الملحق العملي لكتاب مقرر

برمجيات وتطبيقات أمن المعلومات (1272)

المحتويات :

1- التعرف على نظام kali linux

2- تنزيل وتنصيب kali linux

3- التعرف على الوظائف الأساسية لبعض من أشهر الأدوات

4- اختبار اختراق تطبيقات الويب في نظام الـ kali

- **websScarb proxy**
- **sqlninja**
- **websploit framework**
- **Burp Suite**

5- طرق وأدوات Exploitation

- **Social Engineer Tool kit**

التعرف على نظام kali linux

ما هو نظام Kali Linux ؟

قبل الدخول في النظام kali Linux , يجب أن نعرف ما هو إختبار الاختراق . اختبار الاختراق هو طريقة من أجل تقييم النظام الامني للنظام الحاسوبي أو الشبكة الحاسوبية. الفكرة وراء إختبار الاختراق هي إستهداف الحواسيب عبر مجموعة من الهجمات لرؤية فيما إذا كان الحاسوب قادر على التعامل مع هذه الهجمات بدون أي تأثير على أداءه، فالهجمات المختلفة في إختبار الاختراق تتضمن تحديد واستغلال نقاط الضعف المعروفة في مختلف التطبيقات البرمجية وأنظمة التشغيلية وتحديد قوة الاتصال في الشبكة وغيرها .

بالنسبة لاختبار الاختراق يعتبر Kali Linux أفضل نظام تشغيل للمحترفين . حيث أن Kali نظام تشغيل متطور مبني على أساس نظام Linux مع مجموعة من البرمجيات مفتوحة المصدر التي تستخدم لتنفيذ العديد من المهام في إختبار الاختراق و علوم الحواسيب والمجال الأمني وفيما يلي بعض ميزاته :

1- **يحوي الكثير من أدوات الاختراق والتقديرات الأمنية .**
2- **يدعم العديد من التجهيزات الخارجية مثل مستقبلات اللاسلكية وتجهيزات PCI .**
3- **يؤمن بيئة متكاملة للتطوير بعدة لغات برمجة مثل Ruby , Python , C .**
4- **نظام مفتوح المصدر وقابل للتطوير.**

Kali يمكن تنزيله على شكل ISO والتي يمكن إستخدامها إما كـ live أو نظام مستقل .

تنزيل وتنصيب kali linux

للبدء في عملية التنصيب، نحتاج أولا تنزيل النظام وهو متوفر بالأشكال التالية :-

1- **ISO**
2- **Vmware images**
3- **ARM images**

يمكن تنصيب نظام Kali كنظام ثاني على الحاسوب أو كبيئة افتراضية ، لنبدأ بعملية التنصيب بجانب نظام تشغيل اخر وذلك من خلال ثلاث خطوات بسيطة يمكن تنصيب النظام الى جانب نظامك الحالي كما يلي :-

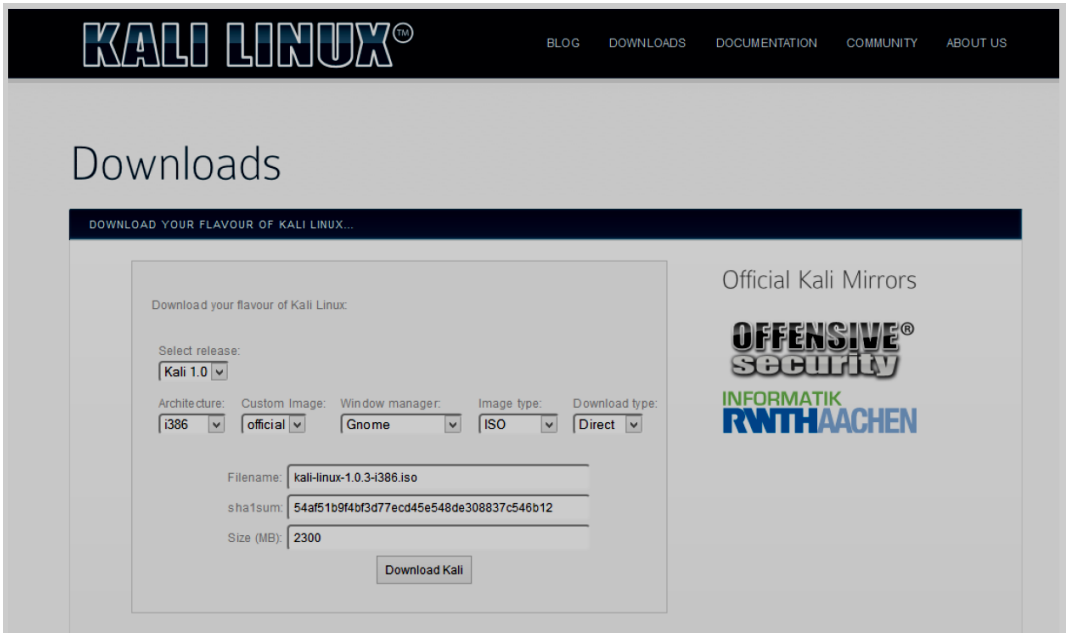
الخطوة الأولى : التنزيل والإقلاع

قبل تنصيب Kali سوف نحتاج إلى المواصفات التالية:

1- **مساحة فارغة على القرص الصلب 12 GB.**
2- **2 GB من RAM على الأقل**
3- **أداة للإقلاع مثل قرص ليزري أو فلاشة USB.**
4- **برنامج لحرق الأقراص الليزرية أو برنامج لجعل الفلاشات إقلاعية.**

يمكن تنزيل ISO من الموقع الرسمي http://www.kali.org/download.

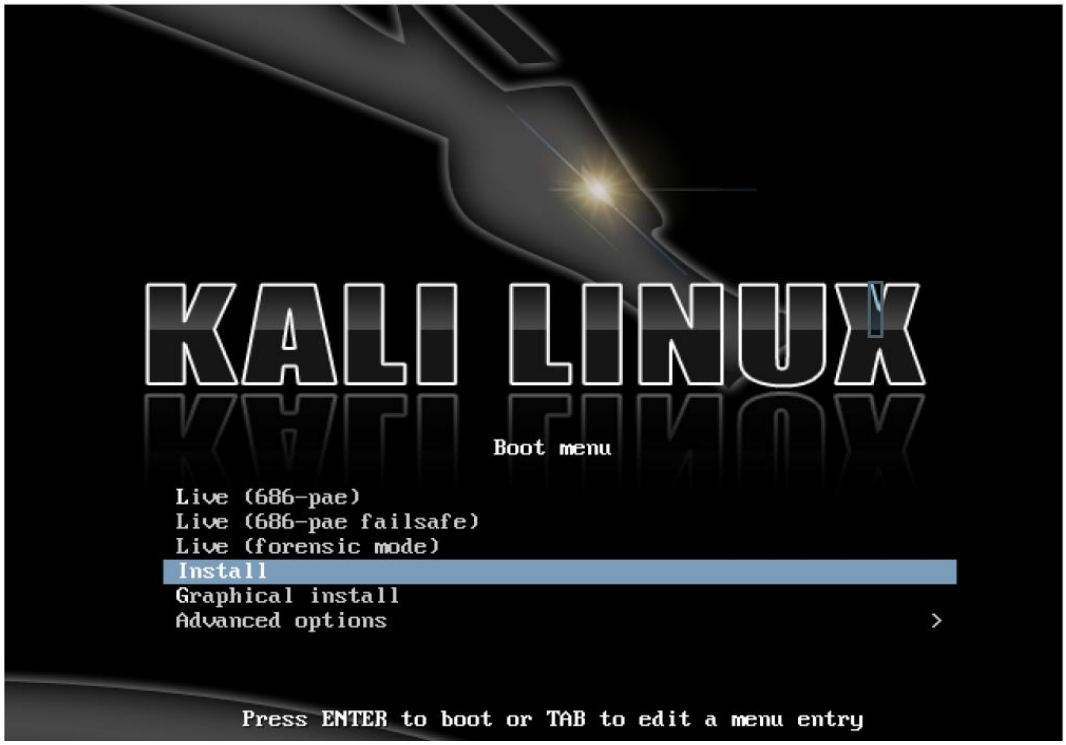
سوف يتم سؤالك فيما إذا كنت تريد أن تسجل اسم و بريد إلكتروني. صفحة التنزيل تحوي خيارات قليلة مثل شكل و بنية النظام. إختر القيمة المتوافقة مع نظامك الحالي.



وبعد الانتهاء من عملية التنزيل يجب أن يتم حفظه على قرص قابل للإزالة ، بحيث يكون هذا القرص معد ليتم إقلاع النظام وتحميل الإعدادات منه .

الخطوة الثانية : إعدادات الإقلاع بجانب نظام آخر

من خلال القرص الذي قمنا بإعداده نقوم بإعادة الإقلاع للنظام مرة أخرى وسوف تظهر لنا الشاشة التالية :-



وسنختار Live boot وسوف يبدأ النظام بالتحميل ويظهر لنا سطح المكتب للنظام Kali .
وبمجرد تحميل سطح المكتب ، نتمكن من الدخول إلى التطبيقات و أدوات النظام ومحرر التقسيم والإدارة وهذا يمثل واجهة المستخدم الرسومية الخاصة بتقسيم النظام الحالي.

