了解First Responder计划（安全防火墙版）

目录

简介

本文档介绍思科安全防火墙的第一个响应程序计划的使用和实施。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档基于思科安全防火墙产品。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

First Responder计划由TAC创建，旨在使为未决案例提供诊断数据更轻松、更快速。该计划由两个主要部分组成：

自动化电子邮件

此电子邮件在案例开始时发出，说明如何收集和上传诊断数据以进行TAC分析。有多种技术可以利用此系统，并且每封电子邮件都映射到创建案例时所选择的“技术”和“子技术”。

脚本/命令

First Responder计划的每个实施都有自己的独特方式处理数据的收集和交付。安全防火墙实施利用TAC编写的firepower.py Python脚本完成此任务。自动电子邮件过程会生成一个单行命令，该命令对于此特定情况是唯一的，可以复制并粘贴到安全防火墙设备的CLI中运行。

此电子邮件的原因

为第一个响应程序启用某些技术。这意味着，每次针对其中一种已启用技术创建案例时，系统会发出第一个响应者电子邮件。如果您收到第一响应者电子邮件且认为数据请求不相关，请忽略通信。

对于安全防火墙使用案例，第一个响应程序仅限于Firepower威胁防御(FTD)软件。如果运行自适应安全设备(ASA)代码库，请忽略此电子邮件。由于这两个产品在同一硬件上运行，通常观察到在安全防火墙技术空间中创建ASA案例，从而生成第一个响应方电子邮件。

自动化电子邮件

下面是作为此程序的一部分发出的自动化电子邮件的示例：

```
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
```

第一响应者程序的自动电子邮件被分为两个部分，称为引入块(introduction block)和数据请求块(data request block)。

介绍块

introduction block是包含在每个第一个响应者电子邮件中的静态字符串。此介绍句仅用于提供数据请求块的上下文。 以下是介绍块的示例：

```
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:
```

数据请求块

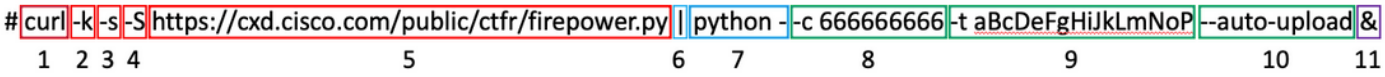
数据请求块是第一个响应程序的核心。每个数据块都是为特定技术收集数据的一组预定义步骤。如**背景信息**部分所述，每个数据请求块都映射到特定技术。选择此项技术来打开支持案例。通常，自动电子邮件中包含一个数据请求块。但是，如果所选技术有多个数据请求块映射到它，则多个数据请求将包含在电子邮件中。以下是包含多个数据请求的数据请求块的示例格式：

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

例如，对于安全防火墙，当提出请求以请求获得有关远程访问VPN(RA-VPN)的Firepower威胁防御(FTD)问题的帮助时，通常包含多个数据请求块，因为VPN技术还配置有映射数据请求块以帮助收集DART捆绑包。

生成的命令

具体来说，对于Secure Firewall使用案例，系统将为每个案例生成唯一的一行命令，作为自动电子邮件的一部分。以下是单行命令结构的明细：



1. curl命令用于下载最新版本的firepower.py脚本
2. **-k**标志是用于在连接期间忽略证书错误的选项。
3. **-s**标志是一个选项，用于在silent模式下运行curl。这用于抑制正常卷曲输出，因为它有噪声。
4. **-S**标志是curl显示错误的选项。这用于强制卷曲在启用silent选项的情况下仍显示输出错误。
5. 托管最新版本的firepower.py脚本的URL。此路径指示curl命令提取要运行的最新脚本正文。
6. 这是Linux管道，它将curl命令的输出（python脚本的内容）传递到下一步中的执行语句。
7. 在此步骤中，使用额外的“ — ”调用设备上的python二进制。 这指示python从stdin获取源（因为脚本的内容从curl通过管道传输）。
8. **-c**标志是firepower.py脚本的一个输入参数，它指示数据必须上载到的案例编号。此666666666项后的值是示例案例编号。
9. **-t**标志是firepower.py脚本的一个输入参数，它表示为此特定案例生成的唯一令牌（密码）。此选项后面的aBcDeFgHiJkLmNoP值是此情况的示例令牌。
10. **—auto-upload**标志是firepower.py脚本的一个特殊参数，它指示脚本在自动化模式下运行。有关此主题的详细信息，请参阅脚本特定部分。
11. **&**指示此整个命令在后台运行，这允许用户在脚本执行时继续与其外壳交互。

注意：对于6.4之前的任何FMC版本和6.7之前的任何FTD版本，都需要 — k标志，因为CXD使用的根证书在FMC 6.4和FTD 6.7之前不受Firepower设备信任，这会导致证书验证失败。

