

امنیت در شبکه

هدف های رفتاری: هنرجو پس از پایان این فصل می تواند:

- دیواره آتش را تعریف کند و با آن کار کند.
- تفاوت آنتی ویروس و دیواره آتش را بیان کند.

امنیت در شبکه دارای سطوح مختلفی است، یک مدیر شبکه برای محدود کردن کاربران غیرمجاز می تواند از سطح نام کاربری و گذرواژه استفاده کند. در حالی که اگر این شبکه به شبکه دیگر متصل شود، مدیر شبکه نیاز به سطح امنیتی بالاتری خواهد داشت که این سطح امنیتی با نام کاربری و گذرواژه میسر نخواهد بود.

بنابراین، مدیر شبکه نیاز به نصب دیواره آتش (Firewall) به صورت سخت افزاری و نرم افزاری خواهد داشت.

رعایت امنیت در شبکه یکی از موارد ضروری است که مدیر شبکه و حتی کاربران باید رعایت نمایند با توجه به اینکه در سال دوم آنتی ویروس آموزش داده شده است در این فصل دیواره آتش^۱ مورد بحث قرار می گیرد.

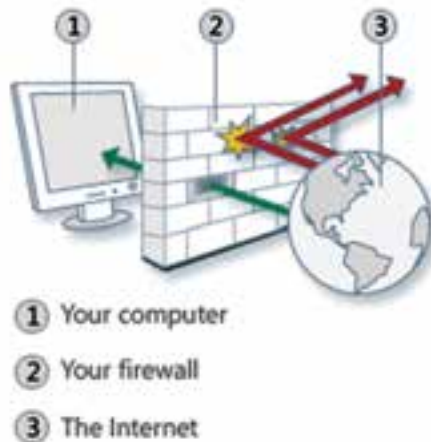
۱-۲- دیواره آتش (Fire wall)

دیواره آتش یکی از موثرترین و مهمترین روش های پیاده سازی امنیت شبکه می باشد که تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی شبکه جلوگیری می کند. دیواره آتش می تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزاری و یا ترکیبی از هر دو باشد که اطلاعات ورودی از اینترنت یا شبکه به سیستم را بررسی کرد. و براساس تنظیمات اعمالی، کلید دسترسی های شبکه را کنترل

^۱ - Firewall

می‌نماید، به طوری که به برخی از درخواست‌ها اجازه ورود به شبکه داده شده و به برخی دیگر اجازه ورود داده نمی‌شود. دیواره آتش سخت‌افزاری معمولاً در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد. به دیواره آتش نرم‌افزاری، دیواره آتش داخلی و به دیواره آتش سخت‌افزاری، دیواره آتش خارجی می‌گویند. دیواره آتش سخت‌افزاری در بین شبکه شما و یک شبکه دیگر در سازمان دیگر و یا اینترنت قرار گرفته و سطوح امنیتی را برای شما فراهم می‌کند. دیواره آتش نرم‌افزاری نیز برای برقراری لایه امنیتی استفاده می‌شوند. در برخی از سیستم‌عامل‌ها این نوع دیواره آتش نصب شده است که باید آن را پیکربندی و فعال نمایید.

دیواره آتش از دسترسی هکرها و برنامه‌های مخرب (مانند کرم‌ها) به رایانه شما از طریق شبکه یا اینترنت جلوگیری می‌کند. یک دیواره آتش همچنین می‌تواند از ارسال برنامه‌های مخرب از طریق رایانه شما به شبکه نیز جلوگیری کند. از طریق دیواره آتش می‌توان با انجام تنظیمات مربوطه از اجرای یک برنامه خاص جلوگیری نمود. دیاگرام ساده‌ای از دیواره آتش در شکل ۷-۱ آورده شده است:



شکل ۷-۱- تصویر عملکرد دیواره آتش

دیواره آتش به لحاظ سطح استفاده به دو دسته تقسیم می‌شود:

دیواره آتش شخصی یا رومیزی (Desktop or personal firewalls): که

برای محافظت از یک میزبان طراحی شده است. دیواره آتش شخصی نرم‌افزاری است که برای محافظت از یک رایانه که به اینترنت متصل است مورد استفاده قرار می‌گیرد. علاوه بر دیواره آتش پیش فرض ویندوز، شرکت‌های دیگری نیز برای رایانه‌های شخصی دیواره آتش تولید کرده‌اند که

Symantec و Trend Micro's PC cillin ، Zone Alarm نمونه‌ای از این شرکت‌ها می‌باشند. دیواره آتش شبکه یا سروری (Network firewalls): که برای محافظت از شبکه در برابر حملات طراحی شده است و بالاترین سطح حفاظت را در اختیار کاربران سازمانی قرار می‌دهد. یکی از ویژگی‌های دیواره آتش شبکه، مدیریت متمرکز می‌باشد که با استفاده از آن می‌توان تمام کاربران شبکه را مورد حفاظت قرار داد.

با استفاده از دیواره آتش شبکه علاوه بر حفاظت دسترسی از خارج، می‌توان برای محدود کردن دسترسی اعضای شبکه به خارج از شبکه نیز پیکربندی لازم را انجام داد. توجه داشته باشید که دیواره آتش یک سطح حفاظتی را ارائه می‌کند ولی هرگز عدم تهاجم به سیستم شما را تضمین نمی‌کند. همچنین دیواره آتش برای مقابله با خطرات شناخته شده طراحی شده است. استفاده از دیواره آتش به همراه سایر امکانات حفاظتی مانند نرم افزارهای آنتی ویروس و رعایت توصیه‌های ایمنی می‌تواند یک سطح مطلوب از امنیت را برای شما و شبکه فراهم سازد. یک دیواره آتش معمولاً نمی‌تواند از ورود ویروس‌ها جلوگیری کند. اغلب دیواره‌های آتش بخش‌های مربوط به آدرس مبدأ و مقصد و شماره پورت مبدأ و مقصد شبکه‌های ورودی را مورد بررسی قرار می‌دهند و به جزئیات داده توجهی ندارند.

نکته ۱: یک دیواره آتش نمی‌تواند شبکه و منابع آن را از خرابکاران داخلی محافظت کند.

۷-۲- وظایف دیواره آتش

وظایف دیواره آتش به شرح ذیل دسته‌بندی می‌شود:

— مدیریت و کنترل ترافیک شبکه: که به عنوان اولین و اساسی‌ترین وظیفه دیواره آتش می‌باشد.

— ثبت و گزارش وقایع: ثبت وقایع یکی از مشخصه‌های بسیار مهم یک دیواره آتش به شمار می‌رود. مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز پردازد. در یک روال ثبت مناسب، مدیر می‌تواند به راحتی به بخش‌های مهم از اطلاعات ثبت شده دسترسی پیدا کند.

همچنین یک دیواره آتش خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را

از وقایع مطلع کند و برای وی اخطار بفرستد.

توصیه می‌شود در حالت پیش فرض تنظیمات زیر برای دیواره آتش انجام گیرد :

- ۱- دیواره آتش فعال باشد.
- ۲- دیواره آتش برای تمام نقاط شبکه فعال باشد (منزل یا محل کار، مکان عمومی، و یا دامنه).
- ۳- دیواره آتش برای تمام اتصالات شبکه فعال باشد.
- ۴- تمام اتصالات ورودی غیرضروری مسدود شوند.

فعالیت کارگاهی

۷-۳- تنظیمات دیواره آتش در ویندوز

در اینجا این سؤال مطرح می‌شود که چگونه می‌توان از فعال بودن دیواره آتش در ویندوز ۲۰۰۸ سرور اطمینان حاصل نمود؟ در ویندوز ۲۰۰۸ سرور آتش به‌طور پیش فرض فعال می‌باشد ولی برای اطمینان از فعال بودن آن ابتدا باید برنامه دیواره آتش را با استفاده از روش‌های زیر اجرا نمود :

روش اول : از Control Panel برنامه Windows Firewall را اجرا کنید.

