HACKLAB #1

RETO 1

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

Enunciado:

Introducción: Todos los días son puestos en operación miles de servidores en Internet, lamentablemente no todos ellos son seguros ya que muchos administradores consideran que nunca serán objeto de un ataque y por ello son muy flexibles en sus controles de seguridad, llegando a usar mecanismos de gestión y transferencia de archivos nada recomendables.

Escenario del laboratorio: Imagina en 3D, una emprea que se dedica al diseño de drones de última generación. Recientemente ha realizado una investigación que ha dado como resultado un prototipo de lo que considerán será el dron más potente de nuestros tiempos. Si el diseño de este prototipo llegará a ser expuesto en Internet antes de la fecha programada, causaría una grán pérdida economica para Imagina en 3D. Para evitar que esto ocurra, has sido contratado con el objetivo evaluar los controles que estan implementados y demostrar si la seguridad puede ser vulnerada.

Tu objetivo: Has llegado a un acuerdo con Imagina en 3D y se definen los siguientes 2 objetivos:

1.- Intentar obtener el diseño del prototipo del dron.

2.- Dejar evidencia (un archivo .txt)

Reglas importantes: A pesar de que fuiste contratado y cuentas con la autorización del cliente, debes seguir las siguientes reglas.

1.- Esta prohibido todo ataque DoS / DDoS. En caso de identificar este comportamiento, el servidor será dado de baja.

2.- Cuando logres acceder al sistema, deberás dejar una evidencia. Dicha evidencia deberá ser exclusivamente un archivo .txt con tu nick del usuario.

3.- El contenido del archivo puede ser lo que tú quieras. Yo digo: ¿porque no usar ascii art?

4.- El servidor estará activo durante 1 semana. Por favor, no publicar durante este tiempo la manera en la que accediste.

Información brindada por Imagina en 3D: La única información que te ha sido brindada para este servicio es el nombre y el facebook del administrador del sistema.

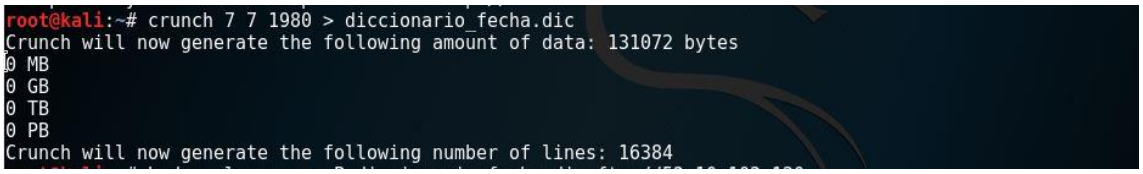
Pistas: Siempre son bienvenidas unas pistas, por ello te compartimos las siguientes:

1.- Realiza un muy buen stalkeo del perfil del administrador, existen personas que ventilan sus problemas o datos sensibles en Internet. Nunca se sabe... este admin puede ser una de esas personas.

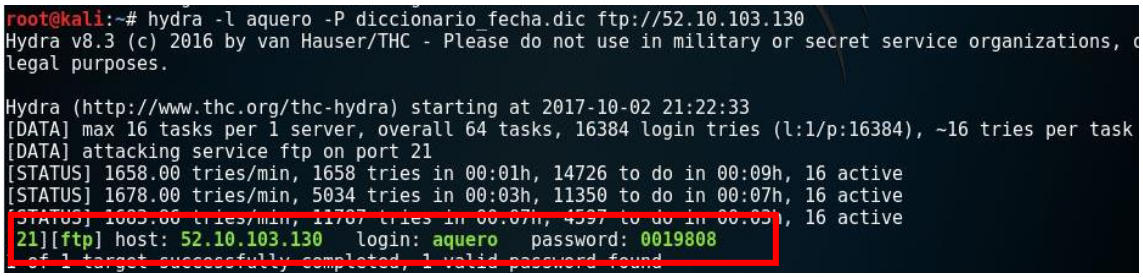
2.- La vulnerabilidad no esta en el servicio Web, por lo que no será requerido ejecutar herramientas como Acunetix o SQLMap.

