امنیت در سیستم عامل لینوکس

منصور سیدی

امروزه در دنیایی متکی بر فناوری اطلاعات زندگی می‌کنیم که هر لحظه به خطر افتادن جریان اطلاعات منجر به بروز خسارت‌های تجاری جبران ناپذیری خواهد شد. امروزه همه به دنبال یک سکوی (Platform) امن‌تر برای اجرای برنامه‌های کاربردی و سروی‌دهنده‌ها هستند. لینوکس حرف‌های زیادی برای گفتن در سمت امنیت دارد. بسیاری از قابلیت‌های امنیتی که در ویندوز وجود ندارند و یا فقط با اضافه کردن نرم‌افزارهای اضافی قابل دسترسی می‌باشند، بطور درونی و پیش‌گزیده در لینوکس پیاده سازی شده‌اند. لینوکس از ابتدا برای محیط‌های شبکه‌ای و چند کاربره طراحی شده است و همین باعث رعایت مسائل امنیتی از ابتدا در ان شده است، درحالی که ویندوز اینگونه نبوده و درحال حاضر نیز از نظر امنیتی دارای نقاط ضعف فراوانی است. مثلا یک برنامه مخرب با استفاده از همین ضعف‌های امنیتی می‌تواند کل سیستم‌عامل را نابود کند، ولی در صورتی که مورد مشابهی در لینوکس وجود داشته باشد، حداکثر به دایرکتوری خانگی کاربر اجرا کننده آسیب خواهد رسید، نه کل سیستم‌عامل.

مقدمه:

اینطور نیست که لینوکس فاقد هر گونه اشکال امنیتی باشد، خیر، ولی باز بودن کد منبع آن باعث می‌شود تا بسیاری از اشکالات امنیتی پیش از ایجاد خسارت و در مراحل توسعه و برنامه نویسی برنامه بر ملا شده و رفع شوند. در صورتی که اشکالی نیز در برنامه‌های منتشر شده یافت شود، بدلیل موجود بودن کد منبع سریعا برطرف می‌گردد. در صورتی که در سیستم عامل ویندوز شما باید منتظر مایکروسافت بمانید و بمانید و بمانید. سیستم‌عامل ویندوز دارای اشکالات امنیتی بسیاری است که به راحتی هم کشف نمی‌شوند و هنگامی کشف می‌شوند که خسارات جبران ناپذیری در اثر حمله از طریق آن ضعف‌های امنیتی رخ دهد که امثال آنرا شاهد هستیم.

می‌توان ادعا کرد که تقریبا هیچ ویروسی برای لینوکس وجود ندارد و این درحالی است که سالیانه بیش از ۱۰۰۰ ویروس و کرم مختلف برای سیستم‌عامل ویندوز ایجاد می‌شود. این بخاطر عدم گسترده بودن لینوکس نیست (حدود ۷۰ درصد از سایت‌های وب در جهان بر روی سیستم‌عامل لینوکس و سرویس‌دهنده وب آپاچی درحال اجرا هستند) بلکه بدلیل وجود حفره‌های امنیتی متعدد ویندوز و سیاست انحصار گرایی مایکروسافت است. یعنی چه؟ مایکروسافت طوری رفتار و سیاست گذاری کرده است که مشتریان خود را تنها به محصولات خودش عادت دهد. بسیاری از کاربران ویندوز از اینترنت اکسپلورر و آتلوک برای مرور وب و پست الکترونیک استفاده می‌کنند. من به عنوان یک ویروس نویس، می‌دانم که اگر ویروسی را برای کاربران ویندوز بنویسم، بر روی کامپیوترهای ۹۰ درصد آنها اثر خواهد کرد. چون اکثرا ازIE وOutlook استفاده می‌کنند. ولی در لینوکس چطور؟ در لینوکس شما طیف وسیعی از انتخاب و عدم اجبار دارید. من از مرورگر موزیلا استفاده میکنم. دوستی دارم کهKonqueror را ترجیح می‌دهد. دیگری از Operaاستفاده می‌کند. من ازKmail استفاده می‌کنم. دوستم ازEvolution ، دیگری ازPine و بعدی از Muttو برادرم هم از.MozillaMail من فقط می‌توانم برای یکی از اینها ویروس بنویسم چون روی بقیه کار نخواهد کرد و عملا میزان اثر آن انداک خواهد بود. ضمنا هیچیک از ویروس‌هایی که برای ویندوز نوشته شده‌اند، بر روی لینوکس کار نمی‌کنند.

لینوکس : تعداد سکوهای اجرایی

لینوکس برخلاف ویندوز بر روی تعداد زیادی از سکوهای مختلف سخت‌افزاری اجرا می‌شود و شما حتی قادرید آنرا برای کار بر روی سکوی مورد نظرتان تغییر دهید. این قابلیت، لینوکس را برای بکارگیری در سخت‌افزارهای درونه‌ای (Embedded)بسیار مناسب می‌سازد. هسته ۲،۶ لینوکس که بتازگی ارائه شده است، این امکان را فراهم می‌سازد تا لینوکس را بر روی دستگاه‌های بسیار کوچک و یا ابر رایانه‌های بسیار بزرگ اجرا نمایید. اصلا ویندوز می‌تواند؟

لینوکس : گسترده‌ترین تنوع در کاربرد

لینوکس را می‌توانید برای انجام وظایف بسیار متعددی بکار بگیرید. از دستگاه چک کردن اتصالات شبکه، دیوار آتش، مسیریاب (Router) شبکه، سرویس‌دهنده‌های مختلف مانند وب، بانک اطلاعاتی، فایل، چاپ و...، میزهای کار (Desktop)، ایستگاه‌های کاری (Workstations) و... سیستم‌عامل لینوکس حتی این امکان را دارد که از آن بتوان به صورت یک سیستم زنده و پرتابل استفاده کرد .به این معنی که کل سیستم‌عامل از روی یک دیسکCD اجرا شود و شما آنرا با خودتان جابجا کنید و میزکار و تنظیماتتان را همراه خودتان منتقل کنید .علاوه بر این، این قابلیت برای رفع اشکال و نمایش آن نیز بسیار مفید است.

لینوکس : تنوع در انتخاب

بدلیل آزاد بودن سیستم‌عامل لینوکس، هر گروه یا موسسه تجاری، یک نسخه خاص از آن که به توزیع یا پخش (Distribution)معروف هستند، منتشر ساخته است. این توزیع‌های مختلف همگی لینوکس هستند، ولی هریک معمولا برای یک یا چند امر خاص مانند سرویس‌دهنده، دیوار آتش، میزکار و... طراحی شده‌اند و هریک قابلیت‌ها و بهینه سازی‌ها خاص خودشان را به کاربران ارائه می‌کنند .کاربران در این میان آزادی انتخاب زیادی داشته و می‌توانند چیزی که کاملا نیازشان را برطرف می‌کند، انتخاب کنند. چیزی که در ویندوز نمی‌توان مفهومی برای آن پیدا کرد.

لینوکس : سیستم‌عاملی حرفه‌ای

لینوکس یک سیستم‌عامل حرفه‌ای است. یعنی ممکن است یک کاربر کاملا غیر فنی برای مدیریت آن و انجام برخی از تنظیمات سخت‌افزاری دچار مشکل شود و نتواند به راحتی این کار را انجام دهد. البته برخی از توزیع‌های لینوکس این امور را بسیار راحت (و حتی راحت‌تر از ویندوز) کرده‌اند، ولی با این حال به طور کلی، لینوکس یک سیستم‌عامل حرفه‌ای است که در عین سادگی، از پیچیدگی‌های فنی زیادی برخوردار است. البته تمام کاربران لازم نیست این امور را بدانند. مثلا یک کارمند دفتری که اموری مانند تایپ و حسابداری را با کامپیوترش انجام می‌دهد، ممکن است از نظر فنی تفاوتی را احساس نکند، ولی لینوکس خوراکی ۴ ساله برای کاربران خوره فراهم می‌سازد! برخلاف ویندوز، نکات بی‌پایانی برای یادگیری در لینوکس وجود دارد. این سیستم‌عامل ۴ سال به راحتی شما را مشغول خواهد کرد و می‌توانید مطمئن باشید پس از آن بازهم مطالب جدیدی برای یادگیری وجود خواهند داشت! پس خوره‌های کامپیوتری از آن لذت وافری خواهند برد و هرگز آنرا رها نخواهند کرد.

برخلاف ویندوز، در لینوکس راحت‌تر هستید تا بسیاری از کارهای پیکربندی و سیستمی را از خط فرمان بسیار قدرتمند و عالی آن انجام دهید. با اینکه برای بسیاری از امور مانند ویندوز ابزارهای گرافیکی طراحی شده است، یک کاربر حرفه‌ای واقعا از خط فرمان لینوکس لذت خواهد برد. خط فرمان ویندوز را اصلا می‌توان خط فرمان نامید؟

لینوکس : بهشت برنامه نویسان

لینوکس را بهشت برنامه نویسان نامیده‌اند. برخلاف ویندوز که اکثر ابزارهای برنامه نویسی روی آنرا باید جداگانه نصب و حتی خریداری نمایید، لینوکس به همراه تمامی ابزارهای برنامه نویسی مورد نیازتان و با هر زبانی که فکر کنید ارائه می‌شود. کافی است آنرا نصب کنید و کار برنامه نویسی‌تان را با ابزارهای دلخواهتان شروع کنید.

لینوکس : یک جعبه ابزار کامل

لینوکس برای کاربران حرفه‌ای، یک جعبه ابزار کامل به شما می‌رود که در آن تمامی ابزارهای مورد نیاز مانند برنامه‌های اینترنتی، ابزارهای امنیتی مانند ابزارهای آزمایش شبکه، ابزارهای برنامه نویسی، هزاران صفحه کتاب و

راهنما در آن پیدا خواهید کرد. ابزارهایی که در اختیارتان قرار دارد چنان متنوع هستند که می‌توانید ۹۰ درصد اطمینان داشته باشید که پس از نصب آن به چیز دیگری نیاز نخواهید داشت.