مع مراعاة ترك مساحة كافية لتنصيب نظام Kali وعند تحديد حجم القرص الصلب نختار .Apply All Operations ومن ثم نخرج من Gparted ونعيد إقلاع النظام Kali

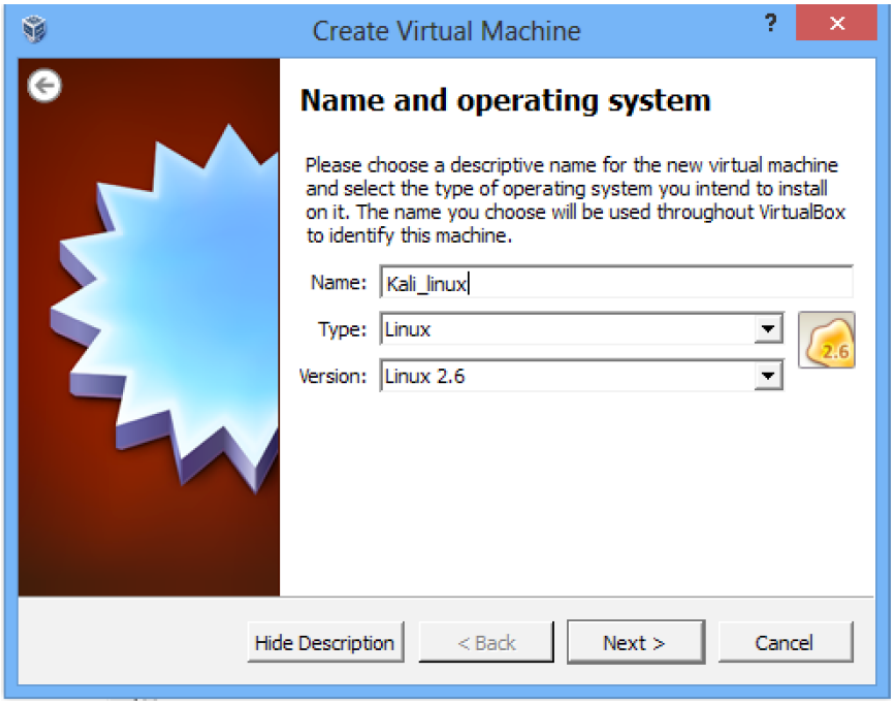
الخطوة الثالثة – بدأ عملية التنصيب

بعد العودة الى الشاشة الرئيسية نختار Graphical install وفي الخطوات الأولى من التنصيب سوف نقوم بتحديد اللغة ، الموقع ، لوحة المفاتيح و هكذا ... ويجب الانتباه عند ضبط كلمة المرور الخاصة بالاقلاع فالكلمة الافتراضية لنظام Kali هي toor .
والخطوات التالية للتنصيب هو اختيار الجزء الذي سوف يتم تنصيب النظام فيه. وسوف نستخدم نفس المساحة غير المستخدمة التي قمنا بتحديدها سابقا ضمن Gparted .
بعد إختيار الجزء، سوف يبدأ النظام في عملية تنصيب نظام التشغيل. هذه العملية سوف تأخذ بعض الوقت للانتهاء . بعد إنتهاء التنصيب سوف تظهر شاشة البداية والسؤال عن النظام الذي تريد الاقلاع إلى Kali Linux أو النظام الاخر وهذا يدعى بـ dual boot

تنصيب Kali ضمن بيئة إفتراضية

إعداد Kali ضمن برامج البيئة الافتراضية سهل جداً، حيث أن هذا النظام متوفر على شكل Vmware Image التي يمكن تنزيلها من الموقع الرسمي http://www.kali.org/download
وبمجرد تنزيله يمكن بداية التعامل معه بشكل مباشرة .
من أجل تشغيل Kali Linux بإستخدام برنامج Virtual Box ،سوف نستخدم ISO التي قمنا بتنزيلها سابقا والإعدادات العادية لـ virtual box .

لبدأ التنصيب، ننشئ بيئة افتراضية و ضبط المتطلبات من مساحة و ذاكرة.



بعد إنشاء بيئة إفتراضية، نقوم بتشغيلها. في أول اقلاع سوف نقوم بإختيار القرص . نختار Kali ISO ونبدأ التنصيب. والخطوات الباقية هي نفس الخطوات السابقة التي قمنا بها عند تنصيب النظام بجانب النظام الاصلي لدينا .

عند إنتهاء التنصيب و تحميل سطح المكتب يمكننا تنصيب VirtualBox guest addition نتبع الخطوات التالية من أجل تحقيق ذلك :-

1- نسخ الملفات للمسار التالي :

```
cp /media/cd-rom/VboxLinuxAdditions.run /root/
```

2- ضبط صلاحيات الملف بالشكل التالي :

```
chmod 755 /root/VboxLinuxAdditions.run
```

3- تنفيذ الامر التالي :

```
./VboxLinuxAdditions.run
```

تحديث Kali Linux

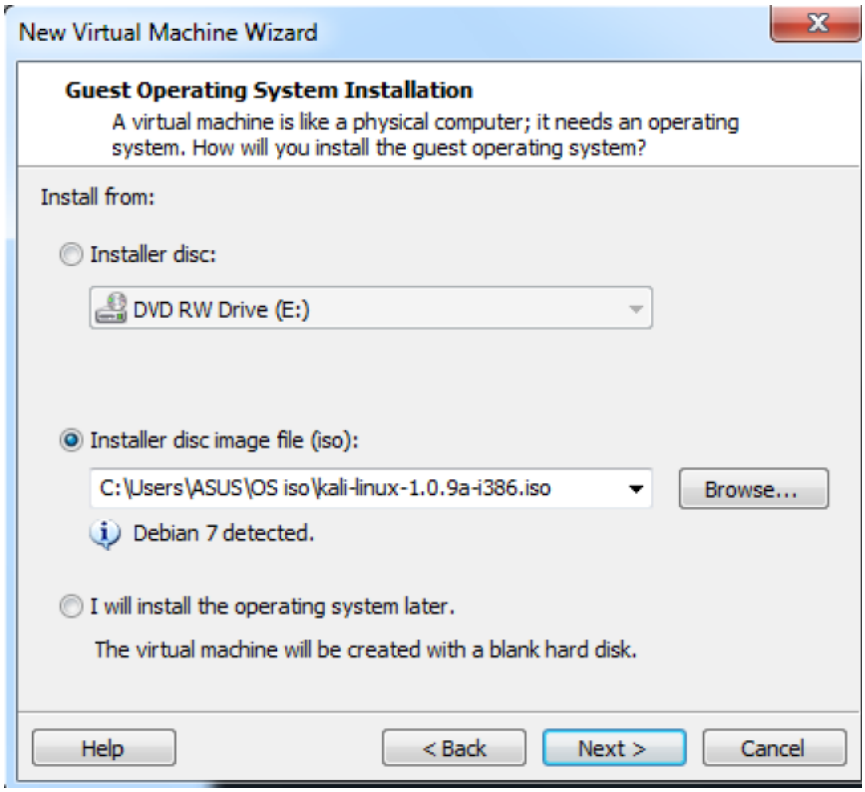
آخر خطوة في عملية التنصيب هي تحديث OS من أجل الحصول على آخر patches .من أجل التأكد من أننا نعمل على آخر إصدار. من أجل تحديث نظام التشغيل ، نقوم بتشغيل terminal و تمرير الأمر التالي :

```
apt-get update
```

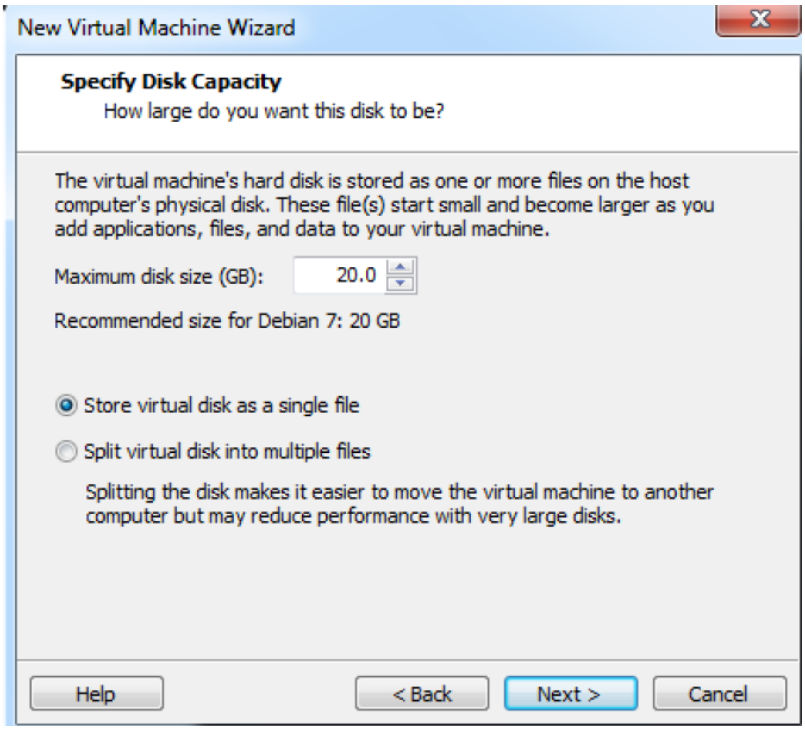
عند هذه النقطة ، نكون قد قمنا بتنصيب نظام Linux Kali و يمكننا أن نستكشف القليل عن هذا النظام

كيفية تنصيب Kali Linux ضمن VMware

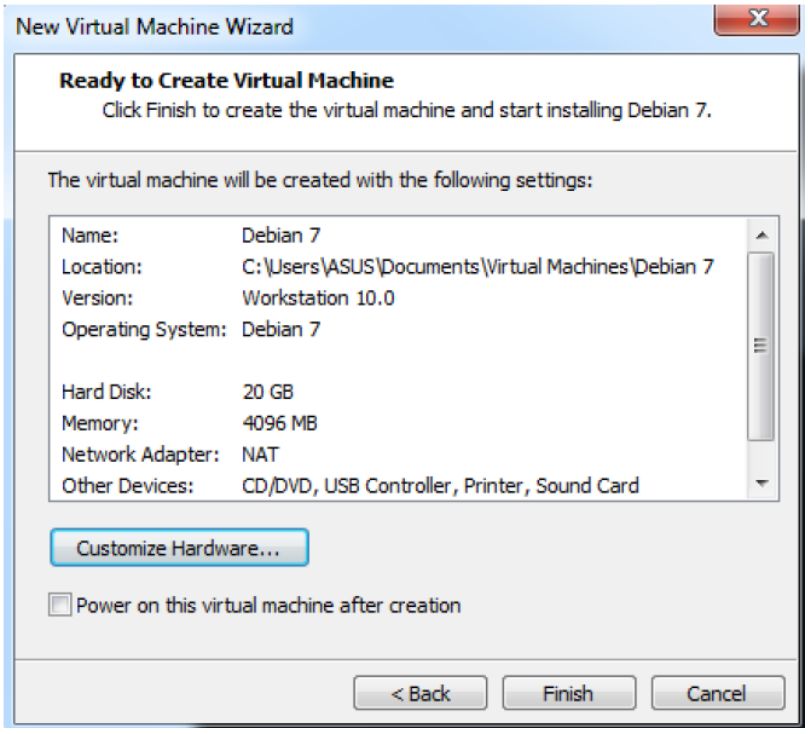
نقوم بتشغيل VMware ومن ثم نختار ملف ISO الذي قمنا بتنزيله من الانترنت كما في الشكل التالي:



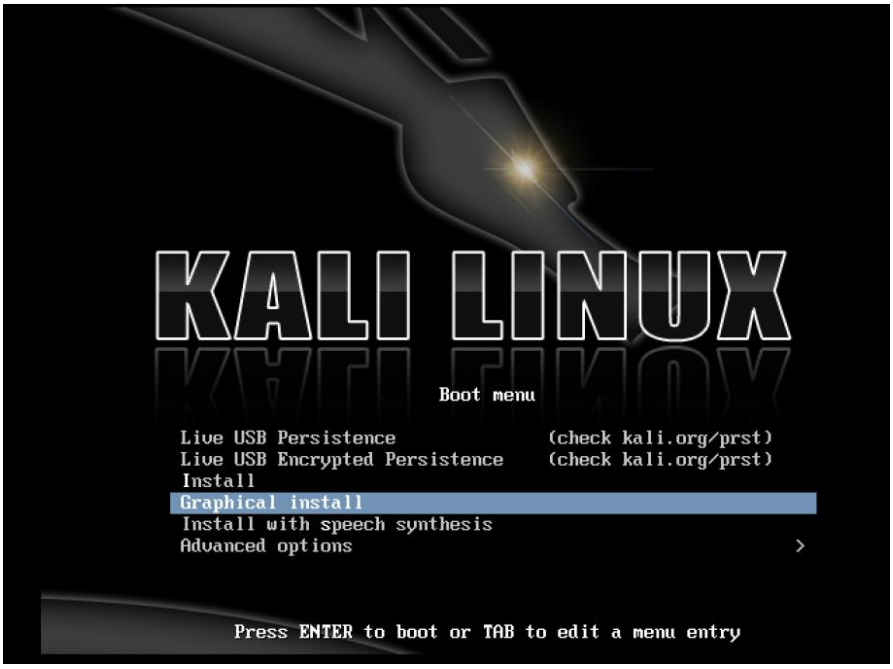
نختار حجم القرص الذي نريد حجزه للنظام :



نحدد الخصائص وبارامترات التي نريد تفعيلها ضمن النظام :



ومن ثم نقوم بتشغيل البيئة الافتراضية للنظام وننتظر حتى ظهور الشاشة الموضحة بالشكل :



الجدول التالي يوضح رقم الشاشة التي ستظهر... وما علينا اختياره في كل شاشة .. وبعد الاختيار المطلوب من كل شاشة نضغط على continue للانتقال للشاشة التالية

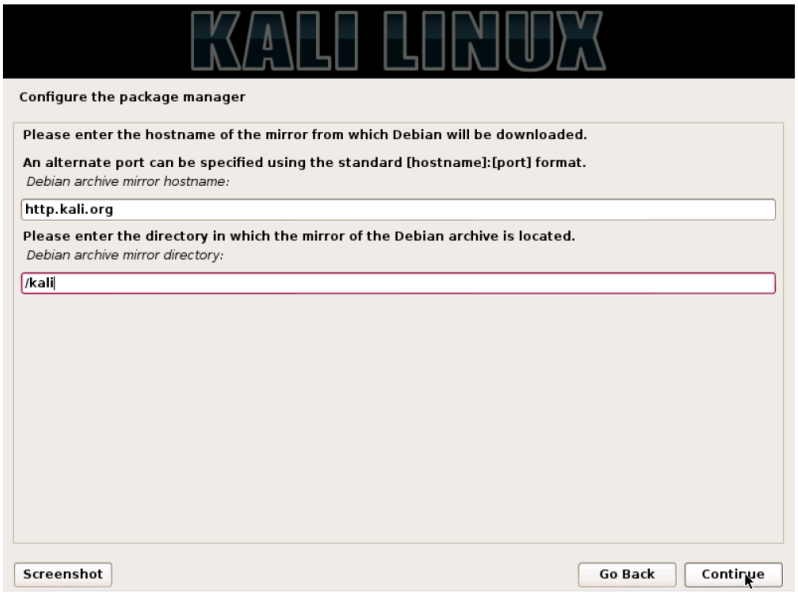
(مع الانتباه للخطوات 5 و 6 لتحديد اسم المستخدم وكلمة المرور)

رقم الشاشة	المطلوب	الاختيار المطلوب
1	Select a language	نختار English (توجد اللغة العربية ولكن يفضل اختيار اللغة الانجليزية)
2	Select your location	نختار United states
3	Configure the keyboard	نختار American English
4	Configure the network	نكتب كلمة kali (للـ host name)
5	Configure the network	نكتب كلمة kali (للـ domain name)
6	Set up users and passwords	نحدد كلمة السر الخاصية بنا ونعمل تأكيد عليها بطباعتها مرة أخرى (ويفضل وضعها toor)
7	Configure the clock	نختار Eastern
8	Partition disks	نختار Guided-use entire disk (للـ Partitioning method)
9	Partition disks	نختار all files in one partition (للـ Partitioning scheme)
10	Partition disks	نختار finish partitioning and write changes to disk
11	Partition disks	نختار yes ... (write the changes to disks)

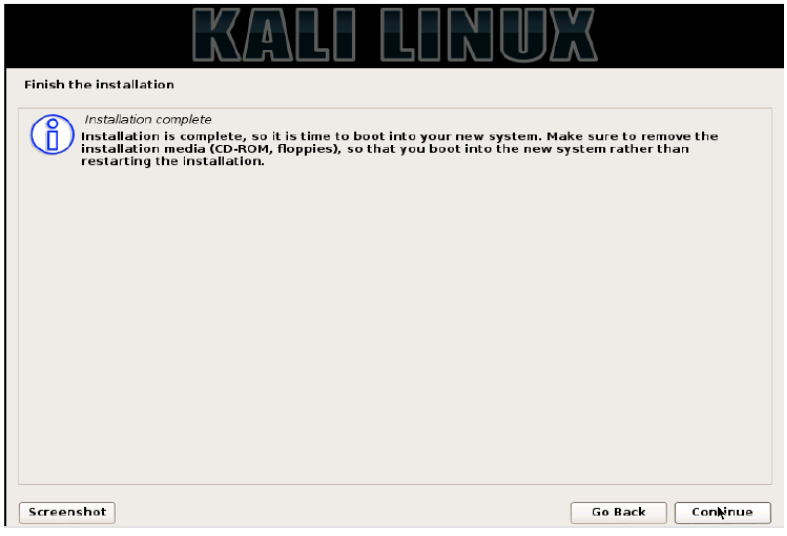
وبعدها تبدأ عملية التنزيل وبعد الانتهاء من التنزيل تظهر مجموعة شاشات علينا اختيار المطلوب منها كما في الجدول أدناه ... وبعدها الضغط على زر continue:-

رقم الشاشة	المطلوب	الاختيار المطلوب
1	Configure the package manager	نختار yes
2	Configure the package manager	(blank for none).... نتركها فارغة بدون تعبئة
3	Configure the package manager	نختار enter information manually

ومن ثم تظهر الشاشات التالية ونعبئ المطلوب كما هو واضح أدناه :

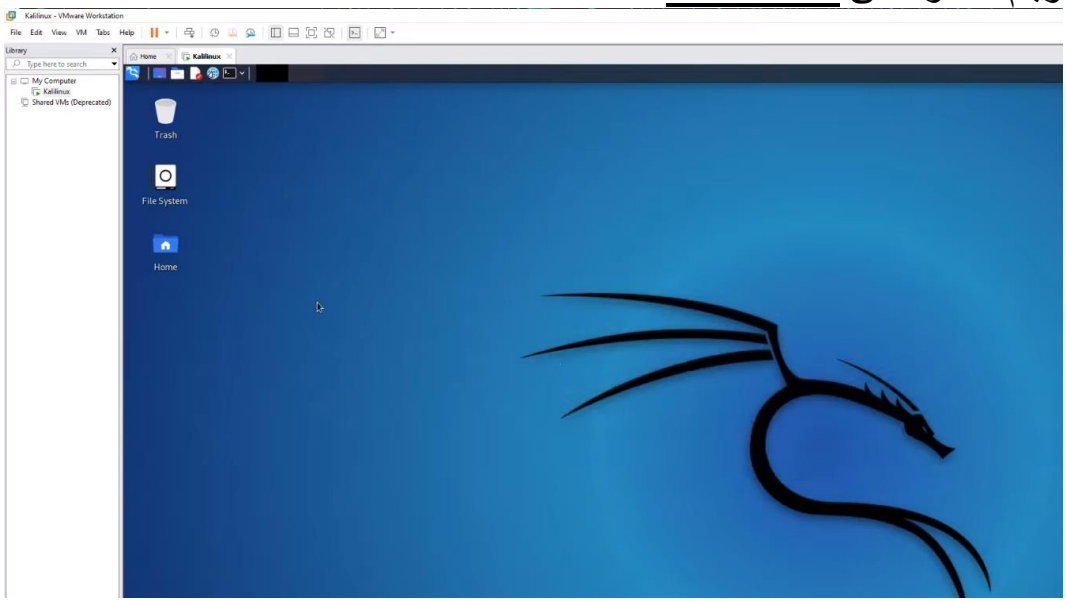


ومن ثم الشاشة التالية



وعند الضغط على continue سيعاد التشغيل وتظهر شاشة تطلب اسم المستخدم (وهي kali كما تم تحديدها أثناء التنزيل) وكلمة السر (وهي toor كما تم تحديدها اثناء التنزيل)

ويتم الدخول الى **Kali Linux**



التعرف على الوظائف الأساسية لبعض من أشهر الأدوات

سوف نبدأ بالتعرف وبشكل بسيط على عالم Kali Linux وفهم الوظائف الأساسية لبعض أشهر الأدوات في هذا النظام. وسوف نبدأ بالمسار الرئيسي أو المجلد الرئيسي المستخدم في النظام Kali.

