Walkthrough

FASE INICIAL

Empezamos descargando la máquina desde Vulnhub, una vez descargada lo que haremos será importarla en VirtualBox/VMWare/UTM o similares, la inicializamos y nos pasamos a nuestra máquina Kali linux.

Una vez en la máquina Kali, abrimos la terminal y con un **arp-scan -I eth0 --localnet** escaneamos nuestra red. (Tenemos que tener en cuenta que ambas máquinas deben tener configuradas las redes con tipo Bridged*). Veremos que aparecerán varias direcciones IP, nos quedaremos con aquella que esté en la misma máquina virtual que nosotros.

Una vez conocida la IP de la máquina “víctima”, haremos un ping para verificar la conectividad, esto además nos dará información sobre qué tipo de máquina es gracias al TTL*. Vemos que TTL = 64, por lo que es una máquina Linux.

FASE DE ESCANEO

Usaremos la herramienta nmap* y realizaremos un escaneo de todos los puerto con el siguiente comando:
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn IpMaquinaVictima -oG nombreFichero

Con este comando indicamos que, usando nmap, queremos escanear los todos los puertos existentes (-p-), de entre estos, descubrir solamente los que estén abiertos (--open), con el tipo de escaneo TCP SYN port Scan (-sS)*, indicando que quieres tramitar paquetes no más lentos que 5000 paquetes por segundo (--min-rate 5000), con triple verbose (-vvv) para que a medida que vaya detectando puertos abiertos los vaya reportando por consola, que no aplique resolución DNS (-n), ya que ralentiza el escaneo, desactivaremos la detección de hosts, asumiendo que este está activo, ya que el ping anterior ha sido exitoso (-Pn), y lo exportaremos en formato grepeable (formato que permite filtrar con Regex) al fichero correspondiente (-oG).

(Esta configuración permite un escaneo rápido, sigiloso y violento que no detecta falsos positivos/negativos.)

Cuando ha finalizado nuestro escaneo, mostramos el contenido que nos ha reportado con cat nombreFichero y vemos que tenemos los puertos 80, 21, 65533 y 18888, que corresponden a http, ftp y TCP/UDP respectivamente.

FASE DE PROFUNDIZACIÓN

Abrimos la web que tenemos en el puerto 80 y rebuscamos un poco en el código fuente, ya que no hay muchos elementos que nos puedan llamar la atención en la propia web y encontramos una cadena de caracteres en Base64 al final del código.

Cuando decodificamos esa cadena, nos da otra aún más larga, esta vez en código Morse, el cual podemos descifrar usando la herramienta “SignalSquirrel”. Una vez traducida la cadena a lenguaje natural podemos leer lo siguiente:

“JIM AND PAM HAVE TALKED ABOUT ME IN MORSE CODE SEVERAL TIMES. SINCE YOU CAN READ THIS, HERE'S THE FIRST FLAG: FLAG1: 8CAF9C64F9D1181206FEC7F40A7524B3”

Hemos obtenido la primera FLAG pero vamos a indagar un poco más para encontrar el resto.

Enumeramos los posibles directorios y subdominios de la pagina con “gobuster”, encontrando los subdominios
“/robots.txt
/nick
/staffblog”

Profundizando en todos encontramos que en robots.txt hay varias rutas desactivadas como /nick, en la cual encontramos un archivo farewell.txt y un nick.pcap. El primero de ellos contiene:
“Hey Michael!
I just wanted to say goodbye. Through Teach for America, I'm gonna go down to Detroit and teach inner-city kids about computers. You know, I'm the lame IT guy and probably you don't even know my name so, who cares. But I just wanted you to know that the old creepy guy uses a pretty weak password. You know, the one who smells like death. You should do something about it.
Nick”

Y el segundo lo analizamos con Wireshark* para inspeccionar el paquete de red.
Siguiendo los TCP del paquete conseguimos unas posibles credenciales del servidor FTP del puerto 21 descubierto anteriormente:

Username: creed
Password: creed

Antes de explorar el puerto 21 investigamos la ruta /staffblog donde hay un archivo “CreedThoughts.doc” que nos da la segunda FLAG: 50f1ff7bc72bb24c0082be83a8b8c497