لینوکس : یکی از زیباترین دستاوردهای بشری

لینوکس در سایه همکاری و تبادلات علمی هزاران نفر در سرتاسر جهان ایجاد شده و توسعه یافته است. این همکاری چنان گسترده و زیبا بوده و هست، که به سیستم‌عامل لینوکس لقب «زیباترین دستاورد همکاری جمعی بشر» داده شده است .فرهنگ حاکم در جامعه لینوکس و بازمتن، فرهنگ کمک، اشتراک اطلاعات و تلاش برای بهبود هرچه بیشتر محصولات و «انجام هرکاری که از دستت برمی‌آید» است .هرکس که می‌خواهد با این سیستم‌عامل کار کند، باید تمامی دیدگاه‌ها و عقاید قبلی خود را درباره نرم‌افزارها و سیستم‌عامل کنار گذاشته و با یک دیدگاه جدید و طرز فکر متحول شده وارد دنیای لینوکس شود، زیرا با فرهنگ حاکم متفاوتی روبرو خواهد بود. لینوکس نوید دهنده آزادی است...

پیش به سوی لینوکس

روز به روز شاهد گسترش سیستم‌عامل لینوکس و فناوری‌های بازمتن (Open Source) در سرتاسر جهان هستیم. متاسفانه به دلیل اینکه کشور ما یک کشور مایکروسافتی است، تاکنون اقدامات کمی در رابطه با معرفی سیستم‌عامل لینوکس و فناوری‌های بازمتن و مزایای آن انجام شده است.

درحالی که بسیاری از کشورهای جهان در حال انتقال سیستم‌های خود به سیستم‌عامل لینوکس بوده، لینوکس را در مدارس خود گسترش داده و در حال تربیت نسلی آشنا با این سیستم‌عامل هستند، مسئولین یکی از بانکها با افتخار اعلام می‌کند که سیستم‌های خود را به ویندوز ۲۰۰۰ منتقل نموده است و یا مسئولین آموزش و پرورش اعلام می‌کنند که تا وقتی مایکروسافت وجود دارد، ما از محصولات آن استفاده خواهیم کرد. شاید اکنون ما ویندوز و آفیس را به قیمت ۲۰۰۰ تومان خریداری می‌کنیم، ولی تا سال ۲۰۰۸ که به سازمان تجارت جهانی خواهیم پیوست، دیگر خبری از ویندوزهای ۲۰۰۰ تومانی نخواهد بود و آن هنگام است که پول نفت ما که متعلق به آیندگان بوده و باید صرف آبادانی این کشور شود، به جیب مایکروسافت سرازیر خواهد شد.

ما چه چیزی از پرو، برزیل، اسپانیا، چین، آلمان، ژاپن، نروژ، ویتنام و ... کم داریم؟ مگر آنها نتوانستند با این سیستم کار کنند؟ مگر این سیستم جواب خود را پس نداده و سیستمی است نا مطمئن که همه ما از آن فراری هستیم؟ به هیچ وجه اینگونه نیست.

ظاهر پوسته فرمان

در صورتی که لینوکس شما فاقد محیط گرافیکی است و یا اکنون محیط گرافیکی آن در حال اجرا نیست، شما باید دستورات خود را از طریق پوسته فرمان به سیستم عامل ارسال کنید. نخستین چیزی که در پوسته فرمان مشاهده میکنید، اعلان فرمان است که بصورت علامت $ میباشد. اعلان فرمان برای کاربر ریشه بصورت # است. در بیشتر سیستمهای لینوکس قبل از اعلان فرمان نام کاربری شما و نام کامپیوترتان قرار میگیرد که بصورت زیر نشان داده میشود:

[alan@memphis home]$

امکان نمایش کاراکترای مورد نیازتان بجای کاراکترهای فوق وجود دارد .چگونگی این کار بعدا شرح داده خواهد شد. محیط پوسته فرمان امکانات زیادی دارد.

تایپ دستورات در محیط پوسته فرمان بسیار آسان میباشد. برای اینکه با محیط پوسته فرمان آشنا شوید، سعی کنید با دستوراتی که در زیر بررسی میشوند، تمرین کنید.
نکته: در صورتی که هنگام راه اندازی سیستم، بجای پوسته فرمان محیط گرافیکی لینوکس اجرا میشود، برای تایپ فرامین پوسته باید از Terminal یا Konsole استفاده کنید. میتوانید در منوی run ، فرمان xterm را نیز تایپ کنید.
در مثالهای زیر علامتهای $ و # نشان دهنده اعلان فرمان میباشند. پس تایپ هر فرمان باید کلید Enter را فشار دهید و خروجی آن فرمان در خطوط پس از آن نمایش داده خواهد شد.

بررسی نشست ورود به سیستم
هنگامی که وارد سیستم لینوکس میشوید، برای سیستم دارای یک هویت خاص هستید. این هویت شامل نام کاربری شما، نام گروه شما، شماره کاربری شما و شماره گروه شماست. همچنین لینوکس اطلاعات زمان ورود به سیستم، مدت حضور، مدت بیکاری و محل ورود شما به سیستم را نگهداری میکند. (حواستان را جمع کنید(!
برای بدست آوردن اطلاعات در مورد هویت کاربری خودتان در جلوی اعلان فرمان دستور زیر را تایپ کنید. خروجی آن در زیر آن نشان داده شده است:

```
$ id
uid=500(Alan) gid=500(Alan) groups=500(Alan)
```

خروجی فرمان نشان میدهد که نام کاربر Alan بوده که عضو گروه Alan است و شماره های کاربری و گروه آن ۵۰۰ میباشد.
با استفاده از فرمان who میتوانید اطلاعاتی در مورد نشست جاری بدست آورید. در زیر این فرمان به همراه خروجی آن نشان داده شده است:

```
$ who
Alan :0 Apr 23 08:46
```

همچنان که می بینید، در خروجی نام کاربر جاری، زمان و تاریخ ورود به سیستم نمایش داده شده است.

بررسی دایرکتوری ها و مجوزهای فایلها
در لینوکس مسیر جاری به مسیری گفته میشود که کاربر در آن لحظه در آن قرار دارد. هنگامی که وارد سیستم میشوید، لینوکس شما را در دایرکتوری خانگی تان قرار میدهد. هنگامی که دستور باز کردن یا ذخیره کردن فایلی را صادر میکنید، لینوکس مسیر جاری را بعنوان محل آن فایل فرض کرده و از آنجا آنرا باز کرده و یا ذخیره میکند. ساختار سیستم فایل لینوکس بعدا شرح داده خواهد شد و لازم نیست نگران آن باشید. برای نمایش دایرکتوری جاری فرمان زیر را جلوی خط فرمان تایپ کنید. خروجی آن در زیر آن نمایش داده شده است:

```
$ pwd
/usr/bin
```

در مثال بالا مسیر جاری usr/bin است. برای یافتن مسیر دایرکتوری خانگی خود، فرمان زیر را تایپ کنید:

```
$ echo $HOME
```

/home/Alan

همچنان که در خروجی ملاحضه میکنید، مسیر دایرکتوری خانگی شما نمایش داده شده است. برای اینکه به دایرکتوری خانگی خود باز گردید، کافی است به سادگی فرمان زیر را تایپ کنید:

$ cd

این فرمان، شما را به دایرکتوری خانگی تان باز می گرداند. خوب بد نیست ببینیم که چه چیزهایی در دایرکتوری خانگی وجود دارد. برای نمایش محتویات یک دایرکتوری، باید از فرمانls استفاده نمایید. در صورتی که در دایرکتوری خانگی خود قرار ندارید میتوانید مسیر کامل آنرا تایپ کنید. در صورتی که فرمانls را بدون هرگونه دایرکتوری تایپ کنید، محتویات مسیر جاری نمایش داده خواهد شد. گزینهa تمام فایلهای مخفی را نمایش میدهد و گزینهl برای نمایش جزئیات کامل فایلها بکار میرود. هنگام تایپ یک فرمان میتوانید گزینه های متعدد آنرا کنار هم تایپ کنید.در زیر این دستور به همراه یک خروجی مثال نشان داده شده است:

```
$ ls -la /home/Alan
total 46740
drwx—— 47 Alan Alan 4096 Apr 23 11:09 .
drwxr-xr-x 8 root root 4096 Mar 12 17:51 ..
-rw——- 1 Alan Alan 616581 Apr 18 23:29 779-red_hat_linux_9.tar.gz
drwxr-xr-x 2 Alan Alan 4096 Mar 20 11:15 .acrobat
drwx—— 2 Alan Alan 4096 Mar 20 11:15 .adobe
drwx—— 2 Alan Alan 4096 Mar 12 17:04 .adonthell
drwxr-xr-x 2 Alan Alan 4096 Feb 14 13:19 .anjuta
-rw——- 1 Alan Alan 18325 Apr 23 00:36 .bash_history
-rw-r–r– 1 Alan Alan 24 Aug 24 2002 .bash_logout
-rw-r–r– 1 Alan Alan 191 Aug 24 2002 .bash_profile
```

هنگامی که از سوئیچl برای نمایش جزئیات بیشتر استفاده میکنید، چیزی بیش از سایز فایلها و دایرکتوری ها نمایش داده میشود. دایرکتوری جاری (.) و دایرکتوری والد (..) در بالای لیست قرار می گیرند. یعنی در حقیقت نقطه نشان دهنده دایرکتوری home/Alan و دونقطه نشاندهنده دایرکتوری /home است. بخش ابتدایی لیست نشاندهنده مجوزهای هر فایل است. سایر اطلاعات نمایش داده شده عبارتند از اندازه فایل به بایت و تاریخ و ساعتی که فایل برای آخرین بار تغییر کرده است.

بررسی فعالیتسیستم

لینوکس علاوه بر چندکاربره بودن، سیستم عاملی است چند وظیفه . (multitasking)چند وظیفه بودن به این معنی است که برنامه های زیادی میتوانند در یک زمان اجرا شوند. هر برنامه در حال اجرا یک پروسه نامیده میشود.لینوکس فرامینی برای نمایش پروسه های در حال اجرا، نمایش استفاده از منابع سیستمی و متوقف کردن پروسه های در مواقع لزوم دارد.