ـ تقسيم الذاكرة

يتبع نظام Kali نفس المسار الأساسي الموجود في Ubuntu Linux. وفيما يلي بعض المسارات المهمة التي يجب معرفتها:

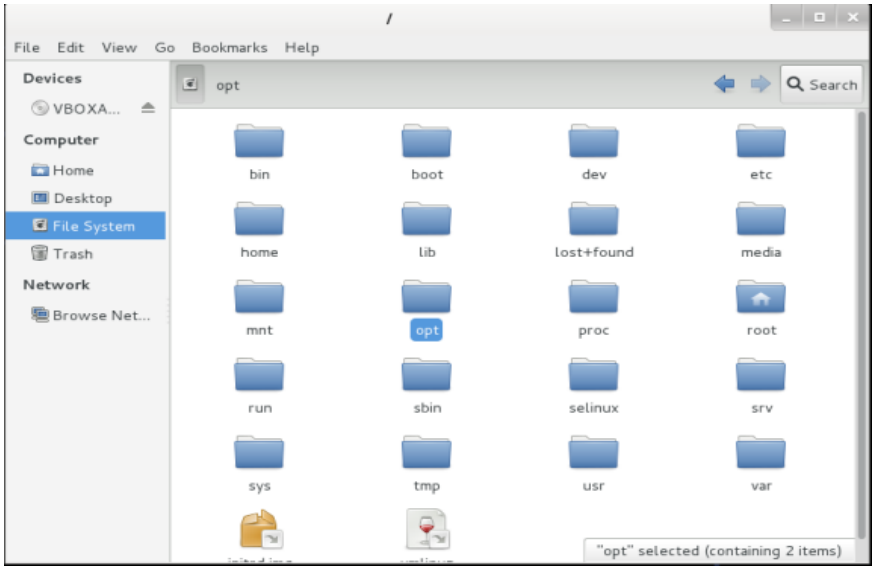
/etc : يحوي ملفات الإعدادات للأدوات المنصبة في النظام.

/opt : يحوي metasploit و موديولاتها.

/sys / : يحوي ملفات الإعدادات للأجهزة الخارجية الموصولة و المنافذ.

/root: مسار أو مجلد المستخدم الأساسي للنظام.

/lib :/ تحوي المكتبات المستقلة عن النظام.



معظم الأدوات و البرمجيات المستخدمة في أختبار و تقدير الأخطار يمكن الوصول لها عبر قائمة التطبيقات على سطح المكتب. وهذه القائمة مرتبة وفق الأدوات الأكثر إستخداماً من أجل الوصول لها ، أبحث في Application | Kali linux.

ـ تجميع و تحصيل المعلومات في نظام Kali Linux

Kali Linux يحوي مجموعة خاصة من الأدوات التي تساعد في عملية تجميع المعلومات مثل :ـ
مثل Nmap (the network port mapper) , Trace , DNSmap وهي أدوات مهمة. سوف نقوم بتغطية بعض هذه الأدوات من وجهة نظر معينة.

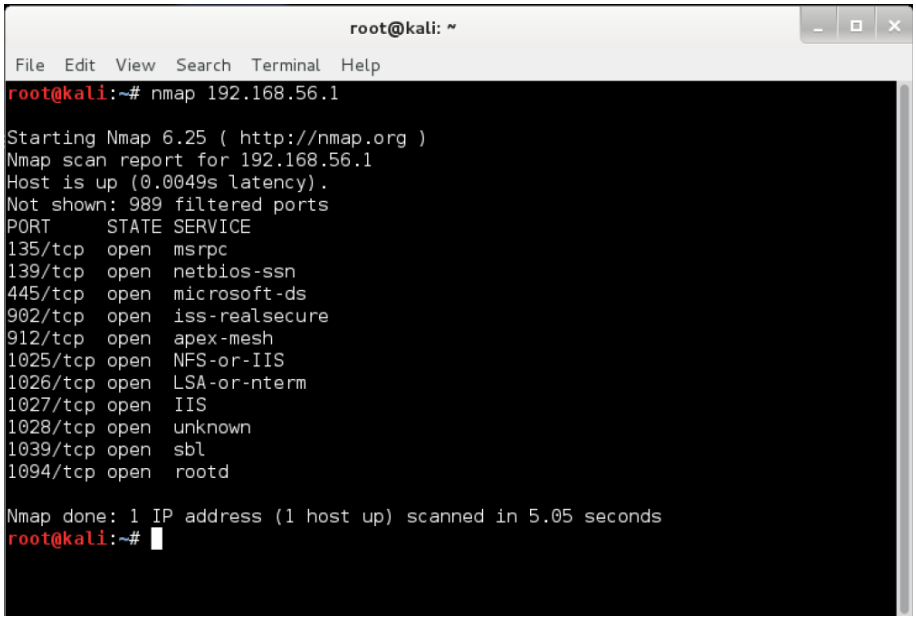
تجميع المعلومات بإستخدام Nmap

تجميع المعلومات يعتبر أول خطوة بإتجاه إختبار الإختراق. في هذه المرحلة سوف نحاول و نجمع أكبر قدر ممكن من المعلومات حول الهدف أو الضحية. Nmap هي الأداة المفضلة للقيام بالمسح و تجميع المعلومات ، ومن أجل تشغيلها نفتح console و نمرر الأمر nmap هذا سوف يعرض لنا العديد من البارامترات والإدخالات التي يمكن إستخدامها في Nmap . دعونا نعمل بعضا منها .

- **لمسح IP واحد، نستخدم الأمر التالي:**

root@kali:~#nmap 192.168.56.1

ومخرجات هذا الأمر موضح بالشكل التالي:



- **لمسح مجال من عناوين IP ضمن شبكة، نستخدم الأمر التالي:**

root@kali:~#nmap 192.168.56.1-255

- **لمسح رقم port محدد عند الهدف ، يتم وفق الأمر:**

root@kali:~#nmap 192.168.56.1 -p 80

- **لمسح مجال من ports في كامل الشبكة نستخدم الأمر:**

root@kali:~#namp 192.168.56.0/24 -p 1-1000

- **من أجل إستثناء host أو أكثر من عملية المسح:**

nmap 192.168.56.0/24 --exclude 192.168.1.5

nmap 192.168.56.0/24 --exclude 192.168.1.5,192.168.1.254

- **لتنفيذ مسح سريع، استخدم الأمر التالي:**

nmap -F 192.168.56.1

- **لمسح معلومات عن نظام التشغيل و نسخته، نستخدم الأمر:**

nmap -A 192.168.56.1

nmap -v -A 192.168.56.1

- **لمعرفة فيما إذا كان الجدار الناري موجود ضمن مجال شبكة أو عناوين IP:**

nmap -sA 192.168.1.254

- **في حال وجود جدار ناري ، Nmap تحوي بارامتر من أجل مسح الهدف والذي يمكن تنفيذه بإستخدام الأمر:**

nmap -PN 192.168.1.1

- **لزيادة الضغط و معرفة فيما إذا كانت كل حزم البيانات أرسلت وأستقبلت، نستخدم الأمرالتالي:**

nmap --packet-trace 192.168.1.1

- **لإكتشاف الخدمات المختلفة التي تعمل على الهدف ، استخدم الأمر التالي:**

nmap -sV 192.168.56.1.

- **لمسح الهدف بإستخدام حزم TCP ACK أو TCP SYN ، نستخدم الأمر التالي:**

nmap -PA 192.168.56.1

nmap -PS 192.168.56.1

- لبدأ مسح سريع و آمن ، سوف نستخدم مسح TCP SYNبإستخدام الأمر التالي:

nmap -sS 192.168.56.1

- لمعرفة خدمات TCP المختلفة التي تعمل عند الضحية، نستخدم مسح إتصالTCP عبرالأمر التالي:

nmap -sT 192.168.56.1

- من أجل مسح UDP نستخدم الأمر:

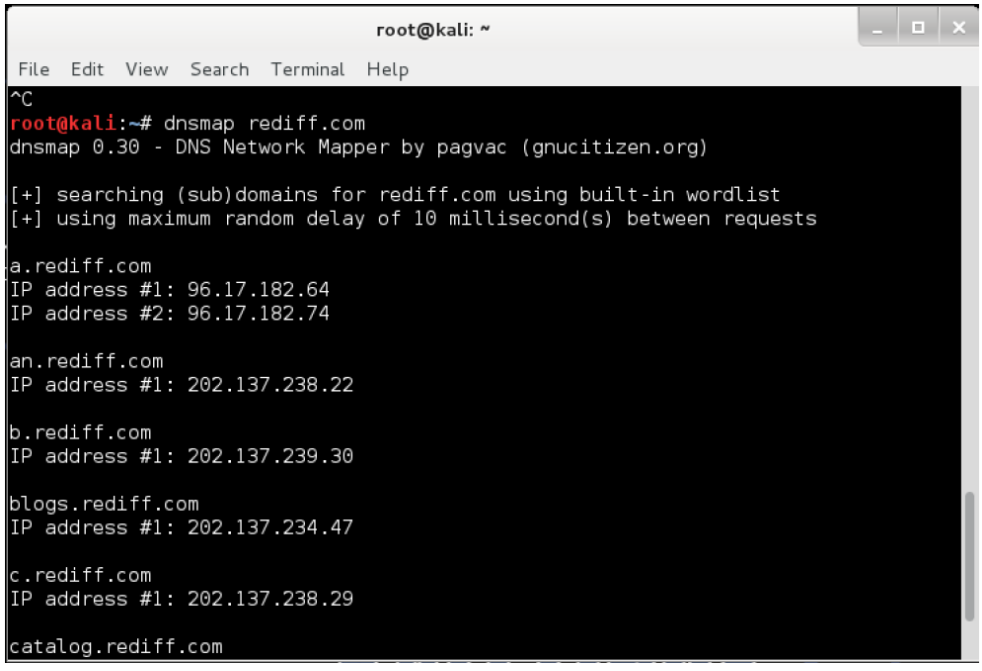
nmap -sU 192.168.56.1

كل نتائج المسح السابق يمكن أن تحفظ ضمن ملف نصي بإستخدام الأمر التالي:
Nmap -sU 192.168.56.1 > scan.txt

هذه كانت مجموعة من الأوامر المهمة عند تجميع المعلومات و المسح .
Nmap تؤمن ميزات الربط بين بارامترات المسح بحيث تصبح أمر مسح واحد من أجل جعل العملية أكثر تقدماً .

- تحليل DNSmap

Domain Name System نظام للخدمات المتصلة بالإنترنت حيث أن اسم domain يستخدم من أجل الدخول لخدمة معينة. مثلا www.Kali.org يستخدم للوصول لخادم HTTP الموجود لدى مؤسس موقع Kali.
أداة DNSmap هي أداة تستخدم لإستكشاف subdomains الموجودة ضمن domain محدد.
تنفيذ الأمر التالي ضمن terminal سوف يرينا كامل خريطة أو شكل DNS لـ www.rediff.com
root@kali:~#dnsmap rediff.com



- أدوات مسح الشبكة

أدوات مسح الشبكة تستخدم لمعرفة تكوين الشبكة خاصة أو عامة و تحصيل معلومات عنها.
Nmap هي أشهر أداة تجميع معلومات وهي أداة قوية تستخدم من أجل مسح الحاسوب أو شبكة الحواسيب بهدف إختبار الإختراق

من أجل إستهداف خدمات معينة بهدف تقوية الهدف وحمايته. عبر تمرير الأمر التالي سوف تظهر لنا قائمة بخيارات المسح المتاحة :
root@kali:~#nmap -h

مسح بسيط عن UDP يتم عبر الأمر التالي:

root@kali:~#nmap -sU 192.168.5.0-255

- إستكشاف live hosts

Fping أداة مشهورة تستخدم من أجل معرفة إذا كان host معين متصل بالشبكة أم لا.

root@kali:~#fping google.com

google.com is live

- تحليل SSL

SSLScan أداة مسح سريعة لمنافذ SSL المتصلة وتحدد فيما إذا كان المشفرات والبروتوكولات مفعلة أم لا وتظهر الشهادة الرقمية لـ SSL.

