
<< back | track 5
the quieter you become, the more you are able to hear


<< back | track 5
the quieter you become, the more you are able to hear

سخن تهیه کننده این کتاب :

سلام دوستان ، من هم مثل شما علاقه زیادی برای یادگیری این سیستم عامل دارم ولی اگر یه جستجویی در گوگل کرده باشید می فهمید که آموزش های پراکنده و ناقصی در این زمینه وجود داره وحتی بعضی از سایت ها و گروه های امنیتی هستن که آموزش رو ارائه دادن اما اگر عضو سایتشون هم بشی یا نمیزان عضوشون بشی یا میگن شما اجاز دانلود ندارید و باید از سوی مدیران تایید بشید .

به هر حال من این مطالب رو از سایت های ایرانی ، انگلیسی و عربی جمع آوری کردم و به شما عزیزان هدیه می دهم .

این کتاب با همت و تلاش های آقای جعفر نیسی گردآوری شده است .

آیا شما هم علاقه برای یاد گرفتن هك و مبحث امنیت هستید؟پس برای کار با سیستم عامل Back|Track آماده شوید!

بك ترك چیست؟

بك ترك یك توزیع لینوکس مبتنی بر GNU است که برای کشف نقاط ضعف امنیتی سیستم های مختلف تهیه شده و به صورت یك دی وی دی لایو(بدون نیاز به نصب و یا وجود هارد دیسك) در اختیار همه قرار گرفته. البته شما نه تنها میتونید اون رو از روی دی وی دی اجرا کنید بلکه می تونید اون رو بر روی هارد دیسك، فلش مموری و یا با ماشین مجازی نصب و اجرا کنید. در حال حاضر آخرین آن نسخه بك ترك ٥ است که از سایت رسمی بك ترك قابله دریافت است. بك ترك مبتنی بر Ubuntu 10.04 با هسته نسخه ٢٫٦ ساخته شده که پیشرفته خوبی برای آن است. بك ترك برای تمام مخاطبان از نوابغ و کهنه کاران امنیت تا نو آموزان هك و امنیت ساخته شده و سریع ترین و آسان ترین راه تست امنیت سیستم های کامپیوتری، شبکه ها و سایتهای اینترنتی است. جالب اینکه بدانید گروه های کلاه سیاه زیرزمینی و هم متخصصان امنیتی که برای دولت های کشورشون کار می کنند از جمله مشتریان اصلی بك ترك هستند.

چه کسانی از بك ترك استفاده می کنند؟

بك ترك 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 اینکه بدونید گروه های کلاه سیاه زیرزمینی و هم متخصصان امنیتی که برای دولت های کشورشون کار می کنند از جمله مشتریان اصلی بك ترك هستند.

ابزار های بك ترك

بك ترك كامل ترین و بروز ترین مجموعه ابزار های امنیتی رو در خودش داره كه رنج وسیعی از ابزار های پسورد كركر گرفته تا ابزار های هك وب سرور و شبكه رو شامل میشه. ابزاهای بك ترك در ۱۱ طبقه دست بندی شدند:

۱. **جمع آوری اطلاعات**(Information gathering)
۲. **شناسایی نقاط ضعف**(Vulnerability Identification)
۳. **آنالیز شبكه های بیسیم** (Radio Network Analysis)**با پروتكل های** ۸۰2.11, Bluetooth, RFID
٤. **كسب مجوز**(Privilege Escalation)
٥. **بازیابی و بازجویی دیجیتال** (Digital Forensics)**یا همون پزشك قانونی دیجیتال**
٦. Voice Over IP**همون**(VOIP)
۷. **نقشه یابی شبكه**(Network Mapping)
۸. **آنالیز برنامه های تحت وب**(Web Application Analysis)
۹. **كشف حفره های امنیتی**(Exploit & Social Engineering Toolkit)
۱۰. **كسب دسترسی غیر مجاز**(Maintaining Access)
۱۱. **مهندسی معكوس**(Reverse Engineering)

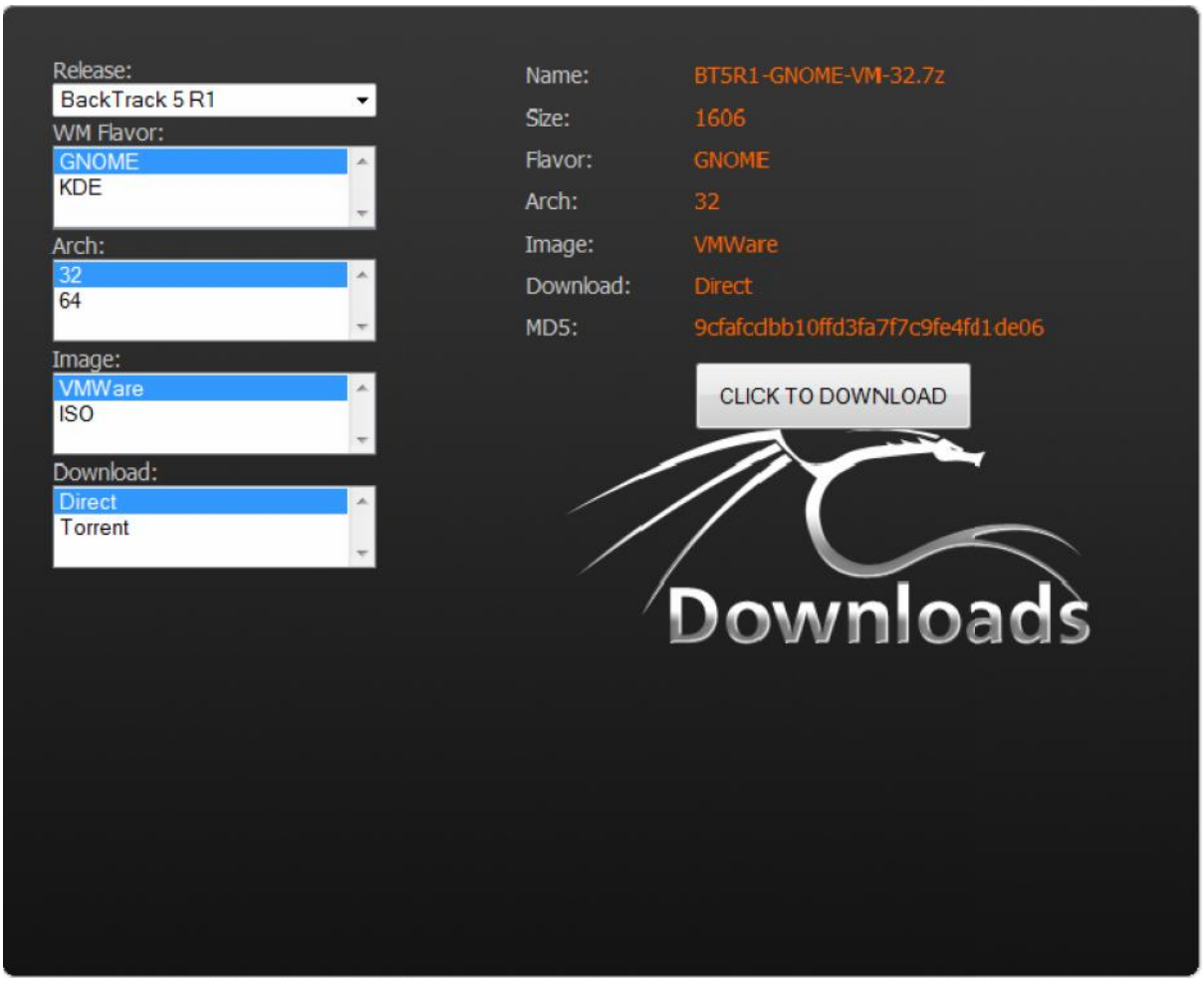
نرم افزار های بك ترك

این هم لیستی از نرم افزار های همراه بك ترك كه همراه با یك مجموعه عظیم از Exploit **های كشف شده عرضه شده:**

- Cisco OCS Mass Scanner
- Metasploit
- RFMON
- Kismet
- Nmap
- Ophcrack
- Ettercap
- Wireshark**یا همون**Ethereal
- BeEF**یا**(Browser Exploitation Framework)
- Hydra
- Quypt

دانلود بك ترك ٥

برای دانلود بك ترك از سایت رسمی بك ترك وارد بخش دانلود بك ترك شوید. در اینجا از شما سوال می شود که قبل ازدانلود قصد ثبت نام در سایت را دارید؟ در صورتی که چنین قصدی ندارید بر روی دکمه Download **کلیك کنید. در حال حاضر آخرین نسخه** backtrack r2 **می باشد .**



در قدم اول کدام انتشار از نسخه ٥ بك ترك را دانلود کنیم؟

شما میتوانید توزیع RC1 **یا** R2 **یا انتشار اول از بك ترك را انتخاب کنید. قطعاً** RC2 **گزینه ی بهتریست. چون مشکلات انتشار اول در** RC2 **اصلاح شده. بعضی ابزار ها اصلاح و بروزرسانی شدند و بعضی مشکلات مربوط به درایور ها و پشتیبانی سخت افزاری در آن حل شده.**

بك ترك را برای VMware **دانلود کنم یا نسخه** DVD **کامل آن را؟**

بهتر است قبل از اینکه در مورد محیط های کاری KDE **و** GNOME **تصمیم بگیریم نوع نصب بك ترك را مشخص کنیم. این بخش خیلی مهم است. در صورتی که قصد دارید از بك ترك فقط بر روی ماشین مجازی استفاده کنید نسخه** VMware **بك ترك با محیط کاری** GNOME **را دانلود کنید(همانطور که در تصویر بالا میبینید). در این حالت امکان استفاده از محیط زیبای** KDE **برای شما فراهم نخواهد بود. من این حالت را پیشنهاد نمیکنم چون در صورت انتخاب حالت** ISO **در بخش** Image **صفحه دانلود علاوه بر امکان استفاده از بك ترك بر روی** VMware **امکان استفاده لایو(به صورت زنده از روی دی وی دی) و به صورت نصب در کنار ویندوز را هم خواهید داشت.**

پس در بخش Image **گزینه** ISO **را انتخاب می کنیم.**

کدام محیط گرافیکی بهتر است KDE **یا** GNOME**؟**

KDE **از بسیاری از جهات بر** GNOME **برتری دارد. به نظرم تنها برتری که** GNOME **برای شما خواهد داشت سبك تر بودنش خواهد بود. من پیشنهاد می کنم** KDE **را دانلود کنید. محیط** KDE **بك ترك تجربه جالب و حتی قابل مقایسه ای با ویندوز ۷ خواهد بود.**

معماری ۳۲ بیتی یا ٦٤ بیتی برای من مناسب تر است؟

معماری ٦٤ بیتی فوق العاده است اما یك ایراد دارد: سازگاری با سخت افزارها و سیستم های مختلف. در صورتی که شما قصد دارید فقط در سیستم هایی که دارای پردازشگر با معماری ٦٤ بیتی هستند از بکترك استفاده کنید نسخه ٦٤ بیتی برای شما مناسب است.

اما در صورتی که میخواهید در هر شرایطی و بر روی هر سیستمی از بك ترك استفاده کنید نسخه ۳۲ بیتی برای شما بهتر است. من در کل نسخه ۳۲ بیتی را ترجیه میدهم و آن را پیشنهاد می کنم.

دانلود با تورنت یا با لینك مستقیم؟

در صورتی که از طرفداران تورنت هستید از این گزینه راضی خواهید بود. تورنت بکترك تعداد سیدهای زیادی دارد و سرعت آن فوق العاده است. اما برای کاربران ایرانی که سرعت آنها معمولاً کمتر از ۵۱۲Kbps است لینك مستقیم شما را سریع تر به نتیجه می رساند. پیشنهاد می کنم از یك نرم افزار مدیریت دانلود برای دریافت فایل ایمیج بکترك استفاده کنید.

