Book Title : Server Management By Linux CentOS

Author : Alireza Azimzadeh

Nickname : Ali MP5

Editor : Mostafa kheiroddin

Nickname: Ali Tahamtan

First published :12 March 2014

Mail(P) : Ali_Parkour68@yahoo.com

Mail(S) : milani@hackermail.com

© 2014. All Rights Reserved

پیشگفتار:

هر راه به جز راه تو کج خواهد شد
بی لطف تو آسمان فلج خواهد شد

ما منتظران اگر بخواهیم همه
امسال همان سال فرج خواهد شد

ازفکرگناه پاک بودن عشق است
ازهجرتو سینه چاک بودن عشق است
آن لحظه که راه می روی آقاجان
زیرقدم تو خاک بودن عشق است

پدرم، تاج سرم، چشم به راهت بودم — همه دم عاشق لبخند نگاهت بود
ای فلک از چه زدی آتش غم بر جگرم — کاش جای پدرم من سر راهت بودم
ای سفر کرده به معراج، به یادت هستیم — ای پدر ما همگی چشم به راهت هستیم
تو سفر کردی وآسوده شدی از دوران — همه ماتم زده هر لحظه به یادت هستیم
گریه کردم، اشک بر داغ دلم مرهم نشد — ناله کردم ذره ای از دردهایم کم نشد
از گلستان بوی گل بسیار بوئیدم ولی — از هزاران گل گلی همچون پدر پیدا نشد

افرادی که در رشته های مرتبط با نرم افزار یا IT در حال فعالیت هستند این موضوع را می دانند که: امنیت لینوکس همیشه از مایکروسافت پیشرفته تر بوده است. پس چرا به سراغ سیستم های لینوکسی نمی رویم؟ دلیل آن اضطراب و نگرانی مدیران شرکت ها بوده است؟ یا اختلاف حقوق، بین متخصصین لینوکس با مایکروسافت؟ یا افزایش دست های مایکروسافتی نسبت به لینوکس؟ که این امر باعث شده است اگر یک شخص بنا به دلایلی نخواهد به کار با شرکت مربوطه ادامه دهد، مدیر شرکت در کوتاه ترین زمان ممکن اقدام به جذب یک نیروی متخصص دیگر کند؟ و کلی سوال دیگر....

اگر چه از این اتفاقات خیلی دلگیر هستم؛ اما چه می شود کرد ....؟

به همین خاطر اینجاب سعی کردم تا آخرین لحظه از نوشتن تا ویرایش، به روزترین مطالب را در این کتاب قرار دهم تا توانسته باشم دِین خود را هرچند اندک، به دنیای کاربران لینوکس ادا نمایم. در این امر سعی کردم کتاب هایی را ترجمه و تألیف کنم که جای خالی آنها به شدت در محیط های کاری احساس می شود.

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، دانشجوی دوره کارشناسی ناپیوسته آزاد کرج در رشته مهندسی تکنولوژی نرم افزار می باشم. مثل هر کار دیگری، باید حاصل تلاش علمی خود را عرضه کنیم؛ باید ارائه کنیم؛ باید کاری کنیم که مخاطبِ ما، کار انجام شده را دریابد. در غیر این صورت از دید او، بین ما و کسی که کاری انجام نداده است، تفاوت چندانی وجود ندارد. در واقع، در هرکاری(بله هر کاری)، که هر عنصری انجام می‌دهد، حداقل، بخشی از آن ارائه است. و این در تمام طول عمر آن عنصر، مطرح است. به این ترتیب ارائه واقعاً مهم است. بخشی از تخصص ها CEH, Hack&Security, Network+, CCNA RHCE, RHCSA, LPIC-1 است.امیدوارم کتاب الکترونیکی حاضر مورد قبول شما خوانندگان عزیز واقع شود.

خداوندا

به بزرگیـــــــت قســـــم...

در عکس های دسته جمعی...

جای هیچ پدر و مـــــــادری رو خـــالی نذار...

آمیـــــــن

تقدیم به خانواده

عزیزتـــر از جانم

که با لطف و صبرشان

مرا در تمام مراحل

زندگی کمک کردند.

سخن نویسنده :

- **برای روح تمام اموات که یک روز پیش ما و شما بودند و حالا نیستند یک صلوات بفرستید و این آدم حقیر را برای خدمت بی منّت در راه خدا دعا کنید.**
- **قرار بود امتیاز این کتاب توسط یکی از انتشارات معروف که در زمینه کامپیوتر مشغول به فعالیت است، خریده و چاپ شود و بابت کار تألیف و ترجمه آن مبلغی به اینجانب پرداخت شود. اگر من این کار را می کردم کسانی که بنیه خرید این کتاب را نداشتند نمی توانستند از مطالب به روز این کتاب استفاده کنند، چون هزینه خرید این کتاب قرار بود معادل 25000 تا 30000 هزار تومان باشد.**
- **نوشتن بخش دوم این کتاب ملزم به خرید یک VPS (CentOS) قوی، چند لایسنس از پنل های مختلف، دامین و هاست .... می باشد. به همین خاطر، اگر دوستان برای همکاری تمایل داشتند، می توانند از طریق شماره حساب زیر و یا با قرض دادن موقت سرور و ... به اینجانب، مرا برای به پایان رساندن این کتاب بسیار جامع یاری کنند.**

لازم به ذکر است حداقل مبلغ پرداختی 5000 هزار تومان می باشد، در صورت تمایل مبالغ بیشتری نیز می توانید پرداخت نمایید.

بانک: مسکن

صاحب حساب: علیرضا عظیم زاده

شماره کارت: 6280 2314 4546 9369

شماره حساب: 710103359166

ایمیل جهت مکاتبه و همکاری:

Ali_parkour68@yahoo.com

milani@hackermail.com

در وبلاگ زیر می توانید از کارهایی که اینجانب در زمینه تألیف و ترجمه کتاب انجام داده ام و دوستانی که حمایت کرده اند، با خبر شوید:

http://www.aliazimzadeh.blogfa.com

نکته مهم: در صورت داشتن هر گونه سؤال در مورد مطالب آموزشی این کتاب می توانید به فروم های زیر مراجعه کنید:

http://forum.mihansetup.com/

http://forum.irsecteam.org/forum.php

فهرست مطالب

مقدمه:

این کتاب بر اساس بازه نسخه های 6.x می باشد، یعنی: شما می توانید هر یک از نسخه های این توزیع را که اول آن با 6 شروع می شود را دانلود کرده و کار با آن را آغاز کنید.

مثل:

6.1 6.2 6.3 6.4 6.5 , ...

نکته مهم:

خواندن این کتاب به کسانی پیشنهاد می شود که مدارک Network+ (اجباری) و LPIC-1 (اجباری) اخذ نموده اند و یا اینکه آشنایی کامل با توزیع های لینوکسی داشته و کار کرده اند.

از شما مخاطب عزیز خواهش می کنم به اخطار، نکات و پیشنهاداتی که در فصل ها به آن اشاره شده دقت کنید، تا در ادامه دچار مشکل نشوید.

در صورت مشاهده ایراد یا خطای فنی در متون با ایمیل نویسنده در ارتباط باشید و آنها را به ایمیل نویسنده با عنوان "مشکل فنی در کتاب CentOS" ارسال نمایید.

با تشکر از لطف شما عزیزان.

مرور کلی بر فصل ها:

فصل اول:

در این فصل با توزیع لینوکس CentOS ، ویژگی ها و روش های نصب آن آشنا خواهید شد.

فصل دوم:

در این فصل در مورد کار با دستورات پایه، مخزن ها، مدیریت دسترسی و حساب های کاربری، متن ها، فایل ها و پوشه ها صحبت خواهیم کرد. این فصل شامل دستورات:

pwd, cd, mkdir, mv, rm, rmdir, touch, file, cp, find, echo, rpm, ls, vi, nano, cat, tail, head, chmod, chown, ll, grep, help, useradd , …

می باشد.

فصل سوم:

در این فصل در مورد مدیریت پروسه ها، سرویس ها، زمان بندی اجرای آنها، گرفتن پشتیبان از فایل ها و فولدرها و مانیتورینگ سیستم صحبت خواهیم کرد. این فصل شامل دستورات:

chkconfig, service, init, shutdown, free, top, sync, ps, kill, pidstat, cron, at, mailx, mutt, rsync, diff , …

می باشد.

فصل چهارم:

در این فصل در مورد تکنولوژی RAID، LVM ، پیاده سازی بخش فیزیکی (هارد دیسک) و حیاتی یک سرور و مدیریت پارتیشن ها صحبت خواهیم کرد. این فصل شامل دستورات:

mdadm, df, dmseg, fdisk, parted, partprobe, quota, fstab, quotacheck, grpguota, edquota, repquota , …

می باشد.

فصل پنجم:

در این فصل در مورد کارهایی که باعث افزایش امنیت در سرور می شود و از نفوذ هکرها به سرور تا حد قابل قبولی جلوگیری می کند ، صحبت خواهیم کرد.

آشنایی و نصب CentOS

در این فصل با توزیع سِنت-او-اِس و روش های مختلف نصب آن آشنا خواهید شد.

CentOS چیست؟

این توزیع بر پایه RHEL(RedHat) استوار بوده و تنها تفاوت آن در این است که RHEL یک نسخه تجاری است، اما توسعه و پشتیبانی سِنت-او-اِس (CentOS) توسط جمعی از کاربران و به صورت رایگان انجام می گیرد. در سال ۲۰۰۶ توسعه دهنده اصلی Tao Linux (کپی دیگری از توزیع RHEL) از توسعه آن کنارگیری و به جمع توسعه دهندگان سِنت-او-اِس پیوست، این امر باعث شد کاربران Tao به استفاده از سِنت-او-اِس روی آورند. طی آمار ارائه شده در جولای ۲۰۱۰ توسط موسسه World Wide Web Technology Surveys این سیستم‌عامل با اختصاص ۳۰٪ از سهم توزیع‌های نصب شده بر روی سرورهای فعال به خود، از توزیع Debian پیشی گرفته و به عنوان محبوب‌ترین توزیع لینوکس نصب شده بر روی سرورها شناخته شد، و این مقام را تا ژانویه ۲۰۱۲ حفظ نمود. پس از آن توزیع Debian با اختلاف بسیار ناچیز موفق شد مجددا مقام اول را از آن خود کند.

به طور قطع می‌توان گفت سیستم‌عامل CentOS نسخه رایگان RedHat می‌باشد.لایسنس RHEL به این صورت است که دسترسی به مد منبع آن رایگان است ولی نسخه build شده و قابل اجرای آن پولی است به همین دلیل پس ازعرضه هر نسخه از RHEL با مدتی تاخیر تیم پروژه CentOS کد منبع RHEL که متن باز(open source) است را می گیرد و build می کند و نسخه قابل نصب آن را به صورت رایگان در اختیار علاقمندان قرار می دهد.

خبر مهم سال ۲۰۱۴:

در حالی که اینجانب مشغول به نوشتن این کتاب کاربردی بودم، سعی کردم تا آخرین لحظه و قبل از انتشار اولین ویرایش این کتاب، اخباری داغ در مورد این توزیع در اختیار شما مخاطبان عزیز قرار بدهم.

آن خبر مهم این است:

RedHat و CentOS برای پیشرفت OpenSource به هم می پیوندند.

http://www.redhat.com/about/news/press-archive/2014/1/red-hat-and-centos-join-forces

برای کسب اطلاعات بیشتر در مورد این توزیع می توانید به سایت های زیر مراجعه کنید:

http://en.wikipedia.org/wiki/CentOS

http://www.makeuseof.com/tag/dont-want-to-pay-for-red-hat-linux-try-centos-instead/

http://www.rackaid.com/blog/things-to-know-about-centos-linux/

http://www.tejasbarot.com/2013/09/18/wha -is-the-relationship-between-centos-rhel-and-fedora/

دانلود توزیع CentOS :

برای آشنایی با این توزیع می توانید از لینک های زیر برای دانلود استفاده کنید (فقط از نظر ویژگی (قابلیت ها) با هم تفاوت دارند):

http://ftp.linux.ncsu.edu/pub/CentOS/6.4/isos/i386/CentOS-6.4-i386-minimal.iso

http://ftp.linux.ncsu.edu/pub/CentOS/6.4/isos/i386/CentC_-6.4-i386-netinstall.iso

http://ftp.linux.ncsu.edu/pub/CentOS/6.4/isos/i386/CentOS-6.4-i386-LiveCD.iso

http://ftp.linux.ncsu.edu/pub/CentOS/6.4/isos/i386/CentC_-6.4-i386-LiveDVD.iso

تا این لحظه از نوشتن کتاب، آخرین ورژن منتشر شده برای کار ما 6.4 می باشد:

پیشنهاد:

در صورت انتشار نسخه جدید، آن را دانلود کنید تا بروزترین بسته ها را برای کار در اختیار داشته باشید.

برای سیستم های ۳۲بیتی:

dvd-1:

http://centosmirror.go4hosting.in/centos/6.4/isos/i386/CentOS-6.4-i386-bin-DVD1.iso

dvd-2:

http://centosmirror.go4hosting.in/centos/6.4/isos/i386/CentOS-6.4-i386-bin-DVD2.iso

برای سیستم های ۶۴بیتی:

dvd-1:

http://centosmirror.go4hosting.in/centos/6.4/isos/x86_64/CentOS-6.4-x86_64-bin-DVD1.iso

dvd-2:

http://centosmirror.go4hosting.in/centos/6.4/isos/x86_64/CentO_-6.4-x86_64-bin-DVD2.iso

در صورت کار نکردن لینک های بالا می توانید به لینک های زیر مراجعه کنید:

http://ftp.linux.ncsu.edu/pub/CentOS/

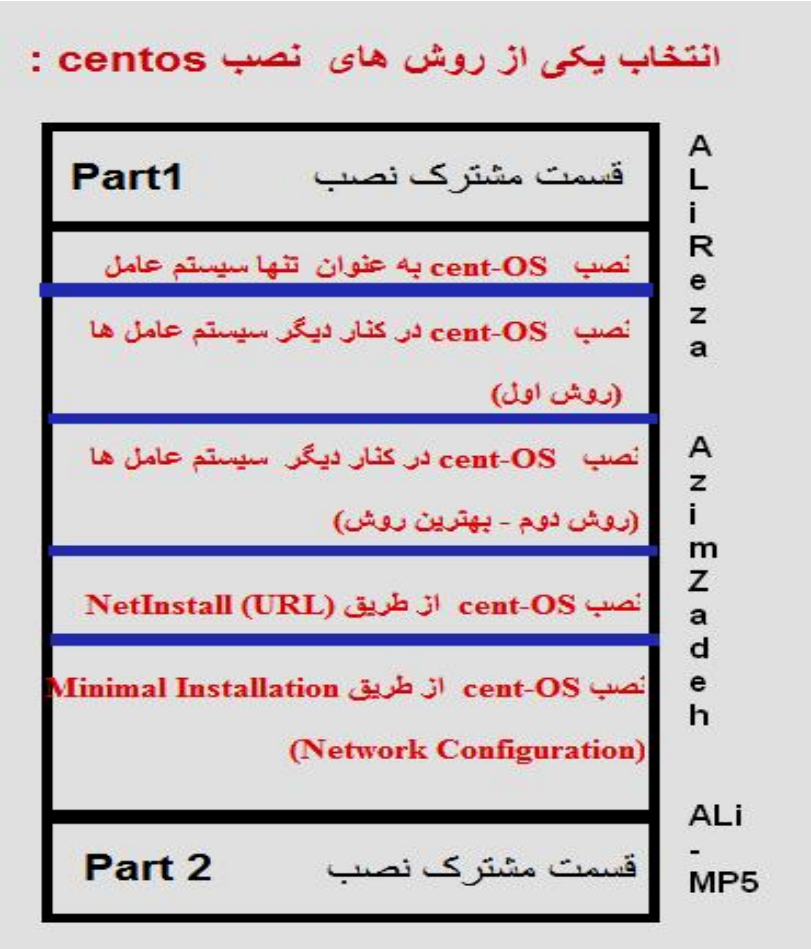
http://mirror-status.centos.org/

http://wiki.centos.org/Download

نکته۱: i386 برای سیستم های ۳۲ بیتی می باشد.

نکته۲: x86-64 برای سیستم های ۶۴ بیتی می باشد.

نمودار کلی روند نصب CentOS :



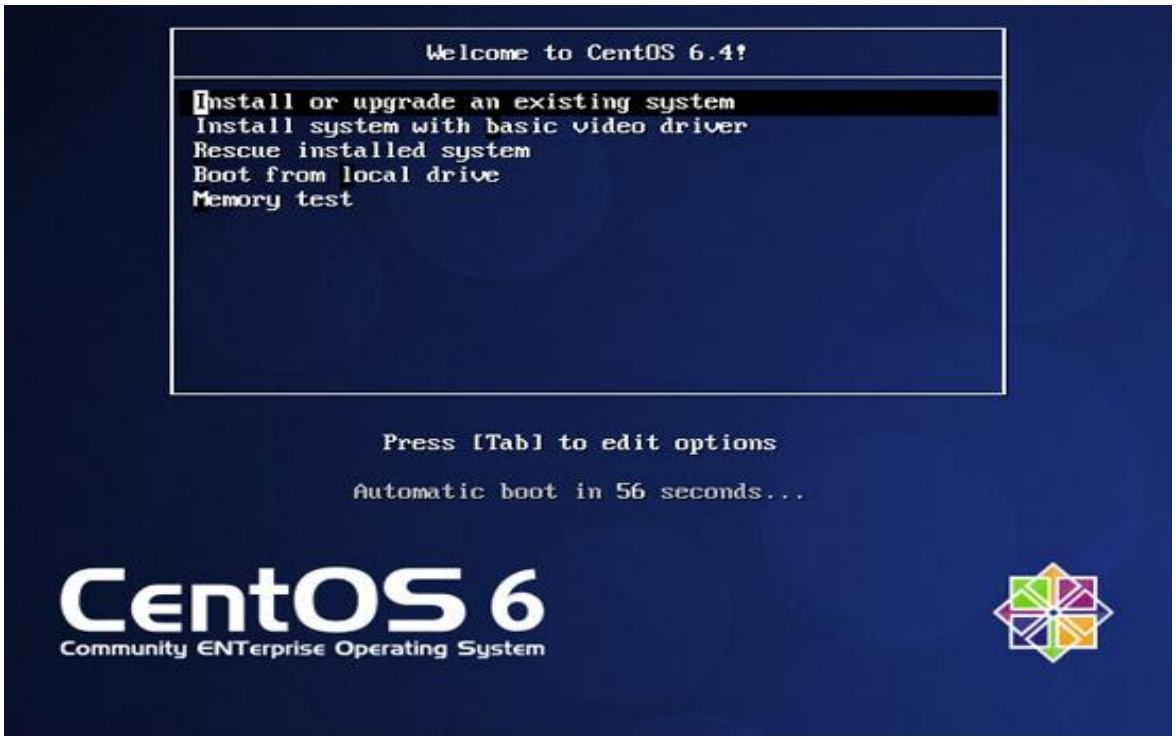
نصب CentOS 6.x (قسمت اول مشترک نصب):

این قسمت، مرحله ابتدایی در تمام روش های نصب این OS (سیستم عامل) می باشد. این بخش شامل۱۴ مرحله می باشد. سپس شما باید روش نصبی را که مد نظر دارید بخوانید و مطالعه کنید و بعد از انجام مراحل آن بخش، مجدد به ادامه نصب (قسمت مشترک نصب) می رسید که آن نقطه مشترک بعد از Restart کردن OS است.

۱) ابتدا dvd-1 را قرار دهید.

۲) بعد از بوت شدن dvd-1، شما باید صفحه زیر را ببینید، سپس گزینه Install or upgrade existing system را انتخاب کنید.

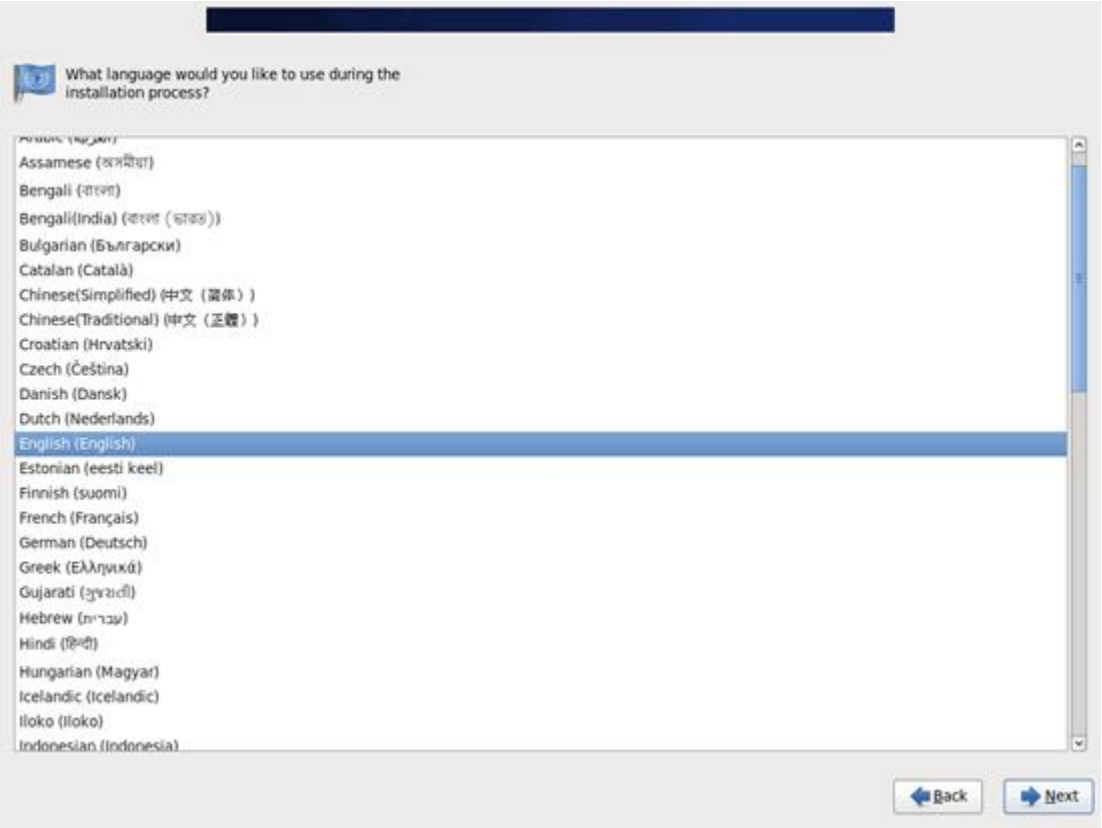
نکته: گزینه دوم را هم می توانید انتخاب کنید.



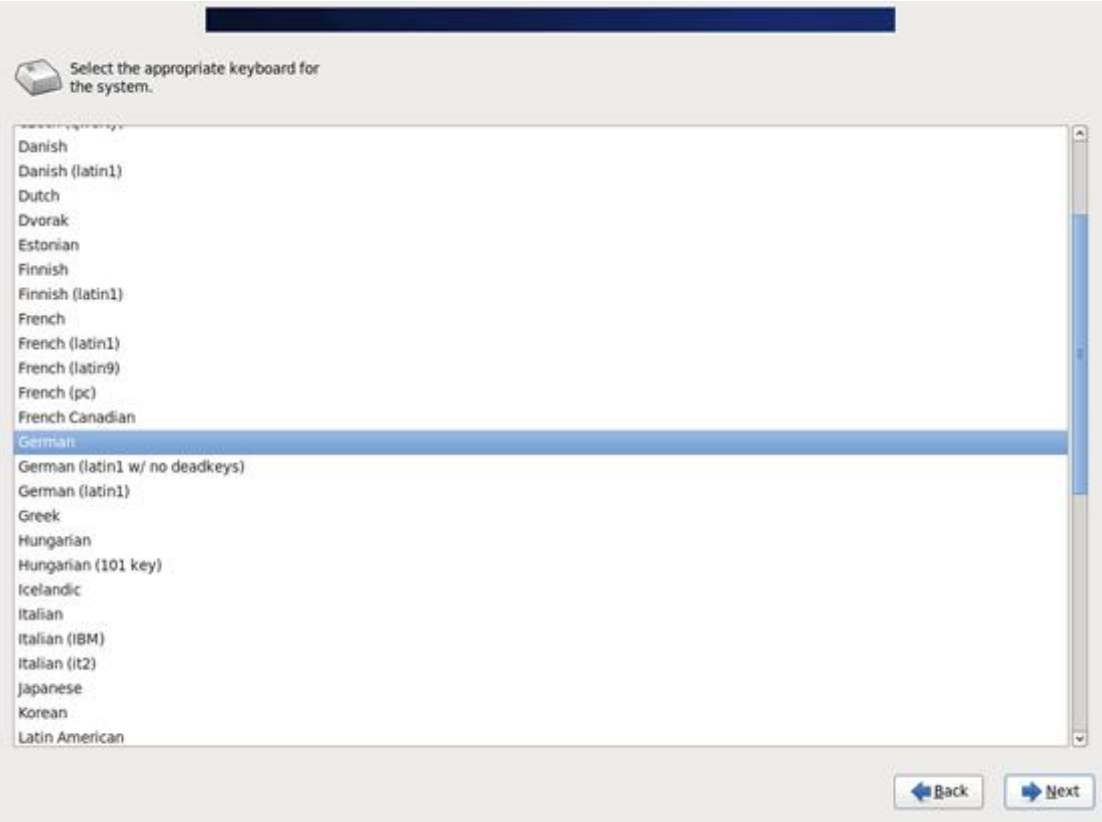
۳) در این مرحله شما می توانید رسانه خود را مورد بررسی قرار دهید که یک وقت دچار مشکل نشده باشد، در صورتی که اطمینان دارید گزینه **Skip** را انتخاب کنید:

۴) سپس وارد محیط خوش آمد گویی می شود، شما روی دکمه **next** کلیک کنید:

۵) زبان خود را در اینجا انتخاب کنید:



۶) سپس زبان **keyboard** را انتخاب کنید:



۷) اگر می خواهید cent-os را روی local-hard خود نصب کنید گزینه اول را انتخاب کنید، و اگر می خواهید روی شبکه نصب کنید گزینه پایینی را انتخاب کنید:

گزینه ما: Basic Storage Devices

Note:

Basic Storage Devices

Select **Basic Storage Devices** to install Fedora on the following storage devices:

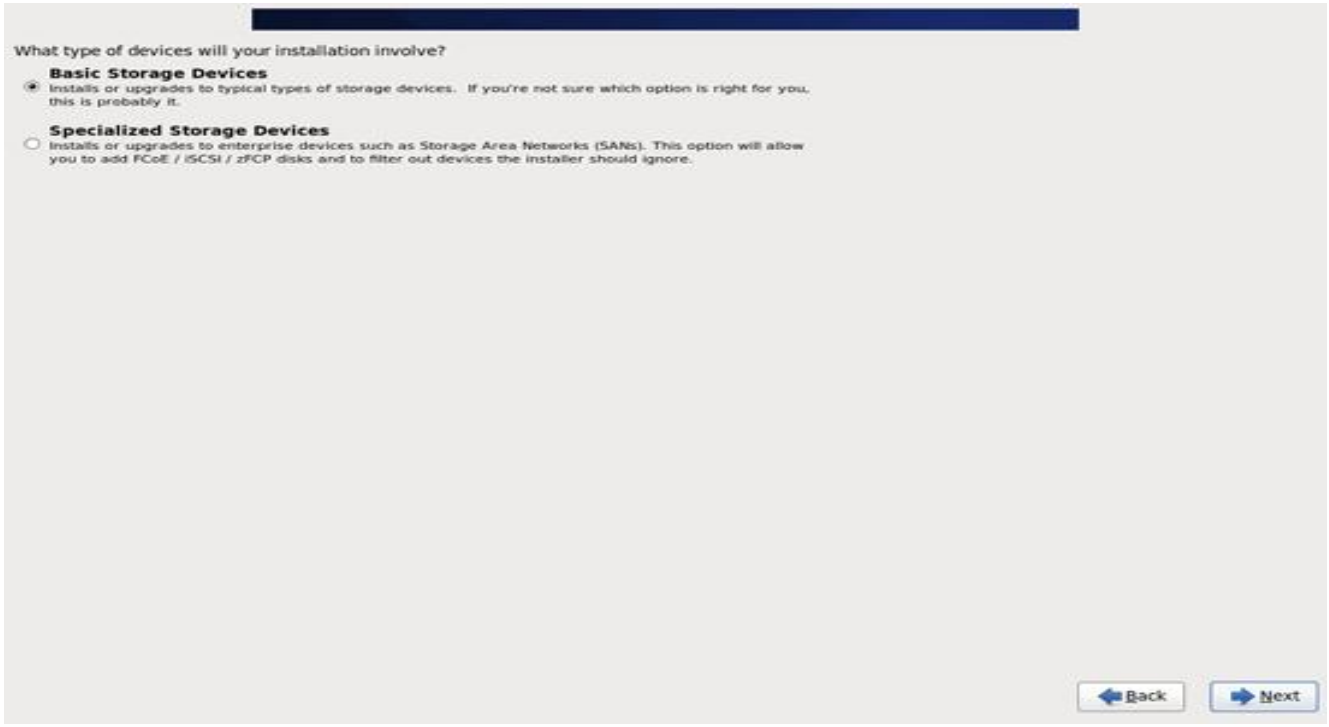
- hard drives or solid-state drives connected directly to the local system.

Specialized Storage Devices

Select **Specialized Storage Devices** to install Fedora on the following storage devices:

- *Storage area networks* (SANs)
- Direct access storage devices (DASDs)
- Firmware RAID devices
- Multipath devices

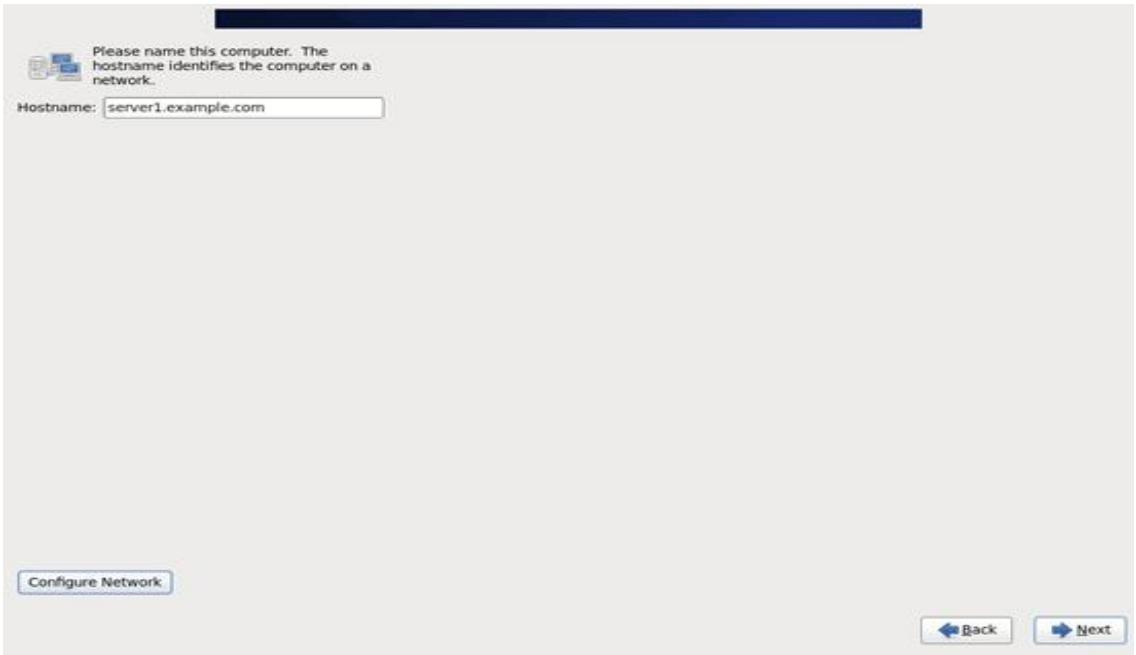
Use the **Specialized Storage Devices** option to configure Internet Small Computer System Interface (iSCSI) and *FCoE* (Fiber Channel over Ethernet) connections.



نکته: در صورتی که تمایل به انتخاب گزینه specialized storage device دارید، نتیجه اش بدین شکل می باشد:

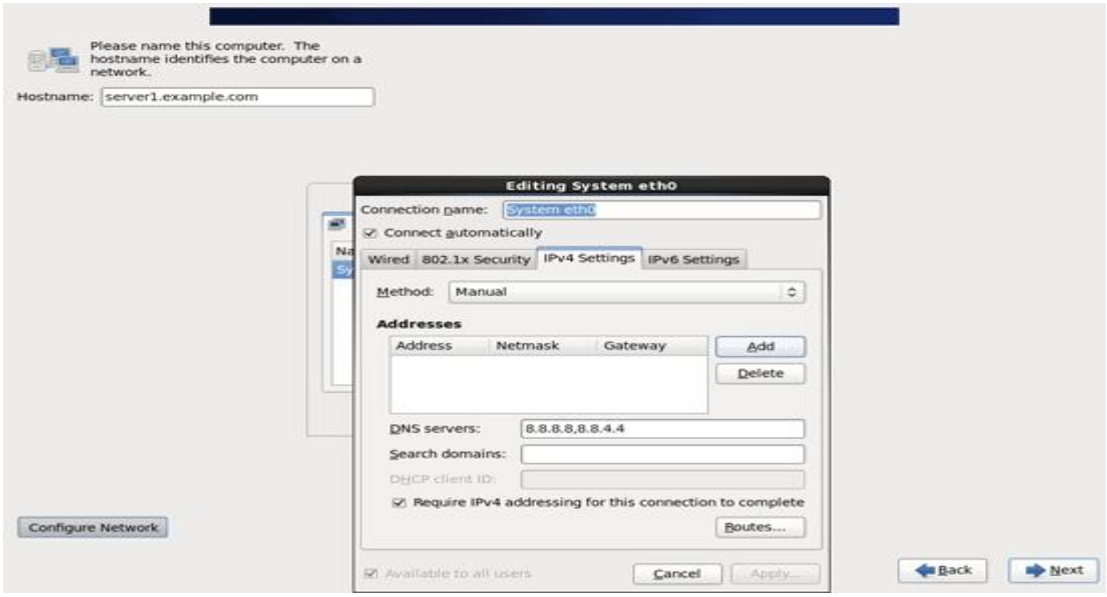
۸) در صورت دیدن عکس زیر، طبق شکل عمل کنید (تیک زدن Yes, Discard... و سپس apply(next)):

۹) در مرحله بعدی یک نام انتخاب کنید :



۱۰) سپس در عکس بالا که دید، در پایین، سمت چپ روی configure network کلیک کنید. به برگه wired بروید و سپس روی edit کلیک کنید.

۱۱) وارد زیر برگه ipv4 شوید و تنظیماتی را که مد نظر دارید اعمال کنید و تیک connect automatically را هم بزنید:

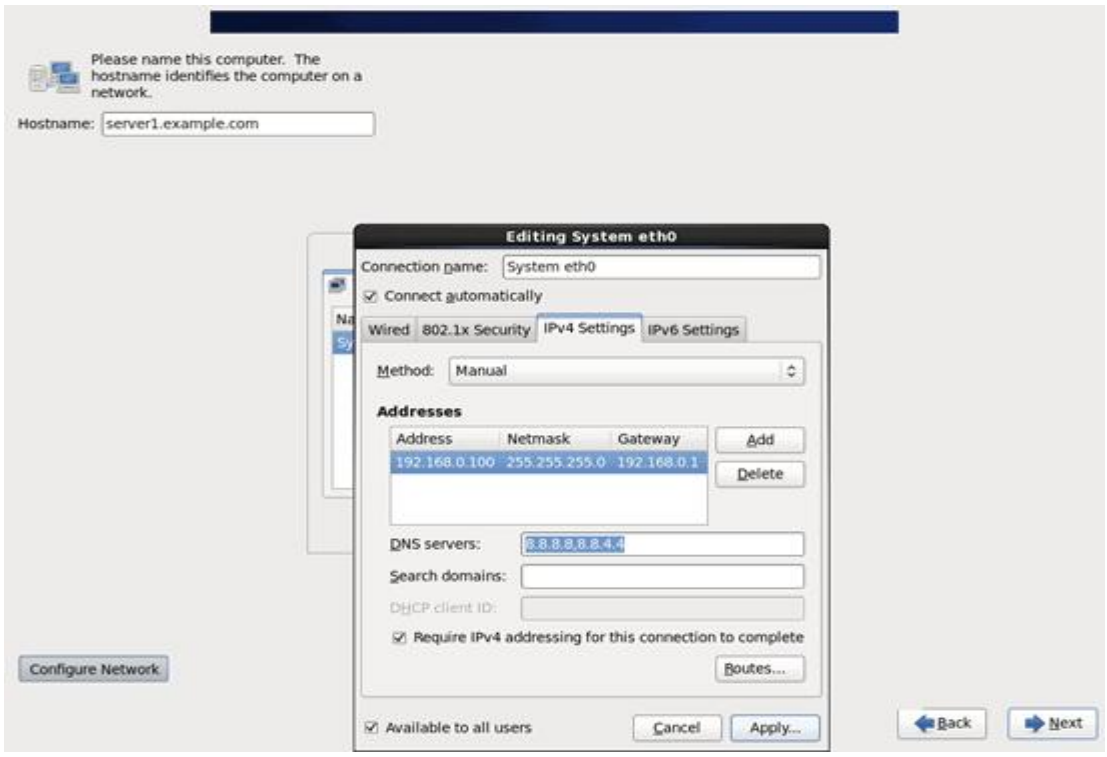


مثل:

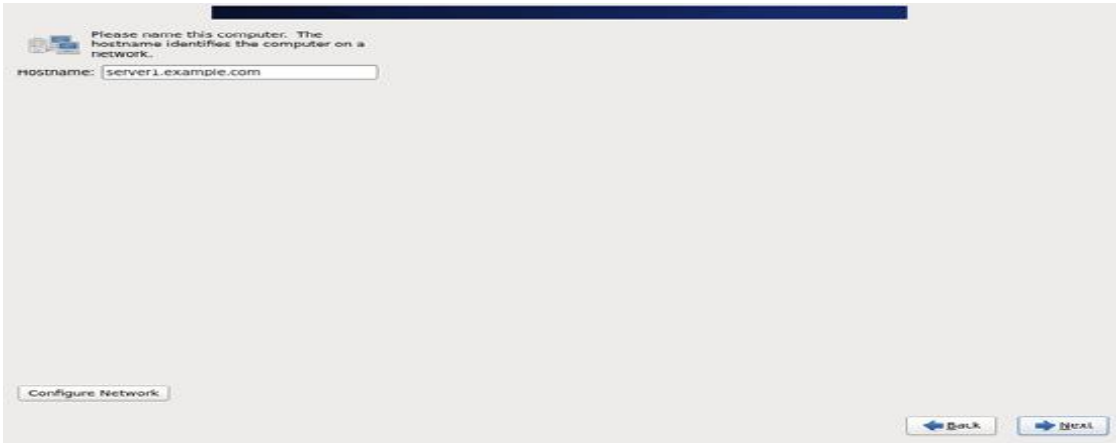
ip address: 192.168.1.5

netmask: 255.255.255.0

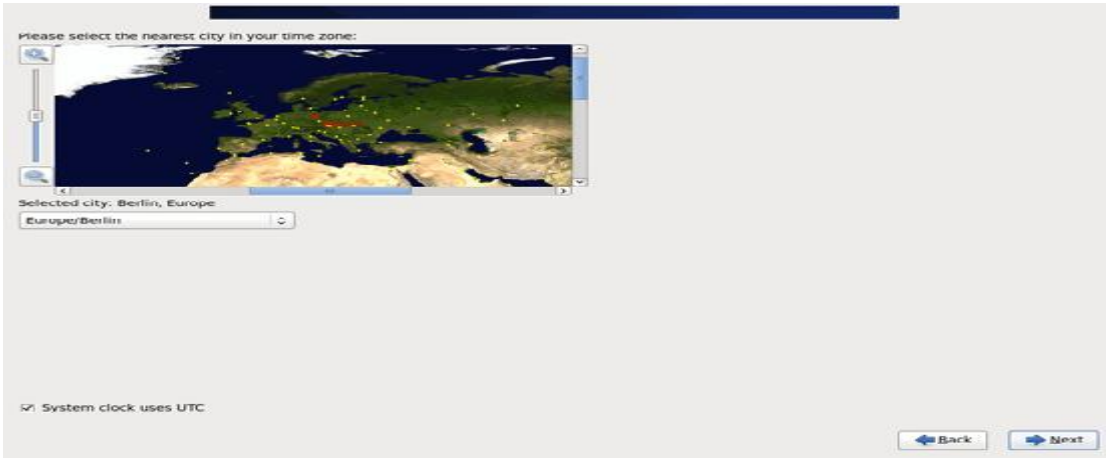
gateway: 192.168.1.1



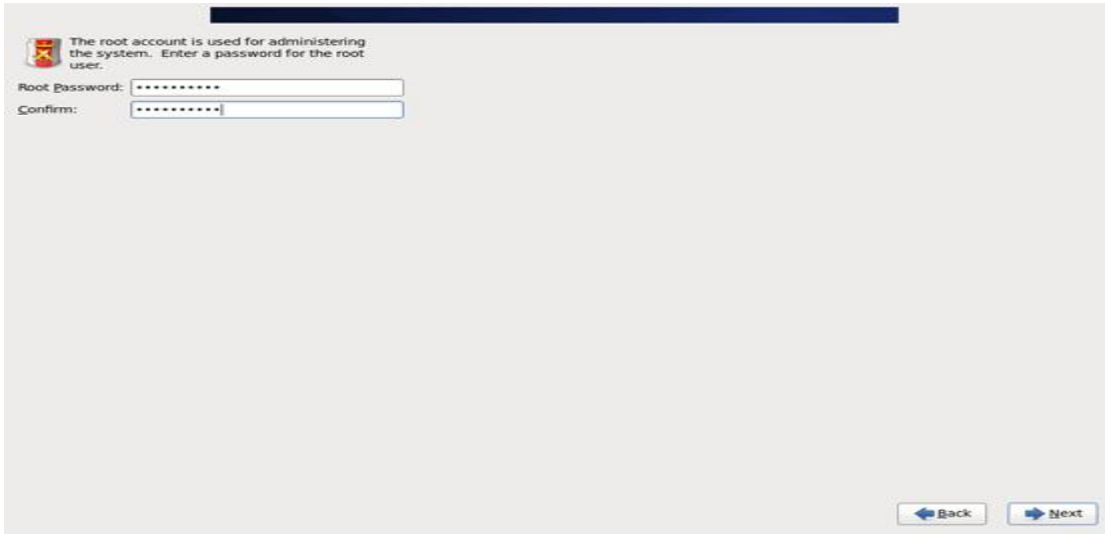
۱۲) سپس روی next کلیک کنید:



۱۳) تعیین zone-location-time خودتان:



۱۴) انتخاب یک پسورد قوی برای کاربر root :



نکته۱: تا اینجا قسمت مشترک تمام روش های نصب را توضیح دادیم، شما در ادامه باید روش خود را انتخاب کرده و کارهای گفته شده در نصب مورد نظر انجام دهید.

نکته۲: ادامه (قسمت دوم مشترک نصب) در صفحه ۴۲ است.

اخطار: از این مرحله بعد دقت لازم را داشته باشید تا به اطلاعات شما آسیبی نرسد.

اخطار: تمام روش های نصب را بخوانید و سپس، بهترین روش نصب را انتخاب کنید.

کلاس های نصب CentOS:

۱. Desktop Class:

این کلاس برای کسانی که می خواهند به صورت گرافیکی (GUI) با این OS در تعامل باشند پیشنهاد می شود.

شامل بسته های: gnome desktop , desktop-tools , open-office-org , internet-tools و ....

۲. Web Server Class:

این کلاس برای کسانی که می خواهند حداقل بسته های لازم برای راه اندازی سرور را داشته باشند پیشنهاد می شود.

شامل بسته های: Apache , SQL , Print-server و ....

نکته: شامل DNS-server , DHCP-server , FTP-server نمی باشد.

۳. Virualization Class :

این کلاس بسته های ضروری برای راه اندازی تکنولوژی های مجازی ساز را فراهم می کند.

۴. Clusterig Class :

این کلاس برای کسانی که با Worker Nodes و HPC(High Performance Computing) مشغول به کار هستند پیشنهاد می شود.

۵. Storage Clustering Class :

این کلاس برای کسانی که با GFS File System و سرورهایی که متصل به SAN(Storage Area Network) مشغول به کار هستند پیشنهاد می شود.

پیشنهاد: برای انتخاب سفارشی بسته ها می توانید از گزینه customize now استفاده کنید.

نصب CentOS به عنوان تنها سیستم عامل :

بعد از انجام مرحله۱۴، طبق مراحل توضیح داده شده عمل کنید.

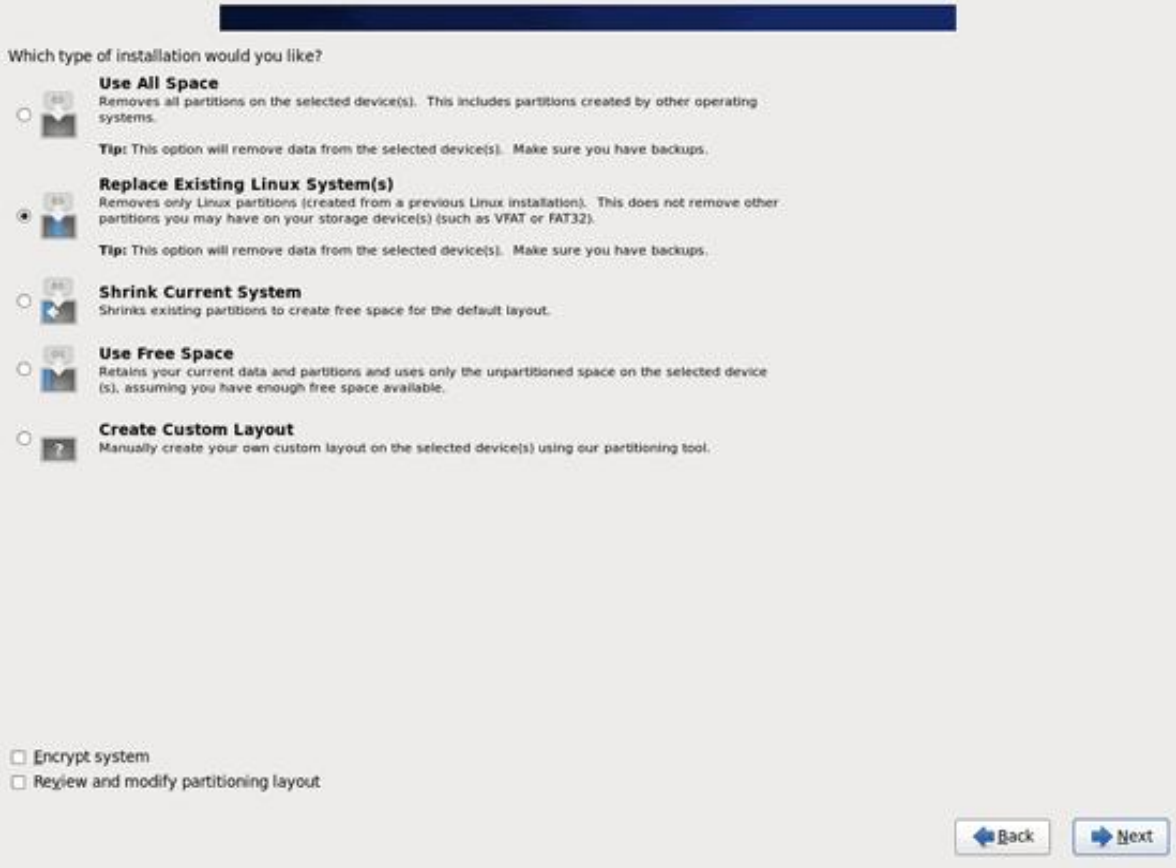
۱. **شما باید گزینه اول را انتخاب کنید.**

۲. **در پایین تیک review and modify.... را بزنید.**

۳. **روی next کیلک کنید.**

Use all space:

از تمام فضای هارد شما برای نصب این (سیستم عامل) OS استفاده می شود. یعنی تمام هارد شما فرمت خواهد شد.

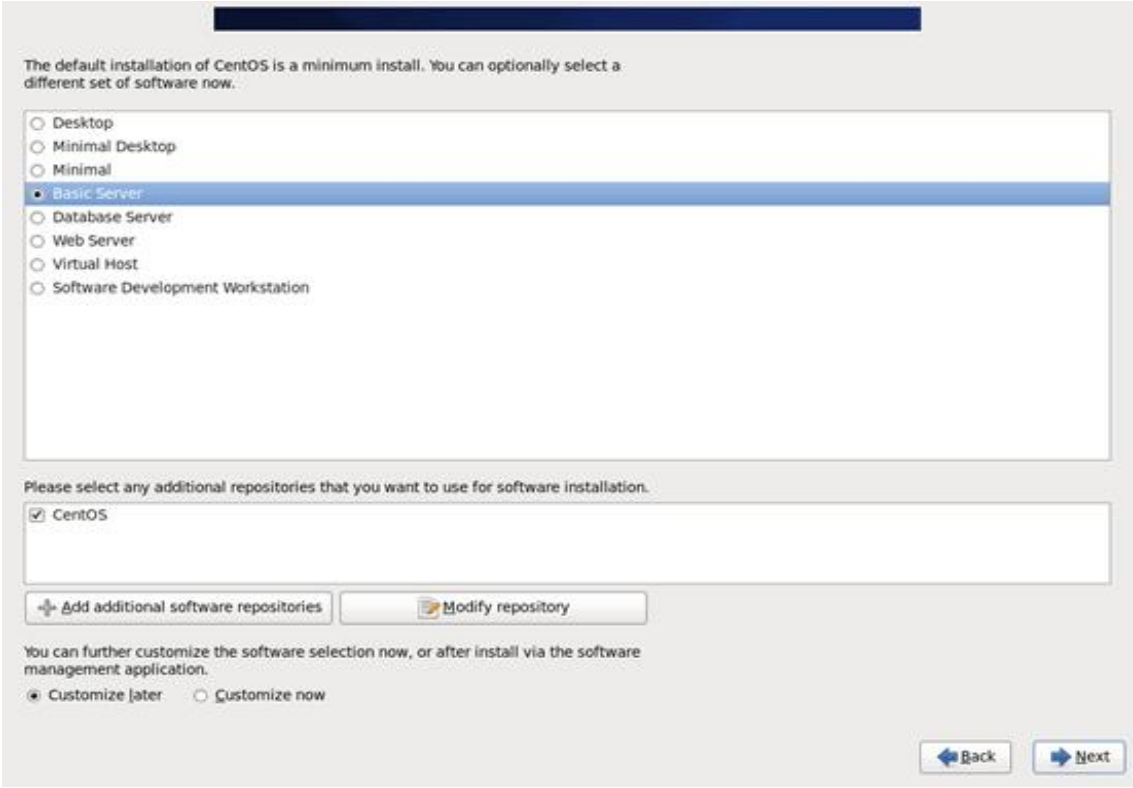


در صورت مشاهده متن زیر، بر روی ... write changes کلیک کنید.

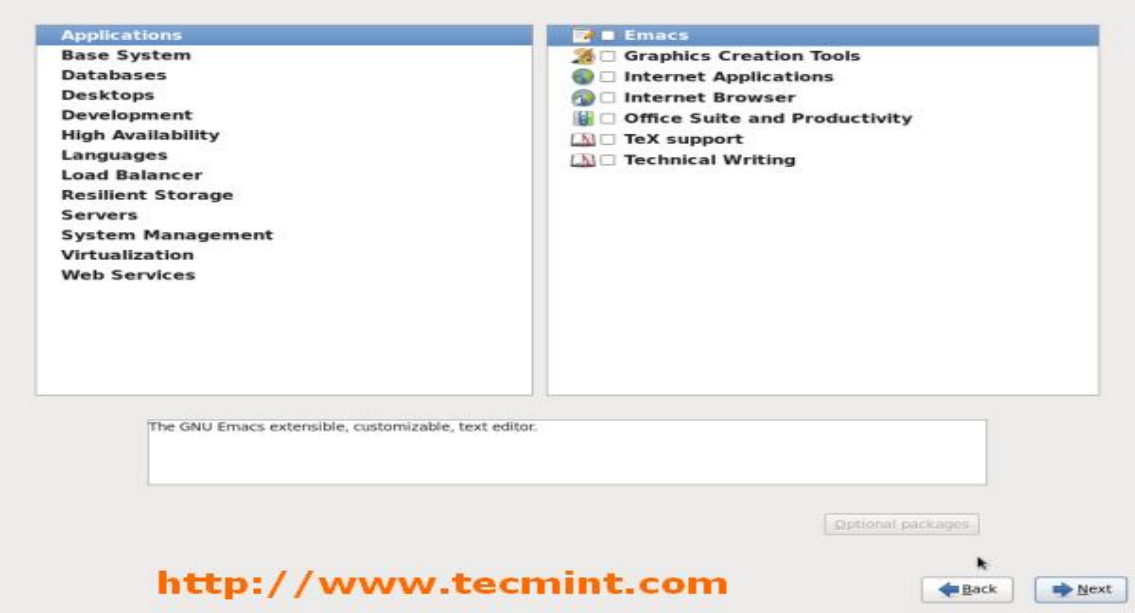
۴. **سپس فقط بر روی گزینه next کلیک کنید و گزینه های دیگر را در مراحل بعد اصلا تغییر ندهید. تا به شکل مرحله ۶ برسید.**

۵. در این مرحله شما باید نوع **cent-os** را انتخاب کنید. با توجه به نیازی که دارید انتخاب کنید.

هر یک از گزینه ها یک سری از بسته ها را روی هارد شما نصب می کند.



۶. سپس در همین مرحله(عکس بالا) می توانید بسته ها را هم به صورت دلخواه با توجه به نیازتان انتخاب کنید. برای این کار روی **Customize now...** در پایین کلیک کنید و سپس روی **next** کلیک کنید، در ادامه صفحه پایین برای شما خواهد آمد:



پیشنهاد: اگر برای اولین بار می خواهید کار با این توزیع را تجربه کنید، حتما بسته های گرافیکی KDE Desktop و Gnome Desktop را نصب نمایید.

۷. سپس فقط بر روی گزینه next یا install کلیک کنید و گزینه های دیگر را در مراحل بعد اصلا تغییر ندهید تا کار نصب تمام شود.

اگر از این روش نصب استفاده کرده اید در ادامه باید به بخش (قسمت دوم نصب مشترک) برگردید تا ادامه نصب را بعد از Restart سیستم عامل انجام دهید. (رجوع به صفحه۴۲)

نصب CentOS در کنار دیگر سیستم عامل ها (روش اول) :

نکته مهم: روش نسبتا خوبی است، اما روش دوم که بعد از این روش قرار است توضیح دهم، بهترین روش برای نصب است.

۱) شما باید یک فضای خالی در هارد خود ایجاد کنید. برای این کار باید نرم افزار Ease US Partition Master-free Home Edition نسخه رایگان آن را دانلود کنید.

