UNIVERSO MARVEL. Episodio 1. 1ª Parte.

Misión:

El agente Coulson ha capturado una trama de comunicación de una base de Hydra.

Tu objetivo será analizarla para descubrir la ubicación de la base secreta donde Hydra mantiene oculta su base de operaciones especiales.

Buena suerte, el éxito de nuestra misión depende de ti.

Nick Furia.

Enlace de descarga de la trama:
https://drive.google.com/open?id=1ltE42DQvMe-q_qVBbgeKQXvvTEiRyhwq

Info: La flag tiene el formato UAM{md5}

Resolución

Descargamos el fichero *capture-01.cap*.

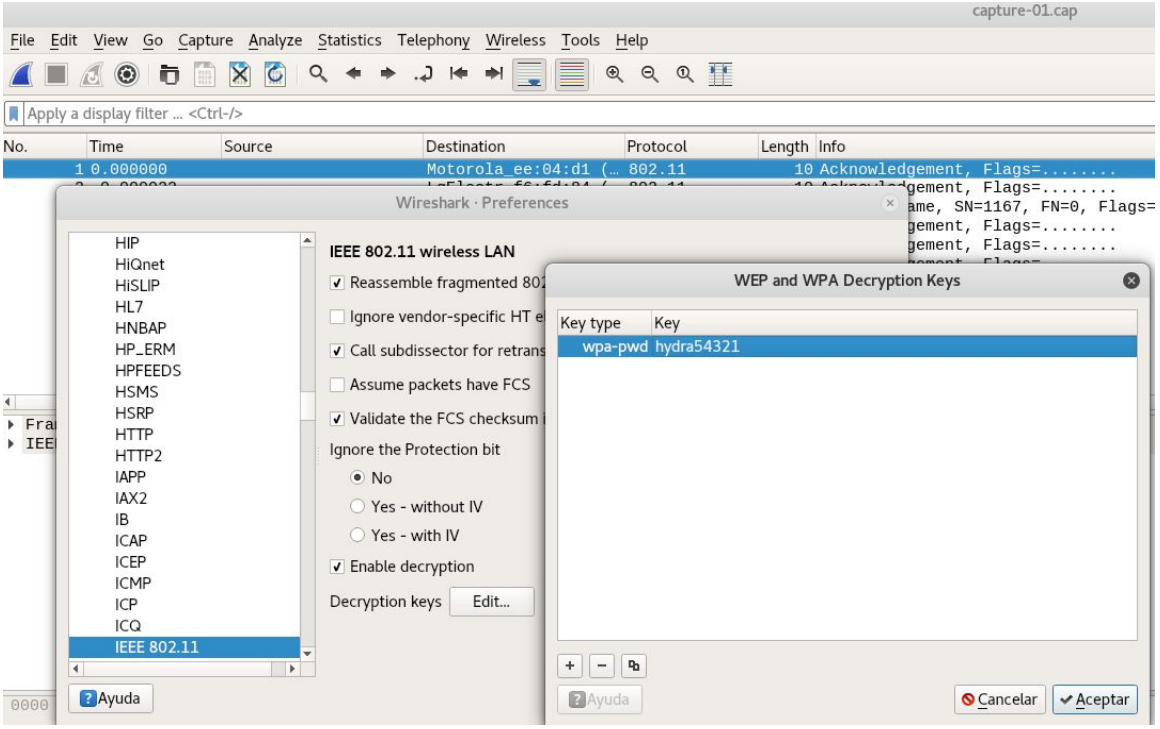
Abrimos con Wireshark, protocolo 802.11, nos tocará buscar la clave de la WIFI, para descifrar los paquetes.

Utilizamos **aircrack** y el diccionario "*rockyou***"**

aircrack-ng capture-01.cap -w /usr/share/wordlists/rockyou.txt

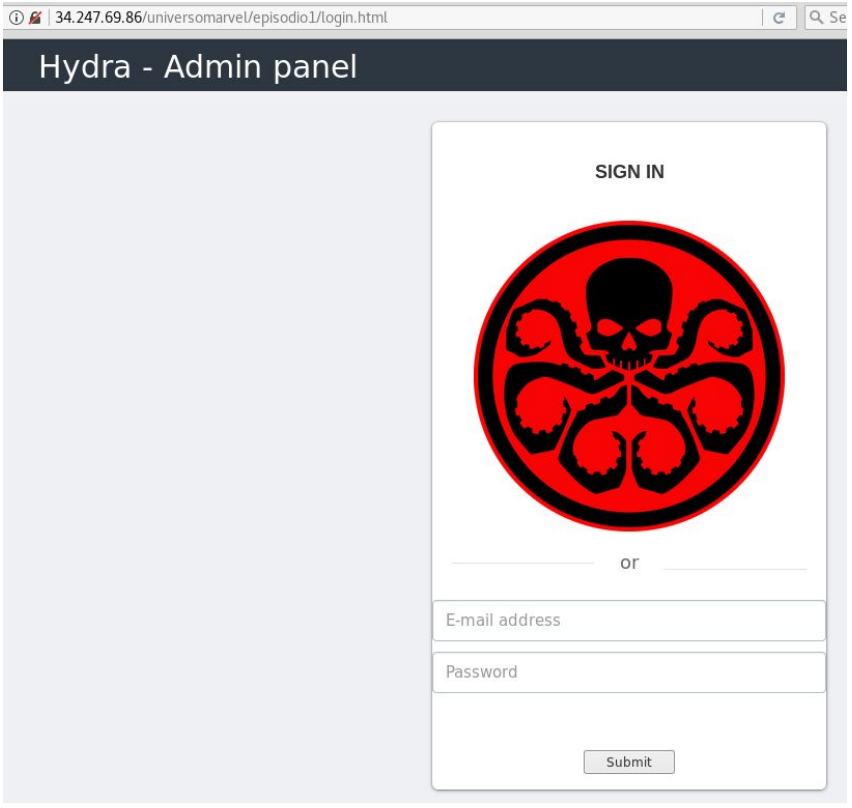
KEY FOUND! [hydra54321]

Agregamos la clave en las preferencias del protocolo en Wireshark.

