بنام خدا

امنیت سیستم عامل

(رشته امنیت اطلاعات)

Operating System Security

ویژه دانشجویان

تدوین : علی ثاقب موفق

پیشگفتار اهمیت امنیت سیستم عامل :

همانگونه که می دانیم محور و هدف نهایی در اعمال امنیت اطلاعات، خود اطلاعات است. داده ها و اطلاعات به دو شیوه می تواند نگهداری می شود. روش اول این است که اطلاعات بـر روی کاغـذ و ابزارهـای مشـابه دستی و سنتی نوشته یا ترسیم شوند و روش دوم اینکه به شیوه مکانیزه در سیستمهای رایانه ای قرار گیرند.

یکی از مهترین ابزارهای کسب اطلاعات منسجم و سازمان یافته، رایانه است. ولی رایانه یک سخت افزار است و انسان نمی تواند به آسانی با آن ارتباط اطلاعاتی داشته باشد و بنابراین نیاز به نرم افزاری واسط دارد تـا از طریق آن دستورات و فرمان های خود را به رایانه بگوید. نام این نرم افزار سیستم عامل است.

رایانه، از جمله مهمترین ابزارهای هدفمند ورود انسان به دنیای اطلاعات و اینترنت اسـت. سیسـتم عامـل رایانه نقش واسط بین انسان، بعنوان کاربر و رایانه را بعهده دارد. لذا امنیت سیستم عامل از امنیت به سزایی بر خوردار است.چرا که ما از طریق سیستم عامل به رایانه و منابع نرم افزاری و سخت افـزاری آن دسترسـی داریم و سپس از آن مسیر نیز با دنیایی از اطلاعات و اینترنت ارتباط برقرار می کنیم.

سیستم عامل نرم افزاری جامع و کامل است که به محض نصب و راه اندازی بر روی رایانه، کنترل و مدیریت کلیه منابع نرم افزاری و سخت افزاری و ذخیره سازی رایانه را در اختیار گرفته و رابـط بـین کـاربر و رایانـه خواهد شد.

فواید و مضرات ماشین بدون سیستم عامل:

فواید ماشین بدون سیستم عامل شامل دسترسی آزادانه به رایانه به طوریکه استفاده کننـده مـی توانـد هـر کاری انجام دهد و سیستم عامل مانع وی نخواهد شد. کاربر به ماشین دسترسی Online داشته و می تواند پیشرفت برنامه اش را دنبال نماید.

مضرات ماشین بدون سیستم عامل این است که کاربر مجبور است برنامه اش را خودش شخصا وارد سیستم و رایانه نماید و ممکن است استفاده کننده در هنگام استفاده ، دچار اشتباه شود.

وظایف سیستم عامل با دید امنیت اطلاعات:

- تعامل موثر با کاربر و ارتباط بین کاربر رایانه و نرم افزار و سخت افزارهای رایانه User Friendly
- مدیریت و سازماندهی برنامه ها، پرونده ها و نرم افزارهای موجود بر روی رایانه , FAT32 , NTFS FAT ....
- راه اندازی، مدیریت و بکارگیری سخت افزار متصل به رایانه Hardware Driver
- مدیریت و سازماندهی ارتباط با شبکه Networking

افزایش روزافزون اطلاعات، اهمیت بررسی سریعتر و ساده تـر اطلاعـات، گسـترش شـبکه هـای رایانـه ای و ارتباط بین آنها از مواردی است که آسیب پذیری و امکان نفوذ به هر رایانه در هرزمان و از هرجـا را فـراهم کرده است. وجود نقطه ظعف و آسیب پذیری در سیستم عامل، منجر به نفوذ در آن می شـود. لـذا سیسـتم عامل بعنوان واسط نرم افزاری بین ما و دنیای مجازی به منزله مهمترین مولفه در امنیت اطلاعـات و شـبکه های رایانه ای است و در صورت بی توجهی به آن مشکلات امنیتی زیر را خواهیم داشت:

- امکان شنود و دزدی اطلاعات از طریق حفره های امنیتی و Backdoor
- واکشی تدریجی اطلاعات از منابع اطلاعاتی رایانه و نرم افزارهای سیستمی و کاربردی
- اختلال و ایجاد مشکل برنامه ریزی شده تدریجی در عملیات رایانه
- ویروس های رایانه ای و اختلالات مترتب به آن
- بدست گرفته کنترل های رایانه ای و نفوذ به آن بدون مجوز
- مختل کردن کلیه ارتباطات شبکه ای رایانه
- جایگزینی اطلاعات غلط در سیستمهای نرم افزاری و اطلاعاتی

حال اگر رایانه، از سیستم عامل ویندوز، استفاده کرده باشد و یا اینکه سیستم عامل اصلی رایانه و یـا سـرور باشد، بنا بر اینکه این سیستم عامل بیشتر در معرض خطر ویروس و هکر ها خواهد بود، لـذا مقولـه امنیـت برای این دسته از رایانه ها و سرورها بسیار جدی ترخواهد بود.

انتخاب نوع سیستم عامل:

- سیستم عامل متن باز مثل لینوکس Open Source
- سیستم عامل ویندوز Windows Operating System

الف) ویژیهای مرتبط با امنیت سیستم عامل ویندوز:

- سیستم عامل ویندوز متعلق به شرکت مایکروسافت بوده و کد برنامه اش در اختیار ما نمی باشد.
- امکان تغییر و سفارشی سازی آن بنا بر نیاز ها و سیاست های ما وجود ندارد.
- احتمال وجود کانال های مخفی (Back door) و آسیب رسانی از طریق آن وجود دارد.
- پشتیبانی رسمی و مطمئن ویندوز در ایران وجود ندارد.

ب) ویژگیهای مرتبط با امنیت سیستم عامل لینوکس

- سیستم عامل لینوکس یک سیستم عامل متن باز است
- برنامه و کد آن در اختیار می باشد
- امکان فارسی و بومی سازی آن و تغییر برنامه منطبق با نیازها میسر می باشد.
- اجرای برنامه یا هر موضوع تحت این سیستم عامل آزاد است.
- توزیع نسخه تغییر یافته آن برای بهره برداری دیگران آزاد و رایگان است.
- حمایت برنامه نویسان، دانشگاه ها و شرکت های تجاری و مراکز علمی از آن
- همراهی با تحولات سخت افزاری و نرم افزاری فناوری اطلاعات
- برنامه نویسان زیادی در توسعه آن سهیم بوده اند.

فناوری های واکشی امنیت اطلاعات در سیستم عامل:

دیواره آتش:

وجود دیواری از آتش، امکان عبور از آن و سپس ورود به سیستم عامل را برای مهاجمان غیرممکن و سخت می سازد. هدف آن جلوگیری از ارتباطات غیرمجاز در درون یا برون شبکه داخل سازمان با میزبان است و هدف آن محافظت از ترافیک نامطلوب اینترنت برای کنترل ارتباطات سازمانها با یکدیگر است.

کلمات عبور:

استفاده از کلمه عبور یکی از ساده ترین شیوه های اعمال امنیت نرم افزاری است و شامل عبارت یا حروف متوالی رمزی است که فرد برای بدست آوردن جواز دسترسی به اطلاعاتی مثل فایل، برنامه و سیستم رایانه باید وارد نماید و برای شناسایی و اهداف امنیتی بکار می رود. به هر کاربر کلمه عبور اختصاص می یابد تا به بخشی از منابع نرم افزاری و سخت افزاری رایانه دسترسی داشته باشد.

