UAM Reto Universo Marvel: Episodio 1 - Hispasec

Descripción

Nombre: UAM- Universo Marvel - Episodio 1 - (Related https://www.universomarvel.com/)
Fecha de liberación: 15 de diciembre de 2018
Autor: 1v4n https://unaalmes.hispasec.com/team/40

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

Objetivo

Formato de la flag: UAM{md5}

Herramientas utilizadas

Google Chrome v71.0.3578.80 (Build oficial) (64 bits) https://www.google.com/chrome/
Gdown v3.6.0 https://github.com/wkentaro/gdown
File v5.34
Wireshark 2.6.4 https://www.wireshark.org/docs/relnotes/wireshark-2.6.4.html
Airgeddon script v8.12 https://github.com/v1s1t0r1sh3r3/airgeddon
Httpie v0.9.8 https://github.com/jakubroztocil/httpie
Audodecoder https://github.com/oreosES/autodecoder/

Resumen:

Comenzamos por visitar el reto descargando el archivo adjunto con la trama de Coulson que es un captura de tráfico de red WiFi utilizando *gdown https://drive.google.com/uc?id=1ltE42DQvMe-q_qVBbgeKQXvvTEiRyhwq*

```
root@kali:~/Desktop/uam/marvel/episodio1# gdown
https://drive.google.com/uc?id=1ltE42DQvMe-q_qVBbgeKQXvvTEiRyhwq
Downloading...
From: https://drive.google.com/uc?id=1ltE42DQvMe-q_qVBbgeKQXvvTEiRyhwq
To: /root/Desktop/uam/marvel/episodio1/capture-01.cap
100%|████████████████████████████████████████| 1.73M/1.73M [00:01<00:00, 1.18MB/s]
```

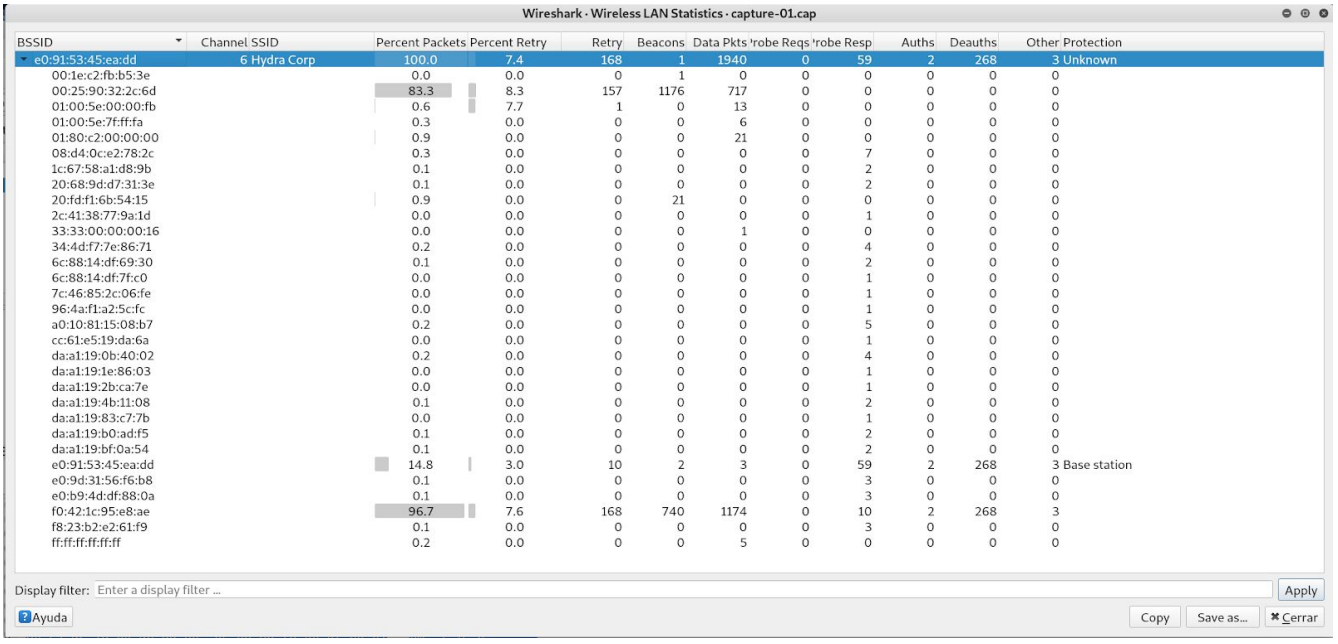
Obteniendo capture-01.cap (SHA1: 414b024b6d3bf7e5c283a6db4382c9ff8da3d09c).

