Kennenlernen des First Responder-Programms (Secure Firewall Edition)

Inhalt

Einleitung

Dieses Dokument beschreibt die Verwendung und Implementierung des First Responder-Programms für die Cisco Secure Firewall.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument basiert auf Cisco Secure Firewall-Produkten.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das First Responder-Programm wurde vom TAC entwickelt, um die Bereitstellung von Diagnosedaten für offene Tickets zu vereinfachen und zu beschleunigen. Das Programm besteht aus zwei Hauptkomponenten:

Automatisierte E-Mails

Diese E-Mail wird zu Beginn des Falls mit Anweisungen zum Sammeln und Hochladen von Diagnosedaten für die TAC-Analyse versendet. Es gibt mehrere Technologien, die dieses System nutzen, und jede E-Mail ist den "Technologien" und "Subtechnologien" zugeordnet, die bei Erstellung des Tickets ausgewählt werden.

Skript/Befehle

Jede Implementierung des First Responder-Programms hat ihre eigene, einzigartige Möglichkeit, mit der Erfassung und Übermittlung von Daten umzugehen. Die Secure Firewall-Implementierung verwendet dazu das vom TAC entwickelte Skript firepower.py Python. Der automatisierte E-Mail-Prozess generiert einen für diesen speziellen Fall eindeutigen einzeiligen Befehl, der kopiert und in die CLI der Secure Firewall-Geräte eingefügt werden kann, um sie auszuführen.

Grund für diese E-Mail

Es gibt bestimmte Technologien, die für das First Responder-Programm aktiviert sind. Das bedeutet, dass jedes Mal, wenn ein Verfahren gegen eine dieser aktivierten Technologien eröffnet wird, eine E-Mail an den Ersthelfer versendet wird. Wenn Sie eine Ersthelfer-E-Mail erhalten und die Datenanfrage für nicht relevant halten, können Sie die Mitteilung ignorieren.

Für den Anwendungsfall "Sichere Firewall" ist das First-Responder-Programm auf die Firepower Threat Defense (FTD)-Software beschränkt. Wenn Sie eine Adaptive Security Appliance (ASA) Code-Base verwenden, ignorieren Sie bitte diese E-Mail. Da diese beiden Produkte auf derselben Hardware ausgeführt werden, wird in der Regel festgestellt, dass ASA-Fälle im Technologiebereich für sichere Firewalls erstellt werden, der die ersten Responder-E-Mails generiert.

Automatisierte E-Mails

Hier ist ein Beispiel für eine automatisierte E-Mail, die im Rahmen dieses Programms versendet wird:

```
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
```

Die automatisierten E-Mails für das erste Responder-Programm sind in zwei Teile aufgeteilt, die als Einführungsblock und Datenanforderungsblock bezeichnet werden.

Einführungsblock

Der Einführungsblock ist eine statische Zeichenfolge, die in jeder E-Mail des ersten Responders enthalten ist. Dieser einleitende Satz dient lediglich dazu, Kontext zu den Datenanforderungsblöcken bereitzustellen. Hier ein Beispiel für einen Einführungsblock:

```
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:
```

Datenanforderungsblock

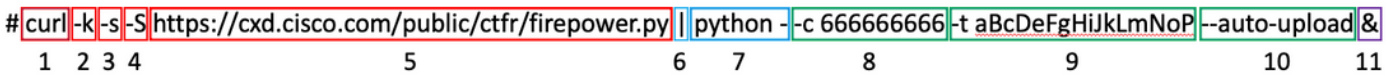
Die Datenanforderungsblöcke sind das Herzstück des ersten Responder-Programms. Jeder Block umfasst eine Reihe vordefinierter Schritte zum Erfassen von Daten für eine bestimmte Technologie. Wie im Abschnitt **Hintergrundinformationen** erwähnt, wird jeder Datenanforderungsblock einer bestimmten Technologie zugeordnet. Dies ist die gleiche Technologie, die zum Öffnen eines Support-Tickets gewählt wird. Normalerweise enthält die automatische E-Mail einen einzelnen Datenanforderungsblock. Wenn der ausgewählten Technologie jedoch mehr als ein Datenanforderungsblock zugeordnet ist, werden mehrere Datenanforderungen in die E-Mail aufgenommen. Das folgende Beispielformat für den Datenanforderungsblock mit mehreren Datenanforderungen wird verwendet:

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

Im Fall einer sicheren Firewall sind häufig mehrere Datenanforderungsblöcke enthalten, wenn eine Anforderung zur Unterstützung bei Remote Access VPN (RA-VPN)-Problemen mit Firepower Threat Defense (FTD) ausgelöst wird, da der VPN-Technologie auch ein zugeordneter Datenanforderungsblock zugeordnet ist, der für die Unterstützung beim Sammeln der DART-Pakete konfiguriert ist.

Generierter Befehl

Speziell für den Anwendungsfall "Sichere Firewall" wird im Rahmen der automatisierten E-Mail für jeden Fall ein eindeutiger einzeiliger Befehl generiert. Hier eine Aufschlüsselung der Struktur des einzeiligen Befehls:



1. Der curl-Befehl wird verwendet, um die neueste Version des firepower.py-Skripts herunterzuladen
2. Das **-k**-Flag ist eine Option für curl, um Zertifikatfehler während der Verbindung zu ignorieren.
3. Das **-s**-Flag ist eine Option, mit der curl im automatischen Modus ausgeführt werden kann. Dies wird verwendet, um die normale Curl-Ausgabe zu unterdrücken, da es laut ist.
4. Die **-S** Flag ist eine Option für curl Fehler anzeigen. Dies wird verwendet, um zu erzwingen, dass curl immer noch Ausgabefehler zeigt, auch wenn die Option silent aktiviert ist.
5. Die URL, unter der die neueste Version des Skripts firepower.py gehostet wird. Dieser Pfad weist den curl-Befehl an, den neuesten Text des auszuführenden Skripts zu ziehen.
6. Dies ist eine Linux-Pipe, die die Ausgabe des curl-Befehls (den Inhalt eines Python-Skripts) an eine Ausführungsanweisung im nächsten Schritt übergibt.
7. In diesem Schritt wird die Python-Binärdatei auf dem Gerät mit einem zusätzlichen "-" aufgerufen. Dadurch wird python angewiesen, dass die Quelle von stdin übernommen wird

(da der Inhalt des Skripts von curl weitergeleitet wird).

8. Das **-c**-Flag ist ein Eingabeargument für das firepower.py-Skript, das die Fallnummer angibt, in die die Daten hochgeladen werden müssen. Der Wert 666666666 nach dieser Option ist die Beispielfallnummer.
9. Das **-t**-Flag ist ein Eingabeargument für das firepower.py-Skript, das ein eindeutiges Token (Kennwort) angibt, das für diesen speziellen Fall generiert wurde. Der Wert aBcDeFgHiJkLmNoP nach dieser Option ist das Beispieltoken für diesen Fall.
10. Das **—auto-upload-**Flag ist ein spezielles Argument für das firepower.py-Skript, das angibt, dass das Skript im Automatisierungsmodus ausgeführt wird. Weitere Informationen hierzu finden Sie im Abschnitt Skriptspezifische.
11. Das **&** weist den gesamten Befehl an, im Hintergrund zu laufen, wodurch der Benutzer während der Skriptausführung weiter mit seiner Shell interagieren kann.

Anmerkung: Das -k-Flag ist für alle FMC-Versionen vor 6.4 und für alle FTD-Versionen vor 6.7 erforderlich, da das von CXD verwendete Root-Zertifikat von Firepower-Geräten bis FMC-Version 6.4 und FTD-Version 6.7 nicht als vertrauenswürdig galt. Dies führt dazu, dass die Zertifikatsüberprüfung fehlschlägt.