زیست سنجی:

می توان از ویژگیهای زیستی منحصر به فرد انسان برای حصول اطمینان از هویت کاربر استفاده نمود. زیست سنجی یک فناوری سنجش و تحلیل داده های زیستی است و برای سنجش و تحلیل ویژگی های بدن انسان مثل اثر انگشت ، قرنیه ، شبکیه چشم، الگوی صدا و الگوی چهره بکار می رود و به تعیین اعتبار کاربر اشاره دارد. معمولا این ویژگی با یک الگوی مرجع مقایسه می شود. ویژگیهای زیست سنجی می تواند در کنار و یا بعنوان جایگزین کارت هوشمند استفاده شود.

آشکار ساز نفوذ IDS :

سیستم تشخیص نفوذ Intrusion Detection System یک نظام تدافعی است که کار آن تشخیص و احتمالا ممانعت از فعالیتهایی است که ممکن است امنیت شبکه را به خطر بیاندازد. که در صورت داشتن امکان جلوگیری از نفوذ به آن IPS یا Intrusion Prevention System هم اضافه خواهد شد و می تواند نمایی از فعالیتهای غیر عادی و هشدار را اعلان نماید که منابع رایانه ای و شبکه را هدف قرار داده اند و مهاجمان

داخلی و خارجی را تشخصی و در صورت لزوم مانع از ورود آنها شود. مثـل Cisco iis Real Secure snort IDS

واقع نگاری و logging **:**

کلیه کارهایی که ما بر روی رایانه و شبکه انجام می دهیم، در جایی درون رایانه و یا شبکه ثبت وضبط مـی شود که به آن Log فایل ها می گویند. به عبارت دیگر به ثبت اعمال یا تـراکنش هـای انجـام شـده توسـط کاربران یا برنامه ها اشاره دارد که معمولا برای تعقیب و پیگیری داده ها در تحلیل آتی مـورد اسـتفاده مـی باشد.

دسترسی راه دور: Remote Access :

امکان کار با رایانه از راه دور را میسر می سازد و به دسترسی به یک سیستم یا برنامه، بدون نیاز به حضـور فیزیکی توجه دارد. دسترسی راه دور خطر جعل هویت را در پی دارد و برای امن سازی این نوع ارتباط بایـد ایمن ترین پروتکل ها و فناوری را به خدمت گرفت. زیرا ممکن است که یک فرد یا فرآیند بـرای اتصـال از راه دور، نیاز به دسترسی بر طبق مجوز دسترسی داشته باشد و این فناوری در سـطح میزبـان قابـل پیـاده سازی است.

انتخاب سیستم عامل متناسب با ملاحظات امنیت اطلاعات:

نوع و میزان محرمانگی اطلاعات، در انتخاب نوع سیستم عامل موثر خواهد بود. وقتی رایانه ای خریداری می شود ، انتخاب سیستم عامل نیز تا حدودی انجام شده است زیرا عموما سیستم عامل نیز بر روی آن نصـب و در اختیار قرار می گیرد. بعنوان مثال رایانه DELL به همراه سیستم عامل ویندوز عرضه می شود. لیکن مـی توان در هر زمان لازم سیستم عامل نصب شده را تغییر داد.

متداول ترین سیستم عامل های موجود:

ویندوز: Windows :

سیستم عاملی کارا و مبتنی بر گرافیک و دارای GUI ، نسبت به سیستم عامل مبتنی بر خط فرمان و متن Ms dos است و ارتباط کاربری آن مناسب می باشد.

سیستم عامل Mac os **:**

سیستم عامل فوق توسط اپل ارائه می شود و از آن بر روی رایانه های مکینتاش استفاده می گردد. این سیستم عامل از نظر شکل ظاهری شبیه ویندوز است.

سیستم عامل لینوکس : Linux & Unix & Redhat :

این سیستم عامل و سایر سیستم عامل های مبتنی بر یونیکس که به نحوی مشتق شده از یونیکس می باشند در همین خانواده قرار می گیرند و در ایستگاه های شبکه ای خاص و یا سرویس دهندگان شبکه مثل سرویس دهنده وب و پست الکترونیکی استفاده می گردد. استفاده از این سیستم عامل به لحاظ تخصصی و حرفه ای، توسط کاربران عادی مشکل است و استفاده از آن به دانش و مهارت های خاصی نیاز دارد. همین موضوع دلیل عدم گسترش عمومی آنان است.

مهمترین نقاط آسیب پذیر ویندوز:

سیستم عامل ویندوز به لحاظ استفاده رایج و عمومی آن بر روی رایانه های شخصی و سرورهای رایانه ای بیشتر مورد حمله واقع می شود و اکثر کرم ها و حملات موفقیت آمیز در اینترنت، بدلیل وجود نقاط آسیب پذیر در تعدادی اندک از سرویس های سیستم های عامل متداول است. مهاجمان از نقاط ضعف امنیتی شناخته شده ویندوز استفاده نموده و با استفاده از ابزارهای متنوع، بر سازمان و شرکت هایی که هنوز مسائل امنیتی و حفره های آسیب پذیر خود را برطرف نکرده اند. متمرکز می شوند.

این مهاجمان، کرم هایی نظیر، بلستر، اسلامر و Code Red را در شبکه منتشر می کنند تا نقاط اسیب پذیر را کشف نمایند. لذا شناخت نقاط آسیب پذیر و سپس بررسی علت وجود ضعف امنیتی می تواند تا حدودی

سیستم عامل را ایمن نماید. همچنین بایستی سیستم عامل های در معـرض تهدیـد، روش هـای تشـخیص آسیب پذیری سیستم و نحوه مقابله یا پیشگیری از آنها را بررسی کرد.

مهمترین نقاط آسیب پذیری ویندوز عبارتند از:

IIS INTERNET INFORMATION SERVICES

MSSQL MICROSOFT SQL SERVER

IE INTERNET EXPLORER

MDAC MICROSOFT DATA ACCESS COMPONENTS

WSH WINDOWS SCRIPTING HOST

WINDOWS PEER TO PEER FILE SHARING P2P

SNMP SIMPLE NETWORK MANAGEMENT PROTOCOL

اولین نقطه آسیب پذیر : iis :

نصب برنامه iis با تنظیمات و پیکربندی پیش فرض، آسیب پذیری خود را به اثبات رسانده و زمینه تهدیدات زیر را فراهم می نماید:

- غیر فعال نمودن سرویس DOS : Denial Of Service و از کـار انـداختن سـرویس. در ایـن حالـت مهاجم با دسترسی های مکرر و فراوران، یک سرویس خاص را در شبکه از کار می اندازد.
- نمایش و به مخاطره انداختن فایل ها و داده های حساس
- اجرای دستورات خودسرانه (اختیاری)
- به مخاطره انداختن کامل سرویس دهنده: Server

مواقعی خطر و تهدید از کار افتادن یک سرویس از روی سرویس دهند وجود دارد که در طراحی برنامه های فوق، عملکرد آنان با لحاظ نمودن مسائل امنیتی در یک محیط عملیاتی و تولیدی مورد توجه قـرار نگرفتـه است. برخی از نمونه برنامه های ارائه شده به همراه IIS ، امکان مشاهده و بازبینی فایـل هـای دلخـواه و یـا

دستیابی از راه دور به اطلاعات حساس، نظیر رمز عبور مدیریت سیستم را فـراهم مـی نمایـد. عـدم بهنگـام سازی و نگهداری مناسب IIS پس از نصب اولیه، از دیگر مواردی است که زمینه تهاجم را فراهم می آورد.

