First Responder Program(Secure Firewall Edition)について

内容

概要

このドキュメントでは、Cisco Secure FirewallのFirst Responder Programの使用と実装について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントは、Cisco Secure Firewall製品に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

First Responderプログラムは、オープンケースの診断データを簡単かつ迅速に提供できるように、TACによって作成されました。プログラムを構成する主なコンポーネントは2つあります。

自動Eメール

この電子メールは、TAC分析のための診断データを収集してアップロードする方法に関する指示とともに、ケースの開始時に送信されます。このシステムを活用するテクノロジーは複数あり、各メールは、ケースの作成時に選択される「テクノロジー」と「サブテクノロジー」にマッピングされます。

スクリプト/コマンド

First Responderプログラムの各実装には、データの収集と配信を処理するための独自の方法があります。Secure Firewallの実装では、TACが作成したfirepower.py Pythonスクリプトを使用してこれを実現します。自動化されたEメールプロセスは、この特定のケースに固有の1行のコマンドを生成します。このコマンドは、実行するSecure FirewallデバイスのCLIにコピーして貼り付けることができます。

この電子メールの理由

最初のレスポンダプログラムで有効になる特定のテクノロジーがあります。つまり、これらの有効なテクノロジーのいずれかに対してケースがオープンされるたびに、最初の応答者の電子メールが送信されます。最初の応答者の電子メールを受信し、データ要求が関連していると思わない場合は、連絡を無視してください。

セキュアファイアウォールの使用例では、最初のレスポンダプログラムはFirepower Threat Defense(FTD)ソフトウェアに限定されます。適応型セキュリティアプライアンス(ASA)のコードベースを実行している場合は、この電子メールを無視してください。これら2つの製品は同じハードウェア上で動作するため、ASAケースは最初の応答側の電子メールを生成するセキュアファイアウォールテクノロジーの領域で作成されることが一般的に観察されます。

自動Eメール

このプログラムの一部として送信される自動化された電子メールの例を次に示します。

```
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
```

最初のレスポンダプログラムの自動化された電子メールは、導入ブロックとデータ要求ブロックと呼ばれる2つの部分に分割されます。

概要ブロック

イントロダクションブロックは、すべての最初の応答側の電子メールに含まれる静的な文字列です。この導入文は、データ要求ブロックにコンテキストを提供するだけです。 次に、導入ブロックの例を示します。

```
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:
```

データ要求ブロック

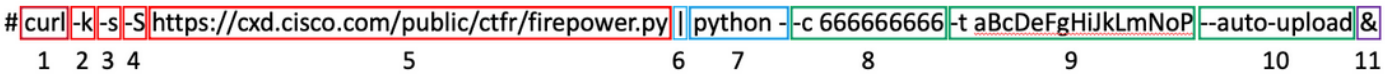
データ要求ブロックは、最初のレスポンダプログラムの中心です。各ブロックは、特定のテクノロジーのデータを収集するための定義済みの一連の手順です。「**背景説明**」セクションで説明したように、各データ要求ブロックは特定のテクノロジーにマッピングされます。これは、サポート・リクエストをオープンするために選択したテクノロジーと同じです。通常、自動化された電子メールには、1つのデータ要求ブロックが含まれています。ただし、選択したテクノロジーに複数のデータ要求ブロックがマッピングされている場合は、複数のデータ要求が電子メールに含まれます。複数のデータ要求を含むデータ要求ブロックのフォーマット例を次に示します。

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

たとえば、セキュアファイアウォールの場合、Firepower Threat Defense(FTD)のリモートアクセスVPN(RA-VPN)の問題に関する支援を求める要求が発行されたときに、複数のデータ要求ブロックが含まれることがよくあります。これは、VPNテクノロジーにも、DARTバンドルを収集するための支援を求めるマッピングされたデータ要求ブロックが設定されているためです。

生成されたコマンド

セキュアファイアウォールの使用例では、自動化された電子メールの一部として、ケースごとに一意の1行のコマンドが生成されます。次に、1行コマンドの構造を詳しく説明します。



