First Responder Program(Secure Firewall Edition) 이해

목차

소개

이 문서에서는 Cisco Secure Firewall용 First Responder 프로그램의 사용 및 구현에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 Cisco Secure Firewall 제품을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

First Responder 프로그램은 공개된 사례에 대한 진단 데이터를 보다 쉽고 빠르게 제공하기 위해 TAC에서 만들었습니다. 프로그램을 구성하는 두 가지 주요 구성 요소가 있습니다.

자동화된 이메일

이 이메일은 케이스 시작 시 TAC 분석을 위해 진단 데이터를 수집하고 업로드하는 방법에 대한 지침과 함께 발송됩니다. 이 시스템을 활용하는 기술은 여러 가지가 있으며 각 이메일은 케이스가 생성될 때 선택한 "기술"과 "하위 기술"에 매핑됩니다.

스크립트 / 명령

First Responder 프로그램의 각 구현에는 데이터 수집 및 전달을 처리하는 고유한 방법이 있습니다. Secure Firewall 구현에서는 TAC에서 제작한 firepower.py Python 스크립트를 활용하여 이를 구현합니다. 자동화된 이메일 프로세스는 이 특정 경우에 고유한 한 줄 명령을 생성하며, 이 명령을 복사하여 Secure Firewall 디바이스의 CLI에 붙여 넣어 실행할 수 있습니다.

이 이메일의 이유

첫 번째 responder 프로그램에 대해 활성화된 특정 기술이 있습니다. 즉, 이러한 활성화된 기술 중 하나에 대해 케이스를 열 때마다 첫 번째 응답자 이메일이 전송됩니다. 첫 번째 응답자 이메일을 받고 데이터 요청이 적절하다고 생각하지 않는 경우, 언제든지 통신을 무시하십시오.

Secure Firewall 활용 사례의 경우 첫 번째 responder 프로그램은 FTD(Firepower Threat Defense) 소프트웨어로 제한됩니다. ASA(Adaptive Security Appliance) 코드베이스를 실행하는 경우 이 이메일을 무시하십시오. 이 두 제품은 동일한 하드웨어에서 실행되므로 일반적으로 Secure Firewall 기술 영역에서 ASA 사례가 생성되어 첫 번째 응답자 이메일이 생성됩니다.

자동화된 이메일

다음은 이 프로그램의 일부로 전송되는 자동화된 전자 메일의 예입니다.

```
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
```

제1 응답자 프로그램에 대한 자동화된 이메일은 소개 블록 및 데이터 요청 블록이라고 알려진 2개의 부분으로 분할된다.

소개 블록

소개 블록은 모든 첫 번째 응답자 이메일에 포함된 정적 문자열입니다. 이 소개 문장은 단순히 데이터 요청 블록(들)에 컨텍스트를 제공하는 역할을 한다. 소개 블록의 예는 다음과 같습니다.

```
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:
```

데이터 요청 블록

상기 데이터 요청 블록들은 상기 제1 responder 프로그램의 심부이다. 각 블록은 특정 기술에 대한 데이터를 수집하기 위해 미리 정의된 일련의 단계입니다. Background Information 섹션에서 **언급한** 바와 같이 각 데이터 요청 블록은 특정 기술에 매핑됩니다. 지원 사례를 열기 위해 선택한 기술과 동일합니다. 일반적으로 자동 전자 메일에는 단일 데이터 요청 블록이 포함됩니다. 그러나 선택한 기

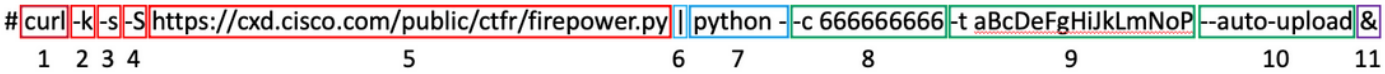
술에 둘 이상의 데이터 요청 블록이 매핑되어 있으면 여러 데이터 요청이 전자 메일에 포함됩니다. 다음은 여러 데이터 요청이 있는 데이터 요청 블록의 예제 형식입니다.

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

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

예를 들어 보안 방화벽의 경우 VPN 기술에 DART 번들 수집을 지원하도록 구성된 매핑된 데이터 요청 블록이 있으므로 FTD(Firepower Threat Defense)에서 RA-VPN(Remote Access VPN) 문제에 대한 지원을 요청하는 경우 여러 데이터 요청 블록이 포함되는 경우가 많습니다.

생성된 명령

특히 Secure Firewall 활용 사례의 경우 자동화된 이메일의 일부로 각 사례에 대해 고유한 한 줄 명령이 생성됩니다. 다음은 1회선 명령의 구조를 분석한 내용입니다.