مثلا نقاط آسیب پذیر nt.dll.webdav در iis 5.0 امکان حملات از نوع dos یا غیر فعال نمودن سـرویس را فراهم و مهاجمان در ادامه قادر به ایجاد و اجرای اسکریپت های مورد نظر خود بر روی سرویس دهنده مـی گردند. امکاناتی که با توجه به ضرورت روی iis نصب می شوند مثل coldfusion , php نیز می توانند زمینه بروز نقاط آسیب پذیر را فراهم سازند. این نوع آسیب پذیری بدلیل عدم پیکر بندی صحیح و یا وجود ضعف و اشکال امنیتی در محصول نصب شده است که به iis نیز سرایت می کند. (توارث مشکلات و ضـعف هـای امنیتی از یک محصول به محصول دیگر).

سیستم عامل های در معرض تهدید :

- ویندوز nt 4.0 که از iis 4.0 استفاده می کند
- ویندوز ۲۰۰۰ سرویس دهنده که از iis 5.0 استفاده می کند
- ویندوز xp نسخه professional که از نسخه iis 5.1 استفاده می کند.

نحوه تشخیص آسیب پذیری سیستم:

در صورتیکه برنامه iis به صورت پیش فرض و استاندارد نصب و یا اینکه patch های مربوطه روی آن نصـب نشده باشد. برای آن می توان به مستندات امنیتی مرتبط به iis از مرکز iis مایکروسافت استفاده نمود. برنامه baseline Microsoft security analyser که شامل روتین های حفاظتی مناسـب و مـرتبط بـا iis اسـت را دریافت و از آن به منظور بررسی وضعیت امنیتی iis استفاده بعمل آید.

نحوه حفاظت در مقابل نقطه آسیب پذیر:

بروز رسانی و نصب آخرین patch ارائه شده ، autopatch , windows patch گزینه مناسـب جهـت بهنگـام سازی iis با توجه به آخرین patch های ارائه شده است. برنامه hfnetchk یـا checker network security

hotfix در مسیر http://www.microsoft.com/technet/security/tools/htnetchk.asp کمک لازم در پویش و بررسی محلی و یا ارائه راه دور سیستم برای patch های موجود را ارائه می نماید. در صورتیکه از برنامه های اضافه شده ای نظیر coulddusion , perliis, php به همراه iis استفاده می گردد لازم است به سایت های عرضه کننده هریک از محصولات فوق مراجعه و نسبت به دریافت آخرین patch ارائه شده در رابطه با هر محصول آگاه و آن را با توجه به توصیه های انجام شده بر روی سیستم نصب نمود.

امکان update windows و سایر سرویس های بهنگام سازی ارائه شده توسط مایکروسافت شامل Patch های لازم و مرتبط با محصولات اضافه شده سایر شرکت ها در برنامه iis مایکروسافت بوده و لازم است مدیران سیستم بهنگام سازی محصولات اضافه شده (غیر مایکروسافت) در iis را خود راسا انجام دهند.استفاده از برنامه کمکی lockdowniis جهت نصب مطمئن تر: مایکروسافت، ابزاری ساده به منظور ایمن سازی نصب iis را ارائه کرد که ویزارد lockdown iis نامیده می شود که در آدرس

http://www.microsoft.com/technet/security/tools/locktool.asp

قرار دارد. اجرای برنامه فوق در حالت custom و یا expert می تواند تغییرات مورد نظر را در ارتباط با نصب iis مشخص نمود. بدین ترتیب امکان اعمال تغییرات زیر در رابطه با نصب iis فراهم می گردد.

- غیر فعال نمودن webdav مگر اینکه محیط مورد نظر شما به وجود آن برای نشر محتوی وب نیاز داشته باشد.
- غیر فعال نمودن extension (isap های غیر ضروری نظیر htr,idq,ism printer)
- حذف نمونه برنامه های ارائه شده به همراه iis
- منع سرویس دهنده وب از اجراء دستورات سیستمی متداول که عموما توسط مهاجمان استفاده می گردد. (نظیر cmd.exe , tftp.exe)

استفاده از urlscan برای فیلتر نمودن درخواست های http با تعداد زیادی از حملات مرتبط با نقاط آسیب پذیر iis نظیر code blue و خانواده code red از کد های مخربی که بصورت درخواست های http

سازماندهی می شوند. (حملاتی از نوع buffer overflow) فیلتر urlscan را می توان به گونه ای پیکربندی نمود که باعث عدم پذیرش اینچنین درخواست های hslockdown ارائه ولـی مـی تـوان آن را ار آدرس نیـز دریافت کرد.

http:// www.microsoft.com/technet/security/tods/urlscan.asp

اعمال سیاست های امنیتی در ویندوز:

برای اعمال دستورات و سیاست های امنیتی بر روی سیستم عامل ویندوز بایستی پس از ورود به بخش کنترلی control panel ویندوز ، به قسمت administrative tools می رویم و از آنجا از طریق local security, Event Viewer اعمال سیاست های لازم را انجام می دهیم. این ابزار امکان مدیریت سطح بالا بر روی سیستم کامپیوتر را برای ما فراهم می نماید، توسط این ابزار می توانیم یک سری محدودیت ها و تنظیمات و کانفیگ های خاص بر روی سیستم عامل در هنگام عملکرد اعمال نماییم.

به عنوان مثال یک user در سیستم عامل ویندوز شما برای اکانت خود password انتخاب و ذخیره می کند ، شما از طریق اعمال تنظیمات در این قسمت می توانید ویندوز را طوری config نمایید که یوز هایی که از طریق ویندوز برای اکانت خود password تنظیم می نمایند جهت امنیت بیشتر پسورد آن ها چند کارکتر باشد و از n مقدار کارکتر کمتر کاربر نتواند برای اکانت خود رمز عبور انتخاب نماید. همچنین اگر یک کاربر بر روی اکانت خود در ویندوز رمزعبور اعمال نموده است و مدت هاست که از اعمال این رمز عبور و استفاده از این رمز عبور توسط کاربر می گذرد ، طبیعی است که پس از گذشت مدت زمان زیاد از یک پسورد ممکن است سایرین از آن مطلع شوند و این خطر امنیتی بزرگی محسوب می شود.