روش دوم : در کادر Start Search در منوی Start عبارت Firewall را تایپ

نموده و سپس برنامه Windows Firewall را اجرا نمایید.

در این هنگام پنجره Windows Firewall نمایش داده شود (شکل ۷-۲) که

حالت فعال بودن (on) دیواره آتش در شکل به‌خوبی مشخص می‌باشد.



شکل ۷-۲- دیواره آتش در ویندوز ۲۰۰۸ سرور

اگر دیواره آتش غیر فعال (off) باشد پنجره مربوطه به صورت شکل ۷-۳ نمایش داده خواهد شد و رایانه شما در حالت خطر یا ریسک قرار خواهد داشت.



شکل ۷-۳- دیواره آتش در حالت غیر فعال

برای فعال یا غیر فعال کردن دیواره آتش بر روی گزینه Change setting شکل ۷-۲ یا ۷-۳ کلیک نمایید تا پنجره تنظیمات دیواره آتش نمایش داده شود.



ب) پنجره تنظیمات دیواره آتش در حالت غیر فعال



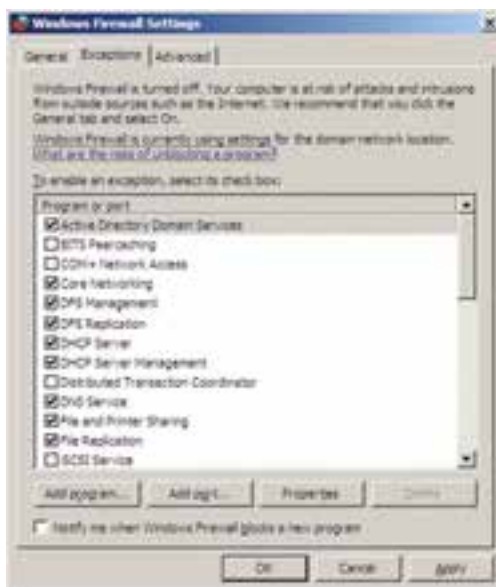
الف) پنجره تنظیمات دیواره آتش در حالت فعال

شکل ۷-۴

نکته: زمانی گزینه Block all incoming connections در شکل ۴-۷ الف را فعال می‌کنند که شما می‌خواهید بالاترین سطح حفاظت را داشته باشید و یا اینکه شما با یک شبکه با امنیت خیلی پایین در ارتباط هستید. توجه داشته باشید که فعال کردن این گزینه باعث می‌شود تا تمامی ارتباطات بیرونی محدود شود.

۴-۷- استثناء کردن یک برنامه یا سرویس با استفاده از زبانه Exceptions

با استفاده از زبانه Exceptions می‌توان برای بعضی از برنامه‌های کاربردی استثناء قائل شد و یا اینکه بعضی از درگاه‌ها را برای تبادل اطلاعات باز گذاشت. در این زبانه بعضی از برنامه‌ها به صورت پیش فرض استثناء شده‌اند و بعضی‌ها نیز انتخاب نشده‌اند که قابل انتخاب می‌باشند. همچنین می‌توان با استفاده از دکمه Add Program برنامه جدیدی را به لیست استثناءها اضافه نمود. توجه داشته باشید فقط برنامه‌هایی را که به طور دستی اضافه نموده‌اید می‌توانید با استفاده از دکمه delete حذف نمایید. البته این کار باید با دقت لازم انجام شود تا امنیت سیستم شما دچار اختلال نشود.