مرسوم ترین ابزار برای بررسی پروسه های در حال اجرا، دستورps است. با این دستور، میتوانید بررسی کنید که چه برنامه هایی در حال اجرا هستند ، از چه منابعی استفاده میکنند و چه کسی در حال اجرای آنهاست. در زیر یک خروجی مثال از این فرمان نشان داده شده است:

```
$ ps au
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
Alan 1152 0.0 0.5 4476 1348 pts/0 S 17:39 0:00 bash
Alan 1831 0.0 0.2 2580 664 pts/0 R 18:14 0:00 ps au
```

در مثال بالا، گزینهa ، برای نمایش تمام پروسه هایی که به ترمینال فعلی شما مربوط است و گزینهu برای نمایش نام کاربری و زمانی که برنامه آغاز به کار کرده است، بکار میرود. مفهوم ترمینال به زمانهای قدیم باز میگردد. در آن زمان کاربران روی ترمینالهای مبتنی بر متن کار میکردند و هر ترمینال نشان دهنده یک نفر بود. اکنون شما میتوانید روی صفحه مانیتور خود تعداد زیادی ترمینال داشته باشید. این کار بوسیله باز کردن تعدادی پنجره ترمینال امکان پذیر است.

در مثال بالا، چیز خاصی اتفاق نیافتاده است. خروجی نشان میدهد که کاربری به نامAlan ، از برنامه هایbash و psدر حال استفاده است. ستونTTY یا ترمینال، نشان دهنده ترمینای است که کاربر با آن به سیستم وارد شده است و ستونSTAT نشاندهنده وضعیت پروسه استR .نشاندهنده پروسه در حال اجرا و Sنشاندهنده پروسه در حال خواب میباشد.

ستونUSER نام کاربری که پروســه را شروع کرده نمایش میدهد. هر پروسه توسط یک عدد یکتا به نام شماره پروسه (Process ID) مشخص میشود. از این شماره هنگام از میان بردن یا اصطلاحاkill کردن پروسه استفاده میشود. ستونهای %CPUو%MEM نشاندهنده مقدار پردازنده و حافظه ای هستند که پروسه ها استفاده کرده اند. ستونVSZ یاVirtual Set Size نشاندهنده سایز پروسهimage به کیلوبایت وRSS یا Resident Set Size نشاندهنده سایز پروسه در حافظه است .ستونSTART نشاندهنده زمان آغاز پروسه و ستونTIME نشاندهنده زمان سیستم استفاده شده برای پروسه است.

بسیاری از پروسه هایی که در کامپیوتر در حال اجرا هستند، به یک ترمینال خاص مربوط نیستند. یک سیستم عادی مبتنی بر لینوکس ، دارای پروسه هایی فراوانی است که در پس زمینه اجرا میشوند. پروسه های پس زمینه پروسه هایی هستند که اعمالی مانند ثبت فعالیتهای سیستم یا گوش کردن به پورتها برای اطلاعات واصله از شبکه را انجام میدهند. این پروسه ها هنگام بوت شدن سیستم آغاز به کار کرده و هنگام خاموش کردن سیستم ، به کار خود پایان میدهند .برای نمایش تمام پروسه های در حال اجرا بر روی کامپیوترتان باید از فرمان زیر استفاده کنید:

```
$ ps aux | less
```

قسمت |less به این دلیل به فرمان اضافه شده است که در صورتی که تعداد پروسه ها از یک صفحه بیشتر شد، امکان نمایش صفحه به صفحه آن وجود داشته باشد. به این فرایند لوله بندی (pipe) فرمان گویند که به معنی هدایت خروجی یک فرمان برای ورودی فرمان دیگر است.

خروج از پوسته فرمان

هنگامی که کارهای خود را انجام دادید و مایل بودید از پوسته فرمان خارج شوید، کافی است که کلیدهایCtrl+D را فشار دهید. در صورتی که در حالت متنی لینوکس را بوت کرده اید، کافی است فرمانlogout یاexit را تایپ کنید.

خوب، تا اینجا با چند فرمان که به شما کمک میکند از سیستمتان اطلاعات لازم را به دست آورید، آشنا شدید. صدها فرمان دیگر نیز وجود دارند که میتوانید آنها را آزمایش کنید. این فرامین در مسیرهایusr/bin وbin قرار دارند.

همچنین فرامین مدیریت سیتم در مسیرهایusr/sbin وsbin قرار دارند .بیشتر این فرامین در ادامه این فصل توضیح داده خواهند شد.

درک دقیق تر پوسته فرمان لینوکس

قبل از اینکه آیکونها و پنجره ها روی صفحه کامپیوترها پدیدار شوند، کاربران برای کار کردن با کامپیوترها باید فرمانهایی را تایپ میکردند. در سیستمهای مبتنی بر یونیکس که لینوکس هم یکی از آنهاست، برنامه ای که برای تفسیر و مدیریت فرمانها ایجاد شده است، پوسته فرمان (Command Shell) نام دارد.

پوسته فرمان راهی برای اجراکردن برنامه ها، کارکردن با فایلها، کامپایل کردن برنامه ها و مدیریت کامپیوتر ایجاد میکند.

با اینکه کارکردن با ابزارهای گرافیکی آسان تر از کار کردن با پوسته فرمان است، ولی بیشتر کاربران حرفه ای لینوکس ترجیح میدهند تا بجای ابزارهای گرافیکی از پوسته فرمان استفاده کنند. زیرا برای انجام بسیاری از کارها مانند پیکربندی های سیستم ، پوسته فرمان بسیار قدرتمند تر از ابزارهای گرافیکی است. حتی برخی کاربران قدیمی یونیکس و لینوکس به ندرت از محیطهای گرافیکی برای انجام کارهایشان استفاده میکنند.

پوسته فرمانی که در این راهنما توضیح داده خواهد شد، bashنام دارد. نام آن برگرفته از Bourne Again Shellاست. پوسته bash از نخستین پوسته سیستمهای یونیکس کهsh یاBourne Shell نام داشت، ایجاد شده است و یکی از پر کاربرد ترین پوسته های فرمان به شمار میرود. البته پوسته های دیگری نیز وجود دارند که از آنها استفاده میشود که میتواند از آنهاcsh یاC Shell که در سیستمهای یونیکسBSD استفاده میشود وksh یاKorn Shell که بیشتر درUnix System V استفاده میشود، نام برد. لینوکس همچنین دارای پوسته هایtcsh وash نیز میباشد.

هنگامی که استفاده از یک پوسته فرمان را در لینوکس فرا بگیرید، به آسانی میتوانید پوسته های دیگر را نیز یاد بگیرید. در صورتی که هرگونه مشکل یا سوالی داشتید، میتوانید به صفحهmanual آن پوسته مراجعه کنید.

نکته : برای نمایش صفحهmanual هر فرمان کافی است در خط فرمان لینوکس دستور زیر را تایپ کنید:

$ man <command>

در لینوکس ، پوسته bash کاملا سازگار با پوسته فرمانsh میباشد.

استفاده از پوسته فرمان در لینوکس

هنگامی که یک فرمان را در پوسته فرمان تایپ میکنید، میتوانید به آن کاراکترهای دیگری اضافه کنید تا چگونگی کارکرد دستور مورد نظر را تغییر دهید.

-گزینه ها :**(Options)**

اکثر فرامین دارای یک یا چند گزینه هستند که با اضافه کردن و بکار بردین این گزینه ها میتوانید نحوه رفتار فرمان را تغییر دهید. برای مثال همانطور که قبلا هم دیدید، در فرمانls-la گزینهl برای نمایش لیست مشروح فایلها و دایرکتوری ها و گزینه a برای نمایش فایلهای مخفی که با نقطه شروع میشدند، بکار رفت.ضمنا گزینه هایی که مخفف یک کلمه هستند با یک – شروع میشوند در صورتی که گزینه هایی که یک کلمه کامل هستند با — شروع میشوند .

برای مثال . ls –help

–آرگومان ها : **(Arguments)**

بسیاری از فرامین، علاوه بر گزینه ها ، آرگومانهایی را نیز قبول میکنند .یک آرگومان یک بخش شامل نوعی اطلاعات مانند مسیر یا نام فایل میباشد. برای مثال در فرمان ls -la /home بخشhome آرگومان فرمانls به شمار میرود.

-متغییر های محیطی : (EnvironmentVariables)

خود پوسته اطلاعاتی را در بر دارد که برای کاربر مفید است. به این اطلاعات متغییرهای محیطی می گویند. برای مثال متغییرSHELL نمایانگر نوع پوسته مورد استفاده ، SP1نشاندهنده اعلان فرمان وMAIL نشاندهنده محل صندوق پستی شما است:

```
$ echo $SHELL
/bin/bash
$ echo $MAIL
/var/spool/mail/Alan
```

توجه داشته باشید که برای فراخوانی متغییر ها به ابتدای آنها علامت $ اضافه میشود.

نکته : برای نمایش تمام متغییرهای محیطی میتوانید از دستور declareاستفاده کنید. برای نمایش یک متغییر خاص میتوانید همانند بالا از دستورecho استفاده کنید.

-کاراکترهای ویژه :(Metacharacters)

کاراکترهایی وجود دارند که دارای معنای خاصی برای پوسته فرمان هستند .این کاراکترها میتوانند برای هدایت خروجی یک فرمان به یک فایل ، لوله بندی خروجی یک فرمان و یا اجرای فرمان در پس زمینه استفاده شوند. کاراکترهای ویژه در این فصل توضیح داده خواهند شد.

برای صرفه جویی در مقدار تایپ و آسانتر شدن کار ، پوسته فرمان دارای ویژگیهایی است که دستورات قبلی تایپ شده را نگهداری میکند. همچنین شما میتوانید برای آسانتر شدن، نامهای مستعاری برای دستورات ایجاد کنید. پوسته فرمان دستوراتی که قبلا وارد کرده اید ذخیره میکند و میتوانید بجای تایپ مجدد دستورات ، دستورات قبلی را فراخوانی نمایید. این موضوع نیز جلوتر بررسی خواهد شد.

در صورتی که پوسته فرمان را تغییر داده نباشید، پوستهbash پوسته ای است که همراه با لینوکس استفاده میکنید. پوستهbash از نظر امکانات و قابلیتها قویتر از انواع دیگر پوسته های فرمان است. در این فصل بیشتر قابلیتهای پوسته فرمانbash بررسی خواهند شد. ولی در صورتی که نیاز به اطلاعات بیشتری داشتید، میتوانید از دستور man bashبرای نمایش راهنمای پوستهbash استفاده کنید.