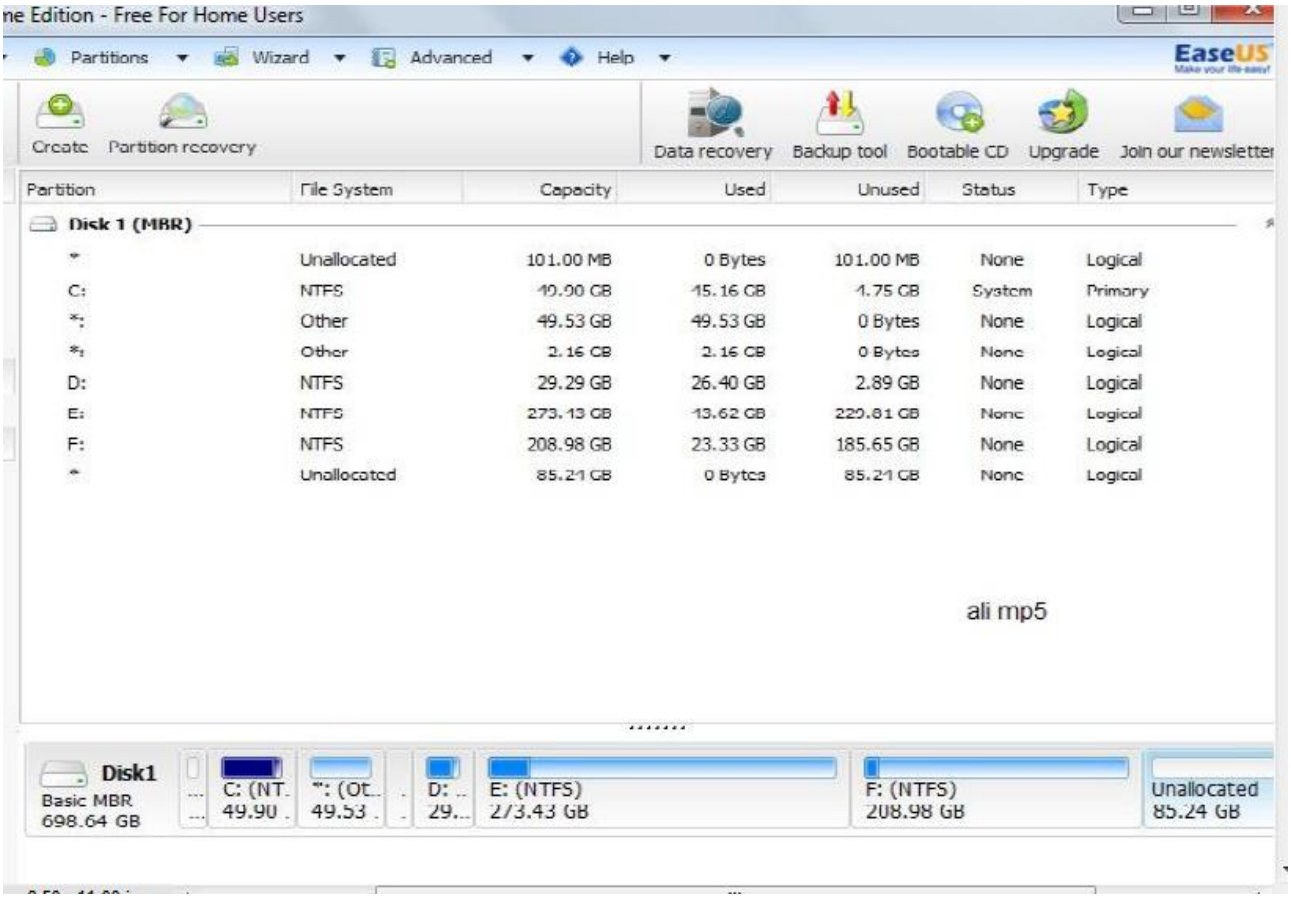
برای دانلود به سایت زیر بروید:

www.partition-tool.com

۲) وارد بخش portions manager شوید.

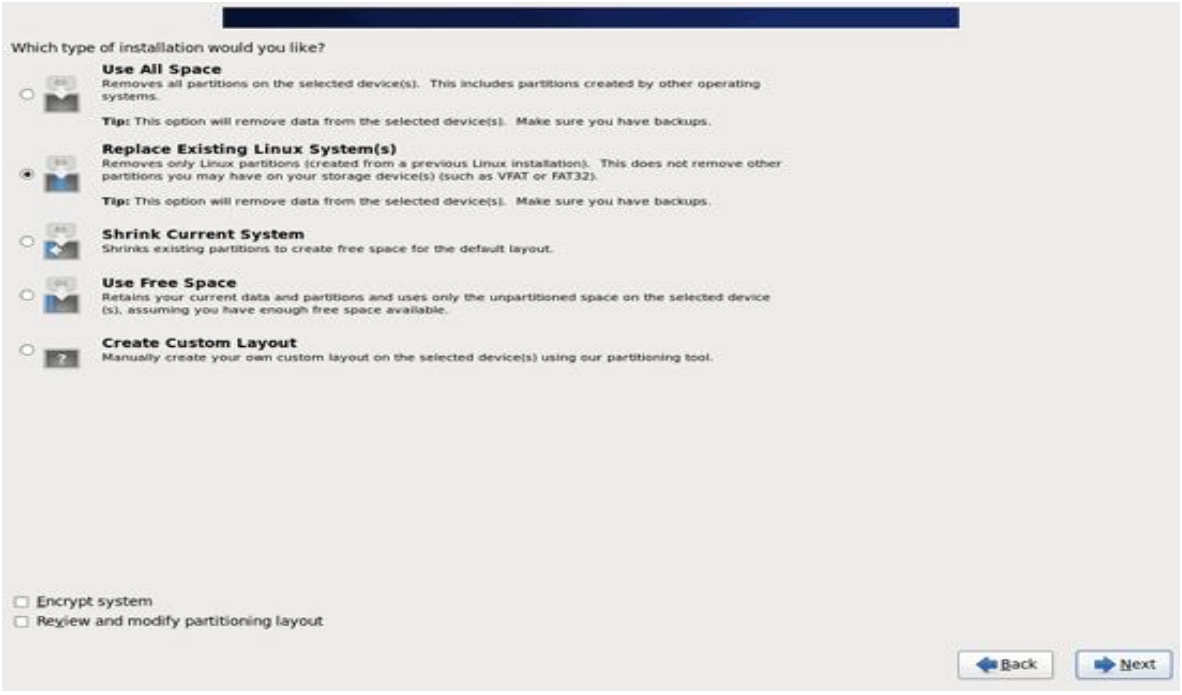
۳) باید فضایی به نام Unallocated با ظرفیت حداقل 73GB بسازید. برای این کار بر روی پارتیشن مورد نظر کلیک راست کرده و گزینه Delete را انتخاب کنید.

مثال: در شکل زیر فضایی با ظرفیت 85GB را ایجاد کرده ام.



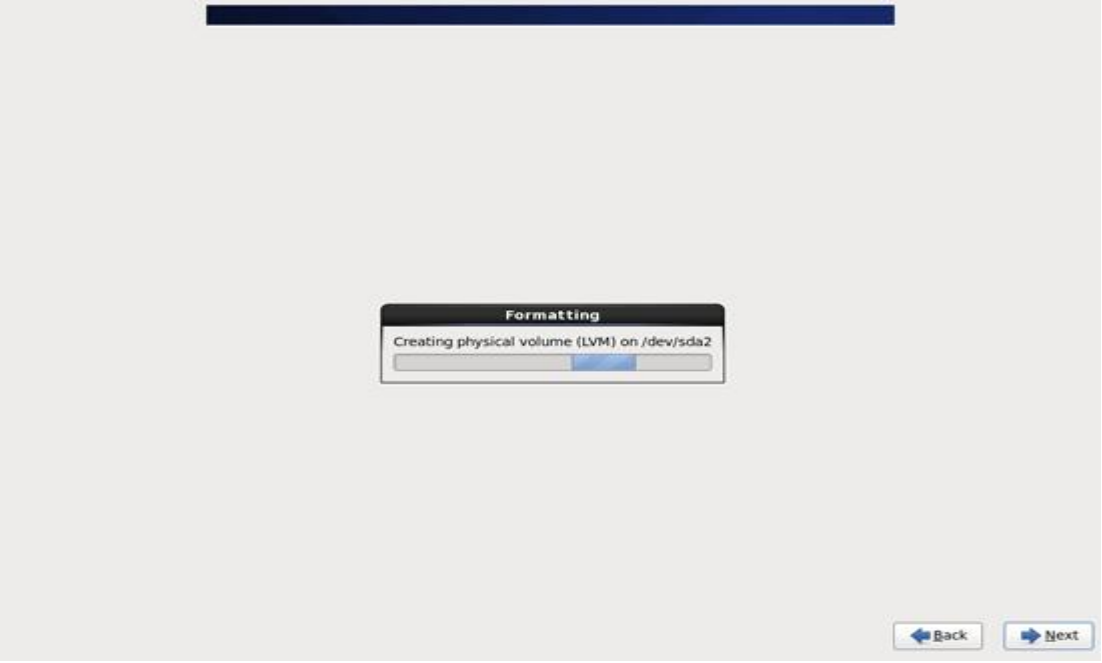
نکته مهم: سپس ویندوز را Restart کنید و وارد (قسمت اول نصب مشترک) CentOS شوید. (رجوع به صفحه ۱۲)

بعد انجام مراحل بالا و برگشت به این مرحله ، گزینه use free space را انتخاب کنید.



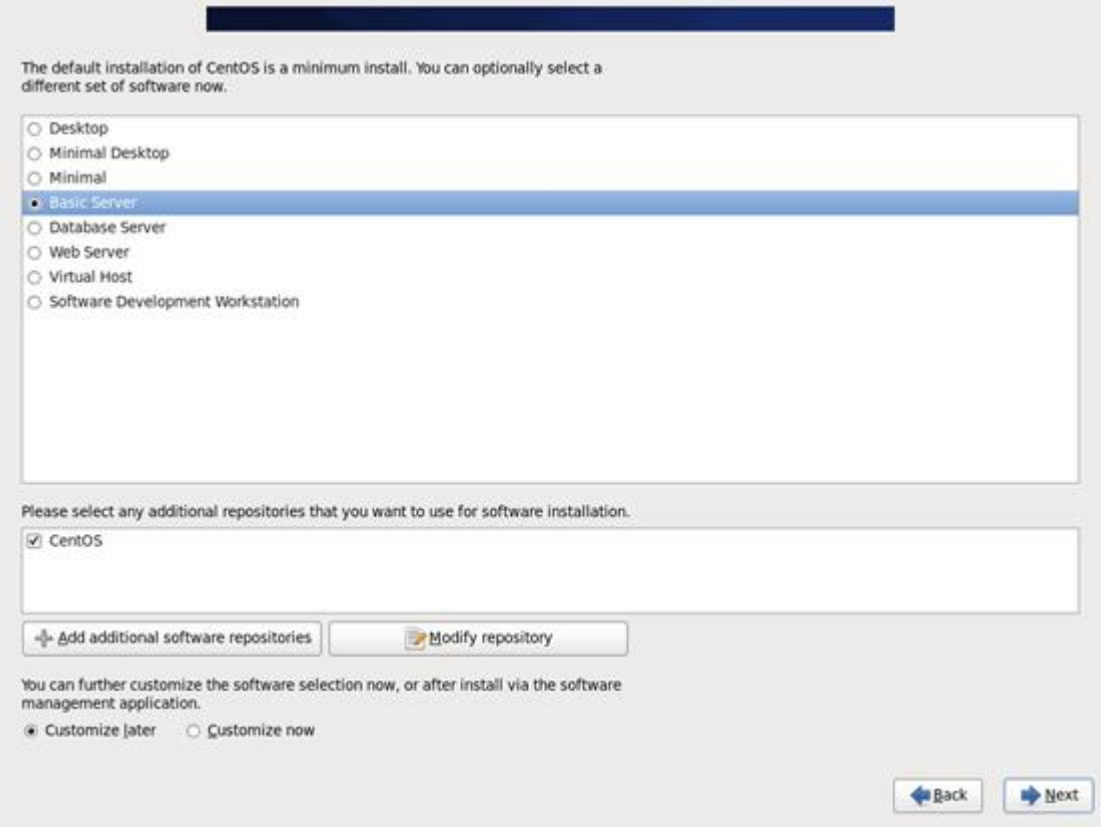
۴) در صورت مشاهده متن زیر، بر روی ... **write changes** کلیک کنید.

۵) سپس فقط بر روی گزینه **next** کلیک کنید و گزینه های دیگر را در مراحل بعد اصلا تغییر ندهید. تا به شکل مرحله ۶ برسید.

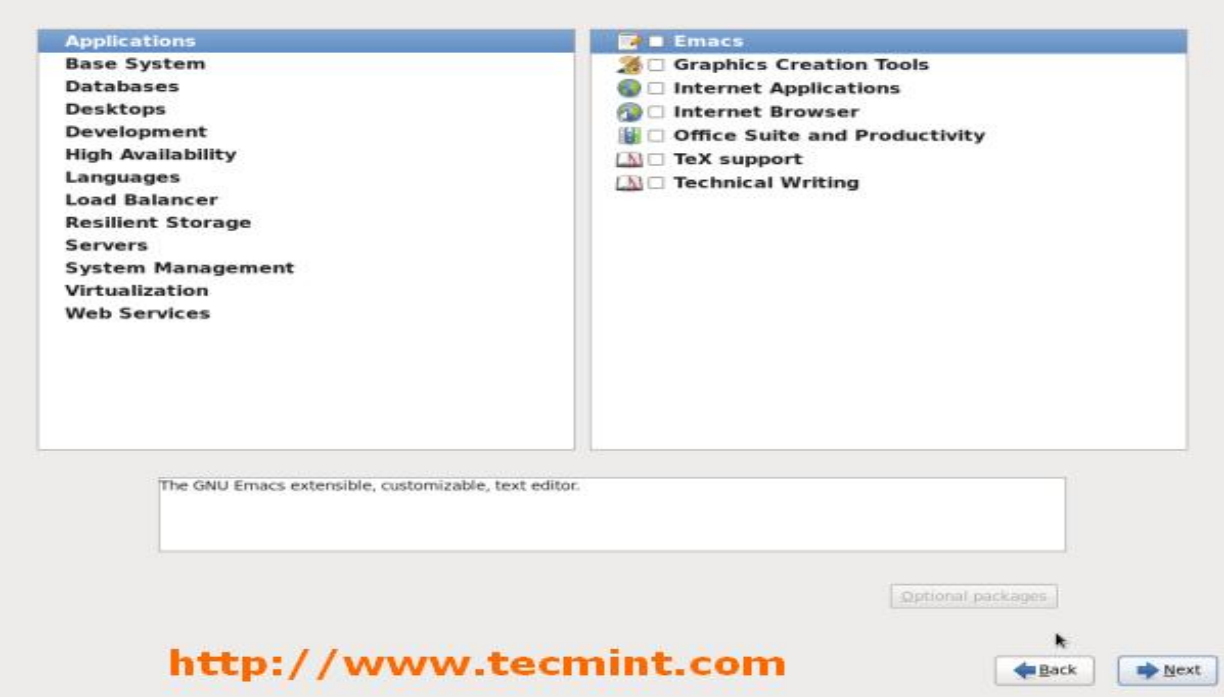


۶) در این مرحله شما باید نوع **CentOS** را انتخاب کنید. با توجه به نیازی که دارید انتخاب کنید.

هر یک از گزینه ها یک سری از بسته ها را بر روی هارد شما نصب می کند.



۷) سپس در همین مرحله (عکس بالا) می توانید بسته ها را هم به صورت دلخواه با توجه به نیازتان انتخاب کنید. برای این کار روی .... customize now در پایین کلیک کرده سپس روی next کلیک کنید که در ادامه صفحه پایینی برای شما خواهد آمد:



پیشنهاد: اگر برای اولین بار می خواهید کار با این توزیع را تجربه کنید، حتما بسته های گرافیکی **KDE Desktop** و **Gnome Desktop** را نصب نمایید.

۸) فقط بر روی گزینه **next** یا **install** کلیک کنید و گزینه های دیگر را در مراحل بعد اصلا تغییر ندهید تا کار نصب تمام شود و سپس انتخاب ... **boot-loader** اگر خواستید می توانید مسیر نصب آن را تغییر دهید.

نکات بسیار مهم:

نکته ۱: اگر یک سیستم عامل ویندوزی داشتید، واین **OS** قرار است که به عنوان **OS** دوم شما باشد.، شما باید بر روی گزینه **change device** کلیک کنید و گزینه ای که در آن اشاره به **first sector of boot...** شده را انتخاب کنید.

نکته ۲: ممکن است بعد از اتمام نصب، برای شما قسمتی که باید **os** ویندوزی را در کنار **os** لینوکسی نشان دهد نیاید (منظورم همان **Boot-Manager** یا **Grub** است). برای رفع این مشکل ۲ راه وجود دارد:

الف) نصب نرم افزار **Easy-BCD** و تنظیماتی که باید در آن ،در داخل ویندوز انجام دهید.

سایت این نرم افزار:

http://neosmart.net/EasyBCD/

ب) نصب نرم افزار **boot-repair-disk** که حتماً پیشنهاد می کنم دانلود کرده و از آن استفاده کنید.

سایت نرم افزار:

http://sourceforge.net/projects/boot-repair/

یا

http://sourceforge.net/projects/boot-repair-cd/?source=recommended

یا

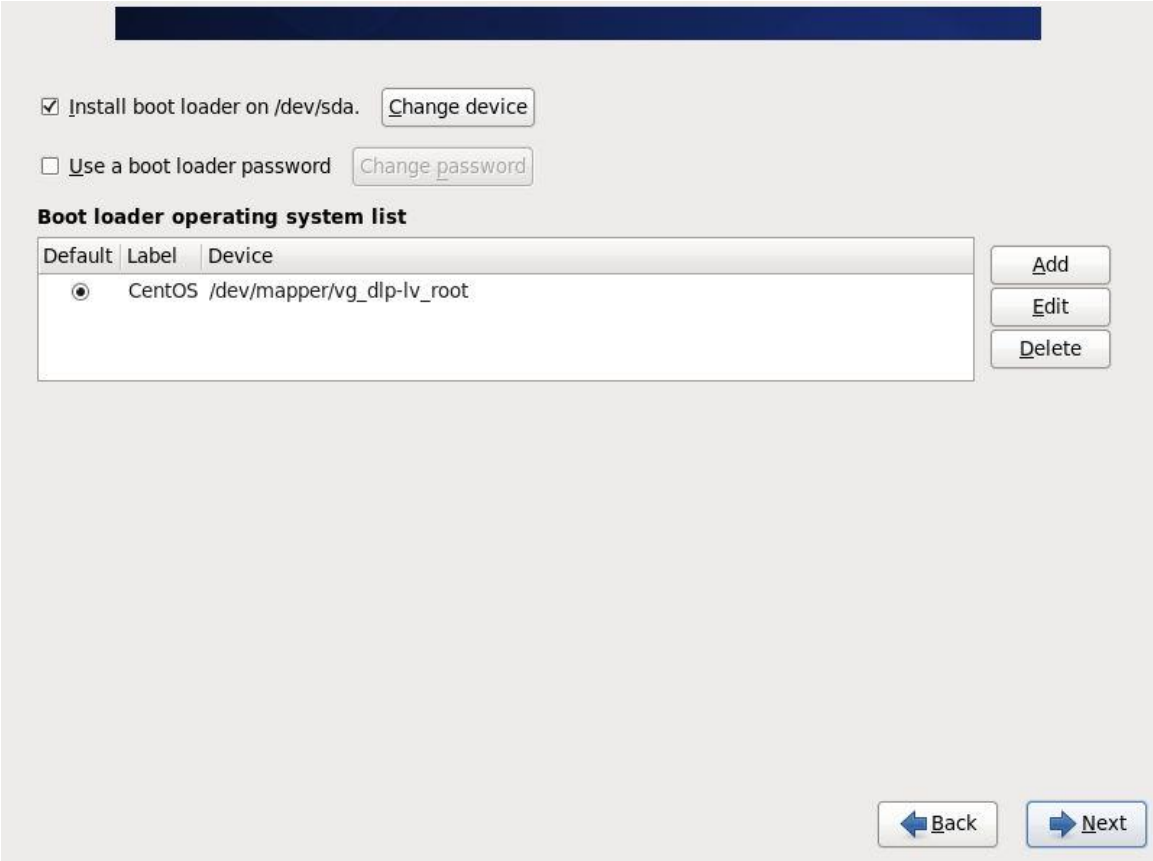
http://sourceforge.net/projects/boot-repair-cd/files/

این فایل با پسوند **ISO.** هست. شما برای نصب آن به یک فلش با ظرفیت حداقل **2GB** یا **CD** نیاز دارید.

سپس نرم افزار **Unetbootin** دانلود کرده و آن را روی **CD** یا فلش خود رایت کنید و از بوت سیستم آن را بالا بیارید.

جزئیات بیشتر در سایت زیر کامل توضیح داده شده است:

http://sourceforge.net/p/boot-repair-cd/home/Home/



۹) سپس فقط بر روی گزینه **next** یا **install** کلیک کنید و گزینه های دیگر را در مراحل بعد اصلاً تغییر ندهید تا کار نصب تمام شود.

۱۰) اگر از این روش نصب استفاده کرده اید در ادامه باید به بخش (قسمت دوم نصب مشترک) برگردید تا ادامه نصب را بعد از **Restart** سیستم عامل انجام دهید. (رجوع به صفحه ۴۲)

نصب CentOS در کنار دیگر سیستم عامل ها (روش دوم – بهترین روش) :

نکته: عددهای انتخابی برای تعیین ظرفیت، بستگی به سلیقه و میزان ظرفیت هارد شما دارد.

۱) شما باید یک فضای خالی در هارد خود ایجاد کنید. برای این کار باید نرم افزار **Ease US Partition Master-free Home Edition** نسخه رایگان آن را دانلود کنید.

برای دانلود به سایت زیر بروید:

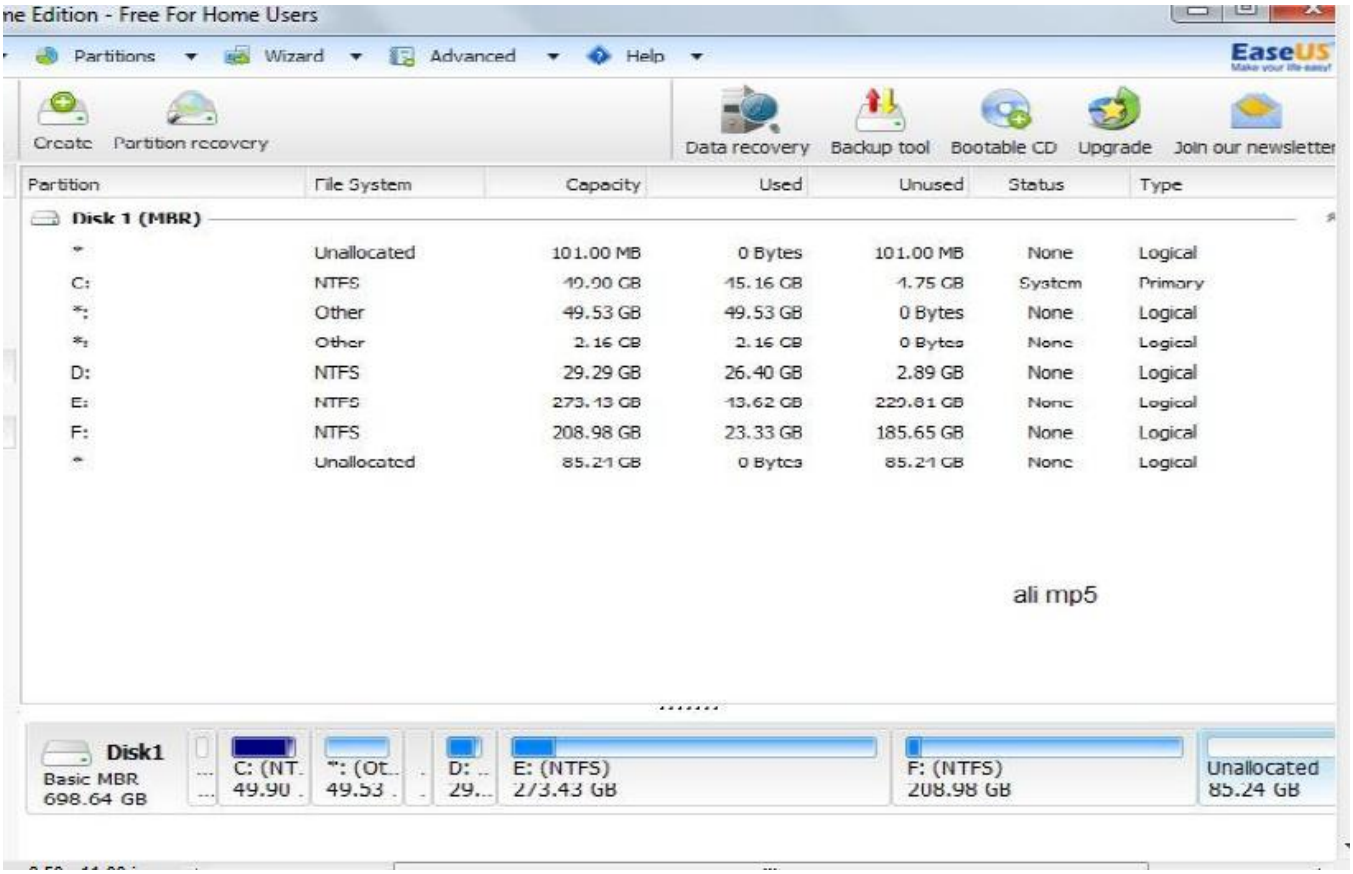
www.partition-tool.com

۲) وارد بخش **portions manager** شوید.

۳) باید فضایی به نام **Unallocated** با ظرفیت حداقل **۴۰GB** بسازید. برای این کار بر روی پارتیشن مورد نظر کلیک راست کرده و گزینه **Delete** را انتخاب کنید.

پیشنهاد: سعی کنید ظرفیت زیادی برای این OS در نظر بگیرد. هرچقدر از کارایی و امکانات آن بگویم، کم گفته ام. چون در فصل های بعدی می خواهیم سیستم عامل ویندوز را در داخل لینوکس خودمان نصب کنیم.

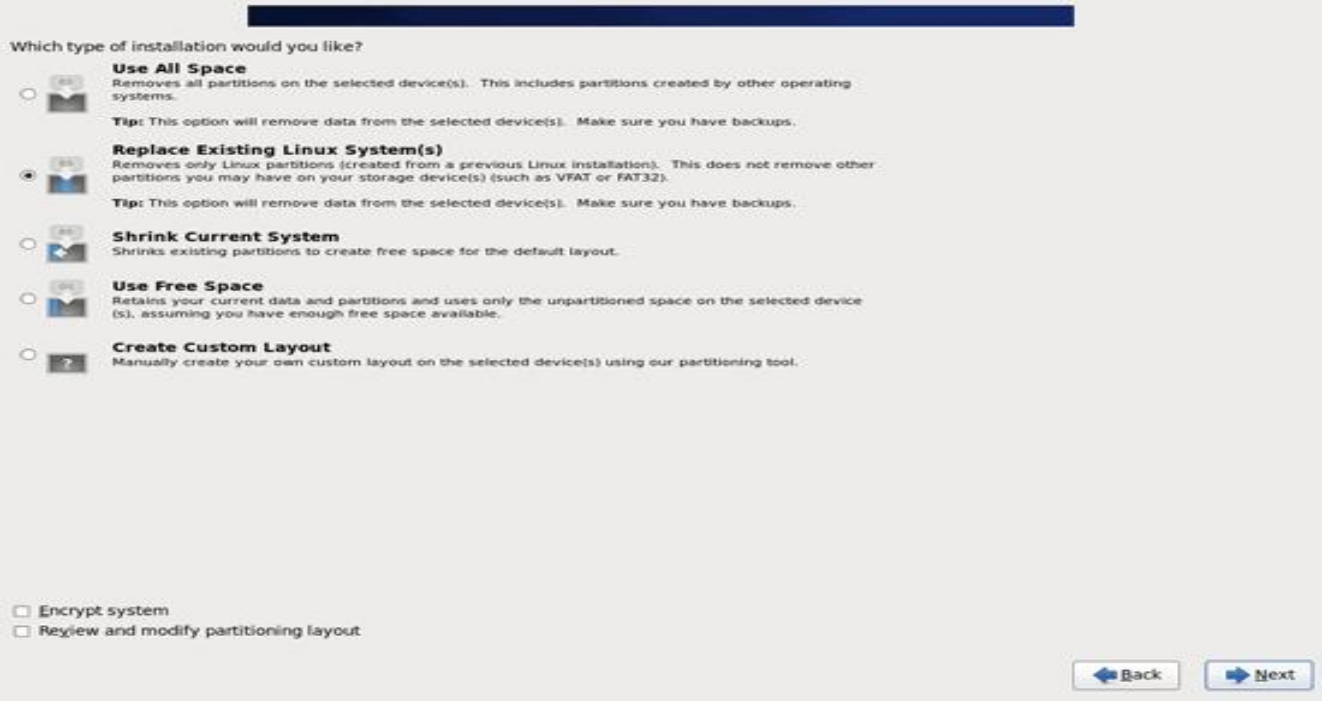
مثال: در شکل زیر فضایی با ظرفیت 85GB را ایجاد کردم.



نکته مهم: سپس ویندوز را Restart کنید و وارد (قسمت اول نصب مشترک) cent-os شوید. (رجوع به صفحه ۱۲)

سپس وقتی به عکس زیر رسیدید طبق توضیحات پایین عمل کنید.

۴) پس از رسیدن به این مرحله(عکس زیر)، شما باید گزینه **create custom layout** همراه با گزینه **review and modify...** که در پایین قرار دارد انتخاب کنید.



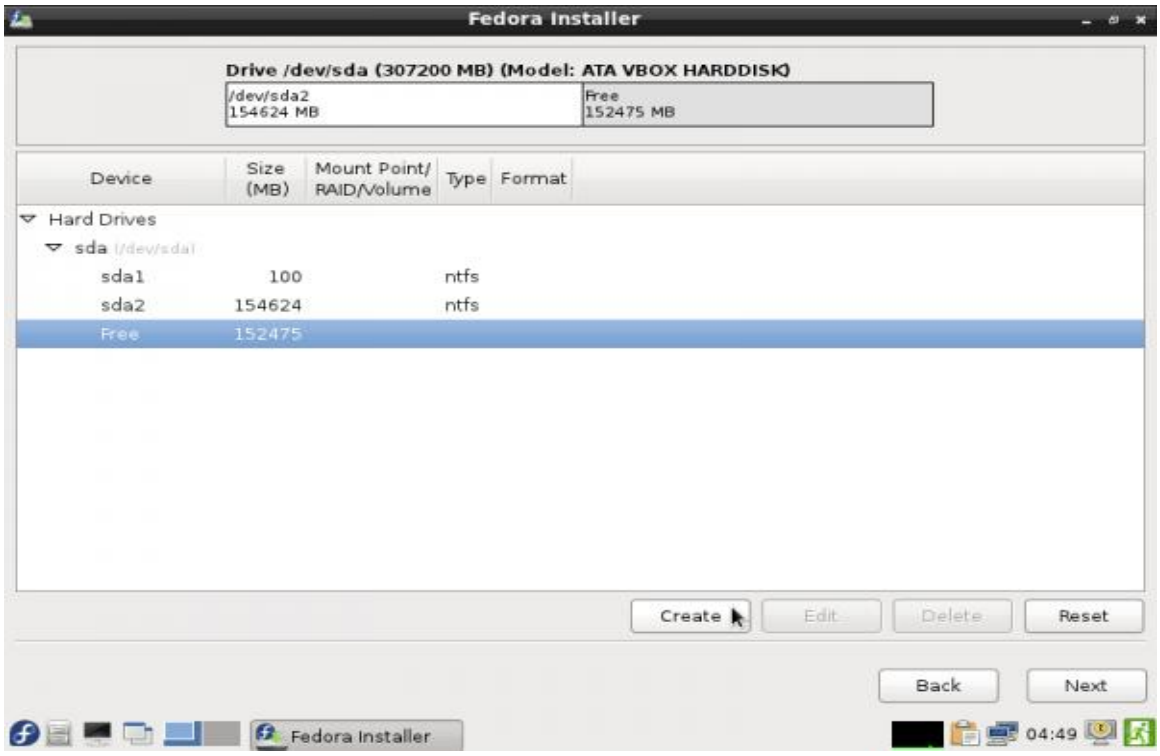
اخطار: دقت خودتان را چند برابر کنید که به دیگر پارتیشن ها آسیبی نرسانید.

۵) شما در این مرحله، به چنین محیطی وارد می شوید.

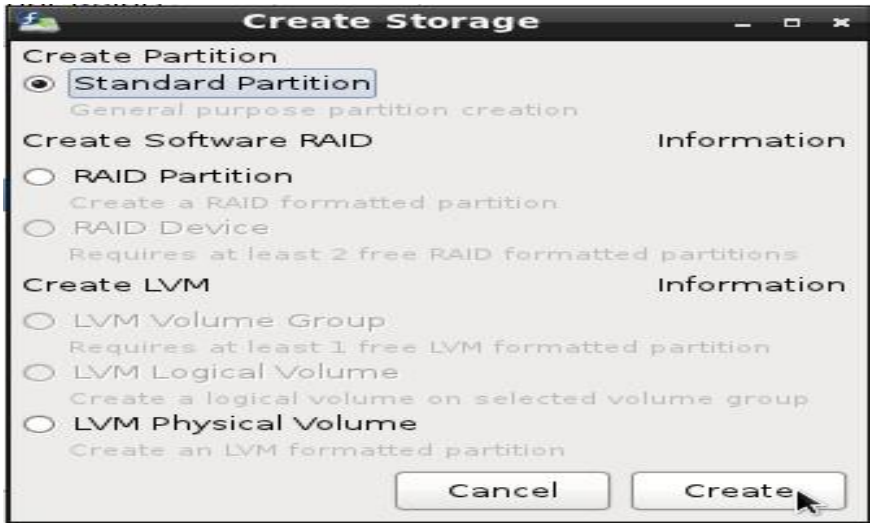
نکته ۱: در اینجا ما یک هارد دیسک بیشتر نداریم و sda فضای کل هارد ما است.

نکته ۲: sda1 و sda2 پارتیشن های ویندوز ما هستند. (یعنی ما در ویندوز ۲ پارتیشن NTFS بیشتر نداریم).

نکته ۳: فضای unallocated (free space) که در ویندوز ساختیم و اینجا آمدیم از آن استفاده کنیم 152GB است.



۶) سپس بر روی **create** (عکس بالا) کلیک کنید و یک **standard portions** بسازید و در ادامه بر روی **create** کلیک کنید.



۷) سپس ما باید یک پارتیشن برای **boot/** بسازیم.

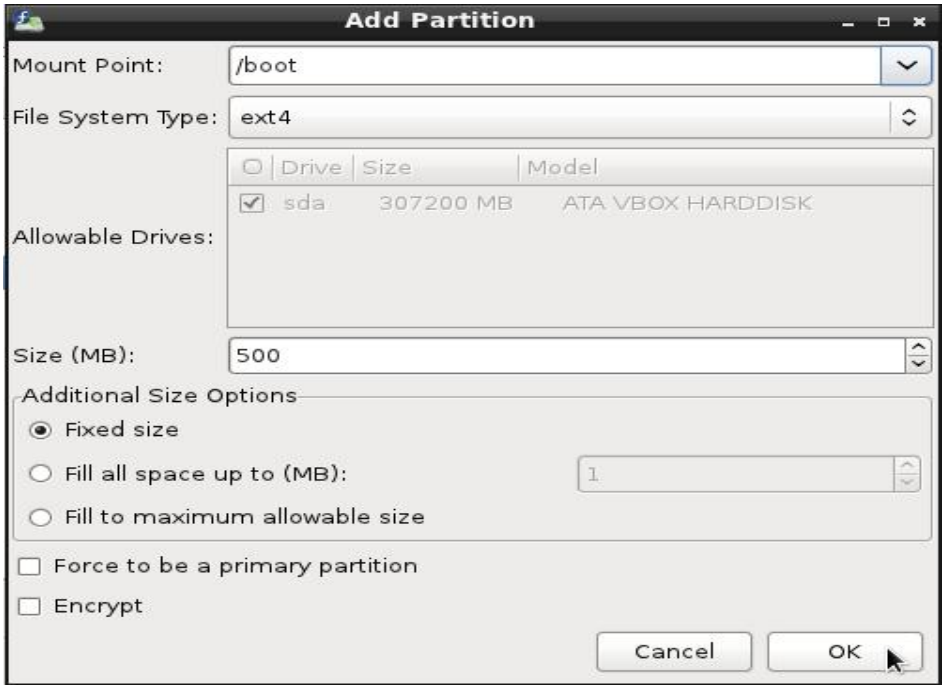
فضای لازم: 500 MB

دوباره بر روی (عکس مرحله ۵) create کلیک کنید.

mount point را روی boot/ انتخاب کنید.

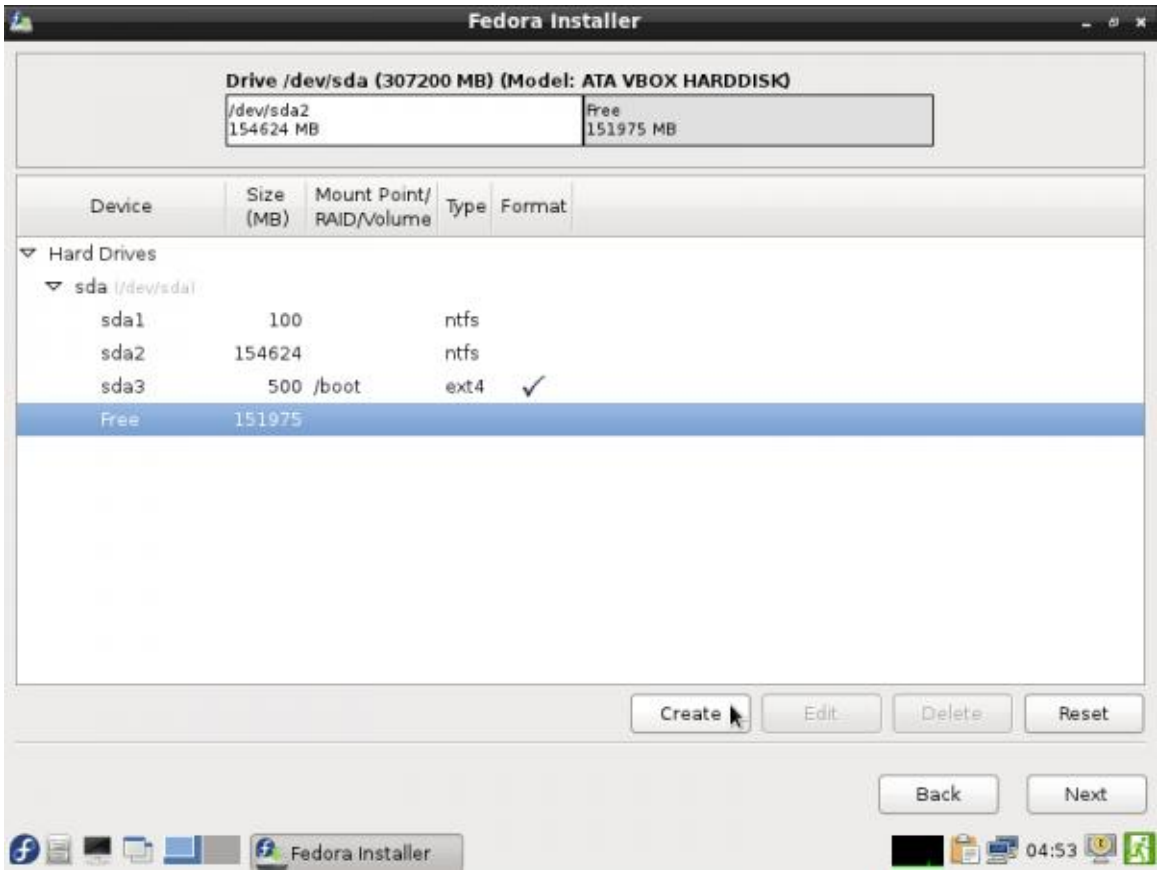
size را برابر مقدار ۵۰۰ قرار دهید.

نوع سیستم فایل را ext4 انتخاب کنید، سپس روی OK کلیک کنید.

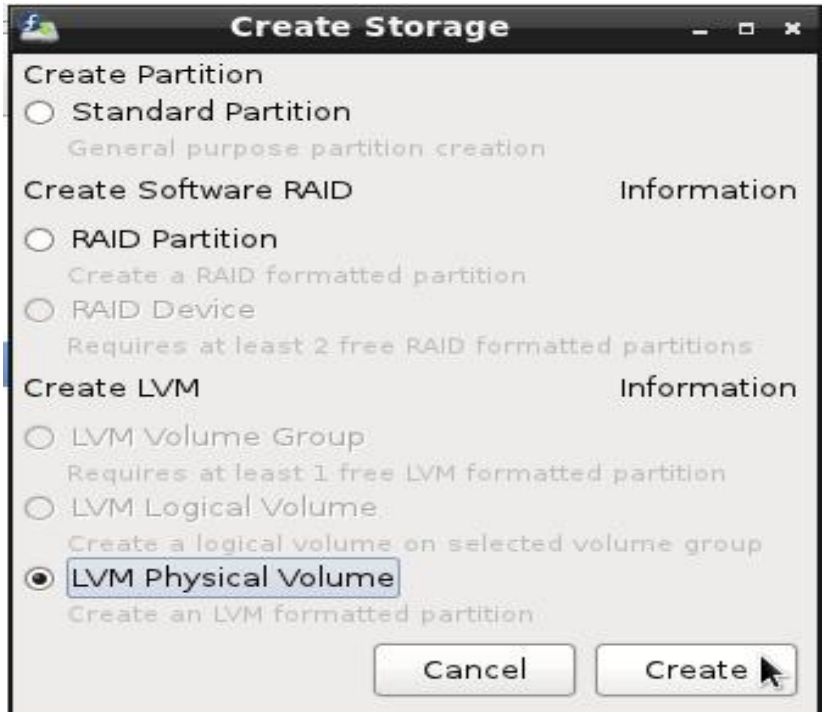


نتیجه در این عکس واضح است:

۸) روی create کلیک کنید.



۹) سپس LVM Physical Volume را انتخاب و بر روی create کلیک کنید.

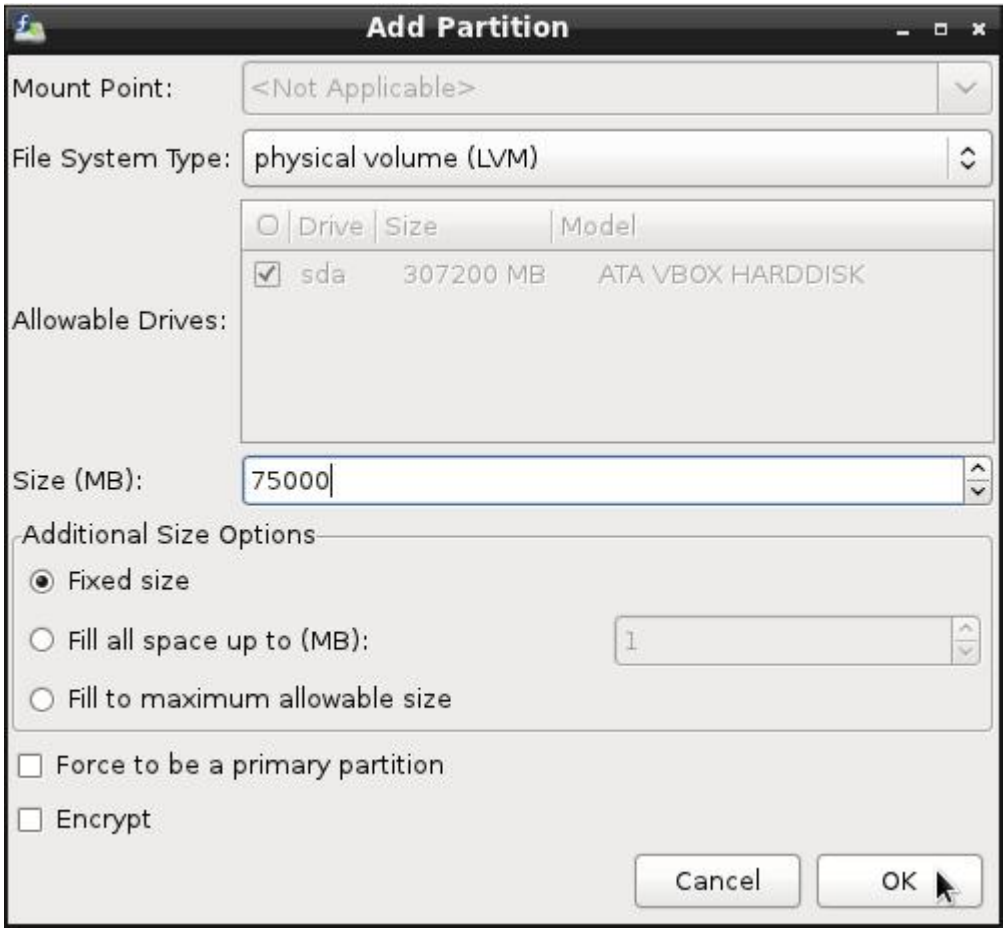


۱۰) در ادامه باید تظیماتی را برای این انجام دهیم.

در مرحله ۵ توضیح دادم که فضای خالی هارد ما 152GB است.

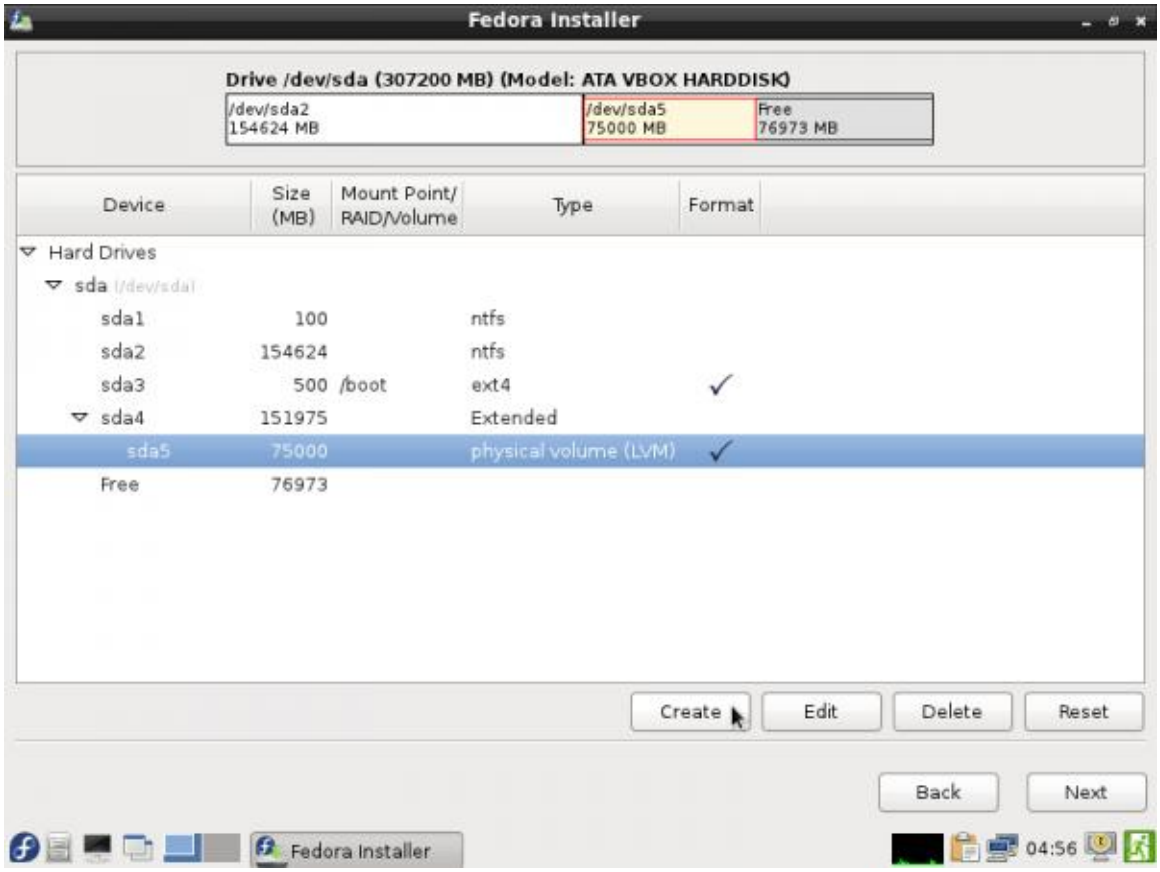
نکته: در این مثال نمی خواهیم از همه ی فضای هارد استفاده کنیم.

نکته: فقط 75GB را برای این volume در نظر گرفتیم.سپس روی ok کلیک کنید.

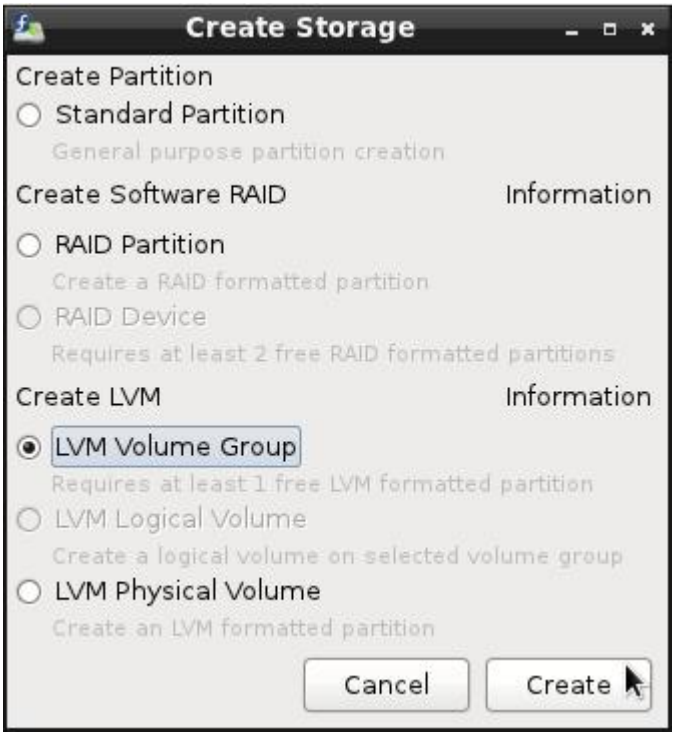


نتیجه در عکس زیر معلوم است

۱۱) مجدد بر روی create کلیک کنید.



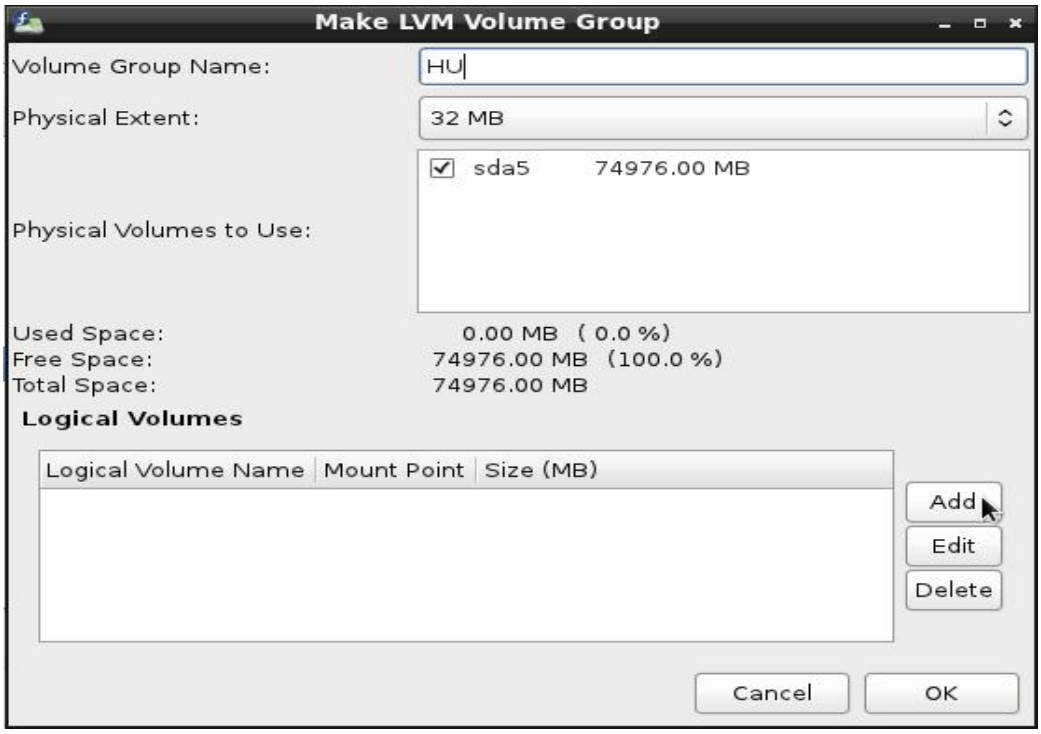
۱۲) گزینه LVM volume Group را انتخاب کنید.



۱۳) سپس شکل زیر نمایان می شود.

ابتدا نامی را بنویسید. مثل: UH

سپس روی گزینه add کلیک کنید.



۱۴) در اینجا ما باید میزان فضای لازم را برای root/ خودمان انتخاب کنیم.

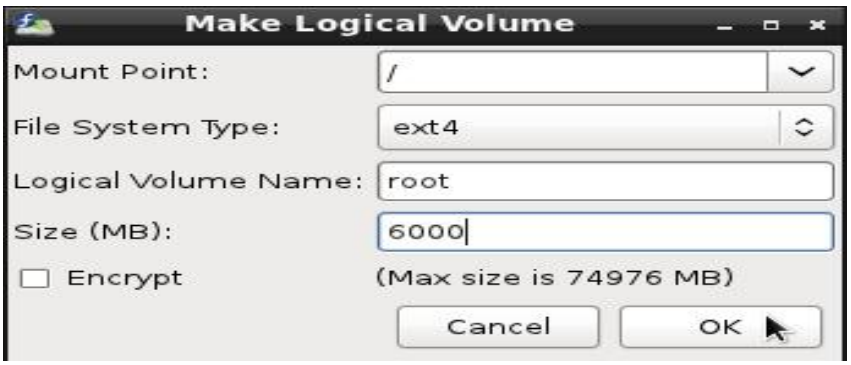
mount point: گزینه / را انتخاب کنید.

file system: ext4 باشد.

اسم آن: root

میزان فضایی که مد نظر دارید. با توجه به حجمی که در نظر گرفتید می توانید اینجا بنویسید. مثل: 6GB این حجم کم است، شما بنویسید 30GB .

پیشنهاد: اگر فضای بیشتری دارید، عدد root را بالا در نظر بگیرید.سپس روی ok کلیک کنید.



روی add مجدد کلیک کنید.

۱۵) در اینجا ما باید میزان فضای لازم برای swap خودمان را انتخاب کنیم.

طبق شکل زیر:

شما برای قسمت size، متناسب با RAM که دارید وارد کنید.

