

# WRITE-UP MARVEL – CTF UAM - HISPASEC

## EPISODIO-1

*Elaborado por: Arsenics*

### 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=1ItE42DQvMe-q\\_qVBbgeKQXvvTEiRyhwq](https://drive.google.com/open?id=1ItE42DQvMe-q_qVBbgeKQXvvTEiRyhwq)

Info: La flag tiene el formato UAM{md5}

### Bibliografía:

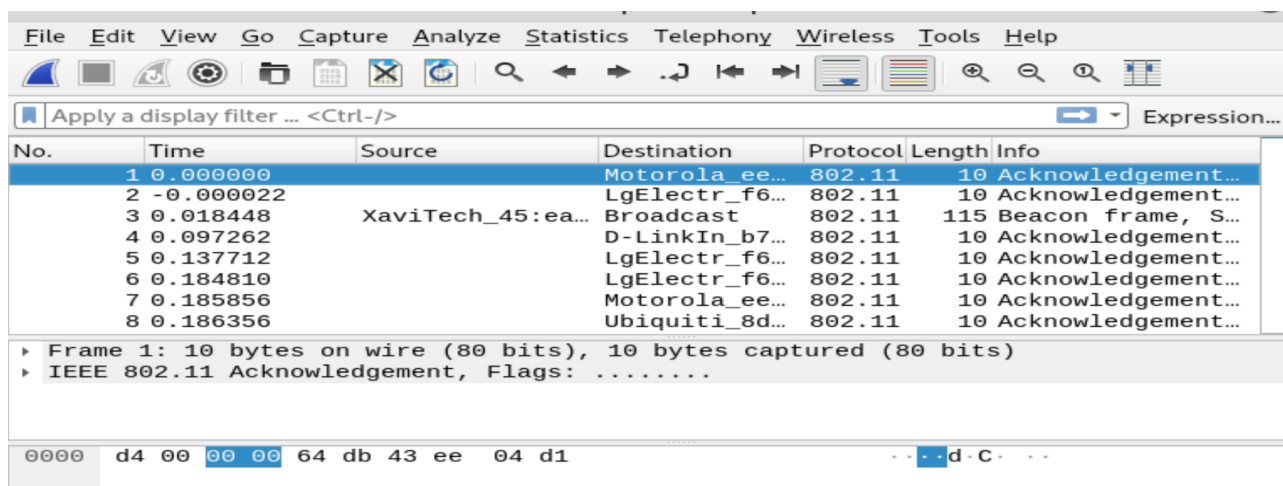
-Wireshark - <https://www.wireshark.org/>

-Aircrack-ng <https://www.aircrack-ng.org/>

-Cyberchef – <http://icyberchef.com/>

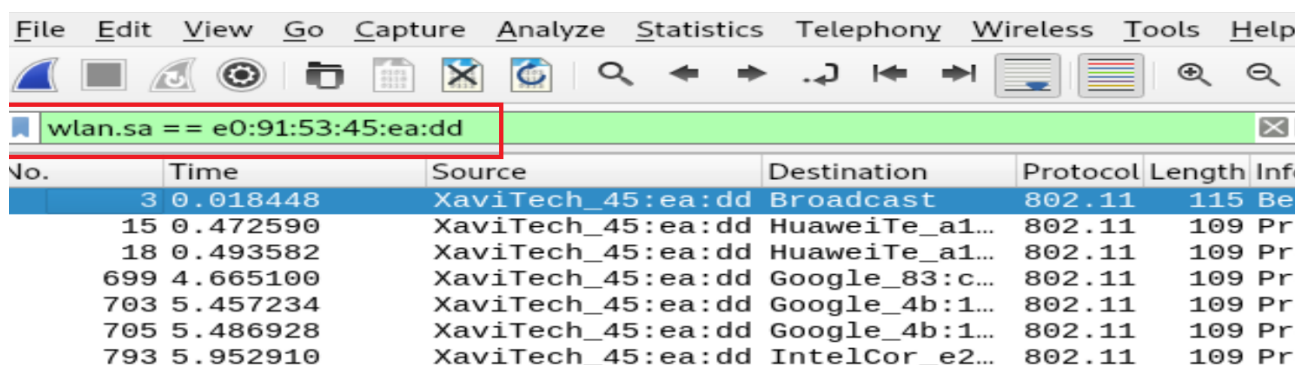
### Walktrough:

El enlace nos lleva a descargar un pcap para analizar la trama de comunicación obtenida de una base de Hydra. Los pcap se pueden analizar bien sea con tcpdump o Wireshark. En mi caso siempre que sea posible prefiero analizar las muestras con Wireshark ya que su interfaz gráfica consigue obtener resultados de tramas complejas con bastante sencillez. Es muy intuitivo y personalizable. Mientras que tcpdump se utiliza por comandos, pero también es muy recomendable saber usarlo para casos en los que no tenemos la opción de poder utilizar la herramienta de interfaz gráfica.



Observando la información que contiene la trama vemos que hay un usuario XaviTech\_45:ea:dd que realiza petición broadcast. Miramos el resto de conexiones y nos llama la atención que todo lo que podemos ver está sobre el protocolo 802.11. Con lo que a priori no tenemos la información de TCP, HTTP y similares que nos ofrecería información de interés. De modo que hacemos como si realizásemos una auditoria wifi contra el pcap para poder descifrar las Keys y llegar al resto de información que necesitamos.

Para ello, hacemos uso de la herramienta Aircrack-ng en la que necesitaremos el tipo de wifi a auditar, el BSSID (Basic Service Set Identifier), el cuál nos identifica puntos de acceso y sus clientes y una wordlist.



No.	Time	Source	Destination	Protocol	Length	Info
3	0.018448	XaviTech_45:ea:dd	Broadcast	802.11	115	Be
15	0.472590	XaviTech_45:ea:dd	HuaweiTe_a1...	802.11	109	Pr
18	0.493582	XaviTech_45:ea:dd	HuaweiTe_a1...	802.11	109	Pr
699	4.665100	XaviTech_45:ea:dd	Google_83:c...	802.11	109	Pr
703	5.457234	XaviTech_45:ea:dd	Google_4b:1...	802.11	109	Pr
705	5.486928	XaviTech_45:ea:dd	Google_4b:1...	802.11	109	Pr
793	5.952910	XaviTech_45:ea:dd	IntelCor_e2...	802.11	109	Pr

- wpa2 = a2 en la herramienta

-BSSID: e0:91:53:45:ea:dd que lo vemos al filtrar por XaviTech\_45 que es el q realiza el broadcast.