Firepower.py-Skript

Das Hauptziel des Skripts besteht darin, ein Diagnosepaket vom Secure Firewall-Gerät zu generieren und hochzuladen. Dieses wird als "Fehlerbehebung" bezeichnet. Um diese Fehlerbehebungsdatei zu erstellen, ruft das Skript firepower.py das integrierte Skript sf_troubleshoot.pl auf, das für die Erstellung dieses Pakets verantwortlich ist. Dies ist das gleiche Skript, das aufgerufen wird, wenn wir eine Fehlerbehebung über die GUI generieren. Neben der Fehlerbehebungsdatei kann das Skript auch andere Diagnosedaten erfassen, die nicht im Fehlerbehebungspaket enthalten sind. Derzeit können nur noch Kerndateien erfasst werden - diese können jedoch bei Bedarf erweitert werden. Das Skript kann entweder im Automatisierungs- oder im Interaktionsmodus ausgeführt werden:

Automatisierung

Dieser Modus ist aktiviert, wenn Sie beim Ausführen des Skripts die Option "—auto-upload" verwenden. Diese Option deaktiviert interaktive Eingabeaufforderungen, aktiviert die Erfassung der Kerndateien und lädt automatisch Daten in das Ticket. Der einzeilige Befehl, der von der automatischen E-Mail generiert wird, umfasst die Option "—auto-upload".

Interaktiv

Dies ist der standardmäßige Ausführungsmodus für das Skript. In diesem Modus erhält der Benutzer Eingabeaufforderungen, mit denen er bestätigen kann, ob zusätzliche Diagnosedaten wie Core-Dateien erfasst werden sollen. Unabhängig vom Ausführungsmodus werden aussagekräftige Ausgaben auf den Bildschirm gedruckt und in einer Protokolldatei protokolliert, um den Fortschritt der Skriptausführung anzuzeigen. Das Skript selbst wird ausführlich über Inline-Code-Kommentare dokumentiert und kann unter https://cxd.cisco.com/public/ctfr/firepower.py heruntergeladen/überprüft werden.

Erwartete Ausgabe des Skripts

Das folgende Beispiel zeigt eine erfolgreiche Ausführung des Skripts:

```
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!
```

Beachten Sie, dass dieses Ausgabebeispiel Uploads von Core-Dateien umfasst. Wenn auf Ihrem Gerät keine Kerndateien vorhanden sind, wird eine Meldung "No core files found. Skipping core file processing" wird stattdessen angezeigt.

Häufige Probleme

Hier sind einige häufige Probleme, die auftreten können (in der Reihenfolge des Prozesses/der Ausführung):

E-Mail-Sicherheit/URL-Re-Write

Häufig wird beobachtet, dass der Endbenutzer eine gewisse Stufe von E-Mail-Sicherheit hat, die die URL umschreibt. Dadurch wird der einzeilige Befehl geändert, der als Teil der automatisierten E-Mail generiert wird. Dies führt zu einem Ausführungsfehler, da die URL zum Abrufen des Skripts neu geschrieben wurde und ungültig ist. Das folgende Beispiel zeigt den erwarteten einzeiligen Befehl:

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

Schritte zur Problembehebung

Wenn die URL im Befehl aus der E-Mail etwas Anderes als "https://cxd.cisco.com/public/ctfr/firepower.py" ist, wurde die URL wahrscheinlich während der Übertragung neu geschrieben. Um dieses Problem zu beheben, ersetzen Sie einfach die URL, bevor Sie den Befehl ausführen.

DNS-Fehler

Dieser Rollfehler tritt häufig auf, wenn das Gerät die URL zum Herunterladen des Skripts nicht

auflösen kann:

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

Schritte zur Problembehebung

Um dieses Problem zu beheben, überprüfen Sie die DNS-Einstellungen auf dem Gerät, um sicherzustellen, dass es die URL richtig auflösen kann, um fortzufahren.

