen, worden meerdere gegevensverzoeken in de e-mail opgenomen. Hier is een voorbeeldformaat van het blok Gegevensverzoek met meerdere gegevensverzoeken:

```
*** <REQUEST NAME 1> ***

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

Bijvoorbeeld, in het geval van Secure Firewall, zijn meerdere gegevensaanvraagblokken vaak opgenomen wanneer een verzoek wordt ingediend voor hulp met problemen met Remote Access VPN (RA-VPN) met Firepower Threat Defence (FTD) omdat de VPN technologie ook een toegewezen gegevensverzoekblok heeft geconfigureerd voor hulp om de DART-bundels te verzamelen.

Gegenereerde opdracht

Voor de Secure Firewall wordt er specifiek een unieke opdracht met één regel gegenereerd voor elke case als deel van de geautomatiseerde e-mail. Hier is een analyse van de structuur van het één-lijn bevel:



1. De krulopdracht wordt gebruikt om de nieuwste versie van het script firepower.py te downloaden
2. De **-k** vlag is een optie voor krullen om certificaatfouten tijdens verbinding te negeren.
3. De **-s** vlag is een optie om krullen in stille modus te laten lopen. Dit wordt gebruikt om de normale kruluitvoer te onderdrukken aangezien het lawaai is.
4. De vlag **-S** is een optie voor krullen om fouten te tonen. Dit wordt gebruikt om krul te dwingen om nog outputfouten te tonen zelfs met de stille toegelaten optie.
5. De URL waar de nieuwste versie van het script firepower.py wordt gehost. Dit pad draagt de curl-opdracht op om de laatste body van het script om uit te voeren.
6. Dit is een Linux-pijp die de uitvoer van de curl-opdracht (de inhoud van een python-script) doorgeeft naar een executie-statement in de volgende stap.
7. In deze stap wordt de python binaire op het apparaat aangeroepen met een extra "-". Dit instrueert python dat de bron uit stdin wordt genomen (aangezien de inhoud van het script uit krul wordt overgepipt).
8. De **-c** vlag is een invoerargument voor het FirePOWER.py script, dat het casenummer

aangeeft waarop de gegevens moeten worden geüpload. De 666666666 na deze optie is het casenummer van het voorbeeld.

9. De **-t** vlag is een invoerargument voor het FirePOWER.py-script dat een uniek token (wachtwoord) aangeeft die voor deze case is gegenereerd. De waarde na deze optie van BCdeFgHiJkLmNoP is het voorbeeldtoken voor deze case.
10. De vlag **—auto-upload** is een speciaal argument voor het script firepower.py, dat het script aangeeft dat uitgevoerd moet worden in de automatiseringsmodus. Meer informatie hierover vindt u in de scriptspecifieke sectie.
11. The **&** draagt deze opdracht op om op de achtergrond te lopen, waardoor de gebruiker kan blijven communiceren met hun shell terwijl het script wordt uitgevoerd.

Opmerking: Vóór 6.4 is de vlag -k vereist voor elke versie van het VCC en voor elke versie van het FTD vóór 6.7, aangezien het basiscertificaat dat wordt gebruikt door CXD niet werd vertrouwd door de Vuurstroomapparaten tot versie 6.4 van het VCC en versie 6.7 van het FTD, waardoor de certificaatverificatie mislukt.

Firepower.py Script

Het belangrijkste doel van het script is om een diagnostische bundel te genereren en te uploaden van het Secure Firewall-apparaat dat een "probleemoplossing" wordt genoemd. Om dit probleemoplossingsbestand te genereren, roept het script firepower.py simpelweg het ingebouwde sf_troubleshoot.pl script dat verantwoordelijk is voor het maken van deze bundel. Dit is hetzelfde script dat wordt aangeroepen wanneer we een probleemoplossing genereren via de GUI. Naast het probleemoplossingsbestand heeft het script ook de mogelijkheid om andere diagnostische gegevens te verzamelen die niet zijn opgenomen als onderdeel van de probleemoplossingsbundel. Momenteel zijn de enige aanvullende gegevens die kunnen worden verzameld Core Files - maar dit kan in de toekomst worden uitgebreid als de noodzaak zich voordoet. Het script kan worden uitgevoerd in "Automation" of "Interactive" modus:

Automatisering

Deze modus is ingeschakeld wanneer we de optie "—automatisch uploaden" gebruiken wanneer we het script uitvoeren. Deze optie schakelt de interactieve aanwijzingen uit, maakt het verzamelen van kernbestanden mogelijk en uploadt automatisch gegevens naar de case. De opdracht met één regel die door de geautomatiseerde e-mail wordt gegenereerd, bevat de optie "—automatisch uploaden".

interactief

Dit is de standaarduitvoermodus voor het script. In deze modus ontvangt de gebruiker aanwijzingen om te bevestigen of hij al dan niet aanvullende diagnostische gegevens zoals kernbestanden moet verzamelen. Ongeacht de uitvoeringsmodus, wordt betekenisvolle output afgedrukt naar het scherm en vastgelegd in een logbestand om de voortgang van de scriptuitvoering aan te geven. Het script zelf is uitgebreid gedocumenteerd via in-line code commentaren en kan worden gedownload / beoordeeld op https://cxd.cisco.com/public/ctfr/firepower.py.

Verwachte uitvoer van het script

Hier is een voorbeeld van een succesvolle uitvoering van het script:

```
root@ftd:/home/admin# curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c
666666666 -t aBcDeFgHiJkLmNoP --auto-upload &
[1] 26422
root@ftd:/home/admin#
`/var/common/first_responder_notify` successfully uploaded to 666666666
Running sf_troubleshoot.pl command to create a troubleshoot file...
Troubleshoot file successfully generated at /ngfw/var/common/results-08-30-2022--135014.tar.gz
Attempting to upload troubleshoot to case...
##################################################################################################
############################## 100.0%
`/ngfw/var/common/results-08-30-2022--135014.tar.gz` successfully uploaded to 666666666
Found the following core files:
(0 B) - /ngfw/var/common/core_FAKE1.gz
(0 B) - /ngfw/var/common/core_FAKE2.gz
(0 B) - /ngfw/var/common/core_FAKE3.gz
Successfully created /ngfw/var/common/cores_666666666-1661867858.tar.gz
Attempting core file upload...
##################################################################################################
############################## 100.0%
`/ngfw/var/common/cores_6666666660-1661867858.tar.gz` successfully uploaded to 666666666
FINISHED!
```

Houd er rekening mee dat dit uitvoervoorbeeld kernbestanden uploadt. Als er geen kernbestanden op uw apparaat aanwezig zijn, een bericht "No core files found. Skipping core file processing" wordt gepresenteerd.

Veelvoorkomende problemen

Hier zijn enkele veelvoorkomende problemen die u kunt ervaren (in volgorde van proces / uitvoering):

E-mail security / URL herschrijven

Vaak wordt opgemerkt dat de eindgebruiker een of ander niveau van e-mailbeveiliging heeft dat de URL herschrijft. Dit wijzigt de opdracht met één regel die als deel van de geautomatiseerde e-mail wordt gegenereerd. Dit resulteert in een executie fout sinds de URL om het script te trekken is herschreven en is ongeldig. Hier is een voorbeeld van het verwachte één-lijn bevel:

```
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &
```

Stappen voor het oplossen

Als de URL in de opdracht uit de e-mail iets anders is dan "https://cxd.cisco.com/public/ctfr/firepower.py", dan is de URL waarschijnlijk herschreven tijdens het transport. Om dit probleem op te lossen, moet u de URL vervangen voordat we de opdracht uitvoeren.

DNS-fout

Deze krulfout wordt vaak gezien wanneer het apparaat niet in staat is om de URL op te lossen om het script te downloaden:

```
curl: (6) Could not resolve host: cxd.cisco.com
```

Stappen voor het oplossen

Om dit probleem te verhelpen, controleert u de DNS-instellingen op het apparaat om er zeker van te zijn dat de URL correct kan worden verwerkt.

Logbestand niet openen / maken

Een van de eerste dingen die het script probeert te doen is het aanmaken (of openen, als het al bestaat) van een logbestand met de naam **first-responder.log** in de huidige werkmap. Als deze operatie mislukt, wordt een fout die een eenvoudige toestemming aangeeft weergegeven:

```
Permission denied while trying to create log file. Are you running this as root?
```

Als onderdeel van deze bewerking worden alle andere fouten geïdentificeerd en op het scherm afgedrukt in deze indeling:

```
Something unexpected happened while trying to create the log file. Here is the error:
----------

----------
```

Stappen voor het oplossen

Om deze fout te repareren, moet u het script uitvoeren als een beheergebruiker zoals "admin" of "root".

Bestand niet openen / schrijven Melden bestand

Als onderdeel van de script uitvoering wordt een 0-byte bestand met de naam "first_responder_notification" aangemaakt op het systeem. Dit bestand wordt vervolgens naar de case geüpload als deel van de automatisering voor dit programma. Dit bestand wordt naar de map "/var/common" geschreven. Als de gebruiker die het script uitvoert niet over voldoende rechten beschikt om bestanden naar deze map te schrijven, dan geeft het script de fout weer:

```
Failed to create file -> `/var/common/first_responder_notify`. Permission denied. Are you
running as root?
```

Stappen voor het oplossen

Om deze fout te repareren, moet u het script uitvoeren als een beheergebruiker zoals "admin" of "root".

> **Opmerking:** Als er een fout optreedt die verband houdt met niet-machtigingen, wordt er een catch-all fout op het scherm afgedrukt "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". De volledige uitzondering

lichaam kan worden gevonden in de **first-responder.log** .

Kan sf_troubleshoot.pid bestand niet vergrendelen

Om er zeker van te zijn dat er slechts één probleemoplossingsgeneratieproces tegelijkertijd wordt uitgevoerd, probeert het probleemoplossingsgeneratiescript het /var/sf/run/sf_troubleshoot.pid bestand te vergrendelen voordat u doorgaat. Als het script het bestand niet kan vergrendelen, verschijnt er een fout:

```
Failed to run the `sf_troubleshoot.pl` command - existing sf_troubleshoot process detected.
Please wait for existing process to complete.
```

Stappen voor het oplossen

Meestal betekent deze fout dat er al een afzonderlijke taak voor het genereren van probleemoplossing in uitvoering is. Soms is dit het resultaat van gebruikers die per ongeluk twee keer op een rij de opdracht met één regel uitvoeren. Om dit probleem op te lossen, wacht u tot de huidige generatie probleemoplossing is voltooid en probeer het later opnieuw.

> **Opmerking:** Als er een fout in het script sf_troubleshoot.pl zelf optreedt, wordt deze fout op het scherm weergegeven **"Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error".** De volledige uitzondering lichaam kan worden gevonden in de **first-responder.log** .

Problemen met uploaden

Er is een algemene uploadfunctie in het script die verantwoordelijk is voor alle geüploade bestanden gedurende de hele scriptuitvoering. Deze functie is gewoon een python wrapper om een curl upload opdracht uit te voeren om de bestanden naar de case te sturen. Daarom worden fouten die tijdens de uitvoering worden aangetroffen, als curlfoutcode teruggegeven. In het geval van een uploadfout wordt deze fout op het scherm weergegeven:

```
[FAILURE] Failed to upload `/var/common/first_responder_notify` to 666666666. Please check the
first-responder.log file for the full error
```

Controleer het bestand **first-responder.log** om de volledige fout te zien. Meestal ziet het bestand first-responder.log er zo uit:

```
08/29/2022 06:51:57 PM - WARNING - Upload Failed with the following error:
----------
Command '['curl', '-k', '--progress-bar',
'https://666666666:aBcDeFgHiJkLmNoP@cxd.cisco.com/home/',
'--upload-file', '/var/common/first_responder_notify']' returned non-zero exit status 6
----------
```

Stappen voor het oplossen

In dit geval, keerde curl een exit status van **6** terug wat betekent **"kon gastheer niet oplossen "**. Dit is een eenvoudige DNS-fout terwijl we proberen om de hostname **cxd.cisco.com** op te lossen. Raadpleeg de documentatie bij de curl om onbekende uitgangsstatussen te decoderen.

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.