Mission Name

Fliying to Euphea

History Background

After being in Paris with the librarian his next step is EUPHEA. Claire and Ethan must obtain authorization in the Recon Car to travel to Euphea.

Technical High-Level Overview

A network dump from a computer connected to a system that manages authorizations is provided to the player. This network dump contains an FTP communication, that simulates traffic with Recon Permissions.

Short Description

Your goal is to analyse a network dump from a computer connected to Skytech Flight Authorization System and get any password that you find.

Mission Description

A network dump from a computer connected to a system that manages authorizations is provided to the player. Your goal is to analyse this network dump from a computer connected to Skytech Flight Authorization System and get any password that you find.

Location

PARIS, FRANCE | PREPARING TO DEPART

Tools

- Wireshark

Questions

Which is the name of the file that was transferred?

- Fly.txt

Which was the IP address of the SkyTech.gov FTP server?

- 192.168.211.1

Which is the full name of the authorised ReconCar?

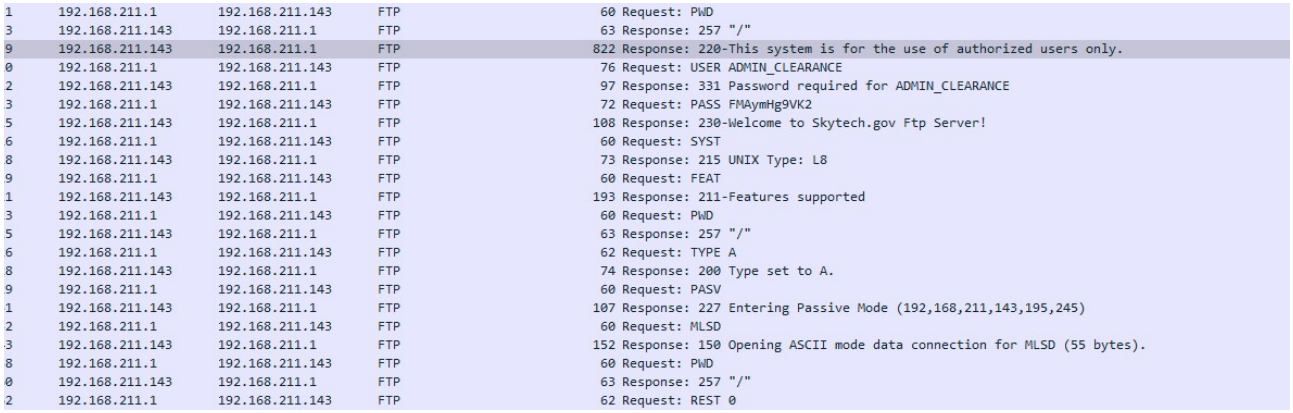
- ReconCar01

Items

1. First. you must analyse Protocol Hierarchy.
2. Analyse TCP protocols.
3. Analyse FTP protocol to get the password.

Write Up

Player must use Wireshark application ir order to analyze this network dump. Once opened, player should set a ftp filter.



1	192.168.211.1	192.168.211.143	FTP	60	Request: PWD
3	192.168.211.143	192.168.211.1	FTP	63	Response: 257 "/"
9	192.168.211.143	192.168.211.1	FTP	822	Response: 220-This system is for the use of authorized users only.
0	192.168.211.1	192.168.211.143	FTP	76	Request: USER ADMIN_CLEARANCE
2	192.168.211.143	192.168.211.1	FTP	97	Response: 331 Password required for ADMIN_CLEARANCE
3	192.168.211.1	192.168.211.143	FTP	72	Request: PASS FMAymHg9VK2
5	192.168.211.143	192.168.211.1	FTP	108	Response: 230-Welcome to Skytech.gov Ftp Server!
6	192.168.211.1	192.168.211.143	FTP	60	Request: SYST
8	192.168.211.143	192.168.211.1	FTP	73	Response: 215 UNIX Type: L8
9	192.168.211.1	192.168.211.143	FTP	60	Request: FEAT
1	192.168.211.143	192.168.211.1	FTP	193	Response: 211-Features supported
3	192.168.211.1	192.168.211.143	FTP	60	Request: PWD
5	192.168.211.143	192.168.211.1	FTP	63	Response: 257 "/"
6	192.168.211.1	192.168.211.143	FTP	62	Request: TYPE A
8	192.168.211.143	192.168.211.1	FTP	74	Response: 200 Type set to A.
9	192.168.211.1	192.168.211.143	FTP	60	Request: PASV
1	192.168.211.143	192.168.211.1	FTP	107	Response: 227 Entering Passive Mode (192,168,211,143,195,245)
2	192.168.211.1	192.168.211.143	FTP	60	Request: MLSD
3	192.168.211.143	192.168.211.1	FTP	152	Response: 150 Opening ASCII mode data connection for MLSD (55 bytes).
8	192.168.211.1	192.168.211.143	FTP	60	Request: PWD
0	192.168.211.143	192.168.211.1	FTP	63	Response: 257 "/"
2	192.168.211.1	192.168.211.143	FTP	62	Request: REST 0

Figure 1

Finally player could get the password: FMAymHg9VK2

Flag Information

flag{FMAymHg9VK2}