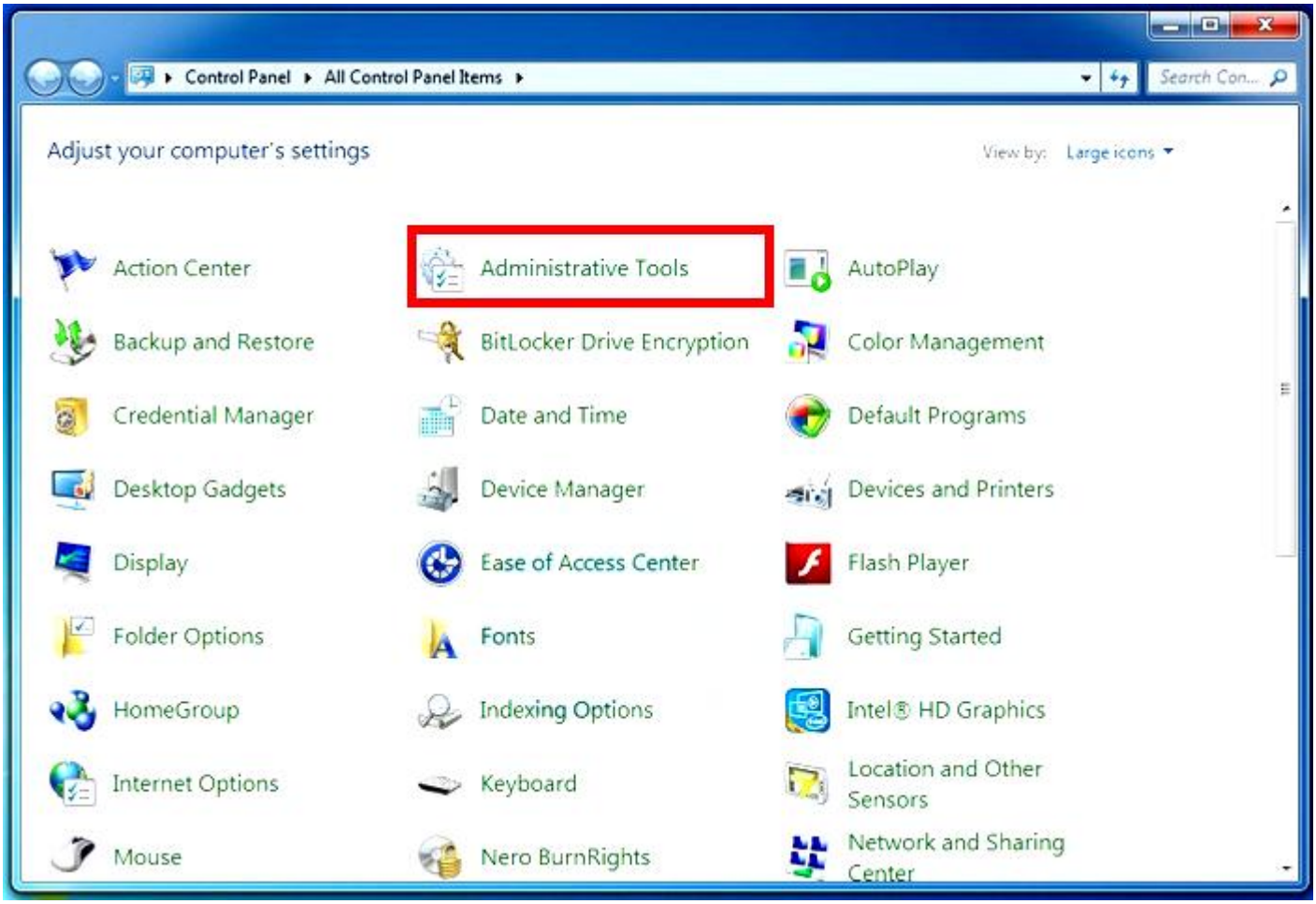
یکی دیگر از کارایی های این قسمت این است که می توانید از این طریق برای یوزر های ویندوز تایم یا زمان تنظیم کنید که مثلا پس از گذشت ۳۰ روز استفاده از یک پسورد ، ویندوز کاربر را جهت افزایش امنیت ویندوز ملزم به تغییر رمز عبور نماید . که این یکی دیگر از کانفیگ های مورد نظر در این قسمت می باشد .

همچنین از طریق پیکربندی ین قسمت می توانید یک کانفیگ بسیار حرفه ای دیگر جهت افزایش امنیت ویندوز اعمال نمایید ، فرض کنید که بر روی اکانت admin ویندوز خود (آموزش فعال کردن اکانت administrator در ویندوز) یک password ست نموده اید ، فرض کنید یک هکر تصمیم دارد وارد سیستم رایانه شما شود و با این صفحه password مواجه می شود ، در این صورت بسیار طبیعی و متداول است که هکر پسورد های مختلفی حدس بزند و آن ها را یکی یکی امتحان کند تا بتواند وارد محیط ویندوز شما شود و اطلاعات شما مورد نفوذ قرار گیرد ، یکی از امکانات local security این است که می توانید برای تعداد دفعات وارد نمودن پسورد اشتباه محدودیت اعمال نمایید ، بدین معنا که اگر کاربری ۵ بار رمز عبور را اشتباه وارد کرد ، یوزر کاربر بلاک شود و مدت زمان برای بلاک ماندن آن یوزر اعمال نمایید ، به عنوان مثال یک کانفیگ این چنینی انجام دهید که اگر رمز عبور ۵ بار توسط کاربر اشتباه وارد شد این یوزر برای ۹۸۰ دقیقه داخل لیست بلاک قرار بگیرد . در قسمت local Security جهت امنیت بیشتر می توانید حتی یوزرهای ویندوز را disable و enable نمایید.

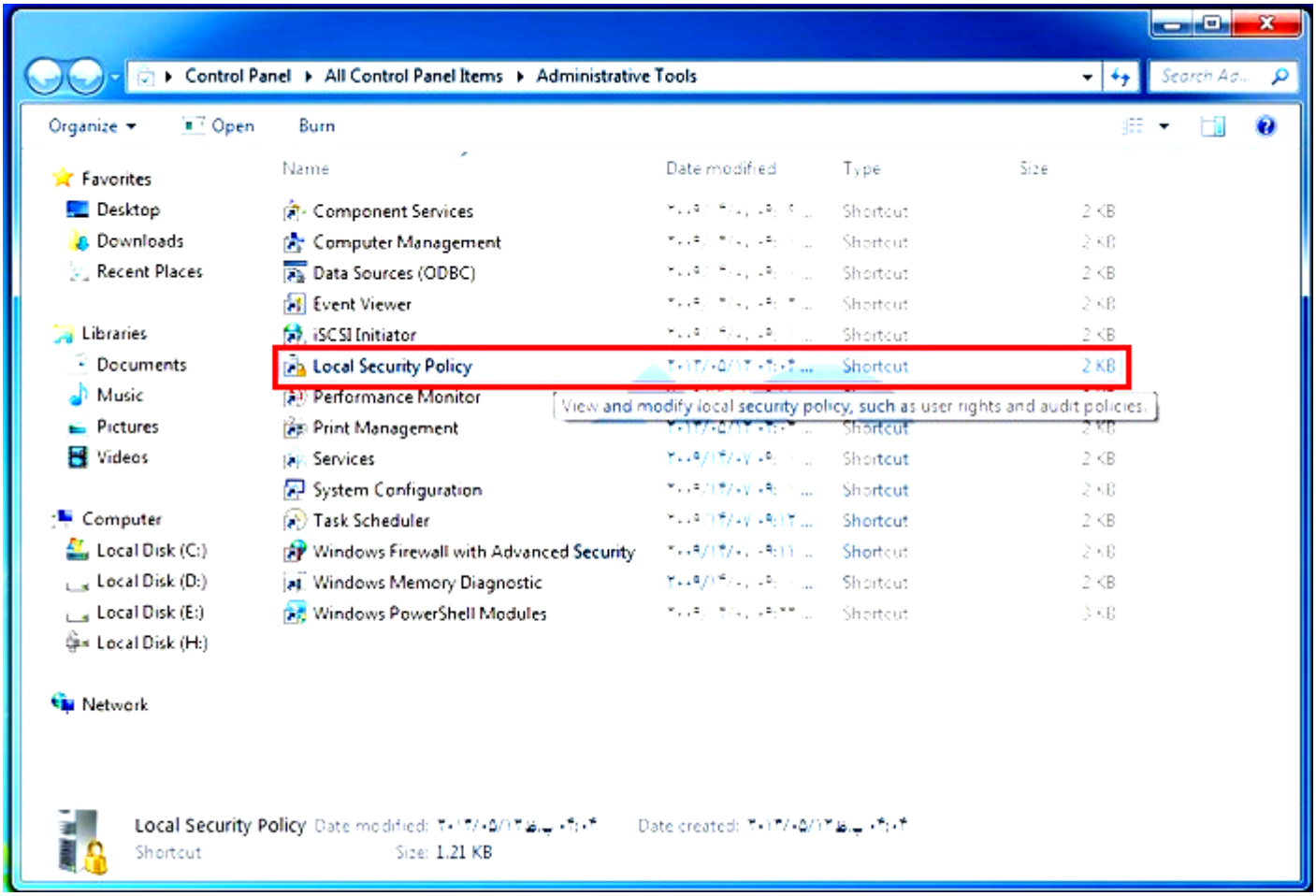
تذکر : از طریق local security می توانید محدودیت های بسیار زیاد و پیشرفته ای را بر روی کامپیوتر و شبکه Local و ... اعمال نمایید .