یافتن فرمانهای لینوکس

در صورتی که بدانید که یک دستور در کجای سیستم فایل لینوکس قرار دارد، میتوانید آنرا با تایپ مسیر کامل اجرا نمایید. برای مثال برای اجرای دستور :date

```
$ /bin/date
```

البته در صورتی که دستوری در مسیرهای سخت و طولانی قرار داشته باشد ، این کار دشوار خواهد بود. بهترین راه حل این مشکل، نگهداری فرامین در یک دایرکتوری خاص است. سپس میتوانید این دایرکتوری را به مسیر جستجوی

پوسته فرمان خود اضافه کنید تا هنگام تایپ یک فرمان، خود پوسته بطور خودکار دایرکتوری فوق را برای وجود فرمان کاوش کند:

علاوه بر خود دستور، موارد دیگری که میتوانید در خط فرمان تایپ کنید عبارتند از:

```
$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/X11R6/bin:/home/Alan/bin
```

خروجی فرمان فوق مسیرهای تعریف شده برای پوسته فرمان را برای یک کاربر خاص نشان میدهد. همانطور که می بینید دایرکتوری ها توسط یک کلون از هم جدا شده اند. بیشتر دستوراتی که همراه با لینوکس ارائه میشوند، در دایرکتوری هایbin ، usr/binیاusr/local/bin قرار دارند. دستورات گرافیکی که با محیطهای گرافیکی استفاده میشوند در مسیرهایusr/bin/X11 وusr/X11R6/bin قرار دارند. آخرین دایرکتوری نشان داده شده در خروجی فرمان، در دایرکتوری خانگی کاربر قرار دارد.

نکته : در صورتی که مایلید دستوراتی که خود ایجاد میکنید مستقیما در خط فرمان اجرا شوند، میتوانید یک دایرکتوری به نامbin در دایرکتوری خانگی خود ایجاد کنید و این دستورات را در آنجا ذخیره کنید. لینوکس این دایرکتوری را بطور خودکار به مسیرهای تعریف شده اضافه میکند.

در صورتی که شما کاربر ریشه هستید، دستورات مربوط به مدیریت سیستم در دایرکتوری هایsbin و usr/sbin قرار دارند.

ترتیب دایرکتوری های موجود در مسیرهای تعریف شده نیز مهم است. این دایرکتوری ها از چپ به راست بررسی میشوند. بنابراین اگر دستوری به نام fooهم در دایرکتوریusr/bin و هم در دایرکتوریbin قرار داشته باشد، اولی اجرا خواهد شد. برای اجرای دستور دومfoo باید مسیر کامل آنرا تایپ کنید و یا مسیرهای تعریف شده را تغییر دهید. چگونگی این کار جلوتر توضیح داده خواهد شد.

تمام فرامینی که تایپ میکنید، در دایرکتوری های مسیرهای تعریف شده شما قرار ندارند. برخی فرامین بصورت درونی در پوسته فرمان گنجانده شده اند. در صورتی که برای یک فرمان خاص یک نام مستعار همراه با گزینه ها و آرگومانهای خاص ایجاد کنید، ابتدا آن اجرا میشود. همچنین راههایی برای ایجاد توابعی که شامل چندی فرمان هستند نیز وجود دارد. ترتیب بررسی محلهای مختلفی که پوسته فرمان برای پیداکردن یک دستور انجام میدهد به شرح زیر است:

-نامهای مستعار:

نامهایی که با دستورalias ایجاد شده اند و نشانگر یک دستور به همراه گزینه ها و آرگومانهای احتمالی میباشند.

-کلمات رزرو شده پوسته فرمان :

کلماتی هستند که برای استفاده های مخصوص رزرو شده اند. بیشتر این کلمات دستوراتی هستند که معمولا در زبانهای برنامه نویسی استفاده میشوند مانند do، while، caseو غیره.

-توابع:

دسته ای از دستورات که همراه هم در پوسته فرمان اجرا میشوند.

-دستورات درونی :

دستوراتی که درون خود پوسته فرمان گنجانده شده اند.

–دستورات سیستم فایل:

دستورات معمولی که بصورت فایلهایی در سیستم فایل لینوکس قرار دارند. مسیرهای این دستورات در متغییر محیطیPATH گنجانده شده است.

نکته : برای نمایش لیستی از فرامین درونیbash و گزینه های آن میتوانید از دستورhelp استفاده کنید. برای نمایش اطلاعات بیشتر در مورد دستور مورد نظر از دستورinfo بعلاوه نام دستور مورد نظر استفاده کنید.
برای اینکه بفهمید که یک دستور در کجا قرار دارد، میتوانید از دستورtype برای این منظور استفاده کنید. برای

مثال:

$type bash
bash is /bin/bash

از دستور بالا برای یافتن محل فرامیت دیگری مانندwhich ، caseو ... استفاده کنید. در صورتی که دستوری در چندین دایرکتوری قرار دارد، میتوانید با اضافه کردن گزینهa به دستورtype ، تمام محلهای وجود آنرا چاپ کنید.
نکته :گاهی اوقات هنگام اجرای یک فرمان با خطاهایی مانند "این فرمان پیدا نشد" و یا "شما مجوز استفاده از این فرمان را ندارید" مواجه میشوید .برای مورد اول بررسی کنید که دستور را صحیح تایپ کرده اید و مسیر آن در مسیر PATHشما قرار داشته باشد. ممکن است فرمان مورد نظر اجرایی نباشد. در بخش کارکردن با فایلها، چگونگی اجرایی کردن یک فایل تشریح خواهد شد.

اجرای مجدد یک فرمان

تصور کنید یک فرمان بسیار طولانی را تایپ کرده اید و پس از اجرای آن متوجه میشوید که مرتکب اشتباه شده اید. مطمئنا چیزی دردآور تر از این وجود ندارد! پوسته فرمان دارای قابلیتهایی است که میتوانید بوسیله آن دستوراتی که قبلا اجرا کرده اید فراخوانی کرده و در صورت لزوم پس از اصلاح یا تغییر وحتی بدون تغییر آنها را مجددا اجرا کنید. پوسته فرمان دارای قسمتی به نام تاریخچه(History) است که فرامینی کهقبلا وارد کرده اید را نگهداری میکند. شمامیتوانید این فرامین را از تاریخچه فراخوانی کرده و استفادهکنید.

ویرایش خط فرمان

در صورتی که در تایپ یک دستور مرتکب اشتباه شده اید، میتوانید به آسانی آنرا فراخوانی کرده و مجددا پس از ویرایش ، آنرا اجرا کنید. میتوانید از برخی کلیدهای میانبر برای راحت تر کردن این کار استفاده کنید. مثلا کلیدهای Ctrl+aاشاره گر را به ابتدای فرمان و Ctrl+E به انتهای فرمان حرکت می دهد .همین کار را کلیدهایHome و Endنیز انجام میدهند. ویرایش کردن فرمان مانند کارکردن در ویرایش گرهای متنی است و بسیار ساده است. پس اتمام ویرایش دستور، کافی است کلیدEnter را برای اجرای آن فشار دهید.

کامل کردن خودکار فرمان

برای اینکه مقدار تایپ شما به حداقل برسد، پوسته فرمان فرمان ناقص شما را به روشهایی کامل میکند. . برای بکارگیری این قابلیت کافی است که ابتدا چند حرف اول فرمان مورد نظر را تایپ کرده و کلیدtab را فشار دهید. در زیر برخی موارد را که میتوانید ناقص تایپ کنید می بینید:

-متغییر های محیطی :

در صورتی که متن با یک علامت دلار شروع شود، با فشردن کلیدtab ، پوسته فرمان آنرا با یک متغییر محیطی کامل خواهد کرد.

-نام کاربری :

در صورتی که متن بوسیله یک کاراکتر ~ شروع شود، پوسته فرمان آن را بوسیله یک نام کاربری کامل خواهد کرد.

-دستورات، نامهای مستعار یا توابع:

در صورتی که متن با یک کاراکتر عادی شروع شود، پوسته فرمان آنرا بوسیله یک دستور، نام مستعار یا تابع کامل خواهد کرد.

-نام میزبان:

در صورتی که متن با یک علامت @ شروع شود، پوسته فرمان آنرا بوسیله یک نام میزبان که از فایل etc/hosts می خواند، کامل میکند.

مواقعی وجود دارد که برای کامل کردن یک فرمان چندین گزینه وجود دارد . مثلا چندین متغییر محیطی وجود دارد که با حرفP شروع میشود. در این موارد در صورتی که شما دوبار کلیدTab را فشار دهید و یا کلیدهای ?+Esc را فشار دهید، تمام حالتهای ممکن به شما نشان داده میشود:

```
$ echo $P<tab><tab> or <Esc+?>
$PATH $PPID $PS1 $PS4
$PIPESTATUS $PROMPT_COMMAND $PS2 $PWD
```

فراخوانی مجدد یک فرمان

پس از اینکه یک دستور را تایپ کردید، همانطوری که قبلا گفتم این دستور بطور کامل در تاریخچه پوسته فرمان ذخیره میشود. برای نمایش محتویات تاریخچه پوسته فرمان میتوانید از دستورhistory استفاده کنید. در صورتی که پس از آن یک عدد اضافه کنید، به تعداد آن عدد دستورات تایپ شده را نشان خواهد داد:

```
$ history 5
ls۱۰۲۳
cd Fonts/۱۰۲۴
man more۱۰۲۵
date۱۰۲۶
history 5۱۰۲۷
```

برای فراخوانی دستورات تایپ شده میتوانید از روشهای زیر استفاده کنید:

-کلیدهای مکان نما :از کلیدهای بالا و پایین مکان نما میتوانید برای حرکت کردن در لیست تاریخچه استفاده کنید. بجای آن از کلیدهای Ctrl+nوCtrl+p نیز میتوانید استفاده کنید.

-کلیدهای :Ctrl+rبرای جستجوی آخر به اول یک رشته در تاریخچه استفاده میشود. برای مثال با تایپ یک یا چند حرف، دستوری که دارای آن حروف است نمایش داده میشود.

-کلیدهای :Ctrl+sمشابه بالا ولی جستجو بصورت اول به آخر صورت میگیرد.