- إلتقاط معلومات عن الشبكة

Dsniff هي مجموعة من الأدوات التي تقوم بالعديد من المهام لتحصيل المعلومات. هذه الأدوات تعمل عبر مراقبة البيانات التي تمر عبر الشبكة من أجل بيانات مفيدة مثل كلمات مرور، مفاتيح المرسلين وعناوين البريد الإلكتروني. بعض هذه الأدوات تتضمن unlsnarf, WebSpy, mailsnarf وهكذا.
Netsniff مجموعة من الأدوات الشبكية السريعة والقوية المصممة خصيصاً لأنظمة Linux . يمكن إستخدامها في تحليل تطوير الشبكات ، المراقبة ، الفحص وهكذا . Netsniff-ng محلل شبكة سريع يعتمد على مكانيكية حزمة mmap تستطيع إلتقاط ملفات pcap وإعادة عرضها وتنفيذ تحليل بشكل online و offline.

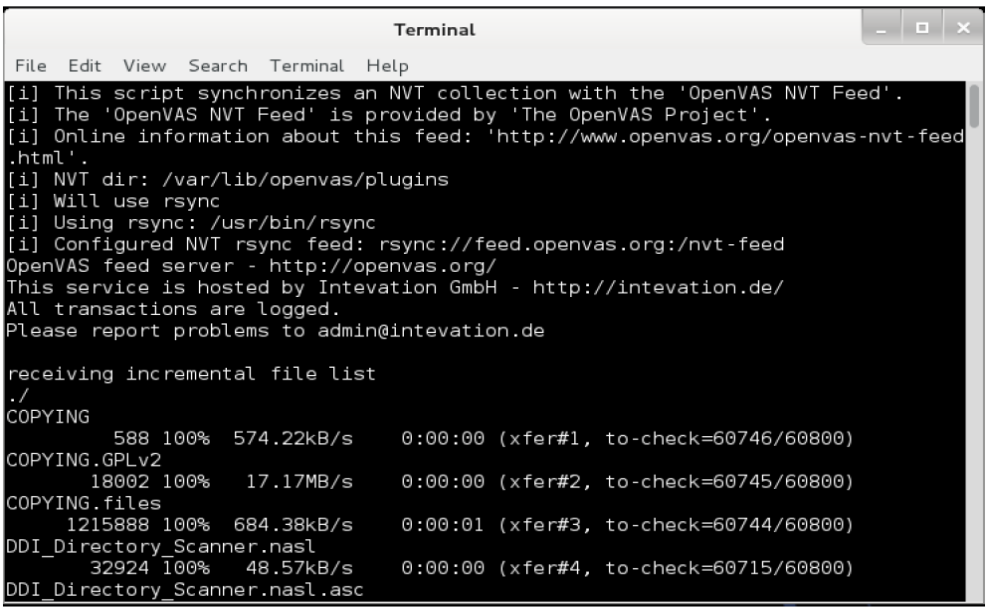
- التعامل مع أدوات البحث عن نقاط الضعف

أدوات البحث عن نقاط الضعف تلعب دور هام في إختبار الإختراق . هذه الأدوات تساعد مختبر الاختراق في عملية تحليل نقاط الضعف و أخطاء النظام. يمكن البحث عن نقاط الضعف على العديد من الخدمات والبرمجيات إعتمادا على المتطلبات.
OpenVAS أداة بحث عن نقاط ضعف مفتوحة المصدر مصممة خصيصاً للبحث العميق عن نقاط الضعف ضمن العديد من الحالات.
لبدء التعامل مع OpenVAS نبحث عن

Application | Kali Linux | Vulnerability Analysis | OpenVAS

عند تشغيلها لأول مرة نستخدم الأمر التالي من أجل تحديث البرنامج و تشغيل كامل ما يلزم لعملها:

openvas-setup



الخطوة التالية هي اضافة مستخدم جديد OpenVAS . نمرر الأمر التالي ضمن terminal:

root@kali:~#openvas-adduser

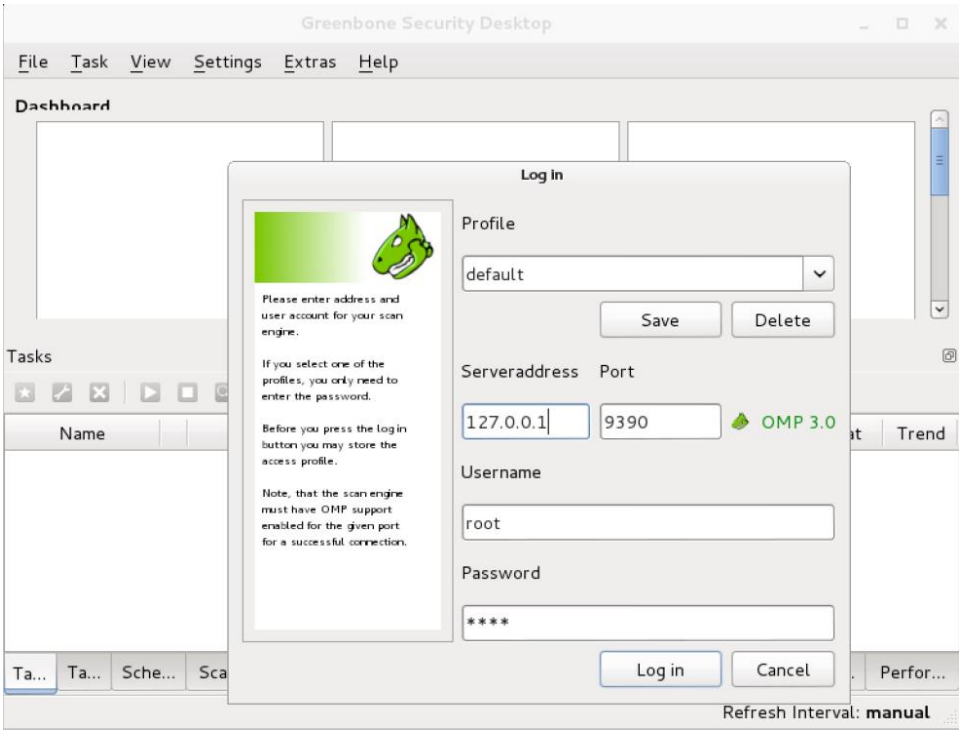
يمكن الخروج من هذه العملية عبر الضغط على ctrl + d ونستطيع إستخدام الأمر التالي من أجل تحديث هذه الأداة بشكل دائم:

root@kali:~#openvas-nvt-sync

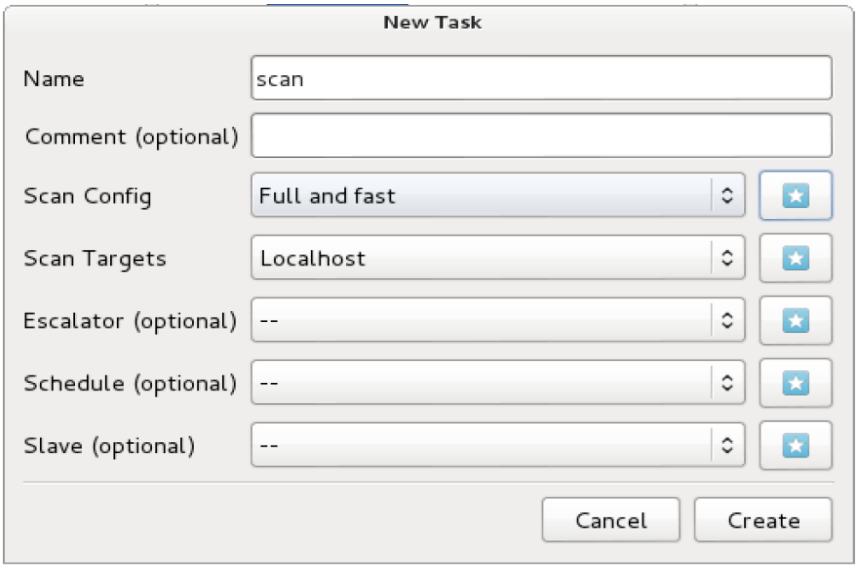
نستطيع الآن تشغيل الأداة و البدء في عملية البحث. ندخل إلى

Application | Kali Linux|Vulnerability Analysis | OpenVAS | openvas-gsd

هذا سوف يشغل الواجهة الرسومية من أجل تسجيل الدخول. نقوم بإدخال المعلومات التي قمنا بإعدادها سابقا و ندخل العنوان المحلي 172.0.0.1 مثلا .



بعد تسجيل الدخول ، نستطيع بدء عملية المسح . للبدء بأول عملية مسح نذهب إلى Task | New. نملأ اسم عملية المسح و باقي المتطلبات كما هو موضح بالشكل التالي:



بعد إنشاء العملية سوف نلاحظ أن العملية سوف تظهر في القسم السفلي من الواجهة الرسومية للمستخدم. ونضغط على زر البدء لبدء المسح.

اختبار اختراق تطبيقات الويب في نظام الـ kali

تطبيقات الويب جزء رئيسي من الأنترنت العالمي هذه الأيام. والحفاظ على الحماية ضمنها هو التركيز الأساسي للدراسات العليا في مجال الويب. بناء تطبيق ويب يمكن أن يكون صعب و يمكن أن تظهر أخطاء صغيرة ضمن التعليمات تؤدي الى حدوث فجوات أمنية. وهنا يأتي دور تطبيقات الويب لتساعد في حماية التطبيقات الأخرى. تطبيقات إختبار إختراق الويب يمكن تطبيقها في العديد من الأماكن مثل الواجهات و قواعد البيانات و خوادم الويب. سوف نستغل قوة بعض الأدوات المهمة في النظام Kali التي ممكن أن تكون مفيدة خلال عملية إختبار إختراق تطبيقات الويب.

