Mission Name

CameraForensics

History Background

Background for this chapter is Ethan got from the datacard, passwords, access codes and in particular some Skytech maps to look for his brother. In this case, there are security cameras installed inside Skytech and Claire has to analyse them.

Technical High-Level Overview

An IP Camera firmware is provided to the player, in order get which is the group ID of user who has the User ID 11 inside the Camera File System. Player must analyse the firmware provided.

Short Description

You´re going to analyse an IP camera Firmware. Your goal is to find out which is which is the default user password and the port which is used by camera to watch videos.

Mission Description

There are security cameras installed inside Skytech and Claire has to analyse them. Your goal is to find out which is the default user password and the port which is used by camera to watch videos. Please insert your finding as: password_port

Location

SYLVARCON | SKYTECH HQ

Tools

- binwalk

Questions

How many seconds the camera lasts to timeout?

- 1000

Which version of cam is?

- CAM3115

Which is the name of binary to use from Windows?

- IPCamera.exe

Items

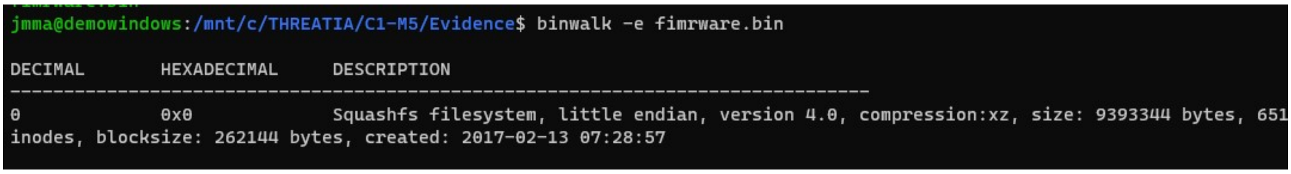
1. Check if the camera has any partition.
2. Use binwalk.
3. Analyse Squash File to locate the necessary files.

TECHNICAL INFORMATION

Write Up

Player must use binwalk to extact camera filesystem, launching the following command:

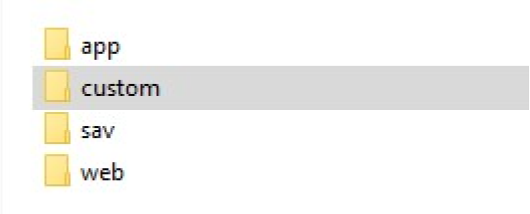
- Binwalk -eM "firmware provided"



```
jmma@demowindows:/mnt/c/THREATIA/C1-M5/Evidence$ binwalk -e fimrware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Squashfs filesystem, little endian, version 4.0, compression:xz, size: 9393344 bytes, 651
inodes, blocksize: 262144 bytes, created: 2017-02-13 07:28:57
```

Figure 1

Once firmware is extracted, player should analyse Squash File system:

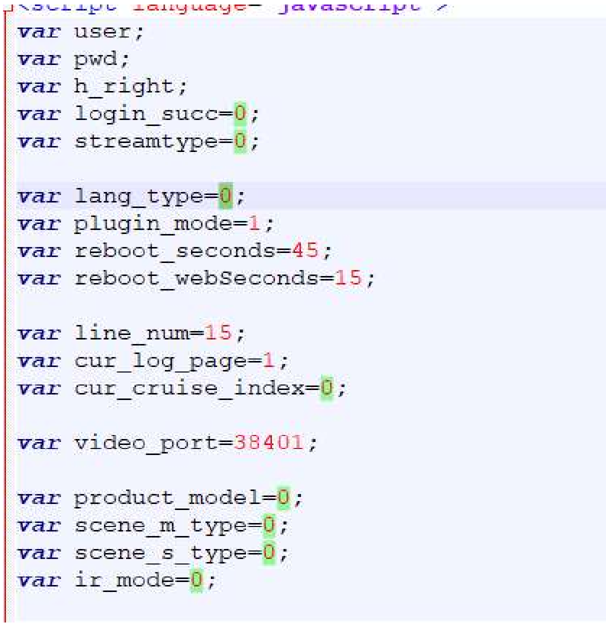


```
app
custom
sav
web
```

Figure 2

To find the port used to broadcast videos, player should open the following file:

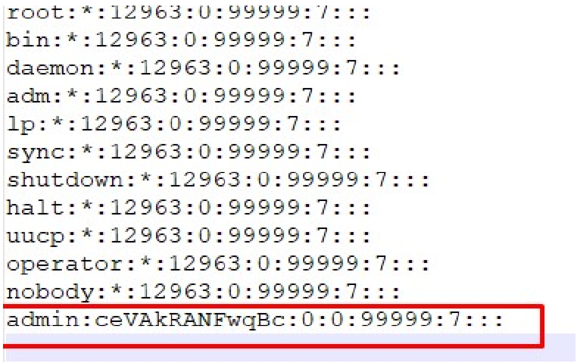
Web\camera.htm



```
<script language="javascript">
var user;
var pwd;
var h_right;
var login_succ=0;
var streamtype=0;

var lang_type=0;
var plugin_mode=1;
var reboot_seconds=45;
var reboot_webSeconds=15;

var line_num=15;
var cur_log_page=1;
var cur_cruise_index=0;

var video_port=38401;

var product_model=0;
var scene_m_type=0;
var scene_s_type=0;
var ir_mode=0;
```

Figure 3

To locate the password of the camera, player must analyse and crack shadow file: squashfs-root\app\etc\shadow

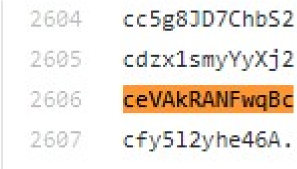


```
root:*:12963:0:99999:7:::
bin:*:12963:0:99999:7:::
daemon:*:12963:0:99999:7:::
adm:*:12963:0:99999:7:::
lp:*:12963:0:99999:7:::
sync:*:12963:0:99999:7:::
shutdown:*:12963:0:99999:7:::
halt:*:12963:0:99999:7:::
uucp:*:12963:0:99999:7:::
operator:*:12963:0:99999:7:::
nobody:*:12963:0:99999:7:::
admin:ceVAkRANFwqBc:0:0:99999:7:::
```

Figure 4

Just admin has password. Player could use online websites to crack the hash, or use local app like John the ripper:

https://gist.github.com/roycewilliams/f3b2188fea7b8beffa8952363248c233



```
cc5g8JD7ChbS2
cdzx1smyYyXj2
ceVAkRANFwqBc
cfy512yhe46A.
```

Figure 5

Password is “admin”

Flag Information

flag{admin_38401}