Introduction

This document explains how to use BXACK. You will learn how to:

- Install prerequisites.
- How to use the tool

Prerequisites

The following python library are required for the tool to run:

- PyFPDF
- paramiko
- Datetime

Using pip install:

```
pip install fpdf
```

```
pip install paramiko
```

```
pip install Datetime
```

Running the tool

```
python program.py
```

Using BXAC

Main Menu:

```
Option A: Collect Cisco Forensic Evidence
Option B: Analyze Cisco Forensic Evidence
Option C: Compare Running-Config & Startup-Config
Please choose an option:
```

Option A: Collect Cisco Forensic Evidence

Step 1: After choosing option “A”, you will be required to enter the Cisco device’s IP address, Username, Password and enable password.

```
Option A: Collect Cisco Forensic Evidence
Option B: Analyze Cisco Forensic Evidence
Option C: Compare Running-Config & Startup-Config
Please choose an option: A
Remote Host: 192.168.133.120
Username: cisco
Password: cisco
Enable Password: cisco
```

Step 2: BXAC will now run a list of “show” commands. A txt file for each command will be created in the same directory as the tool. After all commands are executed a pdf file containing all the output will be created.

```
Executing show history all
Executing show clock detail
Executing show startup-config
Executing show reload
Executing show ip route
Executing show cdp nei detail
Executing show ip arp
Executing show ip interface
Executing show ip int brief
Executing show tcp brief all
Executing show sockets
Executing show ip cache flow
Executing show ip cef
Executing show logging
Executing show processes
Making PDF File Please wait.....
```

Option B: Analyze Cisco Forensic Evidence

Step 1: After choosing option “B”, you will be required to enter the path of the crashinfo file.

```
Option A: Collect Cisco Forensic Evidence
Option B: Analyze Cisco Forensic Evidence
Option C: Compare Running-Config & Startup-Config
Please choose an option: B
File-Path: C:\Users\acupo\Desktop\crash_IOSvL2\IOSVL2\corrupt_memory
```

Step 2: A menu list will appear and you are able to select the option.

```
======================================== Menu List ========================================
Option 1: Commands History
Option 2: Show start of Crash Info Collection
Option 3: Show Alignment
Option 4: Show Malloc and Free Traces
Option 5: Show Stack Trace
Option 6: Show Context
Option 7: Show Stack Dump
Option 8: Show process level info
Option 9: Show Interrupt Level Stack Dump
Option 10: Show Interrupt Stack
Option 11: Show Register Memory Dump
Option 12: Show chunk failures
Option 13: Exit
Choose an Option:
```

Option C: Compare Running-Config & Startup-Config

Step 1: After choosing option “C”, you will be required to enter the Cisco device’s IP address, Username, Password and enable password.

```
Option A: Collect Cisco Forensic Evidence
Option B: Analyze Cisco Forensic Evidence
Option C: Compare Running-Config & Startup-Config
Please choose an option: c
Remote Host: 192.168.133.120
Username: cisco
Password: cisco
Enable Password: cisco
Please wait while we are connecting you...
Executing show running-config
Executing show startup-config
```

Step 2: The output and the legends will be displayed.

```
- show startup-config
- Using 1876 out of 262144 bytes, uncompressed size = 3966 bytes
+
+ ACCESS#show running-config
+ Building configuration...
+
+ Current configuration : 3966 bytes
  !
- ! Last configuration change at 10:48:15 UTC Wed Oct 28 2020
?                               ^    ^^     ^^^     ^^

+ ! Last configuration change at 15:48:04 UTC Sat Oct 31 2020
?                               ^    ^^     ^^^     ^^

  !
  version 15.2
  service timestamps debug datetime msec
  service timestamps log datetime msec
  no service password-encryption
  service compress-config
  !
  hostname ACCESS
  !
  boot-start-marker
  boot-end-marker
```

```
====================== Legends ======================
? > Incremental Difference
+ > in running-config but not in startup-config
- > In startup-config but not in running-config
```