

EPISODIO 1 - 1ª PARTE

879

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_qVBbgeKQXvvTEiRyhqw

Info: La flag tiene el formato UAM{md5}

Nos descargamos un archivo .cap con tramas 802.11, vamos a crackearlo:

```
root@kali:/media/sf_Downloads# aircrack-ng capture-01.cap -w /usr/share/wordlists/rockyou.txt
```

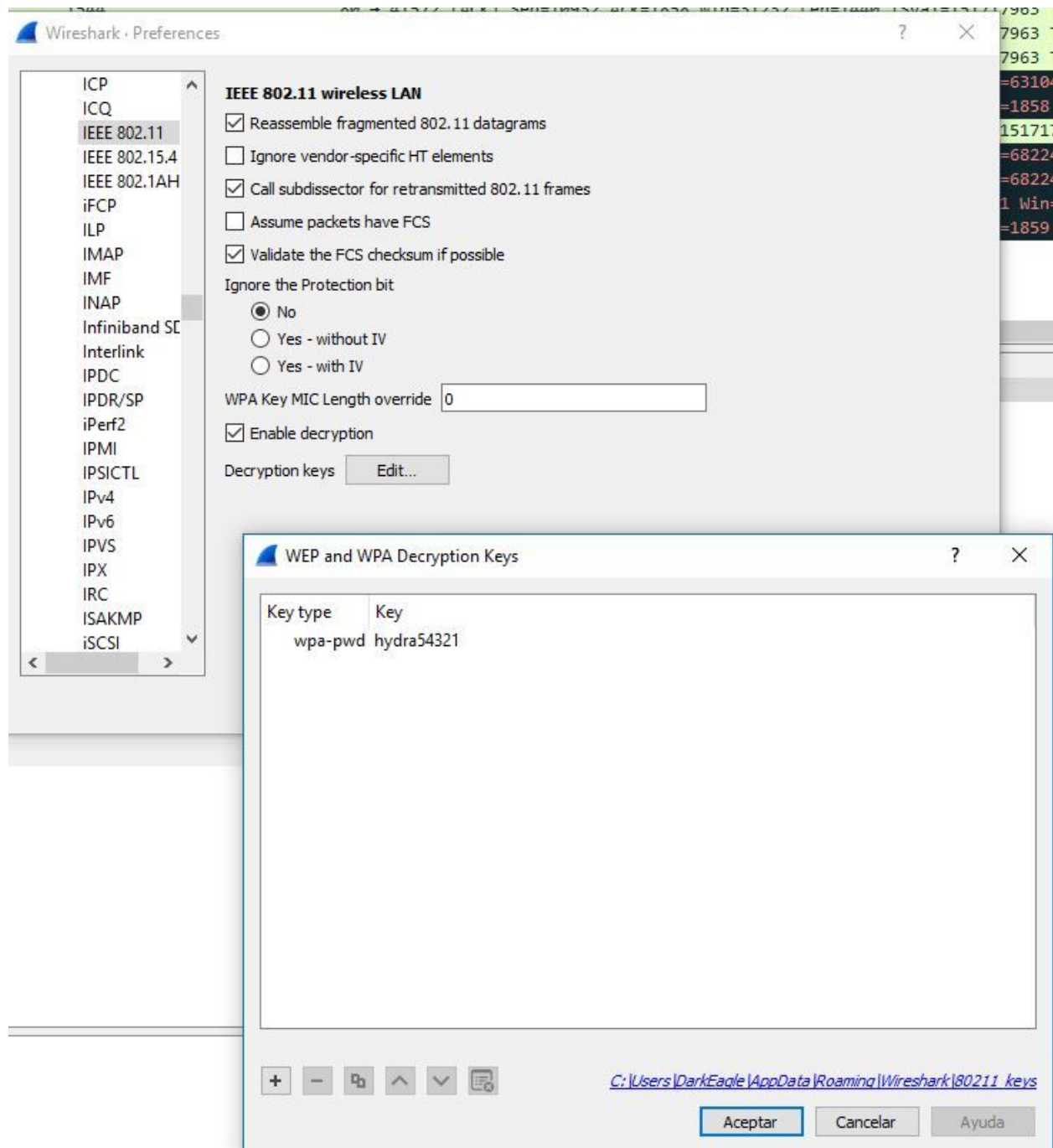
```
[00:05:16] 4868880/9822768 keys tested (15515.50 k/s)
Time left: 5 minutes, 19 seconds 49.57%
KEY FOUND! [ hydra54321 ]

Master Key      : 7F B1 AE 7F BB F1 A7 AF 5E D5 1B D3 17 1F E7 61
                  9C 5F 54 58 44 CD 57 5C A8 B8 B0 0E F6 1E 3B 62

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 8D 07 1F AA BB 62 2B 05 41 A2 82 60 33 80 DA 16
```

Abrimos el wireshark e introducimos la key crackeada en Edit → Preferences → Protocols → IEEE802.11. Dentro de Decryption keys:



Con esto tenemos los paquetes decodificados y podemos inspeccionar la captura.