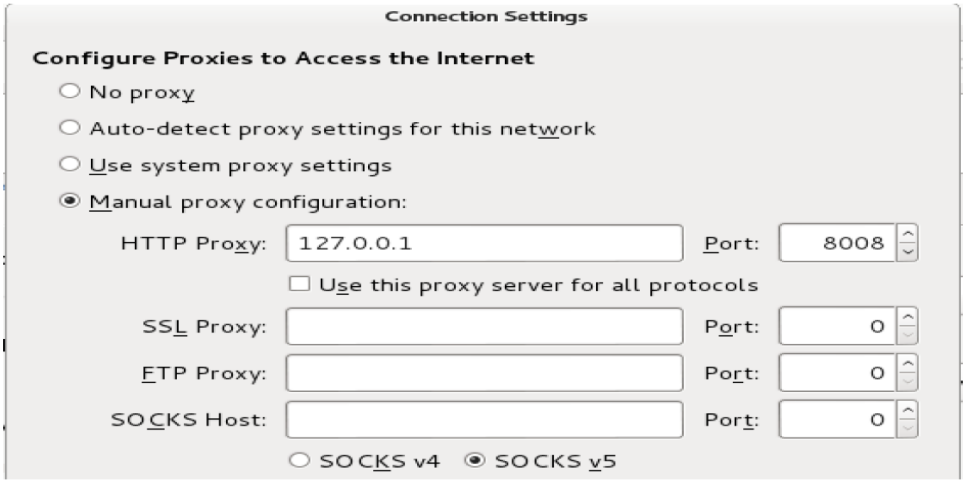
WebScarab proxy

WebScarab هي أداة من أجل مقاطعة طلبات HTTP و HTTPS المرسلة من المتصفح قبل ان يتم إرسالها الى الخادم . وبشكل مشابه يتم وقف الإجابة من الخادم قبل أن تذهب إلى المتصفح. النسخة الجديدة من Webcarab تحوي العديد من الميزات المتقدمة مثل إكتشاف XSS/CSRF و تحليل الرقم المعرف للجلسة . من أجل البدء في التعامل مع WebScarab نتبع الخطوات الثلاثة التالية:

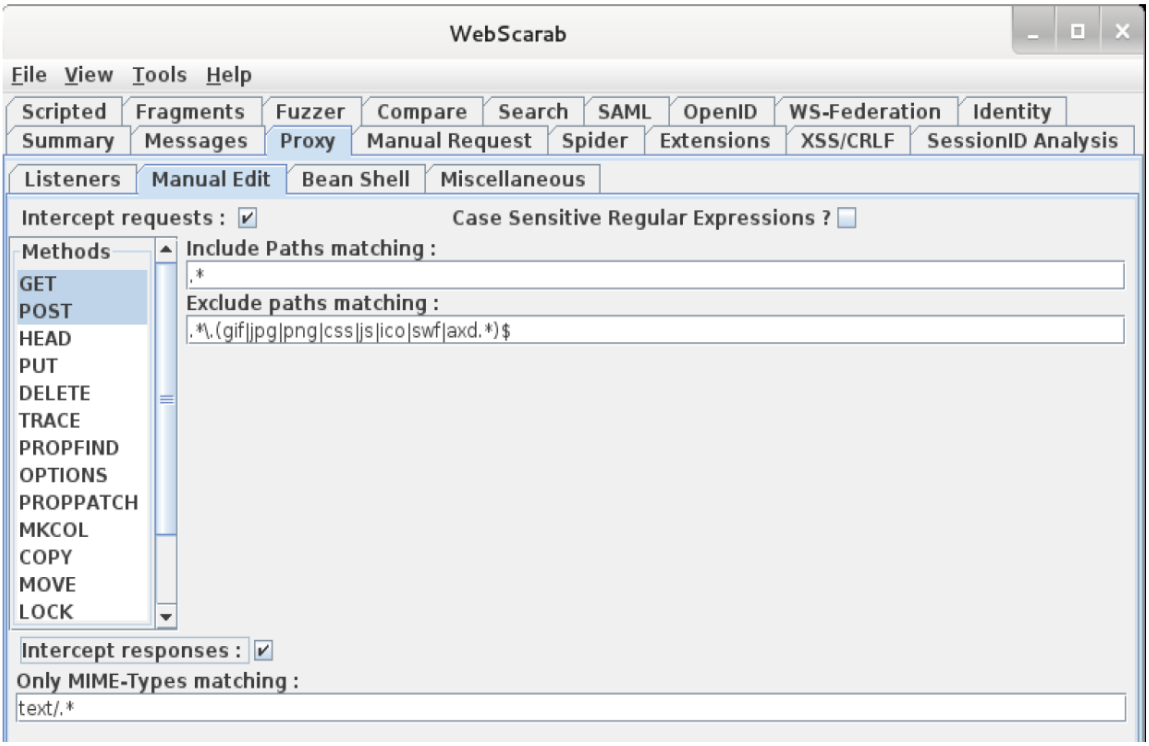
1. **نبدأ Webcarab عبر الذهاب وفق**

Application | Kali Linux | Web applications | Web application proxies | Webscarab

2. **بعد بدء التطبيق يجب علينا تغيير إعدادات المتصفح . نضبط إعدادات الـ 127.0.0.1 و رقم المنفذ على 8008.**



3. **نحفظ الإعدادات و نعود إلى الواجهة الرسومية لـ WebScarab. نضغط على قائمة Proxy ونتفحص طلبات المقاطعة. يجب أن نتأكد أن طلبات GET و POST محددة على الجانب الأيسر من الواجهة من أجل مقاطعة الإستجابة، نتفحص مقاطعة الإستجابة من أجل بدء مراجعة و تفحص طلبات الإستجابة القادمة من الخادم.**



ـ هجمات قواعد البيانات باستخدام sqlninja

Sqlninja أداة مشهورة تستخدم لفحص نقاط الضعف لـ SQL injection في خوادم Microsoft SQL . قواعد البيانات جزء مهم من تطبيقات الويب لذلك حتى تطبيق صغير يمكن أن يؤدي إلى خطأ في إستغلال المعلومات. لذلك دعونا نرى كيف أن sqlninja يمكن أن تستخدم في إختبار إختراق قواعد البيانات.

من أجل إقلاع sql ninja نذهب إلى

Applications | Kali Linux | Web applications | Database Exploitation |sqlninja

هذه الخطوة سوف تؤدي إلى ظهور نافذة terminal مع بارامترات salninja . البارامترات المهمة التي يجب البحث عنها هي mode و m- .

البارامتر m- يحدد نوع العملية التي نريد تنفيذها على قاعدة البيانات الهدف ، دعونا نمرر الأمر الأساسي ونحلل النتيجة:

```
root@kali:~#sqlninja -m test
sqlninja rel. 0.2.3-r1
Copyright (c) 2006-2008 icesurfer
[-] sqlninja.conf does not exist. You want to create it now ? [y/n]
```

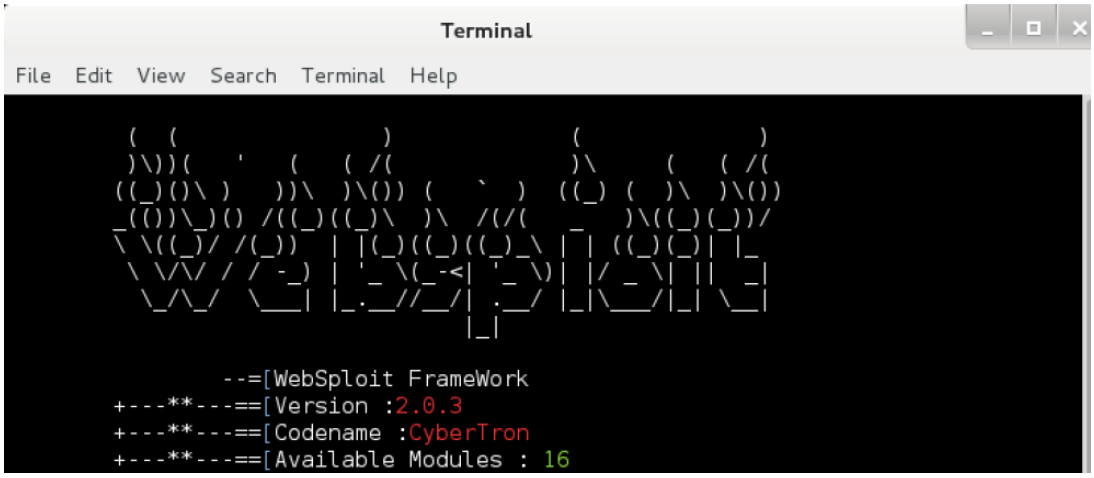
هذا سوف يعطيك خيار لإعداد ملف الإعدادات (salninja.conf). يمكننا تمرير القيم المهمة وإنشاء ملف إعدادات. وبمجرد الإنتهاء من هذا نكون جاهزين لتنفيذ إختبار إختراق قواعد البيانات.

The Websploit framework

Websploit أداة مفتوحة المصدر صممت لتحليل نقاط الضعف وإختبار الإختراق لتطبيقات الويب. وهي مشابهة جدا لـ Metasploit والتعامل مع العديد من البرمجيات لإضافة وظائف إليها.

لنبدأ Websploit نذهب الى

Application | Kali Linux | Web Applications |Web Application Fuzzers | Websploit



يمكن أن نبدأ بتحديث هذه الأداة بتمرير أمر التحديث في الـ terminal وفق التالي:

wsf>update

[*]Updating websploit framework, please wait...