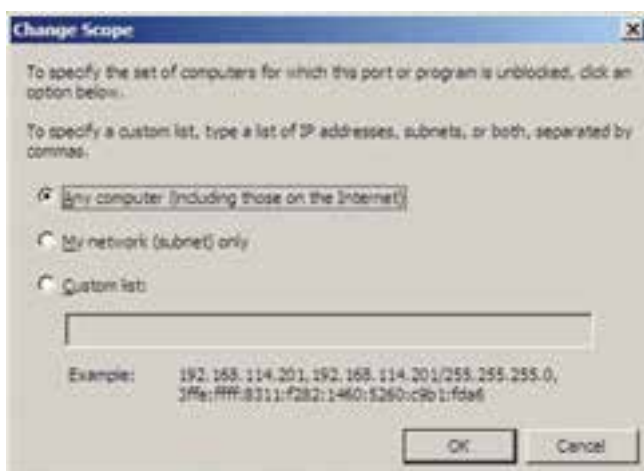
شکل ۵-۷- کادر تنظیمات Exceptions

یکی از نکات مهم در زمان اضافه کردن برنامه جدید به لیست استثناها این است که می‌توان برای آن برنامه دامنه استفاده کاربران را تعیین نمود. بعد از کلیک کردن بر روی دکمه Add Program... کادر Add a Program ظاهر می‌گردد که شما می‌توانید دامنه کاربرانی که بتوانند از برنامه مورد نظر استفاده کنند را انتخاب نمایید (شکل ۶-۷).



شکل ۶-۷. کادر اضافه کردن برنامه به لیست استثناها

برای انتخاب دامنه مجموعه رایانه‌ها بر روی دکمه ... Change scope کلیک کنید تا کادر انتخاب دامنه ظاهر گردد (شکل ۷-۷).



شکل ۷-۷. کادر انتخاب دامنه

در کادر Change scope سه انتخاب وجود دارد :

۱- **Any computer(Including those on the Internet)** : تمام رایانه‌ها

حتی رایانه‌های در اینترنت (پایین ترین سطح امنیتی)

۲- **My Network (Subnet) Only** : فقط رایانه‌های موجود در شبکه‌ای

که دارای subnet یکسانی با این رایانه می‌باشند.

۳- **Custom list** : می‌توان آدرس‌های IP رایانه‌های خاصی که مدنظر می‌باشند

را اضافه نمود. (بالا ترین سطح امنیتی)

کار عملی

تعیین کنید برنامه‌های netsupport ، Msn Messenger و Google Talk از چه درگاه‌هایی برای ارتباط استفاده می‌کنند. برنامه را برای امکان ارتباط با شبکه به دیواره آتش معرفی کنید.

خودآزمایی و پژوهش

- ۱- دیواره آتش چیست؟
- ۲- آیا وجود دیواره آتش در یک شبکه ضروری است؟ چرا؟
- ۳- آیا می‌توان از دیواره آتش به جای ضدویروس استفاده کرد؟ چرا؟
- ۴- کار زبانه Exceptions در پنجره Firewall چیست؟
- ۵- پژوهش کنید که چه برنامه‌های دیواره آتش رایجی وجود دارد؟

بخش دوم

سیستم عامل ویندوز ۲۰۰۸ سرور



سیستم عامل های شبکه ای

هدف های رفتاری: هنرجو پس از پایان این فصل می تواند:

- ویژگی های سیستم عامل های شبکه ای را بیان کند.
- انواع سیستم عامل های شبکه را شناسایی کند.
- مشخصات اصلی سیستم عامل ویندوز ۲۰۰۸ سرور را بیان نماید.
- نسخه های مختلف ویندوز ۲۰۰۸ سرور را شناسایی نماید.