آموزش یک : اعمال محدودیت برای انتخاب تعداد کارکتر های پسورد توسط کاربر در ویندوز

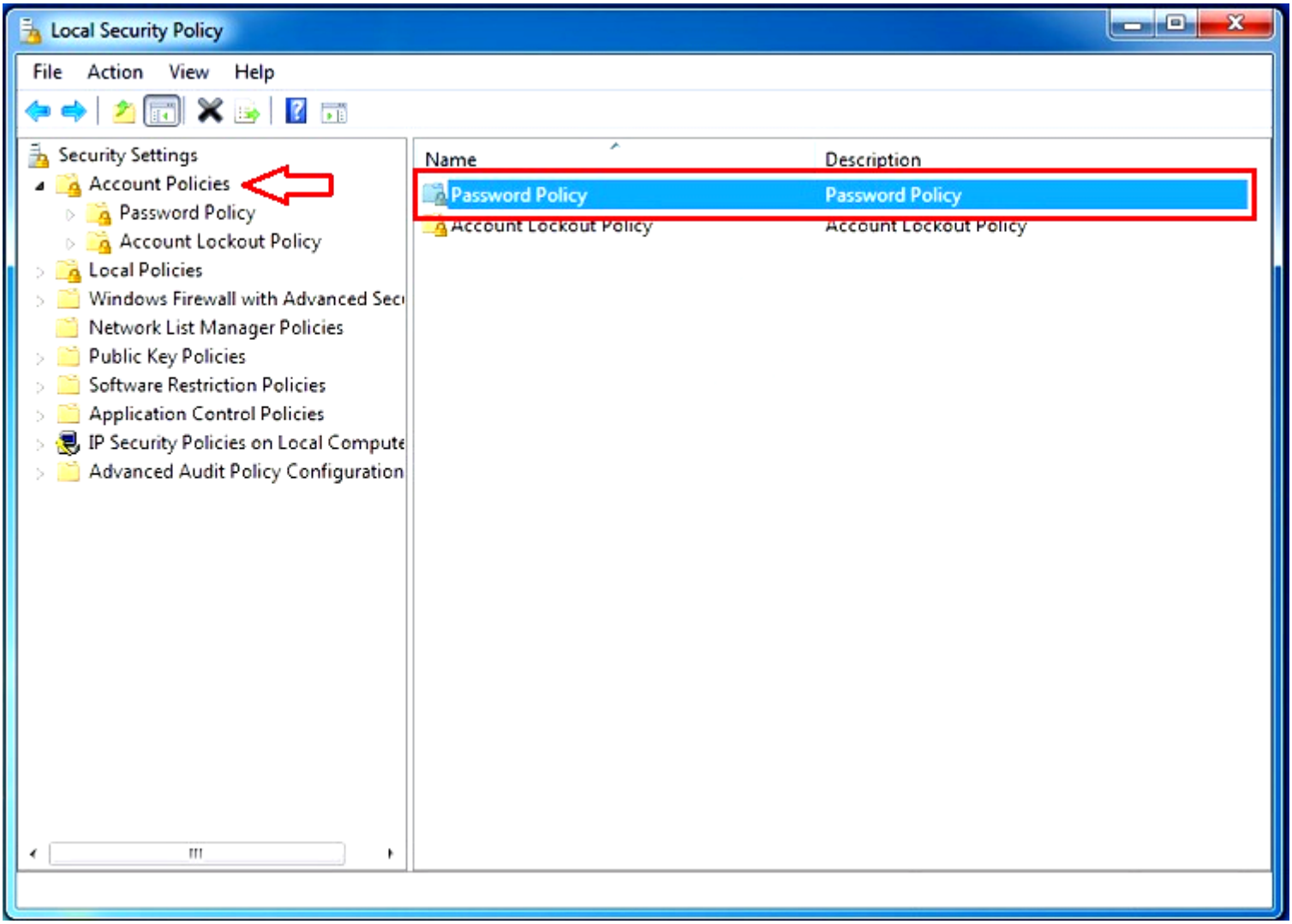
مرحله یک : ابتدا وارد منو استارت شوید و بر روی panel control کلیک نمایید سپس مطابق مرحله یک : تصویر زیر بر روی tools administrative کلیک نمایید .



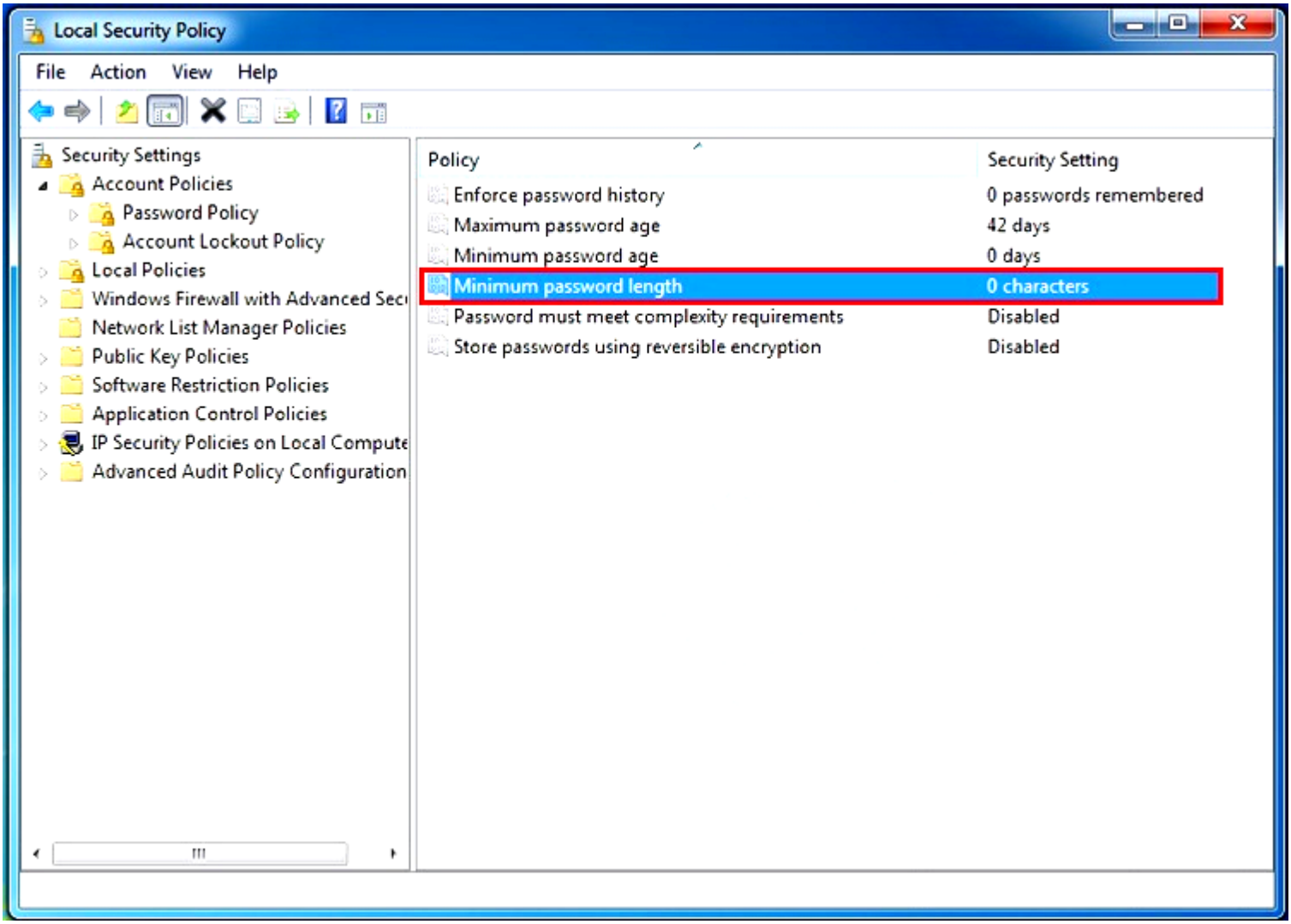
مرحله دو : پس از ورود به پنل administrative tools مطابق تصویر وارد قسمتlocal security شوید .