Fehler beim Öffnen/Erstellen der Protokolldatei

Eines der ersten Dinge, die das Skript zu tun versucht, ist eine Protokolldatei namens **first-responder.log** im aktuellen Arbeitsverzeichnis zu erstellen (oder zu öffnen, wenn sie bereits existiert). Wenn dieser Vorgang fehlschlägt, wird ein Fehler angezeigt, der auf ein einfaches Berechtigungsproblem hinweist:

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

Im Rahmen dieses Vorgangs werden alle anderen Fehler erkannt und in diesem Format auf den Bildschirm gedruckt:

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

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

Schritte zur Problembehebung

Um diesen Fehler zu beheben, führen Sie das Skript als Administrator aus, z. B. als "admin" oder "root".

Fehler beim Öffnen/Schreiben der Benachrichtigungsdatei

Im Rahmen der Skriptausführung wird eine 0-Byte-Datei mit dem Namen "first_responder_notify" auf dem System erstellt. Diese Datei wird dann im Rahmen der Automatisierung für dieses Programm in das Ticket hochgeladen. Diese Datei wird in das Verzeichnis "/var/common" geschrieben. Wenn der Benutzer, der das Skript ausführt, nicht über ausreichende Berechtigungen zum Schreiben von Dateien in dieses Verzeichnis verfügt, zeigt das Skript den folgenden Fehler an:

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

Schritte zur Problembehebung

Um diesen Fehler zu beheben, führen Sie das Skript als Administrator aus, z. B. als "admin" oder "root".

> **Anmerkung:** Wenn ein nicht berechtigungsbezogener Fehler auftritt, wird ein catch-all-Fehler auf dem Bildschirm ausgegeben "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". Der vollständige Ausnahmetext befindet sich in **first-responder.log** .

Fehler beim Sperren der Datei sf_troubleshoot.pid

Um sicherzustellen, dass immer nur ein Fehlerbehebungsprozess ausgeführt wird, versucht das Fehlerbehebungsgenerierungsskript, die Datei /var/sf/run/sf_troubleshoot.pid zu sperren, bevor Sie fortfahren. Wenn das Skript die Datei nicht sperrt, wird ein Fehler angezeigt:

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

Schritte zur Problembehebung

Meistens bedeutet dieser Fehler, dass bereits eine separate Aufgabe zur Fehlerbehebung ausgeführt wird. Manchmal ist dies das Ergebnis von Benutzern, die versehentlich den einzeiligen Befehl zweimal hintereinander ausführen. Warten Sie, bis der aktuelle Fehlerbehebungsgenerierungsauftrag abgeschlossen ist, und versuchen Sie es später erneut.

> **Anmerkung:** Wenn ein Fehler im Skript sf_troubleshoot.pl auftritt, wird dieser Fehler auf dem Bildschirm angezeigt **"Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error".** Der vollständige Ausnahmetext befindet sich in **first-responder.log** .

Probleme beim Hochladen

Es gibt eine gemeinsame Upload-Funktion im Skript, die für alle Datei-Uploads während der Skriptausführung verantwortlich ist. Diese Funktion ist einfach ein Python-Wrapper, um einen Curl-Upload-Befehl auszuführen, um die Dateien an das Gehäuse zu senden. Aus diesem Grund werden alle während der Ausführung aufgetretenen Fehler als Curl-Fehlercode zurückgegeben. Falls der Upload fehlschlägt, wird dieser Fehler auf dem Bildschirm angezeigt:

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

Überprüfen Sie die Datei **first-responder.log**, um den vollständigen Fehler anzuzeigen. Normalerweise sieht die Datei first-responder.log wie folgt aus:

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

Schritte zur Problembehebung

In diesem Fall hat curl den Exitstatus **6** zurückgegeben, was bedeutet*: "***Host konnte nicht**

aufgelöst ". Dies ist ein einfacher DNS-Fehler, während wir versuchen, den Hostnamen **cxd.cisco.com** aufzulösen. In der Curl-Dokumentation können Sie unbekannte Exit-Status entschlüsseln.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.