Inspeccionando las tramas TCP vemos:

```
Wireshark - Follow TCP Stream (tcp.stream eq 10) - capture-01.cap

GET /universomarvel/episodio1 HTTP/1.1
Host: 34.247.69.86
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.14 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,es;q=0.8,ca;q=0.7,sm;q=0.6,fr;q=0.5

HTTP/1.1 301 Moved Permanently
Date: Fri, 14 Dec 2018 09:50:24 GMT
Server: Apache/2.4.25 (Debian)
Location: http://34.247.69.86/universomarvel/episodio1/
Content-Length: 331
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1


<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://34.247.69.86/universomarvel/episodio1/">here</a>.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at 34.247.69.86 Port 80</address>
</body></html>
GET /universomarvel/episodio1/ HTTP/1.1
Host: 34.247.69.86
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.14 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,es;q=0.8,ca;q=0.7,sm;q=0.6,fr;q=0.5

[495 bytes missing in capture file].GET /universomarvel/episodio1/bootstrap/css/bootstrap.min.css HTTP/1.1
Host: 34.247.69.86
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.14 Safari/537.36
DNT: 1
Accept: text/css,*/*;q=0.1
Referer: http://34.247.69.86/universomarvel/episodio1/login.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,es;q=0.8,ca;q=0.7,sm;q=0.6,fr;q=0.5
Cookie: PHPSESSID=dq6vj1t94b4r8sg16gb1pa4pa0
```

Tenemos la URL <http://34.247.69.86/universomarvel/episodio1/>

Hydra - Admin panel

SIGN IN

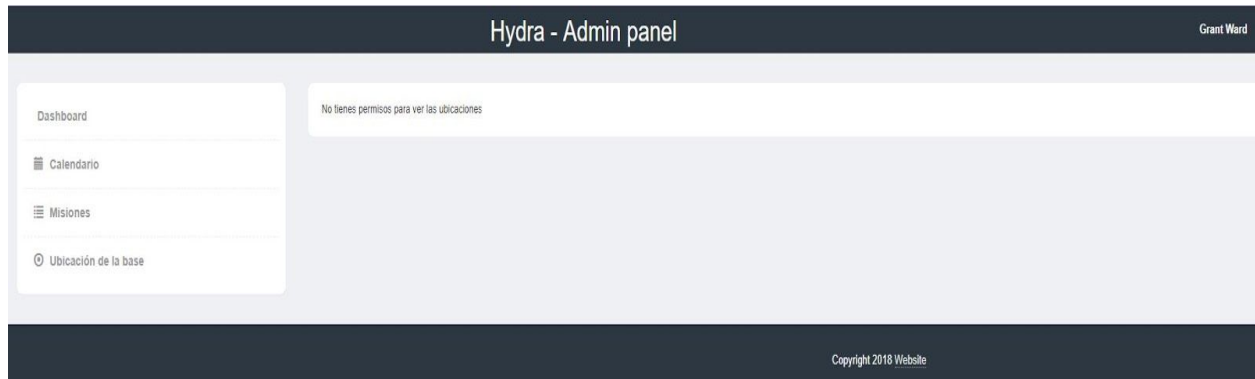


or

Submit

Insertamos cualquier dato en los campos del formulario (no se valida que sea e-mail) e ingresamos en el panel.

En la sección de Ubicación de la base tenemos el siguiente mensaje:



Si miramos el source-code de la web vemos:

```
<script src="https://code.jquery.com/jquery.js"></script>
<script src="bootstrap/js/bootstrap.min.js"></script>
<script src="js/custom.js"></script>
<script src="https://code.jquery.com/ui/1.10.3/jquery-ui.js"></script>
<script src="vendors/fullcalendar/fullcalendar.js"></script>
<script src="vendors/fullcalendar/gcal.js"></script>
<script src="js/calendar.js"></script>
<script>

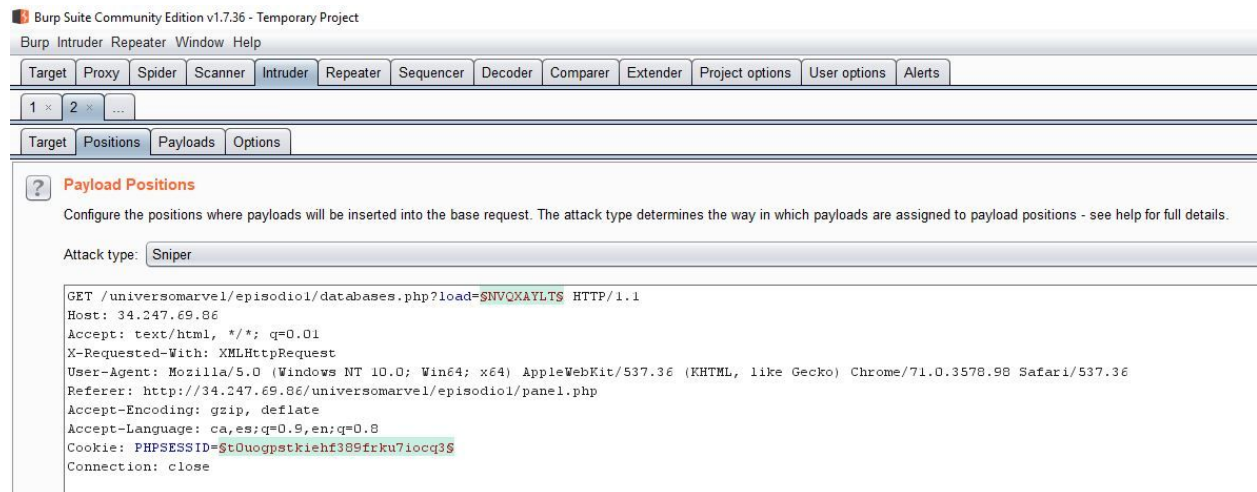
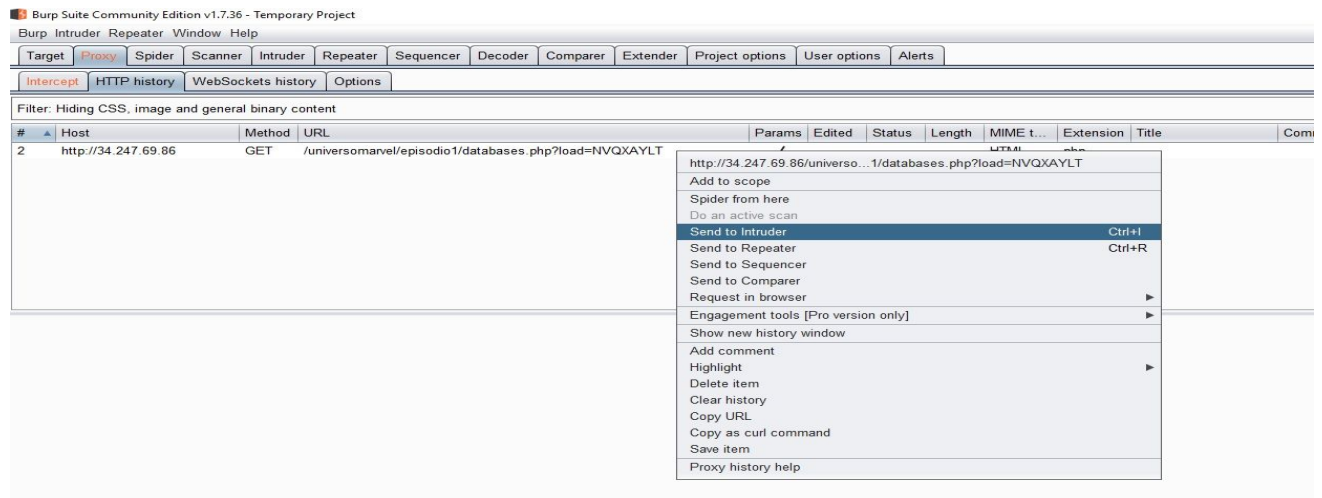
    $(function() {

        $("#dashboard").click(function() {
            $('#content')
                .html('')
                .load('databases.php?load=MRQXG2DCN5QXEZA=');
        });
        $("#calendario").click(function() {
            $('#content')
                .html('')
                .load('databases.php?load=MNQWYZLQMRQXE2LP');
        });
        $("#misiones").click(function() {
            $('#content')
                .html('')
                .load('databases.php?load=NVUXG2LPNZSXG==');
        });
        $("#mapas").click(function() {
            $('#content')
                .html('')
                .load('databases.php?load=NVQXAYLT');
        });

    });
</script>
</body>
</html>
```

En el que tenemos problemas para acceder es el último: NVQXAYLT

Abrimos Burp y utilizaremos Intruder para acceder a lo que nos interesa:





eyJlb3ZwbmB2YmFyZil6IHsKCSAgICAiT25mciBDZXZhcHZjbniOiB7IAoJICAgICAglCAiQWJ6b2VyljogIlZmeW4gVWxxZW4iLAoJICAgICAglCAiUGJiZXFmljogIjM3wrAyMeKAskEgMjPCsDI44oCyUiIsCgkgICAglCAgSwKCSAgICAiT25mciBGcnBlcmduljogewoJICAgICAglCAiQWJ6b2VyljogIlN5bnQiLAoJICAgICAglCAiUGJiZXFmljogIkhOWns0Njg2M3E5Mjg1OG80ODZwMjJzNzU5NzY3cjUzcjkyc30iLAoJICAgICAglH0KCX0=

Que pasado de Base64 a ASCII es:

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

HNZ{46863q92858o486p29s759767r53r92s}

Decodificamos esto con ROT13 y tenemos:

rot13.com
[About ROT13](#)

HNZ{46863q92858o486p29s759767r53r92s}

↓

ROT13 ▾

↓

UAM{46863d92858b486c29f759767e53e92f}

Flag: UAM{46863d92858b486c29f759767e53e92f}

Found : **H41l_Hydr4_S0k0v14**

(hash = 46863d92858b486c29f759767e53e92f)

DarkEagle