روش دیگری که میتوانید از آن برای کار کردن با فرامین استفاده کنید، دستورfc است. با استفاده از این دستور، که پس از آن میتوانید شماره دستور مورد نظر در تاریخچه یا بازه ای از شماره ها را ذکر کنید، این دستورات در یک ویرایشگر متنی باز میشوند که میتوانید آنها را ویرایش کرده و خارج شوید .برای مثال دستور زیر دستورات ۱۰۰ ام تا ۱۵۰ ام تاریخچه را در ویرایشگر باز خواهد کرد:

```
$ fc 100 150
```

لیست تاریخچه در فایلی به نامbash_history. که در دایرکتوری خانگی شما قرار دارد، ذخیره میشود و در آن تا ۱۰۰۰ دستور نگهداری میشود.

اتصال و گسترش فرامین

یکی از قابلیتهای واقعا قدرتمند پوسته فرمان، قابلیت هدایت خروجی یا ورودی یک فرمان به فرامین دیگر است. برای این منظور، همانطور که قبلا اشاره شد، از کاراکترهای ویژه استفاده میشود.

لوله بندی فرامین(Piping Commands)

کاراکتر ویژه لوله بندی کاراکتر (|) است. این کاراکتر، خروجی یک فرمان را به ورودی فرمان دیگر هدایت میکند.

برای مثال:

```
$ cat /etc/passwd | sort | more
adm:x:3:4:adm:/var/adm:/sbin/nologin
Alan:x:500:500:Alan Bachumian,7852020:/home/Alan:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
bin:x:1:1:bin:/bin:/sbin/nologin
Linet:x:501:501:Linet Minasian:/home/Linet:/bin/bash
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
```

این فرمان محتویات فایل etc/passwd را خوانده و خروجی را به فرمان sortهدایت میکند. این فرمان، کاراکتر ابتدای هر سطر را گرفته و خروجی را بصورت الفبایی مرتب کرده و خروجی را به دستورmore میفرستد و این دستور نیز خروجی را بصورت صفحه به صفحه نمایش میدهد.

قابلیت لوله بندی نمایش خوبی است از اینکه چگونه یونیکس، پدر لینوکس بر اساس قطعات مختلف نرم افزاری شکل گرفته است. مثلا در یونیکس ابزارهای مختلف را طوری به هم وصل میکردن که کارهای مختلفی بتوان با آنها انجام داد. مثال خوبی که در این مورد میشود زد: سالها پیش که واژه پردازهای گرافیکی و راحت مانند اکنون وجود

نداشتند، کاربران باید ابتدا سند خود را بصورت متنی ایجاد کرده و سپس آنرا بوسیله ماکروهای خاصی فرمت بندی میکردند و بعد باید بررسی میکردند که چطور از آب در آمده است . برای این کار از فرمانی مانند زیر استفاده میشد:

```
$ nroff -man grep.1 | lpr
```

در دستور بالا ازnroff برای فرمت کردن فایلgrep.1 با استفاده از ماکروی manاستفاده شده و حاصل کار با استفاده از لوله بندی به خروجی چاپگر که lprاست فرستاده شده است.

ابزار تعیین سطح امنیت سیستم(SecurityLevel)

این ابزار تنظیمات مربوط به دیوار آتش سیستم را انجام می‌دهد. در صورتی که کامپیوتر شما در نقش یک سرویس دهنده عمل نمی کند، می‌توانید این سطح را رویHigh تنظیم کنید. در صورتی که بنحوی ارائه کننده سرویس خاصی روی شبکه هستید، گزینهMedium و یاCustomize را انتخاب نمایید. با انتخاب گزینه Customizeسیستم به شما این امکان را می‌دهد تا تعیین کنید بسته‌های ارسالی برای کدامیک از سرویس‌ها از دیوار آتش عبور نمایند و بسته‌های کدامیک از سرویس‌ها فیلتر شوند.

به هیچ عنوان انتخاب گزینهNo Firewall توصیه نمی‌شود. انتخاب این گزینه، امنیت سیستم شما را شدیدا به مخاطره خواهد انداخت. مخصوصا اگر از شبکه‌های عمومی و اینترنت استفاده کنید.

ابزار شناسایی کارت صوتی (Soundcard Detection)

از این ابزار می‌توانید برای پیدا کردن و نصب کارت صوتی سیستم خود استفاده نمایید. در صورتی که این ابزار موفق نبود، می‌توانید از دستور sndconfigبرای این منظور استفاده کنید.

ابزار مدیریت کاربران و گروهها (Users & Groups)

این ابزار برای مدیریت کاربران و گروههای کاربری استفاده می‌شود. با این ابزار می‌توانید گروههای جدید و کاربران جدید به سیستم اضافه نموده و یا آنها را حذف کنید. برای اضافه کردن یک کاربر جدید باید روی دگمه Add Userکلیک کرده و در پنجره ای که باز می‌شود، اطلاعاتی مانند نام، نام کاربری، کلمه عبور، تکرار کلمه عبور، نوع پوسته فرمان و دایرکتوری خانگی کاربر جدید را وارد نمایید. تصویر ۱-۳ این پنجره را نشان می‌دهد.

هنگامی که یک گروه جدید اضافه می‌کنید، می‌توانید دسته ای از کاربران را عضو این گروه نمایید. هنگامی که سطوح دسترسی به منابع اشتراکی در شبکه را تعیین می‌کنید، می‌توانید به سادگی یک گروه را برای استفاده از یک منبع تعیین کنید و با این کار تمام کاربرانی که عضو این گروه هستند، می‌توانند از آن منبع اشتراکی استفاده کنند.

تصویر ۱-۳: پنجره اضافه کردن کاربر جدید

خروج از محیط GNOME

پس از اینکه کار روزانه‌تان به اتمام رسید می‌توانید از سیستم خارج شده (Log out)و یا سیستم را خاموش نمایید.

برای خروج ازGNOME کافی است مراحل زیر را انجام دهید:

۱ .منوی اصلیGNOME را باز کنید.

۲ .گزینهLogout را انتخاب نمایید. یک پنجره باز شده و از شما میپرسد مایل به انجام کدامیک از اعمال خاموش کردن، بوت کردن و یا خارج شدن از سیستم هستید.

نکته : در این مرحله می‌توانید با انتخاب گزینهSave Session نشست خود را ذخیره نمایید. با این کار اکثر برنامه‌هایی که در سیستم باز هستند، در ورود بعدی شما به سیستم، به صورت خودکار اجرا خواهند شد.فراموش نکنید حتما قبل از خروج اطلاعات آنها را ذخیره نمایید.

۳ .گزینه ای را که مایل به انجام آن هستید را انتخاب کرده و روی دگمهYes کلیک کنید. با این کار فرمان مورد نظر شما اجرا خواهد شد.

پیکربندی شبکه: (Network Configuration)

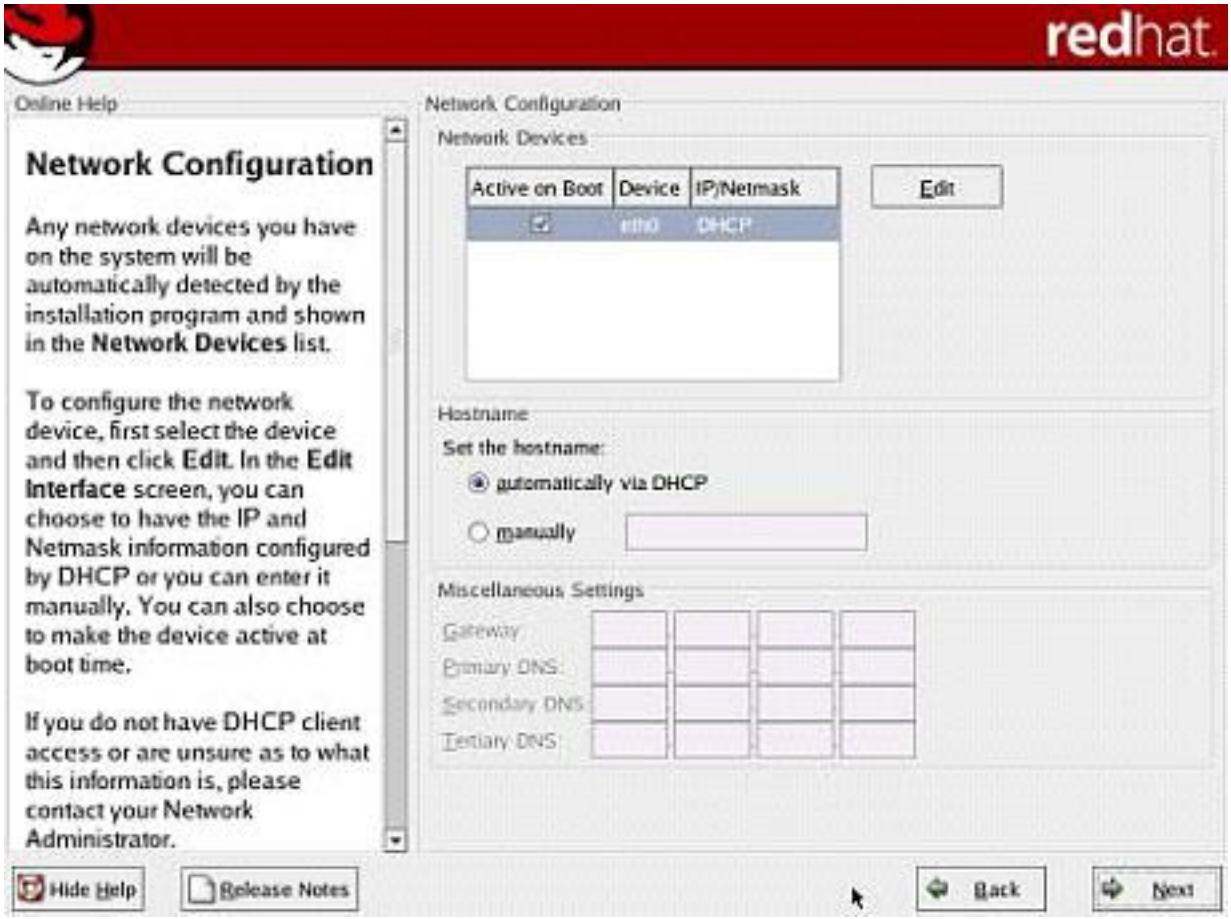
در این قسمت از شما درخواست میشود تا شبکه خود را پیکربندی نمایید. این تنظیمات فقط برای شبکه محلی میباشد. در صورتی که از شبکه بندی تلفنی (Dialup)استفاده میکنید، میتوانید با کلیک رویNext بسادگی از این مرحله عبور نمایید. هچنین در صورتی که کامپیوتر شما به شبکه متصل نیست، از این مرحله عبور نمایید.

