Escenario1

En este escenario tendremos dos contenedores docker, uno el atacante (kali linux) y la víctima (ubuntu). Ambos tienen el servicio SSH instalado y activo.

Para la práctica vamos a conocer el identificador del equipo víctima (lo voy a hacer sin IPs) que utilizaremos como vulnerabilidad. Con el equipo atacante y junto con la herramienta Hydra y un par de diccionarios (personalizados para que la práctica sea más llevadera y no haya que esperar todas las combinaciones de un diccionario convencional) llevaremos a cabo un ataque de fuerza bruta con la que se conseguirá un nombre de usuario y contraseña vulnerable.

Ya para ver si funcionó, nos conectaremos a la máquina atacada con el usuario y contraseña que se consiga en el ataque y podremos observar sus archivos (en este caso se simula un archivo de usuarios y sus contraseñas en claro).

Por último, cambiaremos la contraseña del usuario atacado por una más robusta y volveremos a lanzar el ataque anterior pero esta vez tendremos un final distinto, no obtendremos ninguna coincidencia.

Escenario1 extra

https://www.genbeta.com/seguridad/hacker-que-tumbo-a-orange-espana-explica-como-dejo-conexion-a-miles-clientes

Destacar el ataque de phishing a Orange y destacar que los hacen muy realistas y cada vez es más difícil captarlos por lo que aunque sea algo que no debería ocurrir, un despiste de este tipo lo puede tener cualquiera.

Lo que realmente hay que destacar es el usuario y contraseña utilizados (son realmente débiles) y quizás hubiera acabado antes el ataque con fuerza bruta que haciendo un ataque de phishing elaborado.

Esto anterior se podría hacer creando un diccionario personalizado usando combinaciones algo simples (dominioadmin, admindominio, adminpassword, etc.). La dirección usada se podría conseguir buscando en una página como “Phonebook.cz” con el dominio “orange.es” y filtrando por “admin”.

Escenario2

En este escenario tenemos un contenedor que aloja un servidor Nginx que contiene un archivo con información sensible.

Al principio este servidor se montará con lo básico y sin configurar ningún tipo de permisos. Esto hace que cualquier usuario que conozca la ruta del archivo pueda observar su contenido haciéndolo realmente inseguro.

Para mejorar la seguridad, crearemos un archivo de usuarios validados para leer el archivo y cambiaremos la configuración del archivo de configuración de Nginx para que acepte el archivo. Una vez reiniciado el servidor, volveremos a buscar el archivo tanto desde dentro del contenedor como desde el equipo local pero, solo los usuarios validados podrán ver el contenido del archivo.

Escenario3

En este escenario tenemos a nuestra disposición la web DVWA, una aplicación web PHP/MySQL que es muy vulnerable. Su objetivo principal es ser una ayuda para que los profesionales de la seguridad prueben sus habilidades y herramientas en un entorno legal. Tiene varios tipos de escenarios como: fuerza bruta, XSS, SQL Injection, etc. y varios tipos de niveles de configuración: bajo, medio, etc.