Descripción del programa First Responder (Secure Firewall Edition)

Contenido

Introducción

Este documento describe el uso y la implementación del programa First Responder para Cisco Secure Firewall.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento se basa en los productos Cisco Secure Firewall.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El TAC ha creado el programa First Responder para facilitar y acelerar el suministro de datos de diagnóstico para los casos abiertos. El programa consta de dos componentes principales:

Correo electrónico automatizado

Este correo electrónico se envía al principio del caso con instrucciones sobre cómo recopilar y cargar datos de diagnóstico para el análisis del TAC. Hay varias tecnologías que aprovechan este sistema y cada correo electrónico se asigna a la "tecnología" y la "subtecnología" que se eligen al crear el caso.

Script / Comandos

Cada aplicación del programa First Responder tiene su propia forma única de gestionar la recogida y entrega de datos. La implementación de Secure Firewall utiliza el script firepower.py Python creado por TAC para lograr esto. El proceso de correo electrónico automatizado genera un comando de una línea, único en este caso específico, que se puede copiar y pegar en la CLI de los dispositivos de firewall seguro para su ejecución.

Motivo de este correo electrónico

Hay ciertas tecnologías que están habilitadas para el programa de primera respuesta. Esto significa que cada vez que se abre un caso contra una de estas tecnologías habilitadas, se envía un correo electrónico de respuesta inicial. Si recibe un mensaje de correo electrónico de respuesta inicial y no cree que la solicitud de datos sea relevante, no dude en ignorar la comunicación.

En el caso del firewall seguro, el primer programa de respuesta se limita al software Firepower Threat Defence (FTD). Si ejecuta un código base del dispositivo de seguridad adaptable (ASA), ignore este correo electrónico. Dado que estos dos productos se ejecutan en el mismo hardware, se suele observar que los casos de ASA se crean en el espacio de la tecnología Secure Firewall, que genera el primer correo electrónico de respuesta.

Correo electrónico automatizado

A continuación se muestra un ejemplo del correo electrónico automatizado que se envía como parte de este programa:

```
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
```

Los correos electrónicos automatizados para el primer programa de respuesta se dividen en dos partes conocidas como Bloque de introducción y Bloque de solicitud de datos.

Bloque de introducción

El bloque de introducción es una cadena estática que se incluye en cada correo electrónico de respuesta inicial. Esta frase introductoria sirve simplemente para proporcionar contexto a los bloques de solicitud de datos. A continuación se muestra un ejemplo de un bloque de introducción:

```
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:
```

Bloque de solicitud de datos

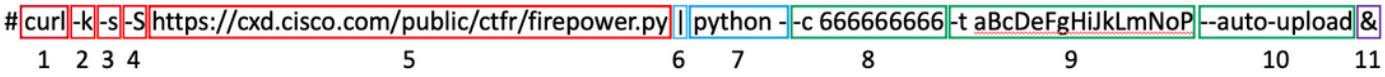
Los bloques de solicitud de datos son el corazón del primer programa de respuesta. Cada bloque es un conjunto predefinido de pasos para recopilar datos para una tecnología determinada. Como se mencionó en la sección **Información de fondo**, cada bloque de solicitud de datos se asigna a una tecnología específica. Esta es la misma tecnología que se elige para abrir un caso de soporte. Normalmente, el correo electrónico automatizado contiene un solo bloque de solicitud de datos. Sin embargo, si la tecnología elegida tiene más de un bloque de solicitud de datos asignado, se incluirán varias solicitudes de datos en el correo electrónico. Este es un ejemplo de formato del bloque de Solicitud de datos con varias solicitudes de datos:

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

Por ejemplo, en el caso de Secure Firewall, cuando se solicita asistencia con problemas de VPN de acceso remoto (RA-VPN) con Firepower Threat Defence (FTD), se suelen incluir varios bloques de solicitud de datos, ya que la tecnología VPN también tiene un bloque de solicitud de datos asignado configurado para ayudar a recopilar los paquetes DART.

