Challenge 1

Instructions

Pre-launch Training

Welcome prospective crew members! Before you are allowed to board the Dauntless, humanity's first faster-than-light capable ship, we must ensure that you are familiar with using all the mission critical systems on board. This simulation will allow you to experience a representative crisis situation, just like you might encounter in-orbit.

The challenges you might face in space are sure to be significantly more complex, but the steps to ensure that the ship's systems register your actions will be the same. Good luck!

NICE Work Roles:

Cyber Defense Forensic Analyst

NICE Tasks:

T0532 - Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.

Background

In this simulation, one of the systems onboard the ship has been damaged by a solar flare. You were able to recover an image from the malfunctioning thumb drive that was plugged into the system, as well as a secured backup file. The password to this file used to be on the thumb drive, but it looks like someone recently deleted it. You must use whatever means at your disposal to gain access to the activation code for this system.

Getting Started

Using the Kali machine, begin by mounting the image file. You must analyze the contents to find the first token. The https://challenge.us site will have the files you need to get started and help you along the way!

Challenge Questions

1. (40) What is the token found within the image file?

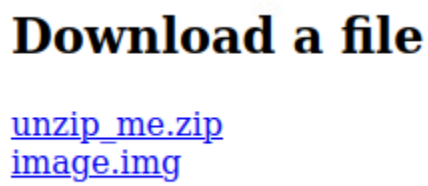
2. (40) What is the token found within the zip file?

3. (20) What is the token found on https://challenge.us

Writeup by Jonathan

After starting the provided Kali VM, the first step I took is visiting the provided URL httpx://challenge.us.

There were two files to download:



After downloading the two files, I attempted to open the .zip file and it was password protected. Before looking at the second .img file, I ran John against the hash of the zip file to see if I could crack it:

sudo zip2john unzip_me.zip > crack_zip

#john –wordlist=/usr/share/wordlists/rockyou.txt

While John was running, I moved the .img file into the mount directory under /mnt/img and used the following command to mount the image to my Kali machine:

#sudo mount -o loop image.img /mnt/img

The mounting command was successful and the files in the image are below:

There is a token within this image file so I began to search in the primary user's files:

```
┌──(user㉿training-simulation-kali)-[/mnt/img/home/user]
└─$ cd Documents

┌──(user㉿training-simulation-kali)-[/mnt/img/home/user/Documents]
└─$ ls
token.txt

┌──(user㉿training-simulation-kali)-[/mnt/img/home/user/Documents]
└─$ cat token.txt
Token 1: 54727a656369616b
```

Found the first token! I then checked on John's progress. The hash was not yet cracked so I thought there might be a password to the .zip file hidden within this disk image. I used grep to search for .txt and .zip extensions in the user's files:

```
┌──(user㉿training-simulation-kali)-[/mnt/img/home]
└─$ sudo grep -r ".*\.zip$"
grep: user/snap/snap-store/common/.cache/gnome-software/appstream/components.xmlb: binary file matches

┌──(user㉿training-simulation-kali)-[/mnt/img/home]
└─$ sudo grep -r ".*\.txt$"
grep: user/snap/snap-store/common/.cache/gnome-software/appstream/components.xmlb: binary file matches
grep: user/.local/share/gvfs-metadata/root: binary file matches
grep: user/.local/share/gvfs-metadata/home: binary file matches
grep: user/.local/share/gvfs-metadata/admin:: binary file matches
user/.local/share/Trash/info/password.txt.trashinfo:Path=/home/user/Desktop/password.txt
```

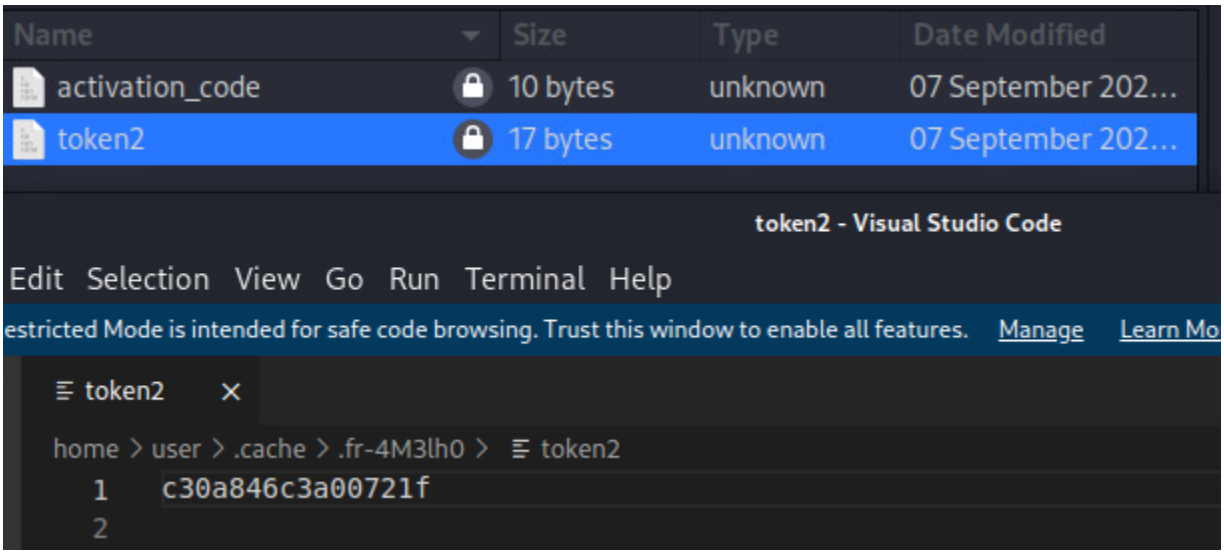
In the trash, there's a file called password.txt. I navigated to that file and there it was!