1. curl 명령은 최신 버전의 firepower.py 스크립트를 다운로드하는 데 사용됩니다
2. **-k 플래그**는 연결 중에 인증서 오류를 무시하기 위한 curl 옵션입니다.
3. **-s 플래그**는 curl을 무음 모드로 실행하는 옵션입니다. 이는 잡음이 있을 때 정상적인 컬 출력을 억제하기 위해 사용된다.
4. **-S 플래그**는 curl을 사용하여 오류를 표시하는 옵션입니다. 이 옵션은 silent 옵션이 활성화된 경우에도 curl이 출력 오류를 표시하도록 강제 조정하는 데 사용됩니다.
5. 최신 버전의 firepower.py 스크립트가 호스팅되는 URL입니다. 이 경로는 curl 명령에 실행할 스크립트의 최신 본문을 가져오도록 지시합니다.
6. Linux 파이프로, 다음 단계에서 curl 명령의 출력(python 스크립트의 내용)을 실행 문으로 전달합니다.
7. 이 단계에서는 추가 "-"를 사용하여 디바이스의 python 이진을 호출합니다. 이렇게 하면 스크립트의 내용이 curl에서 파이핑되므로 소스가 stdin에서 가져온다는 것을 python에 지시합니다.
8. **-c 플래그**는 데이터를 업로드해야 하는 사례 번호를 나타내는 firepower.py 스크립트의 입력 인수입니다. 이 옵션 뒤의 666666666 값은 예제 케이스 번호입니다.
9. **-t 플래그**는 firepower.py 스크립트의 입력 인수로, 이 특정 경우에 대해 생성된 고유한 토큰(비밀번호)을 나타냅니다. 이 옵션 뒤의 aBcDeFgHiJkLmNoP 값은 이 경우에 대한 예제 토큰입니다.
10. —**auto-upload 플래그**는 자동화 모드에서 실행할 스크립트를 나타내는 firepower.py 스크립트의 특수 인수입니다. 이에 대한 자세한 내용은 스크립트 관련 섹션에서 확인할 수 있습니다.
11. 및 **은** 이 전체 명령이 백그라운드에서 실행되도록 명령하므로 사용자는 스크립트가 실행되는 동안 셸과 계속 상호 작용할 수 있습니다.

참고: CXD에서 사용하는 루트 인증서는 FMC 버전 6.4 및 FTD 버전 6.7까지 Firepower 디바이스에서 신뢰하지 않았기 때문에 6.4 이전의 모든 FMC 버전 및 6.7 이전의 모든 FTD 버전에는 -k 플래그가 필요합니다.

Firepower.py 스크립트

스크립트의 주요 목표는 "문제 해결"이라고 하는 보안 방화벽 디바이스에서 진단 번들을 생성하고 업로드하는 것입니다. 이 문제 해결 파일을 생성하기 위해 firepower.py 스크립트는 이 번들을 작성하는 기본 제공 sf_troubleshoot.pl 스크립트를 호출합니다. 이 스크립트는 GUI에서 문제 해결을 생성할 때 호출되는 스크립트와 동일합니다. 스크립트에는 문제 해결 파일 외에도 문제 해결 번들의 일부로 포함되지 않은 다른 진단 데이터를 수집할 수 있는 기능도 있습니다. 현재 수집할 수 있는 추가 데이터는 Core Files뿐이지만, 나중에 필요할 경우 이를 확대할 수 있습니다. 스크립트는 "자동화" 또는 "대화형" 모드에서 실행할 수 있습니다.

자동화

이 모드는 스크립트를 실행할 때 "—auto-upload" 옵션을 사용할 때 활성화됩니다. 이 옵션은 대화형 프롬프트를 비활성화하고, 핵심 파일 수집을 활성화하며, 케이스에 데이터를 자동으로 업로드합니다. 자동 전자 메일에 의해 생성되는 한 줄 명령에는 "—auto-upload" 옵션이 포함됩니다.

대화형

스크립트의 기본 실행 모드입니다. 이 모드에서는 사용자가 코어 파일과 같은 추가 진단 데이터를 수집할지 여부를 확인하는 프롬프트를 수신합니다. 실행 모드에 관계없이 의미 있는 출력이 화면에 인쇄되고 로그 파일에 기록되어 스크립트 실행의 진행 상황을 나타냅니다. 스크립트 자체는 인라인 코드 주석을 통해 폭넓게 문서화되며 https://cxd.cisco.com/public/ctfr/firepower.py에서 다운로드/검토할 수 있습니다.

스크립트의 예상 출력

다음은 스크립트를 성공적으로 실행한 예입니다.

```
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!
```

이 출력 예에는 코어 파일 업로드가 포함되어 있습니다. 디바이스에 코어 파일이 없는 경우 "No core files found. Skipping core file processing" 대신 표시됩니다.

