PROGRAMACION PARA CIBERSEGURIDAD

MANUAL DE USUARIO

DRA. PERLA MARLENE VIERA GONZALEZ

DESCRIPCION Y USO DEL PROYECTO

Este proyecto cuenta con cinco partes de código individuales y funcionales para llevar a cabo la creación de la suite que se necesita. Se explicará parte por parte y al final la función de la suite completa.

Para esto podemos usar el video de apoyo junto con este manual

La primera parte del código que se ha exportado al script principal consiste en extraer el HASH de los archivos que se desea para comprobar que estos no han sido modificados por un externo y para esto, debemos conocer exactamente la ruta en donde se encuentran los archivos de los cuales queremos generar dicho HASH. (Esto se puede hacer colocándose en la carpeta que se desea analizar y en la parte superior donde aparece el nombre damos clic derecho y nos va a permitir copiar la ruta de acceso).

En la segunda parte de las funciones, podemos identificar la práctica de la extracción de metadata de imágenes que se encuentran en una carpeta (no en la red). Para esto, debemos conocer la ruta de donde se encuentran las imágenes de las que deseamos conocer sus datos y esto se puede hacer colocándose en la carpeta que se desea analizar y en la parte superior donde aparece el nombre damos clic derecho y nos va a permitir copiar la ruta de acceso. Esta función nos permite leer cosas sensibles de las fotos como la ubicación de donde fueron tomadas, el modelo de dispositivo que la tomo, las modificaciones que se le hacen a las fotos, fechas, autores y de más informacion que podría ser sensible dependiendo del caso en el que se aplique.

La tercera parte de este proyecto consiste en el escaneo de nmap, esta función nos permite ver el estado de los puertos, así como cuáles de ellos están abiertos y que otros dispositivos están conectados a la ip del Router que sea ingresada para comenzar el proceso. Para esto se debe conocer la ip de puerta de enlace predeterminada, está la podemos obtener fácilmente entrando a la terminal CMD o GIT Bash y ejecutando el comando “ipconfig” y nuestra ip debería aparecer debajo de la opción que dice “mascara de subred” es decir, debe ser la última ip listada en los resultados. Después de eso la copiamos y la ingresamos en la terminal junto con el nombre del archivo, en este caso PCS_PIA.py –N –GWI y la ip que copiamos un momento atrás.

La cuarta parte nos ayuda a identificar el estado de nuestro firewall para así cambiarlo a como el usuario dicte utilizando los comandos necesarios y se ejecuta la opción de cambiar el modo público a privado o privado a público del firewall. (-f public o –f private).

En la quinta parte de este proyecto se nos permite ingresar la ip (puede ser con la técnica que hemos usado antes de conseguir la ip) está la podemos obtener fácilmente entrando a la terminal CMD o GIT Bash y ejecutando el comando “ipconfig” y nuestra ip debería aparecer debajo de la opción que dice “mascara de subred” es decir, debe ser la última ip listada en los resultados. Después de eso, la ejecución de esta parte del código nos va a permitir identificar y analizar los dominios de la ip. Esto nos facilita la identificación y listado de los servidores DNS y la operación de los mismos en la ip deseada.

En la sexta y última parte de este proyecto vamos a analizar más de cerca la práctica de envío de correos. Esta parte en el código se nos permite generar los parámetros que van a determinar la función de nuestro código, es decir, nosotros vamos a decidir qué es lo que se muestra en el correo que va a ser enviado al final del proceso. Vamos a crear un servidor con las credenciales que se necesiten para dicho proceso, es decir, un usuario, una contraseña, un cuerpo, un asunto y a quien va dirigido lo que estamos notificando. En caso de querer adjuntar algún archivo junto con el mensaje, podemos utilizar la técnica que vimos anteriormente que se puede hacer colocándose en la carpeta que se desea analizar y en la parte superior donde aparece el nombre damos clic derecho y nos va a permitir copiar la ruta de acceso para que el archivo se una al correo que se va a enviar. Si el proceso y las credenciales se han llenado correctamente entonces podremos comprobar en la cuenta de correo a la que se ha enviado dicho mensaje que ha procedido con éxito.

Antes de ejecutar el código completo, nuestro script se encarga de verificar que el usuario cuenta con los requerimientos necesarios para poder proceder con las demás fases. En caso de que se incumpla con alguno de los requerimientos, al detectarse se procede a la instalación del mismo para que la ejecución del código no presente fallas al momento de ser usada tipo suite. Es capaz de ejecutar todas las partes individuales (los códigos individuales importados a un solo script final) en una sola para no tener que recurrir a los códigos individuales.

Si todo se ha hecho de forma correcta, ¡el código procederá exitosamente!