-Wordlist rockyou.txt

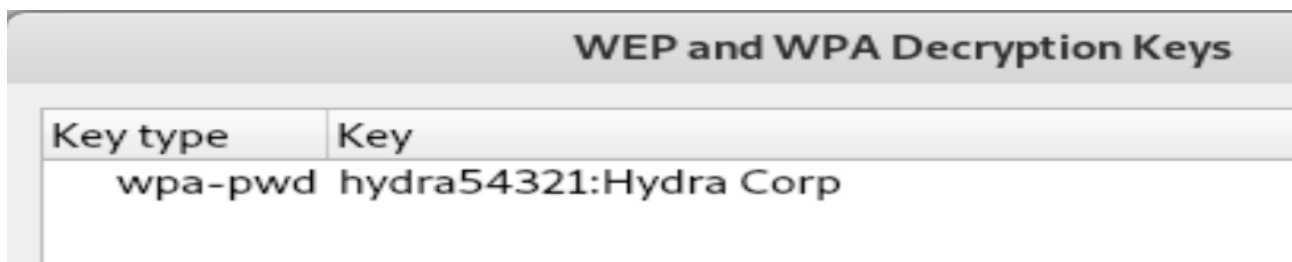
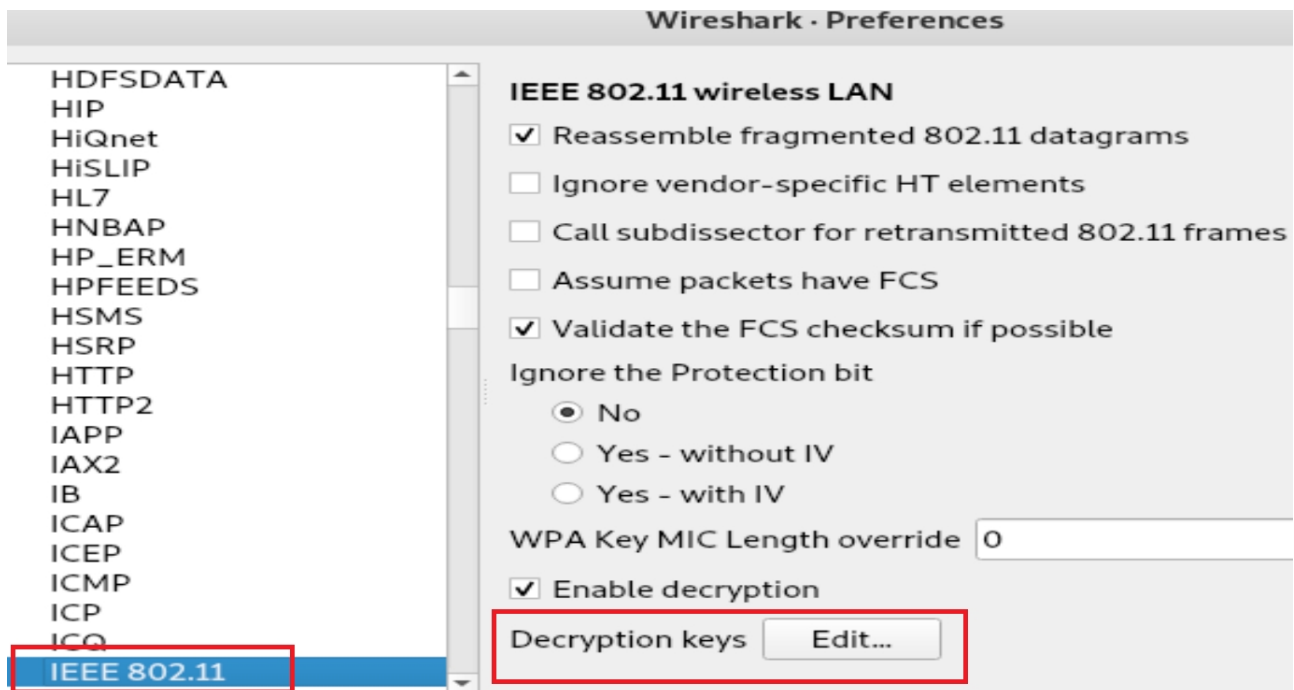
En la cmd: aircrack-ng -a2 -b e0:91:53:45:ea:dd -w rockyou.txt capture-01.cap y tras unas palomitas llega el resultado esperado!

KEY FOUND! [ hydra54321 ]

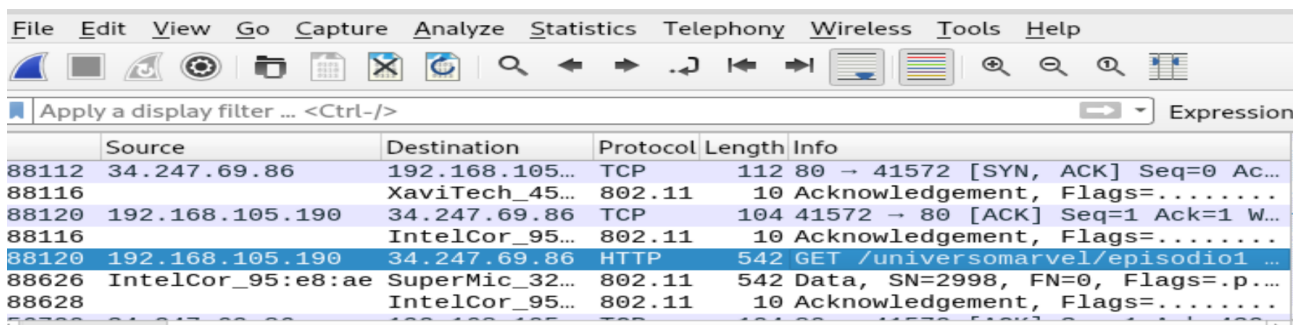
Dado que no tenemos acceso a la wifi real en un primer momento nos podemos quedar estancados aquí. Tras algunas vueltas caemos en la cuenta del protocolo 802.11 mencionado anteriormente el cuál nos dará acceso al resto de conexiones. Pero cómo realizamos un “Decrypt Keys” ?