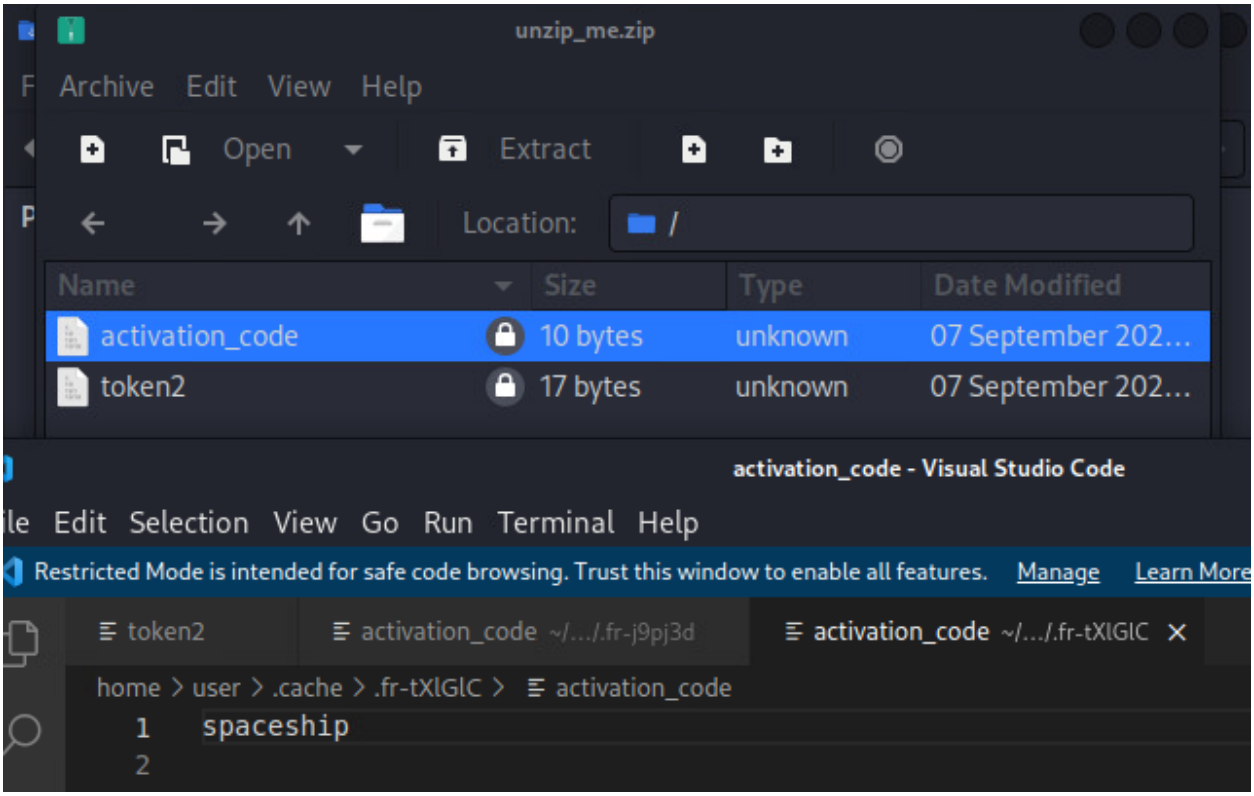
```
┌──(user㉿training-simulation-kali)-[/mnt/…/user/.local/share/Trash]
└─$ cd files

┌──(user㉿training-simulation-kali)-[/mnt/…/.local/share/Trash/files]
└─$ ls
password.txt

┌──(user㉿training-simulation-kali)-[/mnt/…/.local/share/Trash/files]
└─$ cat password.txt
Password: Dauntless
```

I used the password to open the zip file and it was a success! The second token was in the file labeled "token2"





The third challenge required that we get the token at httpx://challenge.us

Enter the text for each field

Enter the activation code:

spaceship

Submit

If this challenge has files to download, you can access them here

This code found in the zip file did not work, so I thought this code may call to the back-end database. I tested for SQL injection by inserting a ‘ in the text field:

Enter the text for each field

Enter the activation code:

'

Submit

If this challenge has files to download, you can access them here

For some reason, this was right!

Your challenge was graded

You submitted the last grade request at 09/07/2022 11:29:01

Enter the activation code:

Success -- You found the final token!

Token: ecdf471530354ea3

Re-Grade Challenge

Challenge 1 is therefore complete!