بمجرد إنتهاء التحديث يمكن رؤية الموديولات المتوفرة بتمرير الأمر التالي:

wdf>show modules

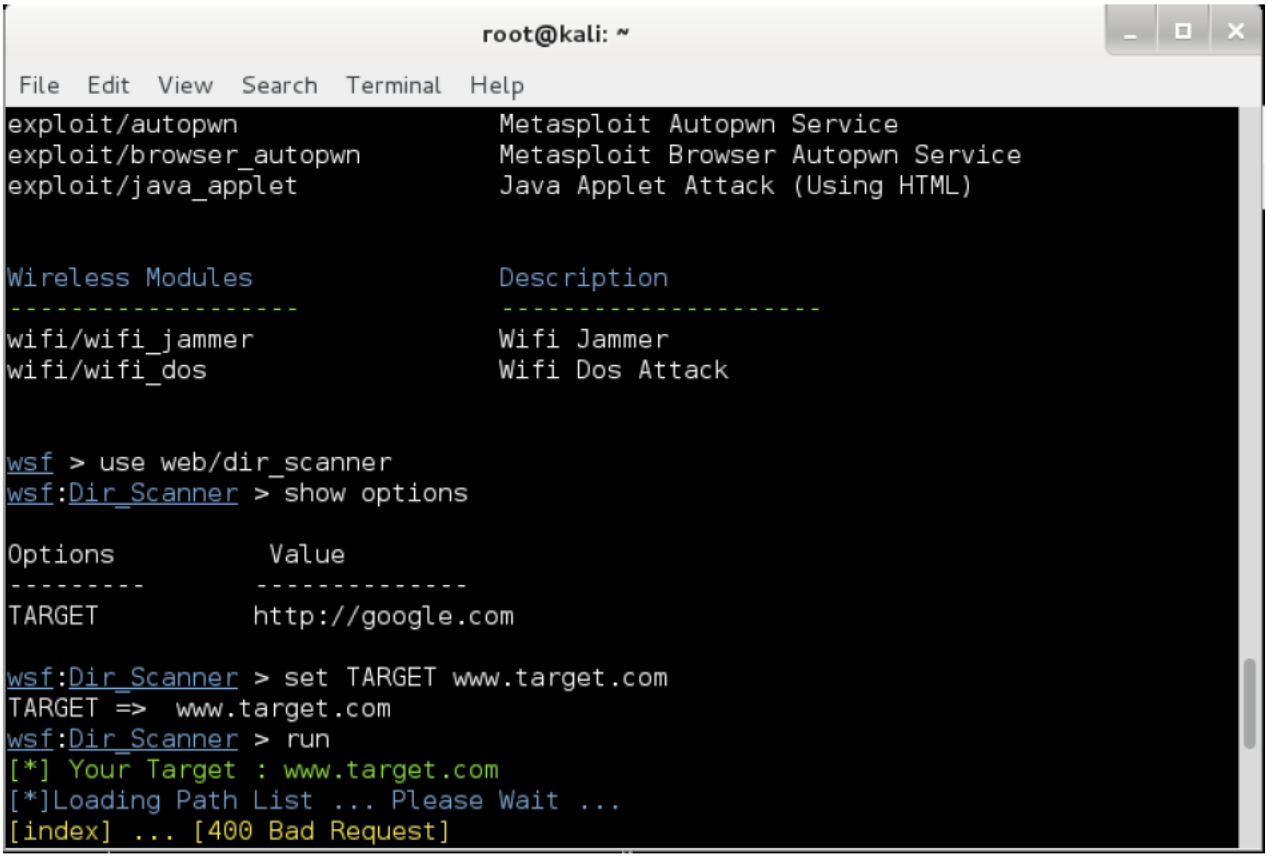
دعونا نبدأ بعملية مسح مسارات أو مجلدات بسيطة عبر موديول على www.target.com كالتالي:

wsf>use web/dir_scanner

wsf: Dir_scanner>show options

wsf: Dir_scanner>set TARGET www.target.com

wsf: Dir scanner>run



بمجرد تنفيذ أمر البدء Websploit سوف يبدأ نموذج الهجوم وتعرض النتيجة ، وبشكل مشابه يمكن استخدام نموذج او موديول اخر اعتماداً على ما نريد القيام به .

اختبار اختراق تطبيقات الويب باستخدام Burp Suite

Burp suite هي أداة معروفة والتي تستخدم بشكل واسع لإختبار تطبيقات الويب. وتوجد منها نسخة مجانية و نسخة تجارية تحوي ميزات إضافية. Kali يحوي بشكل مسبق على النسخة المجانية. و من أجل تشغيل هذه الأداة نتبع المسار التالي:
Applications | Kali Linux | Web Applications | Web Application Fuzzers | Burp Suite.

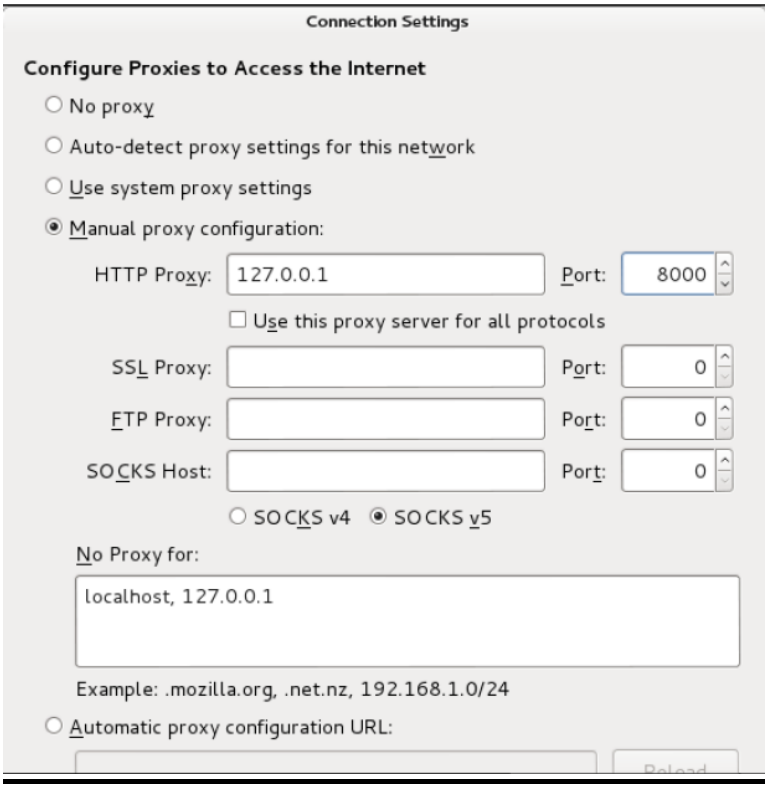
بعض خصائص Burp Suite تتضمن التالي:

- Proxy مقاطعة الذي يمكن أن يحلل الطلبات والإستجابة خلال المتصفح.
- تطبيق من أجل فحص محتوى التطبيقات.
- ماسح تطبيقات ويب من أجل تحديد الضعف و نقاط الضعف.
- إنشاء و حفظ خطوت العمل.
- توسيع الأدوات و تطويرها وفق إدخالات المستخدم.

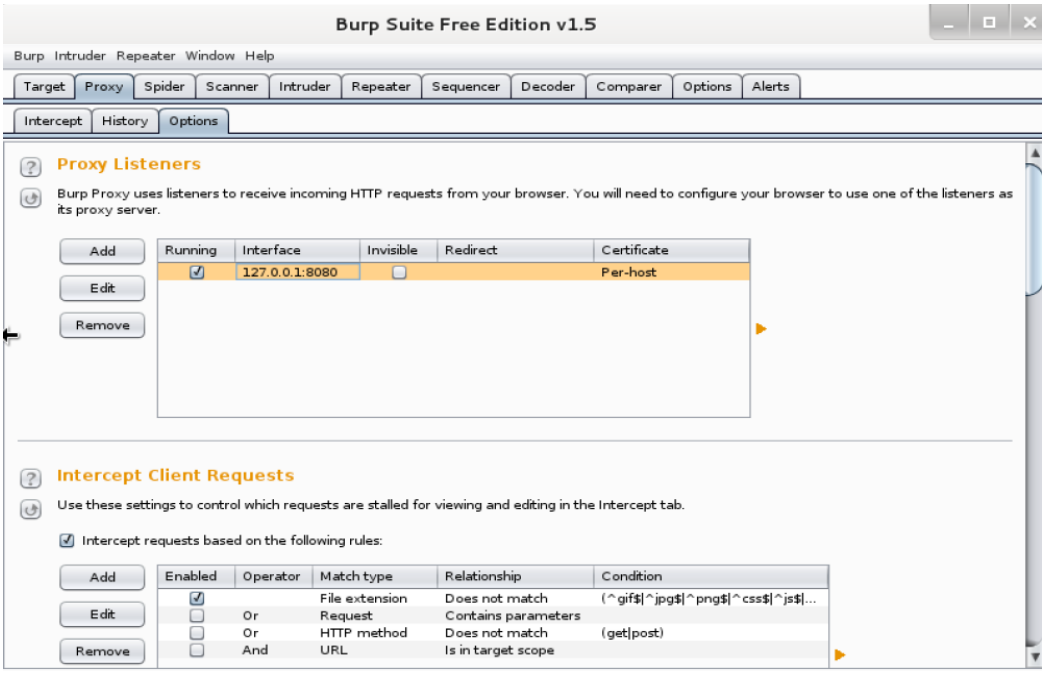
Burp Suite عبارة عن مجموعة من الأدوات التي تعمل مع بعضها ولنلقي نظرة على بعض الوظائف ضمن Burp Suite

Burp proxy

وهو proxy يقوم بقراءة حميع الطلبات والإستجابات التي تمر خلال المتصفح. وتقوم بتنفيذ هجوم man-in-the-middle لبدء العمل مع هذه الأداة سوف نغير إعدادات الشبكة للمتصفح لتمرير البيانات عبر proxy ، نفتح إعدادات الشبكة للمتصفح و نضبط عنوان proxy على localhost و رقم المنفذ على 8000 .