دانلود نسخه های قدیمی تر بکترك

بیشتر منابع و آموزش های بکترك مربوط به نسخه ٤ آن است. اما این نسخه دیگر توسط تیم بکترك پشتیبانی نمیشود. اما در صورتی که به هر دلیلی قصد دانلود نسخه های قدیمی تر را دارید دیگر از طریق سایت رسمی بکترك امکان دانلود آن را نخواهید داشت. بهتربن راه برای دانلود آن استفاده از شبکه های اشتراك فایل(تورنت) است.

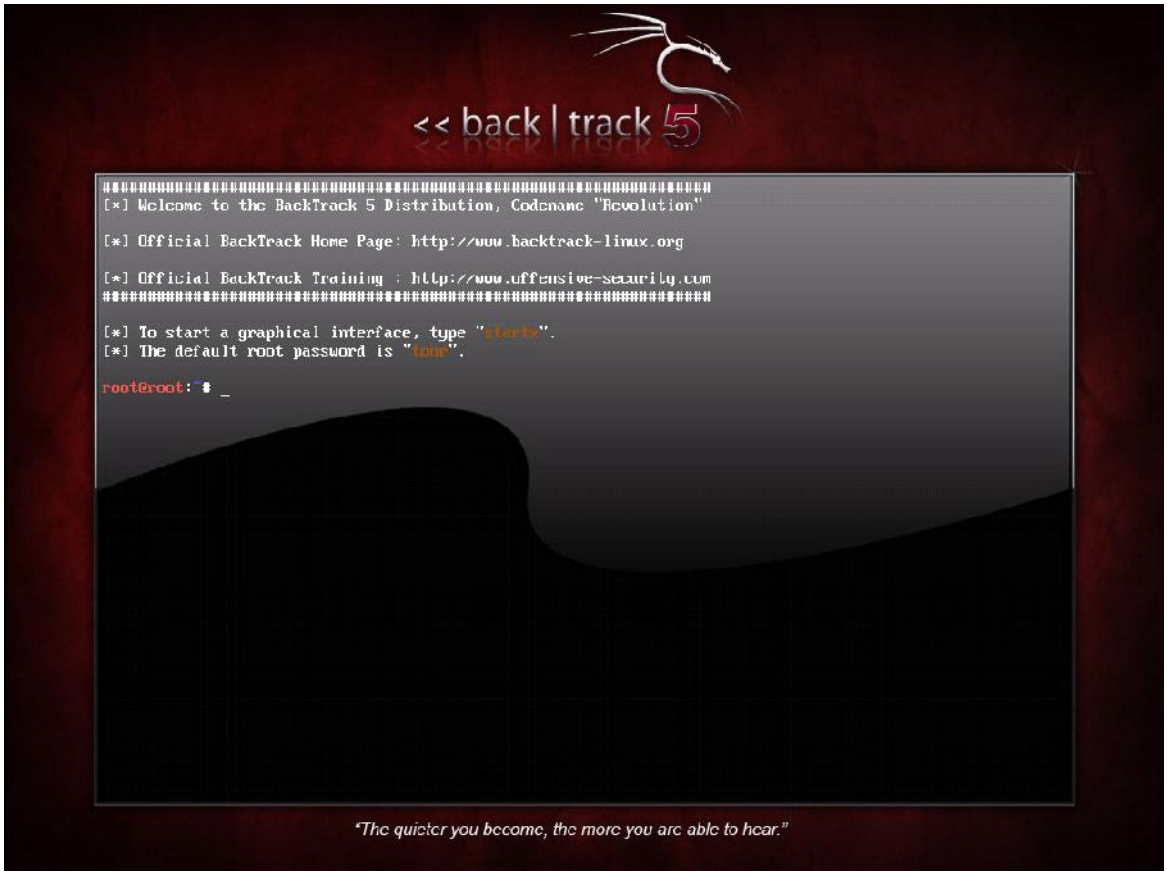
اجرای بك ترك به صورت زنده

اجرای زنده سیتم عامل(Live) **راهندازی سیستم عامل از یك درایو خارجی**(سی دی، دی وی دی، فلش و ...) **است به صورتی که سیستم عامل به حافظه اصلی**(RAM) **بارگزاری می شود و بدون نیاز به هارد دیسك بر روی سیستم اجرا می شود. در اجرای لایو بکترك**(Backtrack Linux) **هیچ تغییری در اطلاعات شما ایجاد نمی شود مگر اینکه پارتیشن های دیسك سخت خود را بارگزاری**(mount) **کرده و خود در آنها تغییر ایجاد کنید.**

برای اجرای زنده backtrack **بعد از دانلود بکترك به صورت یك فایل ایمیج**(ISO) **آن را بر روی یك** DVD **رایت کنید در** DVD-Rom **سیستم خود قرار دهید و سیستم را روشن کنید.سپس با منوی مشابه تصویر زیر روبرو می شوید:**

گزینه اول شما را وارد خط فرمان بکترك میکند. گزینه دوم بکترك را بدون راهندازی اتوماتیك شبکه راهندازی می کند تا در صورتی که قصد دارید بدون شناسایی شدن شبکه خاصی را آنالیز کنید به محض شروع سیستم عامل شما در لوگ سرور ثبت نشوید. بقیه گزینه ها برای خطایابی بکترك را با تنظیمات مختلف اجرا میکنند. با اجری گزینه آخر هم از بوت بکترك صرف نظر کرده و سیستم از هارد دیسك بوت می شود.

با اجرای گزینه اول شما مستقیماً وارد خط فرمان بکترك می شوید. همانطور که در سوالات رایج در بك ترك گفتم نام کاربری اصلی root **و رمز عبور آن** toor **است. البته در صورتی که شما پارتیشن لینوکس روی هارد دیسك های خود نداشته باشید از شما سوالی نمیشود و مستقیماً وارد این صفحه می شوید:**



برای ورود به محیط گرافیکی بکترك فرمان زیر را وارد کنید

```
Startx
```

با اجرای این فرمان یکی از محیط های گرافیکی KDE **یا** GNOME **بسته به انتخاب شما در دانلود بکترك به نمایش در می آید.**

تصویر زیر محیط گرافیکی KDE **در بکترك ٥** RC2 **را نمایش می دهد.**

تبریك میگم. شما با موفقیت لینوکس بك ترك را راهندازی کردید. شما از همین طریق به وسیله آیکن Install BackTrack **در دسکتاپ میتوانید بکترك را بر روی سیستم خود نصب کنید.**

لینوکس بکترك(Backtrack) سیستم عاملیست که در دنیا به عنوان بهترین ابزار هکر ها شناخته میشود. به طوریکه تقریباً هر چیزی که برای یك عملیات کشف ضعفهای امنیتی و نفوذ لازم است در آن گنجانده شده. در این مقاله به صورت قدم به قدم اقدام به نصب این سیستم عامل میکنیم.

در اینجا از بکترك ٥ RC2 استفاده شده. این آموزش هم بر روی نصب بر روی ماشین مجازی و هم به صورت مستقیم(منفرد یا در کنار ویندوز) قابل انجام است.

مرحله اول: اجرا زنده بك ترك

در قدم اول دیسك بکترك را در درایو قرار داده و آن را به صورت لایو اجرا کنید و وارد محیط گرافیکی آن شوید. برای اطلاعات بیشتر مقاله اجرای زنده بکترك را مطالعه کنید.

مرحله دوم: برنامه نصب بکترك را اجرا کنید

برای شروع ویزارد نصب بکترك طبق شکل برنامه نصب بکترك را از دسکتاپ اجرا کنید.

مرحله سه: انتخاب زبان

ما در اینجا زبان انگلیسی را انتخاب میکنیم. جای زبان فارسی تو این لیست بلند از زبان ها خالیه. شما میتوانید گزینه اول(No Localization) **را هم انتخاب کنید.**

مرحله چهار: انتخاب منطقه زمانی

در اینجا کشور خود را میکنیم. من کشور عزیزمون ایران را انتخاب کردم. برای این کار میتونید روی نقشه کلیک کنید.

تا جایی که من اطلاع دارم این تنظیمات نمیتونه باعث رهگیری شما در بکترك بشه اما ممکنه شما بخواهید شرط احتیاط رو رعایت کنید و مقادیر شانسی رو در این تنضیمات وارد کنید.

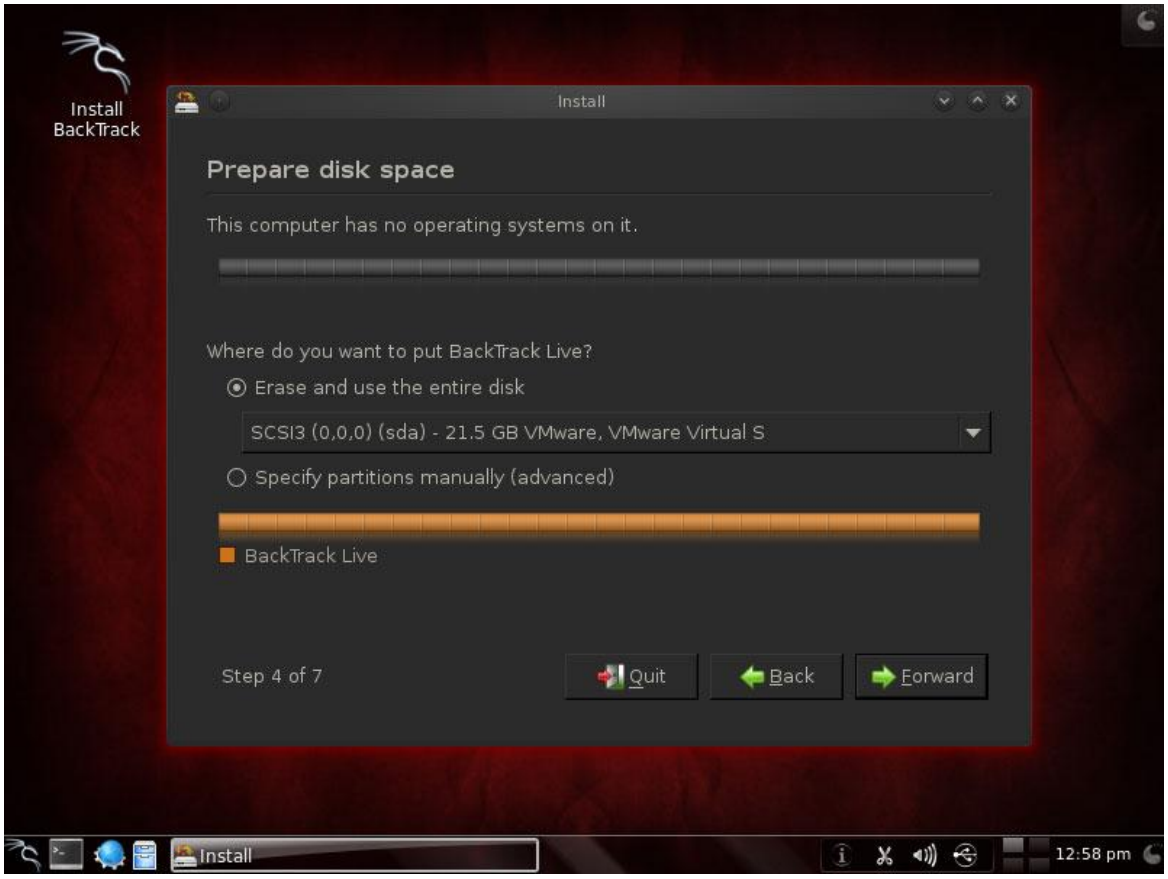
مرحله پنج: انتخاب زبان صفحه کلید

من در این مرحله با انگلیسی پیش میرم و زبان فارسی رو بعداً اضافه میکنم.

البته شما میتونید در همین بخش زبان فارسی رو انتخاب کنید. برای این کار مثل تصویر زیر کشور ایران و در لیست زبان ها گزینه ی آخر رو انتخاب کنید.