آدرسهای شبکه به دو روش به سیستم شما اختصاص داده میشود : بصورت ثابت (Static)که شما آنرا تایپ میکنید و یا با استفاده از سرویس دهندهDHCP که هنگام بوت آدرس کامپیوتر شما را تعیین میکند. برای کسب اطلاعات سرویس دهنده DHCPو یا آدرسIP اختصاصی و ثابت کامپیوتر خود و سایر اطلاعات مورد نیاز شبکه به مدیر شبکه

خود مراجعه نمایید. همچنین میتوانید انتخاب نمایید که شبکه شما در هنگام بوت فعال شود یا نه (اگر از شبکه محلی استفاده میکنید، معمولا مایلید این کار صورت گیرد.(

در صورتی که ورود آدرس ثابت را انتخاب نموده اید، باید گزینهmanually را فعال نموده و اطلاعات زیر را وارد نمایید.

تصویر ۲-۳



تصویر۲-۳ : پیکربندی شبکه هنگام نصب لینوکس ردهت

-آدرس IP:

این آدرس از چهار بخش عددی که توسط نقطه از هم جدا شده اند تشکیل شده است. این شماره در حقیقت نشانی کامپیوتر شما در شبکه است. برای اطلاعات بیشتر در مورد آدرسهایIP میتوانید به فصل ۱۵ مراجعه نمایید. مثالی از یک آدرسIP خصوصی ۱۰،۰،۰،۱۲ است.

-Nemask :

برای تعیین اینکه کدام قسمت آدرسIP شماره شبکه و کدام قسمت آن آدرس کامپیوتر میزبان است. یک مثال برای یک شبکه کلاسA شماره ۲۵۵،۰،۰،۰ است .لینوکس ردهت این شماره را برای شما حدس خواهد زد.

-Network:

شماره شبکه را مشخص میکند. برای مثال اگر شما آدرسIP شماره ۱۰،۰،۰،۱۲ را روی یک شبکه کلاس آ (۲۵۵،۰،۰،۰) داشته باشید، شماره شبکه ۱۰ خواهد بود)همچنین ۱۰،۰،۰،۰.(

-Broadcast:
یک شمارهIP است که برای انتشار اطلاعات روی شبکه بکار میرود. برای یک شبکه کلاس آ با شماره شبکه ۱۰ شماره انتشار ۱۰،۲۵۵،۲۵۵،۲۵۵ خواهد بود.

-Hostname:
این نامی است که کامپیوتر شما در یک حوزه (Domain) توسط آن شناخته میشود. برای مثال اگر کامپیوتر شما memphisنامیده شود و در حوزه truedata.comقرار داشته باشد، نام میزبان (Hostname) کامل شما memphis.truedata.comخواهد بود.

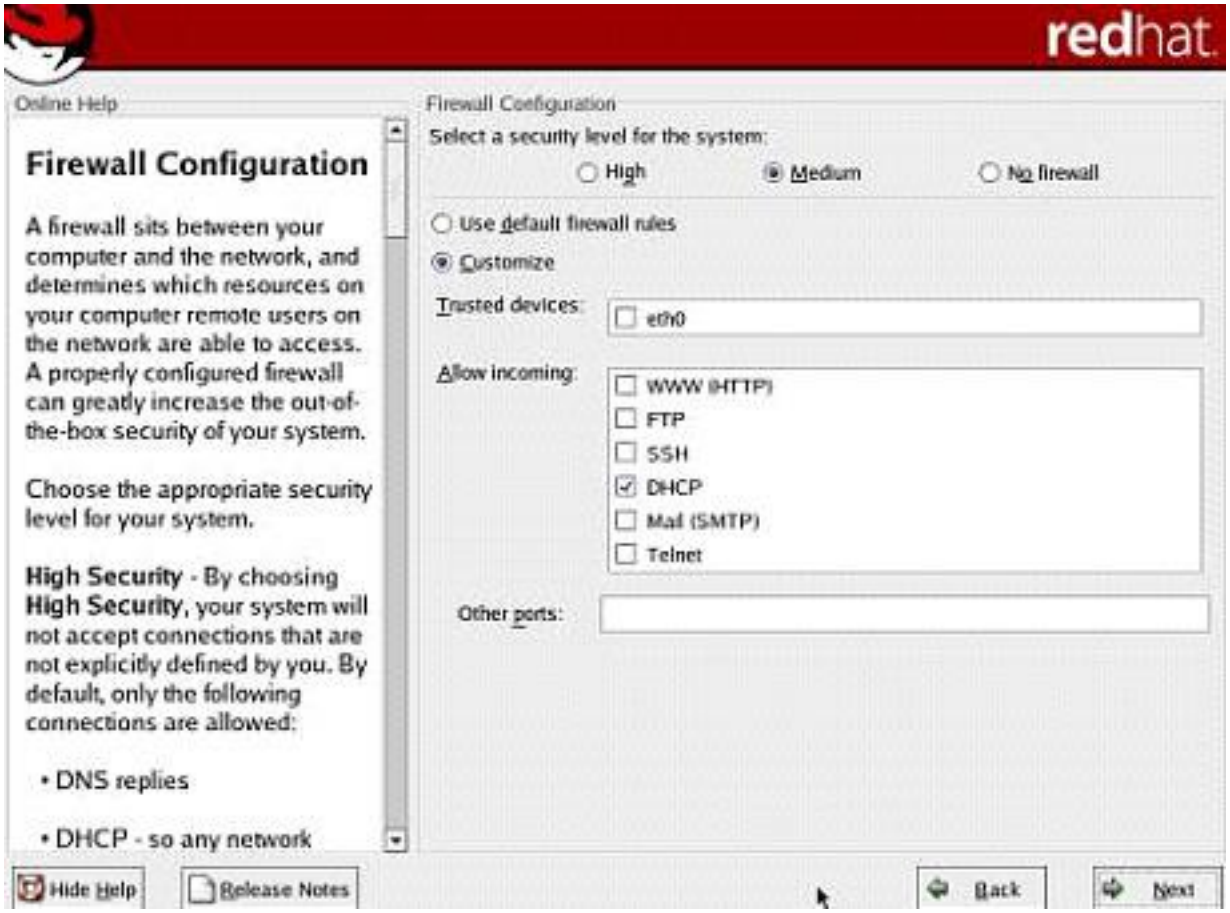
-Gateway:
یک آدرسIP که به عنوان دروازه ای به شبکه های خارج از شبکه محلی شما عمل میکند. معمولا یک میزبان یا مسیریاب (Router) میباشد که بسته ها را بین شبکه محلی شما و اینترنت مسیریابی میکند.
-Primary DNS:
آدرسIP کامپیوتری است که عمل ترجمه نام های کامپیوتر به آدرسهایIP را انجام میدهد. این کامپیوتر سرویس دهندهDNS نام دارد. شما ممکن است دارای سرویس دهنده های دوم و سومDNS باشید که در صورت موجود نبودن هریک دیگری عهده دار کار ترجمه باشد.
انتخاب پیکربندی دیوار آتش(Firewall)
در این مرحله از نصب باید دیوار آتش سیستم خود را پیکربندی نمایید .استفاده از یک دیوار آتش برای حفظ امنیت کامپیوترتان الزامی و بسیار مهم است. در صورتی که شما به اینترنت و یا یک شبکه عمومی دیگر متصل میشوید، دیوار آتش میتواند راههای نفوذ به سیستم لینوکس شما را محدود نماید. برای پیکر بندی دیوار آتش، انتخابهای زیر را در اختیار دارید:

-امنیت بالا : (High)
این گزینه را در صورتی انتخاب کنید که از سیستم لینوکس خود برای اتصال به اینترنت برای مرور وب و... استفاده میکنید. در صورتی که میخواهید از سیستمتان به عنوان سرویس دهنده در شبکه استفاده نمایید از این گزینه استفاده نکنید. با انتخاب این گزینه، تنها برخی اتصالات پذیرفته میشوند .برای اتصال به اینترنت و یک شبکه بندی ساده فقط اتصالاتDNS و پاسخ های DHCPپذیرفته میشوند و بقیه اتصالات در دیوار آتش حذف خواهند شد.

-امنیت متوسط:(Medium)
این سطح امنیت را در صورتی انتخاب نمایید که مایلید دستیابی به برخی از شماره پورت هایTCP/IP را ببندید. (بطور استاندارد شماره پورتهای زیر ۱۰۲۳ .(این انتخاب دستیابی به پورتهای سرویس دهندهNFS ، سرویس گیرنده های راه دور Xو سرویس دهنده قلمX را خواهد بست.
-بدون دیوار آتش:(No Firewall)

این گزینه را در صورتی انتخاب نمایید که به یک شبکه عمومی متصل نیستید و قصد ندارید در شبکه محلی، هیچ یک از درخواستهای ورودی به سیستمتان را حذف نمایید. البته شما همچنان میتوانید فقط سرویسهایی را راه اندازی نمایید که میخواهید در سطح شبکه ارائه نمایید و سرویس های دیگر را از کار بیاندازید.

در صورتی که مایلید دسترسی به برخی سرویسهای خاص را فراهم نمایید، میتوانید روی دگمه سفارشی کردن (Customize)کلیک کنید و پذیرش درخواستهای ورودی برای سرویسهایDHCP، SSH، Telnet، WWW، Mailو FTP را فراهم نمایید .همچنین میتوانید لیستی از شماره پورتهایی که با کاما از هم جدا شده اند را برای باز کردن دسترسی به آنها، وارد نمایید.. فایل etc/services به شما نشان میدهد که چه سرویسهایی به چه پورتهایی مرتبط هستند. تصویر ۱-۴



تصویر ۱-۴ انتخاب سطح امنیتی هنگام نصب لینوکس ردهت

نکاتی ساده در امنیت لینوکس:

به منظور کنترل دسترسی‌ها و سایر مسائل امنیتی در زمینهکامپیوتر بعضی از مسئولین سایت‌ها و سایر عوامل ذینفع، هزینه‌های بسیار گزافی راصرف تهیه و خرید نرم‌افزار و سخت‌افزار می‌نمایند. ولی غافل از اینکه از کنار مسائلبسیار ساده و پیش افتاده امنیتی جهت محفوظ نگه داشتن اطلاعات می‌گذرند.