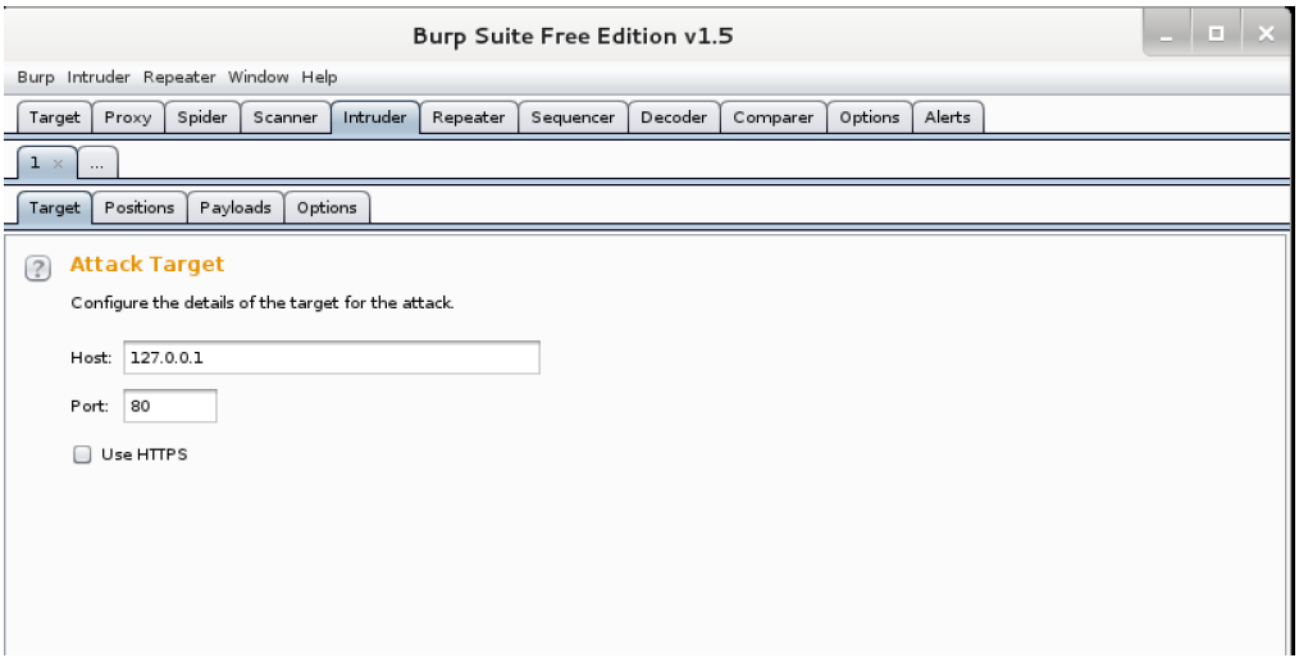
الآن المتفصح تم ضبطه على إتصال HTTP عبر Burp Suite . يمكن رؤية طريقة عمل proxy نضغط على قائمة Proxy ونختار Options. المقاطعة سوف تعيد أي إتصال HTTP من المتصفح. قائمة History تظهر لنا المخطط الزمني للإتصالات الملتقطة.



يمكن تغيير طريقة عمل proxy من قائمة Options .

Burp Intruder

أداة قوية لتنفيذ هجمات وفق الذي نريده على تطبيقات الويب. تسمح للمستخدم ببناء نموذج هجوم وتنفيذ العملية بشكل تلقائي.
Burp Inruder تحوي 4 قوائم مهمة هي: Target, Positions, Payloads, Options .



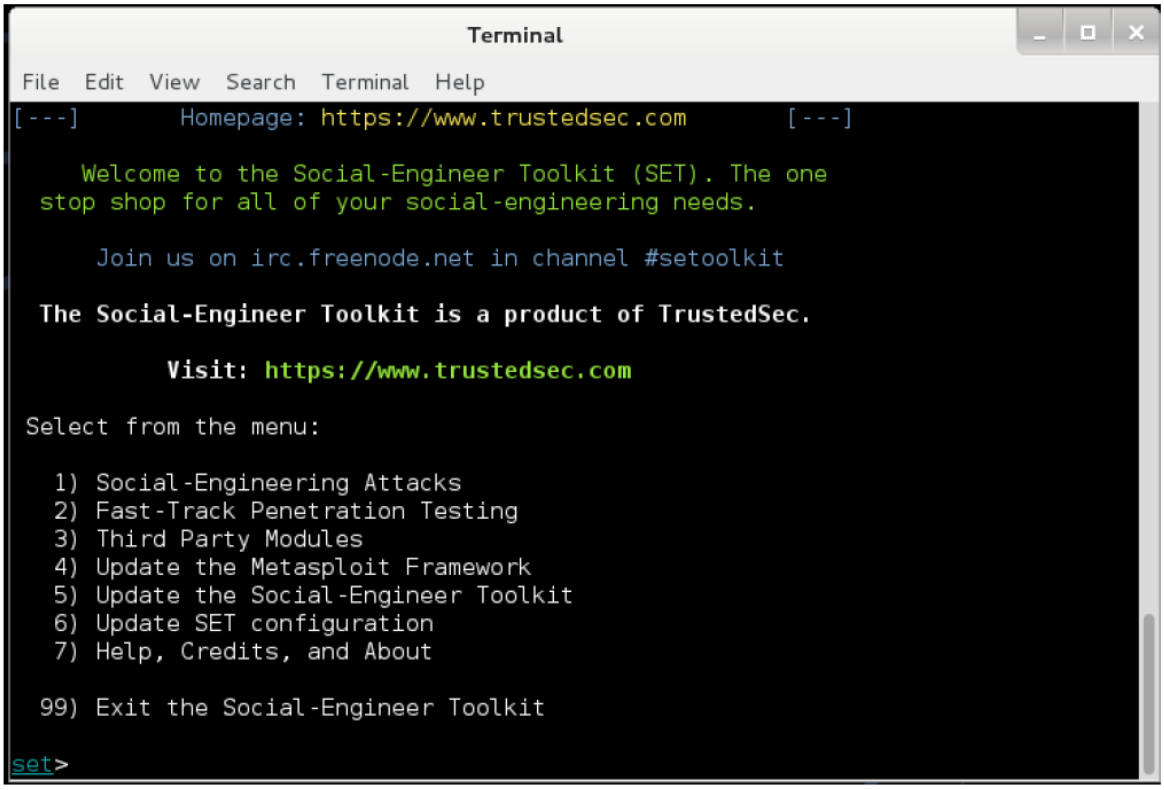
قائمة target تسمح لنا بإختيار عناون التطبيق الهدف من أجل إختبار محلي نختار 172.0.0.1.
قائمة Positions تستخدم من أجل إختيار مواقع التي سوف يتم تنفيذ الهجوم عليها. ويمكن أن تكون طلب أو شكل الحقل أو بارامتر وهكذا هناك عدة أشكال من نماذج الهجوم مثل
Sniper attack, battering ram attack, pitchfork attack, cluster bomb.
قائمة payloads تستخدم لضبط الهجوم الذي نحتاج لتطبيقه على الموقع المختار ضمن القائمة السابقة. على سبيل المثال ، يمكن تطبيق هجوم SQL injection عبر إختيار postions على شكل تسجيل دخول و إختيار الـ payload كـ injection string .
قائمة Options تستخدم من أجل تطبيق إعدادات إضافية كـ عدد المخاطر و المحاولات و تخزين النتيجة.

طرق و أدوات Exploitation

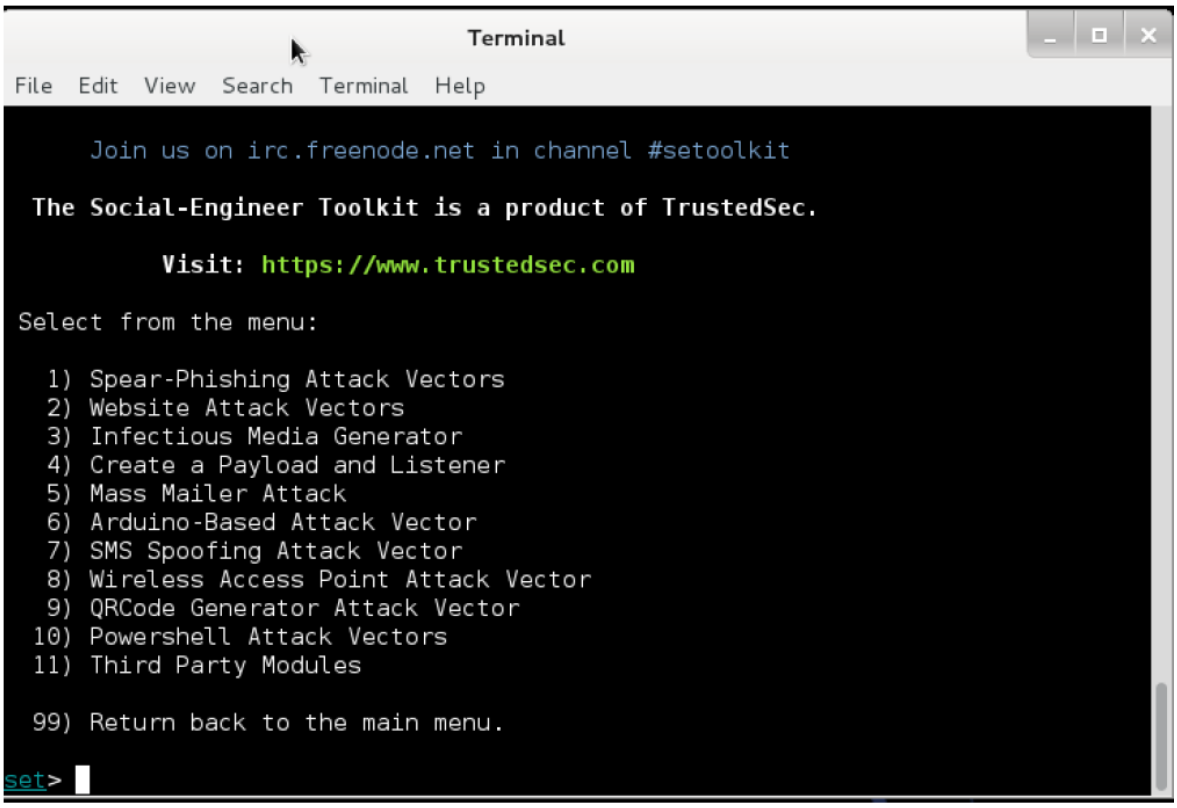
Social Engineer Toolkit

Social Engineer Toolkit (SET) هي أداة سطر أوامر مشهورة التي تستطيع القيام بهجوم على مستخدمين محددين . حيث يتم بناء الهجوم على مجموعة من الخيارات الموجودة ضمن هذه الأداة وستسمح للمهاجم بإستخدام قوة هذه الاداة لبناء سلسة الهجوم. نجاح سلسة الهجوم يعتمد تماماً على العنصر البشري لذلك سميت بأداة الهندسة الإجتماعية. لبدء هذه الأداة نذهب وفق المسار التالي:

Applications | Kali Linux | Exploitation tools | Social Engineering Toolkit | se-toolkit.



نستطيع إختيار نمط الهجوم الذي نرغب به من قائمة الخيارات لتأسيس الهجوم. دعونا نختار 1.
هنا سوف نجد خيارات هجوم عديدة لنختارها . لنختار على سبيل المثال Spear-Phishing Attack Vector و من ثم نختار Create Social Engineering Template. هذا الخيار سوف يسمح لنا بناء نموذج هجوم خاص بنا لتنفيذ هجوم عبر SET .



بالإضافة لذلك نستطيع بدء هجوم إعتماداً على موقع معين أو برنامج جافا وهكذا. SET أداة مفيدة و وسهلة الإستخدام التي تزودنا بالعديد من الخيارات من أجل إختبارالإختراق. SET أيضاً تمكننا من إستغلال قوة Metasploit framework لبناء payload و meterpeter connections و shells و غيرها.