مرحله شش: اختصاص فضا به پارتیشن لینوکس

این مرحله در نصب سیستم عامل در کنار ویندوز خیلی مهمه. در صورتی که که شما بکترك را روی ماشین مجازی(VMWare) نصب میکنید نیازی به تغییر تنظیمات پیش فرض وجود ندارد(تصویر زیر) و میتوانید بدون هیچ تغییری به مرحله بعد بروید.



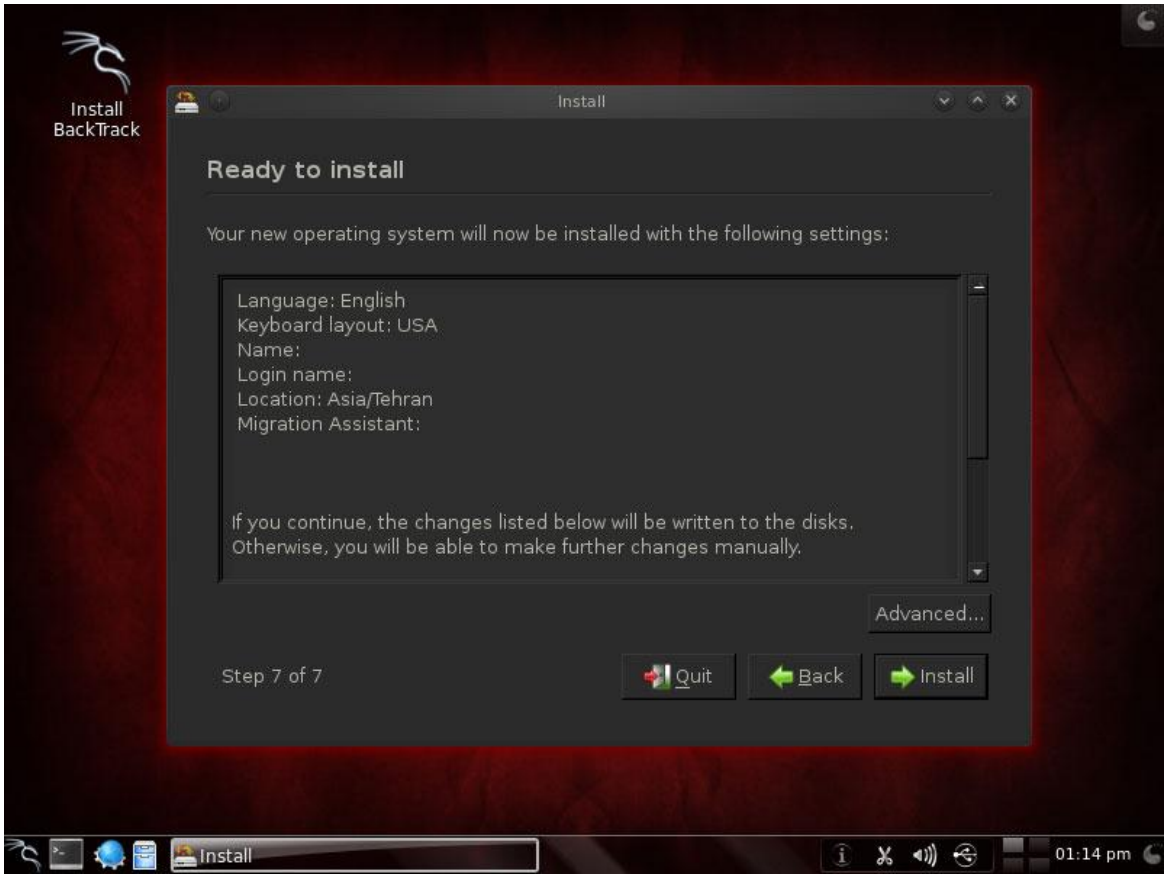
در صورتی که بکترك را در کنار ویندوز نصب میکنید پیشنهاد میکنم که با توجه به دردناك بودن از دست دادن فایلها در ویندوز خود از تمام فایل هایی که برای شما اهمیت دارند پشتیبان تهیه کنید. البته احتمال از دست دادن فایل به خاطر خطای نرم افزاری خیلی پایین و غیر محتمل است و در صورتی که با پارتیشن بندی آشنا باشید احتمالاً هیچ مشکلی به وجود نمی آید. برای از بین بردن هر ریسکی من روش زیر را پیشنهاد میکنم:

در ویندوز مراحل زیر را طی کنید: Manage < Right Click < My Computer **و بر روی** Disk Managment **کلیك کنید. آخرین درایوی که در لیست مشاهده می کنید در نظر بگیرید. در صورتی که در آن حد اقل فضای خالی ۲۲ گیگابایت وجود ندارد تعدادی از فایل ها را به درایو دیگری منتقل کنید. بر روی درایو راست کلیك کرده و گزینه** Shrink Valume **را کلیك کنید.**

با این کار پنجره ای باز میشود که از شما مقدار فضایی که میخواهید از پارتیشن انتخاب شده کم کنید را میپرسد. این مقدار به مگابایت است پس برای کم کردن ۲۰ گیگابایت ۲۰٤۸۰ را از فضای کل دیسك کم کنید. در صورتی که در نصب در کنار ویندوز در این مرحله هستید کافی است از گزینه دوم(Advanced) استفاده کنید و فضای خالی انتهای دیسك را انتخاب کنید. در صورتی که حافظه رم شما کم باشد بهتر است پارتیشن ۲ گیگابایتی برای swap را هم ایجاد کنید.

مرحله هفت: شروع فرایند نصب

در اینجا با کلیك بر روی install نصب شروع میشود. این مکن است مرحله ۱۰ با ۳۰ دقیقه با توجه به نوع نصب و قدرت سخت افزار شما طول بکشد.



مرحله هشت: اتمام نصب

در ادامه نیاز به انجام کاری خاصی نیست. صبر میکنیم تا نصب به پایان برسد و میتوانید سیستم را ری استارت کنید.

حالا در صورتی که شما بك ترك را در کنار ویندوز نصب کرده اید دیسك بك ترك را خارج کنید. با شروع به کار سیستم وارد منوی بوت میشوید. گزینه آخر شما را به ویندوز میبرد و گزینه اول به بکترك.

در صورتی که شما نصب را در VMWare **انجام میدادید بعد از ری استارت میتوانید برای افزایش کارکرد ابزارهای بکترك را نصب کنید.**

آموزش نصب بکترک در ماشین مجازی(VMWare)

بکترک سیستم عاملیست که روز به روز در بین جامعه هکر ها و متخصصان امنیتی محبوب تر میشود و بر کاربران آن اضافه می شود. هر چند که برای دسترسی به حداکثر قدرت پردازشی میتوان آن را به صورت مجزا(یا در کنار ویندوز) نصب کرد اما در صورتی که شما بکترک را بر روی ماشین مجازی(VMWare) نصب کرده باشید از مزایایی مثل استفاده از قابلیت های ویندوز و لینوکس و انجام دو عمل مختلف در کنار هم استفاده کنید.

در این مقاله Backtrack 5 RC2 **را بر روی** VMWare Workstation 7.1.x **نصب شده بر روی ویندوز ۷ استفاده میکنیم. البته نصب در ویندوز** xp **هم تفاوتی در مراحل انجام شده ندارد و مشابه است.**

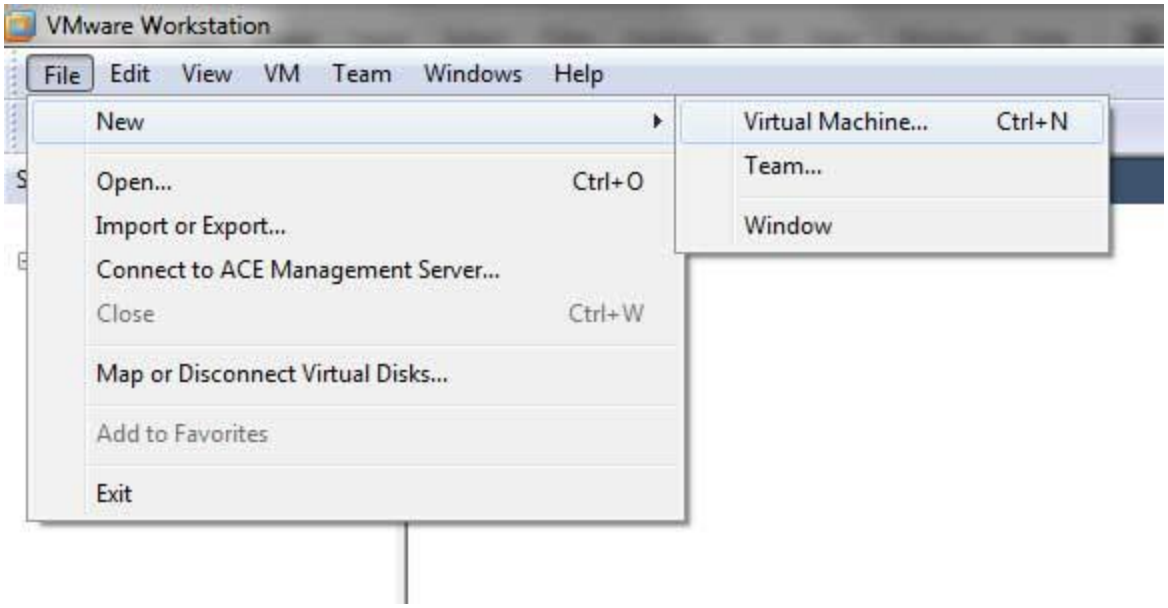
توجه کنید در صورتی که بکترک را دانلود نکرده اید قبل از دانلود بکترک حتماً آموزش دانلود لینوکس بکترک را مطالعه کنید.

مرحله اول: نصب ماشین مجازی بر روی ویندوز

این مرحله نیاز به توضیح اضافی ندارد. فقط توجه کنید که در صورتی که از ویندوز ٦٤ بیتی استفاده میکنید با نصب VMWare 64 **بیتی کارایی خیلی بیشتر افزایش پیدا میکند. البته این ربطی به ۳۲ یا ٦٤ بیتی بودن بکترک ندارد.**

مرحله دوم: ایجاد ماشین مجازی

مثل تصویر یک ماشین مجازی جدید ایجاد کنید.

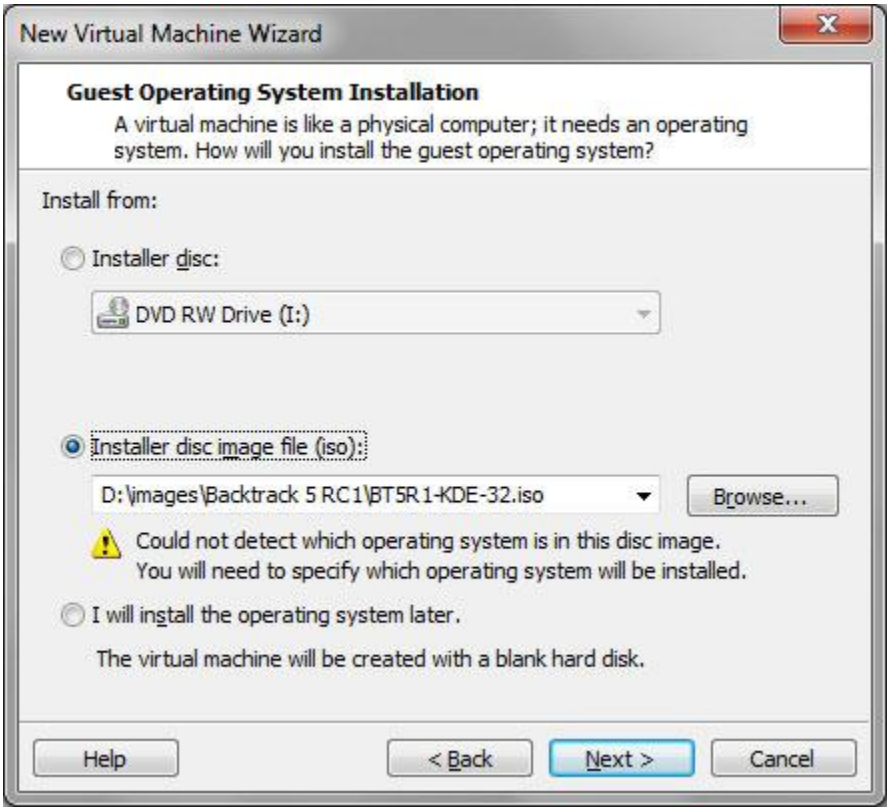


مرحله سوم: انتخاب نوع نصب

در اینجا با دو گزینه نصب عادی(Typical) و نصب پیشرفته(Advaced) روبرو میشویم. من نصب عادی را انتخاب کردم چون از هر جهت با تنضیمات سیستمی بکترك همخوانی دارد. شاید در صورتی که از نسخه های قدیمی بکترك یا VMWare استفاده میکنید یا سخت افزاری دارید که مشکل شناسایی شدن در حالت عادی را دارد بخش نصب پیشرفته به شما انعطاف بیشتری برای سازگار کردن آنها میدهد. البته این حالت خیلی نادر پیش می آید.