۸-۱- آشنایی با ویژگی های سیستم عامل های شبکه ای

سرویس دهنده ها و در کل شبکه ها به چه سیستم عاملی نیاز دارند؟ پاسخ به این سؤال مستلزم آشنایی با ویژگی هایی است که در ادامه بررسی می شود. سیستم عامل هایی که در شبکه استفاده می شوند باید ویژگی هایی را افزون بر سیستم عامل هایی که در کاربردهای خانگی مورد استفاده قرار می گیرند داشته باشند. هرچند امروزه اکثر کاربران خانگی به محض اتصال به اینترنت عملاً به عنوان کاربر شبکه محسوب می شوند بنابراین خصوصیات سیستم عامل های شبکه برای سیستم های خانگی نیز (در حدی کمتر) معنی پیدا می کند. برخی از این ویژگی ها به ترتیب اهمیت عبارتند از:

- Security (امنیت)
- Multitasking (چند وظیفه ای)
- Multi Processor Support (پشتیبانی از چندین پردازنده)
- Reliable & Stable (قابلیت اطمینان و پایداری)
- Fault Tolerance (تحمل خطا)
- Backup Utilities (نرم افزار تهیه نسخه پشتیبان)
- Simple & Unified Administrative Tools (ابزارهای مدیریتی)
- Support (پشتیبانی)

با برخی از این ویژگی‌ها قبلاً در درس سیستم عامل آشنا شده‌اید.

۱-۸-امنیت^۱: مهم‌ترین ویژگی است. مسایل امنیتی هر چند که باعث کندی سیستم

می‌شود اما به عنوان رکن کار هر سیستم عامل شبکه محسوب می‌شود. امنیت برای سیستم عامل را می‌توان در حوزه‌های مختلفی بررسی کرد به عنوان مثال:

الف) امنیت در حوزه دسترسی به دیسک و فایل - سیستم (Disk & File System Security)

ب) امنیت در حوزه عملیاتی که کاربرد عام دارند مانند:

● تغییر ساعت سیستم (Changing System time)

● نصب نرم افزار، سخت افزار و انجام تنظیمات (Hardware & Software Installation)

● اجرای برنامه‌ها و تغییر در پارامترهای مربوطه (Running Applications & Services)

ج) امنیت در حوزه شبکه و اطلاعات تبادل (Network Services)

د) امنیت در ورود به سیستم (System Login)

مثال: سیستم عامل‌های DOS و خانواده 9x جزو آن دسته از سیستم‌هایی هستند که امنیت

چندانی مخصوصاً در حوزه‌های «الف»، «ب» و «ج» ندارند. پس از روشن کردن یک رایانه با سیستم

عامل ویندوز 98 به راحتی می‌توان بدون هیچگونه گذر واژه‌ای وارد آن شده، به هر جا روی دیسک

دسترسی پیدا کرده (که با FAT آماده شده)، هر برنامه‌ای را نصب، حذف یا اجرا کرده و هرگونه تغییر

سخت افزاری را اعمال کرد. در صورتی که این امر در خانواده NT به راحتی امکان پذیر نیست، فقط

کاربرانی که عضو گروه Administrators باشند اختیار کامل در انجام عملیات فوق را دارا هستند.

نکته: کاربرانی که هنگام نصب ویندوز اکس بی تعریف می‌شوند همگی عضو گروه

Administrators بوده و برای کاهش قدرت آنها می‌توان گروه آنها را به Limited users

تبدیل کرد. چنانچه در ویندوز اکس بی فقط یک کاربر تعریف کنیم، در آن صورت رایانه

پس از Boot شدن خود به خود وارد سیستم می‌شود بدون آنکه گذر واژه‌ای از ما خواسته

شود، در این حالت سیستم عامل ویندوز اکس بی به طور خودکار همان یک کاربر را Auto

Login می‌کند و این به معنای نقض امنیت در ورود به سیستم نیست، می‌توان این ویژگی را

غیر فعال کرد. ضمناً این خصوصیت یعنی Auto Login در بقیه اعضای خانواده ویندوز

NT نیز وجود دارد.

الف) نشان دهید که در ویندوز اکس پی کاربران تعریف شده هنگام نصب، عضو گروه Administrators هستند.