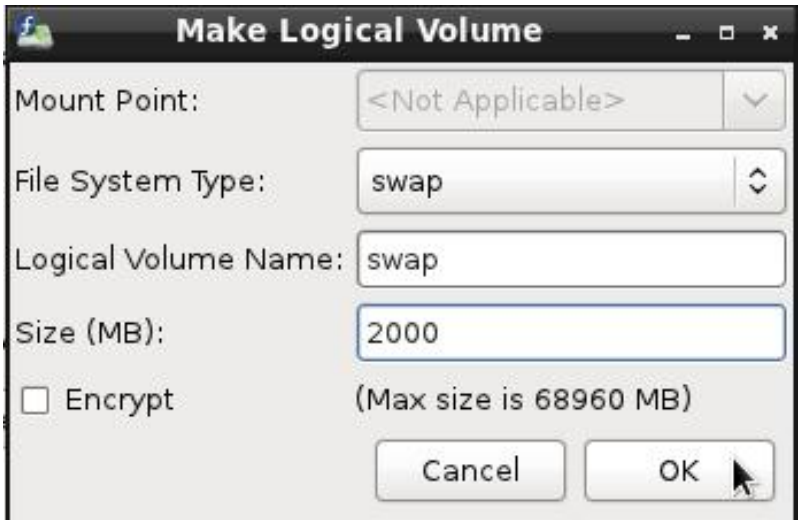
مثلا:

اگر RAM شما 2GB است، عدد ۲۰۰۰ را وارد کنید.

اگر RAM شما 4GB است، عدد ۴۰۰۰ را وارد کنید.

اگر RAM شما 8GB است، عدد 6000 را وارد کنید.

سپس روی ok کلیک کنید.

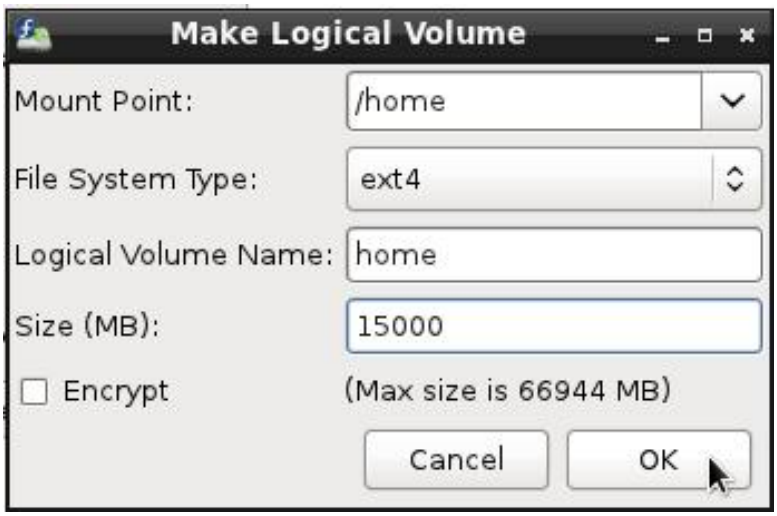


روی add مجدد کلیک کنید.

۱۶) در اینجا ما باید میزان فضای لازم برای Home خودمان را انتخاب کنیم.

میزان فضای لازم را با توجه به فضایی که مد نظر دارید وارد کنید.

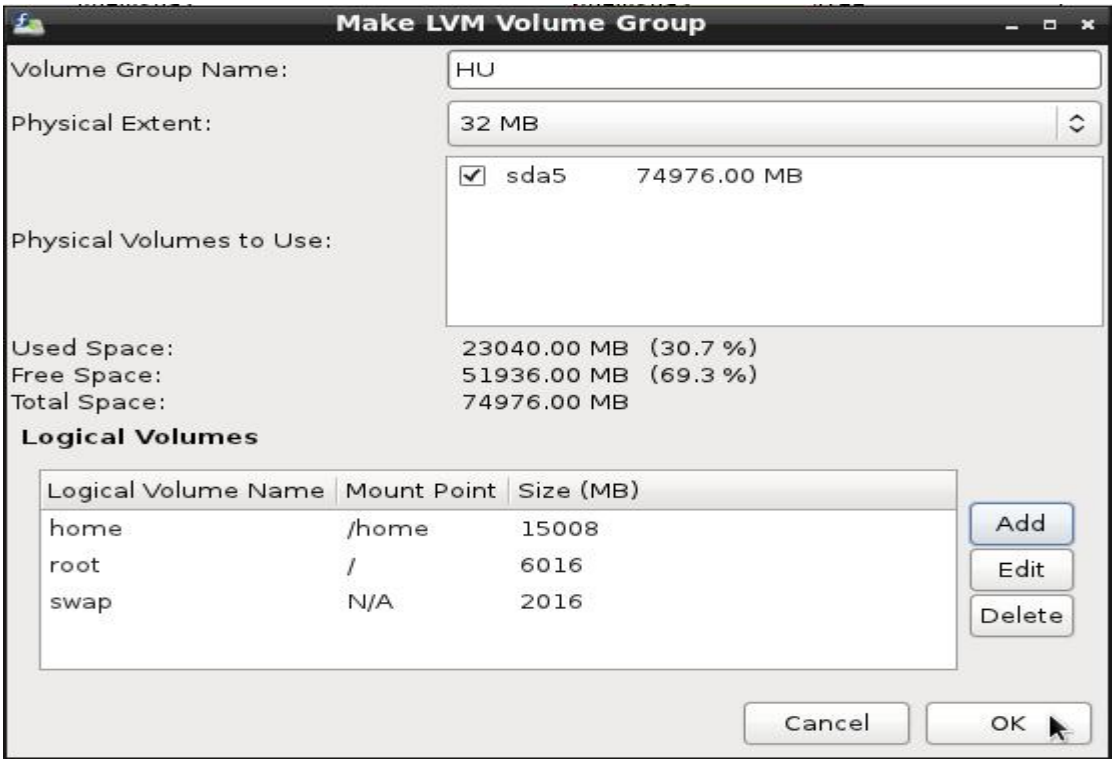
در اینجا 15GB کم است، اگر فضای زیادی داشتید عدد ۳۰۰۰۰ یا به بالاتر را وارد کنید.



نتیجه کارهای بالا در عکس زیر:

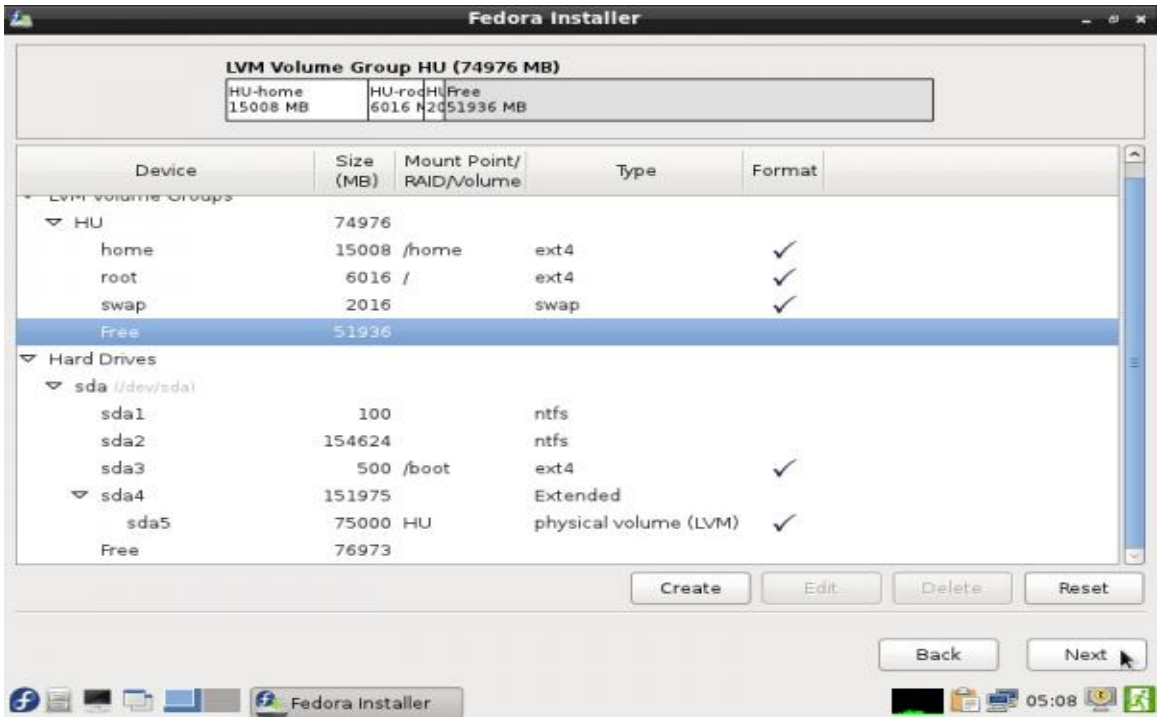
۱۷) طبق مثال و اعدادی که در خود عکس ها بوده، فضای اشغال شده از 75GB، فقط 23GB بوده است.

در نهایت روی ok کلیک کنید.



نتیجه تمام کارهایی را که تا به اینجا انجام داده ایم:

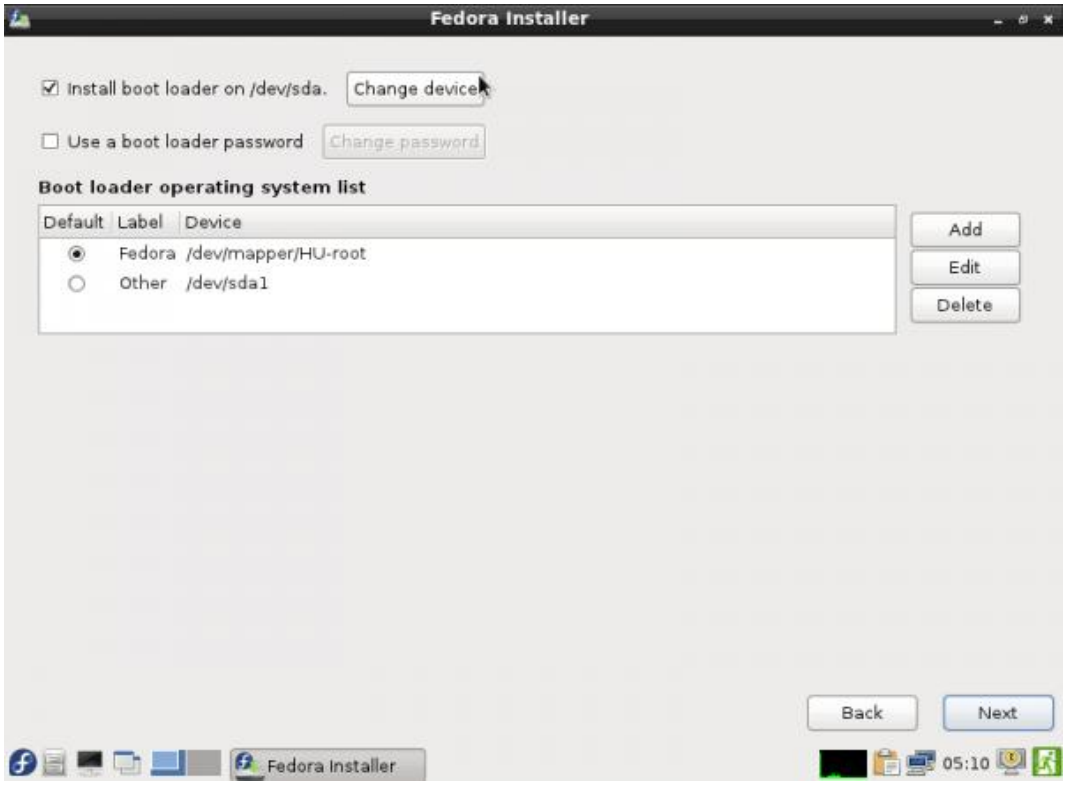
۱۸) سپس بر روی next کلیک کنید.



۱۹) در اینجا وارد بخش boot loader شده ایم.

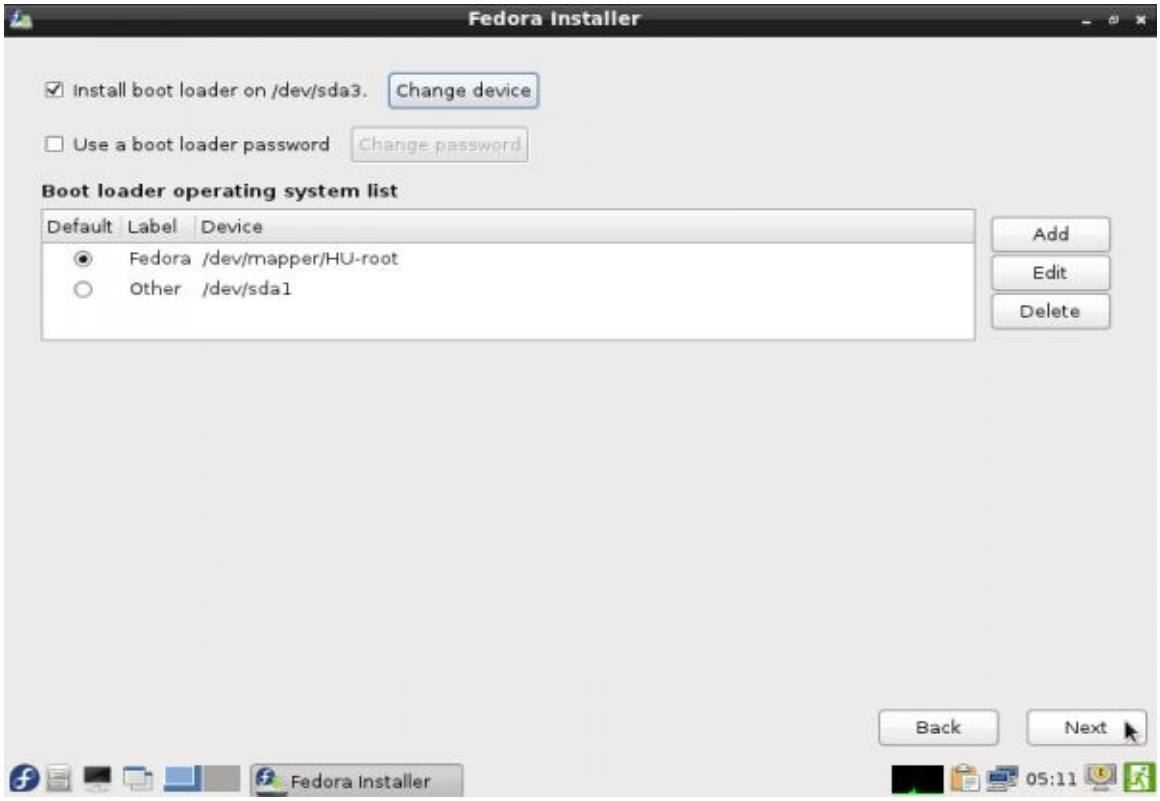
نکته: در یک قسمت می بینید نوشته: other /dev/sda1 که تیک هم نخورده،این همان بوت لودر درایور ویندوزی ما است.

شما روی گزینه change device کلیک کنید.



۲۰) گزینه **first sector of...** را انتخاب کنید و روی **ok** کلیک کنید.

تغییرات ایجاد شده:



۲۱) روی **next** کلیک کنید. و صبر کنید تا نصب **OS** تمام شود.

۲۲) اگر از این روش نصب استفاده کرده اید در ادامه باید به بخش (قسمت ۲ نصب مشترک) برگردید تا ادامه نصب را بعد از **Restart** شدن سیستم عامل انجام دهید. (رجوع به صفحه...)

نکات بسیار مهم:

اگر با مشکلی مواجه شدید با یکی از۲ نکته گفته شده در پایین، کارهای لازم را انجام دهید.

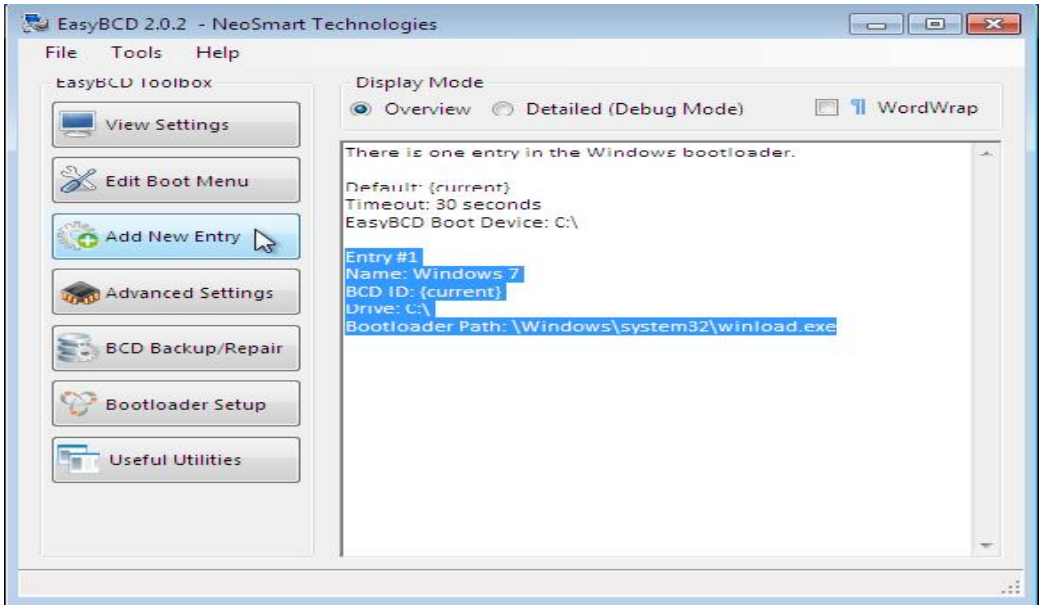
نکته ۱: در صورتی که سیستم را ریست کردید و سیستم عامل ویندوزی شما در لیست بوت-گراب نبود می توانید از نرم افزار boot-repair-disc استفاده کنید.لینک آموزش و دانلود نرم افزار:

http://sourceforge.net/p/boot-repair-cd/home/Home/

نکته ۲: اگر بود، بعد از کامل کردن نصب سیستم عامل تا آخر(بعد از به اتمام رساندن تمام مراحل قسمت نصب مشترک) وارد محیط ویندوز شوید و برنامه Easy-BCD را اجرا کنید.

کار با برنامه Easy-BCD:

۱. گزینه **add new entity** را انتخاب کنید.



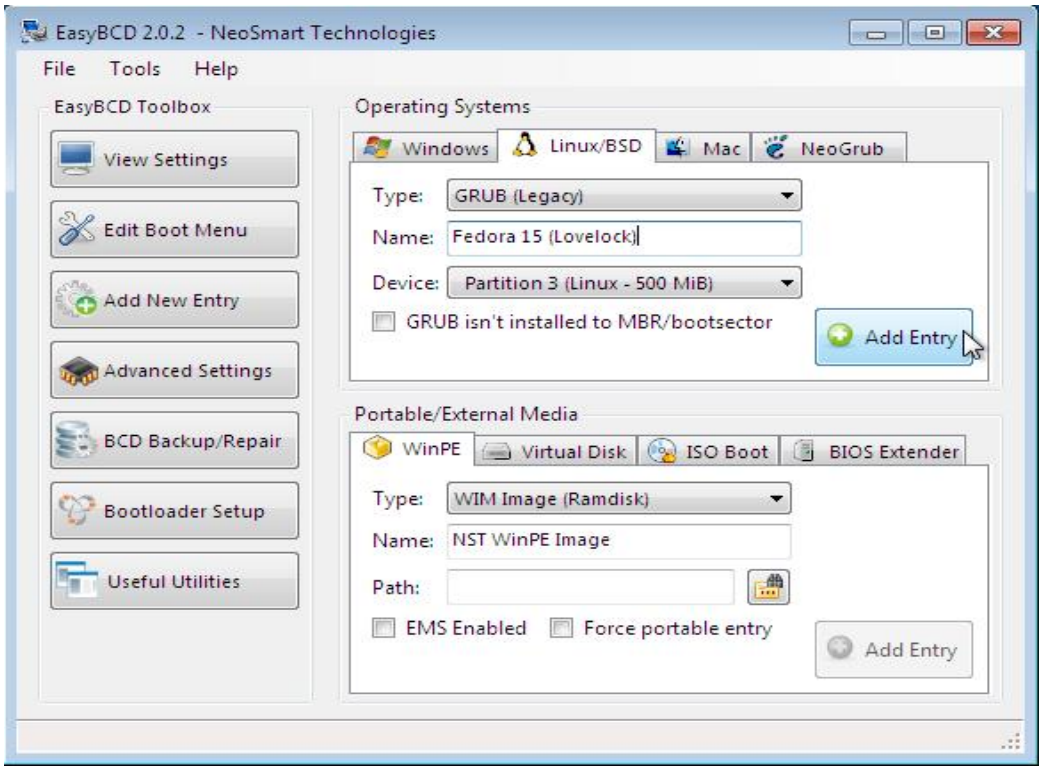
شکل زیر می آید:

۲. **به برگه (tab) لینوکس (linux.bsd) بروید.**

سپس grub legacy را انتخاب کنید و اسم Cent-os را برای آن وارد کنید.

درقسمت Device، پارتیشنی که حجم آن را 500MB در نظر گرفته بودیم انتخاب می کنیم.

سپس روی add entity کلیک کنید.

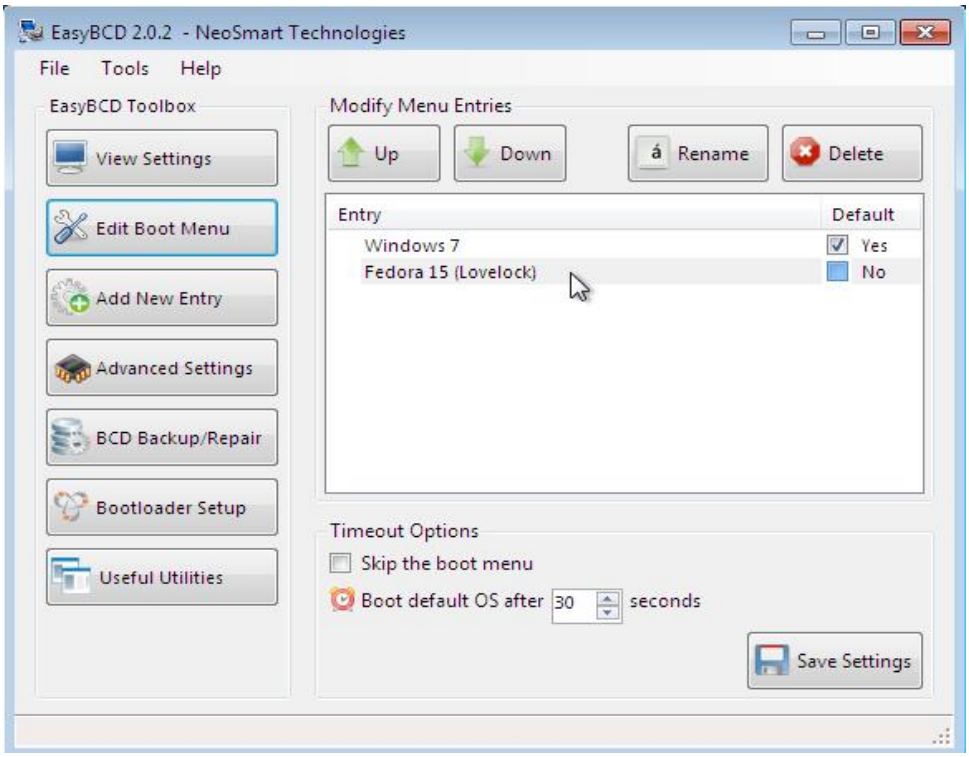


۳. به قسمت edit boot menu بروید.

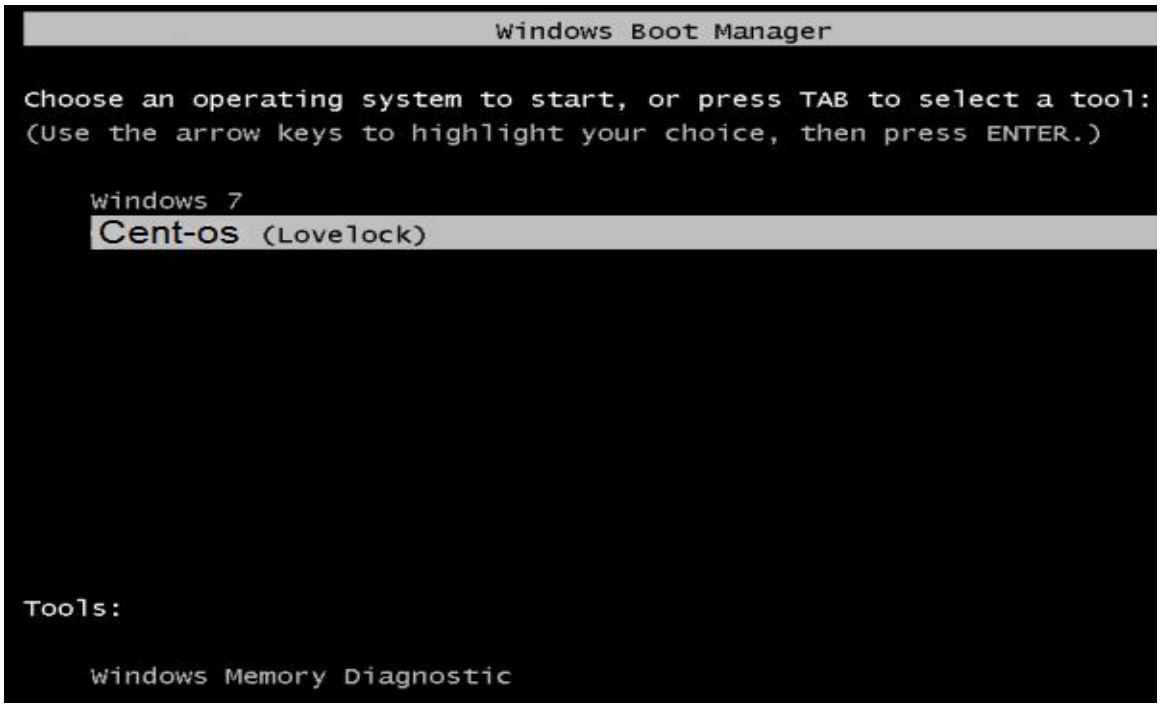
تغییراتی را که می خواهید انجام دهید. به صورت پیش فرض دست نزنید بهتر است.

در نهایت روی save setting کلیک کنید.

سیستم را Restart کنید.



نتیجه کار نهایی :



نصب CentOS (قسمت دوم مشترک نصب) :

این قسمت مربوط به مرحله بعد از Restart شدن سیستم عامل است. برای بالا آمدن سیستم عامل باید کمی صبر کنید، در ادامه با صفحه زیر رو به رو خواهید شد:

بر روی next / forward کلیک کنید تا به مرحله تعریف حساب های کاربری برسید:

در اینجا (عکس بالا) شما می توانید حساب های کاربری تعریف کنید.

نکته: اگر می خواهید تنها حساب کاربری شما همان root باشد، بر روی forward کلیک کنید تا کار شما به پایان برسد.

هم اکنون کار نصب به پایان رسیده است.

نصب Backtrack 5-R3 (Ubuntu) در کنار سیستم عامل (Windows & CentOS) :

نکات بسیار مهم:

نکته۱: فرض بر این است که، اولین سیستم عامل که شما نصب کرده اید ویندوز بوده است.

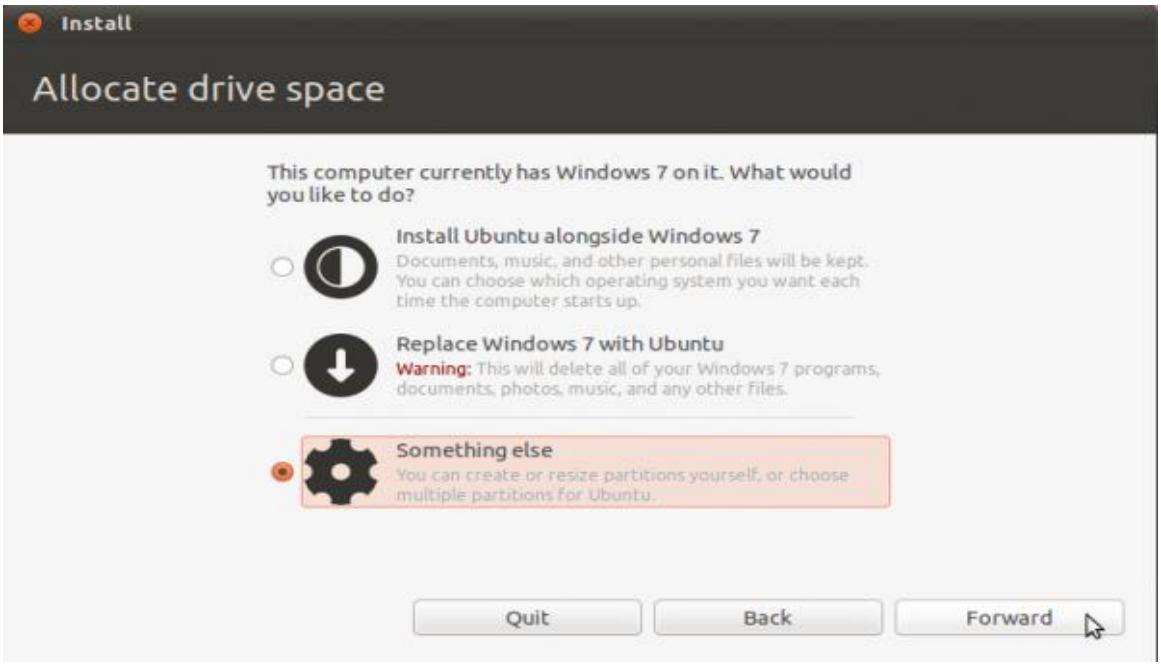
نکته۲: در ادامه شما پس از نصب ویندوز، اقدام به نصب cent-os کرده اید و آن را هم نصب کردید.

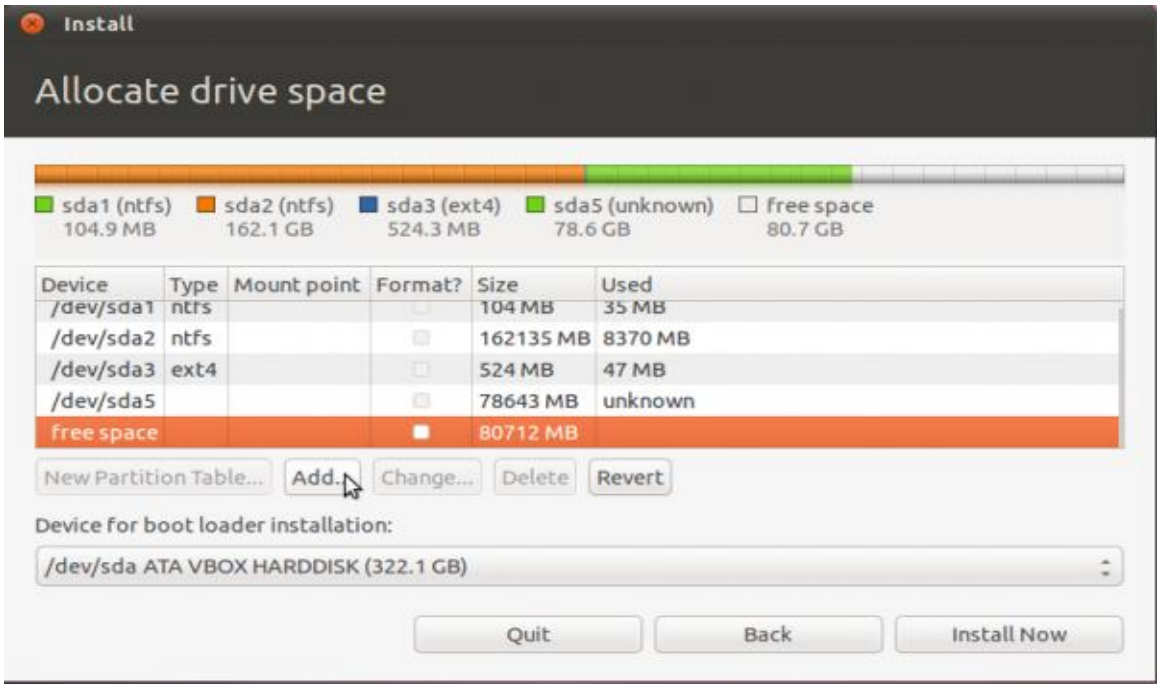
نکته۳: در آخر هم خواسته اید یکی دیگر ار نسخه های لینوکس مثل اوبونتو یا بکترک را نصب نمایید.

این روش را به این کتاب اضافه کردم تا دوستانی که می خواهند به صورت حرفه ای با چند توزیع لینوکسی کار کنند مشکلی نداشته باشند. و این قسمت نمونه ای از نصب چند توزیع لینوکسی به صورت همزمان باشد.

۱) نصب توزیع مورد نظر خود را انجام دهید تا به مرحله پارتیشن بندی برسید.

نمونه ای از مرحله پارتیشن بندی بر روی Ubuntu:





۲) در اینجا ما باید کارهایی را شبیه به نصب cent-os دهیم.

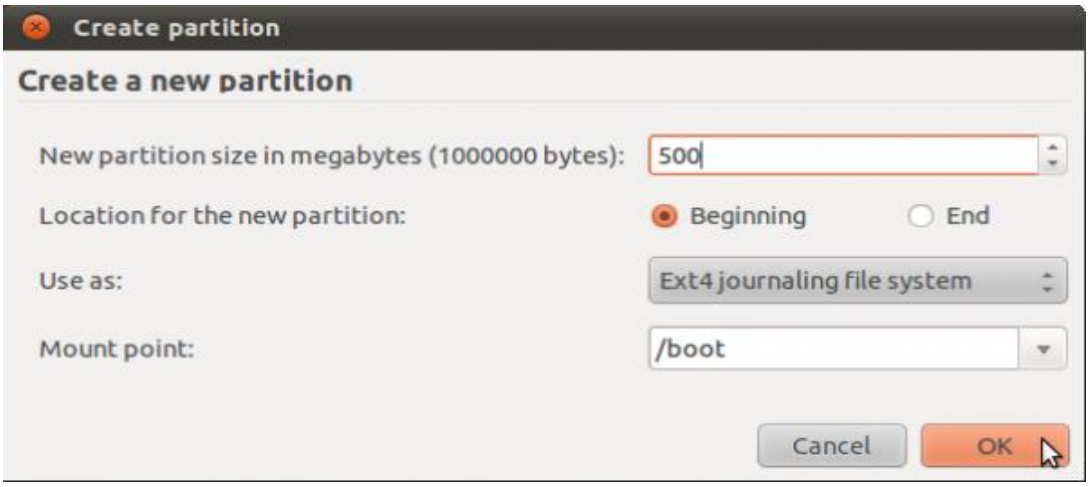
روی add کلیک کنید و یک پارتیشن برای boot بسازید، مثل شکل زیر:

مقدار: 500MB

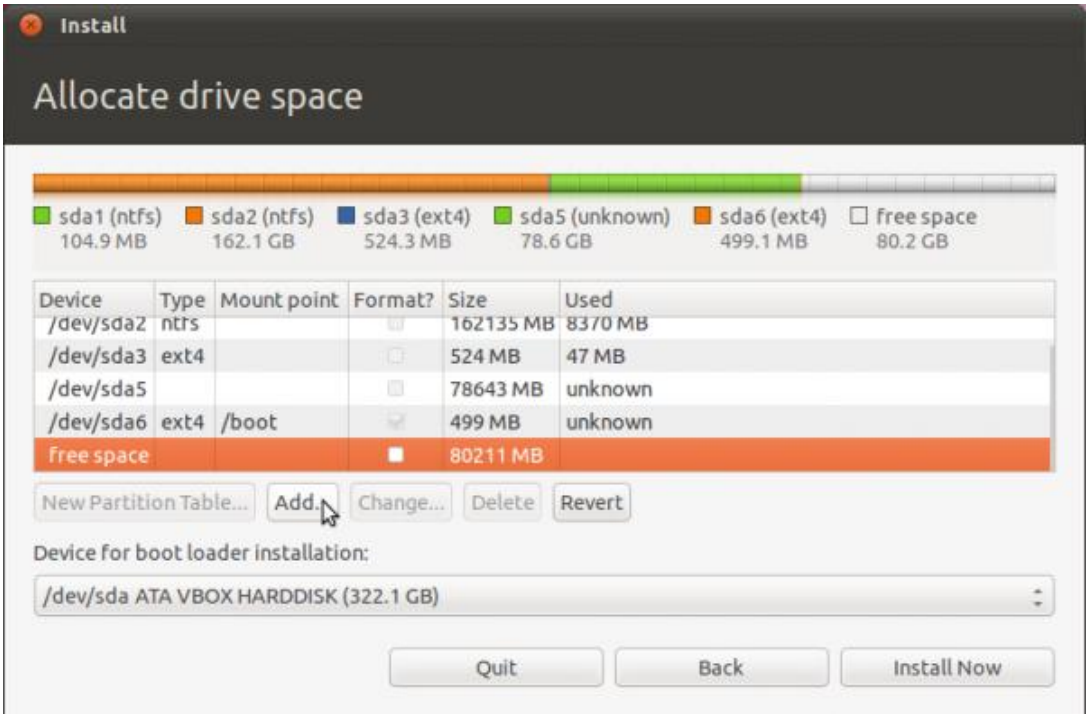
مکان: begin...

سیستم فایل: EXT4

و آخرین: /boot



نتیجه، پس از ساختن پارتیشن boot:



۳) سپس روی add کلیک کنید و یک پارتیشن swap بسازید.

مقدار: بستگی به RAM شما دارد.

RAM 2GB = 2000 MB

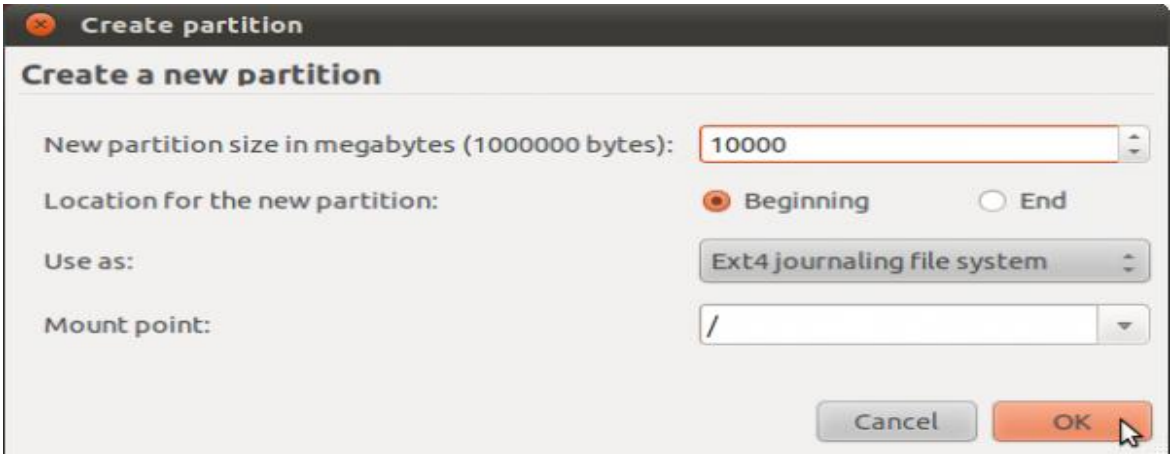
RAM 4GB= بیشتر از 3000MB

RAM 8GB= بیشتر از 5000MB

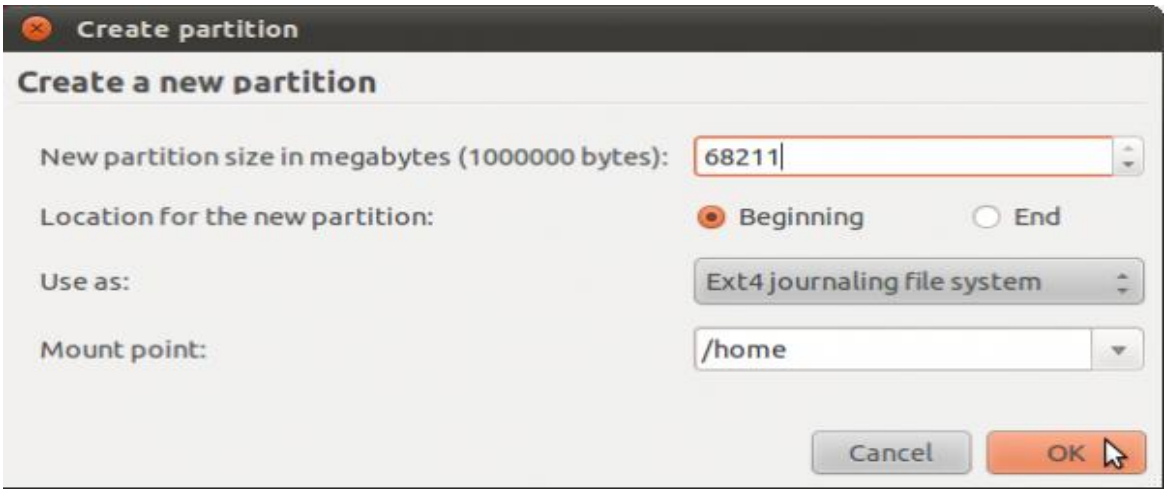
۴) در نهایت باید برای root خودمان، میزان فضایی را که لازم داریم اختصاص دهیم.

حداقل: 14000MB خوب است.

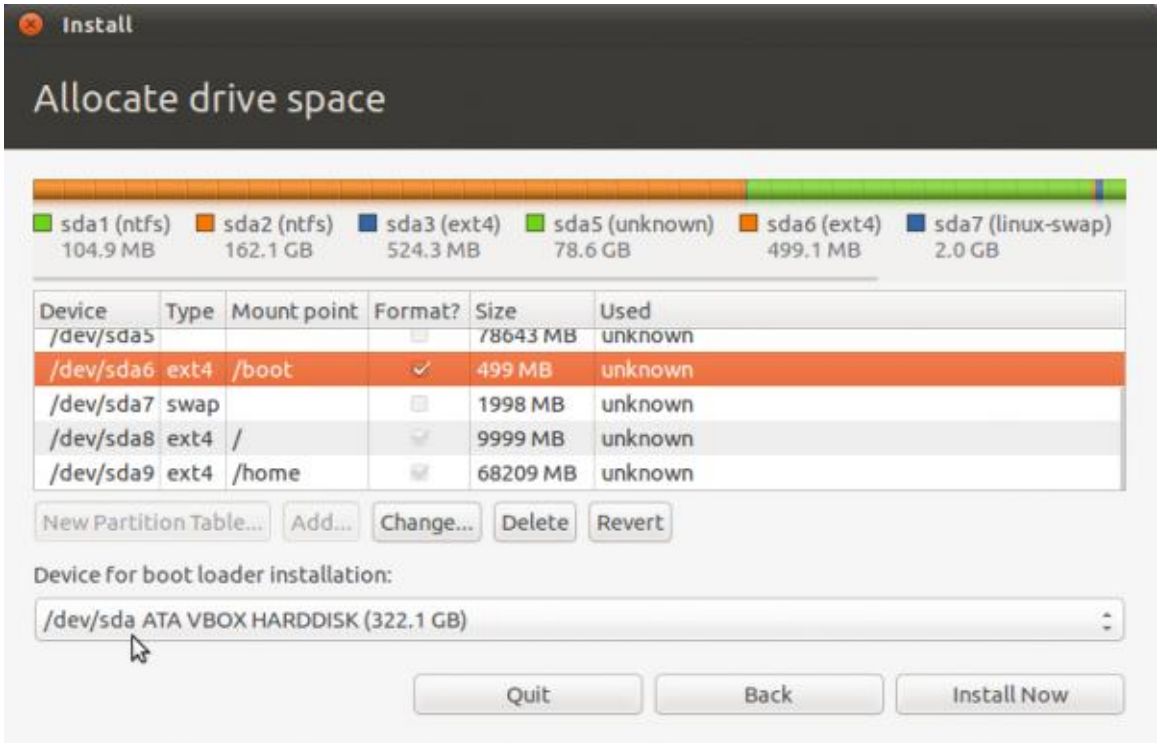
علامت اِسلَش(/)، به معنای root می باشد.



۵) سپس برای پارتیشن home هم، فضایی را که لازم دارید مقدار دهی کنید.



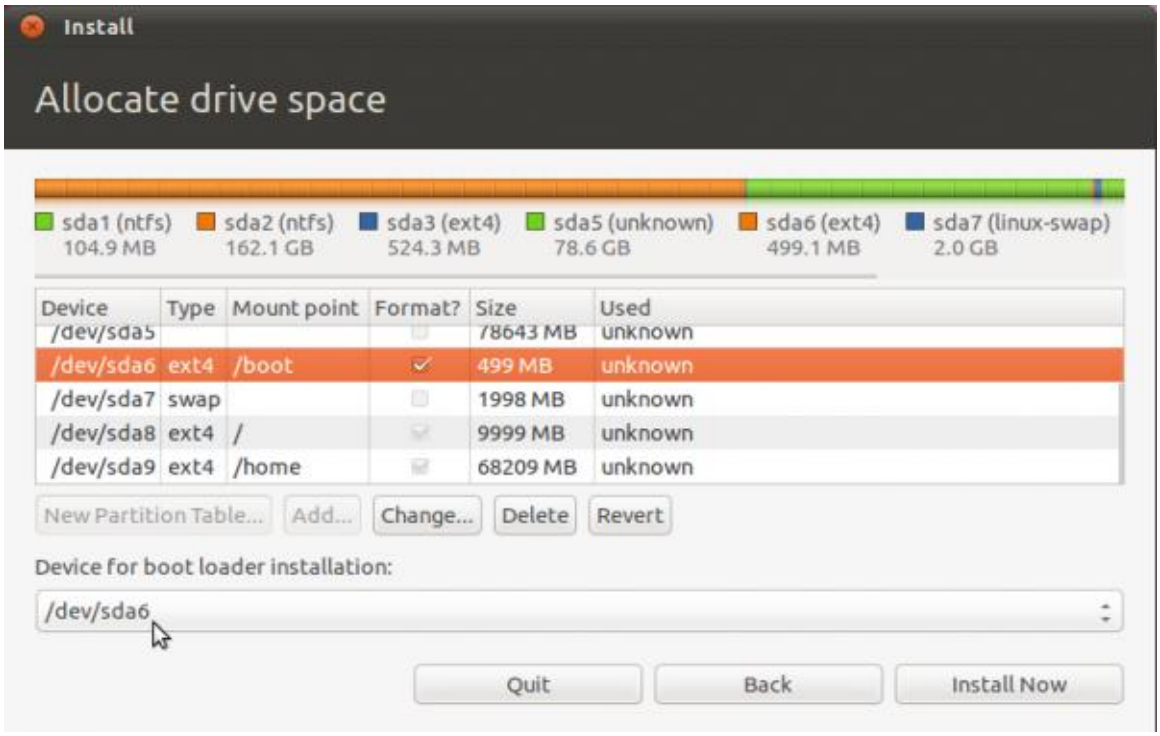
نتیجه کار پس از اعمال تغییرات لازم و ساخت پارتیشن های لازم:



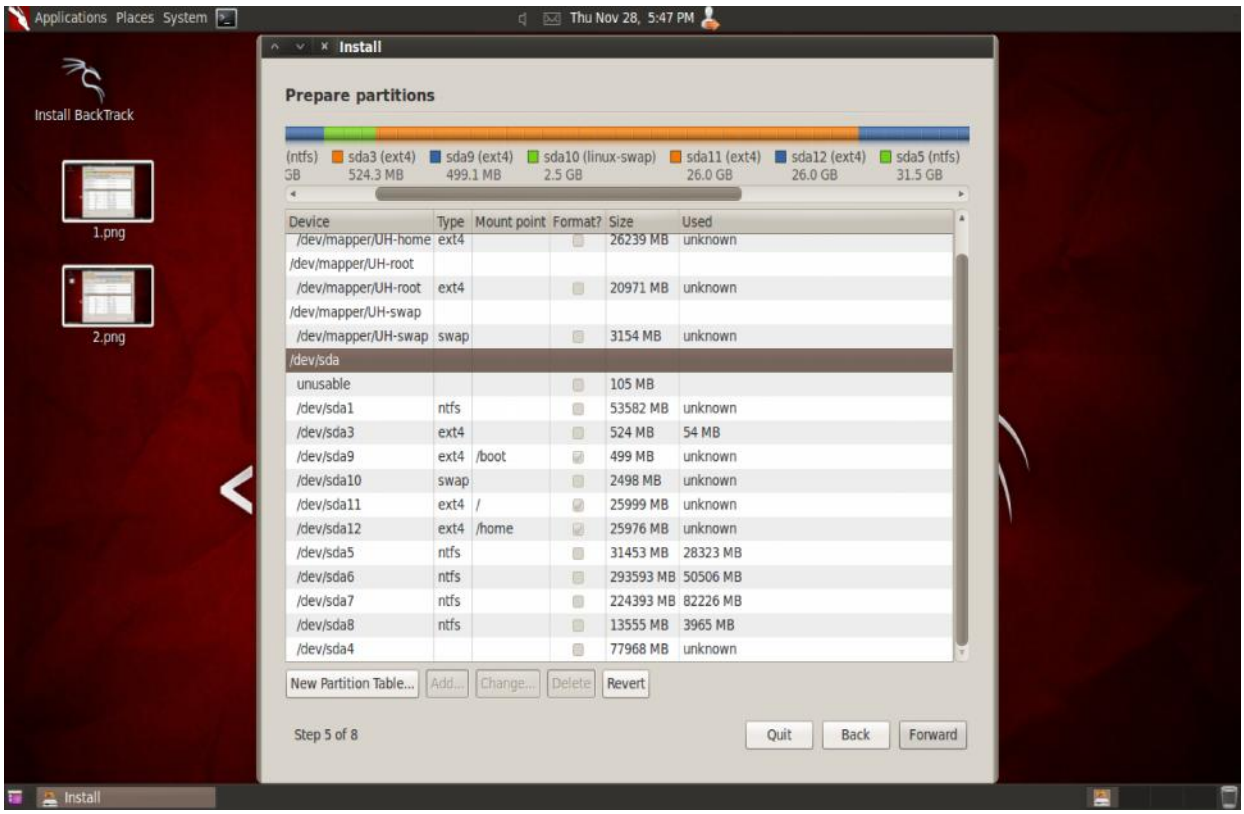
۶) این قسمت بسیار مهم است، در اینجا باید Boot Loader خودمان را انتخاب کنیم.

در عکس بالا می بینید که پارتیشن Boot ما در dev/sda6 قرار دارد، پس ما آمدیم و آن را انتخاب کردیم.