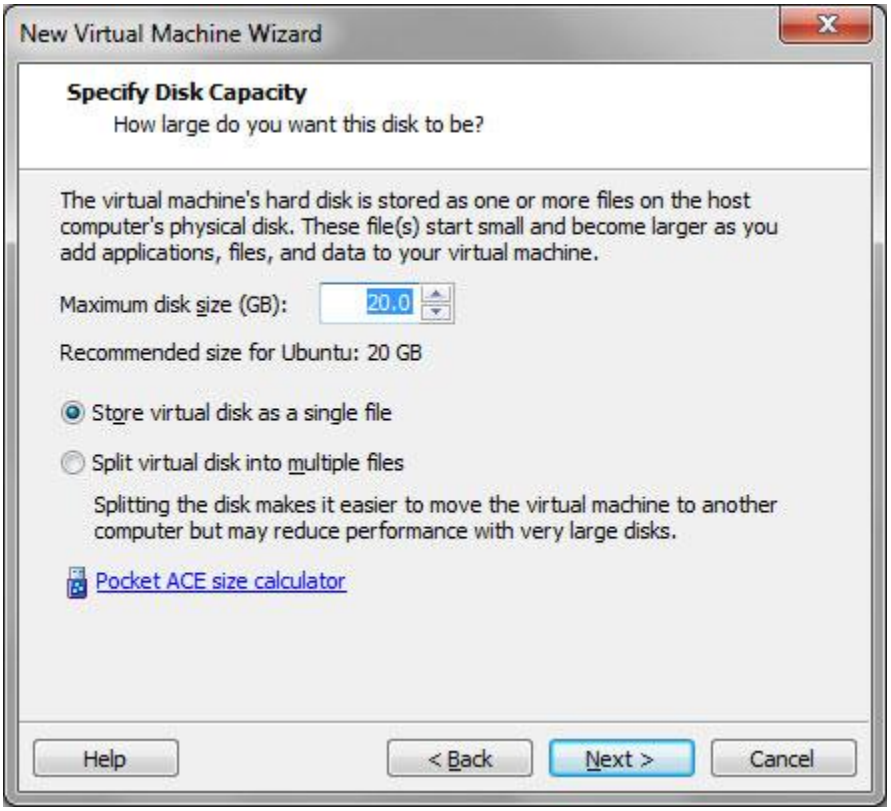
مرحله چهارم: منبع نصب

در اینجا دیسک یا فایل سیستم عامل را در اختیار VMWare قرار میدهید تا شروع به اجرای آن کند. شما میتوانید دی وی دی بکترك را در DVD-ROM قرار دهید و با گزینه اول آن را بوت کنید یا میتوانید فایل ایمیجی که از سایت بکترك دانلود کرده اید را در گزینه دوم انتخاب کنید.



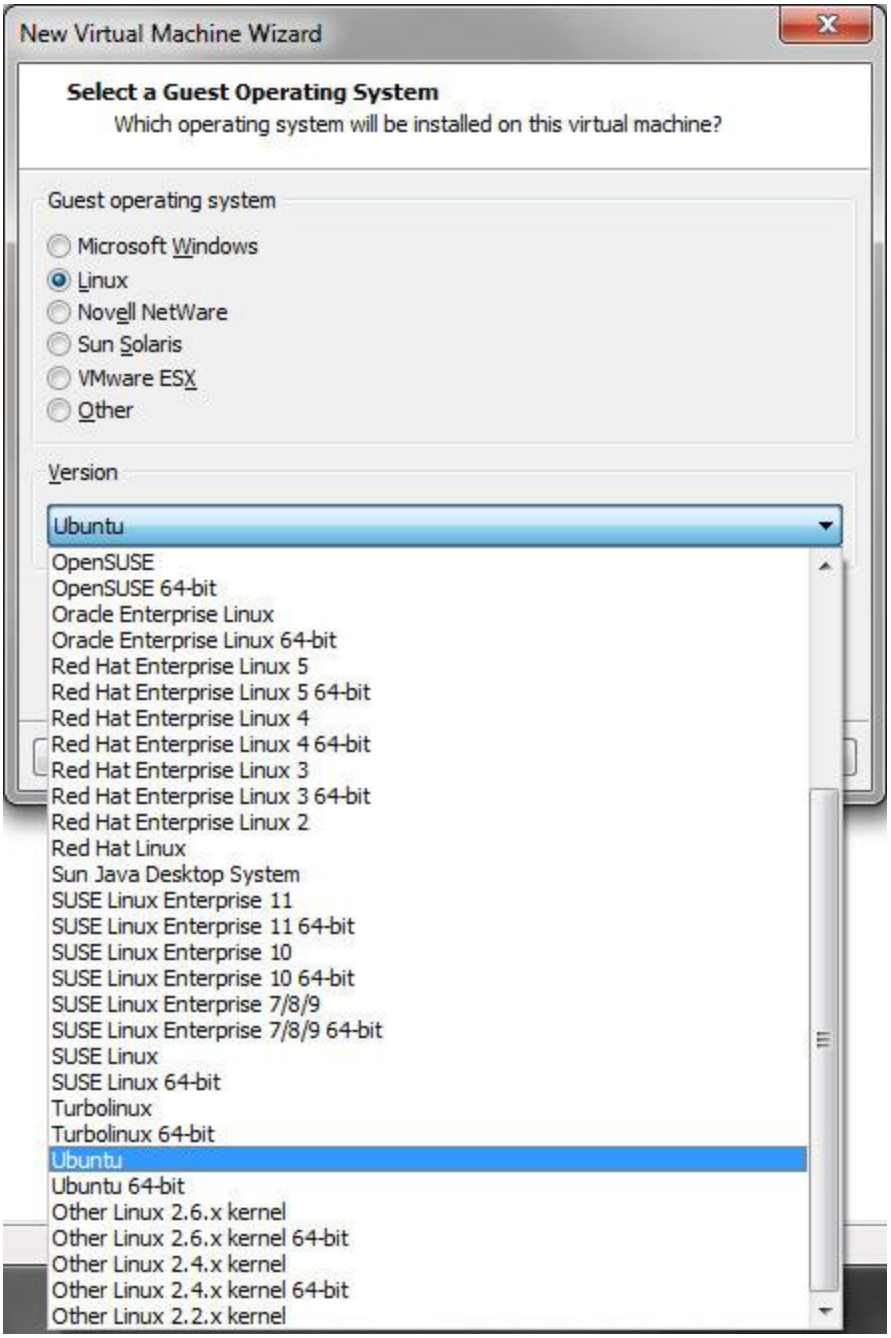
مرحله پنجم: اختصاص فضا

در اینجا فضایی که در اختیار بکترك قرار میدهید را مشخص میکنید. مقدار پیشفرض ۲۰ گیگابایت است که برای بکترك و نرم افزار ها و فایل هایی که بعده به آن انتقال میدهید مناسب است. البته ۱۰ گیگابایت هم میتواند به نیاز شما را برطرف کند.



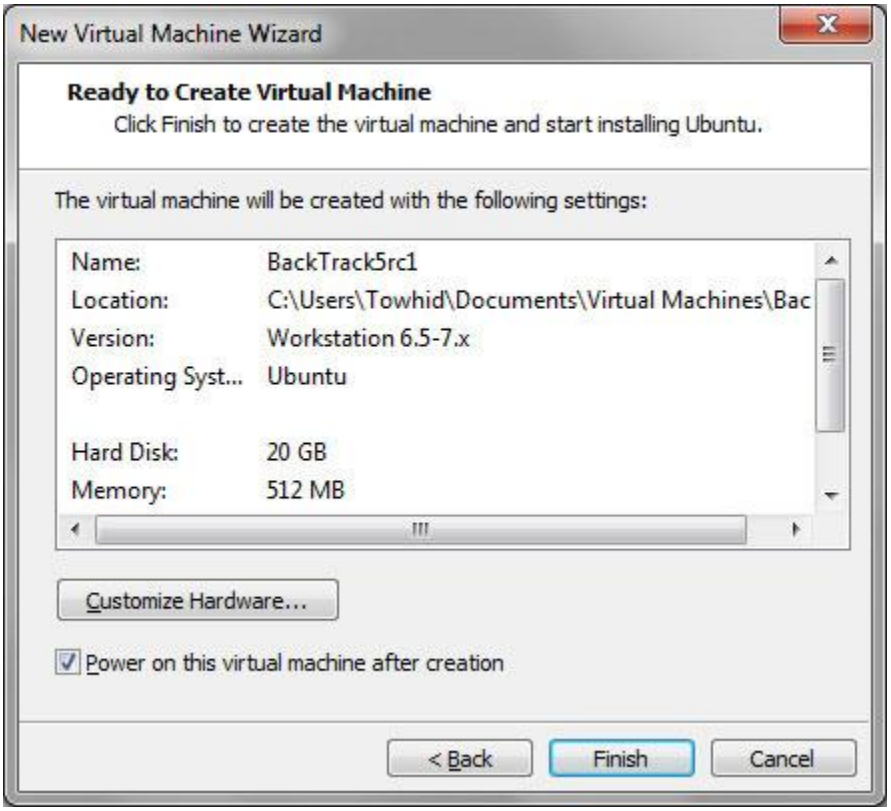
مرحله ششم: نوع سیستم عامل

همانطور که در مقاله بکترك چیست؟ گفتم بکترك یك لینوکس مبتنی بر توزیع اوبونتو است. پس تبعاً در این قسمت هم سیستم عامل اوبونتو را انتخاب می کنیم. فقط به این نکته توجه کنید که در صورتی که نسخه ٦٤ بیتی بکترك را دانلود کرده اید باید گزینه Ubuntu 64-bit **را انتخاب کنید.**