Procesado la captura de tráfico

El fichero obtenido pertenece a la captura de una red WiFi con *SSID:* ***Hydra Corp*** *y BSSID:* ***E0:91:53:45:EA:DD*** protegida por contraseña WPA/WPA2 que obtendremos con ayuda de airgeddon que incluye el ataque con aircrack de diccionario sobre fichero de captura. Utilizaremos en esta ocasión como diccionario rockyou

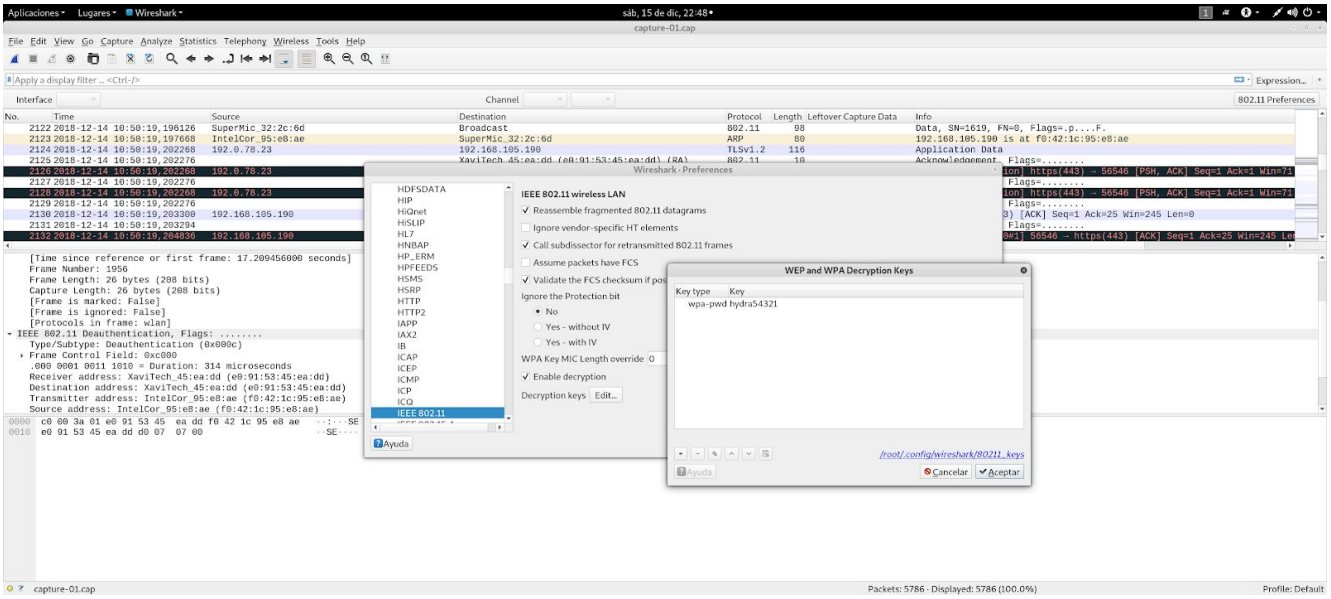
```
root@kali:~/Desktop/uam/marvel/episodio1# capinfos capture-01.cap
```

```
File name:           capture-01.cap
File type:           Wireshark/tcpdump/... - pcap
File encapsulation:  IEEE 802.11 Wireless LAN
File timestamp precision:  microseconds (6)
Packet size limit:   file hdr: 65535 bytes
Number of packets:   5.786
File size:           1.729 kB
Data size:           1.636 kB
Capture duration:    44,854052 seconds
First packet time:   2018-12-14 10:49:55,122874
Last packet time:    2018-12-14 10:50:39,976926
Data byte rate:      36 kBps
Data bit rate:       291 kbps
Average packet size: 282,85 bytes
Average packet rate: 128 packets/s
SHA256:              5b9abc310060bc0548104a5b529a48de419a7b9eba1ff2ed4e44cf5b948fc13b
RIPEMD160:           a86594301bc23e606610c0ec94c8122a5bcdcdc8
SHA1:                414b024b6d3bf7e5c283a6db4382c9ff8da3d09c
Strict time order:   False
Number of interfaces in file: 1
Interface #0 info:
                     Encapsulation = IEEE 802.11 Wireless LAN (20 - ieee-802-11)
                     Capture length = 65535
                     Time precision = microseconds (6)
                     Time ticks per second = 1000000
                     Number of stat entries = 0
                     Number of packets = 5786
```