نتیجه پس از انتخاب در(ubuntu):

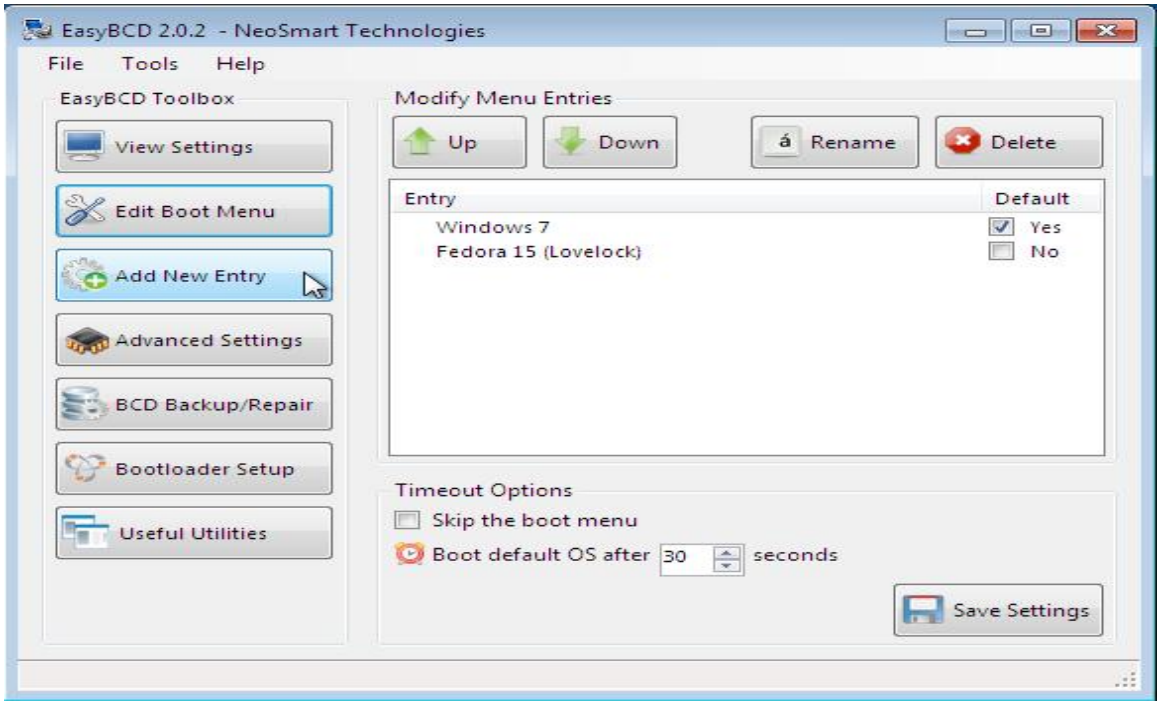


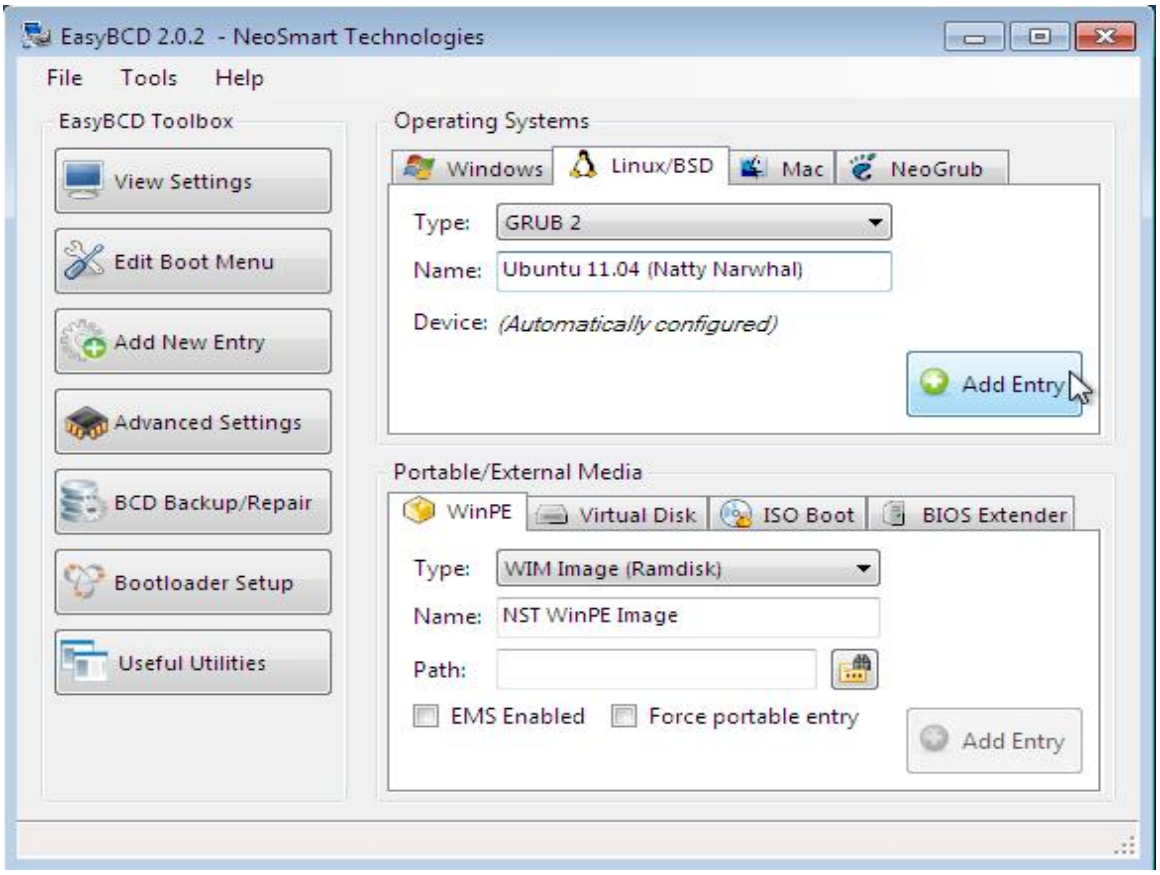
نتیجه پس از پارتیشن بندی در(BackTrack):

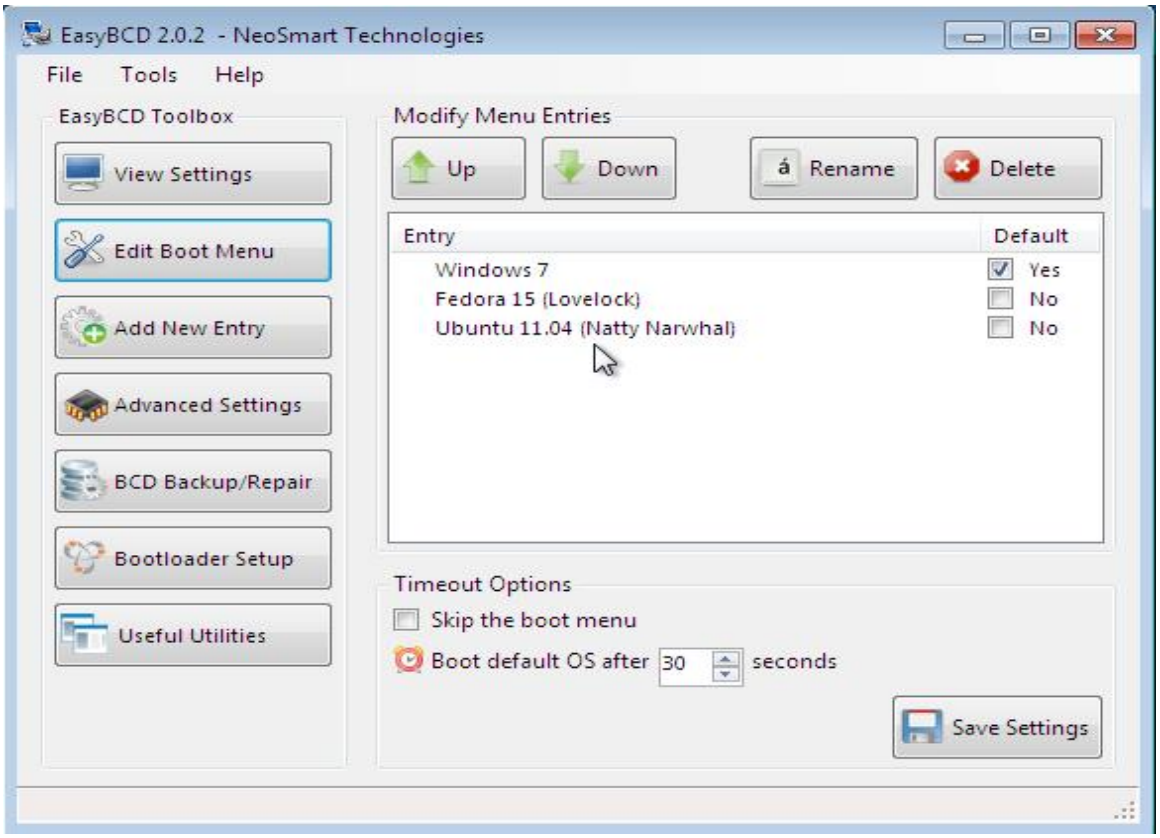


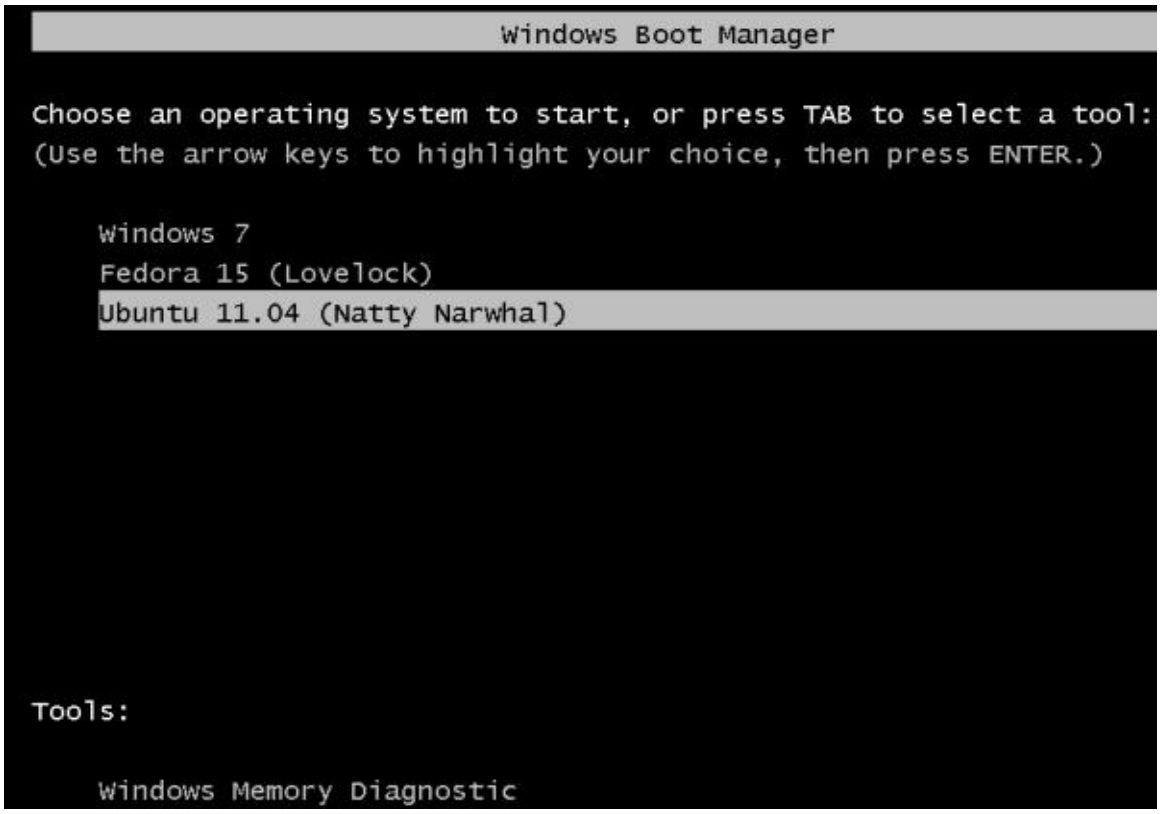
۷) سپس بعد از نصب، باید از ویندوز بالا بیاید و مراحل کار Easy-BCD را مجدد برای این توزیعی که الان نصب کرده اید مجدد انجام دهید.

در صورت تمایل به مرور BCD به صفحه (...) رجوع شود.فقط شکل ها را می گذارم:




EasyBCD 2.0.2 - NeoSmart Technologies
File Tools Help
EasyBCD Toolbox
View Settings
Edit Boot Menu
Add New Entry
Advanced Settings
BCD Backup/Repair
Bootloader Setup
Useful Utilities
Operating Systems
Windows
Linux/BSD
Mac
NeoGrub
Type: GRUB 2
Name: Ubuntu 11.04 (Natty Narwhal)
Device: (Automatically configured)
Add Entry
Portable/External Media
WinPE
Virtual Disk
ISO Boot
BIOS Extender
Type: WIM Image (Ramdisk)
Name: NST WinPE Image
Path:
EMS Enabled
Force portable entry
Add Entry


EasyBCD 2.0.2 - NeoSmart Technologies
File Tools Help
EasyBCD Toolbox
View Settings
Edit Boot Menu
Add New Entry
Advanced Settings
BCD Backup/Repair
Bootloader Setup
Useful Utilities
Modify Menu Entries
Up
Down
Rename
Delete
Entry
Default
Windows 7
Yes
Fedora 15 (Lovelock)
No
Ubuntu 11.04 (Natty Narwhal)
No
Timeout Options
Skip the boot menu
Boot default OS after 30 seconds
Save Settings



نصب CentOS از طریق NetInstall(URL method) :

نکته۱: حداقل RAM مورد نیاز برای این روش: 1GB

نکته۲: حداقل فضای لازم برای نصب این روش: 12-15 GB

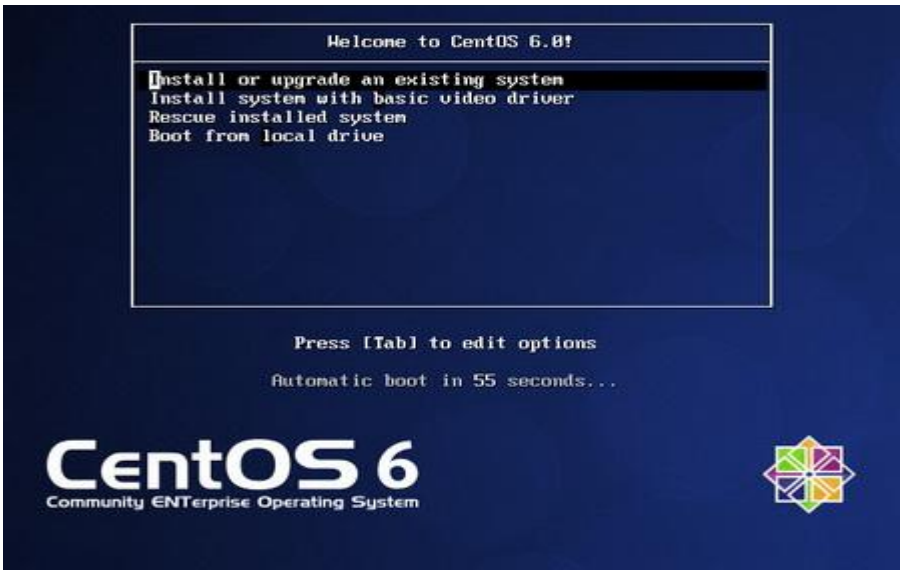
۱) شما برای نصب cent-os از این روش ابتدا بایستی فایل iso مورد نظر را دانلود کنید.

برای ۳۲ بیتی:

http://ftp.linux.ncsu.edu/pub/CentOS/6.4/isos/i386/CentOS-6.4-i386-netinstall.iso

۲) سپس آن را بر روی CD/DVD رایت کرده و از بوت سیستم [CD/DVD]-Rom Drive انتخاب کنید:

۳) انتخاب اولین گزینه:

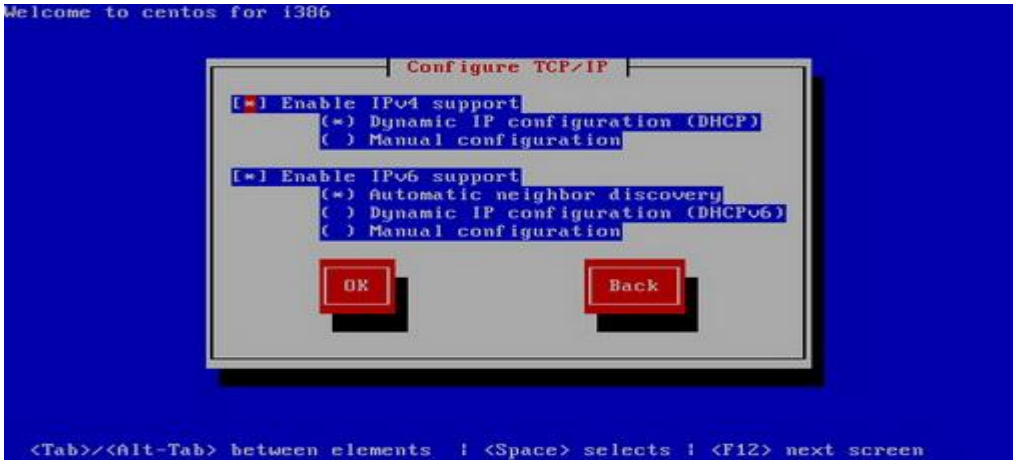


۴) انتخاب **skip**:

۵) انتخاب **URL**:

۶) انتخاب اینترفیسی که متصل به اینترنت است:

۷) کانفیگ TCP/IP برای تنظیمات اینترنت:



۸) نوشتن url زیر در قسمت جای خالی اول.

http://mirrors.kernel.org/centos/6.0/os/i38

۹) در حال پردازش فایل **img.** شما:

۱۰) سپس باید زبان خود را انتخاب کنید:

۱۱) تعیین زبان کیبورد:

۱۲) انتخاب time/zone:

۱۳) نوشتن user و password قوی برای OS:

۱۴) شما ۳ گزینه برای انتخاب دارید:

أ. use entire drive:

از تمام هارد شما برای نصب استفاده می کند.

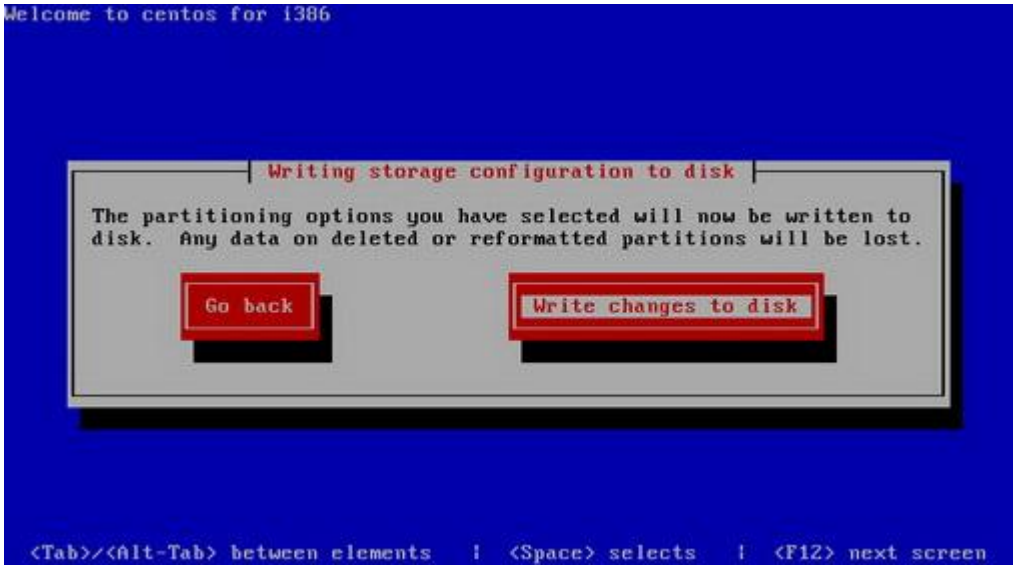
ب. replace existing linux...:

جایگزینی OS جدید شما که درحال نصب آن هستید (cent-os) با دیگر سیستم عامل های لینوکسی.

ج. use free space:

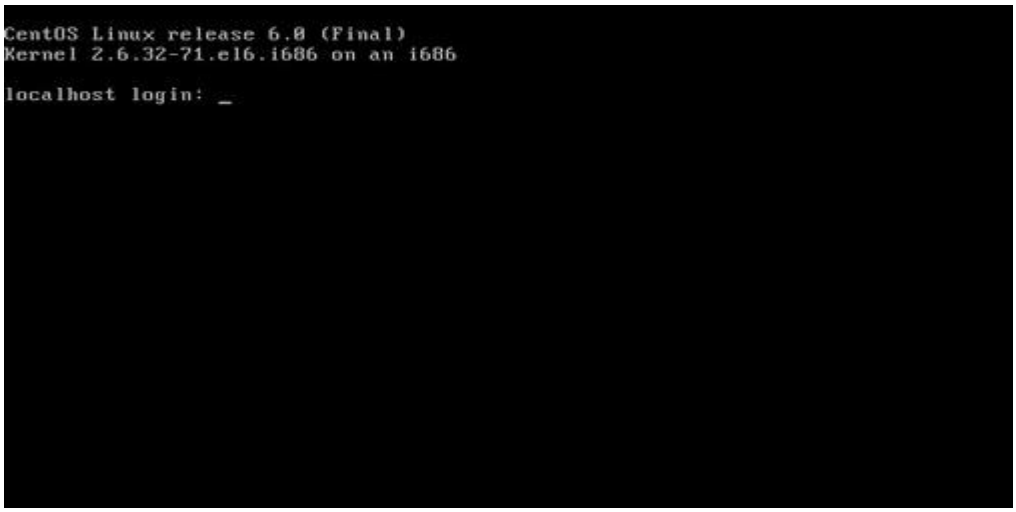
انتخاب فضای آزاد دیسک برای نصب OS.

۱۵) انتخاب Write changes to disk:



۱۶) سپس صبر کنید تا مراحل نصب OS انجام شود و در نهایت reboot را انتخاب کنید:

۱۷) User و password که قبلا ساخته بوده اید را بعد از بالا آمدن OS وارد کنید:



لینک های کاربردی در نصب OS به روش netinstall:

http://www.if-not-true-then-false.com/2010/centos-netinstall-network-installation/

http://www.linuxh0st.net/howto/centos5

http://www.howtoforge.com/how-to-do-a-centos-6.0-network-installation-over-http

نصب CentOS از طریق Minimal Installation (Network Configuration) :

مثل دیگر نصب ها می باشد، با این تفاوت که شما باید یک سری تنظیمات را از طریق Command بنویسید و به کانفیگ OS اضافه کنید تا مشکل شما حل شود.

اگر در این روش نصب مشکل داشتید، می توانید طبق مراحل زیر عمل کنید:

دقت کنید:

Ping google.com

Ping: Unknown host google.com

شما باید تغییرات را اعمال کنید، ابتدا:

vim /etc/sysconfig/network-scripts/ifcfg-eth0

سپس جلوی IP ADDR=x.x.x.x، ip static خودتان را بنویسید.

سپس جلوی GATEWAY=y.y.y.y ، ip Router را بنویسید.

اگر نمی دانید MAC-address کارت شبکه شما چیست از روش زیر بروید:

ifconfig eth0 | grep -o -E '([[:xdigit:]]{1,2}:){5}[[:xdigit:]]{1,2}'

سپس جلوی HWADDR='your mac address' ، mac-address کارت **مورد نظر را** بنویسید.

در ادامه باید این فایل را هم تغییر دهید:

```
vi /etc/sysconfig/network
GATEWAY = y.y.y.y
```

سپس باید سرویس شبکه را Reset کنید:

```
/etc/init.d/networking restart
```

نتیجه:

```
ping google.com
PING google.com (173.194.67.138) 56(84) bytes of data
64 bytes from wi-in-f138.1e100.net (173.194.67.138): icmp_seq=1 ttl=49
time=7.88 ms
64 bytes from wi-in-f138.1e100.net (173.194.67.138): icmp_seq=2 ttl=49
time=7.13 ms
```

لینک های کاربردی در نصب OS به روش Minimal :

http://community.spiceworks.com/how_to/show/57482-centos-minimal-install

http://architects.dzone.com/articles/centos-minimal-installation

http://www.idevelopment.info/data/Unix/Linux/LINUX_AddGNOMEToCentOSMinimalInstall.shtml

اضافه کردن ابزارهای مدیریتی و تکاملی در روش Minimal:

۱) به روز رسانی OS با:

```
yum -y update
```

۲) Reset سیستم برای اعمال آپدیت ها:

دستور reboot

۳) نصب ابزارهای زیر:

```
yum –y groupinstall "Base" "Development Libraries" "Development Tools"
```

۴) دستور reboot .

برای تست دستور زیر را امتحان کنید:

```
nslookup www.packtpub.com
nslookup www.irsecteam.org
```

۵) دستور زیر :

yum –y install firstboot

۶) دستور :

chkconfig firstboot on

باعث می شود سرویس **firstboot** همیشه پس از بالا آمدن سیستم به طور خودکار فعال شود.

۷) سپس دستور **reboot** .

نصب CentOS از طریق KickStart :

این روش، یکی از روش های حرفه ای در نصب تمام توزیع های لینوکس می باشد که خود این **KickStart** نیز به زیر شاخه های متعددی تقسیم می شود.

یکی از پرکاربردترین استفاده آن وقتی است که: فرض کنید شما می خواهید چندین توزیع لینوکس مثل همین **CentOS** را بر روی چندین سیستم در شرکت خود نصب نمایید. شما در نگاه اول، دو راه حل در ذهن خود دارید:

الف) استفاده از یک دی-وی-دی برای نصب (**Single-task**).

ب) استفاده از چندین دی-وی-دی که از روی توزیع اصلی خود کپی کرده اید (**Multi-task**)

ولی این کار فقط باعث اتلاف وقت شما خواهد شد.

راه حل:

شما کافی است یک بار این توزیع را بر روی سرور خود نصب کرده و سپس با استفاده از تنظیماتی که در حین نصب برای آن انجام داده اید آن را کپی کرده و بر روی دیگر سیستم ها و فقط با یک خط دستور اقدام به نصب خودکار توزیع لینوکس مورد نظر خود کنید.

چون نمی خواهم حجم کتاب بالا برود. به همین خاطر خودم یک سری فیلم از **you-tube** دانلود کرده و دیده ام و چون در فیلم ها همه چیز واضح است در اینجا در مورد آن مطلبی قرار نمی دهم.

لینک فیلم ها:

http://www.youtube.com/results?search_query=centos+kickstart+installation&sm=

http://www.youtube.com/results?search_query=install+centos+via+kickstart+installation&sm

سایت های زیر انواع روش های نصب **kickstarat** را به طور کامل توضیح داده است:

http://modlearning.com/linux/building-a-kickstart-server-centos-5/

http://www.openlogic.com/wazi/bid/188083/Automatic-CentOS-6-0-Installation-With-Kickstart

http://www.nathanboyce.com/automatic-centos-6-installation-dvd-with-kickstart/

http://sysadmin.compxtreme.ro/pxe-bootkickstart-centos-6-3-install/

http://venkataraoss.blogspot.com/2011/02/kickstar -server-in-10-steps.html

http://www.server-world.info/en/note?os=CentOS_6&p=pxe&f=3

لینک های کاربردی فصل اول:

http://askubuntu.com/questions/88384/h -can-i-repair-grub-how-to-get-ubuntu-back-after-installing-windows

http://www.linuxbsdos.com/2008/11/17/linu -logical-volume-manager/

http://www.techotopia.com/index.php/Installing_CentOS_6_with_Windows_in_a_Dual_Boot_Environment

http://www.techotopia.com/index.php/Installing_CentOS_6_on_ Clean_Disk_Drive

http://www.linwik.com/installing_centos

http://jadelinux.com/installcentos.html

http://landoflinux.com/linux_install_centos_64.ht


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش لینوکس مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
LINUX
FOUNDATION


شهریه دوره:
۱۱۰ هزار تومان
کلاس آموزش امنیت شبکه مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۷ روز


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش طراحی صفحات وب - مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد -
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
WEB

پیکـــربنـــدی و مدیریت CentOS

امیدوارم در فصل اول با مشکلی رو به رو نشده باشید و الان هم، آماده و سرحال می خواهید ادامه مباحث این توزیع را پیگیری کنید.

در این فصل در مورد نحوه کار با centos توضیح خواهم داد و قسمت هایی که در اینترنت، به زبان فارسی و مفصل توضیح داده شده است فقط لینک قرار می دهم تا خود دوستان در صورت تمایل مراجعه و مطالعه کنند.

کار با رابط خط فرمان (command-line interface) :

شل (shell) یا همان پوسته یک محیطی است که در آن می توانید با سیستم ارتباط برقرار کنید.

قسمت های مهم یک ترمینال در شکل زیر:

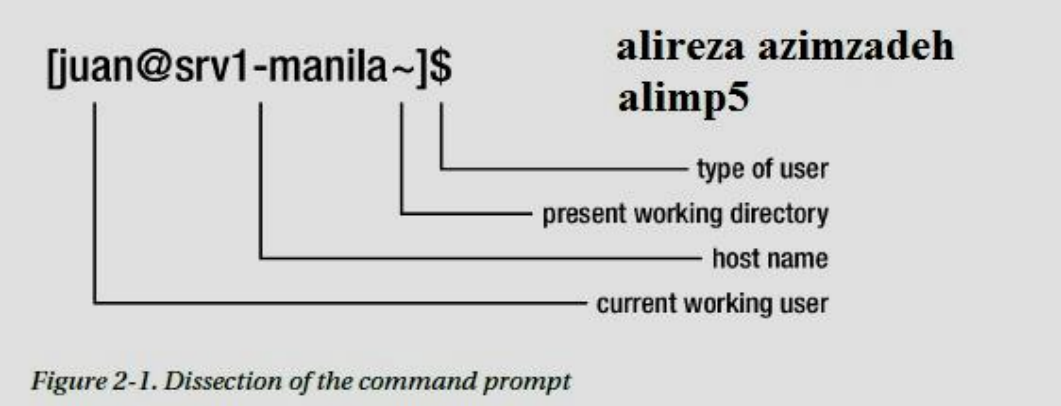


Figure 2-1. Dissection of the command prompt

از چپ به راست توضیح می دهم:

juan : یوزر فعلی که در حال استفاده از سیستم است را برای شما مشخص می کند.

srv1-manila : با @ از یوزر جدا شده و تعیین کننده اسم هاست (hostname) شما می باشد.

~ : محلی که شما در آن قرار هستید نشان می دهد.

$ یا # : نشان دهنده سطح دسترسی شما یا همان مدیر سیستم (root) می باشد.

برای تشخیص این کار از دستور زیر استفاده کنید: **whoami**

```
[juan@srv1-manila ~]$ whoami
juan
```

برای رفتن به مد root از دستور زیر استفاده کنید:

```
[juan@srv1-manila ~]$ su - root
Password:
[root@srv1-manila ~]# whoami
 root
```

نکته: به طور پیشفرض در centos 6.x شما به عنوان root (بالاترین دسترسی) در حال کار هستید.

اجزای FileSystem:

برای آشنایی با اجزای این ساختار و توضیحات دقیق به سایت زیر مراجعه کنید:

http://tazik.ir/139 %8C

مدیریت بسته ها با YUM (YellowDog Updater Modified):

یکی از مهم ترین دستورات کار با توزیع CentOS می باشد، که برای آپگرید، آپدیت، حذف، نصب و به دست آوردن اطلاعات از بسته ها استفاده می شود.

بروز رسانی سیستم (update) :

۱) با دستور زیر می توانید متوجه شوید که آیا بسته بروزتری از بسته شما وجود دارد یا خیر(لیست کردن بسته ها):

yum check-update

```
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: anorien.csc.warwick.ac.uk
 * extras: anorien.csc.warwick.ac.uk
 * updates: mirror.rmg.io
Setting up Update Process
No Packages marked for Update
```

۲) در صورت وجود بسته هایی برای آپدیت می توانید از دستور زیر استفاده کنید:

yum update یا yum -y update

نکته۱: -y بدون سوال از شما، مستقیما اقدام به آپدیت می کند.

نکته۲: برای تاثیر بسته های آپدیت شده، پس از هربار بروز رسانی باید سیستم خود را Restart کنید:

با دستور: **reboot**

```
yum update


Transaction Summary
============================================================
Install        1 Package(s)
Upgrade       14 Package(s)

Total download size: 86 M
Is this ok [y/N]:
```

۳) بروز رسانی بسته ای خاص:

yum update package-name

yum update package-name1 package-name2 package-nameN

مثال۱: بروز رسانی یک بسته:

yum update yum

مثال۲: بروز رسانی چند بسته به طور همزمان:

yum update openssl sshd httpd

پاکسازی کش (cache) با yum :

yum یک کش از محتویات داده ها و بسته ها که در خیلی از موارد وجود این کش سرعت کار را افزایش خواهد داد، خودش می سازد، اما در بعضی مواقع لازم است که کش خالی شود و مجدد بارگذاری شود.

طبق دستورات زیر عمل کنید:

۱) **دستور زیر اطلاعات مربوط به بسته ها را از کش خالی می کند:**

yum clean packages

۲) **دستور زیر اطلاعات مربوط به XML-Based metadata را از کش خالی می کند:**

yum clean metadata

۳) **دستور زیر هرگونه فایل های دیتابیس کش شده را از کش خالی می کند:**

yum clean dbcache

۴) **پاکسازی نهایی:**

yum clean all

۵) آخرین مرحله، ساخت مجدد کش **yum** هست.(در اینجا کش جدید ساخته می شود):

```
yum makecache
```

بروز رسانی خودکار Yum با ابزار Yum-Cron :

برای اینکه مجبور نباشید به صورت دستی عمل آپدیت را انجام دهید می توانید از ابزار **yum-cron** استفاده کنید، این ابزار به طور پیشفرض بر روی سیستم شما نصب نیست. طبق مراحل زیر اقدام به نصب و راه اندازی آن می کنیم:

۱) نصب ابزار:

```
yum install yum-cron
```

۲) فعال کردن ابزار هنگام بوت شدن سیستم:

```
chkconfig yum-cron on
```

۳) خاموش کردن ابزار زیر بعد از بوت شدن سیستم:

```
chkconfig yum-updatesd off
```

۴) غیر فعال کردن سرویس زیر:

```
service yum-updatesd stop
```

۵) در اینجا باید یک سری تغییرات را در ابزار **yum-cron** ایجاد کنیم:

```
vi /etc/sysconfig/yum-cron
```

۶) سپس متن های زیر را پیدا کنید، در صورتی که نبودند طبق زیر آنها را وارد کنید:

```
ERROR_LEVEL=1
MAILTO=your_email_address_here
```

نکته۱: **error_level** عددی بین ۱ تا ۱۰ می باشد، که شما میتوانید مقدار آن برابر یک گذاشته تا از پیغام های خطا در حین آپدیت مطلع شوید.

نکته۲: در قسمت **Mail to** هم ایمیل آدرس خودتان را بنویسید که پیغام ها به آن آدرس ارسال شوند.

۷) سپس باید سرویس **yum-cron** را در بوت شدن سیستم نیز فعال کنیم:

```
service yum-cron start
```

۸) در آخر هم دستور:

```
yum update
```

نصب بسته ها با yum :

می توانید همزمان یک یا چند بسته را نصب کنید.

```
yum install package_name
yum install  package_name1  package_name2  package_name N
```

مثال۱:

```
yum install openssl
```

مثال۲:

```
yum install openssl ssh httpd
```

حذف بسته ها با yum :

```
yum remove package_name
yum remove package_name1 package_name2 package_name N
```

مثال۱:

```
yum remove wget
```

مثال۲:

```
yum remove wget openssl
```

جستجوی بسته ها با yum :

اگر بسته ای را مد نظر دارید و می خواهید بدانید آیا وجود دارد یا خیر می توانید از دستور زیر استفاده کنید:

```
yum search keyword
```

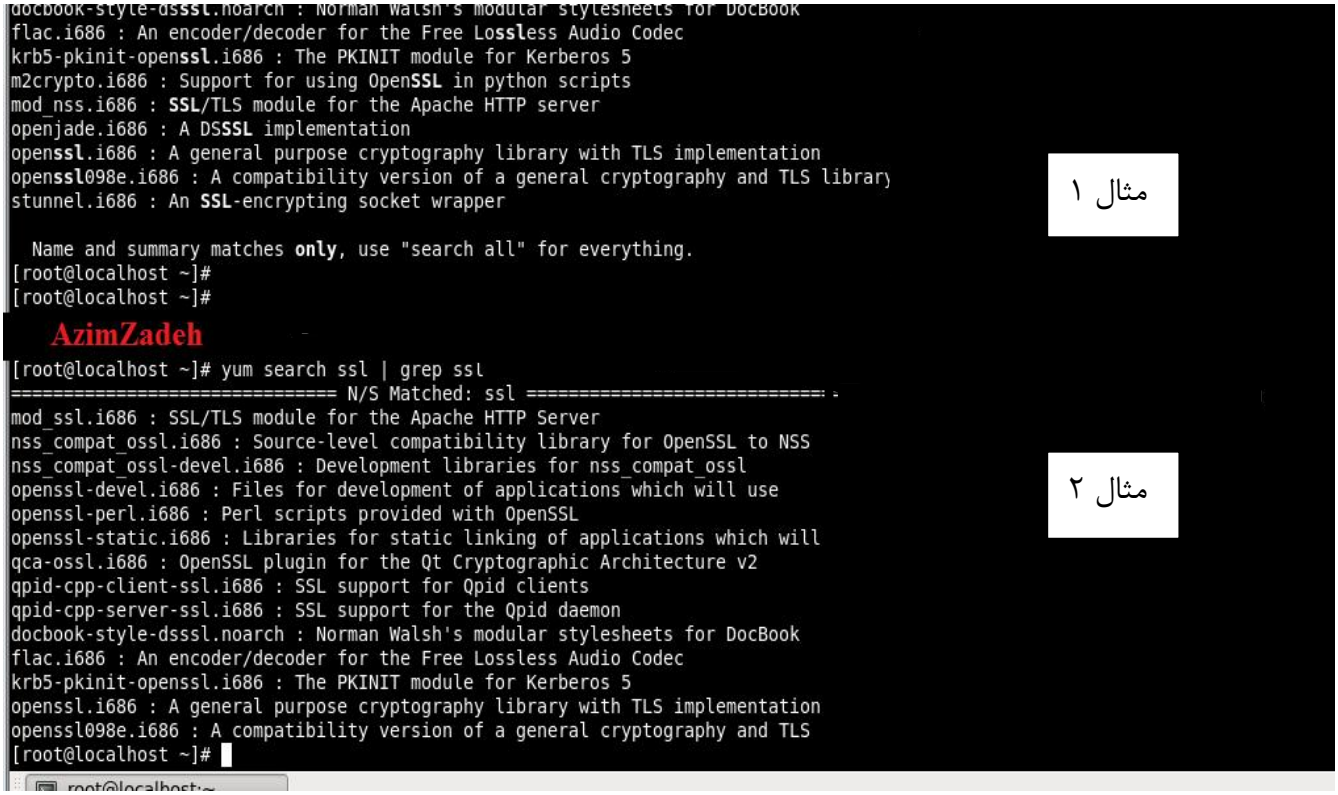
مثال۱: بسته هایی در آنها واژه ssl بکار رفته است:

```
yum search ssl
```

مثال۲: بسته هایی که واژه ssl از دیگر کلمات جدا است (به کوچک و بزرگی حروف نیز حساس باشد):

```
yum search ssl | grep ssl
```

نتیجه دو مثال بالایی :



نکته۱: اگر می خواهید بدانید که بسته مورد نظر شما برای نصب و یا اجرا به چه بسته هایی وابسته است، می توانید از دستور زیر استفاده کنید:

yum deplist package_name

مثال:

yum deplist openssl

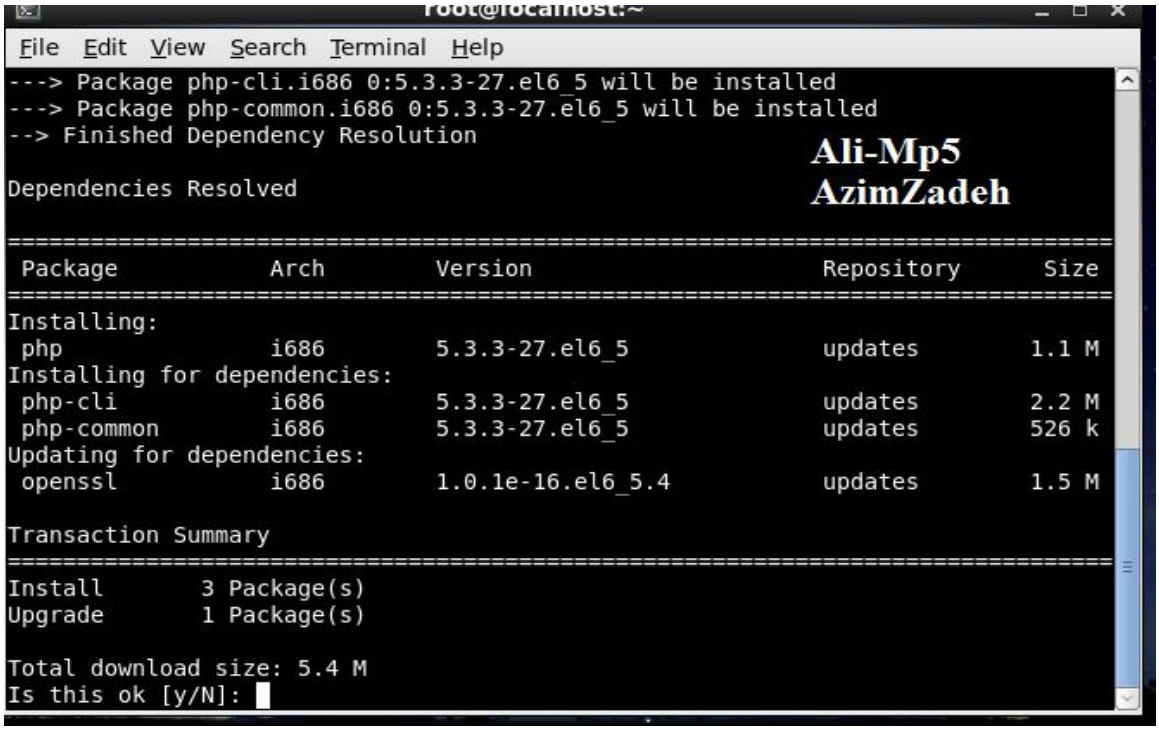
نکته۲: برای این که ببینید چه بسته هایی روی سیستم شما نصب شده است از دستور زیر استفاده کنید:

yum list installed | less

ساخت مخزن محلی برای yum :

خیلی از بسته هایی که شما نیاز به آنها دارید، وقتی که centos DVD را دانلود می کنید داخل خودش دارد، چون شما از آن فقط برای نصب بسته های اولیه استفاده می کنید ، اطلاع ندارید که اگر بخواهید بسته ای را در آینده نصب کنید،در داخل خود این DVD قرار دارد و شما می توانید اقدام به نصب آن بسته کنید و سپس آن را با دستور yum به بروزترین بسته ای که از آن بسته موجود است برسانید. با مثال توضیح خواهم داد، نگران نباشید.

مثال: در اینجا ما می خواهیم بسته های مربوط به PHP را در سیستم خود نصب کنیم. در ابتدا از دستور yum install php استفاده کردم. با اجرای این دستور ما برای نصب php و بسته های وابسته به آن باید به اینترنت وصل شویم که در شکل زیر می بینید:



حالا ما می خواهیم از خود بسته های موجود در DVD centos که دانلود کرده ایم استفاده کنیم، برای این کار یک سری کار لازم است:

نکته: اگر در ماشین مجازی می خواهید این کار را انجام دهید، دقت کنید که گزینه استفاده DVD در داخل ماشین مجازی را انتخاب کرده باشید:

۱. در ابتدا DVD را به مسیر زیر وصل می کنیم:

mount /dev/cdrom /mnt

نتیجه دستور بالا:

mount: block device /dev/sr0 is write-protected, mounting read-only

۲. باید یک مخزن بسازیم:

vi /etc/yum.repos.d/centos6.4.repo

سپس عبارات زیر را در آن کپی کنید :

[CentOS6.4-Repository]

name=DVD-CentOS6.4 repository

baseurl=file:///mnt

enabled=1

gpgcheck=0

سپس ESC کیبورد را بفشارید و در ادامه بنویسید w: و در آخر هم q:

w= فایل شما را ذخیره می کند.

q= فایل شما را ذخیره می کند و از فایل خارج می شود.

نکته: می توانید بدین صورت هم بنویسید wq:

نتیجه:

۳. در ادامه به مسیر زیر بروید و اسم فایل CentOS-Base.repo را به CentOS-Base.backup تغییر دهید:

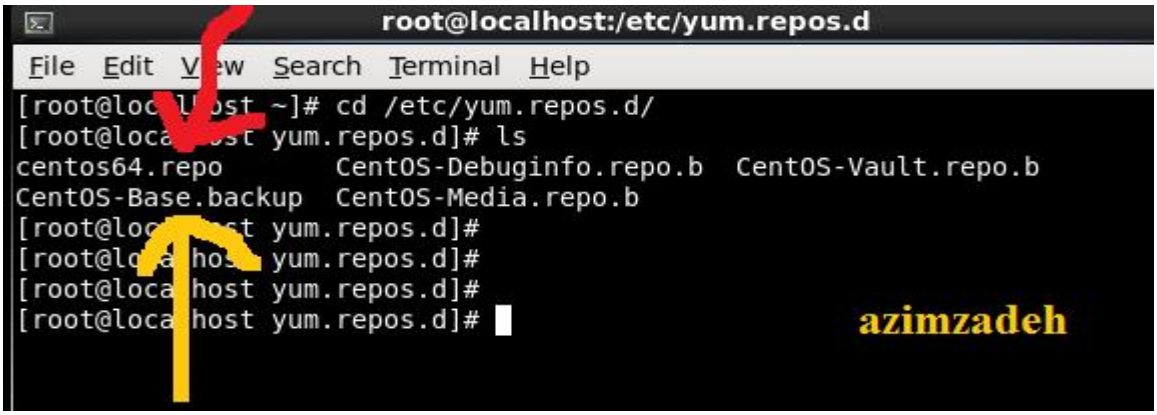
cd /etc/ yum.repos.d/

mv /etc/ yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.backup

۴. از دستور ls استفاده کنید تا مطمئن شوید که فایل شما اسمش تغییر کرده است یا خیر:

ls

نتیجه: می بینیم که عمل تغییر اسم انجام شده و مخزن محلی هم ساخته شده است:



۵. در این مثال ما قصد داشتیم بسته PHP را نصب کنیم، پس ما از دستور زیر استفاده می کنیم:

yum install php

نکته: بسته هایی را که مد نظر دارید می توانید از این روش اقدام به نصب آن کنید.

۶. دوباره باید اسم مخزن را به حالت اولش تغییر دهیم:

mv /etc/ yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo

۷. در نهایت باید از دستورات زیر استفاده کنیم:

yum clean all

yum update php

نتیجه:

```
---> Package php-cli.i686 0:5.3.3-27.el6_5 will be installed
---> Package php-common.i686 0:5.3.3-27.el6_5 will be installed
--> Finished Dependency Resolution
                                    yum update php
Dependencies Resolved

================================================================================
 Package           Arch        Version                   Repository      Size
================================================================================
Installing:
 php               i686        5.3.3-27.el6_5            updates        1.1 M
Installing for dependencies:
 php-cli           i686        5.3.3-27.el6_5            updates        2.2 M
 php-common        i686        5.3.3-27.el6_5            updates        526 k
Updating for dependencies:
 openssl           i686        1.0.1e-16.el6_5.4         updates        1.5 M

Transaction Summary
================================================================================
Install       3 Package(s)
Upgrade       1 Package(s)

Total download size: 5.4 M
Is this ok [y/N]:
```

برای کسب اطلاعات بیشتر در مورد yum می توانید به سایت زیر مراجعه کنید:

http://yum.baseurl.org/wiki/Guides

مخازن مهم CentOS (EPEL و Remi) :

این دو مخرن یکی از پر کاربردترین مخازنی هستند که می توان دراین قسمت به آن اشاره کرد. پس حتما آنها را نصب کنید و از بسته های جالبی که در آنها وجود دارد استفاده لازم را ببرید.

نصب مخزن EPEL :

نکته: چون ممکن است در هر لحظه این دستورات تغییر کنند، شما می توانید به سایت زیر مراجعه کرده و آخرین تغییرات مسیرها را بررسی کنید:

http://dl.fedoraproject.org/pub/epel/ /

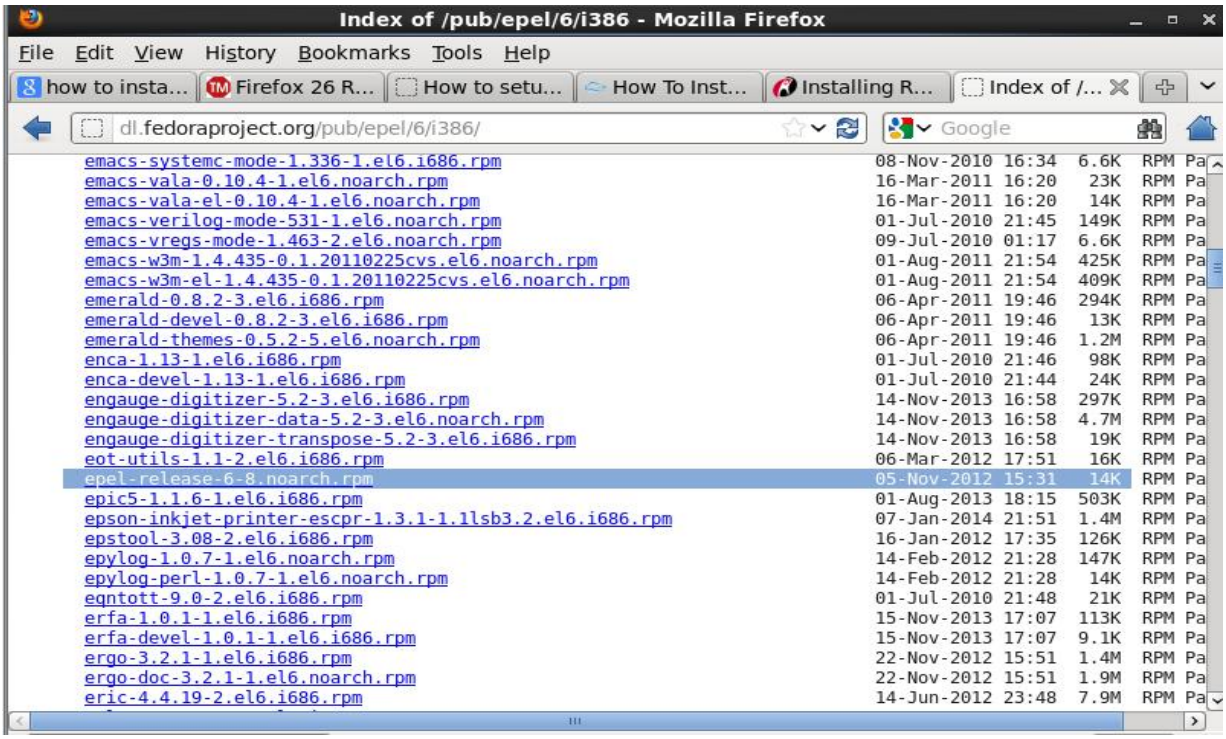
۱. نصب ابزار wget :

yum install wget

۲. دانلود و نصب مخزن :

sudo rpm -Uvh http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

نکته: برای دانلود ورژن 32بیتی ، قسمت " x86_64 " را به " i386 " تغییر دهید.



نصب مخزن Remi :

نکته: ممکن است در هر لحظه این دستور تغییر کند، شما می توانید به سایت زیر مراجعه کرده و آخرین تغییرات مسیرها را بررسی کنید:

http://rpms.famillecollet.com/enterprise/

۱. دانلود و نصب مخزن:

sudo rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-6.rpm

۲. بعد از نصب هر دو مخزن دستورات زیر را بنویسید:

cd /etc/yum.repo

yum clean all

yum check-update

yum update

```
[root@localhost yum.repos.d]#
[root@localhost yum.repos.d]# sudo rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-relea
-6.rpm
Retrieving http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
warning: /var/tmp/rpm-tmp.RLNTmM: Header V3 DSA/SHA1 Signature, key ID 00f97f56: NOKEY
Preparing...                ########################################### [100%]
   1:remi-relea             ########################################### [100%]
[root@localhos  yum.repos.d]#
[root@localhost yum.repos.d]# ls
centos64.repo.bk  CentOS-Debuginfo.repo  CentOS-Vault.repo  epel-testing.repo
CentOS-Base.repo  CentOS-Media.repo      epel.repo          remi.repo
[root@localhost yum.repos.d]#
[root@localhost yum.repos.d]# yum clean all
Loaded plugins: fastestmirror, priorities, refresh-packagekit, security
Cleaning repos: base epel extras updates
Cleaning up Everything
[root@localhost yum.repos.d]#
```

نکته: ممکن است بعد از نصب این دو مخزن دچار مشکل در نصب بسته ها و یا بروز رسانی شوید، نگران نباشید، فقط کافی است ۲۰-۱۵ بار دستور yum check-update یا yum update را اجرا کنید.

```
[root@localhost yum.repos.d]# yum check-update
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
Could not get metalink https://mirrors.fedoraproject.org/metalink?repo=epel-6&arch=i
386 error was
14: PYCURL ERROR 6 - "Couldn't resolve host 'mirrors.fedoraproject.org'"
 * base: repo.boun.edu.tr
 * epel: epel.mirror.srv.co.ge
 * extras: mirrors.prometeus.net
 * updates: centos.fastbull.org
Error: Cannot retrieve repository metadata (repomd.xml) for repository: epel. Please
 verify its path and try again
[root@localhost yum.repos.d]# yum check-update
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
epel/metalink                                            | 5.1 kB     00:00
 * base: mirror.crazynetwork.it
 * epel: ftp.riken.jp
 * extras: mirrors.prometeus.net
 * updates: ftp.otenet.gr
epel                                                     | 4.2 kB     00:00
epel/primary_db            24% [====             ]  30 kB/s | 1.2 MB     02:05 ETA
```

برای کسب اطلاعات بیشتر در مورد مخزن ها می توانید به سایت های زیر مراجعه کنید:

http://blog.famillecollet.com/pages/Config-en

http://wiki.centos.org/AdditionalResources/Repositories

http://sourceforge.net/projects/flexbox/files/?source=navbar

مدیریت فولدرها و فایل ها :

در هنگام کار با یک سرور به ویژه هنگامی که شما دسترسی فیزیکی ندارید، ناچار خواهید بود که از دستورات استفاده کنید.

دستورات مهم را برای اینکه در حین کار با این کتاب و سرور خود با مشکل مواجه نشوید توضیح می دهم.

۱) دستور **pwd** :

نشان دادن مسیری که در آن(فولدر) هستید.

```
[root@localhost ~]# cd /home/
[root@localhost home]# cd alimp5/
[root@localhost alimp5]#
[root@localhost alimp5]#
[root@localhost alimp5]#
[root@localhost alimp5]# pwd
/home/alimp5
[root@localhost alimp5]#
```

۲) دستور **cd** :

برای تغییر مسیر به کار می رود.

cd /etc/sysconfig

برای برگشت به یک فولدر عقب تر:

cd ..

برای برگشت به مسیر **root** :

cd

نکته: پیشفرض در **root** قرار دارید.

۳) دستور **mkdir** :

برای ساخت فولدر استفاده می شود.

مثلاً ساخت فولدر در مسیر **home**:

cd /home

mkdir alimp5

اگر می خواهید به صورت تو در تو فولدر بسازید از دستور زیر استفاده کنید:

mkdir -p alimp5/irsecteam/salam

```
[root@localhost ~]#
[root@localhost ~]# mkdir azimzade
[root@localhost ~]# mkdir -p ali/reza/azimzadeh
[root@localhost ~]# ls
ali              azim      Documents    install.log.syslog  Public
alimp5.txt       azimzade  Downloads    Music               Templates
anaconda-ks.cfg  Desktop   install.log  Pictures            Videos
[root@localhost ~]# cd ali/reza/azimzadeh/
[root@localhost azimzadeh]#
[root@localhost azimzadeh]# pwd
/root/ali/reza/azimzadeh
[root@localhost azimzadeh]#
```

۴) دستور mv :

برای تغییر اسم فولدر یا جا به جا کردن یک فولدر به کار می رود.

مثال ۱:

mv alimp5/ /root/azimzadeh

مثال ۲:

mv alimp5/ /root/alimp5

۵) دستور rm :

برای حذف کردن فایل و فولدرها بکار می رود.

rm irsecteam.txt

rm ali reza.txt pic.png

در مثال های بالا باید شما در جواب بنویسید: y

اما اگر پارامتر Rf- را اضافه کنید، خودکار حذف می کند:

rm -Rf ali

یا

rm -rf ali

```
[root@alimp5 ~]# touch alireza
[root@alimp5 ~]# touch jafar
[root@alimp5 ~]# ls
ali              Desktop    install.log         Music      Templates
alireza          Documents  install.log.syslog  Pictures   Videos
anaconda-ks.cfg  Downloads  jafar               Public
[root@alimp5 ~]# rm alireza
rm: remove regular empty file `alireza'? y
[root@alimp5 ~]# rm -Rf jafar
[root@alimp5 ~]#
[root@alimp5 ~]#
[root@alimp5 ~]#
```

۶) دستور rmdir :

برای حذف فولدر خالی به کار می رود.

اگر خالی نباشد به شما پیغام می دهد.

rmdir alimp5

۷) دستور touch:

برای ساخت فایل استفاده می شود.

touch Alireza

۸) دستور file:

برای اینکه ببینید فایل خالی است یا خیر استفاده می شود.

اگر خالی باشد، می نویسد : empty

اگر پر باشد، می نویسد : ASCI text

file Alireza

```
ot@alimp5 ali]#
ot@alimp5 ali]# touch alireza salam
ot@alimp5 ali]# ls
reza  salam
ot@alimp5 ali]# echo "hi" > salam
ot@alimp5 ali]# file alireza salam
reza: empty
am:   ASCII text
ot@alimp5 ali]#
```

۹) دستور cp :

برای جا به جا کردن فایل ها و فولدرها استفاده می شود و از مبدا به مقصد کپی می شود.

آدرس مسیر مقصد آدرس مسیر مبدا cp

cp /root/alimp5.txt /Home/alimp5.txt

نکته: اگر پارامتر v- را به آخر خط اضافه کنید، یک خروجی از کار انجام شده به شما می دهد.

```
root@alimp5 ~]# cp ali/alireza /root/alireza
root@alimp5 ~]# ls /root/
li              Desktop    install.log         Pictures   Videos
lireza          Documents  install.log.syslog  Public
naconda-ks.cfg  Downloads  Music               Templates
root@alimp5 ~]#
```

۱۰) دستور find :

برای جستجوی فایل ها به کار می رود، چون بسیار کاربردی است، برای هر قسمت عکس می گذارم.

find path pattern

مثال۱: نمایش مسیر فایل های که با حرف alimp شروع می شود (علامت / بدین معناست که از root شروع به گشتن می کند و تمام سیستم را برای پیدا کردن نام هایی که با نام جستجویی ما یکسان است می گردد) :

```
root@localhost ~]#
root@localhost ~]# find / -name alimp*
home/alimp5/alimp5.txt
root/alimp5.txt
tmp/alimp5.txt
root@localhost ~]#
```

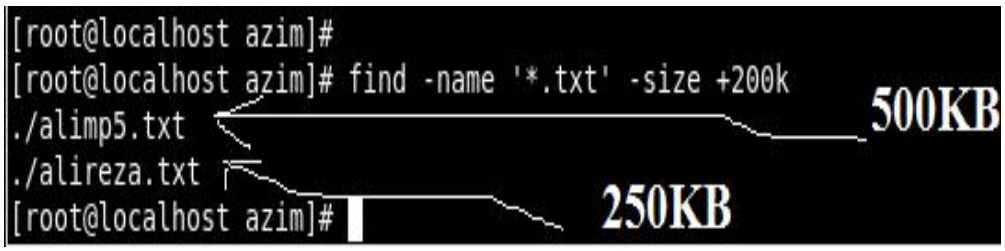
مثال۲: نمایش مسیر فایل هایی با عنوان alimp5 که در داخل فولدر azim قرار دارند:

```
[root@localhost ~]#
[root@localhost ~]# find azim/ -name 'alimp5'
azim/alimp5
[root@localhost ~]#
```

نکته: اگر در مسیر فولدر خاصی قرار داشتید، می توانید بدین صورت هم جستجو کنید:

```
[root@localhost azim]#
[root@localhost azim]# find -name 'alimp5'
./alimp5
[root@localhost azim]#
[root@localhost azim]#
[root@localhost azim]# find -name 'alimp*'
./alimp454545
./alimp546
./alimp5
[root@localhost azim]#
```

مثال۳: نمایش مسیر فایل هایی که نام آنها با به پسوند txt. ختم می شود و حجم آن فایل ها بیشتر از ۲۰۰ کیلو بایت است:



نکته: حتی می توانید از عملگرهای not , or , and نیز استفاده کنید.