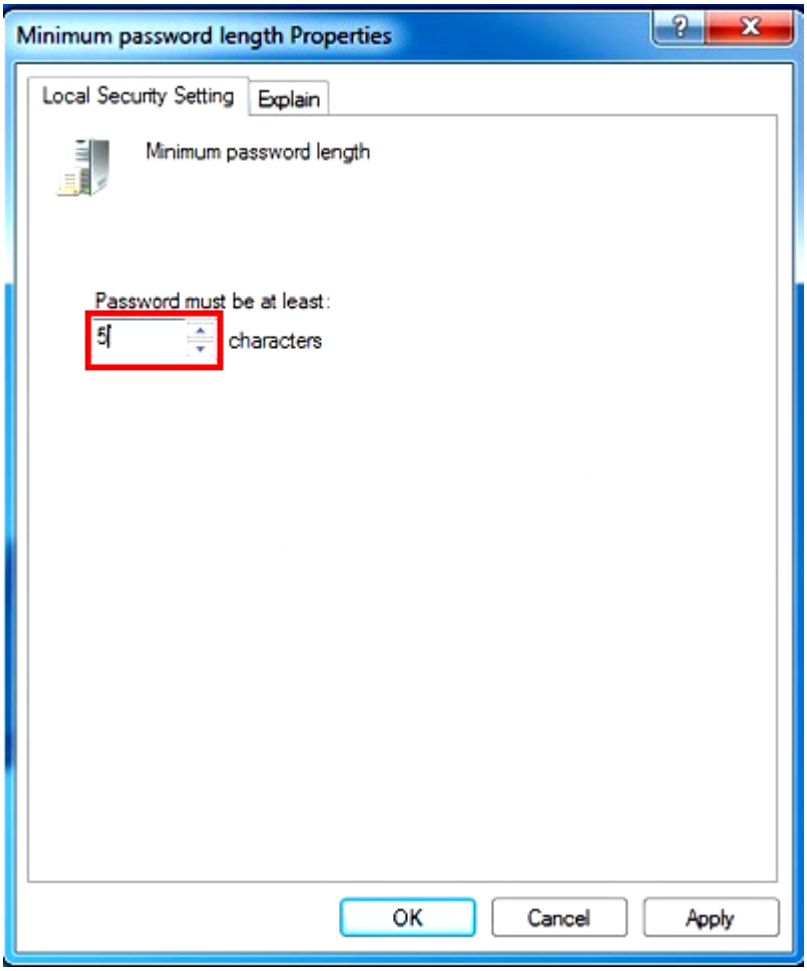
مرحله سه : سپس از پنجره Local security policy بر روی account policy کلیک نموده و مطابق تصویر زیر پس از آن بر روpolicy password کلیک نمایید .



مرحله چهار : سپس بر روی گزینه Minimum password length مطابق تصویر زیر کلیک نمایید.



مرحله پنج : پس از ورود به پنجره properties Minimum password Length در قسمت characters مطابق تصویر زیر حداقل کارکتر مورد نیاز را وارد نمایید .

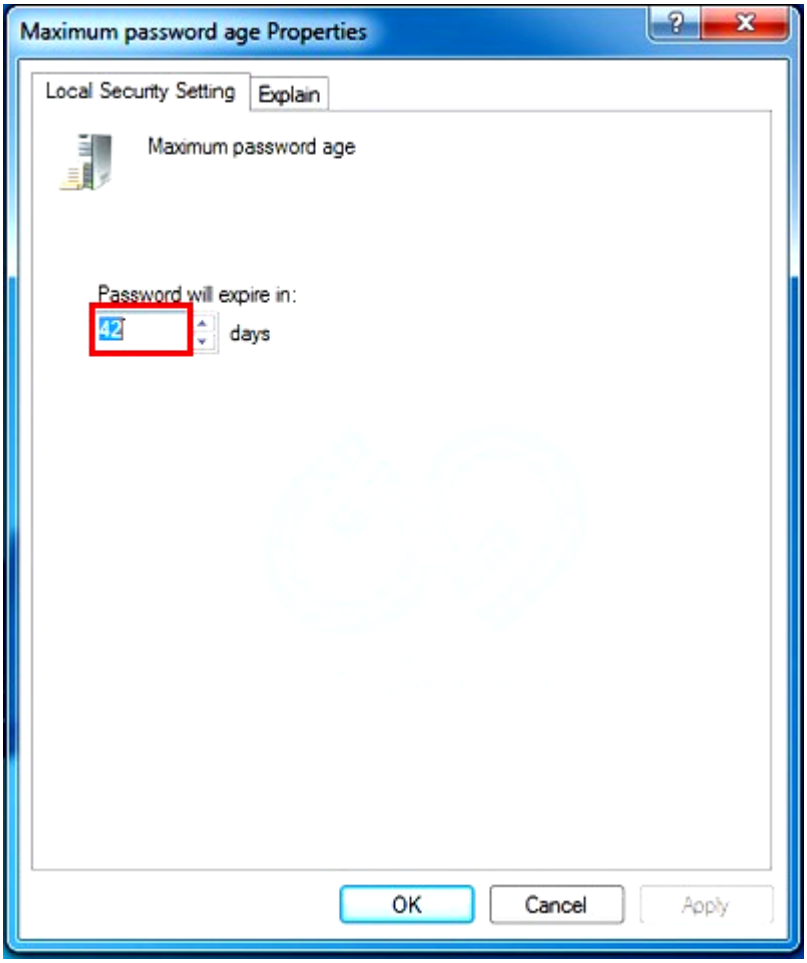


پس از اعمال این تنظیمات هر user از ویندوز که بخواهد برای خود پسورد انتخاب نماید ، حتما پسورد خود را باید بیشتر از ۵ کارکتر وارد کند در غیر این صورت با ارور داخل ویندوز مواجه می شود .

آموزش دو : اعمال محدودیت جهت تعویض پسورد کاربران پس از یک بازه زمانی خاص در این قسمت می توانید تنظیماتی اعمال نمایید که ویندوز پس از یک بازه زمانی مثلا ۳۰ روز User را مجبور نماید که جهت امنیت بیشتر password خود را تغییر دهد .

مرحله یک : جهت انجام این کار تا مرحله ۳ از آموزش قبلی را اجرا نمایید .