1. curlコマンドは、firepower.pyスクリプトの最新バージョンをダウンロードするために使用されます
2. **-k**フラグは、接続時に証明書エラーを無視するcurlのオプションです。
3. **-s**フラグは、カールをサイレントモードで実行するためのオプションです。ノイズが多いため、通常のカール出力を抑制するために使用します。
4. **-S**フラグは、カールでエラーを表示するためのオプションです。これは、silentオプションを有効にしても出力エラーが表示されるようにcurlを強制するために使用されます。
5. 最新バージョンのfirepower.pyスクリプトがホストされているURL。このパスは、実行するスクリプトの最新の本文を取得するようにcurlコマンドに指示します。
6. これはLinuxパイプで、curlコマンド（Pythonスクリプトの内容）の出力を次のステップの実行ステートメントに渡します。
7. このステップでは、デバイス上のpythonバイナリが追加の「 – 」を付けて呼び出されます。これは、ソースがstdinから取得されることをpythonに指示します（スクリプトの内容はcurlからパイプ処理されるため）。
8. **-c**フラグは、データをアップロードする必要があるケース番号を示すfirepower.pyスクリプトの入力引数です。このオ666666666ションの後のデフォルト値は、ケース番号の例です。
9. **-t**フラグはfirepower.pyスクリプトの入力引数で、この特定のケースに対して生成された一意のトークン（パスワード）を示します。このオプションの後のaBcDeFgHiJkLmNoP値は、この場合のトークンの例です。
10. **—auto-upload**フラグはfirepower.pyスクリプトの特別な引数で、スクリプトをオートメー

ションモードで実行することを示します。詳細については、スクリプト固有のセクションを参照してください。

11. &は、このコマンド全体をバックグラウンドで実行するように指示します。これにより、ユーザはスクリプトの実行中もシェルとの対話を継続できます。

注：CXDで使用されるルート証明書はFMCバージョン6.4およびFTDバージョン6.7までFirepowerデバイスによって信頼されなかったため、6.4より前のFMCバージョンおよび6.7より前のFTDバージョンには – kフラグが必要です。これは、証明書の検証が失敗する原因になります。

Firepower.pyスクリプト

スクリプトの主な目的は、「トラブルシューティング」と呼ばれるセキュアファイアウォールデバイスから診断バンドルを生成してアップロードすることです。 このトラブルシューティングファイルを生成するために、firepower.pyスクリプトは、このバンドルの構築を担当する組み込みのsf_troubleshoot.plスクリプトを呼び出します。これは、GUIからトラブルシューティングを生成するときに呼び出されるスクリプトと同じです。トラブルシューティングファイルに加えて、スクリプトはトラブルシューティングバンドルの一部として含まれていない他の診断データを収集することもできます。現在、収集できる追加データはコアファイルのみですが、必要に応じて将来的に拡張できます。スクリプトは、「Automation」または「Interactive」モードで実行できます。

自動化

このモードは、スクリプトの実行時に「 – auto-upload」オプションを使用すると有効になります。このオプションは、対話型プロンプトを無効にし、コアファイルの収集を有効にし、ケースにデータを自動的にアップロードします。自動メールによって生成される1行のコマンドには、「 – auto-upload」オプションが含まれています。

対話型

これは、スクリプトのデフォルトの実行モードです。このモードでは、コアファイルなどの追加の診断データを収集するかどうかを確認するプロンプトが表示されます。実行モードに関係なく、意味のある出力が画面に出力され、スクリプト実行の進行状況を示すログファイルに記録されます。スクリプト自体は、インラインコードコメントによって詳細に文書化されており、https://cxd.cisco.com/public/ctfr/firepower.pyでダウンロードまたは確認できます。

スクリプトの予想される出力

スクリプトの実行が成功した例を次に示します。

```
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!
```