ب) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروه Users) قادر به ایجاد پرونده جدید در ریشه دیسک که با فایل - سیستم NTFS قالب بندی شده نیست (پوشه جدید را می تواند درست کند اما پرونده را خیر).

ج) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروه Users) نمی تواند ساعت سیستم را تغییر دهد.

د) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروه Users) نمی تواند از طریق Device Manager یک سخت افزار را (مثلاً Mouse) غیر فعال (Disable) کند.

ه) بررسی کنید که آیا برنامه ای یا روشی وجود دارد که بتوان به کمک آن گذر واژه Administrator را پیدا کرد یا تغییر داد؟

۲-۱-۸ - چند وظیفه ای^۱: توانایی اجرای هم زمان چندین برنامه با هم است. این ویژگی نیازی به شرح بیشتر نداشته و امروزه در تمامی سیستم ها وجود دارد و یک ویژگی عادی به شمار می رود. سیستم عامل DOS به عنوان یک سیستم عامل قدیمی Multi task نیست اما سیستم عامل های خانواده ویندوز همگی چند وظیفه ای هستند.

۳-۱-۸ - پشتیبانی از چندین پردازنده^۲: می دانیم که هر چه تعداد پردازنده های موجود روی یک برد اصلی بیشتر باشد کارها سریع تر انجام می شود. امروزه بردهای چند پردازنده در دو زمینه عمده کاربرد دارند:

- سرویس دهنده ها،

- رایانه هایی که عملیات سنگین گرافیکی و پویا را انجام می دهند (Graphic Workstations).

بنابراین در مواردی که نیاز به استفاده از بردهایی با بیش از یک CPU باشد لازم است تا سیستم عامل نیز بتواند آنها را شناسایی کرده و استفاده کند. در سیستم عامل های شرکت مایکروسافت، فقط سیستم عامل های خانواده ویندوز NT قادر به شناسایی و بهره برداری از چندین CPU هستند.

پشتیبانی از چندین پردازنده در سیستم عامل‌ها با ۲ سیاست کلی متقارن و نامتقارن انجام می‌شود، (SMP Symmetric Multi Processing, AMP Asymmetric Multi Processing)، هر یک را به اختصار بررسی کرده و بگویید که مایکروسافت در سیستم‌های خود از کدام روش استفاده می‌کند؟

۴-۱-۸- تحمل خطا^۱: عدم تأخیر در ارائه سرویس و قدرت تحمل در هنگام بروز مشکل و خطاهای عمدتاً سخت‌افزاری است به عبارت دیگر تحمل خطا (به اختصار FT) قابلیت است در سیستم عامل که می‌تواند هنگام بروز مشکلات از تجهیزات جایگزین استفاده کرده و بدون تأخیر (یا با تأخیر بسیار کوتاه) به طور خودکار به سرویس دهی ادامه دهد. نکته اصلی در FT این است که هنگام بروز خطا اولاً زمان قطع شدن سرویس بسیار کوتاه بوده، ثانیاً عملیات جایگزینی بدون عوامل انسانی و به طور خودکار صورت می‌گیرد. مسئول سیستم در فرصت مناسب می‌تواند اشکال‌ها را بررسی و رفع کند.

مثال ۱: فرض کنید که یک سرویس‌دهنده داریم که تمامی اطلاعات خود را روی یک دیسک سخت ذخیره کرده است. اگر برای دیسک مشکلی بروز کند مثلاً بر اثر یک شوک الکتریکی در برق بخشی از قطعات آن بسوزد چه اتفاقی می‌افتد؟ بدیهی است که سرویس قطع می‌شود. برای اینکه سرویس همواره پایدار بماند باید:

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا دو دیسک سخت روی سیستم نصب کنید.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه دیسک باشد.

در شرایط عادی سیستم عامل هر اطلاعاتی را که روی دیسک اول می‌نویسد عیناً روی دیسک دوم نیز کپی می‌کند (Disk Mirroring, Disk Duplexing)، حال اگر به هر دلیل یکی از دیسک‌ها از کار بیفتد سیستم عامل می‌تواند بدون لحظه‌ای تأخیر اطلاعات را با دیسک دوم تبادل کند.