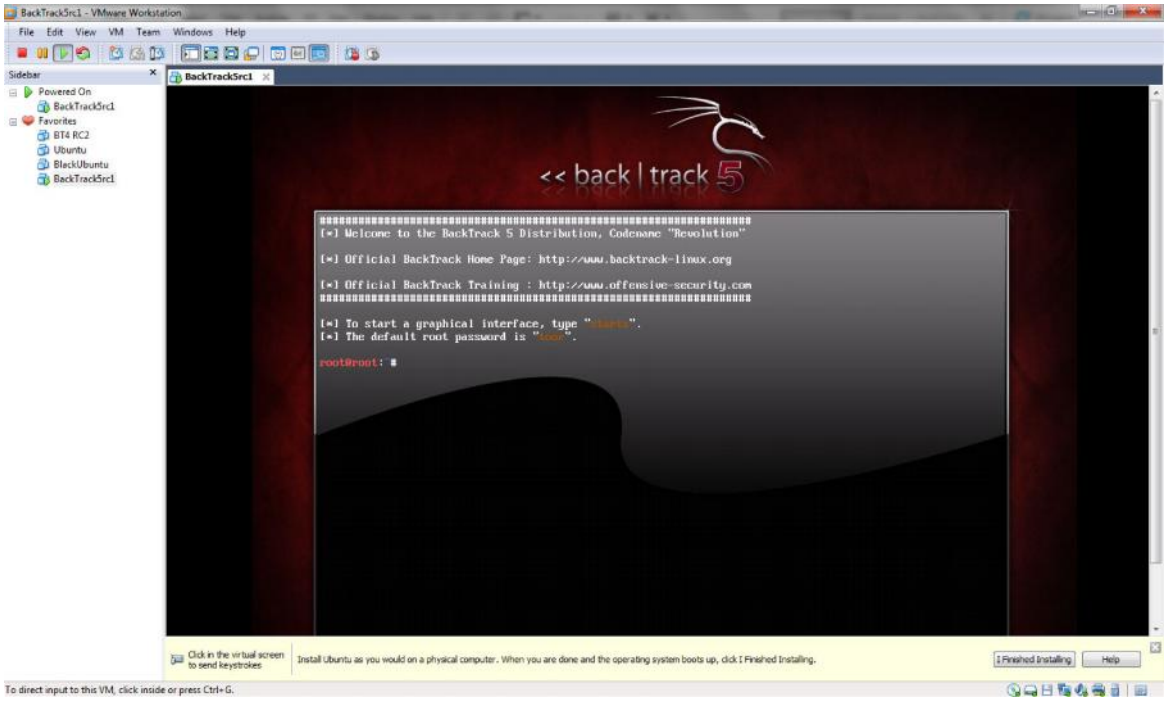
مرحله هفتم: اتمام نصب

ویزارد نصب در این مرحله تمام اطلاعات لازم را کسب کرده و در مرحله بعد نصب خود سیستم عامل بکترک را شروع می کنیم. پس چک باکس Power On **را انتخاب کنید و** Finish **را کلیک کنید.**



مرحله هشتم:

برای نصب بکترك آن را به صورت زنده در ماشین مجازی اجرا میکنیم. این مرحله به صورت کامل در آموزش اجرای زنده بکترك توضیح داده شده است. بعد آن را از طریق ویزارد نصب بکترك نصب میکنیم. این مراحل را در آموزش نصب بکترك دنبال کنید تا بکترك بر روی سیستم مجازی شما نصب شود.

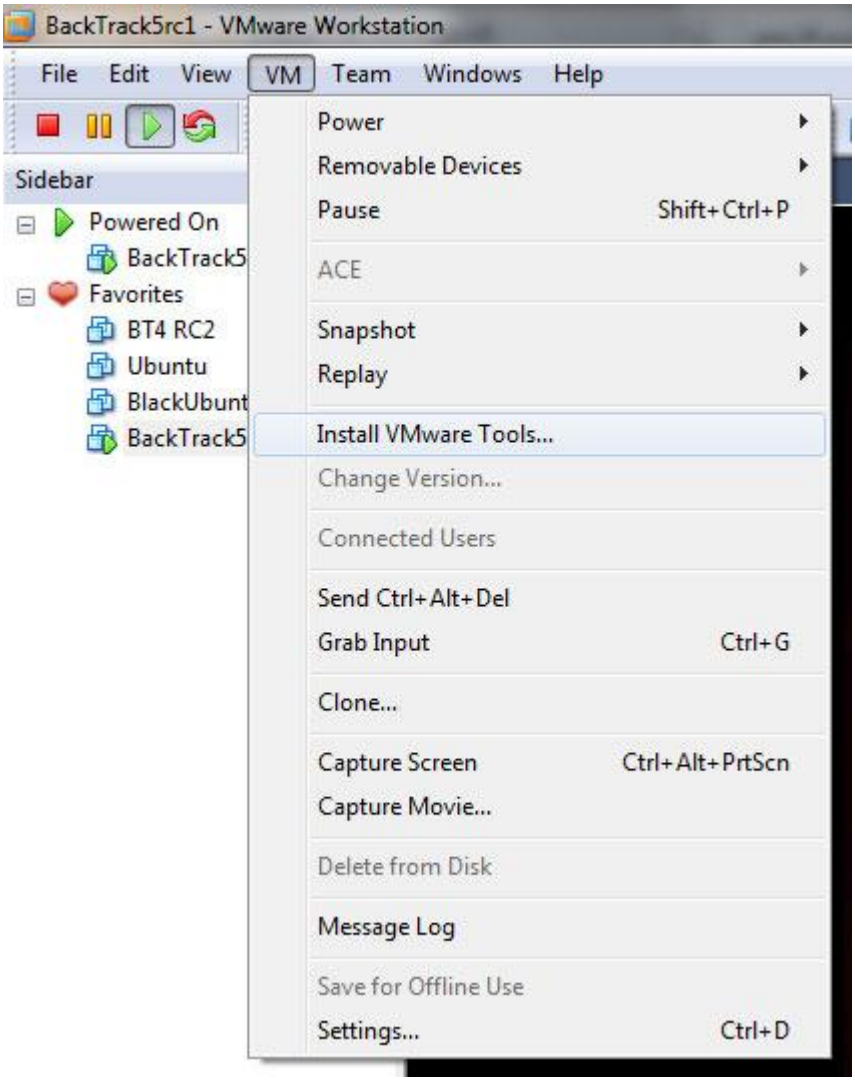


همانطور که در تصویر می بینید در پایین محیط VMWare **نواری نمایش داده شده که از شما می خواهد که بعد از نصب بکترك دکمه** I Finished installing **را کلیك کنید. میتوانید این نوار را ببندید یا طبق دستور العمل بعد از نصب آن را کلیك کنید**

مرحله نهم: نصب ابزارهای VMWare

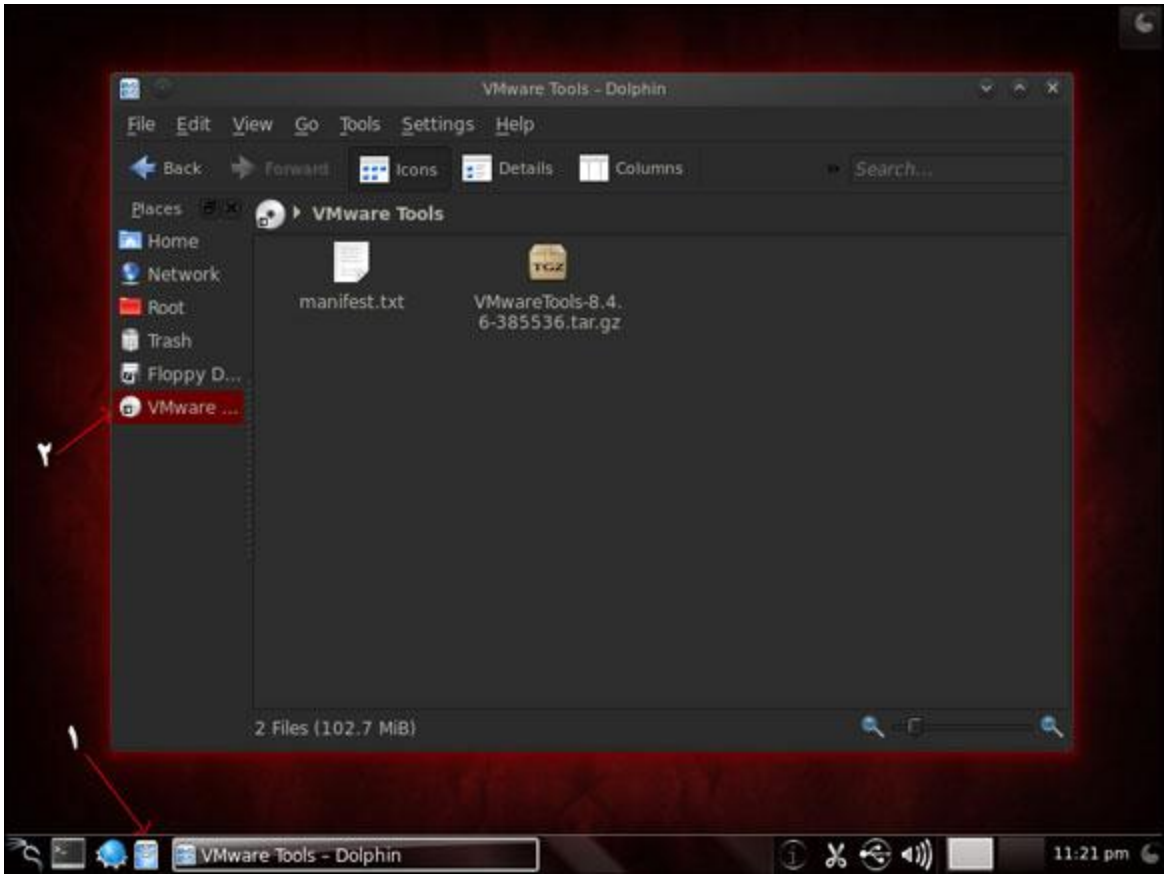
ابزار های VMWare **مجموعه ای از فایل ها و درایور ها هستند که کارایی سیستم عامل نصب شده بر روی ماشین مجازی را بالا برده و سازگاری سخت افزاری بهتری را ارائه می کنند. شما میتوانید از نصب این ابزارها صرف نظر کنید اما من نصب آنها را شدیداً توصیه می کنم.**

برای نصب ابزار های ماشین مجازی بعد از نصب بکترك طبق تصویر در VMWare **از منوی** VM **بر روی** Install VMware Tools **کلیك کنید.**



مرحله دهم: نصب ابزارهای VMWare در بکترك

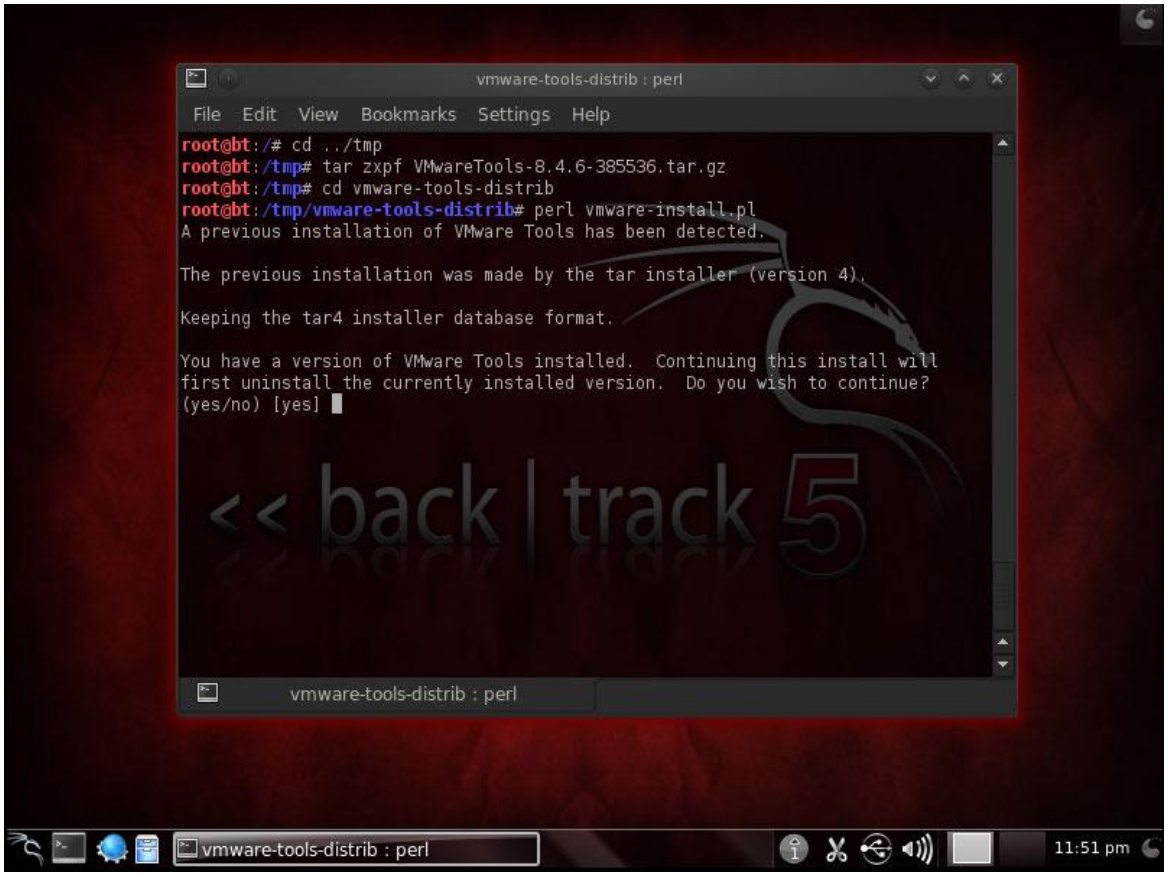
بعد از اجرای مرحله هشت یك درایو مجازی در بکترك ایجاد میشود که در آن فایل نصب ابزار های بکترك وجود دارد. برای دسترسی به آن بر روی علامت دیسك در پانل ایجاد شده کلیك کنید یا از تسکبار بکترك در پایین آیکن آرشیو که در اصل آیکن برنامه دلفین(مدیر فایل در بکترك) را کلیك کنید و در پنجره باز شده از پانل سمت چپ آیکن دیسك را کلیك کنید.



