



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 group ID of user who has the User ID 11 of the IP camera.

Mission Description

There are security cameras installed inside Skytech and Claire has to analyse them. You're going to analyse an IP camera Firmware. Your goal is to find out which is the group ID of user who has the User ID 11 of the IP camera. Please locate the name.

Location

SYLVARCON | SKYTECH HQ



Tools

- binwalk

Questions

Which group has the ID 0?

- root

Which is the size of the device /dev/shm in mb?

- 20

Which is the nameserver used?

- 192.168.31.228

Hints

1. Check if the camera has any partition.
2. User binwalk.
3. Analyse Squash File system and locate passwd file



Write Up

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

```
binwalk -eM "firmware provided"
```

```
jmma@demowindows:/mnt/c/Thratia_2$ binwalk -eM ipcam.bin

Scan Time: 2021-05-12 21:59:40
Target File: /mnt/c/Thratia_2/ipcam.bin
MD5 Checksum: 0dd707275592db8ea154885b197aa161
Signatures: 411

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
217452        0x3516C      CRC32 polynomial table, little endian
524288        0x80000      uImage header, header size: 64 bytes, header CRC: 0xFE93
, image size: 2025296 bytes, Data Address: 0x2000000, Entry Point: 0x20000040, data CRC
image type: OS Kernel Image, compression type: none, image name: "gm8136"
524352        0x80040      Linux kernel ARM boot executable zImage (little-endian)
542452        0x846F4      gzip compressed data, maximum compression, from Unix, la
null date)

WARNING: Extractor.execute failed to run external extractor 'sasquatch -p 1 -le -d 'so
such file or directory: 'sasquatch', 'sasquatch -p 1 -le -d 'squashfs-root-0' '%e'' n
WARNING: Extractor.execute failed to run external extractor 'sasquatch -p 1 -be -d 'so
such file or directory: 'sasquatch', 'sasquatch -p 1 -be -d 'squashfs-root-0' '%e'' n
3670016        0x380000      Squashfs filesystem, little endian, version 4.0, compres
inodes, blocksize: 131072 bytes, created: 2005-08-05 07:41:04
11534956        0xB0026C      Zlib compressed data, compressed
```

Figure 1

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

Nombre	Fecha de modificación	Tipo	Tamaño
846F4	12/05/2021 22:00	Carpeta de archivos	
squashfs-root	12/05/2021 21:59	Carpeta de archivos	
squashfs-root-v	12/05/2021 21:59	Carpeta de archivos	
846F4.gz	12/05/2021 21:59	Archivo WinRAR	15.855 KB
380000.squashfs	12/05/2021 21:59	Archivo SQUASHFS	4.691 KB
B0A0C8.jffs2	12/05/2021 21:59	Archivo JFFS2	5.080 KB
B0A068	12/05/2021 21:59	Archivo	1 KB
B0A068.zlib	12/05/2021 21:59	Archivo ZLIB	5.080 KB
B0ACBC	12/05/2021 21:59	Archivo	1 KB
B0ACBC.zlib	12/05/2021 21:59	Archivo ZLIB	5.077 KB
B0ADB8.jffs2	12/05/2021 21:59	Archivo JFFS2	5.077 KB
B0B9CC	12/05/2021 21:59	Archivo	1 KB
B0B9CC.zlib	12/05/2021 21:59	Archivo ZLIB	5.074 KB
B0BAC8.jffs2	12/05/2021 21:59	Archivo JFFS2	5.074 KB
root	12/05/2021 21:59	Archivo	1 KB

Figure 2

Next step would be to locate, who the user is, with id 11. To accomplish this, player must locate passwd file:

Nombre	Fecha de modificación	Tipo
init.d	03/06/2005 3:03	Carpeta
network	22/05/2005 4:30	Carpeta
Wireless	22/05/2005 4:34	Carpeta
fstab	01/01/2014 7:09	Archivo
group	01/01/2014 7:09	Archivo
host.conf	01/01/2014 7:09	Archivo
hosts	01/01/2014 7:09	Archivo
inetd.conf	01/01/2014 7:09	Archivo
inittab	03/06/2005 3:03	Archivo
issue	01/01/2014 7:09	Archivo
motd	01/01/2014 7:09	Archivo
mtab	01/01/2014 7:09	Archivo
nsswitch.conf	01/01/2014 7:09	Archivo
passwd	01/01/2014 7:09	Archivo
profile	30/05/2005 3:38	Archivo
resolv.conf	01/01/2014 7:09	Archivo
services	01/01/2014 7:09	Archivo
shadow	01/01/2014 7:09	Archivo
version.ini	05/08/2005 9:40	Opcione

```

1 root:x:0:0:root:/root:/bin/sh
2 bin:x:1:1:bin:/bin:/bin/sh
3 daemon:x:2:2:daemon:/usr/sbin:/bin/sh
4 adm:x:3:4:adm:/adm:/bin/sh
5 lp:x:4:7:lp:/var/spool/lpd:/bin/sh
6 sync:x:5:0:sync:/bin:/sync
7 shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
8 halt:x:7:0:halt:/sbin:/sbin/halt
9 uucp:x:10:14:uucp:/var/spool/uucp:/bin/sh
10 operator:x:11:0:Operator:/var:/bin/sh
11 nobody:x:99:99:nobody:/home:/bin/sh
12

```

Figure 3

The name of the user is operator, and the group ID is 11.

Flag Information

flag{operator}