Comando generado

Para el caso práctico de Secure Firewall en concreto, se genera un comando único de una línea para cada caso como parte del correo electrónico automatizado. A continuación se presenta un desglose de la estructura del comando de una línea:



1. El comando curl se utiliza para descargar la última versión del script firepower.py
2. El indicador **-k** es una opción para que curl ignore los errores de certificado durante la conexión.
3. El indicador **-s** es una opción para que curl se ejecute en modo silencioso. Esto se utiliza para suprimir la salida normal del rizo ya que es ruidoso.
4. El indicador **-S** es una opción para que curl muestre errores. Esto se utiliza para forzar a curl a mostrar aún errores de salida incluso con la opción silenciosa habilitada.
5. La URL donde se aloja la última versión del script firepower.py. Esta trayectoria indica al comando curl que extraiga el último cuerpo del script que se ejecutará.
6. Esta es una canalización de Linux, que pasa la salida del comando curl (el contenido de un script python) a una sentencia de ejecución en el siguiente paso.
7. En este paso, se llama al binario python del dispositivo con un "-" adicional. Esto indica a python que el origen se toma de stdin (ya que el contenido del script se canaliza desde curl).
8. El indicador **-c** es un argumento de entrada para la secuencia de comandos firepower.py, que indica el número de caso en el que se deben cargar los datos. El valor 666666666 detrás de esta opción es el número de caso de ejemplo.
9. El indicador **-t** es un argumento de entrada para el script firepower.py, que indica un token único (contraseña) que se generó para este caso en particular. El valor aBcDeFgHiJkLmNoP

después de esta opción es el símbolo de ejemplo para este caso.

10. El indicador **—auto-upload** es un argumento especial para la secuencia de comandos firepower.py, que indica la secuencia de comandos que se debe ejecutar en modo de automatización. Puede encontrar más información sobre esto en la sección específica del script.
11. El comando **&** indica a todo este comando que se ejecute en segundo plano, lo que permite al usuario seguir interactuando con su shell mientras se ejecuta el script.

Nota: El indicador -k es necesario para cualquier versión de FMC anterior a la 6.4 y para cualquier versión de FTD anterior a la 6.7, ya que los dispositivos Firepower no confiaban en el certificado raíz utilizado por CXD hasta la versión 6.4 de FMC y la versión 6.7 de FTD, esto hace que falle la verificación del certificado.

Script Firepower.py

El objetivo principal de la secuencia de comandos es generar y cargar un paquete de diagnóstico desde el dispositivo Secure Firewall denominado "solución de problemas". Para generar este archivo de solución de problemas, el script firepower.py simplemente llama al script sf_Troubleshoot.pl integrado que es responsable de crear este paquete. Este es el mismo script al que se llama cuando generamos un troubleshooting desde la GUI. Además del archivo de solución de problemas, el script también tiene la capacidad de recopilar otros datos de diagnóstico que no se incluyen como parte del paquete de solución de problemas. Actualmente, los únicos datos adicionales que se pueden recopilar son los archivos principales, pero se pueden ampliar en el futuro si surge la necesidad. El script se puede ejecutar en modo "Automatización" o "Interactivo":

Automatización

Este modo se habilita cuando utilizamos la opción "—auto-upload" cuando ejecutamos el script. Esta opción desactiva los mensajes interactivos, activa la recopilación de archivos principales y carga automáticamente los datos en el caso. El comando de una línea generado por el correo electrónico automatizado incluye la opción "-carga automática".

Interactivo

Este es el modo de ejecución predeterminado para el script. En este modo, el usuario recibe indicaciones para confirmar si se recopilan o no datos de diagnóstico adicionales, como archivos de núcleo. Independientemente del modo de ejecución, los resultados significativos se imprimen en la pantalla y se registran en un archivo de registro para indicar el progreso de la ejecución de las secuencias de comandos. El script en sí está ampliamente documentado a través de comentarios de código en línea y se puede descargar / revisar en https://cxd.cisco.com/public/ctfr/firepower.py.

