

Universidad Autónoma de Nuevo León

Facultad de Ciencias Fisco Matemáticas

Programación para Ciberseguridad

**E1 – Lectura de Scripts**

Dra. Perla Marlene Viera González

Emiliano leal Campos

Grupo: 062 Matricula: 1896372

E-manuel Manzanarez Mora

Grupo: 062 Matricula: 1948116

MTY. N.L. a 16 de septiembre de 2021

**SET (Social-Engineer-ToolKit)**

**versión 8.0.3**

**Módulos**:

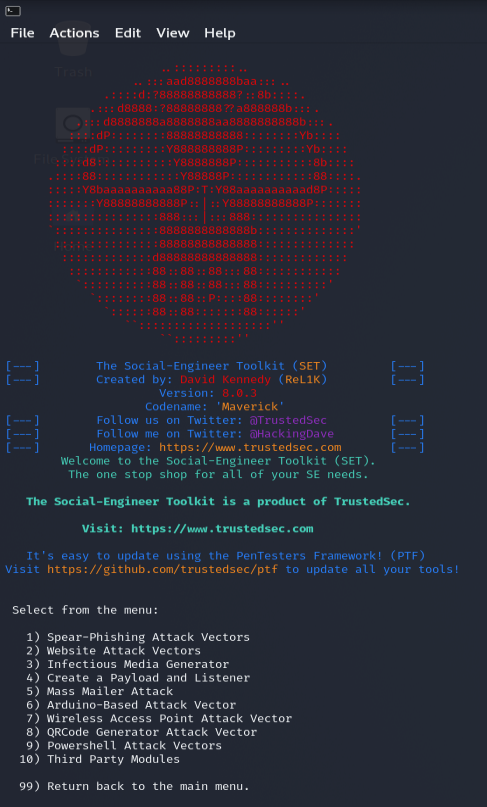
1. os
2. re
3. shutil
4. subprocess
5. sys
6. time
7. socket
8. scr.core.setcore (\*)
9. scr.core.setcore (text)
10. smtplib
11. getpass
12. glob
13. random
14. pexpect
15. base64
16. \_thread
17. cStringIO(StringIO)
18. io(StringIO)
19. email.mime.multipart(MIMEMultipart)
20. email.mime.base(MIMEBase)
21. email.mime.text(MIMEText)
22. email.headre(Header)
23. email.generator(Generator)
24. email.charset(Charset)
25. email.encoders(Enconders)

**Instrucciones y Descripción SET**

Social-Engineer Toolkit es un marco de pruebas de penetración de código abierto diseñado para la ingeniería social. SET tiene varios vectores de ataque personalizados que le permiten realizar un ataque creíble rápidamente, la herramienta completa contiene muchas funciones .



Al correr el programa lo primero que nos aparecerá será un menú, con 7 opciones a elegir, la primera opción que elegiremos será la 1, esta opción nos desplegará lo siguiente:



Como nos podemos dar cuenta en la imagen, nos despliega otro menú, este, menú con 11 opciones.

La primera opción que es spear phishing attack vectors, lo que hace es lo que dice el nombre un ataque de phishing por correo por el método de ataque de vectores.

La opción número 2, WebSite Attack Vectores, como su nombre también lo dice es un ataque a sitios de internet por el método de ataque de vectores.

La opción número 3, Infections Media Generator, este tipo de ataque permite al probador de penetración crear un USB, DVD o CD con contenido malicioso. Cuando el usuario desprevenido abra el archivo, la carga útil se ejecutará y devolverá un shell.

La opción número 4, Create a Payload and Listener. Se utiliza para crear una carga útil ejecutable y un oyente, lo que hace es crear un archivo ejecutable que puede realizar una serie de acciones maliciosas definidas en la computadora de la víctima. El oyente se utiliza para monitorear o controlar las actividades del ejecutable en la computadora de la víctima. Sin embargo, un atacante tiene que colocar físicamente este ejecutable en la máquina de la víctima y ejecutarlo.

La opción 5, Mass Mailer Attack, el fragmento de explicación que daremos del código, en esta opción el ejecutarla, nos dará a elegir, si queremos enviar masivamente este correo o solo a una persona, al elegir a una sola persona, te preguntara su correo, luego te preguntara si quieres usar tu cuenta de correo electrónico para enviar este correo o un servidor propio, al elegir usar nuestro propio correo, nos preguntara nuestro correo eléctrico, al ingresarlo nos preguntara que nombre queremos que salga en el correo, podemos ingresar el que nosotros queramos, te preguntara la contraseña de tu correo, al ingresar la contraseña también nos preguntara si queremos adjuntar un archivo, o si queremos adjuntar un archivo en una línea, luego de todo esto nos preguntará que llevara el Email que enviaremos, y si al inicio elegimos la opción 2, un correo masivo, nos pedirá la dirección del archivo donde tendremos todos los correos a donde enviaremos el Email.