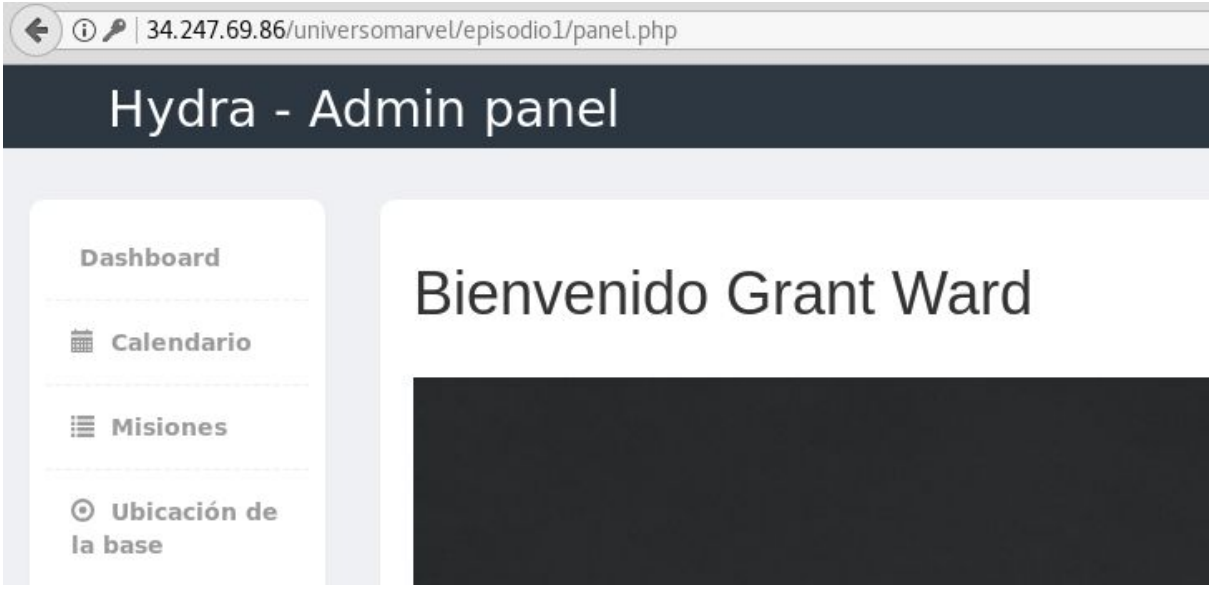


Filtramos por protocolo http, siguiendo el stream, observamos una dirección web:

Referer: **http://34.247.69.86/universomarvel/episodio1/login.html**



Probamos con test - test y aparece otro panel logueado como Grant Ward.



Si probamos el enlace Ubicación de la base, nos aparece el mensaje *"No tienes permisos para ver las ubicaciones"*

Parece que tendremos que obtener los permisos adecuados.

En el código fuente obtenemos la dirección del enlace de la ubicación

```
$("#mapas").click(function() {
                        $('#content')
                          .html('<img src="images/preloader.gif" />')
                          .load('databases.php?load=NVQXAYLT');
                    });
```

http://34.247.69.86/universomarvel/episodio1/databases.php?load=NVQXAYLT

Observamos que se ha creado una cookie de sesión cuando abrimos el panel:

PHPSESSID 2k2pmsskovgm1ieu63b65r84e1

Probamos a modificarla con valor "*test*"

Ahora el resultado del enlace es:

eyJlb3ZwbnB2YmFyZil6lHsKCSAglCAiT25mciBDZXZhcHZjbnkiOiB7lAoJlCAglCAglCAiQWJ6b2VyljoglIZmeW4gVWxxZW4iLAoJlCAglCAglCAiUGJiZXFmljoglM3wrAyMeKAskEgMjPCsDl44oCyUilsCgkglCAgfSwKCSAglCAiT25mciBGcnBlcmduljogewoJlCAglCAglCAiQWJ6b2VyljoglIN5bnQiLAoJlCAglCAglCAiUGJiZXFmljoglkhOWns0Njg2M3E5Mjg1OG80ODZwMjlzNzU5NzY3cjUzcjkyc30iLAoJlCAglH0KCX0=

decodificamos *base64*


```
{"Hovpnpvbarf": {
            "Onfr Cevapvcny": {
               "Abzoer": "Vfyn Ulqen",
               "Pbbeqf": "37°21′A 23°28′R",
            },
            "Onfr Frpergn": {
               "Abzoer": "Synt",
               "Pbbeqf": "HNZ{46863q92858o486p29s759767r53r92s}",
            }
         }
```


Rot13


```
{"Ubicaciones": {
            "Base Principal": {
               "Nombre": "Isla Hydra",
               "Coords": "37°21′N 23°28′E",
            },
            "Base Secreta": {
               "Nombre": "Flag",
               "Coords": "UAM{46863d92858b486c29f759767e53e92f}",
            }
         }
```


CyberChef

UAM{46863d92858b486c29f759767e53e92f}

Found : H41l_Hydr4_S0k0v14
(hash = 46863d92858b486c29f759767e53e92f)