در اینمقاله کوتاه سعی شده که به ۷ مطلب ساده و پیش پاافتاده در زمینه حفاظت اطلاعاتپرداخته شود. ۷ مطلب ساده و پیش پاافتاده‌ای که با عدم رعایت آنها امکان به خطرافتادن سیستم اطلاعاتی یک سازمان وجود دارد.

خطاهای هفتگانه:

۱ -انتخاب اسم رمز ساده و یا اسامی رمز پیش فرض

۲ -باز گذاشتن درگاه‌های (port)شبکه

۳ -استفاده از نرم‌افزارهای قدیمی

۴ -استفاده از برنامه‌های ناامن و یاپیکربندی شده به‌صورت نادرست

۵ -ناکافی بودن منابع و یا نامناسب بودنارجحیت‌ها

۶ -نگهداریUserIDهای قدیمی و غیرلازم و تهیه شناسه‌های عمومی

۷ – به تعویق انداختن فعالیت‌های مهم در زمینه ایجاد امنیت

۱ -انتخاب اسم رمزساده و یا اسامی رمز پیش فرض

با توجه به سریع شدن پردازنده‌ها و امکاندسترسی به نرم‌افزارهایی که اسامی رمز را کشف می‌نمایند، حتی با انتخاب اسامی رمزپیچیده نیز، رمز می‌تواند شکسته شود.

با استفاده از ابزارهایی که در سیستم‌عامل Unix/Linuxپیش‌بینی شده است مسئول سیستم می‌تواند اجازه تولید اسامی رمز و سایرمسائل مرتبط را کنترل نماید.

در بعضی از سیستم‌عامل‌های یونیکس فایلی با نام passwdتحت etc/default/وجود دارد که راهبر یونیکس می‌تواند با ایجاد تغییراتی درآن به کاربر اجازه ندهد که اسامی رمز ساده را انتخاب نماید. اما در لینوکس بهاندازه کافی کنترل بر روی اسم رمز انجام می‌گردد و می‌توان تا حدی مطمئن بود کهکاربر نمی‌تواند اسامی رمز ساده انتخاب نماید.

فراموش نگردد که مسئول سایت(راهبر سیستم) این اختیار را دارد که اسامی رمز ساده‌ای را برای کاربران تهیهنماید، که این کار خطای مسلم راهبر می‌باشد. چرا که هر اسم رمز ساده دروازه‌ای برایورود افراد مهاجم بوده و فرد مهاجم پس از وارد شدن به سیستم می‌تواند با استفاده ازنقاط ضعف دیگر احتمالی و به‌وجود آوردن سر ریز بافر (Buffer Overflow)کنترل سیستمرا در دست بگیرد. در بسیاری از سیستم‌های فعلی Unix/Linuxمجموعه امکانات PAM(Pluggable Authentication Modules)نصب بوده و توصیه اکید می‌گردد که مجموعه زیر را برای بالا بردن امنیت سیستم تحت etc/pam.d/و در فایل passwdقرارگیرد.

passwd password requisite usr/lib/security/pamcraklib.so retry=3 passwd password required /usr/lib/security/pam_pwdb.so use_authtok

در زمان اجرای برنامهpasswd، کتابخانه‌های پویا (Dynamic)بانام‌های pamcraklib.soو pam_pwdb.soبه برنامه متصل شده و کنترل‌های لازم را انجامخواهند داد.

مجموعه نرم‌افزارهای craklibاین امکان را به سیستم اضافه می‌نمایدتا کنترل نماید که آیا اسم رمز تهیه شده توسط کاربر شکستنی است یا خیر .فراموشنگردد که فرمان passwdتابع راهبر سیستم بوده و راهبر سیستم می‌تواند اسم رمز سادهرا انتخاب نماید و این عمل گناهی نابخشودنی را برای مسئول سیستم ثبت خواهد نمود. درمورد اسامی رمز پیش فرض که در نصب بعضی سوئیچ‌ها و مسیریاب‌ها وجود دارد، راهبرسیستم می‌بایست در اسرع وقت (زمان نصب) اسامی رمز از پیش تعیین شده را تعویض نماید.

۲ – باز گذاشتن درگاه‌های شبکه

هر درگاه باز در TCP/IP می‌تواند یک دروازه ورودی برای مهاجمین باشد. باز گذاشتن درگاه‌هایی که محافظت نشده و یا بدون استفاده می‌باشند، به مهاجمین اجازه می‌دهد به نحوی وارد سیستم شده و امنیت سیستم را مخدوش نمایند .فرمان‌های زیادی مانند finger و rwhoو غیره وجود دارند که افراد مهاجم می‌توانند با اجرای آنها در شبکه و قرار دادن آدرس کامپیوتر مقصد، اسامی کاربران و تعداد زیادی از قلم‌های اطلاعاتی مربوط به کاربران را به‌دست آورده و با حدس زدن اسم رمز وارد سیستم گردند. به وسیله‌ی ابزارهاییی که در سیستم‌عامل Unix/Linux وجود دارد می‌توان درگاه‌های باز را پیدا نموده و تمهیدات لازم را انجام داد. یکی از این فرمان‌ها nmap است که با اجرای این فرمان و قرار دادن option های لازم و وارد نمودن آدرسIP ، درگاه‌های کامپیوتر مورد نظر را پیدا نموده و فعالیت‌های اخلال گونه را انجام داد .راهبر سیستم با اجرای فرمان netstat –atuv می‌تواند سرویس‌هایی که در حال اجرا هستند را مشخص نموده و به وسیله انواع روش‌هایی که وجود دارد سرویس را غیر فعال نماید و شاید یک روش مناسب پاک کردن برنامه های سرویس دهنده و یا تغییر مجوز آن به ۰۰۰(به‌وسیله فرمان (chmod باشد. در هرحال می‌توان با فرمان chkconfig اجرای بعضی از سرویس‌ها را در زمان بالا آمدن سیستم متوقف نمود. به عنوان مثال با فرمان chkconfigg –del portmap می‌توان سرویس portmapرا غیرفعال نمود.

۳ – استفاده از نرم‌افزارهای قدیمی

توصیه می‌شود که از نرم‌افزارهایی که نسخه‌های جدید آن به دلیل وجود اشکالات امنیتی در نسخه‌های قدیمی روانه بازار شده است، استفاده شود و گناهی بس نابخشودنی است که راهبر سیستم با استفاده از نرم‌افزارهای قدیمی راه را برای سوءاستفاده کننده‌گان باز بگذارد.

به عنوان مثال فرمان ls دارای مشکلی بوده که با قرار دادن آرگومانی خاص می‌توان سرریز بافر به وجود آورده و کنترل سیستم را به‌دست گرفت. شاید در ماه گذشته بود که مجموعه نرم‌افزار مربوط به نمایش اسامی فایل‌ها و شاخه‌ها (ls , lx , lr ,….)در سایت‌های مهم قرار داده شد تا استفاده کننده‌گان لینوکس آن را بر روی سیستم خود نصب نمایند.

۴ – استفاده ازبرنامه‌های ناامن و یا پیکربندی شده به صورت نادرست

به دلیل مسائل خاصی بعضی از سیستم‌ها نیاز به مجوزهای خاص داشته و اعمال مجوزها می‌تواند مسائل غیرقابل پیش‌بینی را به‌وجود آورد و ضمناً با پیکربندی نامناسب نرم‌افزار، راه برای سوءاستفاده کنندگان باز خواهد شد. به عنوان مثال نرم‌افزارهایی وجود دارد که برای اجرا شدن، مجوز s (Set UserID) را لازم داشته و این مجوز در حالتی که صاحب فایل اجرایی root باشد، بسیار خطرناک است. فرمانی که این اجازه را دارد با اجرای فراخوان‌های سیستم (System call)مانند setidتغییر مالکیت داده و قدرت rootرا کسب می‌نماید و راهبر سیستم می‌بایست تاوان این گناه نابخشودنی را نیز بدهد.

به عنوان مثال استفاده از FTP و telnet که اطلاعات را عیناً بر روی شبکه منتقل می‌نمایند، می‌تواند نگرانی‌هایی را برای مسئول سایت به وجود آورده و شاید راه‌اندازی sshd(secure shell daemon)بتواند کمی از گناهان مسئول سیستم بکاهد و در مورد پیکربندی نادرست فایل‌ها بتوان نامی از فایل rhosts. برد که مجوز نادرست می‌تواند باعث لو رفتن اسم رمز گردد. بد نیست به وسیله فرمان find اسامی فایل‌هایی که مجوز s را داشته کنترل نموده تا خدای ناکرده برنامه اجرایی با مجوز s در سیستم اضافه نگردد.

ضمناً مسئول سیستم در اجرای دستور mount نیز می‌بایست دقت فراوان داشته باشد تا برنامه‌هایی که مجوز s بر روی سی‌دی و فلاپی وجود دارد، اجرا نگردد.

۵ – ناکافی بودن منابع و یا اختصاص دادن ارجحیت نامناسب

کم نمودن هزینه‌های مربوط به امنیت و عدم آموزش‌های لازم و تهیه ننمودن نرم‌افزارهای بازدارنده می‌تواند تعدادی مسائل غیرقابل پیش‌بینی به وجود آورد. مخصوصاً جابجایی اولویت‌های هزیه نمودن اعتبارات می‌تواند امنیت سیستم را خدشته‌دار نماید. لازم به یادآوری است که این مطلب فنی نبوده و مدیریتی می‌باشد ولی راهبر سیستم می‌بایست مرتباً نکات لازم را در این زمینه به مقامات مسئول گوشزد نماید تا مدیریت ارشد سازمان بیش از بیش به اهمیتِ امنیت پی برده و هزینه‌های لازم را تامین نمایند. عدم اطلاع رسانی مسؤول سایت دراین زمینه به مدیریت‌های مافوق که احتمالاً در این زمینه نیز تخصصی ندارند، گناهی نابخشودنی است.