La opción 6, Arduino-Based Arrack Vectors, este vector de ataque generará automáticamente el código necesario para implementar la carga útil en el sistema por usted. Este vector de ataque creará los archivos. pde necesarios para importar a Arduino.

La opción 7, Wirless Access point attack vector, creará un punto de acceso falso aprovechando su tarjeta inalámbrica y le redirigirá todas las consultas de DNS. SET creará un punto de acceso inalámbrico, un servidor DHCP y un DNS falso para redirigir el tráfico a la máquina atacante.

La opción 8, QRCode Attack Vector creará un QRCode para usted con la URL que desee.

La opción 9, PowerShell Attack Vectors, permite crear ataques específicos de PowerShell. Estos ataques le permitirán utilizar PowerShell, que está disponible de forma predeterminada en todos los sistemas operativos Windows Vista y superiores. PowerShell proporciona un panorama fructífero para implementar cargas útiles y realizar funciones que no se activan con tecnologías preventivas.

La opción 10, third party module, es para que ingreses cualquier código escrito por un tercero, puede usarlos para agregar funcionalidad a su código sin tener que escribirlo usted mismo.

La opción 99 te regresara al menú principal.

Regresando al primer menú, ya vimos la primera opción llamada Social-Engineering Attacks, ahora veremos la opción de Penetration Testing (Fast-Track), lo que hace es como dice su nombre es una evaluación de seguridad ejecutada exactamente como lo haría un atacante real y tendrá varias opciones para la herramienta. Una de las opciones de interés es la opción para Powershell.

La tercera opción del menú principal es third party module, es para que ingreses cualquier código escrito por un tercero, puede usarlos para agregar funcionalidad a su código sin tener que escribirlo usted mismo.

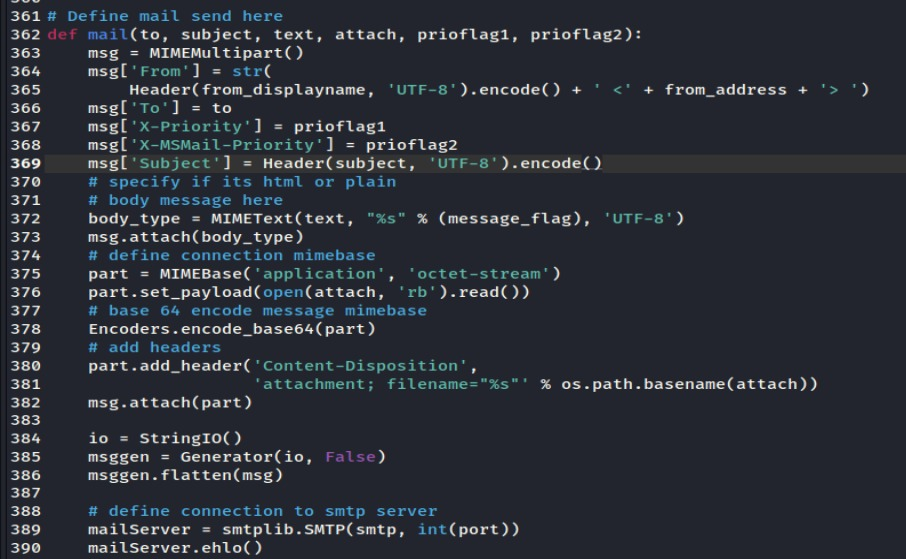
La cuarta opción es para actualizar SET.

La quinta opción es para actualizar la configuración de SET.

La sexta opción es para ayuda, te imprime los créditos y sobre SET

La opción 99 es para salir del programa

**Explicación fragmento del código**



La imagen anterior representa un fragmento del extenso código de set donde se define el cuerpo y se genera la conexión para mandar un email falso.

En la primera línea se puede ver como se define una función llamada “mail” la cual recibe distintos argumentos (to, subject, text, attach, prioflag1, prioflag2)

Después de eso se puede ver como se crea la variable “msg y le dan el valor de MIMEMultipart () esto hace referencia al módulo email.mime el cual obtiene una estructura de texto y le da la forma de un email valido pasandolo por un analizador de texto

Se les da el valor a algunos parámetros de la variable “msg” tales como las prioridades del email, a quien va dirigido y el asunto del correo, todo eso se nos pide anteriormente