Nuestro primer objetivo es acceder al servidor y obtener los planos del dron. Para ello comenzamos accediendo al Facebook del administrador y nos damos cuenta de que tiene varias imágenes subidas, y en una de ellas se puede observar como utiliza un servidor ftp. De esta imagen obtendremos la dirección del servidor y el nombre de usuario, ya solo nos faltará averiguar la contraseña.

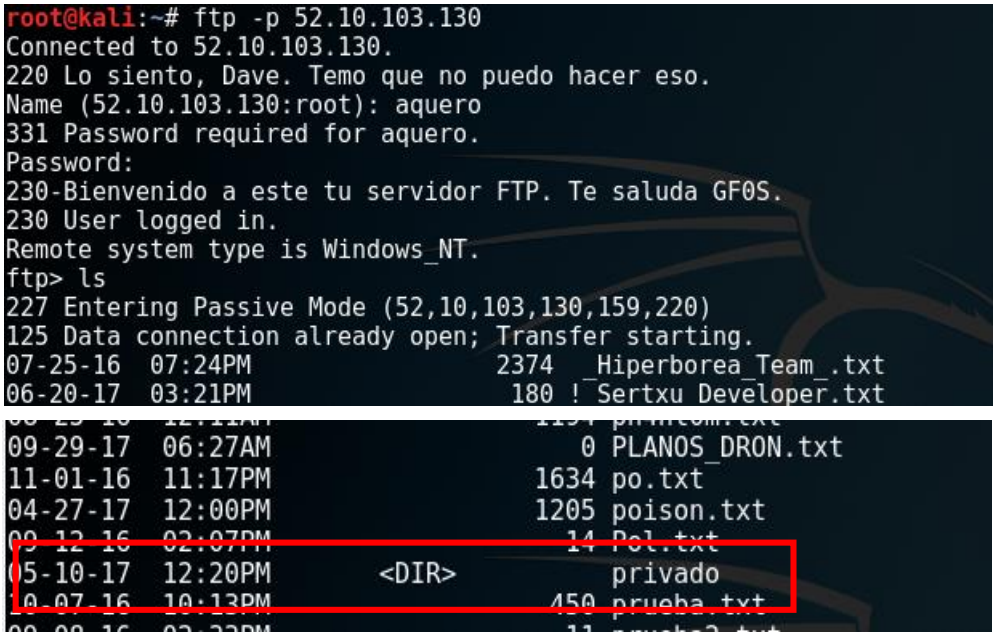
Seguimos buscando información relevante a la contraseña en el Facebook y encontramos otra imagen. Esta vez es de un correo, en él informa del problema existente con las contraseñas y en concreto nos indica que tienen 7 dígitos. Tras esto, procedemos a crear un diccionario para poder obtener todas las combinaciones posibles. Definiremos el diccionario con 7 dígitos y utilizaremos su fecha de nacimiento para aproximarnos más a la contraseña.



Una vez creado el diccionario procedemos a realizar un ataque por fuerza bruta utilizando hydra, esta herramienta nos permite obtener la contraseña a través del diccionario anteriormente creado.



Una vez obtenida la contraseña, tendremos acceso total al servidor ftp. Procedemos a acceder a él y buscamos algo raro/diferente. Durante esta búsqueda nos damos cuenta que todo lo que tiene el servidor son archivos .txt, pero encontramos un directorio con el nombre de privado, aquí se encontrará la información del dron que buscamos. Desde el navegador accedemos al servidor y buscamos este directorio, al entrar en él no encontramos nada **(Se supone que debería de estar un archivo con contraseña el cual será el prototipo. Yo no encuentro nada, supongo que el archivo estará oculto, pero no encuentro la forma de acceder a él).**



El primer objetivo ya está realizado. Ahora vamos a por el segundo, dejar una evidencia en el servidor para demostrar que hemos conseguido entrar. Para ello crearemos un .txt y lo subiremos al servidor.