مثال۴: نمایش فایل هایی که در داخل فولدر(پوشه) azim قرار دارند و ،،، یا سایز آنها بیش از 200KB است و یا اینکه به پسوند txt. ختم می شوند:

```
[root@localhost azim]#
[root@localhost azim]# find -name '*.txt' -or -size +200k
./alimp5.txt
./reza.txt
./alireza.txt
./jafar.txt
[root@localhost azim]#
```

برای به دست آوردن اطلاعت بیشتر در مورد find می توانید به سایت های زیر مراجعه کنید:

http://www.codecoffee.com/tipsforlinux/articles/21.htm

http://www.hypexr.org/linux_find_help.php

۱۱) دستور echo :

برای تولید و یا نمایش استفاده می شود.

پارامتر ها:

الف) علامت > :

برای اضافه کردن متن خود به فایل مورد نظر استفاده می شود.

نکته: عمل بازنویسی را انجام می دهد. یعنی هر متنی داخل فایل شما باشد پاک می شود و متن شما اضافه می شود.

ب) علامت >> :

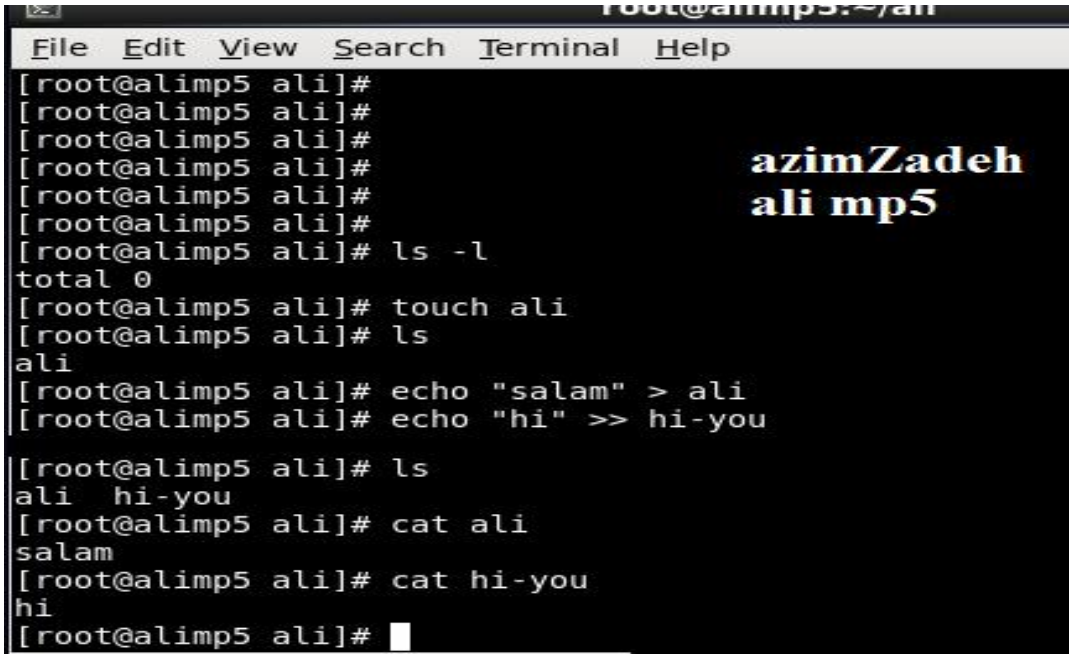
متن شما را در مسیر فایلی که تعیین کرده اید کپی می کند،

نکته: اگر فایل شما وجود نداشته باشد، خودش یک فایل با نام شما برای آن می سازد.

به مثال زیر توجه کنید:

اضافه کردن متن "salam" به فایل ali که ما از قبل ساخته ایم.

اضافه کردن متن "hi" به یک فایلی که وجود ندارد و شما اسم آن فایل را hi-you می گذارید.



مدیریت بسته ها با rpm :

دستور rpm :

از این دستور برای نصب بسته هایی که پسوندشان rpm. است، استفاده می شود.

پارا مترها:

i- : برای نصب بسته استفاده می شود.

rpm -i zlib-devel-1.25..rpm

v- : برای اینکه مطمئن شوید بسته شما نصب شده، از این دستور می توانید برای دیدن خروجی در حین نصب بسته استفاده کنید.

h- : برای نمایش میزان درصد موفقیت آمیز بودن عمل نصب بسته بر روی سیستم شما به کار می رود.

U- : برای آپگرید بسته به کار می رود.

e- : برای حذف بسته به کار می رود.

q- : برای ایجاد یک پرس و جو استفاده می شود.

a- : به معنای همه (all) می باشد.

مثال۳: چون من بسته را قبلاً نصب کرده بودم، فقط پیغامی مبنی بر نصب بسته را نمایش می دهد:

```
[root@alimp5 ~]#
[root@alimp5 ~]# rpm -i '/var/ftp/pub/localrepo/grep-2.6.3-3.el6.i686.rpm'
        package grep-2.6.3-3.el6.i686 is already installed          1

[root@alimp5 ~]# rpm -ivh '/var/ftp/pub/localrepo/grep-2.6.3-3.el6.i686.rpm'
Preparing...                ########################################### [100%]
        package grep-2.6.3-3.el6.i686 is already installed
[root@alimp5 ~]#                                                     2
```

```
rpm -ivh bison-2.3-2.1.i386.rpm                    azimzadeh
                                                   alireza
Listing 7-2. Installing a Package

Preparing...                ########################################### [100%]
   1:bison                  ########################################### [100%]
```

نکته: در صورتی که با عکس زیر مواجه شدید، بدین معناست که شما پیش بسته های لازم برای نصب و راه اندازی بسته مورد نظر نصب نکرده اید:

```
warning: gcc-4.1.2-42.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID e8562897
error: Failed dependencies:
        glibc-devel >= 2.2.90-12 is needed by gcc-4.1.2-42.el5.i386
        libgomp = 4.1.2-42.el5 is needed by gcc-4.1.2-42.el5.i386
        libgomp.so.1 is needed by gcc-4.1.2-42.el5.i386          azimzadeh
```

نکته: می توانید با یک دستور rpm، همزمان چندین بسته را نصب کنید:

rpm lib-deel1.2-5.0.rpm cgg-10.5.rpm .....

مثال۴: آپگرید یک بسته:

rpm –Uvh gcc–4.1.2–43.el5.i386.rpm

مثال۵: حذف یک بسته از سیستم:

rpm –e zlib–devel

نکته: اگر در حذف بسته ها، دقت به پیشنیاز بسته ها نکنید و اقدام به حذف بسته ای کنید که خودش باید باشد، تا بسته ی دیگر اجرا شود، در آن صورت سیستم به شما اخطار خواهد داد:

```
rpm -e zlib-devel

error: Failed dependencies:
        glibc-devel >= 2.2.90-12 is needed by (installed) gcc-4.1.2-42.el5.i386
```

ساخت پرس و جو با rpm :

وقتی که شما مطمئن نیستید که بسته مورد نظرتان بر روی سیستم نصب شده است یا خیر ، می توانید از دستورات زیر استفاده کنید:

مثال۶: می خواهیم بدانیم، آیا بسته bison وجود دارد یا خیر:

rpm –q bison

مثال۷: برای لیست کردن تمام بسته هایی که در سیستم نصب شده است :

rpm -qa package-name

نکته: در این حالت شما باید نام بسته را به طور دقیق به یاد داشته باشید که این هم اصلاً منطقی نیست.

راه حل: چون قبلا آموزش کار با grep را داده ام از ترکیب این دستورات با هم استفاده می کنم:

rpm –qa | grep keyword

نتیجه:

```
oot@alimp5 ~]# rpm -qa ssl
oot@alimp5 ~]#
oot@alimp5 ~]# rpm -qa | grep ssl
d_ssl-2.2.15-29.el6.centos.i686
enssl-1.0.1e-16.el6_5.4.i686
s_compat_ossl-0.9.6-1.el6.i686
oot@alimp5 ~]#
```

به دست آوردن اطلاعات در مورد محتویات بسته ها:

rpm -qi package-name

rpm -qa bison

نکته: در صورتی که بسته روی سیستم شما نصب نشده است، و شما می خواهید از آن اطلاعاتی به دست آورید باید از دستور qip- استفاده کنید:

مثال۸:

rpm –qip yum–3.2.8–9.el5.centos.1.noarch.rpm

```
[root@localhost CentOS]# rpm -qip yum-3.2.8-9.el5.centos.1.noarch.rpm
Name        : yum                           Relocations: (not relocatable)
Version     : 3.2.8                              Vendor: CentOS
Release     : 9.el5.centos.1                 Build Date: Tue 10 Jun 2008 06:13:47
 AM PHT
Install Date: (not installed)                Build Host: builder16.centos.org
Group       : System Environment/Base        Source RPM: yum-3.2.8-9.el5.centos.1
.src.rpm
Size        : 2331786                           License: GPLv2+
Signature   : DSA/SHA1, Sun 15 Jun 2008 07:23:03 AM PHT, Key ID a8a447dce8562897
URL         : http://linux.duke.edu/yum/
Summary     : RPM installer/updater
Description :
Yum is a utility that can check for and automatically download and
install updated RPM packages. Dependencies are obtained and downloaded
automatically prompting the user as necessary.
[root@localhost CentOS]#
```

Alireza azimzadeh

لیست کردن محتویات فولدرها (پوشه):

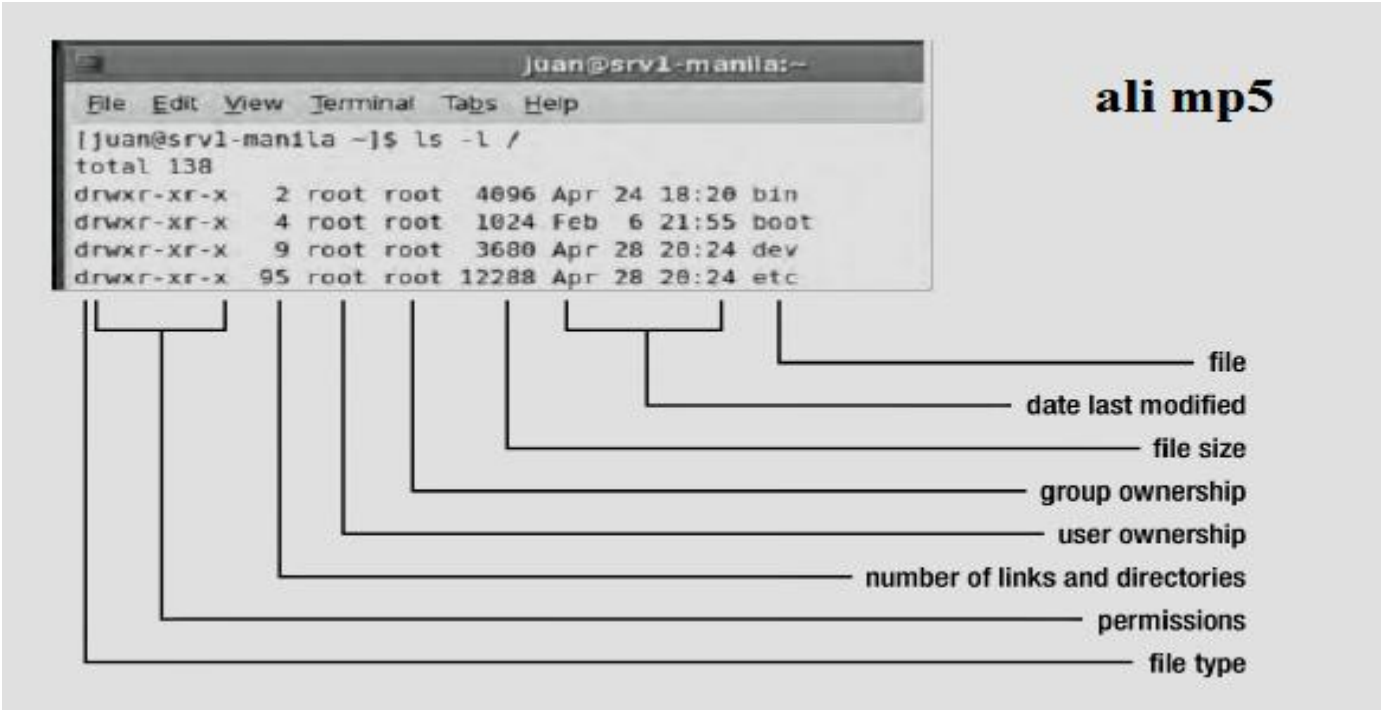
از دستور ls استفاده می شود. و برای دیدن محتویات است.

نکته۱: برای دیدن تمام فایل ها: ls -la

نکته۲: برای دیدن تمام فولدرها: ls -la /

نکته۳: دیدن فایل های پنهان: ls -a

شکل زیر مواردی که دستور ls به شما نشان می دهد را توضیح داده است:



فقط در مورد file type :

انواع سیمبل ها :

۱- سیمبل - : بیانگر فایل هایی با فرمت تکست، دیتابیس، دودویی، عکس و .... می باشد.

۲- سیمبل d : بیانگر وجود فولدر در جایی که از آن لیست گرفته اید می باشد.

۳- سیمبل l : بیانگر بودن یک میانبر به یک جا (یا فایل) خاصی است.

ساخت و دیدن فایل های متنی:

این بخش بسیار مهم است، سعی کنید خوب یاد بگیرید. چرا؟ جواب: چون قرار نیست همیشه به صورت گرافیکی با سیستم در ارتباط باشید، بلکه ممکن است بخواهید از طریق SSH کارهای خود را انجام دهید.

دستورات توضیح داده شده در این بخش شامل: vi , nano , cat , head , tail می باشد.

ابتدا باید ابزار vi و nano را نصب کنید:

```
yum install nano vi
```

برای ویرایش یا ساخت فایل:

```
vi azimzadeh.txt
```

دستور vi :

۱. حرکت کردن به سمت مد نظر= توسط کلیدهای جهت نما.

نکته: برای کار با دستوراتی که از : استفاده می کنند، باید روی کیبورد ESC و سپس : را بفشارید.

۲. خروج از فایل و ذخیره آن= نوشتن :q

۳. خروج از فایل، بدون ذخیره آن= نوشتن :q!

۴. ذخیره فایل و ماندن در فایل= نوشتن :w

۵. جستجو در فایل = نوشتن متن جستجو/ مثل: /ali

۶. جستجو در فایل و چاپ کلمه مورد نظر= نوشتن متن جستجو :g/ مثل: :g/alireza

۷. کپی برداری از یک خط در جایی که مکان نمای موس است = yy

۸. کپی یک کلمه = yw

۹. برای نوشتن در فایلی که قبلا بوده= فشردن i

۱۰. برای لغو کردن اعمال هرگونه دستور در فایل = فشردن Esc

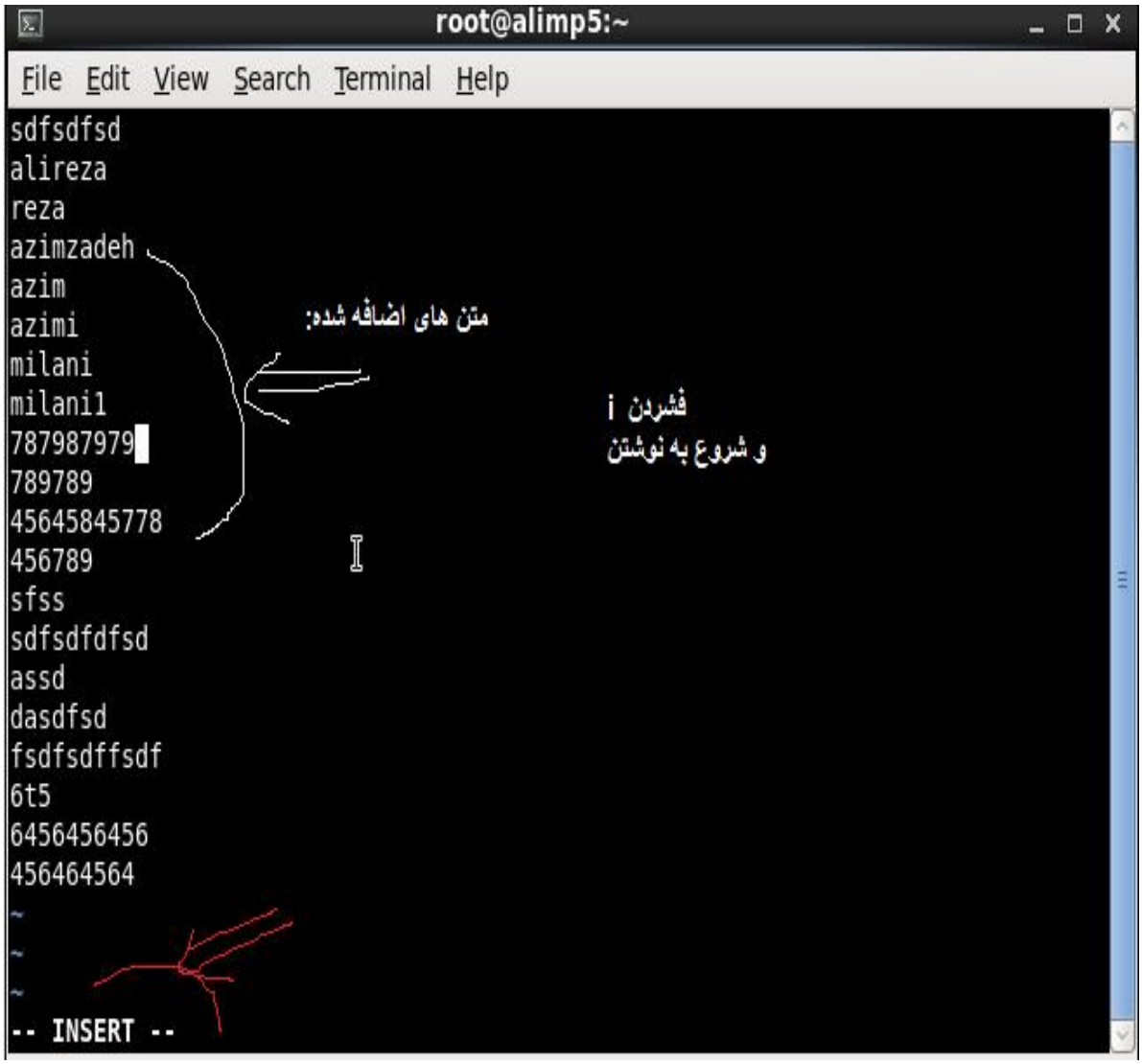
۱۱. درج هر متنی در فایل = فشردن p

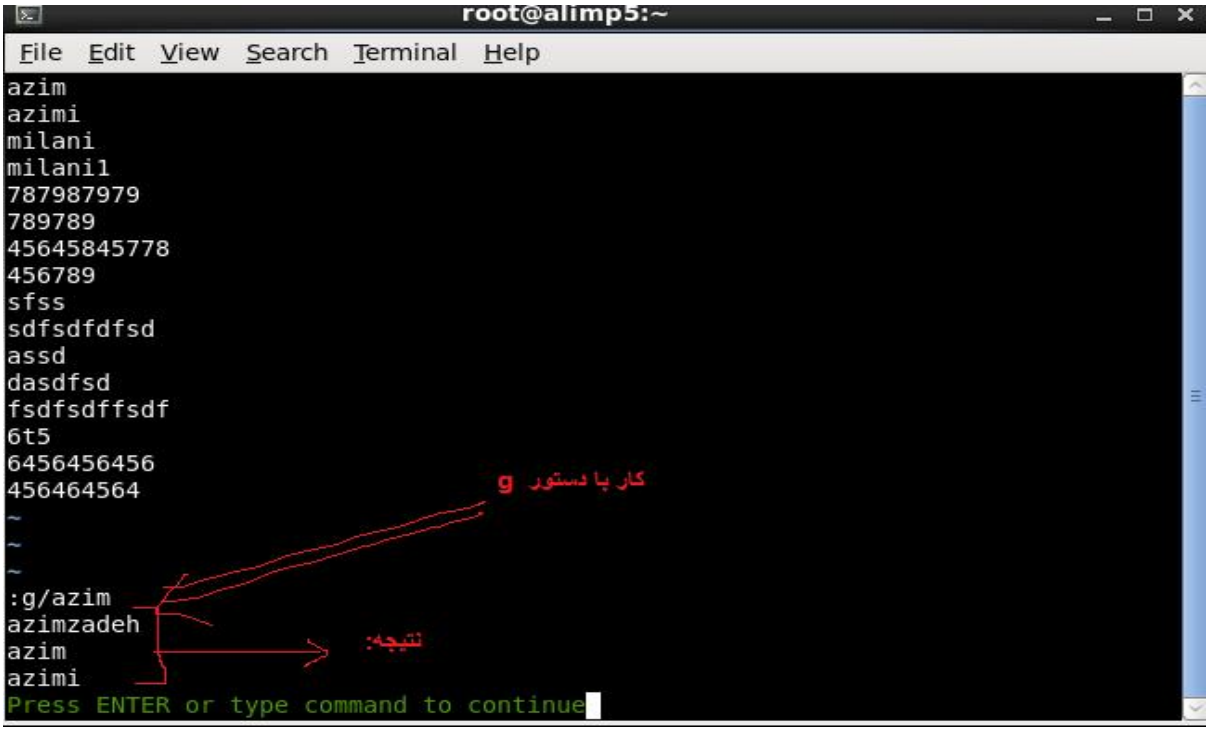
۱۲. برای رفتن به انتهای خط (جایی که مکان نما موس قرار دارد) = فشردن e

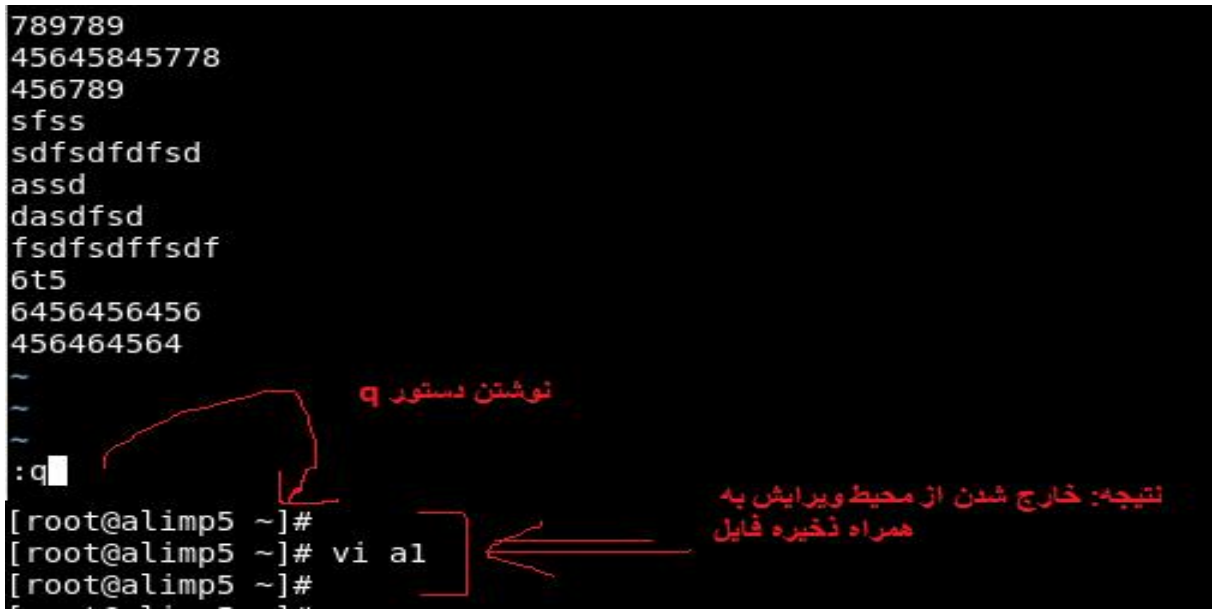
۱۳. برای رفتن به ابتدای خط (جایی که مکان نما موس قرار دارد) = فشردن b

۱۴. برای دیدن شماره خط متن ها = نوشتن set number:

مجموعه ای از مثال ها :







برای کسب اطلاعات بیشتر در مورد دستور vi می توانید به سایت های زیر مراجعه کنید:

https://www.washington.edu/computing/unix/vi.html

http://www.cs.rit.edu/~cslab/vi.html

http://forum.synology.com/wiki/index.php/Basic_commands_for_the_Linux_vi_Editor

http://www.cyberciti.biz/faq/vi-show-line-numbers/

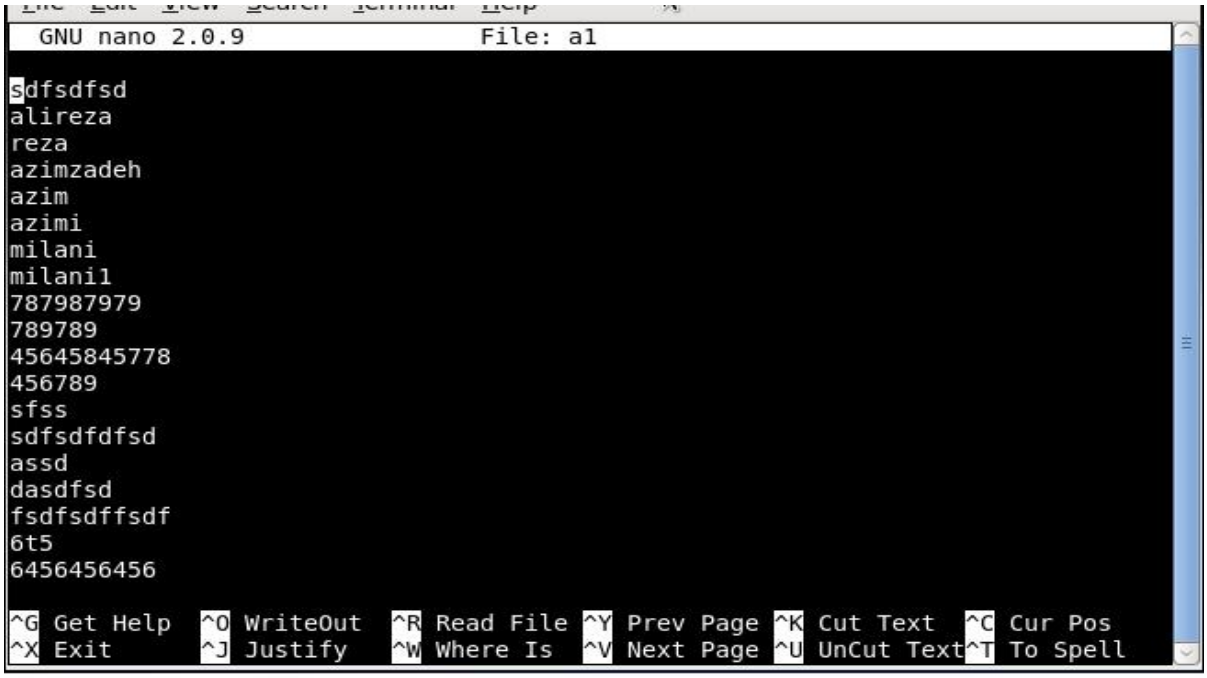
دستور **nano** :

بیشتر کارها توسط کلیدهای میانبر کیبورد انجام می شود.

برای ویرایش یا ساخت فایل متنی:

nano azimzadeh.txt

عکس از محیط این ابزار:



برای کسب اطلاعات بیشتر در مورد دستور **nano** می توانید به سایت های زیر مراجعه کنید:

https://www.linux.com/learn/tutorials/325049:linuxable -introduction-to-the-nano-text-editor

http://staffwww.fullcoll.edu/sedwards/Nano/IntroToNano.html

دستور **cat** :

برای دیدن محتویات یک فایل به کار می رود.

cat alimp5.txt

دستور **tail** و **head** :

tail = به صورت پیشفرض ۱۰ خط آخر فایل را نمایش می دهد.

یکی از پارامترهای کاربردی آن: **f-**

tail -f /var/log/messages

head = به صورت پیشفرض ۱۰ خط اول فایل را نمایش می دهد.

نکته: برای لغو این دستورات، ctrl+c کیبورد را بفشارید.

برای کسب اطلاعات بیشتر در مورد ابزارهای ویرایش متن می توانید عناوین زیر را گوگل جستجو کنید:

1- gedit : اگر در حال کار با محیط گرافیکی CentOS-Gnome هستید، این ویرایشگر بسیار مفید است.

2- kedit : اگر در حال کار با محیط گرافیکی CentOS-KDE هستید، این ویرایشگر بسیار مفید است.

مبانی ایجاد مجوز(دسترسی) به فایل ها:

در این قسمت خواهید آموخت که چگونه به فولدرها، فایل ها، دستگاه ها (device) دسترسی متناسب با نیازشان را بدهید.

۱) دستور chmod :

برای تغییر مجوز فایل ها یا فولدرها به کار می رود.

chmod 777 AzimZadeh.txt

chmod 654 FolderGame

```
[root@alimp5 ~]#
[root@alimp5 ~]# ls -l
total 120
-rw-r--r--. 1 root root   160 Feb  9 10:10 a1
-rw-r--r--. 1 root root   153 Feb  9 09:31 a2
-rw-------. 1 root root  2098 Feb  9 03:47 anaconda-ks.cfg
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Desktop
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Documents
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Downloads
-rw-r--r--. 1 root root 57217 Feb  9 03:47 install.log
-rw-r--r--. 1 root root 13715 Feb  9 03:43 install.log.syslog
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Music
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Pictures
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Public
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Templates
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Videos
[root@alimp5 ~]#
[root@alimp5 ~]# chmod 777 a1
[root@alimp5 ~]#
[root@alimp5 ~]# ls -l
total 120
-rwxrwxrwx. 1 root root   160 Feb  9 10:10 a1
-rw-r--r--. 1 root root   153 Feb  9 09:31 a2
-rw-------. 1 root root  2098 Feb  9 03:47 anaconda-ks.cfg
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Desktop
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Documents
drwxr-xr-x. 2 root root  4096 Feb  9 03:57 Downloads
```

۲) دستور chown :

برای تغییر مالک و گروهی از فایل ها و یا فولدرها استفاده می شود.

۳) دستورات ls –l : دیدن نوع دسترسی که در بخش های قبل توضیح داده ام (در بخش لیست کردن محتویات فولدرها):

ls -l

۴) دستور ll :

برای دیدن تغیرات ایجاد شده روی فایل یا فولدر مورد نظر استفاده می شود.

ll Alireza

شکل زیر مقادیری که با آن می توانید دسترسی ایجاد کنید را نشان می دهد:

Operation	Digit	Mnemonic	Description
Read	r	4	View file contents
Write	w	2	Write to or change
Execute	x	1	Run the file

برای درک بیشتر از دستورات بالا به مثال های زیر توجه کنید:

مثال۱: ابتدا به فولدر ali می رویم، سپس دو فایل با نام ali و Alireza می سازیم. و نوع کاربری و گروه آنها را عوض می کنیم.

ali را از مالک root پس می گیریم و آن را به مالک (یوزر) ali می دهیم، ولی هیچ تغییری در گروه آن ایجاد نمی کنیم (همان root باشد).

فایل alireza را در همان مالیکت root قرا می دهیم، ولی گروه آن را به alireza-group تغییر می دهیم.

نکته: عینا همان کاری است که در user and group policy در ویندوز انجام می دهید.

نتیجه:

```
[root@alimp5 ~]#
[root@alimp5 ~]# cd ali
[root@alimp5 ali]# touch ali alireza
[root@alimp5 ali]# ls -l
total 0
-rw-r--r--. 1 root root 0 Jan 19 04:20 ali
-rw-r--r--. 1 root root 0 Jan 19 04:20 alireza
[root@alimp5 ali]# chown ali ali
[root@alimp5 ali]# chown :alireza-group alireza
[root@alimp5 ali]# ls -l
total 0
-rw-r--r--. 1 ali  root          0 Jan 19 04:20 ali
-rw-r--r--. 1 root alireza-group 0 Jan 19 04:20 alireza
[root@alimp5 ali]#
```

در نهایت هم مجوز ۷۷۷ را به فایل alireza بدهید :

chmod 777 alireza

مدیریت یوزرها(حساب های کاربری) :

شما ممکن است به عنوان یک مدیر سرور، بخواهید به کارمندان خود اکانت هایی با دسترسی مختلف بدهید تا با این کار هم امنیت سرور را حفظ کرده باشید و هم از به وجود آمدن مشکلات احتمالی جلوگیری کنید.

نکته۱ : برای نمایش لیست کاربران و گروه ها می توانید از دستورات زیر استفاده کنید:

1. cut -d : -f 1 /etc/passwd
2. cat /etc/passwd | wc -l
3. cat /etc/passwd | cut -d":" -f1
4. cut -d : -f 1 /etc/group

نکته۲: برای نمایش کاربران لاگین شده به سیستم از دستور زیر استفاده کنید:

w

نتیجه:

```
[root@localhost ~]# w
 06:49:17 up 8 min,  2 users,  load average: 0.00, 0.22, 0.19
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     :0               06:42    8:23  15.62s 15.62s /usr/bin/Xorg :0 -nr -verbo
root     pts/0    :0.0             06:45    0.00s  0.02s  0.01s w
[root@localhost ~]#
```

Alireza Amimzadeh Ali-MP5

ایجاد حساب کاربری جدید (new user account):

برای این کار از دستور useradd و برای گذاشتن پسورد برای آن نیز از دستور passwd استفاده می کنیم.

نکته: می توانید از پارامتر c- برای اضافه کردن توضیح استفاده کنید.

useradd alimp5

یا

useradd alimp5 -c "this account is ROOT"

passwd alimp5

نکته: برای این که بدانید الان با چه نام کاربری وارد سیستم شده اید می توانید از دستور زیر استفاده کنید:

whoami

اضافه کردن کاربر به گروه :

وقتی استفاده می کنیم که شما می خواهید تعدادی دسترسی مثل هم را به چند کاربر بدهید، راحت ترین راه، ساخت یک گروه و عضو کردن دیگر یوزرها (کاربران) به این دسته می باشد: اسم گروه ما در اینجا sales می باشد.

G- برای گروه های ثانویه ما می باشد.

نکته: برای اضافه کردن آن به گروه اصلی باید از g- باید استفاده کنید.

useradd -G sales -m jerry

passwd jerry

مسیر یوزرهای تعریف شده به طور پیشفرض در فولدرhome می باشد.

برای تغییر مسیر می توانید بدین صورت عمل کنید:

vi/etc/default/useradd

مسیر فعلی: **HOME=/home**

مسیر مد نظر ما:

HOME=/iscsi/use

Useradd vivek

Passwd vivek

برای صحت از مسیر انتخاب شده از دستور زیر استفاده کنید:

Finger vivek

خروجی:

Login: vinek **Name: Vinek Gite**

Directory : /iscsi/user/vivek **shell:/bin/bash**

Last login Thu Sep 13 07:58 2007 (IST) on pts/1 from 10.16.15.2

No mail.

No Plan.

غیر فعال کردن یوزرها:

شما با دستور زیر می توانید کار کنید که پس از تاریخ مشخص شده، آن اکانت ساخته شده به کل غیر فعال شود:

useradd -e {yyyy-mm-dd} {username}

مثل:

useradd -e 2008-12-31 jerry

تعیین مدت زمان برای انقضای پسوردهای یوزرها:

useradd -f {days} {username}

مثل:

useradd -e 2009-12-31 -f 30 jerry

حذف یوزر:

از دستور زیر استفاده کنید:

userdel name-user

userdel alimp5

ساخت گروه جدید:

groupadd group-name

groupadd group-admin

حذف گروه:

grupdel group-name

grupdel group-admin

مسیر ذخیره اطلاعات یوزرها،گروه ها،پسوردها،، کجا می باشد؟

جواب: مسیر آنها در /etc/passwd و /etc/group و /etc/shadow می باشد.

مثلا در /etc/passwd اطلاعات هر کاربر بدین صورت نمایش داده می شود و هر خط بیانگر یک ویژگی از کاربر می باشد:

chivas:x:500:500::/home/chivas:/bin/bash

توضیح بخش های بالا از چپ به راست:

chivas: همان نام کاربری ما می باشد.

قسمت بعدی که همان حرف x است بیانگر پسورد ما است. اما پسوردی که در مسیر /etc/shadow ذخیره شده است.

نکته: اگر پسورد در مسیر /etc/passwd باشد، پسورد یوزر مربوطه به طور واضح قابل دیدن است (clear text).

۵۰۰: ۵۰۰ اول مربوط به UID یوزر می باشد.

۵۰۰: ۵۰۰ دوم مربروط به GID گروه می باشد.

قسمت پنجم: برای همان توضیح است که در بالا گفتم دستور مربوط به نوشتن کامنت را: c-

قسمت ششم: نمایانگر مسیر اطلاعاتی یوزر شما است که در آنجا قرار گرفته است.

قسمت آخر: بیانگر پوسته پیشفرض کاربر در ورود است.

مثلا در **/etc/group** اطلاعات مربوط به هر گروه ذخیره شده است و هر خط بیانگر یک ویژگی از گروه می باشد:

staff:x:502:anna,chivas

توضیح بخش های بالا از چپ به راست:

staff: همان نام گروه ما می باشد.

x: بیانگر پسورد گروه می باشد. مثل همان توضیح مثال بالا می باشد.

۵۰۲: نشان دهنده شماره گروه می باشد.

و بخش پایانی: نام یوزرهایی که در گروه عضو هستند را نمایش می دهد.

مثلا در **/etc/shadow** اطلاعات مربوط به پسوردهای یوزرها ذخیره می شود.

chivas:1XQLzic8C$5CQ9OMD/uBf.1HCouZQAa1:14281:0:99999:7: : :

توضیح بخش های بالا از چپ به راست:

chivas: بیانگر یوزر مورد نظر می باشد.

قسمت دوم(آبی رنگ): نشان دهنده پسورد کاربر می باشد و نوع رمزنگاری آن به طور پیشفرض **MD5** است.

نکته: اگر این ستون این علامت !! را داشت، یعنی اینکه کاربر نمی تواند وارد سیستم شود.

قسمت سوم: عدد ۱۴۲۸۱، بیانگر تاریخ آخرین باری که پسورد تغییر داده شده است می باشد. معنای عدد: ۱۴۲۸۱ روز پس از تاریخ ۱۹۷۰.

قسمت چهارم: عدد صفر به معنای عدم محدودیت روز در تغییر پسورد می باشد.

قسمت پنجم: مدت روزی که پسورد شما می تواند معتبر باشد را نشان می دهد.

قسمت ششم: به عنوان یک روز شمار است و وقتی به آن برسد، سیستم به شما هشدار می دهد.

قسمت هفتم: تعداد روزی که اکانت شما بعد از منقضی شدن آن در حالت غیر دسترس است را نشان می دهد.

لینک های کاربردی برای مطالعه دقیق تر در مورد مدیریت حساب های کاربری :

http://falearn.ir/?p=6

http://falearn.ir/?p=11

http://www.thegeekscope.com/linux-adduser-command-to-create-new-user/

http://www.yolinux.com/TUTORIALS/LinuxTutorialManagingGroups.html

دستورات پردازش متن:

شما وقتی بخواهید یک چیز خاصی را پیدا و مشاهده کنید بسیار عالی می باشد، حتما یاد بگیرید.

دستور grep :

برای نمایش خط ها و چیزهایی که با عنوان جستجو شما یکی است به کار می رود.

```
grep <pattern> <file>
```

پارامترهای دستور grep :

نکته: به صورت پیش فرض به متن جستجو شما حساس است.(حروف بزرگ و کوچک)

i- : برای غیرحساس کردن جستجو است.

v- : برای نمایش هرچیزی که با متن شما تطابق ندارد.

r- : برای جستجوی متن شما در یک فولدر به کار می رود.

مثال۱:

```
cd /etc/sysconfig
grep -i "iptables" iptables-config
```

مثال۲:

```
grep –r "passwd" /etc
```

یک مثال ترکیبی از دستورات grep و cat :

نکته: این خط عمود | به نشانه پایپ (pipe) است.

```
[juan@srv1-manila ~]$ cat /etc/passwd | grep "root"
```

نتیجه:

```
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
```

برای کسب اطلاعات بیشتر در مورد grep می توانید به سایت زیر مراجعه کنید:

http://www.cyberciti.biz/faq/howto-search-find-file-for-text-string/

دستورات کمکی:

۱. دستور **help--** :

برای دیدن جزییات یک دستور است.

cat --help

۲. دستور **apropos** :

برای دیدن دستورات به همراه توضیحی مختصر در مورد دستوراتی که تطابق با متن ما دارند:

apropos passwd

apropos cat

۳. دستور **man**:

همانند دستور بالایی عمل می کند:

man cat

۴. دستور **whatis** :

Whatis iptables

Whatis mkdir

لینک های کاربردی فصل دوم:

http://www.linux-commands-examples.com/

http://www.thegeekstuff.com/2010/11/5(-linux-commands/

http://www.tecmint.com/3 -practical-examples-of-linux-find-command/

http://www.if-not-true-thenm/2010-quickly-and-efficiently/

http://www.ee.surrey.ac.uk/Teaching/Unix/

http://www.tldp.org/LDP/gs/node5.html

http://community.linuxmint.com/tutorial/view/77

http://www-uxsup.csx.cam.ac.uk/pub/doc/suse/suse9.0/userguide-9.0/ch24s04.html

http://www.tecmint.com/1 -practical-examples-of-linux-grep-command/

http://www.tharunpkarun.com/2012/07/lis -of-basic-commands-in-centos-linux-server/


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش لینوکس مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
LINUX
FOUNDATION


شهریه دوره:
۱۱۰ هزار تومان
کلاس آموزش امنیت شبکه مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۷ روز


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش طراحی صفحات وب - مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد -
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
WEB

کار با CentOS

یکی از فصل های مهم می باشد که هیچ فرقی هم ندارد شما در حال کار با محیط گرافیکی (GUI) CentOS هستید یا اینکه با محیط دستوری آن (SSH or Command-line) کار می کنید، باید و حتما به عنوان یک کاربر لینوکس به دستورات و سرفصل های زیر تسلط لازمه را پیدا کنید تا در آینده کاری خودتان دچار مشکل نشوید.

دستورات کاربردی Kernel , init , RunLevels , chkconfig , service:

در این بخش در مورد کار با دستورات chkconfig و service و runlevel صحبت خواهیم کرد.

برای ایجاد محدودیت،مدیریت، فعال و غیر فعال کردن نرم افزارها، ابزارها و سرویس ها در یک سرور به کار می رود.

به شکل زیر نگاه کنید: (این اعداد بیانگر اولویت runlevel ها در مدیریت سرویس ها به کار می رود).

Table 3-2. Run Levels

Runlevel	Description
0	System shutdown
1	Single-user mode, no networking
2	Multi-user mode, no networking
3	Multi-user mode, text user interface, with networking
4	Reserved
5	Multi-user mode, graphical user interface, with networking
6	System reboot

cent os to persian BY: alimp5 azimZadeh

نکته: در مورد سرویس ها ، فقط با اعداد ۵/۳/۲/۱ خیلی کار داریم.

۱) دستور chkconfig:

دستوری که برای مشخص کردن سرویس ها و فعال کردن آن بعد از بالا آمدن سیستم (بوت شدن) می باشد.

سرویس های حیاتی ما در یک سرور apache, ssh , iptables ,cron و ... می باشد که باید فعال باشند.

پارامترها:

on : فعال کردن سرویس بعد از بوت شدن سیستم.

off : غیرفعال کردن سرویس بعد از بوت شدن سیستم.

برای حذف سرویس بعد از بوت شدن:

chkconfig --del [servicename]

۲) دستور service:

برای فعال،غیرفعال و ریست کردن (راه اندازی مجدد) سرویس ها به کار می رود.

پارامترها:

أ. start = برای فعال کردن سرویس استفاده می شود.

ب. stop = برای غیرفعال کردن سرویس استفاده می شود.

ج. status = برای متوجه شدن از اینکه آیا سرویس مربوطه در حال اجرا است یا خیر.

د. Restart = برای بارگذاری مجدد سرویس استفاده می شود.

کاربرد آن: زمانی که شما یک سری تغییر در کانفیگ های سرویس اعمال می کنید، باید آن را Restart کنید تا تنظیمات جدید اعمال شوند.

مثال۱: برای فعال کردن همیشگی سرویس ها بعد از بوت شدن سیستم:

```
service httpd start
chkconfig httpd on
```

یا

```
service httpd start
chkconfig --levels 235 httpd o
```

مثال۲: دیدن سرویس ها به همراه RunLevels مربوطه به آنها :

```
chkconfig –list | less
```

مثال۳: لیست کردن سرویس هایی که با اسم جستجویی شما تطابق دارند:

```
chkconfig --list | grep[servicename]
```

مثال۳: اضافه کردن سرویس هایی که در لیست سرویس ها نیستند :

```
chkconfig --add [servicename]
```

نکته۱: وقتی شما یک برنامه ای نصب می کنید، به صورت اتوماتیک به /etc/init.d اضافه می شود.

نکته۲: دستور cd /etc/init.d و سپس دستور: ls –la که اسم سرویس ها را نشان می دهد.

۳) دستور init :

برای تغییر دادن RunLevel ها به کار می رود.

init 0 = خاموش کردن سیستم.

init 6 = Restart کردن سیستم.

۴) دستور shutdown :

برای آوردن سیستم به وضعیت خاموش یا Restart کردن سیستم به کار می رود.

این دستور می تواند به نوعی از اهمیت بالایی برخوردار باشد، چرا؟ جواب : فرض کنید سرور شما قرار هست که ساعت ۱۲ شب شروع به آپدیت و کارهایی که شما برایش تعیین کرده اید بکند، شما یک زمانی را برایش تخمین زده اید دیگر؟ حالا اگر اینترنت دچار نوسان شد یکی از راه ها این است که این دستور را به اسکریپت خود اضافه کنید، تا بعد از زمانی مشخص، عمل خاموش کردن را برای شما انجام دهد.

پارامترهای دستور shutdown :

k- : فقط برای نمایش پیغام به کار می رود.

r- : برای Restart کردن.

n- : نابود کردن تمام پروسه ها (پیشنهاد نمی شود).

t- : ایجاد تاخیر برای Restart یا خاموش کردن سیستم.

مثال۱: برای خاموش کردن سیستم:

shutdown -h now یا init 0

مثال۲: برای Restart کردن سیستم:

shutdown -r now یا reboot

مثال۳: خاموش کردن سیستم بعد از ۲دقیقه:

shutdown -h 120

نکته: بعضی ورژن ها به ثانیه است، و بعضی دیگر به دقیقه.

نکته: برای قطع کردن انجام این عمل ، روی کیبورد ctrl+c را فشار دهید.

مانیتورینگ عملکرد سیستم:

در اینجا خواهید آموخت که چگونه از وضیعت حافظه و میزان حافظه ، cpu و .... که توسط سرویس ها اشغال شده است آگاهی پیدا کنید.

نکته: این قسمت در بحث troubleshooting برای شما عزیزان بسیار کاربردی خواهد بود.

۱. دستور free :

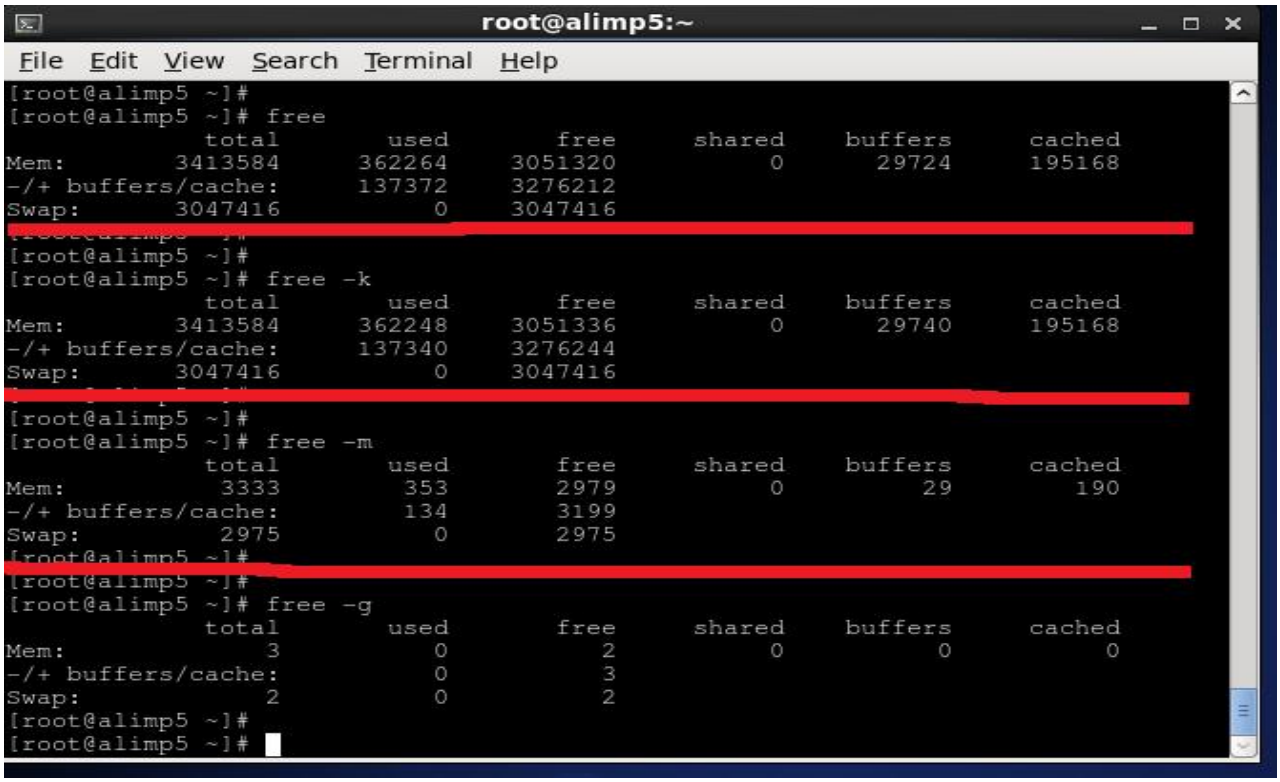
برای نمایش حافظه با جزییات دقیق به کار می رود.

برای آشنایی با جزییات دستور:

free --help

نکته۱: m- نمایش مقدار رم بر اساس مگابایت.

نکته۲: g- نمایش مقدار رم بر اساس گیگابایت.



نکته: برای آزاد کردن حافظه رم خود، باید حافظه کشی (cache) که از رم شما برداشته است را با دستور زیر پاک کنید:

sync

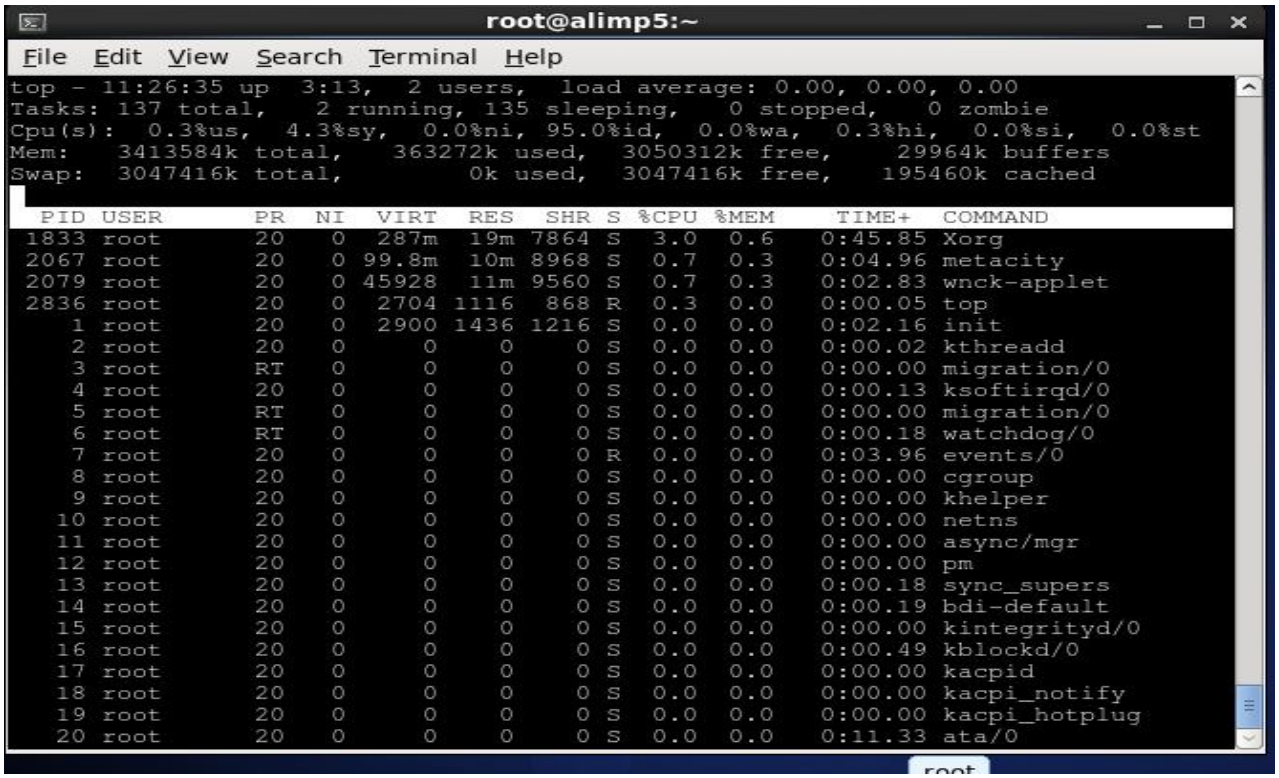
echo 3 > /proc/sys/vm/drop_caches

free

۲. دستور top :

برای نمایش اطلاعات دقیق به صورت real-time و داینامیک (پویا) که چه یوزری، چه چیزی، چقدر حافظه،چقدر پردازنده و ....

را اشغال کرده است نمایش می دهد.



۳. دستور ps :

برای نمایش پروسه های در حال اجرا است.

ps u

ps aux | grep ssh

۴. دستور kill :

برای از بین بردن پروسه است و بر اساس PID کار می کند.

نکته: از 9- برای بالا بردن اولویت در از حذف استفاده می شود.