La contraseña de la red WiFi es ***hydra54321***.

```
airgeddon. Contraseña desencriptada con aircrack
BSSID: E0:91:53:45:EA:DD
---------------
hydra54321
```



Acceso al servicio web de Hydra

Aplicando el filtro *http and tcp.stream eq 20* extraemos el servicio web en la URL http://34.247.69.86/universomarvel/episodio1/login.html y una credencial de acceso del usuario ***gward@hydra.com*** con password **rUHp6e7FV**

```
GET
/universomarvel/episodio1/authenticate.php?username=gward%40hydra.com&password=rUHp6e7FV
ds2nRPZ HTTP/1.1
Host: 34.247.69.86
Connection: keep-alive
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/72.0.3626.14 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
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=dq6vijt94b4r8sg16gb1pa4pa0

HTTP/1.1 302 Found
Date: Fri, 14 Dec 2018 09:50:36 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: panel.php
Content-Length: 6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Level1GET /universomarvel/episodio1/panel.php HTTP/1.1
Host: 34.247.69.86
Connection: keep-alive ...
```

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

Extracción de la ubicación de la base de Hydra

El código anterior de la web de Hydra nos muestra como acceder a la información de la ubicación de la base a través de *http://34.247.69.86/universomarvel/episodio1/databases.php?load=NVQXAYLT*

```
root@kali:~/Desktop/uam/marvel/episodio1# http
http://34.247.69.86//universomarvel/episodio1/databases.php?load=NVQXAYLT
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 230
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Dec 2018 18:01:32 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=sjrgb2sqm4ebhg8om6sa4vdpe6; path=/
Vary: Accept-Encoding

eyJIb3ZwbnB2YmFyZiI6IHsKCSAgICAiT25mciBDZXZhcHZjbnkiOiB7IAoJICAgICAgICAiQWJ6b2VyIjogIlZm
eW4gVWxxZW4iLAoJICAgICAgICAiUGJiZXFmIjogIjM3wrAyMeKAskEgMjPCsDI44oCyUiIsCgkgICAgfSwKCSAg
ICAiT25mciBGcnBlcmduIjogewoJICAgICAgICAiQWJ6b2VyIjogIlN5bnQiLAoJICAgICAgICAiUGJiZXFmIjog
IkhOWns0Njg2M3E5Mjg1OG80ODZwMjlzNzU5NzY3cjUzcjkyc30iLAoJICAgIH0KCX0=
```

Decodificación y obtención de la Flag

Pasamos a decodificar la cadena que identificamos como base64 utilizamos la herramienta online de Audodecoder

```
python3 audodecoder.py -m
"eyJIb3ZwbnB2YmFyZiI6IHsKCSAgICAiT25mciBDZXZhcHZjbnkiOiB7IAoJICAgICAgICAiQWJ6b2VyIjogIlZ
meW4gVWxxZW4iLAoJICAgICAgICAiUGJiZXFmIjogIjM3wrAyMeKAskEgMjPCsDI44oCyUiIsCgkgICAgfSwKCSA
gICAiT25mciBGcnBlcmduIjogewoJICAgICAgICAiQWJ6b2VyIjogIlN5bnQiLAoJICAgICAgICAiUGJiZXFmIjo
gIkhOWns0Njg2M3E5Mjg1OG80ODZwMjlzNzU5NzY3cjUzcjkyc30iLAoJICAgIH0KCX0=" -p UAM{
base64 > rot13: {"Ubicaciones": {
          "Base Principal": {
              "Nombre": "Isla Hydra",
              "Coords": "37°21′ N 23°28′ E",
          },
          "Base Secreta": {
```

```
            "Nombre": "Flag",
            "Coords": "UAM{46863d92858b486c29f759767e53e92f}",
        }
    }
```

Y la solución es ***UAM{46863d92858b486c29f759767e53e92f}***

```
Found : H41l_Hydr4_S0k0v14
(hash = 46863d92858b486c29f759767e53e92f)
```

Autor: MXY0bg== a.k.a. 1v4n
Twitter: https://twitter.com/Hackers4f // https://twitter.com/1r0Dm48Q