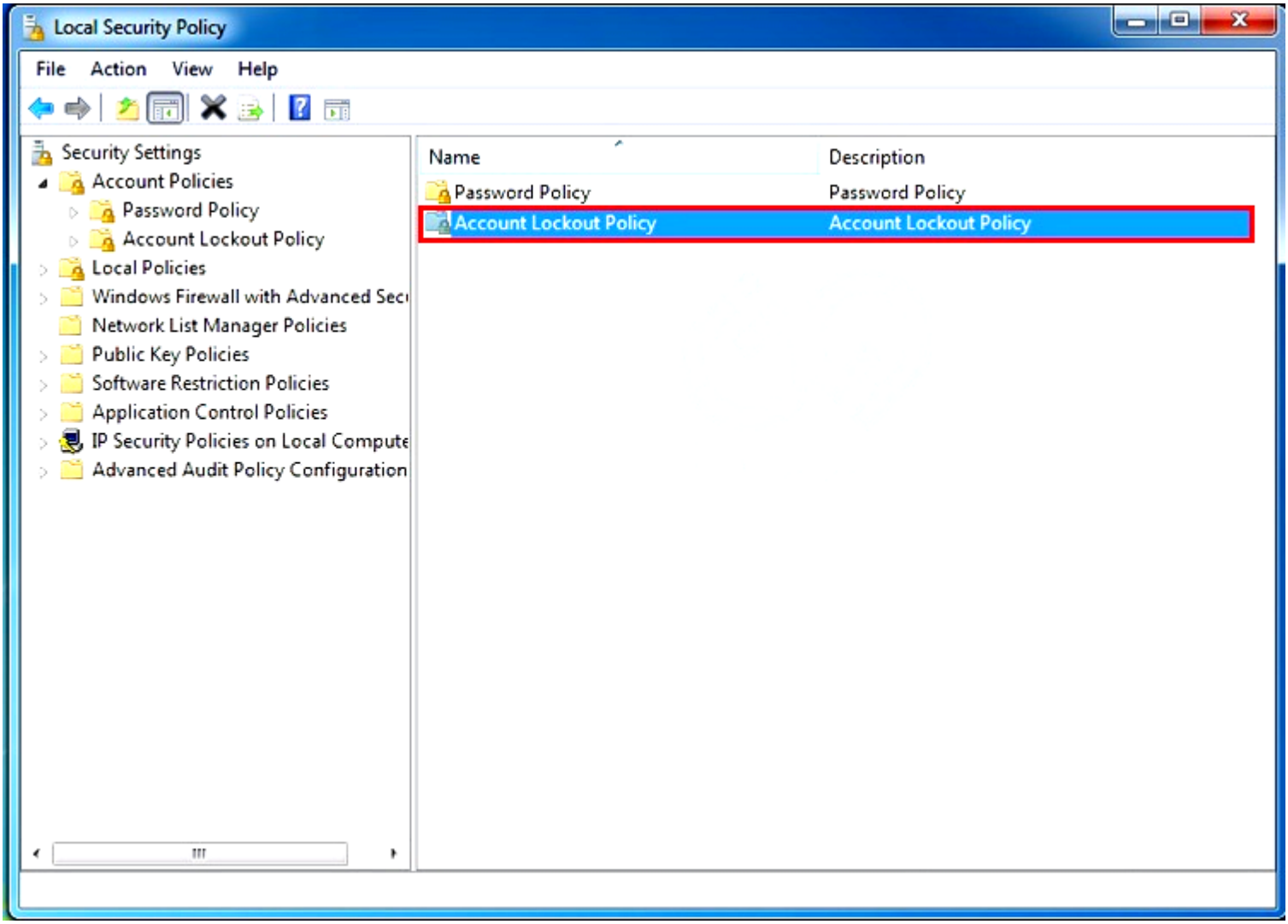
مرحله دو : سپس بر روی گزینه maximum password age کلیک نمایید و مطابق تصویر زیر مقدار روز مورد نظر را در فیلد Day وارد نمایید و مطابق تصویر زیر بر روی دکمه apply کلیک نمایید .



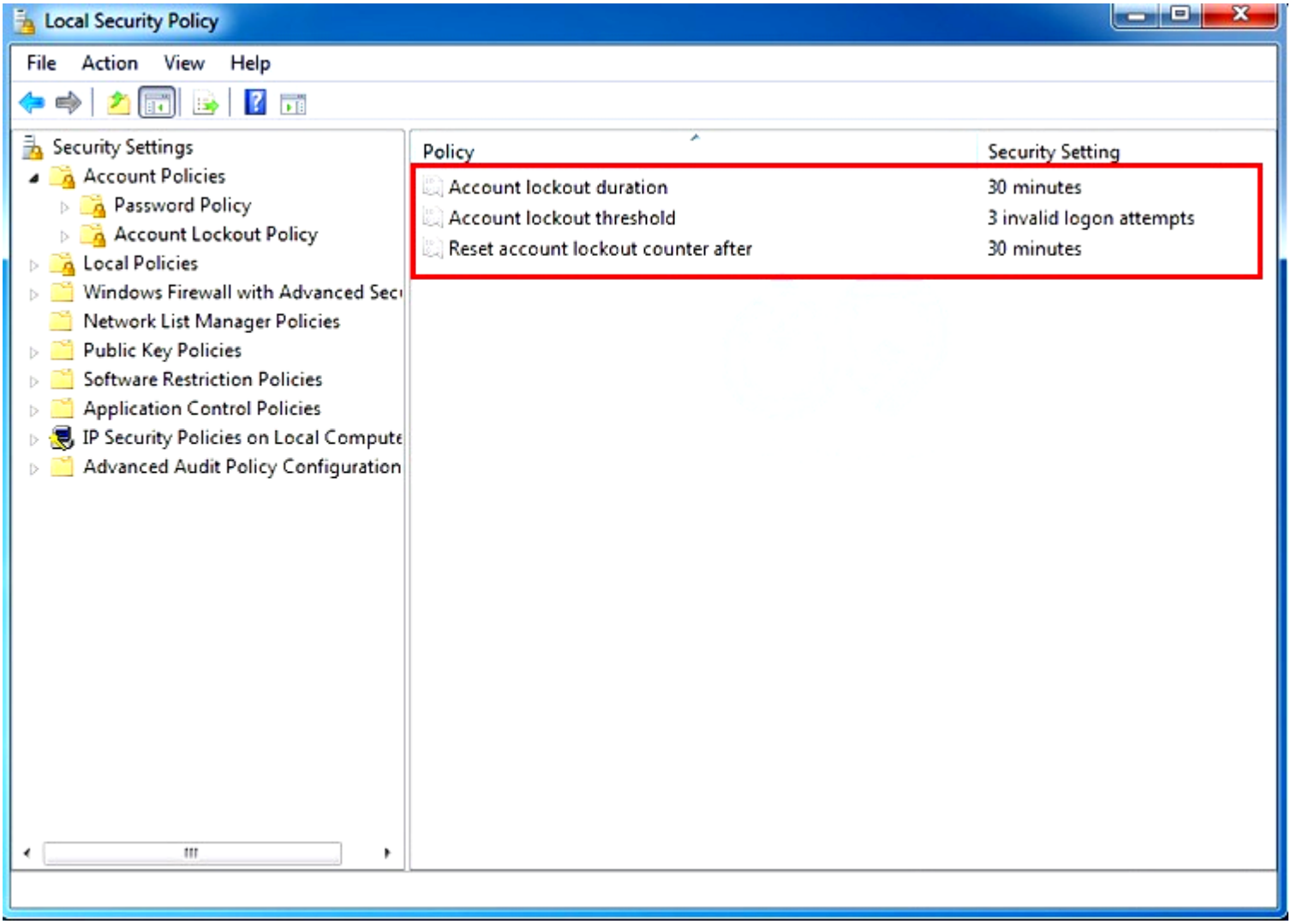
آموزش سه : اعمال محدودیت برای تعداد دفعات وارد کردن پسورد اشتباه در این قسمت شما می توانید سیستم را طوری Konfig نمایید که پس از این که کاربر بیشتر از N (منظور از N مقدار انتخابی توسط کاربر می باشد)مرتبه پسورد جهت Login به ویندوز را اشتباه وارد کند ، user برای N دقیقه بلاک شود .

