AXproyect

Writeups

- **Ax00 -> Ax01**

    - En el directorio principal, encontraremos varios directorios, moviéndonos entre ello encontraremos diferentes ficheros que debemos de analizar
    - Con cd nos moveremos entre directorios y con ls mostraremos su contenido
    - Para mostrar el contenido de los ficheros podemos usar cat, o abrirlos en editor de texto mediante nano o vim
    - En este caso el fichero que nos interesa se encuentra en dir2 -> 'Números de teléfono'
    - Mostraremos su contenido con cat, y el nombre entre comillas ya que contiene espacios, si nos fijamos al final de cada número de teléfono y separado por: encontraremos un carácter, la cadena de esos caracteres nos mostrara la contraseña.
    - Para filtrar y mostrar ese carácter utilizaremos awk
    - Cat "Números de teléfono" | awk -F ":" '{print $2}' | xargs
    - Con cat mostramos, con awk imprimimos el carácter después de los dos puntos y con xargs mostramos en horizontal

- **Ax01 -> Ax02**

    - Una vez ingresemos con ax01 e intentamos mostrar el contenido de su directorio principal, nos daremos cuenta de que aparentemente esta vacío, debemos de tener en cuenta que podemos tener ficheros ocultos asique para mostrarlos usaremos ls -la
    - Encontraremos un fichero llamado .lista_de_objetivos
    - Encontraremos un fichero el cual lo mostraremos de la misma manera que en Ax00 pero cambiando el delimitador de ":" a "]" y añadiendo una búsqueda por el signo +
    - Cat .lista_de_objetivos | grep "+" |awk -F "]" `{print $2}` | xargs

- **Ax02 -> Ax03**

- Entramos en el directorio del usuario Ax02, al listar el directorio vemos una serie de caracteres, en realidad es un simple nombre de fichero, tenemos que mostrar su contenido con cat, y veremos una cadena codificada en base64, tenemos que descodificarla
- Cat cGFzc3dvcmQk | base64 -d
- La cadena nos devolverá una pregunta, la respuesta a esa pregunta será la clave para Ax03

- **Ax03 -> Ax04**

  - Entramos en el directorio principal Ax03, vemos un programa llamado myprivatekey, si lo ejecutamos nos pedirá un usuario y un numero de teléfono
  - El usuario del que queremos obtener la contraseña es ax04, ahora falta conseguir su número de teléfono
  - Los usuarios guardan información propia que ha sido configurada en la creación del mismo, para obtener esta información utilizaremos **finger**
  - Utilizamos Finger ax04 y buscaremos su número de teléfono en la información, este lo utilizaremos en el script y nos devolverá su contraseña

- **Ax04 -> Ax05**

  - Si con el usuario ax04 hacemos un poco de investigación nos daremos cuenta de que en el directorio raíz hay una carpeta llamada BCK la cual dentro contiene un comprimido con el nombre BckAx05.zip
  - Si listamos permisos nos daremos cuenta que con el usuario ax04 podremos descomprimir el archivo para examinarlo, como el archivo cuenta con la extensión .zip descomprimiremos con unzip
  - Unzip BckAx05.zip
  - Si intentamos esto, no nos dejara ya que no podemos escribir en la carpeta actual por lo cual utilizaremos el parámetro -d para indicar la ruta donde queremos descomprimir el archivo
  - Unzip BckAx05.zip -d /home/ax04

- Listaremos el contenido de la carpeta y veremos diferentes extensiones, están puestas para despistar, todo son ficheros de texto plano, por lo cual haremos cat en cada uno de ellos hasta encontrar la flag

- **Ax05 -> Ax06**

  - Al entrar al directorio veremos un fichero, si lo listamos y nos fijamos detalladamente encontraremos una cadena de texto cifrada, esta cadena utiliza un cifrado Cesar, asique no será muy difícil pasarla a un formato legible, para ello utilizaremos el comando Tr
  - Para sacar la cadena de texto usaremos el comando cut con el parámetro -d para indicar el delimitador y -f para sacar el grupo
  - Cut -d "-" -f 2 pr01
- Tr para descodificar -> [Terminar este nivel]

- **Ax06 -> Ax07**

  - Al entrar en el directorio del usuario Ax06 nos daremos cuenta que está vacío, no tenemos ni ficheros ocultos, pero explorando un poco más por el sistema veremos que el directorio /home/ax07 tiene permisos del grupo ax06 por lo cual nosotros con ax06 podremos acceder
  - En ax07 encontramos un Script que cada vez que se ejecuta suma un minuto a un contador, hasta que llega al máximo de tiempo que tiene que trabajar ese usuario y se reinicia, no creo que haya una persona ejecutando el script cada minuto que pasa por lo cual tendrá una tarea programada que se ejecute a cada minuto
  - El usuario ax06 tiene permisos para manipular este script por lo cual si podemos editarlo y el crontab está programado como el usuario ax07 podremos realizar consultas como si fuéramos el usuario ax07
  - Si nos fijamos también contamos con una carpeta llamada private, a la cual no podremos acceder, pero podríamos listar el contenido mediante el script
  - Este Script contiene un fallo al intentar trabajar todo el rato con el mismo fichero, mirar video de s4vitar para arreglarlo
  - Podríamos inyectar en el siguiente script el comando **cat mypassword > contador2**
  - Donde lo que estamos haciendo es mostrar el fichero y redirigirlo a un fichero donde ax06 tenga permisos de lectura

- **Ax07 -> Ax08**

    - En ax07 encontraremos un script llamado Seguridad, parece que este script tiene algo oculto en él, si nos fijamos en el titulo veremos lo que aparentemente es la versión del programa, en realidad son los pasos que tenemos que seguir
    - 1- Al generar contraseñas si nos fijamos hay una contraseña que siempre es la misma, nos quedaremos con ella
    - 2-En el generador de pings pasa justamente lo mismo en el apartado mixto, hay un ping que siempre es igual, juntaremos la contraseña y el ping para crear una misma cadena
    - NOTA -> Podemos ver cómo está montado este script, lo cual nos ayudara a entender muchas cosas e incluso crear nuestras propias acciones aparte para agilizar el proceso
    - 4- Decodificamos la cadena que hemos sacado extendiendo la contraseña con el ping
    - Desciframos la cadena con un cifrado cesar
    - Comprobamos el checksum de la respuesta la cual será la flag para el user ax08

- **Ax08 -> Ax09**

    - Este ejercicio está en proceso de construcción