この出力例には、コアファイルのアップロードが含まれることに注意してください。デバイスにコアファイルがない場合は、メッセージが表示されます "No core files found. Skipping core file processing" が表示されます。

一般的な問題

次に、発生する可能性のある一般的な問題を（プロセス/実行順に）示します。

電子メールセキュリティ/URLの書き換え

多くの場合、エンドユーザがURLを書き換えるEメールセキュリティのレベルを持っていることが確認されます。これにより、自動電子メールの一部として生成される1行のコマンドが変更されます。スクリプトをプルするURLが書き換えられ、無効なため、実行が失敗します。次に、予想される1行コマンドの例を示します。

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

問題解決の手順

電子メールからのコマンドのURLが「https://cxd.cisco.com/public/ctfr/firepower.py」以外の場合、URLは送信中に書き換えられた可能性があります。この問題を解決するには、コマンドを実行する前にURLを置き換えます。

DNS障害

このcurl工ラーは、スクリプトをダウンロードするURLをデバイスが解決できない場合によく発生します。

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

問題解決の手順

この問題を解決するには、デバイスのDNS設定を確認し、URLを正しく解決して続行できることを確認してください。

ログファイルを開く/作成できない

スクリプトが最初に試みることの1つは、現在の作業ディレクトリにfirst-responder.logという名前の口グファイルを作成する（または既存の場合は開く）ことです。この操作が失敗すると、単

純な権限の問題を示すエラーが表示されます。

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

この操作の一部として、他のすべてのエラーが識別され、次の形式で画面に出力されます。

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




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

問題解決の手順

このエラーを修正するには、「admin」や「root」などの管理ユーザとしてスクリプトを実行します。

通知ファイルを開く/書き込みできない

スクリプト実行の一環として、「first_responder_notify」という名前の0バイトのファイルがシステム上に作成されます。このファイルは、このプログラムの自動化の一環としてケースにアップロードされます。このファイルは「/var/common」ディレクトリに書き込まれます。スクリプトを実行するユーザに、このディレクトリにファイルを書き込むための十分な権限がない場合、スクリプトは次のエラーを表示します。

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

問題解決の手順

このエラーを修正するには、「admin」や「root」などの管理ユーザとしてスクリプトを実行します。

> **注：**権限に関連しないエラーが発生すると、画面にcatch-allエラーが表示されます "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error".例外の完全な本文は、first-responder.logにあります。

sf_troubleshoot.pidファイルをロックできない

一度に1つのトラブルシューティング生成プロセスだけが実行されるように、トラブルシューティング生成スクリプトは処理を進める前に/var/sf/run/sf_troubleshoot.pidファイルをロックしようとします。スクリプトがファイルのロックに失敗すると、エラーが表示されます。

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

問題解決の手順

ほとんどの場合、このエラーは、別のトラブルシューティング生成タスクがすでに実行中であることを意味します。これは、ユーザが誤って1行のコマンドを連続して2回実行した結果である場合があります。この問題を解決するには、現在のトラブルシューティング生成ジョブが終了するのを待って、後でもう一度やり直します。

> **注**：sf_troubleshoot.plスクリプト自体でエラーが発生すると、このエラーが画面に表示されます 「」Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error". 例外の完全な本文は、first-responder.logにあります。

アップロードの問題

スクリプトには、スクリプトの実行中のすべてのファイルアップロードを担当する共通のアップロード機能があります。この関数は、curl uploadコマンドを実行してファイルをケースに送信するためのPythonラッパーです。このため、実行中に発生したエラーはcurlエラーコードとして返されます。アップロードに失敗した場合、次のエラーが画面に表示されます。

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

first-responder.logファイルを調べて、完全なエラーを確認します。通常、first-responder.logファイルは次のようになります。

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

問題解決の手順

この場合、curlは終了ステータス6を返しました。これは、「Could not resolve host 」を意味します。 これは、ホスト名cxd.cisco.com を解決しようとする際の単純なDNS障害です。不明な終了ステータスをデコードするには、curlドキュメントを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。