بر روی فایل VMwareTools-x.x.x-xxxxxx.tar.gz **راست کلیک کنید و کپی را کلیک کنید. نام فایل با توجه به نسخه** VMware **شما ممکن است متفاوت باشد.**

دوباره از پانل سمت چپ بر روی root **کلیک کنید و با دابل کلیک وارد پوشه** tmp **شوید. حالا بر روی محیط خالی راست کلیک کرده و** paste **را کلیک کنید.**

در اینجا ترمینال بکترک را باز کرده و فرامینی که در تصویر میبینید را اجرا کنید.




```
cd ../tmp
```

این فرمان شما را وارد پوشه tmp **که فایل فشرده ابزارهای** VMware **در آن است وارد میکند.**

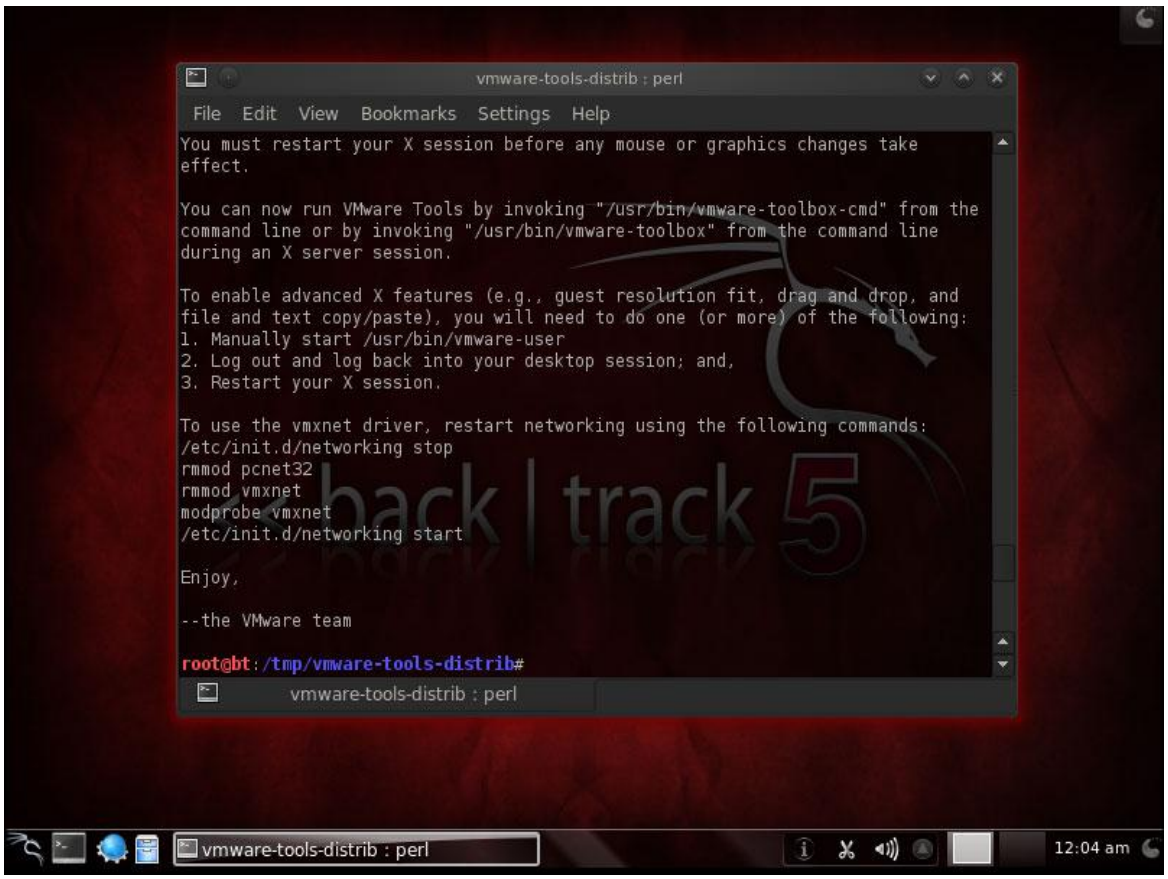
```
tar zxpf VMwareTools-x.x.x-xxxxxx.tar.gz
```

این فرمان فایل فشرده ابزارها را از حالت فشرده خارج میکند. توجه کنید که سیستم فایل لینوکس بر خلاف ویندوز به حروف بزرگ و کوچك حساس است و در صورتی که اسم فایل یا فرمان ها را درست وارد نکنید فرمان درست اجرا نخواهد شد. در وارد کردن اسم فایل ها بعد از وارد کردن قسمت اول آن مثلا بعد از وارد کردن دو حرف VM **در فرمان کلید** Tab **را از صفحه کلید فشار دهید تا بقیه نام فایل به صورت اتوماتیك تایپ شود.**

```
perl vmware-install.pl
```

این فرمان دستور شروع برنامه نصاب ابزارهای بکترك را میدهد. بعد از این مرحله تعدادی سوال از شما میشود که مسیر نصب اجزای برنامه را می پرسد. در تمام موارد مسیر پیشفرض مناسب است پس در هر سوال بدون وارد کردن حرفی کلید Enter **را می زنیم.**

در مرحله آخر پیغامی مشابه تصویر زیر نمایش داده میشود که میگوید نصب با موفقیت به اتمام رسید و درایو مجازی اجکت شد.



حالا شما میتوانید فایل فشرده ابزارها را به زباله دان ارسال کنید.

تبریك میگم، نصب شما با موفقیت به اتمام رسید. حالا قدرتمندترین تسلیحاتی که میتواند در اختیار یك جنگجوی سایبری قراربگیرد در اختیار شماست. از آن درست استفاده کنید.

تغییر زبان در بك ترك

اگر می خواهید زبان دیگری را درون بك ترك نصب کنید ابتدا باید وارد system **می شویم و از گزینهای ظاهر شده** preferences **را بر میگزینیم و از لیست گزینه** keyboard **و سپس** layouts **را انتخاب می کنیم بعد گزینه** Add **را میزنیم و باانتخاب کشور محل سکونت زبان به صورت خودکار تغییر می کند و برای پایان کار** Add **را می زنیم .**

محیط مخفی در بك ترك (محیط Fluxbox)

شما می توانید در بك ترك از محیط Fluxbox **استفاده کنید. برای این کار در خط فرمان مسیر زیر را طی کنید:**

کد :

```
root@bt:~# dragon

2010 (C) Dragon v 0.1 – Back|Track Command Line Control Panel

upgrade Upgrade your Back|Track box

follow Install and Follow all Back|Track tools by Category

...

dragon >> desktop fluxbox
```

Selecting Fluxbox as default Desktop Manager

dragon >> quit

Good Bye

root@bt:~#

خطوطی که با رنگ قرمز مشخص شده اند فرمان ها و بقیه خروجی ترمینال هستند. جلسه فعلی را قطع کنید تا فلوکس باکس اجرا شود.

backtrack

نصب فونت های فارسی در بك ترك (برای نمایش بهتر سایت های فارسی)

ابتدا فایل های (tahoma . bfonts) **را دانلود و آن ها را اکسترکت کنید حالا وارد فایل سیستم توزیع شوید و به مسیر زیر بروید:**

کد:PHP

```
usr/share/fonts/truetype
```

حالا به دنبال فایلی به نام ttf-persian-fonts **بگردید اگر هم چین فایلی رو یافت نکردید آن را ایجاد کنید**

حالا دقیقا دو فایلی را که دانلود کردید (را در این پوشه کپی کنید .

یك سایت فارسی باز کنید مشاهده می کنید که فونت های فارسی به درستی به نمایش در می آیند.

****

نصب فلش پلیر در بك ترك (نمایش بهتر سایت ها ی فارسی)

به صورت پیش فرض نه تنها فلش پلیر بلکه خیلی از نرم افزار های مورد نیاز در بك ترك نصب نمی باشد برای نصب Flash Player **ابتدا یك ترمینال باز کنید و در آن دستور زیر را تایپ کنید:**

کد:PHP

```
apt-get update
```

پس از این که پاکت ها به دربافت شد و به روز رسانی بسته ها تمام شد دستور زیر را نیز اجرا کنید:

کد:PHP

```
apt-get install flashplugin-installer
```

حالا کافیست سایت مورد نظر خودتون را یك باز refresh **کنید**

شر کردن و نصب کدك های پخش

در این قسمت به Share **کردن اطلاعات بین ویندوز و بك ترك و نصب کدك ها اجرای فایل های صوتی و تصویری در بك ترك خواهیم پرداخت.**

Share کردن اطلاعات بین ویندوز و بك ترك

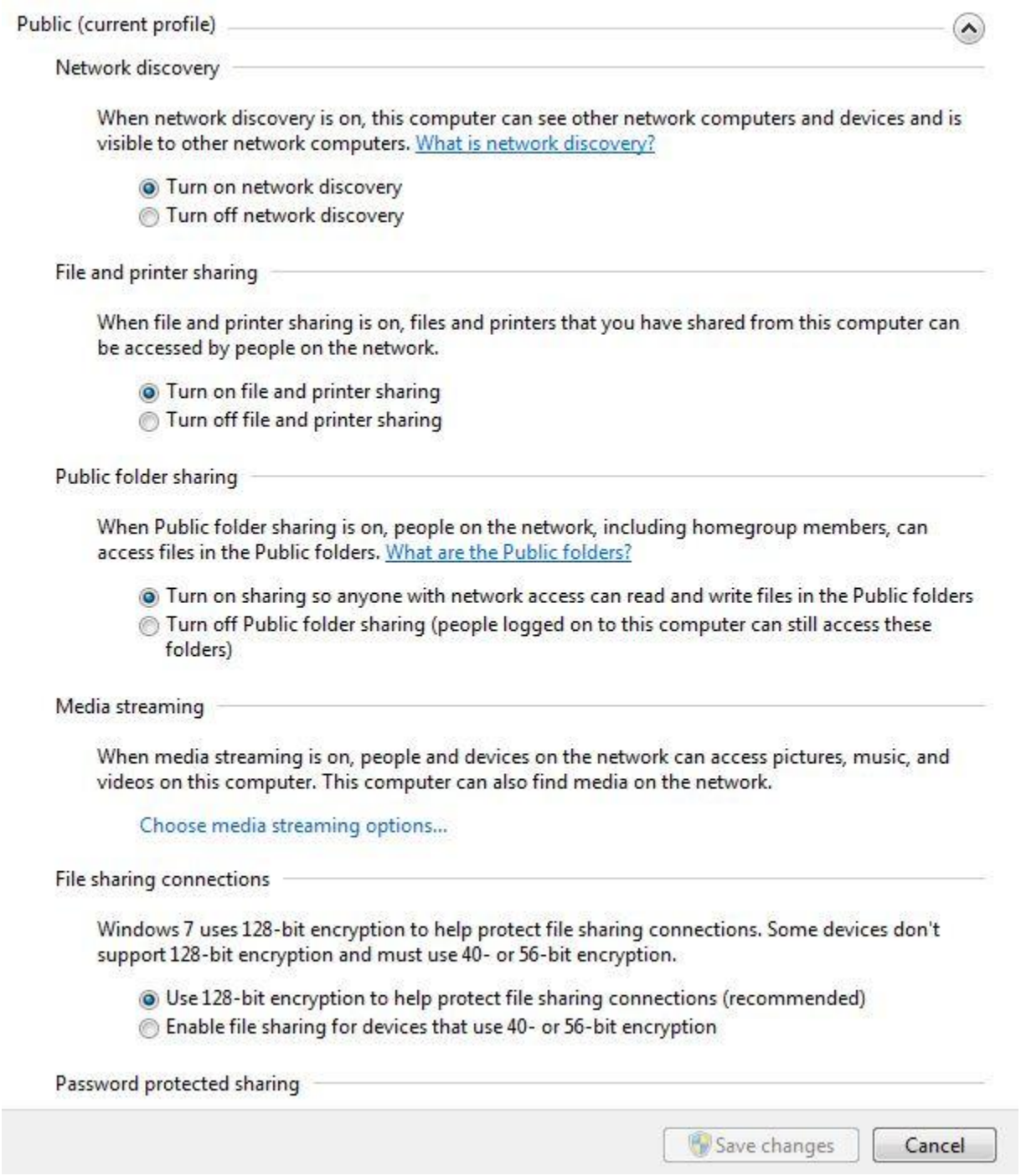
همون طور که می دونید یکی از روش ها برای دسترسی به فایل ها و اطلاعات در سیستمی دیگر شبکه کردن دو سیستم است از این روش هم می توان بین دو سیستم واقعی و یا ماشین مجازی استفاده کرد