Resultado esperado del script

A continuación se muestra un ejemplo de una ejecución correcta del 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!
```

Tenga en cuenta que este ejemplo de salida incluye cargas de archivos de núcleo. Si no hay archivos de núcleo presentes en su dispositivo, un mensaje "No core files found. Skipping core file processing" se presenta en su lugar.

Problemas comunes

Estos son algunos problemas comunes que puede experimentar (en orden de proceso / ejecución):

Seguridad del correo electrónico/reescritura de URL

A menudo, se observa que el usuario final tiene algún nivel de seguridad de correo electrónico que reescribe la URL. Esto altera el comando de una línea que se genera como parte del correo electrónico automatizado. Esto provoca un error de ejecución, ya que la URL para extraer el script se ha reescrito y no es válida. Aquí hay un ejemplo del comando esperado de una línea:

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

Pasos a resolver

Si la URL en el comando del correo electrónico no es "https://cxd.cisco.com/public/ctfr/firepower.py", es probable que la URL se haya reescrito en tránsito. Para solucionar este problema, simplemente reemplace la URL antes de ejecutar el comando.

Falla de DNS

Este error curl se ve a menudo cuando el dispositivo no puede resolver la URL para descargar el script:

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

Pasos a resolver

Para solucionar este problema, compruebe la configuración de DNS en el dispositivo para asegurarse de que puede resolver la URL correctamente para continuar.

Error al abrir/crear el archivo de registro

Una de las primeras cosas que la secuencia de comandos intenta hacer es crear (o abrir, si ya existe) un archivo de registro denominado **first-responder.log** en el directorio de trabajo actual. Si esta operación falla, se muestra un error que indica un simple problema de permiso:

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

Como parte de esta operación, todos los demás errores se identifican e imprimen en pantalla en este formato:

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

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

Pasos a resolver

Para corregir este error, simplemente ejecute el script como un usuario administrativo como "admin" o "root".

Error al abrir/escribir el archivo de notificación

Como parte de la ejecución de la secuencia de comandos, se crea un archivo de 0 bytes denominado "first_responder_notify" en el sistema. Este archivo se carga en el caso como parte de la automatización de este programa. Este archivo se escribe en el directorio "/var/common". Si el usuario que ejecuta la secuencia de comandos no tiene permisos suficientes para escribir archivos en este directorio, la secuencia de comandos mostrará el error:

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

Pasos a resolver

Para corregir este error, simplemente ejecute el script como un usuario administrativo como "admin" o "root".

> **Nota:** Si se encuentra un error no relacionado con permisos, se imprime un error de captura de todo en la pantalla "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". El cuerpo completo de la excepción se puede encontrar en el archivo **first-responder.log** .

Error al bloquear el archivo sf_Troubleshoot.pid

Para asegurarse de que sólo se ejecuta un proceso de generación de problemas a la vez, la secuencia de comandos de generación de problemas intenta bloquear el archivo /var/sf/run/sf_troubleshoot.pid antes de continuar. Si la secuencia de comandos no bloquea el archivo, se muestra un error:

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

Pasos a resolver

La mayor parte del tiempo, este error significa que una tarea independiente de generación de solución de problemas ya está en proceso. A veces, esto es el resultado de usuarios que accidentalmente ejecutan el comando de una línea dos veces seguidas. Para solucionar este problema, espere a que finalice el trabajo de generación de problemas actual e inténtelo de nuevo más tarde.

> **Nota:** Si se produce un error dentro de la secuencia de comandos sf_troubleshoot.pl, este error se muestra en la pantalla **"Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error".** El cuerpo completo de la excepción se puede encontrar en el archivo **first-responder.log** .

Problemas de carga

Hay una función de carga común en el script que es responsable de todas las cargas de archivos a lo largo de la ejecución de scripts. Esta función es simplemente un contenedor de Python para ejecutar un comando curl upload para enviar los archivos al caso. Debido a esto, cualquier error encontrado durante la ejecución, devuelve un código de error curl. En caso de que se produzca un error en la carga, se muestra este error en la pantalla:

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

Verifique el archivo **first-responder.log** para ver el error completo. Normalmente, el archivo first-responder.log tiene el siguiente aspecto:

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

Pasos a resolver

En este caso, curl devolvió un estado de salida de **6** , que significa **"No se pudo resolver el host "**. Esto es una falla simple de DNS mientras intentamos resolver el nombre de host **cxd.cisco.com** . Consulte la documentación de curl para decodificar cualquier estado de salida desconocido.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).