مثال: در شکل زیر می بینید که در حال کار با bash ها هستیم، دستور kill بدون پارامتر 9- جواب نداده است.

kill 3297

kill 3206

حذف یکی از bash ها:

kill -9 3206

```
[root@localhost ~]# ps u
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      2358  0.0  0.0   2008   480 tty2     Ss+  02:13   0:00 /sbin/minge
root      2360  0.0  0.0   2008   480 tty3     Ss+  02:13   0:00 /sbin/minge
root      2362  0.0  0.0   2008   480 tty4     Ss+  02:13   0:00 /sbin/minge
root      2369  0.0  0.0   2008   484 tty5     Ss+  02:13   0:00 /sbin/minge
root      2373  0.0  0.0   2008   484 tty6     Ss+  02:13   0:00 /sbin/minge
root      2383  1.4  2.2  36364 23068 tty1     Ss+  02:13   0:27 /usr/bin/Xo
root      3206  0.0  0.1   5260  1704 pts/0    Ss   02:44   0:00 bash
root      3297  0.0  0.1   5260  1636 pts/1    Ss+  02:45   0:00 bash
root      3309  0.0  0.1   4932  1052 pts/0    R+   02:45   0:00 ps u
[root@localhost ~]# kill 3297
[root@localhost ~]# kill 3206
[root@localhost ~]# kill -9 3206
```

```
root@localhost:~
File  Edit  View  Search  Terminal  Help
root@localhost ~]#
```

۵. دستور pidstat :

اطلاعات زیر را برای شما نمایش می دهد:

نکته: اگر سرویس خاصی را مد نظر دارید می توانید از دستور زیر استفاده کنید:

pidof sshd

pidof httpd

```
[root@localhost ~]# pidstat
Linux 2.6.32-358.el6.i686 (localhost.localdomain)       01/27/2014      _i686_  (1 CPU)

02:51:54 AM       PID    %usr %system  %guest    %CPU   CPU  Command
02:51:54 AM         1    0.00    0.07    0.00    0.07     0  init
02:51:54 AM         4    0.00    0.00    0.00    0.00     0  ksoftirqd/0
02:51:54 AM         6    0.00    0.00    0.00    0.00     0  watchdog/0
02:51:54 AM         7    0.00    0.01    0.00    0.01     0  events/0
02:51:54 AM        13    0.00    0.00    0.00    0.00     0  sync_supers
02:51:54 AM        16    0.00    0.01    0.00    0.01     0  kblockd/0
02:51:54 AM        20    0.00    0.02    0.00    0.02     0  ata/0
02:51:54 AM        28    0.00    0.00    0.00    0.00     0  kswapd0
02:51:54 AM       283    0.00    0.00    0.00    0.00     0  scsi_eh_0
02:51:54 AM       286    0.00    0.01    0.00    0.01     0  scsi_eh_1
02:51:54 AM       293    0.00    0.00    0.00    0.00     0  mpt_poll_0
```

اجرای اسکریپت و دستورات به صورت اتوماتیک با cron و at :

برنامه cron، مثل scheduler (زمانبند) در ویندوز می باشد. و شما که قرار نیست و نمی توانید همیشه پشت سیستم یا سرور باشید، پس باید کاری کنید که در زمانی که مد نظر دارید کارهای نصب و آپدیت و ... به طور خودکار انجام شوند.

پارامترهای دستور cron :

e- : برای ساخت یا ویرایش.

l- : لیست cronهای فعلی.

r- : برای حذف cron خاص.

v- : نمایش آخرین باری که شما اقدام به ویرایش cron کرده اید.

مثال: دیدن cron های مربوط به یک یوزر خاص:

crontab -u username -l

crontab -u alimp5 -l

فرمت کلی نوشتن در این دستور دارای ۵ قسمت می باشد.

minute hour day-of-month month day-of-week week function-to-be-performed

View the /etc/crontab file to understand its syntax:

```
# grep ^# /etc/crontab
# For details see man 4 crontabs
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,etc.
# |  |  |  |  |
# *  *  *  *  *  command to be executed
```

برای شروع کار باید دستور زیر را بنویسید:

crontab -e

که برای شما یک صفحه خالی ایجاد می کند.

مسیر ذخیره فایل های ایجاد شده توسط cron:

مثل شکل زیر:

مسیرهای دیگر cron:

/var/spool/cron/

/var/log/cron

/tmp

مثال۱: اجرای اسکریپت زیر در ساعت ۲۳و ۳۰دقیقه PM هر روز:

30 23 * * * /root/memcache.sh

مثال۲:اجرای اسکریپت زیر در هر جمعه و در ساعت ۲۳ و ۳۰دقیقه :

30 23 * * 5 /root/memcache.sh

مثال۳: پاک کردن کش (cache) حافظه رم در ساعت۲۳ و ۳۰دقیقه هر روز:

vi /root/clean.sh

#!/bin/sh

sync; echo 3 > /proc/sys/vm/drop_caches

30 23 * * * /root/clean.sh

مثال ۴: اجرای اسکریپت php. زیر، از دوشنبه تا جمعه هر هفته، راس ساعت 8PM :

0 20 * * 1-5 /root/script.php

مثال۵ : نوشتن "تاریخ و زمان" به همراه کلمه "hello world" ، در هر ۱۵ دقیقه، در داخل فایل alimp5.txt :

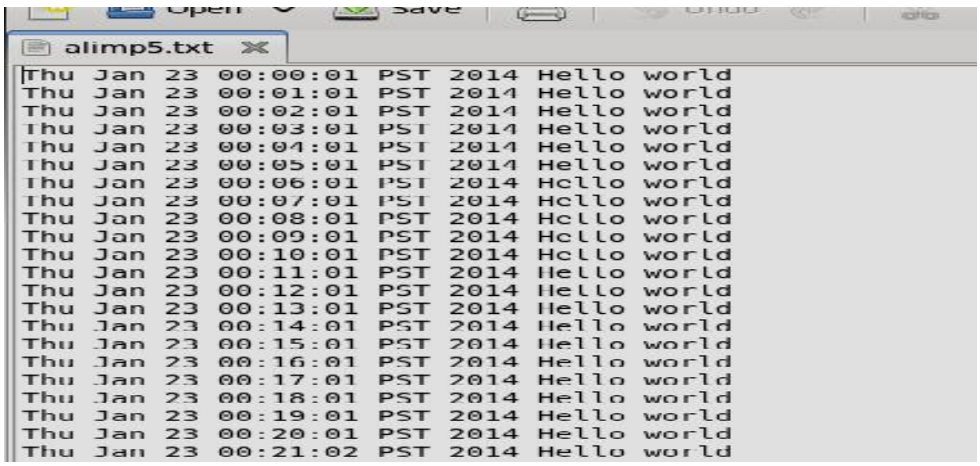
***/15 * * * * echo `date` "Hello world" >>$HOME/alimp5.txt**

نکته۱: فایل alimp5.txt در root قرار دارد.

نکته۲: */15 به معنای انجام عمل در هر ۱۵ دقیقه می باشد.

نتیجه:

crontab: installing new crontab



نکته مهم: همیشه بعد از نوشتن هر cron باید دستور زیر را هم بنویسیم :

```
service crond restart
```

و در نهایت:

```
chkconfig crond on
```

مثال۶ : نمایش پیغام زیر برای کاربر root در هر ۱ دقیقه:

```
nano /tmp/sample_script
```

نوشتن ۳ خط زیر:

```
#!/bin/bash
# Send a msg to all users on the console
wall “Hello World”
```

اجرای دستور:

```
crontab -u root -e
```

نوشتن خط زیر در صفحه باز شده:

```
* * * * * /tmp/sample_script
```

مثال۷: پاک کردن Cache موجود در RAM، در هر ۲ دقیقه برای افزایش سرعت:

```
vi /root/clear-cache-ram.sh
sync; echo 3 > /proc/sys/vm/drop_caches
```

سپس ذخیره و خروج از فایل.

```
chmod +x clear-cache-ram.sh
```

سپس:

```
crontab -e
*2/ * * * * /root/clear-cache-ram.sh
```

برای اطمینان:

```
crontab -l
```

برای کسب اطلاعات بیشتر در مورد crontab می توانید به سایت های زیر مراجعه کنید:

http://en.wikipedia.org/wiki/Cron

http://pubs.opengroup.org/onlinepubs/9699919799/utilities/ crontab.htı

ابزار at :

این ابزار همانند cron کار می کند، فقط کمی از نظر دستورات و اجرا تفاوت دارد. امتحان این ابزار خالی از لطف نیست.

پارامترها:

l- : نمایش تمام زمان بندی ها بر اساس ID .

m- : ارسال ایمیل به آدرس مورد نظر پس از انجام شدن کارها.

f- : خواندن فایل ها از ورودی برای انجام زمانبندی.

مثل: مسیردهی یک اسکریپت برای اجرا شدن در زمانی خاص.

d- : حذف یک زمانبند از لیست at ، بر اساس ID .

نکته مهم: برای اجرا شدن از ctrl+d کیبورد استفاده کنید.

مثال۱: اجرای اسکریپت زیر در ساعت ۵:۵۰ am :

```
at -f /root/Desktop/ali.txt 5:50am
```

at -l یا atq

مثال۲: حذف یک زمانبند با ID=9 :

```
at -d 9
```

ارسال گزارشات به ایمیل با Mutt و Mailx :

یکی دیگر از مفیدترین ابزارهایی که می توانم بگویم از کارایی بسیار برخوردار است ابزار mailx می باشد که به طور پیشفرض بر روی سیستم شما نصب نیست و شما باید آن را نصب کنید و یک سری تنظیمات را انجام برای راه اندازی آن انجام دهید:

۱) نصب ابزار:

```
yum install mailx
```

۲) برای تست از دستور زیر استفاده کنید:

نکته: در اینجا ما در بالاترین سطح دسترسی(root) هستیم.

```
echo "Test Email" | mail -s "This is a test email." externalemail@ domain.com
```

مثل:

```
echo "Test Email" | mail -s "This is a test email." alimp5@irsecteam.org
```

۳) به میسر زیر بروید (فایل را برای ویرایش باز کنید):

vi /etc/aliases

۴) ۲خط زیر را پیدا کرده:

 # Person who should get root's mail

#root: marc

۵) آن را به ایمیل موردنظر خودتان تغییر دهید:

۶) سپس دستور زیر را برای ذخیره تغییرات و بازسازی مجدد دیتابیس در ترمینال وارد کنید:

newaliases

۷) تست دستور:

echo "Test Email" | mail -s "This is a test email" root

نکته: با دستور **mailq** هم می توانید لیست پیغام هایی که در صف فرستاده شدن برای ایمیل موردنظر خودتان که قبلاً تعیین کرده اید ببینید:

mailq

نتیجه:

Mail queue is empty

یا اگر صفی وجود داشته باشد بدین صورت است:

```
[root@localhost ~]#
[root@localhost ~]# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
1234481657*     616 Thu Jan 23 05:43:41  root@localhost.localdomain
                                         ali_parkour68@yahoo.com

5A7C481655*    3066 Thu Jan 23 05:43:46  MAILER-DAEMON
                                         ali_parkour68@yahoo.com

-- 4 Kbytes in 2 Requests.
[root@localhost ~]#
```

ابزار **Mutt** :

به صورت خط-فرمان است و از پروتکل های **POP** و **IMAP** نیز پشتیبانی می کند.

برای کسب اطلاعات بیشتر در مورد کار با ابزار **Mutt** می توانید به سایت های زیر مراجعه کنید :

http://www.mutt.org/

http://www.mutt.org/doc/manual/manual-6.html

http://www.tecmint.com/send-mail-from-command-line-using-mutt-command/

http://www.cyberciti.biz/tips/sending-mail-with-attachment.html

همگام سازی فایل ها و فولدرها با rsync :

یکی از مهمترین ابزارهایی که یک مدیر سرور به آن نیاز دارد، اجرای خودکار دستورات از راه دور، کپی، جایگزینی، گرفتن پشتیبان از فایل ها و .... و کارهایی از این قبیل می باشد.

طبق مراحل زیر برای فعال سازی این ابزار اقدام کنید:

۱. نصب ابزار **rsync** :

```
yum install rsync
```

۲. ساخت فولدری برای گرفتن پشتیبان از فایل ها:

```
mkdir /home/backup
```

نکته: مسیر را می توانید به دلخواه خود تعیین کنید و یا اینکه برای هر چیزی که مد نظر دارید یک زیرشاخه در مسیر خودتان بسازید.

مثل: /home/backup/doc /home/backup/video /home/backup/image

پارامترهای دستور rsync :

v- : برای نمایش عملیات انجام شده استفاده می شود.

r- : برای انتقال اطلاعات بدون اینکه دسترسی ها و برچسب (timestamp) آنها را حفظ کند، استفاده می شود.

a- : دقیقا عکس پارامتر r- عمل می کند و همه چیز را در حین انتقال حفظ می کند.

z- : برای فشرده سازی اطلاعات فایل استفاده می شود.

h- : خروجی را طوری نمایش می دهد که انسان قادر به خواندن و درک آن باشد.

progress-- : نمایش میزان درصد کارهای انجام شده در حین عمل کپی و انتقال فایل ها.

delete-- : برای حذف فایل ها استفاده می شود.

ابزار diff :

برای مقایسه فایل های بین مبدا و مقصد استفاده می شود. یعنی شما با این دستور می توانید مطمئن شوید که آیا تمام فایل یا فولدر ارسال شده کامل کپی شده است یا خیر!

diff /path/to/source/files/ /home/backup/

مثال:

diff /root/alimp5 /home/backups

مثال۱: کپی یک فایل فشرده شده به مسیر پشتیبان ها:

```
[root@tecmint]# rsync -zvh backup.tar /tmp/backups/

created directory /tmp/backups

backup.tar

sent 14.71M bytes  received 31 bytes  3.27M bytes/sec

total size is 16.18M  speedup is 1.10
```

مثال۲: کپی یک فولدر به مسیر پشتیبان ها و فشرده سازی فایل ها در مسیر پشتیبان ها:

```
[root@tecmint]# rsync -avzh /root/rpmpkgs /tmp/backups/
sending incremental file list
rpmpkgs/
rpmpkgs/httpd-2.2.3-82.el5.centos.i386.rpm
rpmpkgs/mod_ssl-2.2.3-82.el5.centos.i386.rpm
rpmpkgs/nagios-3.5.0.tar.gz
rpmpkgs/nagios-plugins-1.4.16.tar.gz
sent 4.99M bytes  received 92 bytes  3.33M bytes/sec
total size is 4.99M  speedup is 1.00
```

مثال۳: کپی یک فولدر از یک سرور محلی و انتقال آن به یک سرور خارجی:

```
[root@tecmint]$ rsync -avz rpmpkgs/ root@192.168.0.101:/home/
root@192.168.0.101's password:
sending incremental file list
./
httpd-2.2.3-82.el5.centos.i386.rpm
mod_ssl-2.2.3-82.el5.centos.i386.rpm
nagios-3.5.0.tar.gz
nagios-plugins-1.4.16.tar.gz
sent 4993369 bytes  received 91 bytes  399476.80 bytes/sec
total size is 4991313  speedup is 1.00
```

مثال ۴: کپی یک فولدر از یک سرور خارجی و انتقال آن به یک سرور محلی در مسیر پشتیبان ها:

```
[root@tecmint]# rsync -avzh root@192.168.0.100:/home/tarunika/rpmpkgs /tmp/my

root@192.168.0.100's password:

receiving incremental file list

created directory /tmp/myrpms

rpmpkgs/

rpmpkgs/httpd-2.2.3-82.el5.centos.i386.rpm

rpmpkgs/mod_ssl-2.2.3-82.el5.centos.i386.rpm

rpmpkgs/nagios-3.5.0.tar.gz

rpmpkgs/nagios-plugins-1.4.16.tar.gz

sent 91 bytes  received 4.99M bytes  322.16K bytes/sec

total size is 4.99M  speedup is 1.00
```

مثال ۵: اگر یک فایل یا یک فولدر در مبدأ وجود نداشته باشد، اما در مقصد از آن داشته باشیم و شما بخواهید آنها را برای همگام سازی حذف کنید بدین صورت می باشد:

یعنی: فایل های مقصد را که در مبدا وجود نداشته اند، حذف می کند.

```
[root@tecmint]# touch test.txt
[root@tecmint]# rsync -avz --delete root@192.168.0.100:/var/lib/rpm/ .
Password:
receiving file list ... done
deleting test.txt
./
sent 26 bytes  received 390 bytes  48.94 bytes/sec
total size is 45305958  speedup is 108908.55
```

```
[root@localhost ~]# rsync -avzh --delete ali/  /home/alimp5/
sending incremental file list
./
deleting .mozilla/plugins/
deleting .mozilla/extensions/
deleting .mozilla/
deleting .gnome2/
deleting alimp5.txt
deleting .bashrc
deleting .bash_profile
deleting .bash_logout
ali
reza/
reza/azimzadeh/

sent 139 bytes  received 42 bytes  362.00 bytes/sec
total size is 0  speedup is 0.00
[root@localhost ~]#
```

مثال ۶: اگر شما می خواهید فایل های خودتان را از سرور به USB کپی کنید و نمی خواهید شامل فایل هایی با پسوند ISO. باشد، بدین طور باید بنویسید:

```
rsync --delete -avz --exclude="*.iso" /path/to/source/ /path/to/external/ disk/
```

یک مثال کامل: در اینجا ما می خواهیم یک اسکریپتی با ابزار Mutt بنویسیم و محتویات مسیرهای زیر را به صورت خودکار در زمان های مشخص به ایمیل شما ارسال کند:

۱. ساخت یک فولدر:

```
mkdir /root/bin/
```

۲. ایجاد یک فایل برای نوشتن اسکریپت:

```
vi /root/bin/mymuttscript.sh
```

۳. وارد کردن خط های زیر و تغییرات لازم:

```
#!/bin/sh
echo " Here is a log summary report sent by Mutt." | mutt -s "Log
  summary report" youremail@domain.com -a /var/log/messages -a /var/log/maillog -a /var/log/cron
```

۴. دادن دسترسی لازم برای اجرا شدن اسکریپت:

```
chmod a+x /root/bin/mymuttscript.sh
```

۵. ایجاد یک cron:

```
crontab –e
```

۶. قرار دادن متن زیر:

```
00 22 * * * /root/bin/mymuttscript.s
```

نتیجه:

```
crontab: installing new crontab
```

۷. راه اندازی مجدد (ریست) سرویس cron :

service crond restart

برای کسب اطلاعات بیشتر در مورد ابزار rsync می توانید به سایت های زیر مراجعه کنید:

http://www.cyberciti.biz/tips/linux-use-rsync-transfer-mirror-files-directories.html

http://www.evbackup.com/support-commonly-used-rsync-arguments/

http://www.cyberciti.biz/tips/linux-use-rsync-transfer-mirror-files-directories.html

http://www.computerhope.com/unix/rsync.htm

http://www.tecmint.com/rsync-local-remote-file-synchronization-commands/

http://linuxcommand.org/man_pages/rsync1.htn

لینک های کاربردی فصل سوم:

http://www.tecmint.com/useful-linux-commands-for-system-administrators/

http://www.thegeekstuff.com/2011/06/chkconfi -examples/

http://www.tecmint.com/chkconfig-command-examples/

http://www.rpm-based.org/how-to-manage-services-with-chkconfig-and-service

http://www.thegeekstuff.com/2009/06/1! -practical-crontab-examples/

http://www.adminschoice.com/crontab-quick-reference/

http://v1.corenominal.org/howt -setup-a-crontab-file/

http://content.hccfl.edu/pollock/unix/atdemo.htm

http://www.thegeekstuff.com/2010/06/a -atq-atrm-batch-command-examples/

http://pcsupport.about.com/od/commandlinereference/p/at-command.htm

http://www.computerhope.com/unix/umailx.htm

http://www.folkstalk.com/2012/08/ma -command-examples-in-unix-linux.html

http://www.binarytides.com/linux-mail-command-examples/

http://www.thegeekstuff.com/2010/09/rsyn -command-examples/

http://www.tecmint.com/rsync-local-remote-file-synchronization-commands/

http://www.cyberciti.biz/tips/linux-use-rsync-transfer-mirror-files-directories.html

https://calomel.org/rsync_tips.html

http://www.liquidweb.com/kb/usinize-loce-systems/

http://www.evbackup.com/support-commonly-used-rsync-arguments/

http://www.computerhope.com/unix/rsync.htm


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش لینوکس مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
LINUX
FOUNDATION


شهریه دوره:
۱۱۰ هزار تومان
کلاس آموزش امنیت شبکه مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۷ روز


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش طراحی صفحات وب - مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد -
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
WEB

مدیریت ذخیره سازی داده ها

در این فصل در مورد ساخت پارتیشن ها، دیسک ها، مدیریت آنها و ایجاد محدودیت برای کاربران در حین استفاده از سرور صحبت خواهیم کرد.

اخطار: اگر برای اولین بار می خواهید اقدام به تغییراتی در هارد دیسک خود کنید، حتماً دستورات این فصل را در داخل ماشین های مجازی **Vmware** یا **Virtual-Box** تست کنید تا به اطلاعات هارد دیسک شما آسیبی وارد نشود.

پیشنهاد: اگر با ماشین مجازی در حال تست دستورات این فصل هستید، یک **SnapShot** از ماشین مجازی خود بگیرید، این کار باعث سهولت در کار شما می شود.

در این بخش به تکنولوژی های **RAID(Redundant Anyway)** و **LVM(Logical Volume Manager)** اشاره خواهیم کرد.

مدیریت هارد دیسک:

با استفاده از دستور زیر برای نمایش جزییات دقیق فضاها و پارتیشن ها و... می توانید مطلع شوید.

```
df --help
```

با اجرای دستورات زیر کاملا متوجه می شوید:

```
df
df -h
df -T -H
df -H
df /root -h
df -h /root
df -h /home
```

```
Filesystem                  Size   Used  Avail Use% Mounted on
/dev/md0                    127G   1.9G   119G   2% /
tmpfs                       1.1G      0   1.1G   0% /lib/init/rw
udev                        1.1G   267k   1.1G   1% /dev
tmpfs                       1.1G      0   1.1G   0% /dev/shm
/dev/md2                    1.6T   706G   800G  47% /data
/dev/mapper/cryptvg-mybackup
                            635G    83G   520G  14% /securebackup
root@nas01:~#
```

نکته: از دستور زیر برای مشاهده حجم کل هارد دیسک می توانید استفاده کنید:

dmesg | grep blocks

دستور **fdisk** :

برای دیدن جزییات دقیق هارد دیسک شما به کار می رود.

[root@server1 ~]# fdisk -l

نکته: می توانید از **parted -l** نیز استفاده کنید.

Listing 4-1. Listing Details of the Hard Disks

```
[root@server1 ~]# fdisk -l

Disk /dev/hda: 8388 MB, 8388108288 bytes
255 heads, 63 sectors/track, 1019 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1   *           1          13      104391   83  Linux
/dev/hda2              14        1019     8080695   8e  Linux LVM

Disk /dev/hdb: 10.4 GB, 10485522432 bytes
16 heads, 63 sectors/track, 20317 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

   Device Boot      Start         End      Blocks   Id  System
 [root@server1 ~]#
```

برای کسب اطلاعات بیشتر به سایت زیر مراجعه کنید:

http://en.wikipedia.org/wiki/Hard_disk_partition

۲ دستور مهم بخش مدیریت هارد دیسک : **fdisk** و **parted**

می خواهم با یک مثال برای شما عزیزان توضیح دهم.

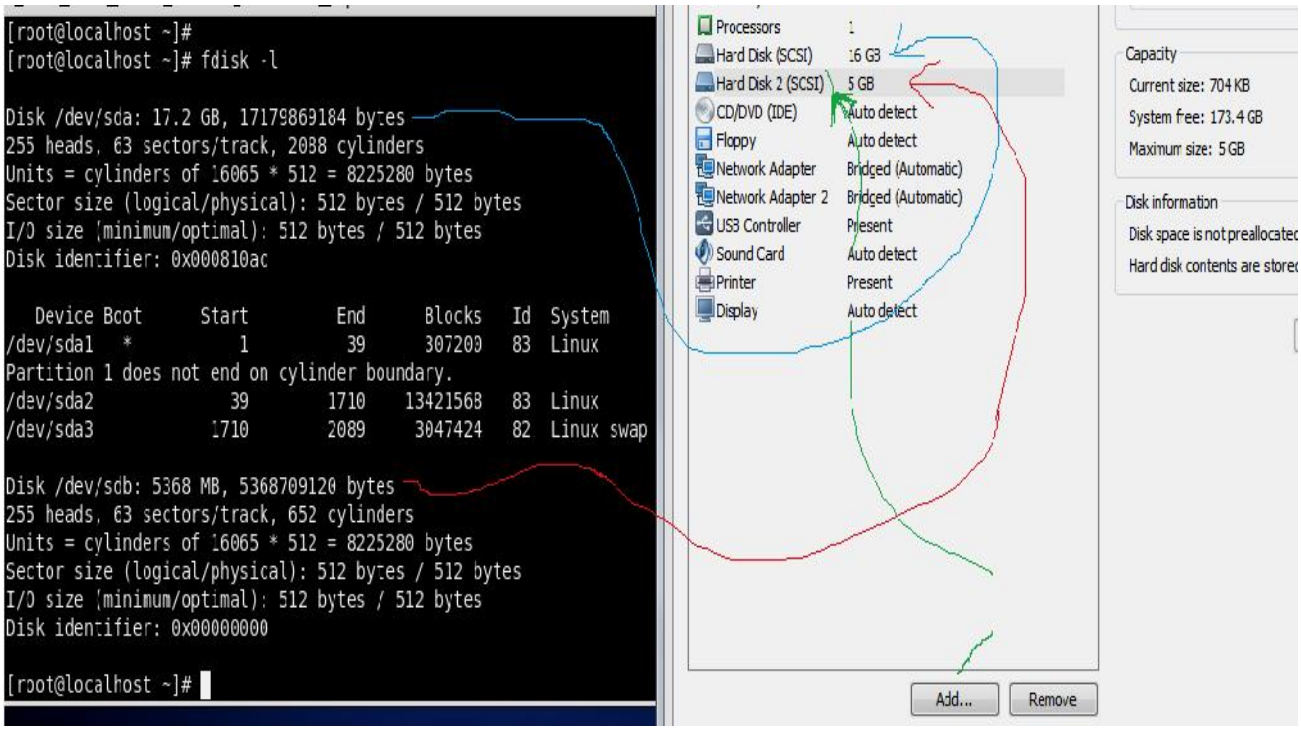
پیشنهاد: سعی کنید برای کار کردن با این ابزارها ابتدا بار علمی لازم را به دست آورید و سپس اقدام به تغییر دادن پارتیشن کنید، چون ممکن است به سیستم خودتان آسیب وارد کنید و اطلاعات مهم را از دست دهید.

مثال ۱: ممکن است شما بخواهید یک درایو ویژه برای نگهداری کش داده های خودتان استفاده کنید. پس برای این کار باید یک درایو از روی هاردتان بسازید. به دستورات زیر کامل توجه کنید:

طبق شکل بالا، ما یک دیسک **/dev/hdb** داریم، که سایزآن **10GB** است.

نکته ۱: **hd** برای دیسک های **IDE** و **sd** برای دیسک های **SCSI** می باشد.

نکته۲: به ماشین مجازی خود به تعداد دلخواه می توانید هارد دیسک جدید اضافه کنید و دستورات را بر روی دیسک ها تست نمایید:



ساخت یک پارتیشن جدید:

۱) در ابتدا دستور زیر را می نویسیم:

fdisk /dev/hdb

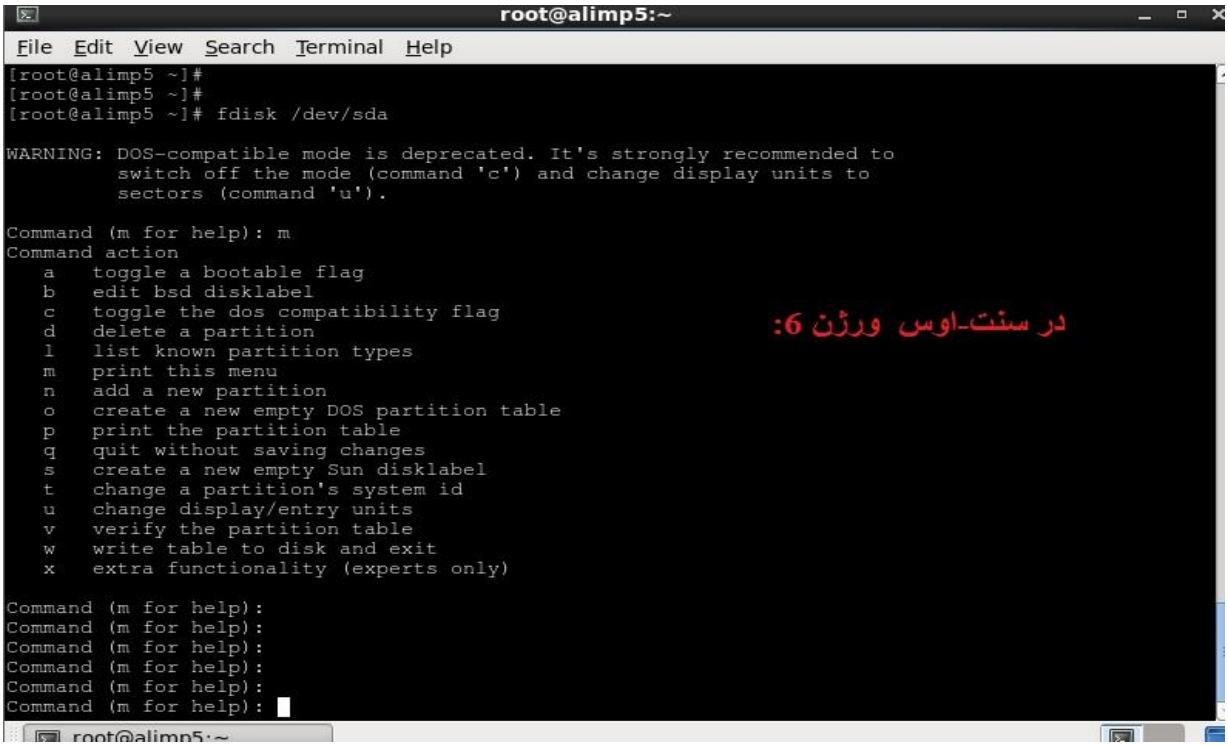
```
[root@server1 ~]# fdisk /dev/hdb
The number of cylinders for this disk is set to 20317.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help)
```

azimzadeh
ali-mp5

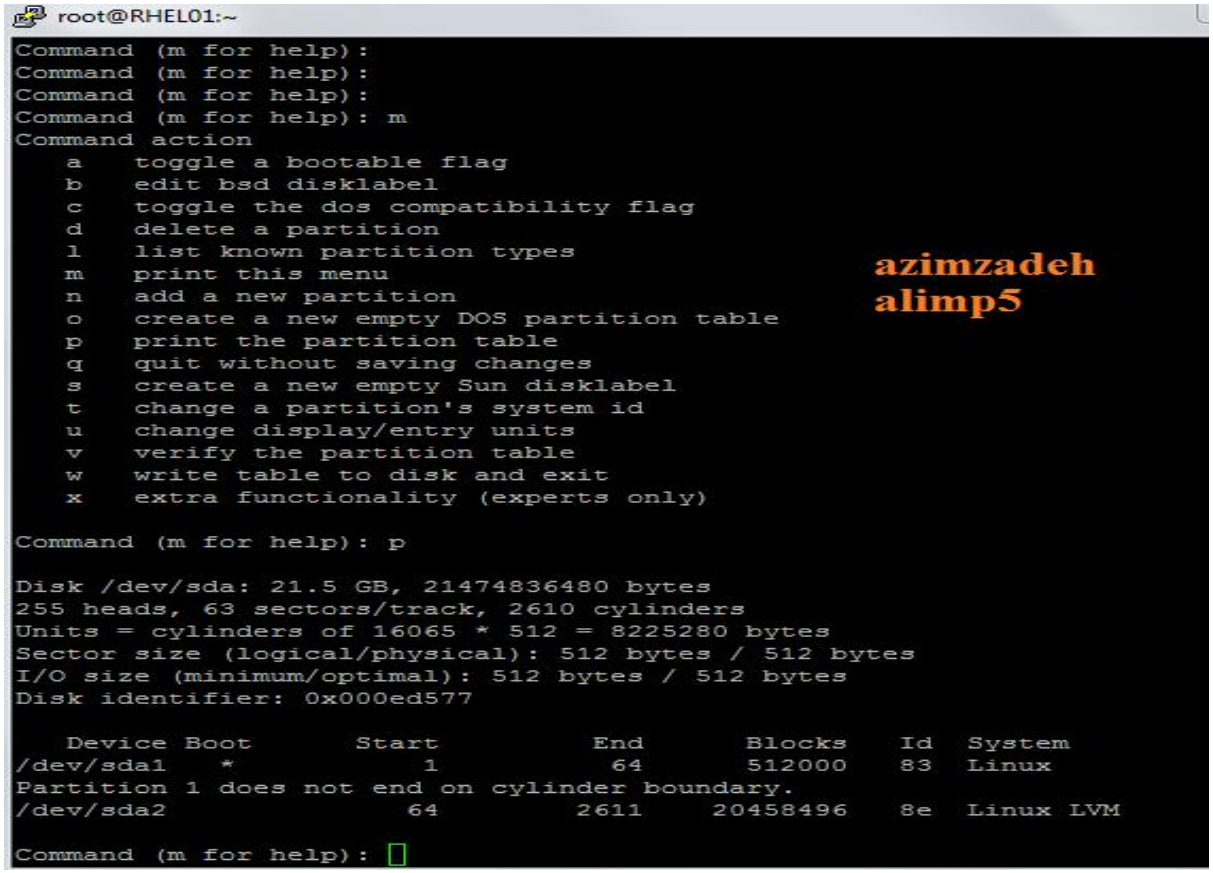
Follow these steps to create a new partition (see Listing 4-3 as a guide):

1. Type **n**, and press Enter.
2. Specify that you will create primary partition by typing **p** and pressing Enter.
3. At the Partition number prompt, type **1**, and press Enter.
4. Press Enter to start the partition on the first cylinder of the hard disk.
5. On the last cylinder prompt, press Enter again so that this partition uses all of the available space on this disk.
6. Type **p**, and press Enter to have a preview of the partition table. Finally, type **w**, and press Enter to write your changes into the hard disk.



۲) طبق توضیحات عمل کنید:

ابتدا m را نوشته و enter را فشار دهید. طبق شکل بالا، باید جلوی حرف p، عبارت .....print the نوشته شده باشد. p را بنویسید و enter کنید تا جدول پارتیشن ها نمایش داده شود. نتیجه کار:



سپس حرف **n** را نوشته و **enter** کنید.

سپس نوع مد نظر را انتخاب کنید.، ما **primary** انتخاب می کنیم، پس **P** را می نویسیم و **enter** می زنیم:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-20317, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-20317, default 20317):
Using default value 20317

Command (m for help): p

Disk /dev/hdb: 10.4 GB, 10485522432 bytes
16 heads, 63 sectors/track, 20317 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hdb1               1       20317    10239736+  83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

۳) شماره پارتیشن خود را بنویسید. عددی بین ۱ تا ۴ است.

۴) اگر می خواهید تغییرات در جداول اعمال شود حرف **w** را بنویسید و **enter** کنید. نتیجه:

```
   Device Boot      Start         End      Blocks   Id  System
/dev/hdb1               1       20317    10239736+  83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Listing 4-4. Verifying That the New Partition Has Been Created

```
[root@server1 ~]# fdisk -l
Disk /dev/hda: 8388 MB, 8388108288 bytes
255 heads, 63 sectors/track, 1019 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1   *           1          13      104391   83  Linux
/dev/hda2              14        1019     8080695   8e  Linux LVM

Disk /dev/hdb: 10.4 GB, 10485522432 bytes
```

۵) فرمت و ایجاد کردن **FileSystem** :

mkfs.ext4 /dev/hda1

نکته: شما می توانید با دستور **partprobes** از تغییرات جدول پارتیشن کرنل سیستم عامل خودتان آگاهی پیدا کنید.

مثل:

partprobe /dev/hda2

یک برنامه دیگر به نام **parted** هست؛ برای کسب اطلاعات بیشتر می توانید به سایت زیر مراجعه کنید:

http://www.cyberciti.biz/tips/re-read-the-partition-table-without-rebooting-linux-system.html

http://linux.about.com/library/cmd/blcmdl8_partprobe.htı

برای کسب اطلاعات بیشتر در مورد "ساخت یک پارتیشن جدید" می توانید به سایت های زیر مراجعه کنید(لینک های زیر عالی می باشد):

http://www.techotopia.com/index.php/Adding_a_New_Disk_Drive_to_a_CentOS_6_System

http://docs.tinyfactory.co/centos/2013/01/11/formcen_-os.html

http://www.geekpeek.net/linux-partitioning-with-fdisk/

فرمت درایو /dev/hdb1 :

برای فرمت این درایو و انتخاب یک **FileSystem** مناسب باید از دستور **mkfs** استفاده کنیم.

مثال۱: ساخت درایو با فرمت **ext3.** :

Listing 4-5. Formating /dev/hdb1

azimzadeh

```
[root@server1 ~]# mkfs.ext3 /dev/hdb1
mke2fs 1.39 (29-May-2006)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1281696 inodes, 2559934 blocks
127996 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2621440000
79 block groups
32768 blocks per group, 32768 fragments per group
16224 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

برای کسب اطلاعت بیشتر به سایت زیر مراجعه کنید:

http://www.cyberciti.biz/faq/howto-format-create-linux-filesystem/

سپس ما باید از دستور **mount** در ادامه استفاده کنیم. ما می دانیم که **FileSystem** ما در **/dev/hdb1** قرار گرفته است. اما به طور پیشفرض کش **Squid** در مسیر **/var/cache** قرار دارد.

برای این کار بدین صورت عمل می کنیم:

mount /dev/hdb1 /var/cache

سپس: **df -h**

Listing 4-6. Mounting /dev/hdb1 in /var/cache

```
[root@server1 ~]# mount /dev/hdb1 /var/cache
[root@server1 ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup02-LogVol02
                      4.7G  2.4G  2.1G  55% /
/dev/mapper/VolGroup02-LogVol00
                      1.9G   35M  1.8G   2% /home
/dev/hda1              99M   12M   83M  13% /boot
tmpfs                 189M     0  189M   0% /dev/shm
/dev/hdb1             9.7G  151M  9.0G   2% /var/cache
 [root@server1 ~]# mount -l
/dev/mapper/VolGroup02-LogVol02 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/mapper/VolGroup02-LogVol00 on /home type ext3 (rw)
/dev/hda1 on /boot type ext3 (rw) [/boot]
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
/dev/hdb1 on /var/cache type ext3 (rw)
[root@server1 ~]#
```

اگر خواستید از این کاری که کردید جلوگیری کنید و به حالت اول برگردید ، باید از دستور **unmount** استفاده کنید.

برای این کار دستورات زیر را وارد کنید:

unmount /dev/hdb1 /var/cache

سپس: **df -h**

سپس : **mount -l**

```
[root@server1 ~]# umount /dev/hdb1
[root@server1 ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup02-LogVol02
                      4.7G  2.4G  2.1G  55% /
/dev/mapper/VolGroup02-LogVol00
                      1.9G   35M  1.8G   2% /home
/dev/hda1              99M   12M   83M  13% /boot
tmpfs                 189M     0  189M   0% /dev/shm
[root@server1 ~]# mount -l
/dev/mapper/VolGroup02-LogVol02 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/mapper/VolGroup02-LogVol00 on /home type ext3 (rw)
/dev/hda1 on /boot type ext3 (rw) [/boot]

tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
[root@server1 ~]#
```

سهمیه بندی (Quota) استفاده از دیسک:

اگر به عنوان یک مدیر سرور قصد دارید برای کاربران خود در هنگام استفاده از فضای هارد دیسک محدودیت ایجاد کنید، این بخش را حتماً مطالعه کنید.

برای ایجاد quota طبق مراحل زیر عمل کنید:

۱) نصب یا بروز رسانی quota :

yum install quota

yum update quota

۲) قسمتی را که می خواهید برای آن محدودیت اعمال کنید در قسمت fstab باید انجام دهید:

vi /etc/fstab

در اینجا ما قصد داریم این کار را بر روی /home انجام دهیم.

دو کلمه رو به رو را به جلوی /home اضافه کنید: **usrquota,grpquota**

Listing 5-1. Adding User and Group Quota Features on a Filesystem in /etc/fstab

```
LABEL=/home          /home          ext3          defaults,usrquota,grpquota          1 2
```

نکته: می توانید grpquota را هم اضافه نکنید.

سپس فایل را ذخیره کنید.

۳) دو راه در این قسمت پیش روی شما است:

الف) دستور زیر احتمال دارد بر روی سیستم شما کار نکند (اگر کار کرد، از راه حل دوم استفاده نکنید):

```
mount -o remount /home
cat /proc/mounts
```

ب) راه اندازی مجدد سیستم با دستور:

```
reboot
```

۴) با استفاده از ابزار **quotacheck** می توان فایل های **quota** را مدیریت کرد.

پارامترهای ابزار **quotacheck** :

c- : ساخت یک **quota** فایل جدید

u- : بررسی فایل های کاربر

g- : بررسی فایل های گروه

v- : نمایش خروجی کار

ساخت یک فایل **quota**:

```
quotacheck -um /home
```

نتیجه:

```
/dev/mapper/vg_data-lv_data [/home]: user quotas turned on
```

۵) بررسی مجدد تنظیمات برای مطمئن شدن:

نکته: اگر **grpguota** را در مرحله دوم اضافه نکرده باشید، در اینجا با پیغام مبتنی بر خاموش بودن آن باید مواجه شوید.

دستور زیر:

```
quotaon -p -a
```

نتیجه:

```
group quota on /home (/dev/mapper/vg_data-lv_data) is off
user quota on /home (/dev/mapper/vg_data-lv_data) is on
```

۶) ساخت فایل **quota** برای کاربران:

```
edquota -u  UserNme
edquota -u ali
```

```
Disk quotas for user ali (uid 501):
  Filesystem                blocks       soft       hard     inodes     soft     hard
  /dev/sda2                     32          0          0          9        0        0
```

توضیح ستون ها، از چپ به راست:

FileSystem : نام filesysm شما می باشد که برای آن quota فعال شده است.

blocks : بیانگر تعداد بلوک هایی است که کاربر در حال حاضر از آن استفاده می کند.

soft و hard : این دو ستون برای ایجاد محدودیت در استفاده از بلوک های file system می شود.

inodes : اطلاعاتی در مورد فایل ها، فولدرها و ایمیل ها .... در خودش ذخیره و نگهداری می کند (می توان آن را یک شمارنده صدا کرد).

نکته: با حذف فایل ها و .... این عدد کاهش پیدا می کند.

soft و hard : این دو ستون برای ایجاد محدودیت در استفاده از inodes های file system می شود.

در این مرحله قصد داریم محدودیت استفاده از فضا برای کاربر ایجاد کنیم : مثلا: 1GB

Disk quotas for user cent (uid 500):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/mapper/vg_data-lv_data	32	1024000	1024000	8	0	0

۷) بررسی مجدد تنظیمات برای مطمئن شدن:

```
*** Report for user quotas on device /dev/mapper/vg_data-lv_data
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard    grace    used    soft    hard    grace
----------------------------------------------------------------------
root    --      20      0       0                3       0       0
ali     --      32      1024000 1024000          8       0       0
```

نکته: اگر خواستید این تنظیمات را برای دیگر کاربران اعمال کنید، کافی است از پروفایل این کابر کپی بردارید و آن را اعمال کنید. مثلا اعمال تنظیمات انجام شده کاربر ali، به کاربر azimzadeh :

edquota -p ali azimzadeh

برای نمایش نتیجه:

repquota -a

برای کسب اطلاعات بیشتر در مورد quota می توانید به سایت های زیر مراجعه کنید:

http://www.centos.org/docs/5/html/Deployment_Guid_-en-US/ch-disk-quotas.html

http://en.wikipedia.org/wiki/Disk_quota

http://support.hostgator.com/articles/pre-sales-policies/rules-terms-of-service/inode-usage

https://access.redhat.ce/ch-disk-quotas.html

آشنایی با تکنولوژی RAID :

برای این کار، حداقل نیاز به ۲ دیسک خواهید داشت. ما می توانیم از این تکنیک برای نوشتن اطلاعات بر روی هر دو دیسک استفاده کنیم، و وقتی که یکی از دیسک ها آسیب دید از دیسک دوم برای ادامه کار استفاده کنیم.

centos هر دو دیسک را در قالب یک دیسک شناسایی می کند، ولی در واقع ما دو دیسک داریم که این برای ما بسیار مفید خواهد بود. فقط یک مشکل بزرگ وجود دارد و آن هم این هست که اگر دیسک کنترلر ما آسیب ببیند، ما به این دیسک ها دسترسی نخواهیم داشت.

انواع RAID :

۱. سخت افزاری: این مدل، یکی از گرانترین RAID ها می باشد، در صورتی که شما بودجه لازم برای این کار را دارید بهترین پیشنهاد است. چون سیستم عامل به راحتی آن را تشخیص می دهد و هیچ مشکلی هم وجود ندارد.

۲. نرم افزاری: این نوع در مقایسه با نوع اول، از سرعت کمتری برخوردار هست. چون که باید اطلاعات را روی خودش در n جایی که تعیین کرده ایم ذخیره کند. یکی از قابلیت های جالب آن لینک کردن دو USB device به یکدیگر است. مثلا: لینک یک جفت USB device ، یک SATA و یک SAN (storage area network) به یکدیگر.

۳. fake (جعلی): شاید معنا خاصی داشته باشد، ولی من به جعلی بودن معنا کردم. اصول اولیه تکنولوژی را برای RAID توضیح داد و به صورت عملی هم پیاده سازی نشد. و مهمتر از همه این هست که توسط توزیع های لینوکسی پشتیبانی نمی شد.

ما ۶ سطح مختلف در RAID داریم، که فقط ۳ تا از آنها توسط نوع نرم افزاری آن پشتیبانی می شود: RAID0 , RAID1 .RAID5

RAID 0 چیست؟

حداقل به ۲ دیسک نیاز دارید. و دیسک ها هم به صورت منطقی با یکدیگر ترکیب شده اند، و اطلاعات به صورت عادلانه (تقریبا مساوی) روی دیسک ها قرار می گیرند.

RAID 1 چیست؟

به mirroring نیز معروف است و برای این کار حداقل به ۲ دیسک نیاز دارید. اطلاعات بر روی هر دو دیسک نوشته می شود. فقط عمل نوشتن کمی طول می کشد، اما عمل خواندن سریعتر خواهد بود.

چون centos می تواند تشخیص دهد که از کدام دیسک بخواند. و جالب تر این است که اگر یک دیسک شما ظرفیتش 20GB باشد و دیسک دیگر شما 30GB، شما می توانید فقط از 20GB هر دیسک خودتان استفاده کنید. و در اینجا 10GB از فضای شما بلا استفاده می ماند.

RAID 5 چیست؟

پر کاربردترین نوع در استفاده های حرفه ای می باشد و به ۳دیسک نیاز دارد. سرعت نوشتن کمی دارد. کاربرد آن در وب سرورها و ISPها بیشتر می باشد. و از امنیت نسبتا خوبی برخوردار است.

برای کسب اطلاعات بیشتر در مورد RAID ها می توانید به سایت های زیر مراجعه کنید:

http://parspack.com/the-news/177-hardware-software-raid

http://technologyworld.blogsky.com/1389/04/10/pos -200/

http://anegar.blogfa.com/post-3.aspx

http://www.sarzamindownload.com/contents/1125

http://en.wikipedia.org/wiki/RAID

بررسی RAID ها:

راحت ترین راه برای بررسی RAID های نرم افزاری نگاه کردن به /proc/mdstat است.

از دستور زیر برای بررسی RAID ها استفاده می شود و در صورت وجود مشکل، به ایمیل شما مشکلات را ایمیل می کند:

```
mdadm --monitor --mail=your@email.com –delay 1800 /dev/md0
```

LVM (Logical Volume Manager):

LVM مخفف عبارت Logical Volume Manager است که در لینوکس دیسک درایوها و سایر دستگاه های ذخیره اطلاعات را مدیریت می کند.

مقصود از عبارت "volume" یک درایو دیسک یا پارتیشن آن است.

در کل LVM و RAID ها جز مباحث حرفه ای لینوکس می باشد.

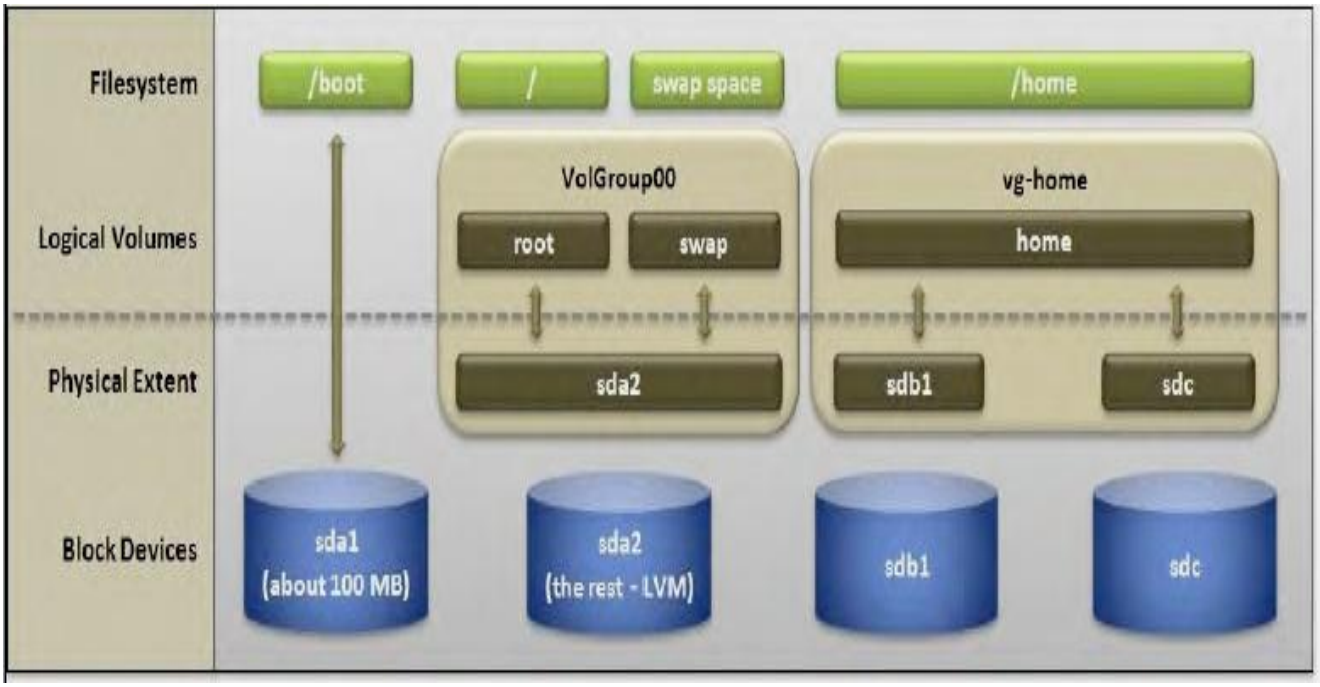
چون نمی خواهم حجم کتاب زیاد شود، در جاهایی که احساس کنم مطالب فارسی خوبی هست لینک های آن را قرار می دهم:

http://linuxsecurity.blogfa.com/post-9.aspx

http://www.hamcodi.ir/qa/questions/1044/lvmD%A

http://www.persianadmins.ir/v2/articles/linux/list/190-lvm.html

http://www.tldp.org/HOWTO/LVM-HOWTO/



لینک های کاربردی فصل چهارم:

http://en.wikipedia.org/wiki/Comparison_of_file_systems

http://www.thegeekstuff.com/2013/01/mke2f -examples/

http://www.tutorialspoint.com/unix_commands/mkfs.htm

http://www.omnisecu.com/gnu-linux/redhat-certified-engineer-rhce/linux-mkfs-commands-howto.php

http://www.linuxtopia.org/onlinee_RAID-ppc.html

لینک های بسیار عالی برای ساخت RAID5 و RAID1 :

http://richard.blog.kraya.co.uk/2012/04/27/3t -hdd-raid5-centos-6-2/

http://www.sysadminhub.in/2013/07/rai -5-configuration-on-centos-using.html

http://www.centos.org/docs/5/html/Deployment_Guid -en-US/s1-raid-config.html

http://infoliser.com/how-to-configure-software-raid1-with-centos-6-x/

http://sammit.net/mirror-raid-1-centos-6-4/

http://www.cyberciti.biz/faq/centos-redhat-rhel-linux-setup-create-raid1/

www.cobranix.com/index.php/raid1-mirrored-array-on-centos-6/

https://www.jcputter.co.za/centos/setup-lvmraid-on-centos/


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش لینوکس مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
LINUX
FOUNDATION


شهریه دوره:
۱۱۰ هزار تومان
کلاس آموزش امنیت شبکه مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۷ روز


شهریه دوره:
۵۰ هزار تومان
کلاس آموزش طراحی صفحات وب - مقدماتی
ظرفیت کلاس: ۵ نفر
مکان برگذاری دوره: کرج - میدان آزادگان - خ مسجد -
تلفن جهت هماهنگی: ۰۹۳۶۳۷۶۷۳۶۱ مهندس عظیم زاده
جلسه اول آزمایشی (رایگان) در صورت پذیرش هزینه آن دریافت خواهد شد.
تاریخ برگزاری:
به مدت ۳ روز
WEB

امنیـــت در CentOS

یکی از حیاتی ترین کارهای یک مدیر سرور در کنار پیکربندی ، نصب و ارتقاء و ... انجام می دهد، برقراری امنیت در سرور می باشد. شما اگر بتوانید حداقل های امنیتی را در سرور خود ایجاد و آنها را درست تنظیم کنید، تا حدی آسوده خاطر می توانید به کارهای خود بپردازید. این فصل را باید به عنوان یک کتاب می نوشتم، چون نمی خواهم حجم کتاب بالا برود، سعی می کنم به مهمترین آنها اشاره کنم.

افزایش امنیت در SSH (Hardening the Secure Shell) :

یکی از قسمت هایی که مدیران شبکه روزانه با آن سر و کار دارند کار با SSH می باشد. پس یک مدیر باید یک سری حداقل ها را برای ارتقای امنیت در این بخش ایجاد کند تا از نفوذ هکرها به سرور، تا حد قابل قبولی جلوگیری کند.

مسیر ذخیره پیکربندی مربوط به SSH در مسیر زیر قرار دارد:

```
/etc/ssh/sshd_config
```

نکته مهم: از فایل مسیر بالا ، قبل از تغییرات در آن، یک پشتیبان تهیه کنید.

نکته مهم: پس از هربار تغییر در پیکربندی SSHD باید این سرویس را دوباره راه اندازی کنید:

```
service sshd restart
```

می توانید از هر یک از روش های زیر برای ارتقای امنیت SSH استفاده و یا همه ی آنها را اعمال کنید.

۱- خط زیر پیدا کنید و علامت # را بردارید:

```
PermitRootLogin no#
```

این کار باعث می شود تا به root ، به صورت مستقیم دسترسی نداشته باشیم.

۲- محدود کردن کاربران به SSH :

می توانید از دستور زیر برای ایجاد محدودیت برای یوزرها (کاربران) استفاده کنید:

```
AllowUsers alimp5 reza root
```

۳- تغییر پورت 22 :

به طور پیشفرض باید از پورت ۲۲ به سیستم وصل شوید، ما در اینجا آن را تغییر می دهیم.

```
#Port 22
port 2345
```

نکته: بعد از تغییر پورت باید، یک تغییر در فایروال خود اعمال کنید:

iptables- A INPUT -m state --state NEW -m tcp -p tcp --dport 2345 -j ACCEPT

نکته: اگر خط بالا نبود، آن را اضافه کنید.