일반적인 문제

다음은 (프로세스/실행 순서로) 발생할 수 있는 몇 가지 일반적인 문제입니다.

이메일 보안/URL 재작성

엔드 유저가 URL을 재작성하는 E-mail Security 수준이 있는 경우가 많습니다. 이렇게 하면 자동화된 전자 메일의 일부로 생성되는 한 줄 명령이 변경됩니다. 따라서 스크립트를 가져올 URL이 다시 작성되어 유효하지 않으므로 실행이 실패합니다. 다음은 예상되는 한 줄 명령의 예입니다.

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

해결 단계

전자 메일의 명령에 있는 URL이 "https://cxd.cisco.com/public/ctfr/firepower.py"이 아닌 경우 전송 중에 URL이 다시 작성되었을 가능성이 높습니다. 이 문제를 해결하려면 명령을 실행하기 전에 URL을 교체하기만 하면 됩니다.

DNS 실패

이 curl 오류는 디바이스에서 스크립트를 다운로드하기 위해 URL을 확인할 수 없는 경우 자주 나타납니다.

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

해결 단계

이 문제를 해결하려면 디바이스에서 DNS 설정을 확인하여 URL을 올바르게 확인할 수 있는지 확인하십시오.

로그 파일 열기/생성 실패

스크립트에서 가장 먼저 시도하는 작업 중 하나는 현재 작업 디렉토리에 first-responder.log라는 로그 파일을 만들거나 엽니다. 이 작업이 실패하면 단순 권한 문제를 나타내는 오류가 표시됩니다.

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

이 작업의 일부로 다른 모든 오류가 식별되어 다음 형식으로 화면에 출력됩니다.

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




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

해결 단계

이 오류를 해결하려면 "admin" 또는 "root"와 같은 관리 사용자로 스크립트를 실행하면 됩니다.

알림 파일 열기/쓰기 실패

스크립트 실행의 일부로 "first_responder_notify"라는 0바이트 파일이 시스템에 생성됩니다. 이 파일은 이 프로그램의 자동화의 일부로 케이스에 업로드됩니다. 이 파일은 "/var/common" 디렉토리에 기록됩니다. 스크립트를 실행하는 사용자에게 이 디렉터리에 파일을 쓸 수 있는 권한이 없으면 스크립트에 다음 오류가 표시됩니다.

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

해결 단계

이 오류를 해결하려면 "admin" 또는 "root"와 같은 관리 사용자로 스크립트를 실행하면 됩니다.

> **참고:** 비권한 관련 오류가 발생하면 화면에 모두 적용 오류가 출력됩니다 "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error". 전체 예외 본문은 first-responder.log에서 찾을 수 있습니다.

sf_troubleshoot.pid 파일 잠금 실패

한 번에 하나의 문제 해결 생성 프로세스만 실행되도록 하려면 문제 해결 생성 스크립트에서 계속 진행하기 전에 /var/sf/run/sf_troubleshoot.pid 파일을 잠급니다. 스크립트가 파일을 잠그지 못하면 다음 오류가 표시됩니다.

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

해결 단계

대부분의 경우 이 오류는 별도의 문제 해결 생성 작업이 이미 진행 중임을 의미합니다. 경우에 따라 사용자가 실수로 한 줄 명령을 두 번 연속으로 실행한 결과이기도 합니다. 이 문제를 해결하려면 현재 문제 해결 생성 작업이 완료될 때까지 기다린 후 나중에 다시 시도하십시오.

> **참고:** sf_troubleshoot.pl 스크립트 자체에 오류가 발생하면 이 오류가 화면에 표시됩니다 "Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error". 전체 예외 본문은 first-responder.log에서 찾을 수 있습니다.

업로드 문제

스크립트에는 스크립트를 실행하는 동안 모든 파일 업로드를 담당하는 공통 업로드 기능이 있습니다. 이 기능은 단순히 파일을 케이스에 보내기 위해 curl upload 명령을 실행하는 python 래퍼입니다. 따라서 실행 중에 발생한 오류는 curl 오류 코드로 반환됩니다. 업로드에 실패하는 경우 이 오류가 화면에 표시됩니다.

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

전체 오류를 보려면 first-responder.log 파일을 확인합니다. 일반적으로 first-responder.log 파일은 다음과 같습니다.

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

해결 단계

이 경우 curl은 종료 상태 6을 반환했으며, 이는 "Could not resolve host"를 의미합니다. 호스트 이름 cxd.cisco.com을 확인하려고 시도하는 동안 단순 DNS 오류입니다. 알 수 없는 종료 상태를 디코딩하려면 curl 문서를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.