مرحله یک : ابتدا تا مرحله ۲ از آموزش شماره یک را اجرا نمایید .

مرحله دو : مطابق تصویر زیر از قسمت account policies بر روی account lockout policy کلیک نمایید .



مرحله سه : پس از ورود به پنجره local security policy سه فایل قابل ویرایش مطابق تصویر زیر آشکار است که به تشریح آن ها می پردازیم .

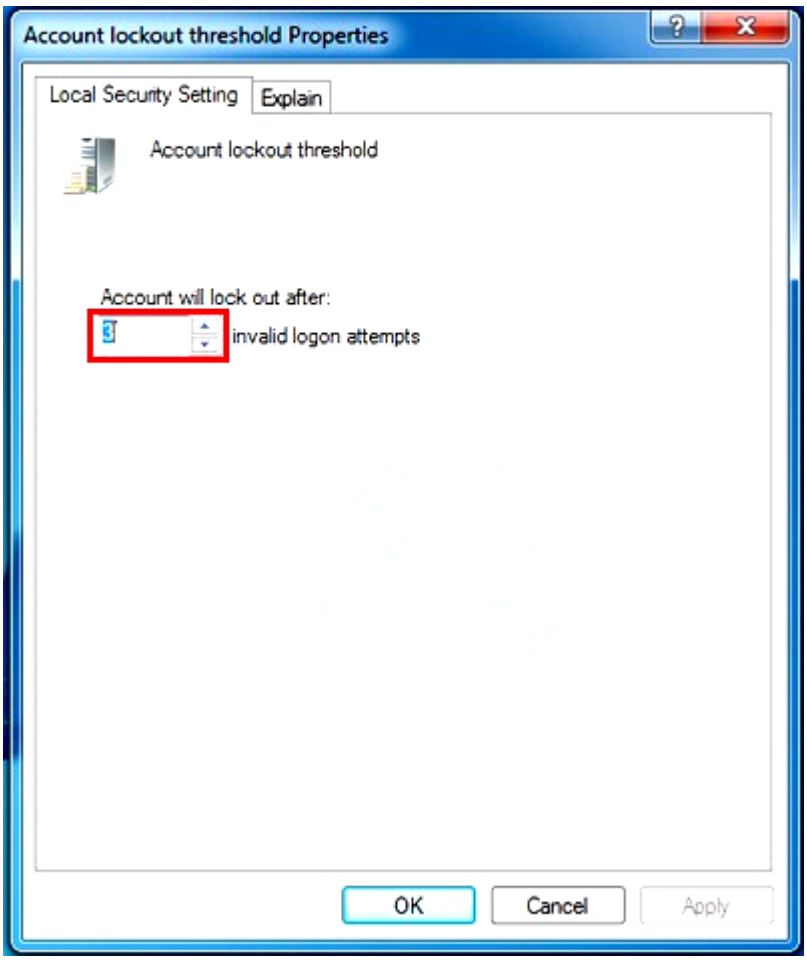


گزینه account lockout duration : این گزینه به User ویندوز اجازه می دهد که پس از گذشت N دقیقه از زمان ورود پسورد اشتباه و بلاک شدن وی ، password صحیح خود را وارد کند و وارد ویندوز شود .

گزینه account lockout thereshold : اصلی ترین گزینه می باشد و پس از باز کردن پنجره مربوط به این فایل می توانید تعداد مرتبه هایی که کاربر می تواند پسورد خود را اشتباه وارد کند و بلاک نشود را وارد کنید ، به عنوان مثلال اگر عدد ۳ را وارد کنید کاربر پس از وارد کردن ۳ بار پسورد اشتباه به مدت زمان n دقیقه بلاک می شود .

گزینه reset account lockout counter after : این گزینه تعیین می کند کا کاربر پس از وارد کردن ۳ مرتبه پسورد اشتباه برای چه مدت (N دقیقه) بلاک شود .

مرحله چهار : مطابق تصویر زیر بر روی account lockout thereshold کلیک نمایید و در فیلد مقابل گزینه invalid logon attempys مقدار مجاز ورود پسورد اشتباه را وارد نمایید ، ما عدد ۳ را وارد کرده ایم ، سپس بر روی apply کلیک نمایید .



مرحله پنج : پس از اعمال تنظیمات بالا مقدار گزینه های account lockout thereshold و reset account lockout counter after را طبق توضیحات داده شده در باره هر گزینه در چند سطر بالا تر تنظیم نمایید .

برای سایر دستورات و تنظیمات امنیتی بر روی سیستم عامل ویندوز کافی است از طریق همین منو وارد شویم و متناسب با دستورالعمل امنیتی، یکی از گزینه ها و زیر منوها را انتخاب و نسبت به درج ملاحظات و سیاست امنیتی اقدام نماییم.

مقایسه امنیت در ویندوز و لینوکس:

هنگامی که ویندوز و لینوکس با هم مقایسه می شوند، نقطه ضعف های امنیتی آن 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 که ۳۹ حوزه آن در لیست خطرناک ترین نقاط ضعف امنیتی قرار دارند و برای لینوکس Redhat نیز ۴۶ حفره امنیتی گزارش شده است که سه حفره آن در لیست آسیب پذیری های امنیتی بسیار خطرناک قرار دارند .

دلایل قانع کننده ای برای تفاوت امنیتی میان دو سیستم عامل وجود دارد. به عنوان مثال مدل توسعه ای سورس برنامه های لینوکس، امکان گزارش و شناسایی باگ ها 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 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.

همچنین 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. 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 تمایل به ایجاد یک سیستم ساده دارد که برای استفاده کننده بسیار آسان باشد. اما این سیاست 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.

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 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.

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. البته 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.

خط فرمان در لینوکس :

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]$

تایپ دستورات در محیط پوسته فرمان بسیار آسان میباشد. در صورتی که هنگام راه اندازی سیستم، بجای پوسته فرمان محیط گرافیکی لینوکس اجرا میشود، برای تایپ فرامین پوسته باید از Terminalیا Konsoleاستفاده کنید. میتوانید در منویrun ، فرمانxterm را نیز تایپ کنید. در مثالهای زیر علامتهای $ و # نشان دهنده اعلان فرمان میباشند. پس تایپ هر فرمان باید کلیدEnter 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. 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 کاربرAlan بوده که عضو گروهAlan است و شماره های کاربری و گروه آن ۵۰۰ میباشد. با استفاده از فرمانwho 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 جاریusr/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. 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

خروج از پوسته فرمان

هنگامی که کارهای خود را انجام دادید و مایل بودید از پوسته فرمان خارج شوید، کافی است که کلیدهای Ctrl+Dرا فشار دهید. در صورتی که در حالت متنی لینوکس را بوت کرده اید، کافی است فرمان logoutیاexit را تایپ کنید. فرامین دیگری در مسیرهایusr/bin وbin قرار دارند. همچنین فرامین مدیریت سیستم در مسیرهایusr/sbin وsbin قرار دارند.

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

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 روی Highتنظیم 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 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 دگمهAdd User کلیک 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. 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.

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 هایDHCP پذیرفته 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 دورX و 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.

نکات امنیتی لازم:

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

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 passwd تحت 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 به اندازه کافی کنترل بر روی اسم رمز انجام می‌گردد و می‌توان تا حدی مطمئن بود که کاربر نمی‌تواند اسامی رمز ساده انتخاب 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.

بوسیله ابزارهایی 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

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. 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. 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 استفاده از FTP و telnet که اطلاعات را عیناً بر روی شبکه منتقل می‌نمایند، می‌تواند نگرانی‌های امنیتی به وجود آورد .

من الله التوفیق