Seleccionamos la source del BSSID en este caso XaviTech\_45, pulsamos botón derecho: Protocol preferences/ open IEEE 802.11 wireless LAN preferences y nos aparece la siguiente pantalla donde ponemos en este caso wpa-pwd con la estructura :Contraseña:SSID.

Dónde la contraseña será la encontrada hydra54321 y la SSID: Hydra Corp tal y como se puede ver en la trama.



Y buscando entre las peticiones TCP, ICMP, ARP, HTTP encontramos una particularmente útil:






Una petición GET con destino 34.247.69.86 y directorios *universomarvelepisodio1* !!!! Vamos a ver que encontramos aquí. Y voilà!!! Una web de universo marvel con login. Esto se pone interesante.

Dado que pide email en vez de usuario me decanto por probar si es susceptible a XSS. Posiblemente en la trama residan las credenciales, pero si funciona te ahorras faena.



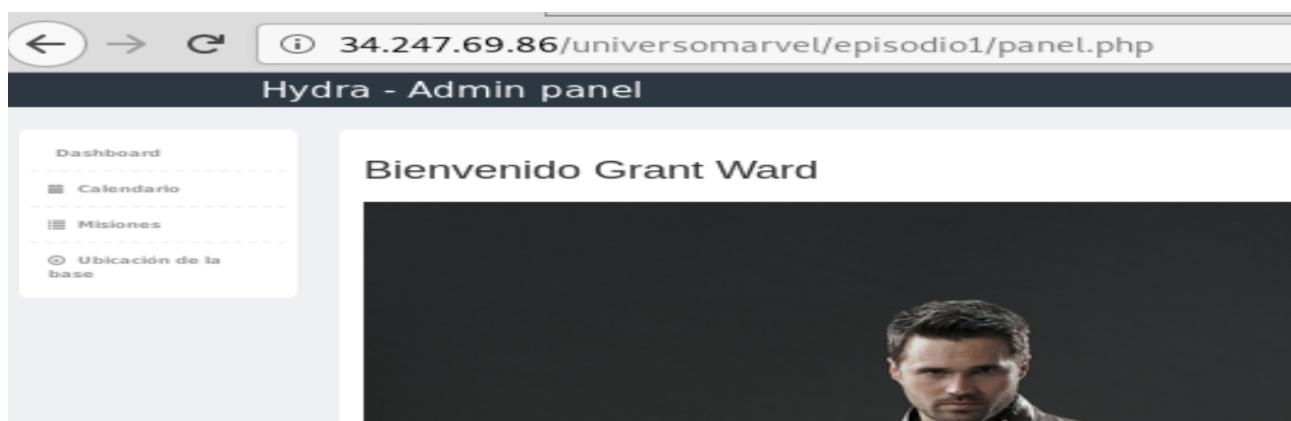
# Index of /universomarvel

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">episodio1/</a>	2018-12-11 14:19	-	
 <a href="#">test.html</a>	2018-12-11 13:48	43	