برای این کار ابتدا باید ویندوز خودتون را آماده کنید لذا اول مسیر زیر را دنبال کنید:

کد:PHP

```
Control panel - Network and Internet - Network adn sharing Center
- change advanced sharing settings
```

حالا تمامی تنظیمات را همانند عکس زیر تغییر دهید:



پس از این که تغییرات را در ویندوز خودتون اعمال کردید به سیستمی بروید که بك ترك بر روی آن نصب هست و تغییرات زیر را هم در آن اجرا کنید:

ابتدا یك ترمینال باز كنید و عبارت زیر را در آن تایپ كنید:

كد:PHP

```
apt-get install samba
```

پس از این كه نصب samba **تمام شد دستور زیر را اجرا كنید:**

كد:PHP

```
apt-get install system-config-samba
```

نرم افزار samba **با موفقیت نصب شد حالا از منوی بك ترك به قسمت** system **و از آن جا سامبا را انتخاب كنید . در پنجره ی باز شده روی گزینه ی** add share **كلیك كنید تا صفحه ی** creat samba share **باز شود.**

از قسمت Directory **فولدر مورد نظر خودتون را كه می خواهید** share **كنید انتخاب و تیك گزینه ی** Visible **را نیز بگذازید.**

هم چنین می توانید به سریرگ Accsess **رفته و از آن جا یوزر را محدود به استفاده كنید برای این كه بر روی یوزر شما مثلا** Root **پسورد بگذارید از دستور زیر استفاده كنید:**

كد:PHP

```
smbpasswd -a root
```

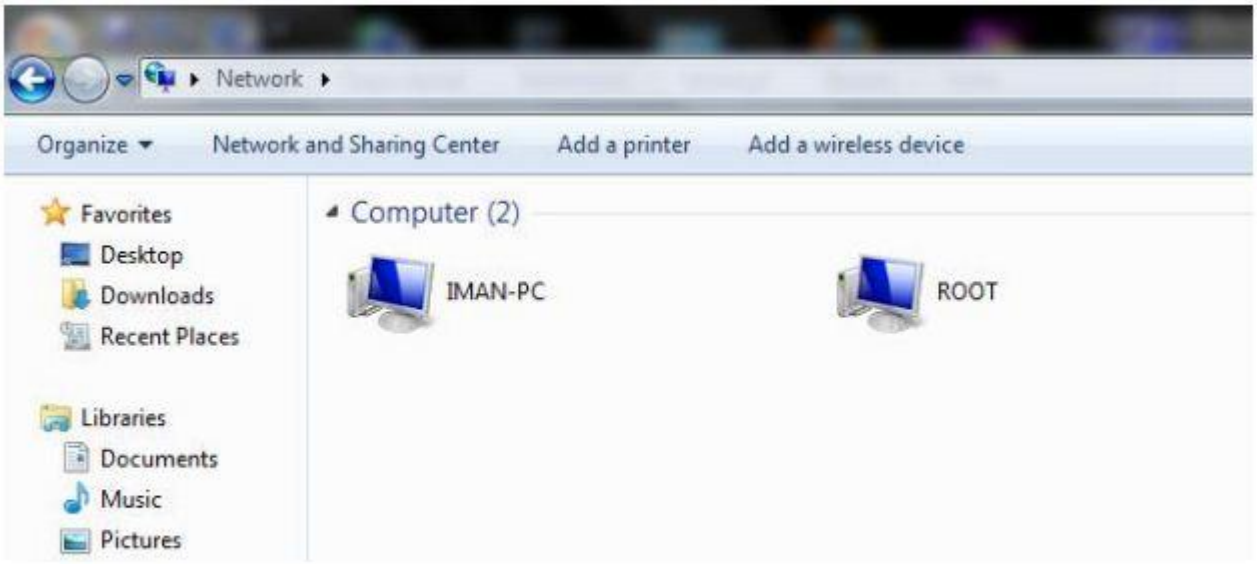
روی ok **کلیك کنید حالا دوباره به ویندوز خود برگردید و به آدرس زیر بروید**:

کد:PHP

```
Network and Internet - View network computer and devices
```

حالا یك باز صفحه را Refresh **کنید . مشاهده می کنید که** share network folder **بك ترك شما که اسم آن** Root**می باشد به وجود آمده است . حالا کافیست که روی آن کلیك کنید تا فولدری که در سامبا به اشتراگ گذاشته اید را مشاهده کنید .**

توجه کنید اگر در سامبا مثلا یوزر Root **پسورد گذاشته باشید در هنگام ورود به فایل اشتراك گذاشته شده در بك ترك . از شما پسورد می خواهد .**


Network
Organize
Network and Sharing Center
Add a printer
Add a wireless device
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Computer (2)
IMAN-PC
ROOT

نصب کدك ها اجرای فایل های صوتی و تصویری در بك ترك

یکی از مشکلات اکثر کسانی که از بك ترك استفاده می کنند پخش فایل های صوتی و به ویژه تصویری است برای حل این مشکل ابتدا باید به صورت دستی کدك ها و سپس یك نرم افزار پلیر را نصب کنیم

برای رفع این مشکل ایتدا یك ترمینال باز کنید و عبارت زیر را در آن اجرا کنید:

کد:PHP

```
aptitude install gstreamer0.10-pitfdll gstreamer0.10-ffmpeg
gstreamer0.10-gl gstreamer0.10-plugins-base gstreamer0.10-
plugins-good gstreamer0.10-plugins-bad gstreamer0.10-plugins-bad-
multiverse gstreamer0.10-plugins-ugly gstreamer0.10-plugins-ugly-
multiverse libxine-extracodecs w32codecs
```

با اجرای این دستور کدك ها شروع به دانلود از مخازن و نصب می شود که حجمی حدود ٤٠ مگ دارد

بعد از نصب کدك ها باید یك پلیر در بك ترك نصب کنید برای این کار از دستور زیر استفاده کنید (پلیر پیشنهادی (gxine

کد:PHP

```
apt-install gxine
```

حالا روی فایل صوتی یا تصویری خودتون راست کلیك کنید و از قسمت open with پلیر مورد نظر خودتون را انتخاب کنید تا فایل اجرا شود

اتصال به اینترنت در بك ترك ٤

دوستان اگه دقت کرده باشید در بك ترك ٤ همانند بك ترك ٥ همان اول اینترنت ندارید برای حل این مشکل از دو دستور زیر استفاده کنید:

کد:PHP

```
if config eth0 up
```

و بعد از آن:

کد:PHP

```
start-network
```

در صورتی مشکلی وجود نداشته باشد با دستور زیر مواجه می شوید:

کد:PHP

```
starting network connection manager : wicd.
```

حالا یك مرورگر باز کنید و سعی کنید که یك سایت باز کنید اگر باز هم مشکل داشتید در قسمت URL **عبارت زیر را بنویسید:**

کد:PHP

```
192.168.1.1
```

حالا یوزر و پسورد خودتون رو وارد کنید که از آن جا وارد صفحه ای می شوید

از آن جا به قسمت Advanced Setup **برید و از قسمت سمت چت روی** Edit **کلیك کنید**

حالا روی Next **کلیك کنید . در صفحه ی جدید از قسمت** Connection Type **گزینه ی** PPP over Ethernet (PPPoE)**را انتخاب کنید و روی** Next **کلیك کنید**

حالا دوباره سعی کنید یك سایت باز کنید که خواهید دید اینترنت شما وصل شده است

راه اندازی Armitage در بك ترك

یکی از دغدغه های استفاده کنندگان از بك ترك مشکلات Armitage **می باشد که در این آموزش قصد داریم این مشکل را بر طرف کنیم برای این منظور یك ترمینال باز کنید و دستور زیر را اجرا کنید:**

کد:PHP

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

سپس عبارت زیر را تایپ کنید

کد:PHP

```
msfgui
```

مشاهده می کنید یك صفحه با نام Connect to msfrpcd **برای شما باز شد که فقط بر روی** Start new msfrpcd**کلیك کنید**

حالا برای شما برنامه ی msfgui **باز خواهد شد پس از کامل لود شدن از بالا روی** File **کلیك کنید و گزینه ی**

کد:PHP

```
Show connection details
```

را انتخاب کنید مشاهده می کنید که صفحه ی Connect Details **پسورد را ذخیره کنید (بعدا مورد استفاده قرار میگیره)**

دوباره بك ترمینال باز کنید و دستور زیر را اجرا کنید:

کد:PHP

```
armitage
```

حالا پسوردی را که در بالا بهتون داد رو به جای پسورد test **وارد کنید و تك** use ssl **را بردارید و از قسمت** DB **گزینه ی** driver Mysql **را انتخاب کنید و در آخر هم روی** Cennect **کلیك کنید مشاهده می کنید که** Armitage **با موفقیت اجرا شد.**

حل مشکل صدا در back track Gnome

به آدرس زیر بروید

```
system - preferences - startup applications
```

در صفحه باز شده add **را بزنید تا وارد صفحه** add startup program **حالا جا های خالی را مانند تصویر پر کنید**