سپس:

```
service iptables save
service iptables restart
```

برای مطمئن شدن فایل زیر را ببینید:

```
vi /etc/sysconfig/iptables
```

۴- ایجاد محدودیت با ip :

می توانید از دستور زیر استفاده کنید:

```
iptables -A INPUT -p tcp -s 190.160.50.85 --dport 22 -j ACCEPT
```

سپس:

```
service iptables save
service iptables restart
```

۵- جلوگیری از حملات brute-force :

دستورات زیر باعث می شود کسی که قرار است از طریق SSH به سیستم وصل شود، اگر بیشتر از ۳ بار در ۱ دقیقه تلاش به وصل شدن به سیستم کند، فایروال به مدت ۱دقیقه آن ip را بلاک خواهد کرد:

```
iptables -F
iptables -N SSH_CHECK
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j SSH_CHECK
iptables -A SSH_CHECK -m recent --set --name ssh
iptables -A SSH_CHECK -m recent --update --seceonds 60 --hitcount 4 --name SSH -j DROP
```

سپس:

```
service iptables save
service iptables restart
```

۶- ساخت کلید های عمومی و خصوصی:

طبق مراحل زیر عمل کنید

```
ssh-keygen -t rsa
```

در ادامه اینتر کنید تا تنظیمات در مسیر زیر ذخیره شوند:

/root/.ssh/

در ادامه می توانید یک پسورد انتخاب کنید.

در نهایت هم دستورات زیر:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_rsa
cat id_rsa.pub >> ~/.ssh/authorized_keys
```

و در آخر هم:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
restorecon -Rv ~/.ssh
```

سپس باید خط زیر را به **sshd_config** اضافه کنید :

PasswordAuthentication no

و راه اندازی مجدد سرویس:

service sshd restart

برای درک بیشتر از این بخش به سایت زیر مراجعه کنید:

https://www.digitalocean.com/community/articles/how-to-set-up-ssh-keys--2

```
[root@localhost ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
5a:fb:b3:7e:52:af:6f:dc:fd:bb:ea:b1:d6:02:d7:16 root@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|               E |
|        S     . .|
|       o . ... o |
|      . .  .o+o..|
|         .o .o*.o|
|         .+=+B+o=|
+-----------------+
[root@localhost ~]#
[root@localhost ~]#  chmod 700 ~/.ssh
[root@localhost ~]# chmod 600 ~/.ssh/id_rsa
```

```
[root@localhost ~]# chmod 700 ~/.ssh
[root@localhost ~]# chmod 600 ~/.ssh/id_rsa
[root@localhost ~]# cat id_rsa.pub >> ~/.ssh/authorized_keys
cat: id_rsa.pub: No such file or directory
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# cd .ssh
[root@localhost .ssh]#
[root@localhost .ssh]#
[root@localhost .ssh]#
[root@localhost .ssh]# cat id_rsa.pub >> ~/.ssh/authorized_keys
[root@localhost .ssh]# chmod 700 ~/.ssh
[root@localhost .ssh]#
[root@localhost .ssh]#
[root@localhost .ssh]# chmod 600 ~/.ssh/authorized_keys
[root@localhost .ssh]#
[root@localhost .ssh]# restorecon -Rv ~/.ssh
[root@localhost .ssh]#
```

۷- مدت زمان بیکاری :

شما با دستور زیر می توانید تعیین کنید که اگر کاربر تا ۱ دقیقه چیزی وارد نکند، ارتباطش قطع شود.

نکته: می توانید زمان آن را هم تغییر دهید.

#LoginGraceTime 2m

به:

LoginGraceTime 60 یا LoginGraceTime 1m

۸- خط های زیر را پیدا کرده و طبق کارهای گفته شده آنها را انجام دهید:

#X11Forwarding no

X11Forwarding yes

به:

X11Forwarding no

#X11Forwarding yes

۹- خط های زیر را پیدا کرده وعلامت # انها را بردارید :

PrintMotd yes

PrintLastLog yes

۱۰- ساخت یک motd :

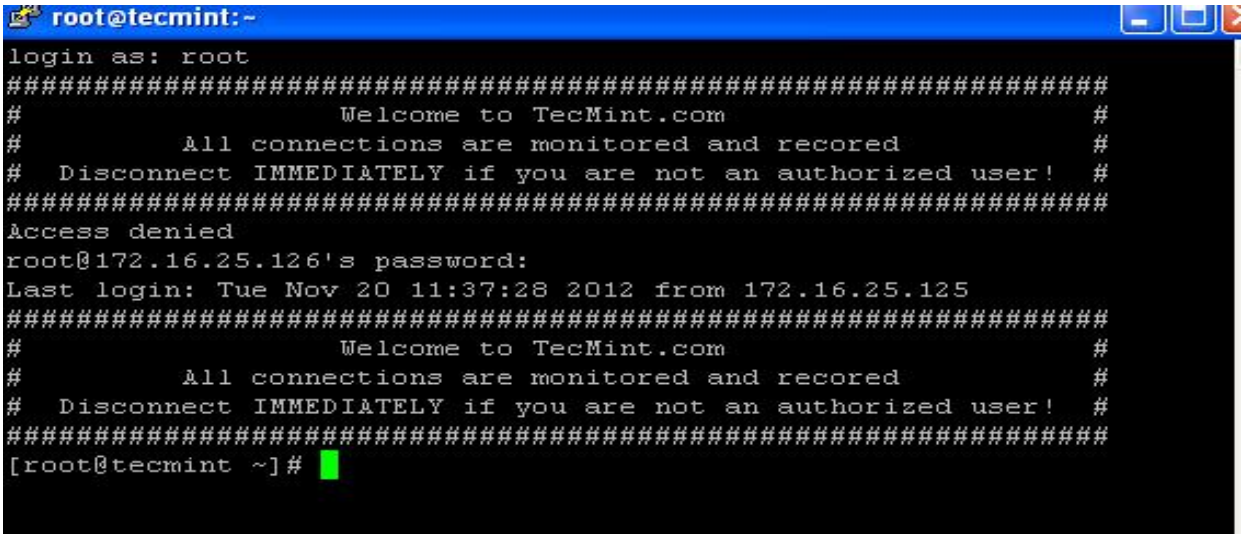
برای نمایش پیغام بعد از ورود کاربر به سیستم استفاده می شود:

vi /etc/motd

برای نمونه خط های زیر را در آن وارد کنید:

welcome to my server

---------- Ali-MP5 was here



۱۱- ساخت یک banner :

با انجام کارهای زیر می توانید به کسانی که می خواهند وارد سیستم شما شوند یک پیغام اخطار بدهید.

ابتدا :

vi /etc/banner.txt

متن زیر را وارد کنید:

This computer system is for authorized users only. All activity is logged and regularly checked. Individuals using this system without authority or in excess of their authority are subject to having all their services revoked...

در ادامه:

vi /etc/ssh/sshd_config

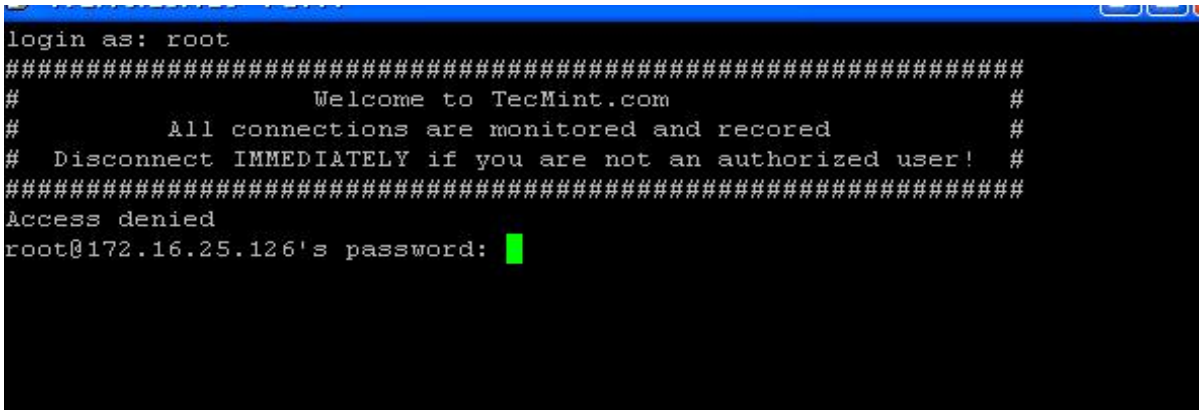
سپس به دنبال خط زیر باشد و علامت # را بردارید و مسیری که متن banner شما در آن قرار دارد را بدهید.

#Banner none

به:

banner /etc/banner.txt

نتیجه:



۱۲_ استفاده از fail2ban :

یکی عمومی ترین راه های پیشنهادی برای امن سازی SSH استفاده از fail2ban می باشد که از امکانات نسبتا خوبی هم برخوردار است.

نکته: مخازن Remi و EPEL باید نصب باشند. در صورت نصب نبودن مخزن ها از سایت سازنده این ابزار آن را دانلود کنید:

http://www.fail2ban.org/wiki/index.php/Downloa

https://github.com/fail2ba /

ابتدا:

```
yum install fail2ban
```

سپس:

```
vi /etc/fail2ban/jail.conf
```

توضیح مهمترین خطوط:

ignoreip : نوشتن ip هایی که قصد دارید به عنوان لیست مجاز (سفید) در نظر گرفته شوند.

مثل:

```
ignoreip = 127.0.0.1  10.0.0.0/8
```

bantime : مدت زمانی که از ورود کاربر به سیستم جلوگیری می شود.

مثل:

```
bantime = 15
600 sec = 10 min
```

maxrety : تعداد دفعاتی که کابر مجاز است پسورد وارد کند.

```
maxrety = 3
```

پیشنهاد: می توانید از طریق مسیر زیر، ip هایی که مدام در حال حمله هستند را به صورت دستی از دسترس سرور خارج کنید:

vi /etc/hosts.deny

سپس:

sshd:ip-attacker

sshd:175.16.25.127

نمایش ip هایی که نتوانستند به سرور وصل شوند(Failed):

cat /var/log/secure | grep 'Failed password' | sort | uniq -c

برای کسب اطلاعات بیشتر در مورد امن سازی SSH می توانید به سایت های زیر مراجعه کنید:

http://www.tecmint.com/install-fail2ban-on-rhel-centos-fedora/

http://www.pontikis.net/blog/fail2b -install-config-debian-wheezy

http://www.tecmint.com/block-ssh-server-attacks-brute-force-attacks-using-denyhosts/

http://webees.me/setting-up-ssh-access-between-mac-osx-and-centos-in-virtualbox/

http://www.cyberciti.biz/faq/rhel-linux-block-ssh-dictionary-brute-force-attacks/

http://www.tecmint.com/ -best-practices-to-secure-and-protect-ssh-server/

https://wiki.archlinux.org/index.php/Secure_Shell

http://freecode.com/projects/dropbear-ssh

http://www.tecmint.com/ssh-passwordless-login-using-ssh-keygen-in-5-easy-steps/

http://www.thatsgeeky.com/2011/01/limitir -brute-force-attacks-with-iptables/

افزایش امنیت در PHP.ini :

اگر شما بر روی سرورخودتان اقدام به نصب PHP کرده باشید، برای ارتقای امنیت آن باید یک سری کارهای لازم را انجام دهید:

نکته: مسیر ذخیره فایل php.ini :

/etc/php.ini

vi /etc/php.ini

۱- دستورات زیر را در این فایل وارد کنید:

disable_functions = foreach, glob, openbasedir, posix_getpwuid, f_open, system,dl, array_compare, array_user_key_compare, passthru, cat, exec, popen, proc_close, proc_get_status, proc_nice,

proc_open, escapeshellcmd, escapeshellarg, show_source, posix_mkfifo, ini_restore, mysql_list_dbs, get_current_user, getmyuid,pconnect, link, symlink, fin, passthruexec, fileread, shell_exec, pcntl_exec, ini_alter, parse_ini_file, leak, apache_child_terminate, chown, posix_kill, posix_setpgid, posix_setsid, posix_setuid, proc_terminate, syslog, allow_url_fopen, fpassthru, execute, shell, curl_exec, chgrp, stream_select, passthru, socket_select, socket_create, socket_create_listen, socket_create_pair, socket_listen, socket_accept, socket_bind, socket_strerror, pcntl_fork, pcntl_signal, pcntl_waitpid, pcntl_wexitstatus, pcntl_wifexited, pcntl_wifsignaled, pcntl_wifstopped, pcntl_wstopsig, pcntl_wtermsig, openlog, apache_get_modules, apache_get_version, apache_getenv, apache_note, apache_setenv, virtual

۲- دستورات زیر را در این فایل وارد کنید:

allow_url_fopen= off

allow_url_include= off

safe_mode = on

register_globals= off

safe_mod_gid= on

open_basedir= on

exec= off

shell_exec= off

display_errors= off

session.cookie_httponly=

max_execution_time = 300

cgi.force_redirect= on

magic_quotes_gpc= off

magic_quotes_runtime = off

magic_quotes_sybase = off

session.use_trans_sid = off

asp_tags = off

expose_php = off

html_errors = off

ServerSignature = off

UseCanonicalName = off

HostnameLookups = off

ExtendedStatus = off

register_long_arrays = off

track_errors = off

ignore_repeated_errors= off

ignore_repeated_source = off

display_startup_errors = off

safe_mode_gid = off

output_buffering = 4096

php_value session.use_trans_sid = 0

php_value session.use_only_cookies = 1

session.auto_start = 0

session.cookie_lifetime =

post_max_size = 256K

variables_order = "EGPCS"

توابع هش برای نشست ها:

0: MD5 (128 bits)

1: SHA-1 (160 bits)

session.hash_function =

برای کسب اطلاعات بیشتر در مورد هر یک از خط های بالا می توانید به سایت "تیم امنیتی ایران" مراجعه کنید:

در همین بخش باید از دوست عزیزم YuSeF_HaCkeR برای نوشتن این مطالب بسیار ارزشمند تشکر کنم.

http://forum.irsecteam.org/forum45/thread1282.htm

برای کسب اطلاعات بیشتر در مورد امن سازی PHP.ini می توانید به سایت های زیر مراجعه کنید:

http://www.cyberciti.biz/tips/php-security-best-practices-tutorial.html

http://docs.cpanel.net/twiki/bin/view/AllDocumentation/WHMDocs/PhpIni

http://www.openlogic.com/wazi/bid/221168/Improv -PHP-performance-with-PHP-eAccelerator

http://www.symantec.com/connect/articles/securing-php-step-step

http://www.tenable.com/blog/configuration-auditing-phpini-to-help-prevent-web-application-attacks

http://blog.grik.net/2007/03/som -security-settings.html

http://php.net/manual/en/security.php

https://kb.mediatemple.net/questions/1700/Increase+PHP+security+with+PHPSecInfo

https://github.com/funkatron/phpsecinfo

http://www.mediawiki.org/wiki/Manual:Security

http://docs.cpanel.net/twiki/bin/view/EasyApache/Php/RequestHandling

http://www.prestatraining.com/1 -tips-to-optimise-your-php-ini-file-for-prestashop/

پیکربندی یک دیواره آتش و کار با iptables :

خود این iptables یک کتاب ۲۰۰ صفحه ای است، اما سعی می کنم قسمت های مهم را همراه با مثال توضیح بدهم.

نکته مهم: بعد از هربار تغییر در فایروال باید دستورات زیر را اجرا کنید:

```
service iptables save
service iptables restart
```

نکته۱: دیدن مسیرهایی که iptables در آنجا قرار دارد:

```
find / -name 'iptables'
```

نکته۲: دیدن قوانین درج شده در iptables :

```
cat /etc/sysconfig/iptables
```

درآخر فایل می بینید که نوشته COMMIT ، این خط آخر باعث می شود تمام قوانین در حافظه قرار گیرند و سیستم بتواند از آنها استفاده کند.

نکته۳: برای مشاهده قوانین فعلی iptables می توانید دستور زیر را وارد کنید:

```
iptables -L -n
```

نکته ۴: -v شمارنده تعداد بسته هایی است که از اینترفیس مربوطه شما عبور می کند :

```
iptables -L -n -v
```

نکته۵: -Z شمارنده تعداد بسته ها را به عدد صفر مقداردهی می کند، تا عمل شمردن از صفر شروع شود :

```
iptables -L -n -v -Z
```

Listing 10-2. Viewing the Current Rules

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with
 icmp-host-prohibited
```

توضیحات مختصر از چهار جدول اصلی iptables :

۱- جدول filter:

قوانین فیلترینگ، برای ایجاد محدودیت در جدول filter استفاده می شوند.

زنجیره (chain):

هر جدول دارای یک سری مجموعه ساخته شده از زنجیره های خودش است، اما زنجیره های تعریف شده توسط کاربر نیز می تواند ایجاد شود،

به طوری که کاربر می تواند یک سری از مجوعه قوانینی که با یک تگ مشترک و مرتبط به هم هستند را بسازد، مثل:

INPUT_ESTABLISHED یا DMZ_NETWORK .

مهمترین زنجیره ها:

الف) input= برای بسته هایی استفاده می شود که مقصدشان سوکت های محلی ما هستند.

ب) forward= فیلتر بسته هایی که به سرورهای در دسترس توسط NIC دیگر بر روی فایروال و بررسی پکت هایی که به واسطه سیستم لینوکس روت(عمل مسیریابی) شده اند.

مثلا: زمانی که فایروال از iptables استفاده می کند برای اتصال یک شبکه به شبکه دیگر، پکت ها باید از طریق جریان فایروال عبور کنند.

پ) output= برای بسته هایی استفاده می شود که به طور محلی (از سمت ما) تولید شده اند و می خواهند خارج شوند.

۲- جدول nat (network address Translation) :

برای ترجمه آدرس شبکه و همچنین در port forwarding و نیز در ترجمه فیلد منبع بسته یا مقصد استفاده می شود.

نکته: همان کاری که یک هکر با فعال کردن گزینه زیر در iptables انجام می دهد:

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

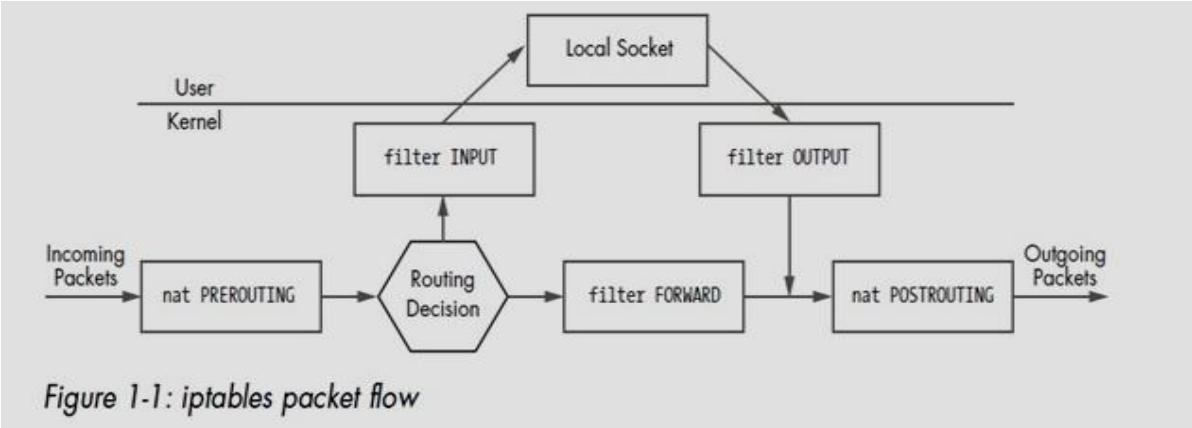


Figure 1-1: iptables packet flow

PREROUTING= برای تغییر دادن بسته ها به محض ورود استفاده می شود.

POSTROUTING= برای تغییر دادن بسته ها به محض خروج استفاده می شود.

۴ مورد از اهدافی که فقط در داخل جدول nat معتبر (در دسترس) هستند:

الف) DNAT= برای ترجمه آدرس شبکه مقصد و بازنویسی آدرس ip مقصد از یک بسته که اگر با MACTH ها مطابقت داشت انجام می شود.

و فقط هم در PREROUTING و OUTPUT معتبر است.

سایت زیر با یک مثال واضح این موضوع را توضیح داده است:

https://www.frozentux.net/iptables-tutorial/chunkyhtml/x4033.html

ب) SNAT= برای تغییر دادن آدرس مبدا بسته استفاده می شود.

سایت زیر با یک مثال واضح این موضوع را توضیح داده است:

http://www.fwbuilder.org/4.0/docs/users_guide5/source-address-translation.shtml

پ) MASQUERADE= فقط در POSTROUTING معتبر می باشد.

سایت زیر با یک مثال واضح این موضوع را توضیح داده است:

http://syrlug.org/contrib/ipmasq.html

ت) REDIRECT= یکی از قسمت های کارآمد و عالی در nat برای ایجاد تغییر و هدایت بسته ها از پورت به پورت دیگر و .... می باشد.

مثال: فرض کنید شما می خواهید ترافیک ورود به سرور را از پورت ۸۰ ، روی پورت ۸۰۸۰ هدایت کنید:

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport $srcPortNumber -j REDIRECT --to- port $dstPortNumber

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to- port 8080

سایت زیر با یک مثال واضح این موضوع را توضیح داده است:

http://www.cyberciti.biz/faq/linux-port-redirection-with-iptables/

۳- جدول mangle :

برای خرد کردن یا همان تغییر در نوع فیلد سرویس یک بسته استفاده می شود.

۲ مورد از اهدافی که فقط در داخل جدول mangle معتبر هستند و در خارج از این جدول نمی توان از آنها استفاده کرد:

الف) TOS= هدف آن برای تنظیم و/ یا تغییر نوع فیلد سرویس در بسته می باشد.

ب) TTL= time to live، می توان مدت زمان عمر(حیات) یک بسته را تعیین کرد.

مثلا: اگر ttl را درهنگام خروج از مرز روتر توسط فایروال با عدد ۱ مقدار دهی کنید، آن بسته به جایی نخواهد رفت و ارتباط هاست موردنظر با اینترنت قطع خواهد شد.

سایت زیر با یک مثال واضح این موضوع را توضیح داده است:

http://unix.stackexchange.comles-set-mark-route-diferent-ports-through-different-interfaces

۴- جدول raw :

کاربرد اساسی آن وقتی است که شما می خواهید بسته ها را به گونه ای علامت گذاری کنید تا توسط سیستم ردیابی چک نشوند.

این کار با هدف گذاری از طریق NOTRACK روی بسته ها انجام می شود

این جدول از PREROUTING و OUTPUT به خوبی پشتیبانی می کند.

توضیحات بیشتر در مورد این جدول در سایت زیر است:

http://www.inetdoc.net/guides/iptables-tutorial/rawtable.html

هدف ها:

الف) ACCEPT= فایروال بسته را برای عبور از خودش می پذیرد تا در مراحل بعد پردازش های لازم روی آن صورت گیرد.

ب) DROP= فایروال بسته را برای عبور از خودش نمی پذیرد و هیچ پیغامی برای فرستنده نمی فرستد.

پ) REJECT= فایروال بسته را برای عبور از خودش نمی پذیرد و پیغام(خطا) برای فرستنده می فرستد.

مثلا: دو پروتکل UDP و TCP را در tcp/ip در نظر بگیرید،TCP مدام با Acknowledge چک می کند آیا بسته رسیده یا خیر، اگر نرسیده، مجدداً سعی می کند بسته را بفرستد. اما در UDP چنین نیست.

ت) LOG= جزئیات بسته ها برای عمل log (ثبت رویداد) به syslogd ارسال می شود.

ث) RETURN= ادامه پردازش یک بسته در داخل زنجیره را خواستار است.

دستورات :

A- : می توانید یک قانون جدید به فایروال اضافه کنید.

F- : برای پاک کردن تمام قوانین موجود در جدول استفاده می شود.

D- : برای حذف یک یا چندین قانون از زنجیره انتخاب شده استفاده می شود.

I- : برای درج یک یا چندین قانون در زنجیره انتخاب شده استفاده می شود.

R- : برای جایگزینی یک قانون در داخل زنجیره انتخاب شده استفاده می شود.

L- : برای لیست کردن تمام قوانین در زنجیره انتخاب شده استفاده می شود.

N- : برای ساخت یک زنجیره استفاده می شود.

X- : برای حذف یک زنجیره استفاده می شود.

و ....

پارامترها :

P- : تعیین کننده نوع پروتکل می باشد. مثل: udp , tcp , icmp

s- : آدرس مبداء می باشد.

d- : آدرس مقصد می باشد.

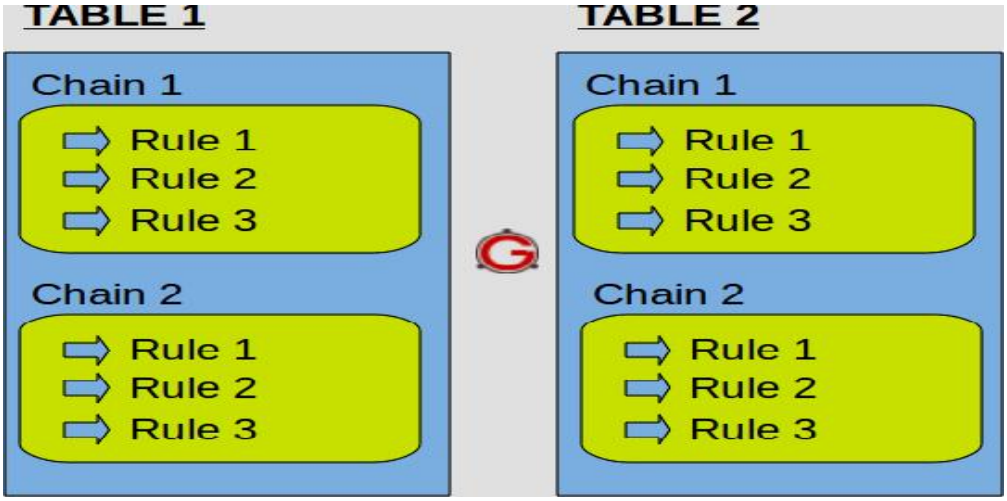
i- : نام اینترفیسی که قرار است بسته ها توسط آن دریافت شوند. مثل: eth0

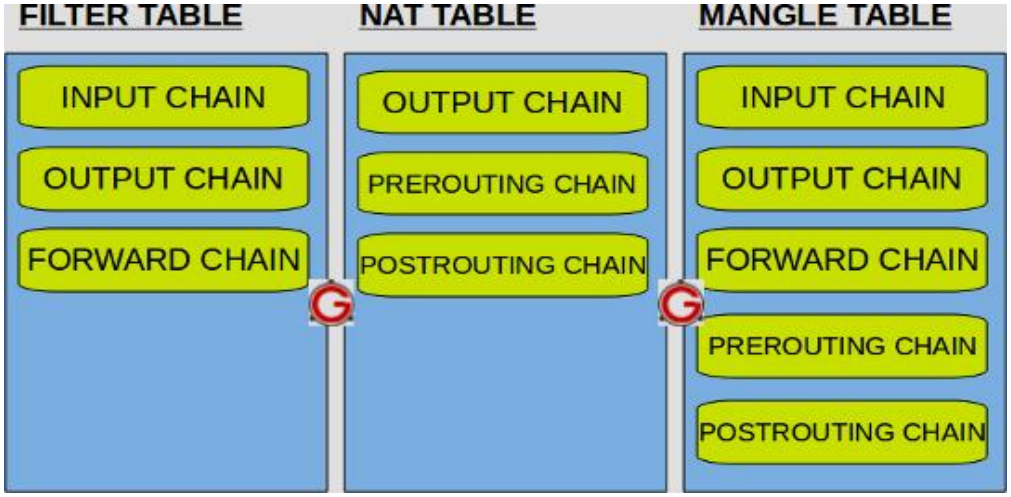
نکته: فقط برای بسته هایی است که می خواهند وارد زنجیره های INPUT و FORWARD و PREROUTING شوند.

o- : نام اینترفیسی که قرار است بسته ها از آن خارج شوند. مثل: eth0

و ....

دو شکل زیر بیانگر برخی از توضیحات بخش های بالایی می باشد:





برای درک بیشتر از توضیحات بالا می توانید به سایت های زیر مراجعه کنید:

http://forum.irsecteam.org/forum46/thread1648.htm

http://ipset.netfilter.org/iptables.man.html

http://www.thegeekstuff.com/2011/01/iptable_-fundamentals/

http://www.linuxtopia.org/Linux_Firewall_iptables/index.html

http://www.linuxcommand.org/man_pages/iptables8.htn

http://blog.adityapatawari.com/2011/12/i_-packet-filtering-iptables-explained.html

http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO-6.html

http://ipset.netfilter.org/iptables.man.html

http://www.iptables.info/en/structure-of-iptables.html

http://www.karlrupp.net/en/computer/nat_tutorial

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

http://www.cyberciti.biz/faq/rhel-fedorta-linux-iptables-firewall-configuration-tutorial/

http://www.cyberciti.biz/faq/?s=iptables

http://www.iptables.info/en/connection-state.html

۱- دستور زیر تمام قوانین را پاک می کند:

iptables --flush

برای اطمینان از اینکه هیچ مشکلی در ارتباط نباشد، فعلا از دستور موقت زیر می توانید استفاده کنید:

iptables -P INPUT ACCEPT && iptables -P FORWARD ACCEPT && iptables -P OUTPUT ACCEPT

۲- ایجاد ترافیک(دسترسی) نامحدود برای **LoopBack** :

lo=127.0.0.1

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

۳- محدود کردن دسترسی از مبداء به مقصد:

iptables -A INPUT -i lo -s XXX.XXX.XXX.XXX -d XXX.XXX.XXX.XXX -j ACCEPT

-s : **ip** آدرس مبداء می باشد.

-d : **ip** آدرس مقصد می باشد.

مثال۱: اجازه دسترسی به سرویس های **HTTPD , FTP , NTP** از طرف دیگر سیستم ها در شبکه:

iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 143 -j ACCEPT

iptables -A INPUT -p tcp --dport 143 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 20:21 -j ACCEPT

iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT

مثال۱ : یک قسمت ساده از **-s** را در شکل زیر برای شما نشان داده ام:

Listing 10-4. An Example of Address Matching

```
-s 192.168.3.20 # packet sent from a single host
-s 192.168.3.0/24 # packet sent from any host on the subnet
-s ! 10.0.0.0/8 # packet has sent from a host not on the subnet
```

مثال۲: بررسی بسته های **SYN** و بلاک کردن آنها:

iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

مثال۳: بررسی بسته های در حال ورود به صورت تکه تکه و بلاک کردن آنها:

iptables -A INPUT -f -j DROP

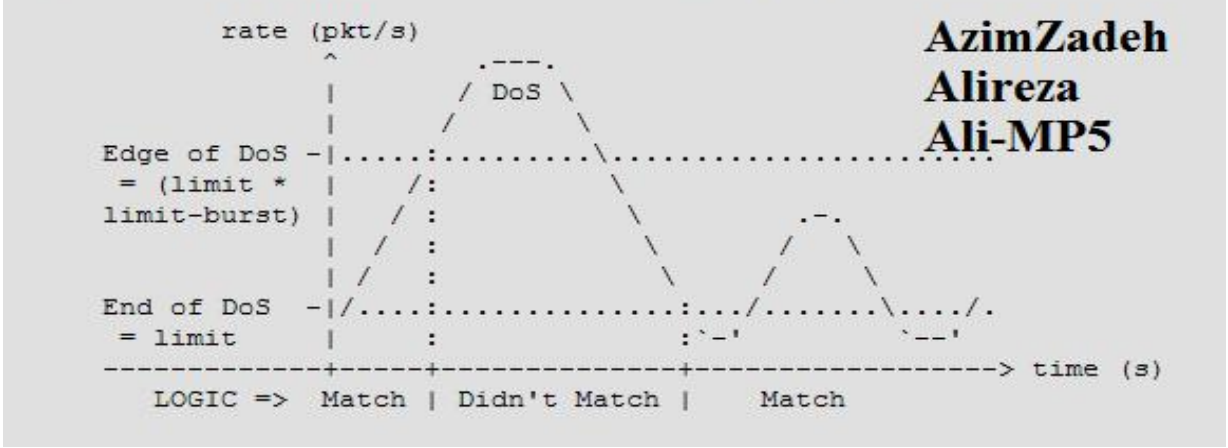
مثال۴: بلاک کردن بسته های XMAS و Null :

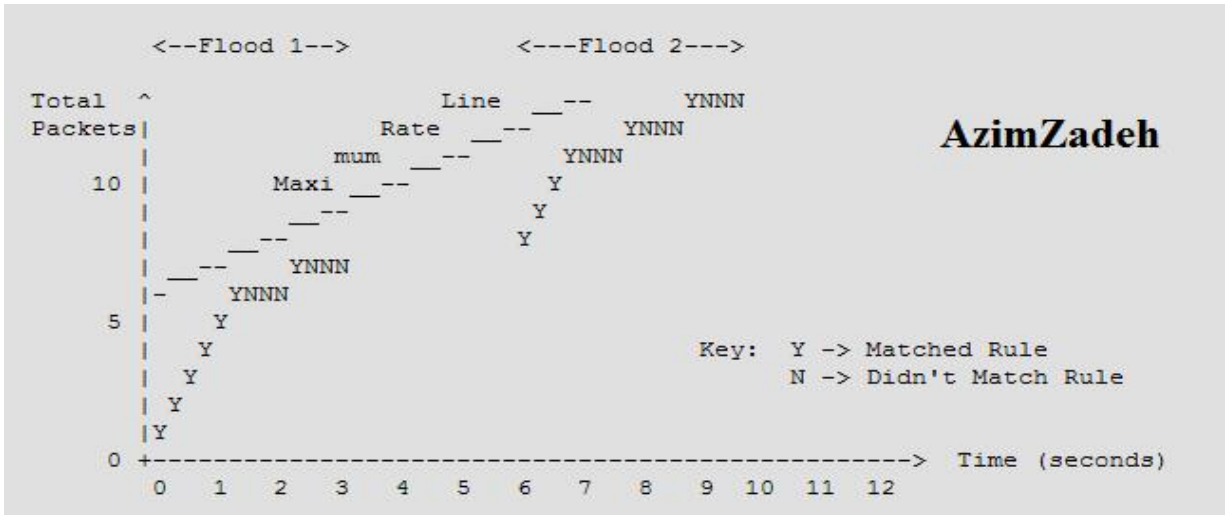
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP

iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

مثال۵: بلاک کردن حملات ساده DOS :

This module works like a "hysteresis door", as shown in the graph below.





iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT

iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT

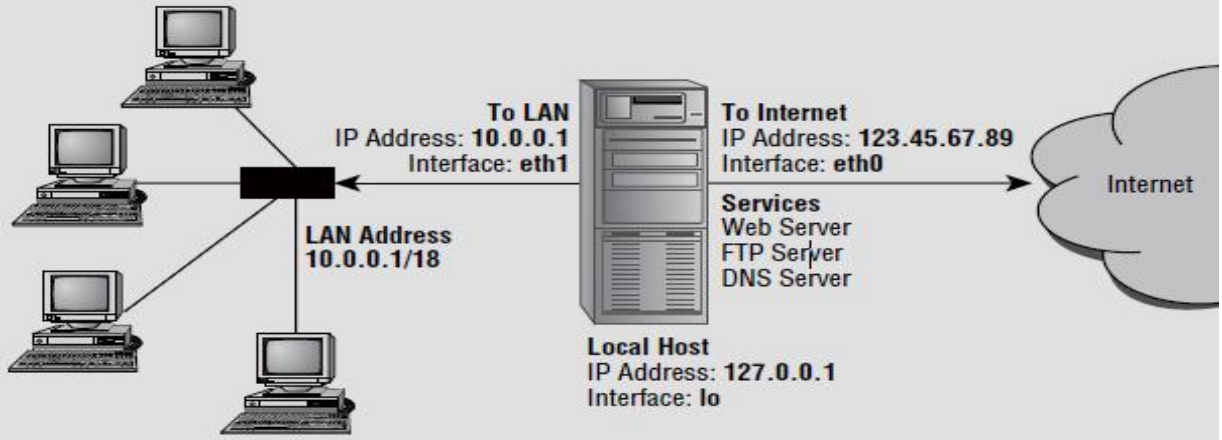
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT

مثال5 : طبق دو شکل زیر قصد دارم حداقل دستوراتی که در پیکربندی ساده این شبکه لازم است را برای شما بنویسم:

اخطار: این سناریو برای یک شبکه محلی LAN می باشد، پس دقت کنید.

FIGURE 13-2

Using iptables as a firewall between the Internet and a LAN



Firewall Computer

The firewall computer is set up as follows:

- **Local Host** — `127.0.0.1` (IP address) and `lo` (interface). You shouldn't need to change these.
- **Connection to the Internet** — `123.45.67.89` (IP address) and `eth0` (interface). Replace them with the static IP address and interface name associated with your connection to the Internet, respectively.
- **Connection to the LAN** — `10.0.0.1` (IP address) and `eth1` (interface). Replace `10.0.0.1` and `eth1` with the static IP address and interface name associated with your connection to your LAN, respectively.
- **Computers on the LAN** — Each computer on the LAN in the example has an IP address from `10.0.0.2` to `10.0.0.254`. Change `10.0.0.255` to a number that matches your LAN's range of addresses.

۱- بخش اول:

```
# (1) Policies (default)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

۲- بخش دوم:

```
# (2) User-defined chain for ACCEPTed TCP packets
iptables -N okay
iptables -A okay -p TCP --syn -j ACCEPT
iptables -A okay -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A okay -p TCP -j DROP
```

۳- بخش سوم:

```
# (3) INPUT chain rules
# Rules for incoming packets from LAN
iptables -A INPUT -p ALL -i eth1 -s 10.0.0.0/24 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 127.0.0.1 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 10.0.0.1 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 123.45.67.89 -j ACCEPT
iptables -A INPUT -p ALL -i eth1 -d 10.0.0.255 -j ACCEPT
# Rules for incoming packets from the Internet
# Packets for established connections
iptables -A INPUT -p ALL -d 123.45.67.89 -m state --state ESTABLISHED,RELATED -j ACCEPT
# TCP rules
iptables -A INPUT -p TCP -i eth0 --destination-port 21 -j okay
iptables -A INPUT -p TCP -i eth0 --destination-port 22 -j okay
iptables -A INPUT -p TCP -i eth0 --destination-port 53 -j okay
iptables -A INPUT -p TCP -i eth0 --destination-port 80 -j okay
iptables -A INPUT -p TCP -i eth0 --destination-port 113 -j okay
# UDP rules
iptables -A INPUT -p UDP -i eth0 --destination-port 53 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 --destination-port 2074 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 --destination-port 4000 -j ACCEPT
# ICMP rules
iptables -A INPUT -p ICMP -i eth0 --icmp-type 3 -j ACCEPT
iptables -A INPUT -p ICMP -i eth0 --icmp-type 8 -j ACCEPT
iptables -A INPUT -p ICMP -i eth0 --icmp-type 11 -j ACCEPT
```

۴- بخش چهارم :

```
# (4) FORWARD chain rules
# Accept the packets we want to forward
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

۵- بخش پنجم :

```
# (5) OUTPUT chain rules
# Only output packets with local addresses (no spoofing)
iptables -A OUTPUT -p ALL -s 127.0.0.1 -j ACCEPT
iptables -A OUTPUT -p ALL -s 10.0.0.1 -j ACCEPT
iptables -A OUTPUT -p ALL -s 123.45.67.89 -j ACCEPT
```

۶- بخش ششم :

```
# (6) POSTROUTING chain rules
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 123.45.67.89
```

مثال۶ : استفاده از iptables به عنوان یک پروکسی شفاف:

در اینجا می خواهیم پورت ۸۰ را به پورت ۳۱۲۸ که مربوط به پروکسی است، بدون آن که کامپیوترهای میزبان شما در شبکه متوجه آن شوند از این راهکار برای امنیت بیشتر استفاده کنیم.

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --toports 3128
```

چک کردن Log (رویداد های ثبت شده):

به طور پیشفرض در cnetos ابزار sysklogd نصب است، پیشنهاد من به شما حذف این ابزار و جایگزین کردن آن با ابزار جدیدی به نام rsyslog است.

```
yum install rsyslog && yum remove sysklogd
```

نکته: بعد از هربار تغییر در پیکربندی ، باید سرویس را مجدد راه اندازی کنید.

سپس:

```
service rsyslog start
chkconfig rsyslog on
```

مسیر فایل rsyslog :

/etc/rsyslog.conf

مثال: در اینجا قصد داریم یک سیستم را در شبکه مسئول جمع آوری log ها و نگه داشتن آنها کنیم.

برای این کار باید از پورت ۵۱۴ udp استفاده کنیم. خط زیر را پیدا کرده و # آن را بردارید (نتیجه):

$UDPServerRun 514

iptables -I INPUT 5 -p udp -m udp --dport 514 -j ACCEPT

service iptables save

service iptables restart

در سیستم مقصد به مسیر زیر بروید و تغییرات لازم را اعمال کنید :

nano /etc/rsyslog.conf

بر اساس ip آدرس و توسط پروتکل UDP:

authpriv.* @172.168.1.1

یا بر اساس hostname :

authpriv.* @alimp5

سپس:

service rsyslog restart

نکته۱: ارسال تمام پیغام ها از طریق پروتکل TCP :

authpriv.* @@172.168.1.1

نکته۲: نمایش پیغام ها در کنسول، به جای فرستادن آنها:

authpriv.* @system

نکته۳: درو انداختن تمام پیغام های تولید شده برای این فایل:

authpriv.* -

بررسی Log ورود کاربران:

با دستور زیر می توانید از ورود کاربران به سیستم آگاه شوید.

lastlog

و یا:

w

```
[root@localhost ~]#
[root@localhost ~]# lastlog
Username         Port     From             Latest
root             pts/1    192.168.1.2      Mon Jan 27 02:20:06 -0800 2014
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
uucp                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
gopher                                     **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
```

محدود کردن کاربران با TCP- Wrappers :

به کمک این ابزار می توانید برای کاربرانی که قصد دارند با سرور شما ارتباط برقرار کنند محدودیت ایجاد کنید.

این سرویس به عنوان یکی دیگر از لایه های بسیار مهم در افزایش امنیت سرورها می باشد.

با استفاده از قدرت این سرویس شما می توانید ACL(Access Control List) های مختلف برای ایجاد محدودیت و کنترل دسترسی از سمت کاربران راه دور به سمت سرور خودتان بنویسید.

نکته: این سرویس به طور پیشفرض بر روی سیستم نصب است و قوت آن بر اساس کار با IP است. برای اطمینان از دستور زیر استفاده کنید:

rpm -qa | grep -i Wrappers*

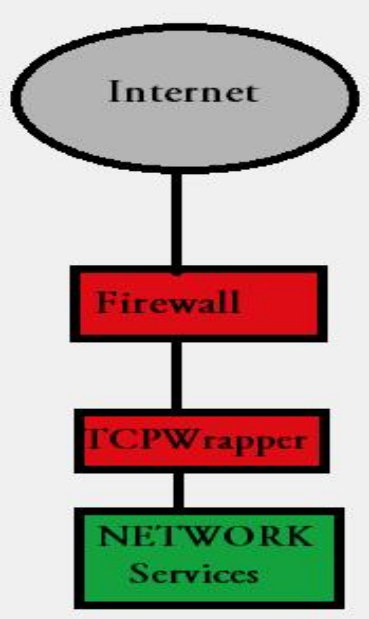
نحوه کارکرد سرویس TCP-Wrapper :

هنگامی که کانکشن ها در حال تلاش برای استفاده از سرویس ها هستند اتفاقات زیر در TCP-Wrapper رخ می دهد:

۱- پروسه با قوانین موجود در فایل etc/hosts.allow بررسی می شوند، اگر اجازه دسترسی داشتند می توانند به مسیر خود ادامه دهند.

۲- پروسه با قوانین موجود در فایل /etc/allow.deny بررسی می شوند، اگر در این لیست قرار داشت، اجازه ادامه دادن نخواهد داشت.

۳- در صورت نبود قانون برای بررسی، دسترسی بدون محدودیت خواهد بود.



مثال۱: برای نمایش هر چیزی که در حال استفاده از TCP-Wrappers می باشد:

strings -f <program_name> | grep hosts_access

ls /usr/lib/libwrap.so

```
[root@localhost ~]#
[root@localhost ~]# strings -f /usr/sbin/* | grep hosts_access
/usr/sbin/rpc.rquotad: hosts_access
/usr/sbin/sshd: hosts_access
/usr/sbin/tcpd: hosts_access_verbose
[root@localhost ~]#
[root@localhost ~]#
```

دستورات TCP-Wrappers :

۱- ALL :

اگر در hosts.deny باشد: به معنای رد کردن تمام درخواست ها می باشد.

اگر در hosts.allow باشد: به معنای قبول کردن تمام درخواست ها می باشد.

اما توضیح لفظی آن: همه چیز را شامل می شود، می تواند برای لیست Daemon ها یا کلاینت ها مورد بررسی قرار گیرد.

۲- LOCAL :

همه هاست هایی را که نام آن ها دارای نقطه (.) نیست شامل می شود. مثل: localhost

۳- UNKNOWN :

با هر یوزر و کامپیوتری که اسم یا آدرس آن ناشناخته باشد همخوانی دارد .توجه داشته باشید که این الگو باید با دقت به کار گرفته شود چون ممکن است اسامی کامپیوترها به خاطر مشکلات سرور غیرقابل دسترس شوند. زمانی که نرم افزار نتواند تشخیص دهد با چه نوع شبکه ای در حال صحبت است آن آدرس غیرقابل دسترس خواهد بود.

۴- KNOWN :

با هر یوزر و کامپیوتری که اسم یا آدرس آن مشخص باشد همخوانی دارد. توجه داشته باشید که این الگو باید با دقت به کار گرفته شود چون ممکن است اسامی کامپیوترها به خاطر مشکلات سرور غیرقابل دسترس شوند. زمانی که نرم افزار نتواند تشخیص دهد با چه نوع شبکه ای در حال صحبت است آن آدرس غیرقابل دسترس خواهد بود.

۵- PARANOID :

هر کامپیوتر و هاستی که نام آن با آدرس آن همخوانی ندارد را شامل می شود. زمانی که tcpd با -DPARANOID (حالت پیش فرض) ایجاد می شود، حتی قبل از اینکه جدول کنترل دسترسی بررسی شود درخواست های صادره از چنین کلاینت هایی رد می شود. زمانی که می خواهید کنترل بیشتری روی چنین درخواست هایی داشته باشید، آن را بدون -DPARANOID ایجاد کنید.

۶- EXCEPT :

اگر بخواهید در شرط خود استثناء قائل شوید، استفاده می شود. مثل: قبول کردن یک رنج از IP ، به جز تعدادی از IP های مشخص.

دستورات بالا را همراه با مثال توضیح خواهم داد.

مثال۲: رد کردن تمام دسترسی ها برای ارتباط و فقط اجازه دادن به ip=192.168.1.2 برای ارتباط با سرویس SSH :

vi /etc/hosts.allow

و نوشتن:

sshd : 192.168.1.2

سپس:

vi /etc/hosts.deny

و نوشتن:

ALL : ALL

نتیجه:

```
[root@ali~]# ssh 192.168.0.2
ssh_exchange_identification: Connection closed by remote host
[root@ali~]#
```

مثال۳: پذیرفتن تمام درخواست های دسترسی که از دامین slashroot.in برای ما می آید:

vi /etc/hoss.allow

ALL : .slashroot.in

مثال۴: پذیرفتن دسترسی از دامین slashroot.in ، فقط برای سرویس SSH :

vi /etc/hosts.allow

sshd : .slashroot.in

مثال۵: پذیرفتن دسترسی از رنج ip آدرس های *.*.172.16 :

vi /etc/hosts.allow

ALL : 172.16.

نکته۱: اگر شما در قسمت deny نوشته باشید: ALL : 172.16.100.200 هیچ وقت این قانون اجرا نخواهد شد. چون در allow، اجازه دسترسی از رنج ip های *.*.172.16 صادر کرده اید.

نکته۲: مثال بالا را بدین شکل هم می توان نوشت:

ALL : 172.16.0.0/255.255.0.0

مثال۶: پذیرفتن دسترسی ها از SSH با توجه به هاست/IP های نوشته شده در مسیر زیر(/etc/sshd.hosts):

vi /etc/hosts.allow

sshd: /etc/sshd.hosts

مثال۷: پذیرفتن دسترسی ها به تمام سرویس ها به جز SSH در رنج IP زیر(172.16.0.0/255.255.0.0):

vi /etc/hosts.allow

ALL EXCEPT sshd: 172.16.0.0/255.255.0.0

برای کسب اطلاعت بیشتر در مورد TCP-Wrapper می توانید به سایت های زیر مراجعه کنید:

http://www.cyberciti.biz/faq/tcp-wrappers-hosts-allow-deny-tutorial/

http://www.slashroot.in/linux-access-control-using-tcp-wrappers

http://en.wikipedia.org/wiki/TCP_Wrapper

https://access.redhat.com/sieide/ch-tcpwrappers.html

http://linuxgazette.net/162/prestia.html

https://protect.iu.edu/cybersecurity/tcp-wrappers

http://en.wikipedia.org/wiki/Access_control_list

http://www.aboutlinux.info/2005/10/usin_-tcp-wrappers-to-secure-linux.html

https://www.ibm.com/developerworks/aix/library/au-tcpwrapper/

پیگیری پیغام های Log با ابزار logwatch :

۱- نصب ابزارهای لازم:

```
yum install logwatch sendmail postfix mailx
chkconfig sendmail on
```

۲- رفتن به مسیر زیر:

```
cd /usr/share/logwatch/default.conf/services
```

۳- ایجاد تغییرات زیر:

```
sudo nano zz-disk_space.conf
```

خط های زیر را پیدا کرده و # آنها را بردارید:

نتیجه:

```
$show_home_dir_sizes = 1
$home_dir= "/home"
$show_mail_dir_sizes = 1
$mail_dir= "/var/spool/mail"
$show_disk_usage = 1
```

۴- سپس:

```
nano http.conf
```

خط زیر را پیدا کرده و آن را به صورت زیر تغییر دهید:

```
$HTTP_IGNORE_ERROR_HACKS = 1
```

۵- باز کردن فایل پیکربندی:

```
vi /usr/share/logwatch/default.conf/logwatch.conf
```

خط زیر را پیدا کرده و ایمیل خود را بنویسید:

```
#MailTo= root
MailTo= alimp5@irsecteam.org
```

خط زیر را هم بنویسید:

```
output = mail
```

۶- به مسیر زیر بروید:

```
vi /etc/aliases
```

خط زیر را پیدا کرده و آن را تغییر دهید:

root: youremail@yourdomain.com#

root: alimp5@irsecteam.org

۷- در ترمینال:

newaliases

و در ادامه:

/etc/init.d/sendmail start

۸- مشاهده ۱۰خط آخر از log ها:

tail -f /var/log/maillog

پیکربندی سیستم های تشخیص نفوذ (IDS) و پیشگیری از نفوذ(IPS) :

یکی دیگر از کارهای مهم یک مدیر سرور نصب و راه اندازی این دو سیستم قدرتمند می باشد، سیستم های فوق در قالب نرم افزارهای قوی Snort و Psad قرار داده شده اند.

قسمت اول (Snort):

snort چیست؟

یکی از معروف‌ترین سیستم‌های تشخیص نفوذ مبتنی بر شبکه است که به دلیل متن باز و رایگان بودن آن، بسیار مورد توجه کاربران قرار گرفته است. نصب Snort بر روی سیستم‌عامل Linux به دو صورت است: نصب با استفاده از نسخه‌های از پیش کامپایل شده و نصب با استفاده از کد منبع امکان پذیر می‌باشد..

پلتفرم های سازگار با نرم افزار Snort:

x86	Sparc	M68k/PPC	Alpha	Other	
X	X	X	X	X	Linux
X	X	X			OpenBSD
X			X		FreeBSD
X		X			NetBSD
X	X				Solaris
	X				SunOS 4.1.X
				X	HP-UX
				X	AIX
				X	IRIX
			X		Tru64
		X			MacOS X Server

Table from: http://www.snort.org/what_is_snort.htm

snort دارای ســـه مـد معروف می باشد:

الف) شنود بسته sniff >> snifer mode

ب) ثبت وقایع بسته logger >> packet logger mode

پ) NIDS (Network Intrusion Detection System) >> این مد ترافیک شبکه را آنالیز و بررسی می کند و از پیچیدگی و قدرت بالایی در پیکربندی برخوردار است.

اگر بخواهید به طور دقیق و حرفه ای ابزار Snort را نصب کنید به دقت مراحل زیر را انجام دهید:

۱) در ابتدا فایل های زیر را نصب کنید:

yum install gcc flex bison zlib libpcap zlib-devel libpcap-devel pcre pcre-devel libdnet libdnet-devel tcpdump

نکته: در صورت نصب نبودن ۲ مخزن Repi و RHEL، یا باید این دو را نصب کنید یا از دیگر سایت ها، فایل های لازم را دانلود کنید.

۲) برای centos از نسخه ۶.۲ به بعد، باید فایل های زیر را از اینترنت پیدا کرده و آنها را نیز نصب کنید :

نکته: فایل های زیر برای ورژن ۶۴ بیتی می باشد، شما جدیدترین ورژن از عناوین زیر را تهیه کنید.

libpcap-devel-1.0.0-6.20091201git117cb5.el6.x86_64.rpm

libdnet-devel-1.12-6.el6.x86_64.rpm

libdnet-debuginfo-1.12-6.choon.centos6.x86_64.rpm

۳) به سایت زیر رفته و بسته های لازم را با توجه به ورژن انتخابی Snort خودتان دانلود کنید:

http://sourceforge.net/projects/snort.mirror/files/

پیشنهاد: اگر در حال کار با ورژن CentOS 6.4 به بالا می باشید، ورژن ۲.۹.۵ را دانلود کنید.