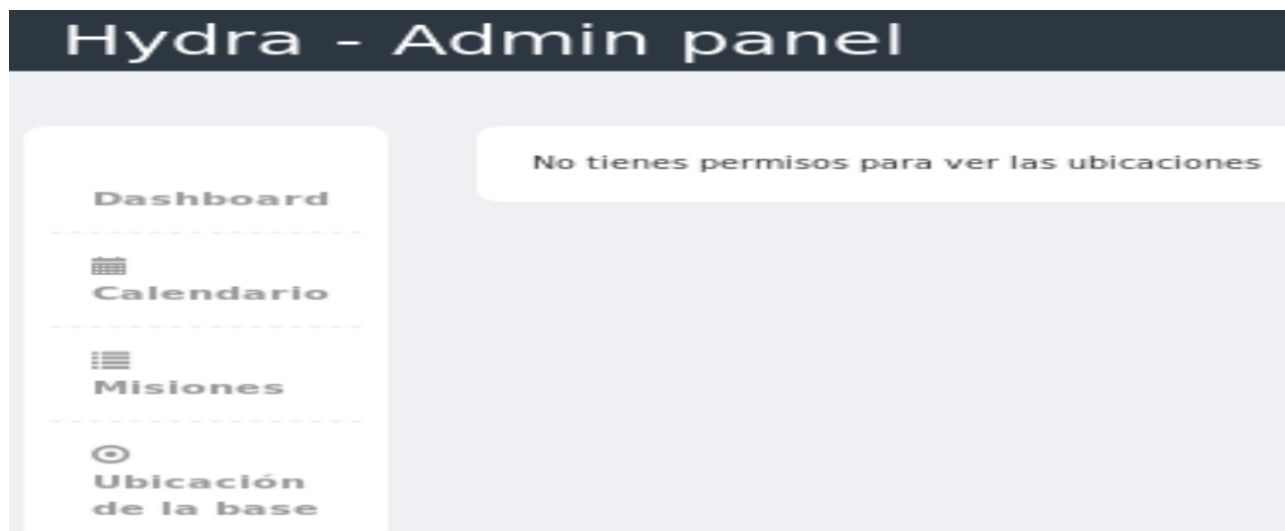
*Apache/2.4.25 (Debian) Server at 34.247.69.86 Port 80*



Y vaya, vaya, parece que si es vulnerable cross site scripting...



En el dashboard vemos que hay 3 opciones. El calendario, las misiones y nuestra ansiada ubicación de la base de hydra!! Sin embargo cuando presionamos sobre ellas, la opción del calendario y las misiones funcionan correctamente pero claro, la que nos interesa de la ubicación de la base de Hydra no tenemos permisos. Si los tuvieramos no sería tan divertido por supuesto jaja. En consecuencia, el juego continúa.

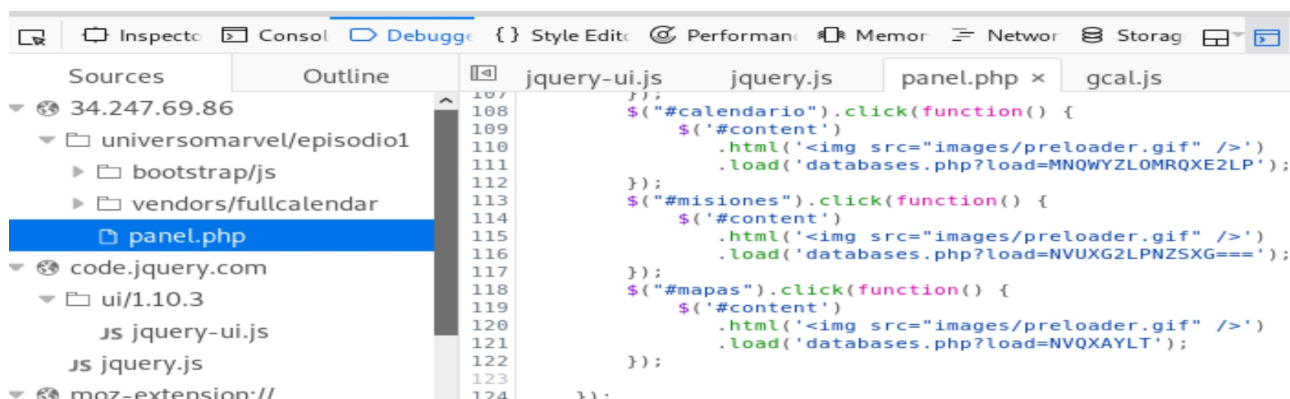


Miramos en el código por las opciones de desarrollador a ver cómo está estructurado y que encontramos que pueda jugar en nuestro favor. En Ubicación de la base pulsamos botón derecho / Inspect element y vemos lo siguiente:

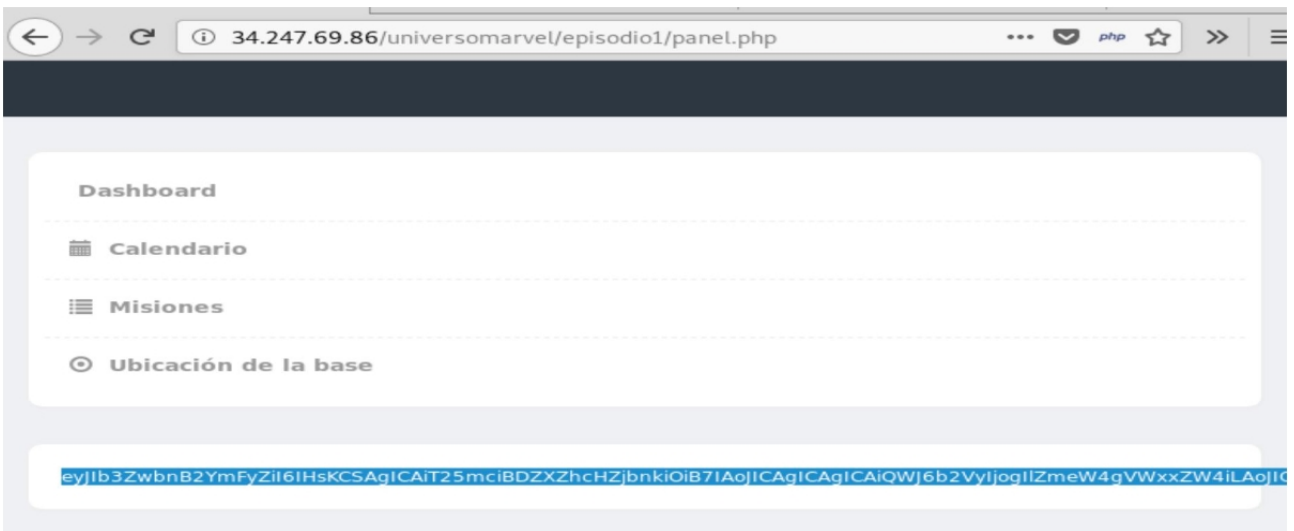




Ubicación, mapas, la función que carga la base de datos de la ubicación...aixxx ahí esta nuestro premio, pero cómo llegamos a él? Seguimos investigando y dando vueltas al asunto.

En la pestaña del debugger vemos toda la estructura del panel.php, pero tampoco podemos acceder a la info que buscamos.




Jugando con las queries conseguimos cargar y desbloquear la información de la ubicación.



Download CyberChef  Last build: 2 days ago - New in v8: Automated encoding detection and simplified operatio... Options  About / Support

### Operations

- rot13
- ROT13**
- Favourites 
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time
- Extractors
- Compression
- Hashing

### Recipe

From Base64

Alphabet  
A-Za-z0...

☒ Remove non-alphabet chars

ROT13

☒ Rotate lower case chars

☒ Rotate upper case chars

Amount  
13

### Input

```
eyJib3ZwbmB2YmFyZiI6IH5KC5AgICA1T25mc1BDZXZhcHZjbkn01b7IAoJICAgICAiQWJ6b2VvYjogIlZmeW4gVWxxZW41LAoJICAgICAiUGJlZXFMIjM3wraYMeKAskEgMjPCs0I440cyu1IsCgkgTCAgfSwKCSAgICA1T25mc1B6cmduIjogewoJICAgICAiQWJ6b2VvYjogIlN5bnQ1LAoJICAgICAiQWJ6b2VvYjogIkh0wns0Njg2M3E5Mjg1OGE0ODZwMjZlNzU0NzY3cjuZcjkyc301ICAgIH0KCX0=
```

start: 257	length: 332
end: 307	lines: 1
length: 50	

### Output

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

start: 103	time: 10ms
end: 230	length: 242
length: 37	lines: 10

Luego vamos a comprobar dónde está la base principal de Hydra. Pero que buena sorpresa!!



Gracias a los admins por este bello episodio.

**UAM{4636863d92858b486c29f759767e53e92f}**

**Autoría: Arsenics**