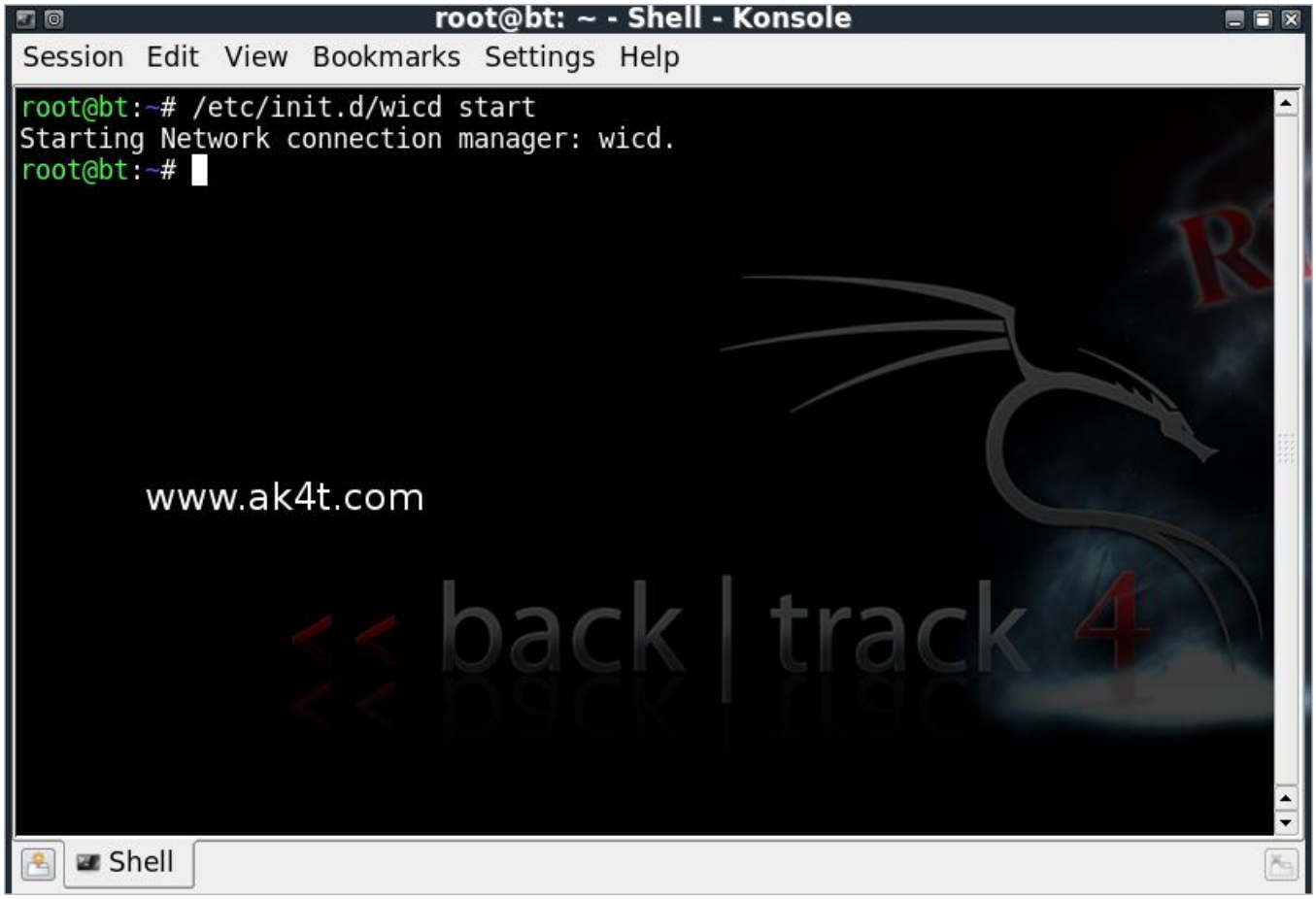
همانطور که مشاهده می کنید این دستورات استارت آپ شده و همچنین شما می توانید از قسمت استارت آپ تیک برخی از دستوارتی که نیاز ندارید را بردارید .

فعا سازی شبکه و وایرلس بعد از نصب بك ترك

ابتدا دستور Konsole را فعال کنید

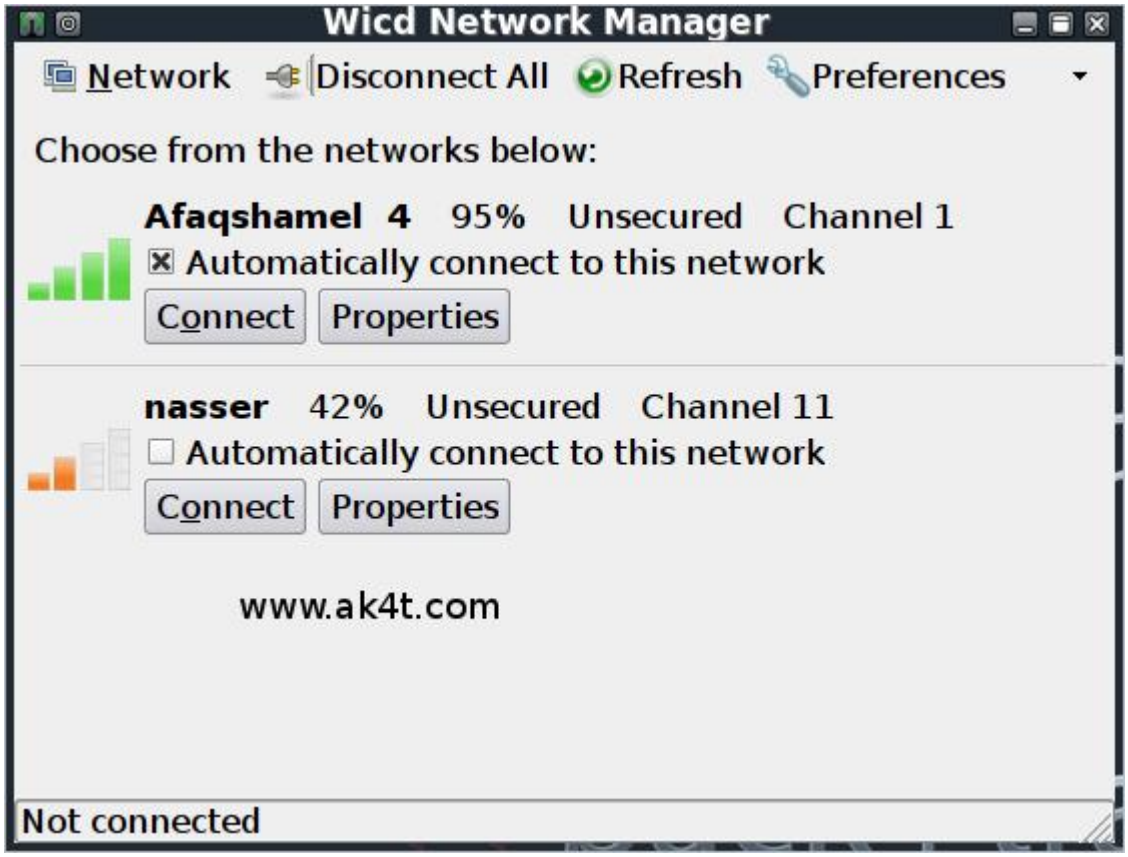
سپس دستور زیر را وارد نماید

/etc/init.d/wicd start



بعد از فعال سازی وارد بخش اینترنت در لیست برنامه شوید و برنامه wicd را فعال کنید .

بعد از آن شبکه های در دسترس برای شما نمایان می شود .



آموزش نصب ابزارهای بك ترك ۵ روی اوبونتو ۱۱.۱۰

ابتدا ترمینال رو باز کنید و sudo su **رو بزنید . بعدشم پسوردو...**

حالا دستور زیر رو وارد کنید

کد:

```
sudo gedit /etc/apt/sources.list
```

بعد به آخر ادیتوری که باز میشه این عبارت رو اضافه کنید:

کد:

```
###### Repository Backtrack

deb http://all.repository.backtrack-linux.org revolution main microverse non-free testing
deb http://32.repository.backtrack-linux.org revolution main microverse non-free testing
deb http://source.repository.backtrack-linux.org revolution main microverse non-free testing
```

بعدش save **کنید و تو ترمینال دستور زیر ور اجرا کنید.**

کد:

```
wget -q http://all.repository.backtrack-linux.org/backtrack.gpg -O- | sudo apt-key add -
```

بعدشم این

کد:

```
sudo apt-get update
```

حالا میتونید ابزارهای بك ترك مورد نظرتونو نصب کنید.

مثال:

```
sudo apt-get install nmap

sudo apt-get install nikto

sudo apt-get install framework3

sudo apt-get install hydra
```

برخی خط فرمان های مفید برای تازه کاران

startx برای روشن نمودن صفحه شروع

login = root

reboot ریستارت

/etc/init.d/networking start دستور فعال سازی اینترنت

/etc/init.d/networking stop دستور قطع اینترنت

poweroff خاموش کردن

cal نمایش تاریخ

touch دستور ایجاد فایل

rm-rf دستور حذف پوشه و محتویات آن

pentest/exploits/framework3 مسیر المیتا در بك ترك

(fast-track.py -i مسیر فست ترك برای ایجاد حفره های امنیتی /cd /pentest/exploits/fasttrack)

فشرده سازی و استخراج فایل ها

فشرده سازی zip

qzip failname.zip

استخراج zip

unzip failname.zip

فشرده سازی tar

tar -zcf zz.tar daily

استخراج tar

tar -zxf zz.tar

فشرده سازی فایل gz

tar -czvf file name.tar.gz

استخراج gz

gzip -d file.gz

استخراج rar

unrar x 123.rar

فشرده سازی فولدر یا فایل

tar -czvf file name.tar.gz file name.sql

استخراج فولدر یا فایل

tar -zxvf file name.tar.gz

فشرده سازی tar.gz

tar -czvf /home/user/public_html/n3.tar.gz n3

امر نمایش فایل یا فولدر

ls

امر نمایش فایل یا فولدر ، فایل های مخفی و صلاحیت آنها

ls -la

امر برش یا cut

wget

أمر نمایش تمامی دستورهای داده شده

history

أمر ایجاد فولدر

mkdir SNiPER

أمر حذف فایل

rm SNiPER

أمر حذف پوشه

rm -r dir

أمر برگشت به يك عمليات قبل

.. cd

أمر جستجو

find

أمر اعطای مجوز ۷۷۷

chmod 777

امر ترميم و اصلاح نظام

sudo dpkg –configure -a

امر اصلاح فايل های كه مشكل دارند

sudo apt-get install –f

حالا باهم یك سری اوامر نصب برنامه ها را مرور می کنیم

برنامه banshee (پخش صدا)

sudo apt-get install banshee

برنامه minitunes (پخش صدا ولی نیاز به اتصال اینترنتی داره)

sudo apt-get update && sudo add-apt-repository ppa:nilarimogard/w e bupd8 update

و در ادامه

sudo apt-get install minitunes

برنامه vlc (نمایش صدا و ویدیو)

apt-get install vlc

و این هم راه حل عدم اجرای آن

Terminal رو باز کنید

مرحله اول

apt-get install vlc

مرحله دوم

apt-get install okteta

مرحله سوم

okteta /usr/bin/vlc

و در صفحه نمایش یك سری اعداد را مشاهده می کنیم

به دنبال کلمه بگردید: geteuid و نام آن را به getppid تغییر دهید eu الی pp

سپس تغییر را ذخیره می کنیم و به Video & Sound می رویم

واز آن به آسانی استفاده می کنیم

برنامه معروف mplayer

apt-get install mplayer

برنامه Emesene (برای برقراری ارتباط از طریق MSN)

sudo apt-get install emesene

برنامه Skype (تماس صوتی)

sudo apt-get install skype

برنامه های فشرده سازی

sudo apt-get install unace rar unrar zip unzip p7zip-full p7zip-rar sharutils aish uudeview mpack lha arj cabextract file-roller

برنامه FileZilla (برای FTP)

sudo apt-get install filezilla filezilla-common

برنامه gftp

sudo apt-get install gftp

برنامه فیلم برداری از دکستاپ

sudo apt-get install gtk-recordMyDesktop

مرورگر گوگل کروم

sudo aptitude install chromium-Browser chromium-Browser-l10n

مرورگر اوپرا

sudo aptitude install Opera

برنامه UFW (دیوار آتشی قوی)

sudo apt-get install gufw

برنامه تورنت

sudo aptitude install deluge-Torrent

برنامه ادوبی pdf

sudo aptitude install acroread acroread-fonts

برنامه openoffice.org (که معادل آفیس می باشد)

sudo apt-get install openoffice.org

برنامه Virtualbox

sudo apt-get install virtualbox-ose

برنامه kate

sudo apt-get install kate

برنامه firestarter

sudo apt-get install firestarter

برنامه gwibber (برای ارتباط از طریق فیس بوک و توتیر و ...)

sudo apt-get install gwibber

// شکست ، هیچ گاه پایان زندگی نیست ، خودت را دریاب //

امیدوارم از این مطالب لذت برده باشید

Alien_evil33