

ATAQUE POR FUERZA BRUTA

Una vez hemos escaneado un sistema y sabemos que servicios tiene, si encontramos alguno en el cual podamos loguearnos podremos probar nuestro ataque por fuerza bruta. Este ataque consiste en ir introduciendo combinaciones de usuarios y contraseñas que tendremos en listas enormes llamadas diccionarios o directamente probar todas las posibles combinaciones, aunque esto es realmente lento en la mayoría de casos.

Como podéis imaginar esta acción se puede automatizar con herramientas como Hydra o Medusa (esto parece un acuario pero son herramientas no os asustéis).

Podéis descargaros un diccionario de esta página web

<http://www.blackploit.com/2013/03/diccionarios-para-realizar-ataques-de.html#more>. (Con el más pequeño os servirá)

Para arrancar estas aplicaciones os vais a Inicio -> Buqtraq -> -> Fuerza Bruta -> Hydra o Medusa y podéis elegir la opción que interfaz grafica o la línea de comandos. Si es la primera vez que las utilizáis la interfaz grafica está muy bien, es muy intuitiva.

Deberéis seleccionar para el usuario y la contraseña el mismo diccionario que hemos descargado para ambos. A continuación poner la IP a atacar y por último, en el servicio deberéis de elegir el que queráis (los más típicos que tienen credenciales de acceso suelen ser ftp, telnet y ssh).