بسته های زیر باید نصب کنید (اگر از این ورژن ها بالاتر باشد بهتر است):

gcc version (4.4.6 including libraries)

flex (2.5.35)

bison (2.4.1)

zlib (1.2.3 including zlib-devel)

libpcap (1.0.0 including libpcap-devel)

pcre (7.84 including pcre-devel)

libdnet (1.11 or 1.12 including libdnet-devel)

tcpdump (4.1.0)

یا:

rpm -qa gcc tcpdump pcre

```
[root@alimp5 ~]#
[root@alimp5 ~]# rpm -qa gcc
gcc-4.4.7-4.el6.x86_64
[root@alimp5 ~]# rpm -qa flex
flex-2.5.35-8.el6.x86_64
[root@alimp5 ~]# rpm -qa bison
bison-2.4.1-5.el6.x86_64
[root@alimp5 ~]# rpm -qa zlib
zlib-1.2.3-29.el6.x86_64
[root@alimp5 ~]# rpm -qa libpcap
libpcap-1.4.0-1.20130826git2dbcaa1.el6.x86_64
[root@alimp5 ~]# rpm -qa pcre
pcre-7.8-6.el6.x86_64
[root@alimp5 ~]# rpm -qa libdnet
libdnet-1.12-6.el6.x86_64
[root@alimp5 ~]# rpm -qa tcpdump
tcpdump-4.0.0-3.20090921gitdf3cb4.2.el6.x86_64
[root@alimp5 ~]#
```

این بسته ها را هم باید دانلود کنید (اگر از این ورژن ها بالاتر باشد بهتر است) :

libpcap-devel-1.0.0-6.20091201git117cb5.el6.x86_64.rpm

libdnet-devel-1.12-6.el6.x86_64.rpm

libdnet-debuginfo-1.12-6.choon.centos6.x86_64.rpm

۴) از اینجا به بعد به طور کامل در سایت زیر توضیح داده شده است:

http://wiki.aanval.com/wiki/Community:Snort_2.9.5.X_Installation_Guide_for_CentOS

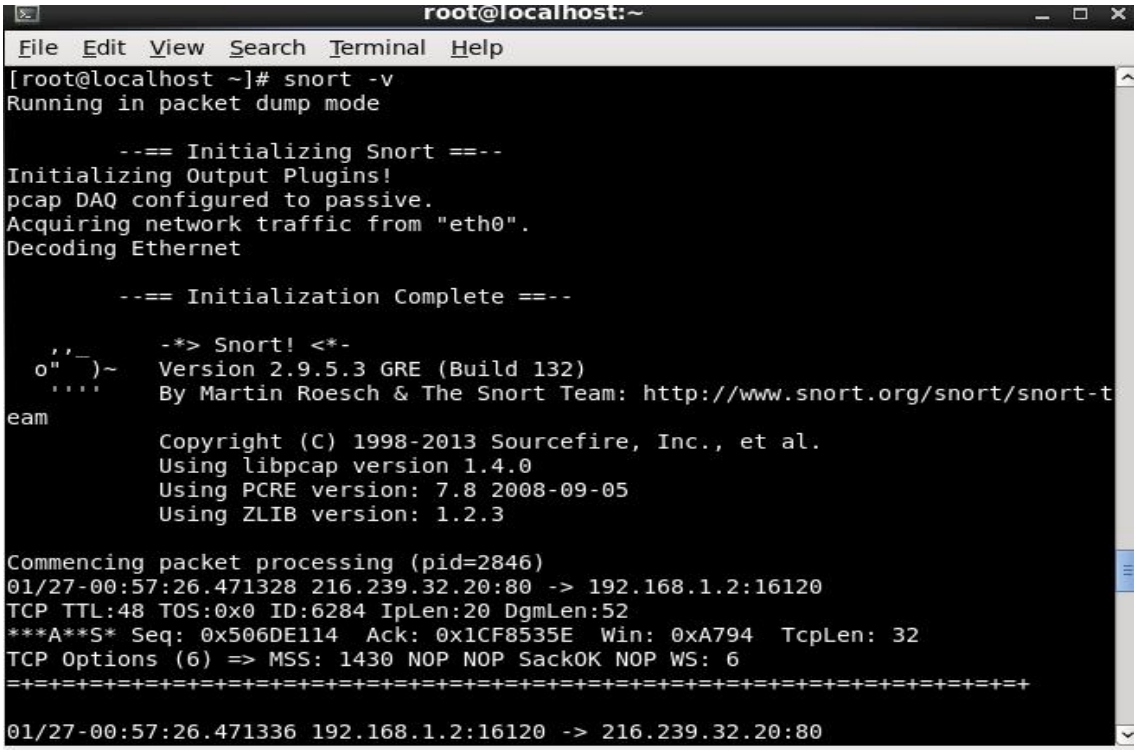
در صورت مشکل با زبان انگلیسی، به سایت "دانشگاه مشهد" مراجعه کنید:

http://cert.um.ac.ir/index.php?r=articles/view&id=7

یا

http://cert.um.ac.ir/index.php?r=fileManager/getFile&id=17

نتیجه نهایی:



نکته مهم: برای لغو کردن کار **snort** باید از **ctrl+c** کیبورد استفاده کنید.

۱) تست کارکرد **snort**:

snort -v -i eth0

به شکل زیر توجه کنید:

```
11/05-18:29:42.554864 192.168.1.2 -> 192.168.1.1
ICMP TTL:64 TOS:0x0 ID:275
ID:63745   Seq:0  ECHO

11/05-18:29:42.554962 192.168.1.1 -> 192.168.1.2
ICMP TTL:255 TOS:0x0 ID:2323
ID:63745   Seq:0  ECHO REPLY

===============================================================
Snort received 6 packets and dropped 0(0.000%) packets

Breakdown by protocol:
    TCP: 0           (0.000%)
    UDP: 0           (0.000%)
   ICMP: 2           (100.000%)
    ARP: 0           (0.000%)
    IPX: 0           (0.000%)
  OTHER: 0           (0.000%)
===============================================================
```

توضیح: در شکل بالا(خط اول) می بینید که یک شخص با ip:192.168.1.2 در حال گرفتن پینگ از ip:192.168.1.1 می باشد.

در خط دوم، ip:192.168.1.1 در حال پاسخ به درخواست ip:192.168.1.2 می باشد.

۲) اطلاعات لایه کاربردی شبکه:

با دستور زیر می توانید متن ها (پسورد) که بین ماشین ها در شبکه در حال جا به جایی است را ببینید:

```
snort -d -v -i eth0
```

۳) اطلاعات اترنت:

با دستور زیر می توانید اطلاعات جزیی مربوط به اترنت مورد نظر خودتان را ببینید:

```
snort -d -v -e -i eth0
```

یا

```
snort -dev -i eth0
```

۴) عمل Logging :

با دستور زیر می توانید لاگ ها را در مسیر /root/log ذخیره کنید:

```
snort -dev -i eth0 -l $HOME/log
```

۵) تشخیص شبکه :

با دستور زیر می توانید هر بسته ایی که به سمت شبکه شما می آید از آن log بگیرید:

```
snort -dev -i eth0 -l $HOME/log -h 192.168.1.0/24
```

۶) استفاده از قانون ها :

یکی از بخش های مهم این ابزار قوانین آن هستند، سایت snort قوانین تجاری برای کارهای حرفه ای هم دارد، که شما باید با توجه به سنسورهایی که نیاز دارید اقدام به خرید کنید. البته برای اینکه خیلی از افراد پی به قدرت قوی این ابزار ببرند، قوانین ساده ای را برای دانلود قرار داده است.

```
snort -dev -i eth0 -l $HOME/log -c rule-file
snort -dev -i eth0 -l $HOME/log -h 192.168.1.0/24 -c rule-file
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

برای کسب اطلاعات بیشتر در مورد snort می توانید به سایت های زیر مراجعه کنید:

http://manual.snort.org/node1.htn

http://openmaniak.com/snort_tutorial_base

http://www.aboutdebian.com/snort.htm

http://www.thegeekstuff.com/2010/08/snor -tutorial/

https://help.ubuntu.com/community/SnortIDS

http://www.cse.sc.edu/~okeefe/tutorials/cert/i042.14.htm

قسمت دوم (Psad):

Psad چیست؟

این نرم افزار به عنوان یک سیستم تشخیص دهنده (IDS) عمل می کند. مخفف کلمه Psad می شود: Detect Port Scan Attacks.

از قدرت بسیار بالایی برخوردار است، و تمام تشخیص ها بستگی به قدرت قانون های اعمال شده روی فایروال و تنظیمات پیکربندی این نرم افزار دارد.

در ابتدا می خواهم یک سایت بسیار عالی برای Rule-Script IPTables معرفی کنم:

این سایت متعلق به آقای Arno می باشد:

http://rocky.eld.leidenuniv.nl/jooom_conte&layo18&Itemid=86

خصوصیات این اسکریپت را ببینید و لذت ببرید:

http://rocky.eld.leidenuniv.nl/jooomle&id=46&Itemid=

نکته: آموزش مربوط به Psad را طبق این اسکریپت توضیح می دهم.

ابتدا نصب فایروال Arno:

۱) دانلود و نصب آن:

```
wget http://rocky.eld.leidenuniv.nl/arno-iptables-firewall/arno-iptables-firewall_2.0.1d.tar.gz
tar zxvf arno-iptables-firewall_2.0.1d.tar.gz
cd arno-iptables-firewall_2.0.1d
./install.sh
```

سپس از شما سوالاتی پرسیده می شود، با توجه به نیاز خود به آنها پاسخ دهید.

۲) به خط 501 در فایل زیر بروید:

```
vi /etc/arno-iptables-firewall/firewall.conf
```

نکته: احتمالا ۱۰ تا ۲۰ خط بالا یا پایین را باید بگردید تا متن زیر را پیدا کنید:

```
#FIREWALL_LOG="/var/log/firewall.log"
```

نتیجه:

FIREWALL_LOG="/var/log/firewall.log"

۳) وارد فایل زیر شوید:

vi /etc/rsyslog.conf

خط زیر را به آن اضافه کنید:

kern.* -/var/log/firewall.log

۴) دانلود و نصب Psad :

wget http://cipherdyne.org/psad/download/psad-2.2.2.tar.gz
cd psad-2.2.2
./install.pl

۵) بعد از نصب Psad، وارد تنظیمات شوید:

vi /etc/psad/psad.conf

نوشتن Email خودتان:

EMAIL_ADDRESSES ali_parkour68@yahoo.com;

یا

EMAIL_ADDRESSES ali_parkour68@yahoo.com,alimp5@irsecteam.org;
HOME_NET any;

اگر یک کارت شبکه دارید:

HOME_NET NOT_USED;

تغییر خط ۵۰۱ زیر :

ENABLE_AUTO_IDS y;

تغییر خط ۱۴۴ زیر:

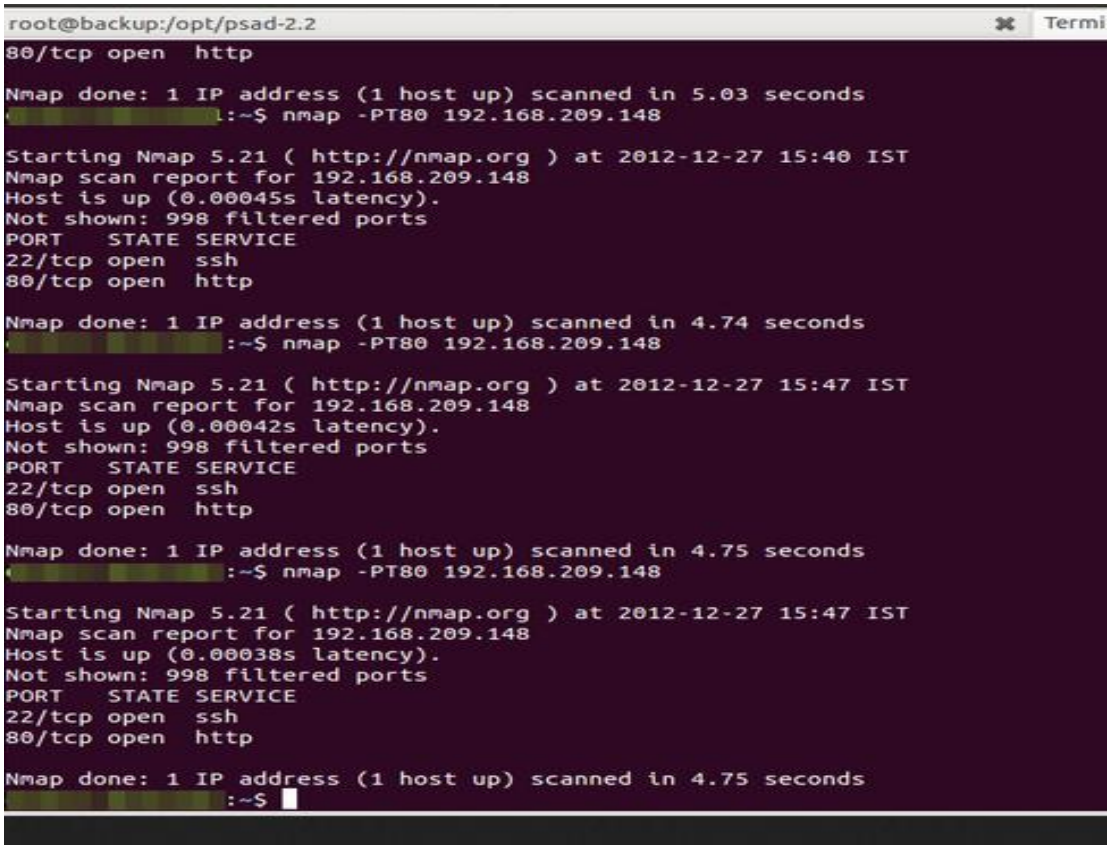
IPT_SYSLOG_FILE /var/log/firewall.log;

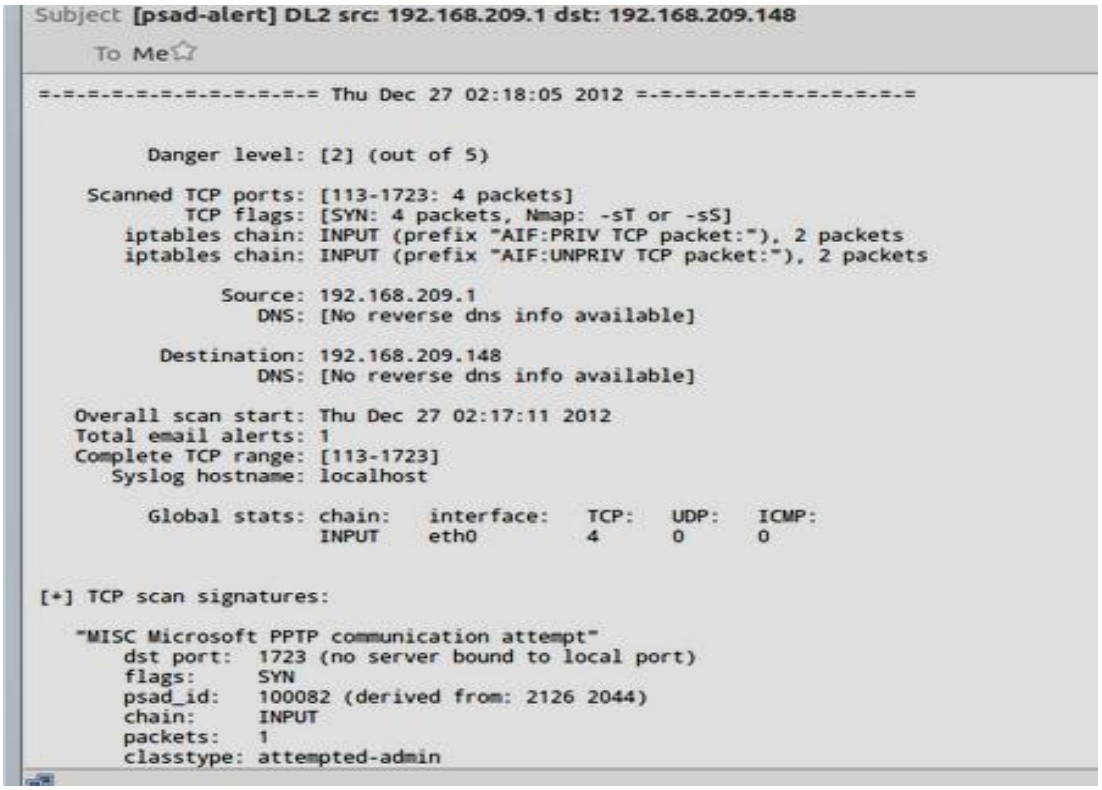
و در نهایت فایل را ذخیره کنید.

سپس:

/etc/init.d/rsyslog restart
/etc/init.d/psad start

نتیجه: پس از اجرای دستور nmap -PT80 192.168.209.148 توسط مهاجم:


root@backup:/opt/psad-2.2
Termi
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
:~$ nmap -PT80 192.168.209.148
Starting Nmap 5.21 (http://nmap.org) at 2012-12-27 15:40 IST
Nmap scan report for 192.168.209.148
Host is up (0.00045s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
:~$ nmap -PT80 192.168.209.148
Starting Nmap 5.21 (http://nmap.org) at 2012-12-27 15:47 IST
Nmap scan report for 192.168.209.148
Host is up (0.00042s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
:~$ nmap -PT80 192.168.209.148
Starting Nmap 5.21 (http://nmap.org) at 2012-12-27 15:47 IST
Nmap scan report for 192.168.209.148
Host is up (0.00038s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
:~$


Subject [psad-alert] DL2 src: 192.168.209.1 dst: 192.168.209.148
To Me
=-=-=-=-=-=-=-=-=-=-=-= Thu Dec 27 02:18:05 2012 =-=-=-=-=-=-=-=-=-=-=-=
Danger level: [2] (out of 5)
Scanned TCP ports: [113-1723: 4 packets]
TCP flags: [SYN: 4 packets, Nmap: -sT or -sS]
iptables chain: INPUT (prefix "AIF:PRIV TCP packet:"), 2 packets
iptables chain: INPUT (prefix "AIF:UNPRIV TCP packet:"), 2 packets
Source: 192.168.209.1
DNS: [No reverse dns info available]
Destination: 192.168.209.148
DNS: [No reverse dns info available]
Overall scan start: Thu Dec 27 02:17:11 2012
Total email alerts: 1
Complete TCP range: [113-1723]
Syslog hostname: localhost
Global stats: chain: interface: TCP: UDP: ICMP:
INPUT eth0 4 0 0
[+] TCP scan signatures:
"MISC Microsoft PPTP communication attempt"
dst port: 1723 (no server bound to local port)
flags: SYN
psad_id: 100082 (derived from: 2126 2044)
chain: INPUT
packets: 1
classtype: attempted-admin

پیشنهاد: اگر سرویس sendmail را نصب کردید، می توانید آن را پاک کنید تا log های مربوط به هر سرویس را مجزا مشاهده کنید.

دستورات کاربردی Psad :

S- : برای نمایش خروجی از رخدادهای Psad.

--fw-rm-block-ip : برای حذف ip از لیست سیاه.

F- : حذف تمام ip های بن شده.

-H psad && --sig-update : به روز رسانی امضاء های Psad.

مثال ها:

```
psad -S
psad --fw-rm-block-ip 9.48.65.150
psad -F
psad --sig-update && psad -H
psad -H
```

نکته: از طریق مسیر زیر می توانید به صورت دستی لیست های سفید و سیاه خود را تغییر دهید:

/etc/psad/auto_dl

برای کسب اطلاعات بیشتر در مورد Psad می توانید به سایت های زیر مراجعه کنید:

http://www.cipherdyne.org/psad/docs/config.html

http://linuxdrops.com/install-arno-firewall-with-psad-iptables-on-steroids/

http://www.pontikis.net/blog/psad-install-config-debian-wheezy

http://marc.info/?l=psad-discuss&m=121807386229970

http://www.cyberciti.biz/faq/linux-detect-port-scan-attacks/

پیکربندی SELinux :

به Security Enhanced linux یا همان " امنیت پیشرفته لینوکس" معروف است و یکی از لایه های امنیتی در سیستم عامل های لینوکس است که از طرف NSA(National Security Agency) توسعه یافته است. خیلی از کاربران لینوکسی برای کاهش مشکلات خودشان این سرویس را غیر فعال می کنند تا راحت تر کارهای خودشان را انجام دهند.، آیا این کار درست است؟ جواب من: کار چندان درستی نیست.

کسانی که به طور حرفه ای با بحث امنیت در لینوکس کار می کنند بیشتر با این ۲ مد خود را درگیر می کنند:

Permissive: از این مد بیشتر در عیب یابی (Troubleshooting) استفاده می شود.

ارزش عدد صفر= قرار گرفتن در مد permissive .

Enforcing

ارزش عدد یک= قرار گرفتن در مد Enforcing .

و مد آخر در selinux :

Disabled

دستورات کار با SELinux :

-1 getenforce

sestatus -2

v- : یک خروجی کلی از SELinux را نمایش می دهد.

b- : برای نمایش وضیعت ارزش بولین ها استفاده می شود.

دو دستور بالا برای نمایش وضیعت مد SELinux به کار می روند:

```
root # getenforce

  Enforcing
```

```
root # sestatus

  SELinux status:                 enabled
  SELinuxfs mount:                /sys/fs/selinux
  SELinux root directory:         /etc/selinux
  Loaded policy name:             strict
  Current mode:                   enforcing
  Mode from config file:          enforcing
  Policy MLS status:              disabled
  Policy deny_unknown status:     denied
  Max kernel policy version:      28
```

3- setenforce : برای تغییر مد به کار می رود

setenforce 1

4- getsebool : برگرداندن و نمایش ارزش بولین ست شده برای سرویس(ها).

getsebool httpd_can_network_connect_db

نتیجه:

httpd_can_network_connect_db --> off

مثال۱:

getsebool -a | grep http

```
# getsebool -a | grep http
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> on
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> off
httpd_execmem --> off
httpd_read_user_content --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_tmp_exec --> off
httpd_tty_comm --> on
httpd_unified --> on
httpd_use_cifs --> off
httpd_use_gpg --> off
httpd_use_nfs --> off
```

5- setsebool : برای تغییر دادن ارزش بولین سرویس (ها) و تعیین نوع عملکرد استفاده می شود.

setsebool httpd_can_network_connect_db on

نکته ۱: این نام یک ماژول است: httpd_can_network_connect_db

به صورت پیشفرض هم توسط SELinux غیرفعال است و این کار از اجرا شدن یک سری اسکریپت برای وصل شدن به HTTP(Apache) و دیتابیس سرور ما جلوگیری می کند.

نکته۲: عدد صفر برابر off است ،،، و عدد یک برابر on می باشد.

برای درک بیشتر از ارزش های بولین سرویس ها می توانید به سایت زیر مراجعه کنید:

e_Linux/6/html/Security-Enhanced_ith_SELinux-Booleans.html

https://access.redhat.x-Working_with_SELinux.html

5- semanage : یک توضیح مختصری از هر ماژول با توجه به ارزش بولی آنها می دهد.

مثال ۱ :

semanage boolean -l | grep http

```
# semanage boolean -l | grep http
httpd_can_network_relay         -> off   Allow httpd to act as a relay
httpd_can_network_connect_db    -> off   Allow HTTPD scripts and modules to
connect to databases over the network.
httpd_use_gpg                   -> off   Allow httpd to run gpg in gpg-web
domain
httpd_enable_cgi                -> on    Allow httpd cgi support
httpd_use_cifs                  -> off   Allow httpd to access cifs file
systems
allow_httpd_mod_auth_pam        -> off   Allow Apache to use mod_auth_pam
allow_httpd_anon_write          -> off   Allow Apache to modify public files
used for public file transfer services.  Directories/Files must be labeled
public_rw_content_t.
httpd_enable_homedirs           -> off   Allow httpd to read home directories
allow_httpd_sys_script_anon_write -> off   Allow apache scripts to write to
public content. Directories/Files must be labeled public_rw_content_t.
httpd_dbus_avahi                -> on    Allow Apache to communicate with avahi
service via dbus
httpd_unified                   -> on    Unify HTTPD handling of all content
files.
httpd_can_network_connect       -> off   Allow HTTPD scripts and modules to
connect to the network using TCP.
allow_httpd_mod_auth_ntlm_winbind -> off   Allow Apache to use mod_auth_pam
httpd_tty_comm                  -> on    Unify HTTPD to communicate with the
terminal. Needed for entering the passphrase for certificates at the terminal.
httpd_read_user_content         -> off   Allow httpd to read user content
httpd_use_nfs                   -> off   Allow httpd to access nfs file systems
```

مسیر ذخیره پیکربندی فایل SELinux :

/etc/selinux/config

برای کسب اطلاعات بیشتر در مورد SELinux می توانید به سایت های زیر مراجعه کنید:

http://wiki.centos.org/HowTos/SELinux

https://access.redhat.com/site/documentationbleshooting.html

http://www.centos.org/docs/5/html/Deployment_Guid_-en-US/sec-sel-admincontrol.html

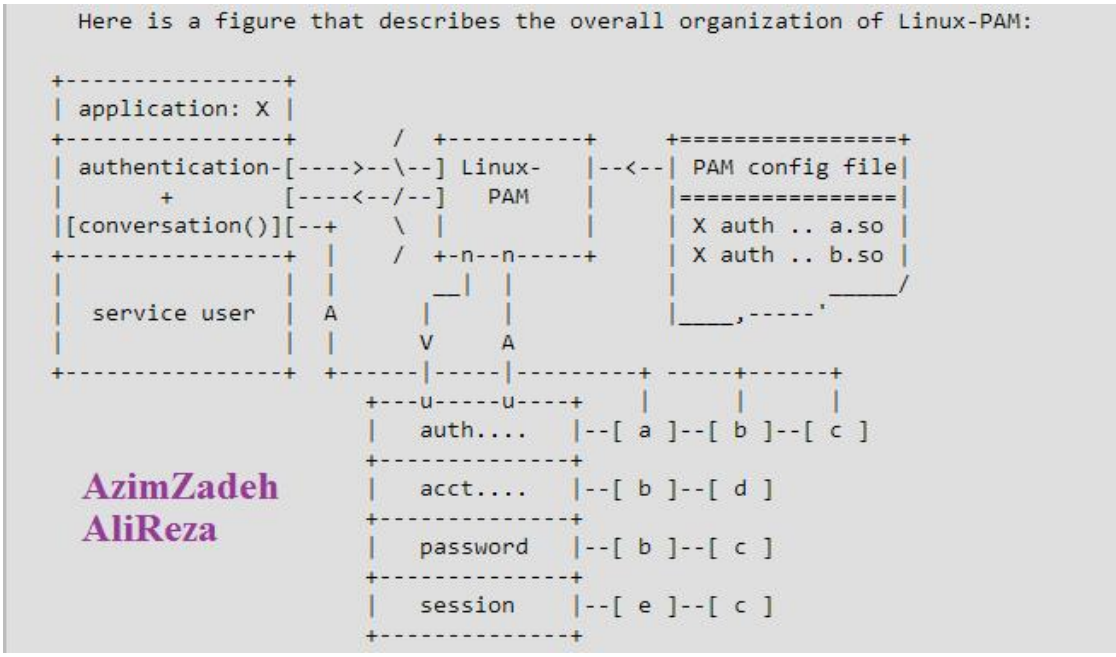
http://docs.oracle.com/cd/E37670_01/E36387/html/ol_selinux_sec.htm

کار با ماژول Pluggable Authentication Modules (PAM) :

یکی از ماژول های بسیار قوی برای ایجاد امنیت در لینوکس برای جدا کردن بخش ها مدیریتی از هم و کنترل راحت تر آنها نسبت به هم، مثل:

مدیریت اعتبار(تایید هویت)	(authentication management)
مدیریت حساب ها	(account management)
مدیریت جلسه ها	(session management)
مدیریت پسورد ها	(password management)

شکل زیر بیانگر قدرت این ماژول می باشد:



نکته: مسیر ذخیره پیکربندی های مربوط به ماژول PAM و کتابخانه های آن در مسیرهای زیر قرار دارد:

/etc/pam.d

/etc/security

/lib/security

/lib64/security

نکته: اگر بسته زیر را هم نصب کنید خالی از لطف نیست:

```
sudo yum install pam-devel
```

اخطار: قبل از کار با این ماژول، از تمام فولدرهای بالا یک پشتیبان تهیه کنید تا در صورت مشکل آنها را به حالت اول خود برگردانید.

syntax قوانین PAM بدین صورت است:

servicename servicetype control modulepath moduleargumentsservicename: اسم برنامه مورد نظر ما می باشد، مثل: su , crond

Servicetype: گروه های مدیریتی ما می باشند که برای قوانین استفاده می شوند.این گروه ها عبارتند از:

۱. Account :

این ماژول برای تایید و بررسی دسترسی مجاز است. مثل: بررسی یک حساب کاربری که عمرش به پایان رسیده است یا خیر؟ و یا بررسی اینکه یک نام کاربری در یک روز خاص حق دسترسی به سیستم را دارد.

۲. Auth :

این رابط ماژول برای احراز هویت است. مثل: بررسی اعتبار یک پسورد.

۳. Password :

این رابط ماژول برای تغییر پسوردهای کاربران استفاده می شود.

۴. Session :

این رابط ماژول برای پیکربندی و مدیریت جلسه (نشست)های کاربر است.

Control: بخشی از یک قانون است که برای ارزیابی و کنترل قانون مورد نظر استفاده می شود.این بخش ها عبارتند از:

۱) required

حاصل این flag-control اگر با موفقیت همراه باشد، حتی در مواجه با شکست نیز ادامه می دهد.

۲) requisite

در صورت مواجه شدن با شکست متوقف می شود.

۳) sufficient

اگر ماژول های flag-required با شکست مواجه نشوند، و اگر این ماژول در نتیجه به موفقیت برسد، اجازه دسترسی خواهد داشت.

۴) optional

۵) include

۶) binding

modulepath: مسیر برنامه است. به صورت پیشفرض این مسیر وجود دارد:

/lib/security

moduleargumentsآرگومان هایی که به ماژول ها ارسال می شوند.:

مثل: db

Auth required pam_userdb.so db=/path/to/BerkeleyDB_file

برای کسب اطلاعات بیشتر در مورد مطالب بالا می توانید به سایت های زیر مراجعه کنید:

http://www.freebsd.org/doc/en/articles/pam/pam-essentials.html

http://www.linux-pam.org/Linux-PAM-html/old/pam-4.html

مثال۱: فرض کنید یک کاربر می خواهد سیستم را با دستور reboot سیستم را Restart کند:

```
[root@MyServer ~]# cat /etc/pam.d/reboot
#%PAM-1.0
auth       sufficient   pam_rootok.so
auth       required     pam_console.so
#auth      include      system-auth
account    required     pam_permit.so
```

توضیح خط های بالا:

۱. auth sufficient pam_rootok.so:

این خط از ماژول pam_rootok.so برای چک کردن نام کاربری استفاده می کند که ببیند آیا در درجه root هست یا خیر؟

اگر UID=0 باشد، خط های بعدی تست نمی شوند و دستور reboot اجرا می شود. در غیر این صورت خط بعدی مورد بررسی قرار می گیرد.

۲. auth required pam_console.so:

این خط از ماژول pam_console.so برای تایید هویت کاربر تلاش می کند.

مثال۲: توضیح ۳خط زیر برای درک بیشتر از مفاهیمی که در بالا توضیح داده ام:

```
auth       required     pam_moduleA
auth       sufficient   pam_moduleB
auth       required     pam_moduleC
```

Pam...A اگر با شکت مواجه شود و ماژول Pam...B با موفقیت مواجه شود، در نهایت دسترسی ممنوع خواهد بود.

دسترسی وقتی خواهد بود که یا ((Pam...A و Pam...B به موفقیت ختم شوند)) و یا اینکه: Pam...A و Pam...C با هم به موفقیت ختم شوند.

مثال۳: توضیح ۳ خط زیر برای درک بیشتر از مفاهیمی که در بالا توضیح داده ام:

```
auth       sufficient   pam_moduleB
auth       required     pam_moduleA
auth       required     pam_moduleC
```

وقتی به دسترسی خواهیم رسید که یا ((Pam...B به موفقیت ختم شود)) و یا اینکه Pam...A و Pam...C با هم به موفقیت ختم شوند.

افزایش امنیت SSH با Captcha:

اگر تمایل دارید به در کنار استفاده از password ، ازCaptcha نیز برای ورود به سیستم استفاده کنید، این بخش را حتما بخوانید.

این کار باعث می شود شما دو لایه امنیتی بر روی SSH خود ایجاد داشته باشید و امنیت آن بیشتر باشد.

نکته مهم: آموزش کار با این ابزار را در اینجا برای شما عزیزان قرار می دهم. ولی برای استفاده از این ماژول باید آن را بخرید.

هزینه خرید: ۵۰۰۰ هزار تومان می باشد. راه های خرید:

الف) با ایمیل نویسنده در ارتباط باشید: ali_parkour68@yahoo.com

ب) به قسمت فروش "http://mihanuptime.com " مراجعه کنید.

نکته: مطمئن شوید که مخازن Remi و EPEL را نصب کرده اید.

اخطار: از فایل SSHD مسیر /etc/ssh/sshd.config پشتیبان تهیه کنید.

۱. ابتدا بسته های زیر را نصب کنید:

```
yum install figlet gcc pam-devel
```

۲. در ادامه نیاز به بسته OpenPAM داریم:

از سایت زیر آخرین نسخه آن را دانلود و نصب کنید:

http://www.openpam.org/downloads

نصب openpam:

```
./configure
```

یا

./configure --with-pam-unix --with-su

سپس:

sudo make

sudo make install

۳. بعد از خرید و دریافت فایل، آن را از حالت فشرده خارج کنید.

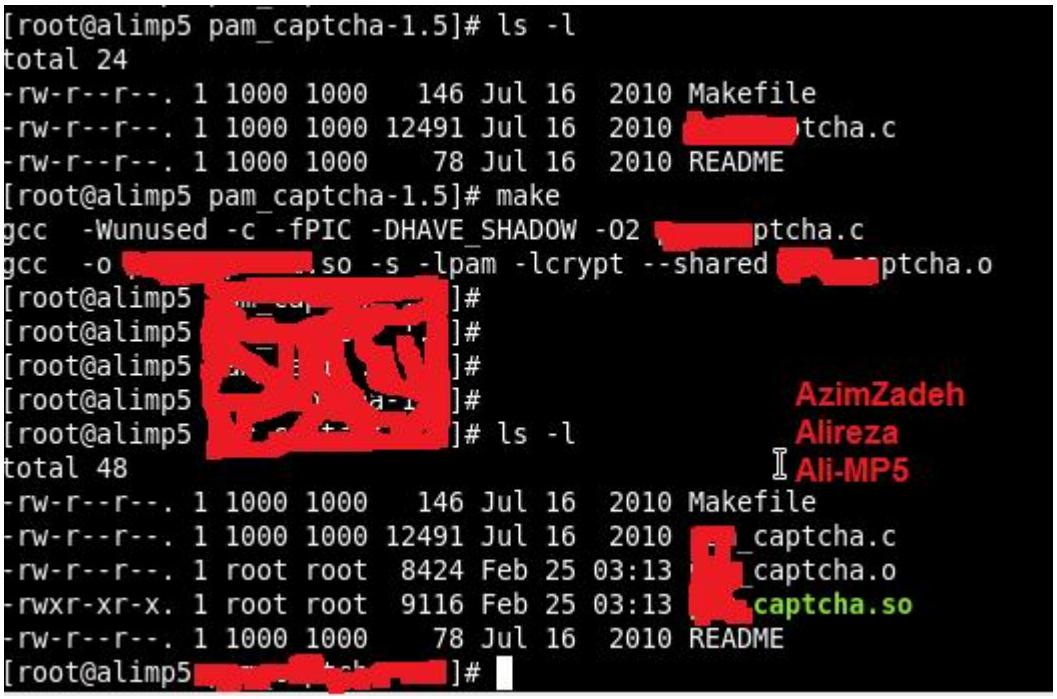
سپس وارد مسیر فایل شوید و دستور زیر را بنویسید:

make

بعد از نصب فایل، باید فایلی که نام آن pam_captcha.so است را در مسیر زیر کپی کنید:

/lib/security

/lib64/security



۴. برای فعال کردن captcha نیاز به کمی تغییرات در فایل sshd_config داریم:

خط های زیر را پیدا کرده و آنها را بدین شکل در فایل اعمال کنید (نتیجه):

PasswordAuthentication no

ChallengeResponseAuthentication yes

service sshd restart

۵. در آخر هم باید کمی تغییرات در sshd pam.d ایجاد کنیم.

vi /etc/pam.d/sshd

خط زیر را به ابتدای این فایل اضافه کنید:

auth required pam_captcha.so math randomstring

و در نهایت فایل را ذخیره کنید.

نکته: اگر نتیجه ای حاصل نشد، سیستم را Restart کنید و سپس از طریق کانکشن ssh برای اتصال به سرور تلاش نمایید.

نتیجه کار:

برای کسب اطلاعات بیشتر در مورد PAM می توانید به سایت های زیر مراجعه کنید:

http://susefaq.sourceforge.net/howto/pam.html

http://wpollock.com/AUnix2/PA -Help.htm

http://pig.made-it.com/pam.html

http://www.cyberciti.biz/tips/centos-redhat-vsftpd-ftp-with-virtual-users.html

http://www.mylinuxguide.com/pam-login-notification-centos/

http://www.cyberciti.biz/tips/rhel-centos-fedora-linux-log-failed-login.html

http://xmodulo.com/2013/04/hov -to-monitor-failed-ssh-login-attempts-on-centos.html

https://access.redhat.com/n_Files-PAM_Service_Files

بخش دوم:

به چند دلیل، ادامه فصل های این کتاب را در جلد بعدی قرار می دهم.

دلیل اول: تا این قسمت از کتاب ۱۶۰ صفحه توسط اینجانب ترجمه و تألیف شده، اگر می خواستم تمام فصل ها را بنویسم تقریبا بالای ۲۸۰ صفحه می شد و زیاد بودن تعداد صفحات برای مخاطب کمی خسته کننده به نظر می رسد و شاید این کار مخاطب را از خواندن کتاب دلسرد کند.

دلیل دوم: با این کار خواستم، به کار ویرایش در کنار نوشتن سرعت بدهم. چرا؟ جواب: اگر دوستان با مشکلی فنی مواجه شدند به اینجانب اطلاع دهند تا در حین نوشتن فصل های بخش دوم، فصل های بخش اول را ویرایش کنم.

نکته مهم: تا آخرین لحظه نوشتن، سعی کردم لینک های ارائه شده را پیوسته بررسی کنم، به همین خاطر احتمال وجود خطا بسیار کم است.

دلیل سوم: نوشتن فصل های این بخش ملزم به داشتن یک VPS قوی، لایسنس از پنل های مختلف و... غیره می باشد. امیدوارم با یاری شما عزیزان بتوانم کار تألیف و ترجمه این کتاب را با موفقیت به پایان برسانم.

مطالب بخش دوم:

Time-Zone

Hardware-Clock

NTP

X.org

XDMCP Remote Connections

Static/Dynamic IP-Address

bind multiple IP addresses to a single Ethernet device

Bonding Ethernet devices

HostName and Domain Name(FQDN)

Samba

Working with FTP

Working with NFS

Working with Domains

Working with File Server

Working with DHCP Server

Working with Virtualization

Working with Directory Services

Providing Mail Services

Secure Web Servers

Extra Firewalls(CSF, PHPsecInfo, APF, ...) and .....

Working with Databases, MySQL and .....

Working with Web Servers, Panels(Cpanel, DirectAdmin, ...) and .....

Working With Apache, LightSpeed and .....

کتاب های ترجمه و تألیف شده:

دوستان علاقه مند در زمینه هک و امنیت می توانند کتاب "هک و امنیت با BackTrack5-R3" که توسط اینجانب ترجمه و تألیف شده را نیز مطالعه کنند.

لینک مستقیم:

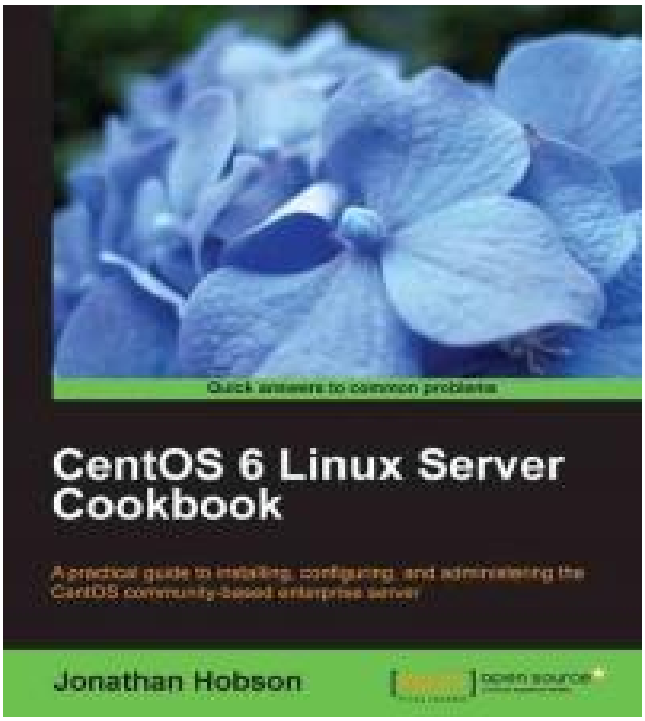
http://forum.irsecteam.org/forum86/thread1114.htm

http://aliazimzadeh.blogfa.com/

منابع و مراجع:

به جرأت می توان گفت: این کتاب یکی از بهترین کتاب های فارسی ترجمه و تألیف شده در زمینه لینوکس می باشد.

بدین خاطر این مطلب را می گویم که، صفر تا صد کتاب های زیر را مطالعه کرده ام و کاربردی ترین مطالب را برای شما عزیزان جمع آوری کرده ام.



Publisher: Packt Publishing

By: Jonathan Hobson

ISBN: 978-1-84951-902-1

Year: 2013

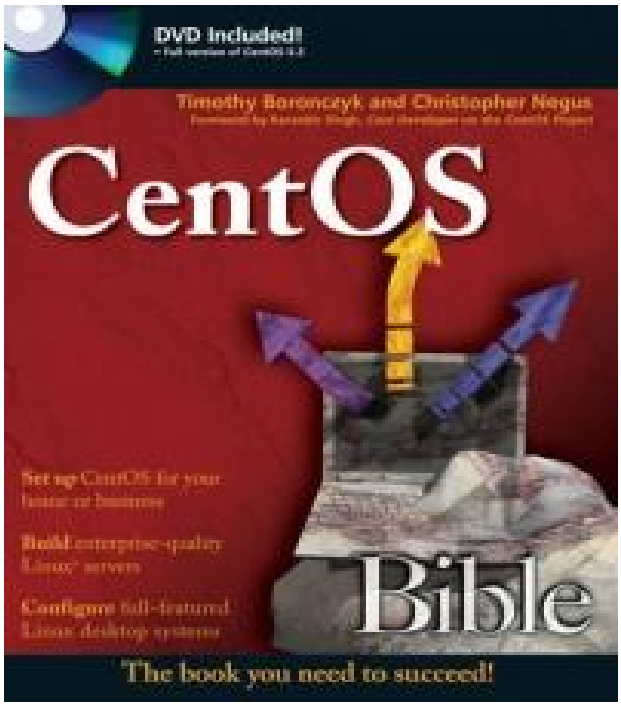
First published: April 2013

Pages: 374

Language: English

Description:

CentOS is a community-based enterprise class operating system and this book will provide a series of practical solutions that will not only show you how to install and maintain CentOS as a server, but to explore this well-known Linux distribution with the intention of tackling many common issues by providing some tricks of the trade in order to simplify the task of building a server. CentOS 6 Linux Server Cookbook is a practical guide to installation, configuration, administration, and maintenance. This is a one-stop-shop to all things CentOS, so regardless as to whether you need a mail server, web server, database server, domain server or a file sharing platform, this book provides a comprehensive series of starting points that will give you direct access to the inner workings of this open source, community-based enterprise server.



Publisher: Wiley

By: Christopher Negus, Timothy Boronczyk

ISBN: 978-0-470-48165-3

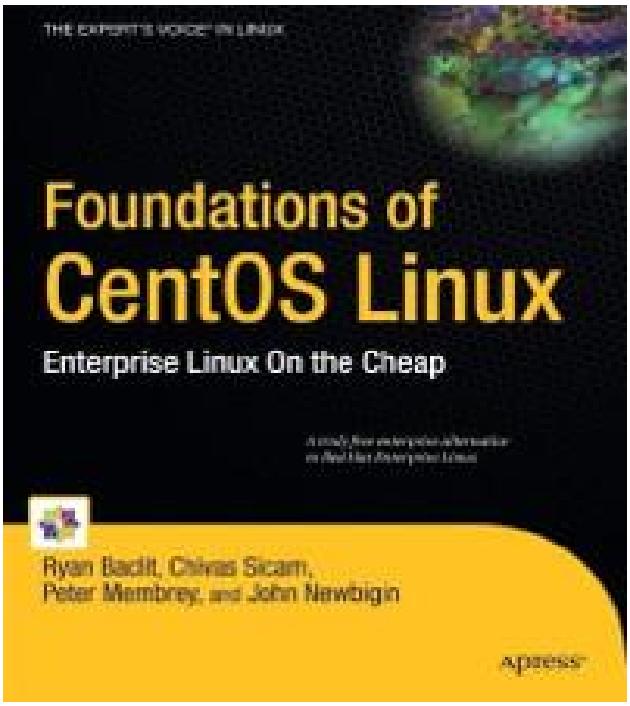
Year: 2009

Pages: 984

Language: English

Description:

This is one of the first, if not the first comprehensive guide to the CentOS Linux operating system. First find out how to install and configure CentOS. From there, you'll cover a wealth of Linux and CentOS tools, functions, and techniques, including: how to work in the GNOME and KDE desktop environments; how to use the Linux shell, file system, and text editor; how to configure CUPS printers, Samba for file and printer sharing and other features using GUI tools; and more.



Publisher: Apress

By: Ryan Baclit, Chivas Sicam, Peter Membrey, John Newbigin

ISBN: 978-1-4302-1964-4

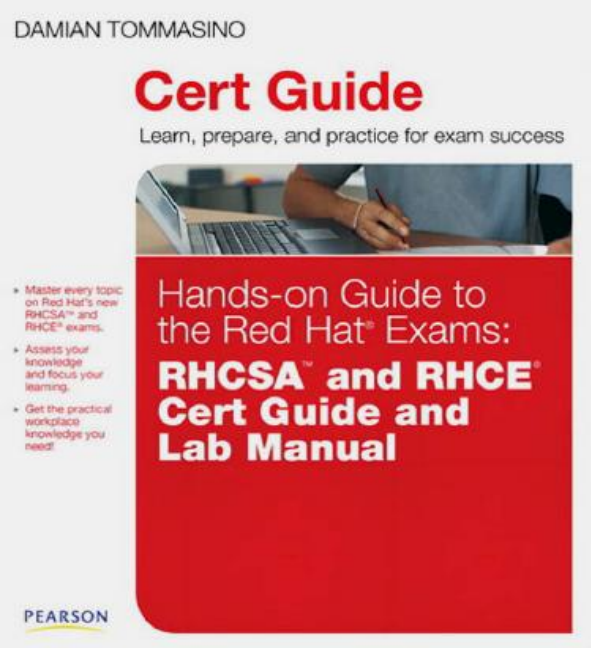
Year: 2009

Pages: 528

Language: English

Description:

You need to maintain clients, servers and networks, while acquiring new skills. Foundations of Cent OS Linux: Enterprise Linux On the Cheap covers a free, unencumbered Linux operating system within the Red Hat lineage, but it does not assume you have a Red Hat Enterprise Linux license. Now you can learn CentOS Linux, the most powerful and popular of all Red Hat clones, keep maintaining your network at work, and become an Red Hat Certified Engineer, all just for the cost of this book.



Publisher: Pearson

By: Damian Tommasino

ISBN-10: 978-0-321-76795-0

ISBN-13: 0-321-76795-0

Year: 2011

First published: May 2011

Pages: 536

Language: English

Description:

This is the eBook version of the printed book.

This certification guide to the Red Hat RHCSA (EX200) and RHCE (EX300) exams gives candidates all the hands-on practice they need, through a series of more than 20 realistic, detailed labs. These exceptionally thorough labs are task based, similar to what might be encountered on the exams. This will give readers the background they need to perform key tasks, and get the results they're trying to achieve. Built from content originally published on the author's popular blog, Security Nut, this book reflects extensive input and feedback from IT professionals and exam candidates. It is organized to help readers learn incrementally, and quickly find the related information they need. Each section logically flows in the order you would accomplish tasks when setting up or configuring a system. The author provides tutorials for administrators at all levels of experience, dozens of real-world tips, and a set of downloadable scripts designed to give students hands-on problem-solving experience.

پیوست ها و ضمائم :

همانند کتاب "هک و امنیت با بکترک" در اینجا نیز می خواهم کتاب های ترجمه و تألیف شده در زمینه لینوکس را معرفی کنم تا مشتاقان کار با لینوکس بتوانند اِن شاء الله در کوتاه ترین زمان ممکن، بیشترین بهره را از مطالب کتاب ها ببرند.

نام کتاب: آموزش لینوکس ردهت ۹

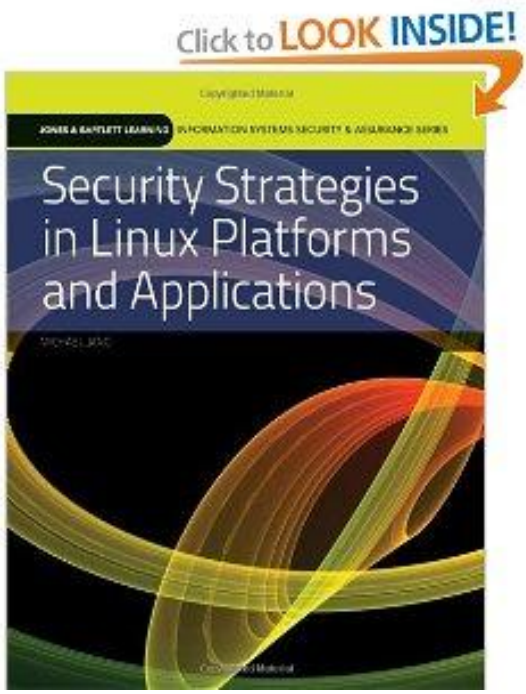
نویسنده: آلن باغومیان

تاریخ انتشار: آبان – ۱۳۸۲

تعداد صفحات: ۲۵۰

لینک دانلود:

http://www.EDHAT-9%29.html



نام کتاب: security strategies in Linux platforms

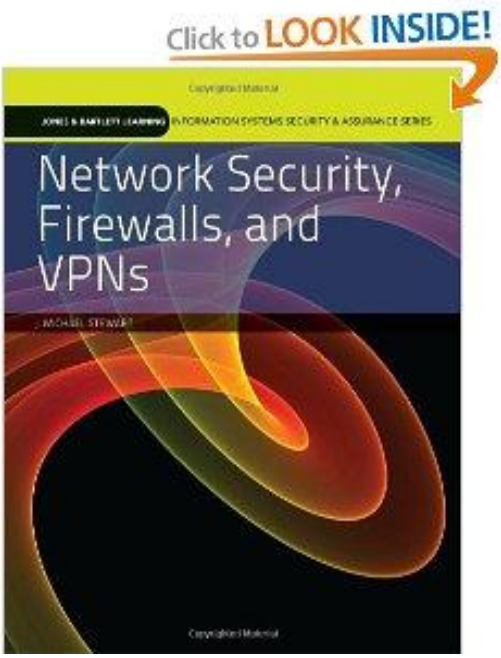
نویسنده: Dan Barrett

تاریخ انتشار: September 3, 2010

تعداد صفحات: 512

لینک:

http://www.amaecurity



نام کتاب: **network security, firewalls, vpn's**

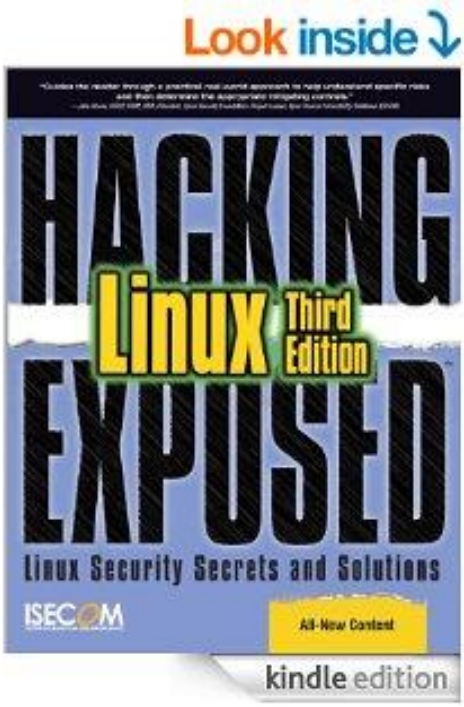
نویسنده: **Jones & Bartlett**

تاریخ انتشار: **August 27, 2010**

تعداد صفحات: **482**

لینک:

http://www.amS8D913KH



نام کتاب: **hacking exposes Linux, third edition**

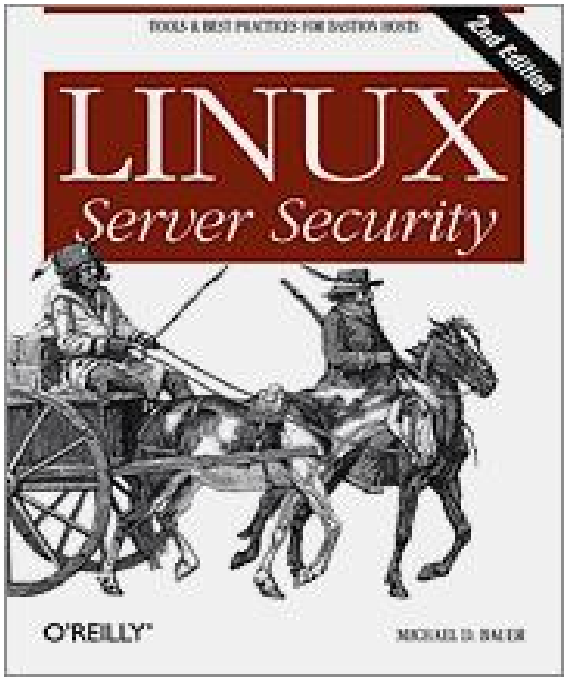
انتشارات: **ISECOM**

تاریخ انتشار: **July 15, 2008**

تعداد صفحات: **614**

لینک:

http://www.amok/dp/B0013TRRV



نام کتاب: **Linux Server Security, 2nd Edition**

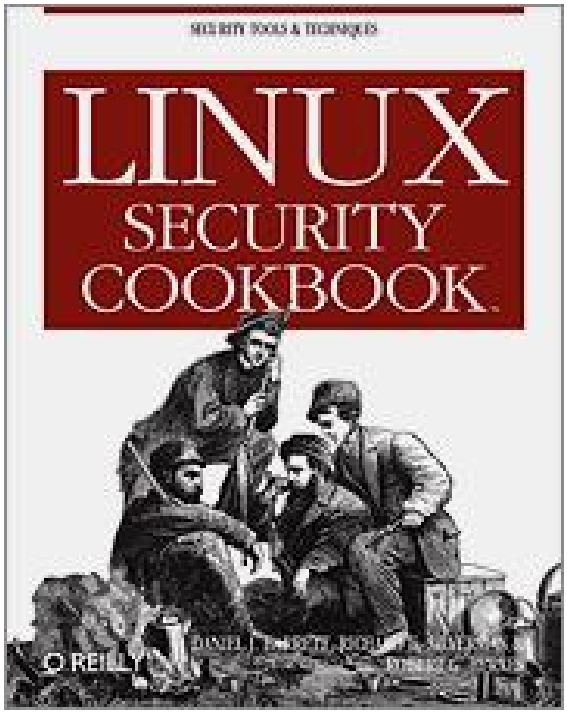
نویسنده: **Michael D. Bauer**

تاریخ انتشار: **January 2005**

تعداد صفحات: **544**

لینک:

http://www.oreilly.com/catalog/linuxss



نام کتاب: **Linux Security Cookbook**

نویسنده: **Dan Barrett**

تاریخ انتشار: **June 9, 2003**

تعداد صفحات: **352**

لینک:

http://www.amy+cookbook

معرفی فروم و کتب الکترونیکی:

www.irsecteam.org

http://www.mihansetup.com

http://it-ebooks.info/

http://www.pa%A9%D8%E

http://radio110.blogfa.com/po -1207.aspx

http://www.shabakeh-mag.com/article.aspx?id=100522

http://www.e-booksdirectory.com/listing.php?category=2

http://royal.pingdom.com/2012/02/24/1(-free-linux-e-books/