Después genera el cuerpo del email con la subclase MIMEMessage, el cual recibe los parámetros de texto el cual se había pedio antes, después de define si el cuerpo será con un templete de HTML o será texto plano y al final se define con una codificación de texto UTF-8

después se hace la conexión con MIMEBASE dándole los parámetros de ('application', 'octetstream') el cual hace referencia a que será un archivo binario que será leído por una aplicación analizadora de texto, después se hace el set\_payload el cual se encargara de realizar la codificación de los datos para el trasporte, abriendo de forma binaria el cuerpo de texto que antes habíamos definido, y posteriormente se hace una codificación de base64

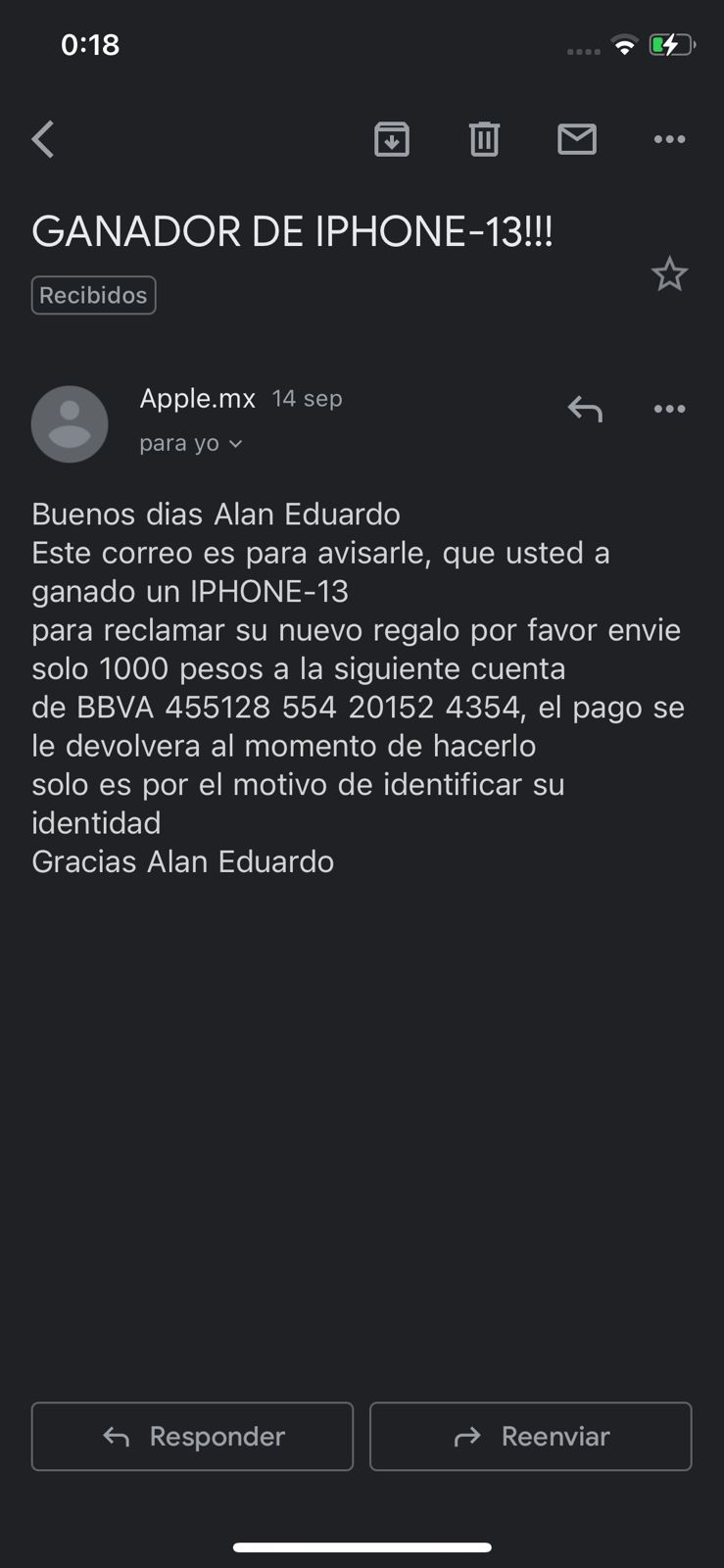
Se agrega el encabezado al correo con la función add.header obteniéndolo del método “os.path.basename(attach))” el cual obtiene el nombre de una dada

después de todo lo anterior se procede a generar el email con distintos métodos, siendo el primero el de StringIO() se inicializa como un constructor de strings, después se hace el generador del mensaje como el método (generator) y por último usamos la función flattern() para convertir una matriz en una lista

Y por último definimos la conexión con el servidor smtp

Se crea un pequeño servidor local de correos con el protocolo stmp usando el método smtplib.stmp donde defines que usará el protocolo stmp y será enviado por puerto que por default es el 25, y después se identifica en el servidor usando el argumento predeterminado que es “host”

**PUEBAS DE FUNCIONAMIENTO**

****