Firepower.py脚本

该脚本的主要目标是从安全防火墙设备生成并上传诊断捆绑包，称为“故障排除”。 要生成此故障排除文件，firepower.py脚本只需调用负责生成此捆绑的内置sf_troubleshoot.pl脚本。此脚本与从GUI生成故障排除时调用的脚本相同。除了故障排除文件，脚本还能够收集未包含在故障排除捆绑包中的其他诊断数据。目前，可以收集到的唯一额外数据是Core Files，但将来需要时可以展开该数据。脚本可以在“自动化”或“交互”模式下运行：

自动化

当我们运行脚本时，使用“ — auto-upload”选项时，会启用此模式。此选项禁用交互式提示，启用核心文件收集，并自动将数据上传到案例。自动电子邮件生成的单行命令包括“ — auto-upload”选项。

互动

这是脚本的默认运行模式。在此模式下，用户会收到确认是否收集其他诊断数据（如核心文件）的提示。无论执行模式如何，有意义的输出都会打印到屏幕上，并记录到日志文件中，以指示脚本执

行的进度。脚本本身通过内联代码注释进行了大量记录，并可在 https://cxd.cisco.com/public/ctfr/firepower.py下载/查看。

脚本的预期输出

以下是成功执行脚本的示例：

```
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!
```

请注意，此输出示例包括核心文件上传。如果设备上不存在核心文件，则会显示一条消息 "No core files found. Skipping core file processing" 的示例。

常见问题

以下是您可以遇到的一些常见问题（按流程/执行的顺序）：

电子邮件安全/URL重写

通常，人们会观察到最终用户具有某种级别的电子邮件安全性，可以重写URL。这将更改作为自动化电子邮件的一部分生成的单行命令。这会导致执行失败，因为用于提取脚本的URL已被重写，并且无效。以下是预期的一行命令的示例：

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

解决步骤

如果电子邮件命令中的URL不是“https://cxd.cisco.com/public/ctfr/firepower.py”，则该URL可能在传输过程中被重写。要解决此问题，只需在运行命令之前替换URL。

DNS故障

当设备无法解析URL以下载脚本时，经常出现此curl错误：

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

解决步骤

要解决此问题，请检查设备上的DNS设置，以确保能够正确解析URL以继续。

打开/创建日志文件失败

脚本尝试执行的第一个操作之一是在当前工作目录中创建名为first-responder.log的日志文件（如果该文件已存在，请将其打开）。如果此操作失败，则会显示指示简单权限问题的错误：

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

作为此操作的一部分，所有其他错误均会按以下格式标识并打印到屏幕上：

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

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

解决步骤

要解决此错误，只需以管理用户（如“admin”或“root”）身份运行脚本。

打开/写入通知文件失败

作为脚本执行的一部分，将在系统上创建名为“first_responder_notify”的0字节文件。然后，此文件作为此程序自动化的一部分上传到案例。此文件被写入“/var/common”目录。如果执行脚本的用户没有足够的权限将文件写入此目录，则脚本将显示错误：

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

解决步骤

要解决此错误，只需以管理用户（如“admin”或“root”）身份运行脚本。

> **注意：**如果遇到与权限无关的错误，屏幕上将显示一条全捕获错误 "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error".可以在first-responder.log中找到完整的异常正文。

锁定sf_troubleshoot.pid文件失败

为确保每次只运行一个故障排除生成过程，故障排除生成脚本会尝试在继续之前锁定/var/sf/run/sf_troubleshoot.pid文件。如果脚本无法锁定文件，则会显示错误：

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

解决步骤

在大多数情况下，此错误表示单独的故障排除生成任务已在进行中。有时，这是用户意外连续两次执行单行命令的结果。要解决此问题，请等待当前故障排除生成作业完成，然后重试。

> **注意**：如果sf_troubleshoot.pl脚本本身发生错误，则此错误将显示在屏幕上 "Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error". 可以在first-responder.log中找到完整的异常正文。

上传问题

脚本中有一个通用的上载函数，负责在整个脚本执行过程中上载所有文件。此功能只是一个python包装程序，用于执行curl上传命令以将文件发送到案例。因此，在执行期间遇到的任何错误都会返回为curl错误代码。如果上传失败，则此错误显示在屏幕上：

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

检查first-responder.log文件以查看完整错误。通常，first-responder.log文件如下所示：

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

解决步骤

在这种情况下，curl返回退出状态为6，意*味着*"无法解析主机"。 尝试解析主机名cxd.cisco.com时，这是一个简单的DNS故障。请参阅curl文档以解码任何未知退出状态。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。