۶ -نگهداری User ID های قدیمی و غیرلازم و تهیه شناسه‌های عمومی

نگهداریUserID های قدیمی و شناسه‌هایی مانند TEST می‌تواند معضلات زیادی را به وجود آورده و امکان سوء استفاده را بالا برد. تهیه‌ی شناسه‌های عمومی نیز به دلیل نامشخص بودن هویت اصلی کاربر می‌تواند مشکل‌زا باشد. مسؤول سایت می‌بایست رویه‌ای را برای کشف UserID های غیر فعال اتخاذ نماید و به وسیله‌ی هر روشی که صلاح می‌داند پس از تهیه فایل پشتیبان لازم، UserIDهای غیرفعال را در مقاطع معینی متوقف نماید و شاید یکی از بهترین روش‌ها برای این کار عوض نمودن اسم رمز باشد. به عنوان مثال به وسیله دستور زیر می‌توان UserID با نام someoneرا غیر فعال نمود:

chmod 000 /home/someone

تولید UserID های عمومی مانند test و guest و غیره که مورد علاقه بسیاری از مهاجمین است، یکی از گناهان غیرقابل بخشش راهبر سیستم می‌باشد.

۷ -به تعویق انداختن فعالیت‌های مهم در زمینه ایجاد امنیت

با کم اهمیت دادن مسائل حفاظتی از جمله عدم نصب ترمیم‌ها (Patch)و عدم تهیه فایل‌های پشتیبان، می‌توان گفت که مسئول سیستم تیر خلاص را به کامپیوتر تحت الحفظ خود شلیک نموده است و چنان گناهکار خواهد بود که بخشش جایز نمی‌باشد.

مقایسه امنیت در ویندوز و لینوکس:

امنیت نرم افزاری به طور کلی یک مفهوم انتزاعی است که به پارامترهای فکری هر شخص وابسته است. چون درجه آسیب پذیری امنیتی، از خط به خط کدهای برنامه نویسی به وجود می آید. هر حوزه امنیتی از درجه حساسیت خاصی برخوردار است که ممکن است برای کاربران یک پایه فوق العاده مهم باشد یا بر عکس. در نتیجه تعابیر بسیار زیادی برای امنیت وجود دارد. مخصوصا اگر بخواهید درباره امنیت برنامه کامل و پیچیده ای مانند سیستم عامل ها و مثلا ویندوز و لینوکس صحبت کنید.

پارامترهای عینی متعددی برای درجه بندی امنیت وجود دارد که می توان از آن طریق باگ های برطرف شده یک مجموعه نرم افزاری خاص را محاسبه کرد. هنگامی که ویندوز و لینوکس با هم مقایسه می شوند، نقطه ضعف های امنیتی دیگری ظاهر می شوند که در این مقایسه دخیل هستند. اخیرا موسسه CERT گزارشی از اسیب پذیری های استاندارد این دو سیستم عامل را منتشر نمود که طی آن ۲۵۰ حفره امنیتی حساس برای ویندوز گزارش شده کخ ۳۹ حوزه آن در لیست خطرناک ترین نقاط ضعف امنیتی قرار دارند و برای لینوکس ردهت نیز ۴۶ حفره امنیتی گزارش

شده است که سه حفره آن در لیست آسیب پذیری های امنیتی بسیار خطرناک قرار دارند .هزاران گزارش از مقایسه امنیتی میان لینوکس و ویندوز وجود دارد. اما مبنای این تحقیق CERT گزارش هایی بوده که توسط کاربران موسسات دولتی ارائه شده اند و در ان حفره های امنیتی خطرناک مشابهی گزارش شده است. رلایل قانع کننده ای برای ان تفاوت امنیتی میان دو سیستم عامل وجود دارد. به عنوان مثال مدل توسعه اپن سورس برنامه های لینوکس، امکان گزارش . شناسایی باگ های را در فاصله زمانی زودتری امکان پذیر می کند. این مزیتی است که در ویندوز از آن بی بهره است. دیگر پارامترها نامطلوب برای ویندوز، اعتماد بسیاری از کرنل برنامه های کاربردی ویندوز به RPC) Remote Procedure(،متد توسعه جامعه کامپیوترهای خانواده اینتل،است. نتیجه این رویه،ضعف قوانین دیواره های آتش در مقایسه با سیستم عامل هایی مانند لینوکس است که در سطح بسیار کمتری از RPC استفاده می کنند. میان این دو سیستم عامل، تفاوت های امنیتی دیگر نیز وجود دارد که برای کاربران پایانه ای این سیستم عامل ها بروز خواهد کرد و در حوزه آسیب پذیری های مدیریتی سیستم گنجانده نمی شوند . برای مثال ویندوزها قطعا زمینه مساعدتری برای شیوع ویروس ها در سمت کاربران پایانه ای داراست که ایمنی سیستم به خود کاربر و استفاده از آنتی ویروس ها واگذار شده است. اخیرا ویندوز شاهد ربودن اطلاعات سیستم ها توسط ابزارهایی به نام Spyware یا جاسوس افزار بود که می توانند به صورت محرمانه و پنهانی اطلاعات شخصی شما را در سطح اینترنت پخش کنند که در وبگردی، از روی خطا یا اختیار آن ها را بر روی سیستم فعال می کنید. مایکروسافت جدیدا برای مقابله با این پدیده یک شرکت ضد ویروس و ضد جاسوس افزار را خریداری کرده است .امکان دارد که بتوان توسط مدیر سیستم یا کاربران ارشد، ویندوز لینوکس را به درستی مدیریت کرد. اما بسیاری از برنامه های کاربردی دیگر ویندوز با این سیستم یکپارچه نیستند و نیاز است توسط کاربران، با مجوزدهی صحیح مدیر سیستم، اجرا شوند. اما برنامه های کاربردی لینوکس غالبا نیازمندی های امنیتی را رعایت کرده و در نتیجه کمتر می توانند مورد سوء استفاده قرار گیرند. ویندوز تنها از طرف توسعه دهنده خود دچار مشکل است که دوست دارد یک سیستم ساده را خلق کند که برای استفاده کننده بسیار آسان باشد. اما این سایت با هزینه بسیار زیادی از ناحیه امنیت سیستم همراه است. این امتیاز حتی موجب سست شدن امنیت سیستم نسبت به نسخه های قدیمی تر می شود، ضعفی که لینوکس هنوز با آن مواجه نشده است. لینوکس نیز دارای ضعف های امنیتی است.
عموما سازندگان خودشان سخت افزار یا درایوهای مخصوص خود را برای سازگاری با ویندوز توسعه می دهند. اما در جامعه لینوکس غالبا از مهندسی معکوس برای ساخت این محصولات استفاده می شود. در سیستم عامل های اپن سورس، گاهی قدم اول همین مهندسی معکوس، غیرقابل پیش بینی خواهد بود. در برخی موارد، سازگاری یک سخت افزار با لینوکس، به کندی صورت می پذیرد که نسبت به ویندوز، شاید ماه ها و شاید تا دو سال به طول بینجامد. خوشبختانه با پشتیبانی شرکت هایی مانند IBM و Novell از استانداردهای اپن سورس، برخی از مشکلات پیچیده حل شده و پروسه سازگاری با لینوکس ساده تر شده است. فارغ از محیط های گرافیکی، رابط خط فرمان لینوکس برای بسیاری از کاربران سخت و پیچیده است و آنان درک درستی از آن ندارند. همین امر موجب می شود مدیران سیستم ها، از به کار گرفتن ابزارو مفاهیم پیچیده برای برقرای امنیت در سیستم اجتناب کنند .لینوکس اصولا دارای قابلیت های سیستم عاملی یک شبکه است و در نصب پیش فرض، بسیاری از برنامه های کاربردی شبکه فعال نیست. این موضوع می تواند آسیب پذیری های ناشناخته ای را به وجود آوردکه هر یک از آن ها تهدیدی امنیتی برای سیستم عامل محسوب شوند. خوشبختانه این موارد و بسیاری از نقاط ضعف دیگر لینوکس، با به کارگیری یک لایه سخت گیرانه امنیتی و ابزار ساده خط فرمان برای آسان کردن کار مدیر سیستم بهبود یافته است. یکی دیگر از

امتیازات لینوکس، وجود تعداد بی شماری ابزار متنوع مبتنی بر لینوکس برای فراهم کردن امنیت در سیستم (Nessus)امکان پویش شبکه، حفره های موجود بر روی سیستم راه دور، باگ های نرم افزاری اجرا شده بر روی شبکه و دیگر ابزار نصب شده موجود در سیستم را فراهم می کند Nessus . در سیستم هایی که به تازگی نصب شده اند، می تواند به کار گرفته شود . علاوه بر این قابلیت گزارشگیری از یک سیستم سرور را در یک دوره مشخص دارد .

Nmapابزار دیگری برای اسکن شبکه است که نسبت به Nessus کاربردهای کمتری دارد. این ابزار می تواند به صورت پیش فرض همراه لینوکس نصب شود. گذشته از سودمندی این ابزار برای هر کارشناس IT ، هنوز ابزاری به راحتی آن در پیکربندی لینوکس ارائه نشده است. متخصصان امنیتی در هنگام اتصال به یک شبکه اینترنت از فایروال نیز استفاده می کنند. فایروال ها به صورت بسته های افزودنی به سیستم سرور برای تامین امنیت بیشتر به کار گرفته می شوند. ابزاری مانند، ACIDمی توانند اطلاعات را آنالیز کرده و مطابق این اطلاعات مشخصه های یک را تشخیص دهد ACID .امکان گزارش از طریق ایمیل را دارد و از طریق یک رابط گرافیکی، تمامی اطلاعات یک بسته فعال شبکه را نمایش می دهد. استفاده از این ابزار برای هر شرکتی که در حوزه امنیت IT فعالیت می کند، توصیه می شود ACID .ممکن است گزارش های متناقض و ناصحیح بسیاری برای مدیر سیستم تولید کند و از این رو نیاز به تنظیم و پیکربندی همیشگی آن وجود دارد. فارغ از سیستم عاملی که استفاده می کنیدف عدم به کارگیری ابزار مناسب، می تواند یکپارچگی امنیتی کار شما را به خطر بیندازد. عدم پشتیبان گیری کافی ضعیف بودن رمزهای عبور، اشتراک گذاری حساب های کاربری و پروژه های امنیتی که توسط تیم بازرسی نادیده گرفته شوند، و بازبینی و نظارت ضعیف، از دیگر موارد نقض امنیت سیستم هستند.