یادآوری: این کار در تکنیک RAID1 انجام می‌شود که در درس سخت‌افزار بررسی شده است.

از میان محصولات مایکروسافت، سیستم عامل‌های ویندوز NT که در گروه سرویس‌دهنده قرار

دارند همگی قابلیت Disk Fault Tolerance را دارا هستند.

مثال ۲: یک سرویس دهنده داریم (از هر نوع دلخواه) که با یک کارت شبکه (NIC) به شبکه متصل شده و رایانه‌ها از آن سرویس می‌گیرند. اگر برای کارت شبکه یا خط متصل به آن اتفاقی بیفتد چه می‌شود؟ بدیهی است که سرویس قطع می‌شود اگر بخواهیم که سرویس قطع نشود باید:

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا دو عدد NIC روی سیستم نصب کنید.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت تحمل خطا در این زمینه باشد. سیستم عامل در شرایط عادی اطلاعات را تقسیم کرده و از هر دو کارت برای ارسال و دریافت استفاده می‌کند (که البته باعث افزایش سرعت نیز می‌شود) حال اگر به هر دلیل یکی از کارت‌ها از کار بیفتد، سیستم از کارت دیگری برای ادامه کار استفاده می‌کند. مثال فوق در اصطلاحات رایانه‌ای NIC Fault Tolerance خوانده می‌شود و از میان محصولات مایکروسافت، سیستم عامل‌های خانواده ویندوز NT اعم از سرویس گیرنده یا سرویس دهنده در صورتی که کمپانی سازنده کارت شبکه درایور مناسب را برای محصول خود ارائه داده باشد می‌توانند از این خاصیت بهره ببرند.

مثال ۳: فرض کنید که یک سرویس دهنده داریم (از هر نوع دلخواه) و این سرویس دهنده ممکن است هر یک از موارد قبلی تحمل خطا را اعم از Disk یا NIC داشته باشد یا خیر. اگر به هر دلیل سرویس دهنده به طور کامل از کار بیفتد چه می‌شود؟ بدیهی است که سرویس قطع می‌شود، چه کار کنیم اختلالی در سرویس دهی بروز نکند؟

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا دو یا چند سرویس دهنده را با تجهیزات ویژه به یکدیگر متصل کنید. به این مجموعه از سرویس دهنده‌ها اصطلاحاً یک «خوشه سرور» یا Server Cluster گفته می‌شود.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت تحمل خطا در زمینه Clustering باشد. کلیه سیستم‌ها در شرایط عادی اطلاعات مورد نیاز را به یکدیگر تبادل کرده (Synchronize) و چنانچه یکی از اعضای Cluster (یعنی یکی از سرویس دهنده‌ها) از کار بیفتد بقیه می‌توانند به سرعت و بدون تأخیر کار او را جبران کنند. از میان محصولات مایکروسافت فقط چند سیستم عامل از مجموعه NT در خانواده سرویس دهنده‌ها دارای قابلیت Cluster هستند به عنوان مثال Server 2000 فاقد آن بوده اما Advanced Server 2000, Data center Server 2000 دارای قابلیت Cluster هستند.

۱- در برخی از متون به آن Port Trunk یا Port Aggregat on یا L nk Aggregat on می‌گویند.

۵-۱-۸- نرم افزار تهیه نسخه پشتیبان : امروزه اهمیت تهیه پشتیبان برای یک کاربر با

تجربه پوشیده نیست، اگر در لحظه ای متوجه شود که به هر دلیل اطلاعات اصلی اش مخدوش یا غیر قابل دسترس شده است در این حالت با نسخه پشتیبان می تواند اطلاعات را دوباره بازگرداند.

اطلاعات را در حالت کلی می توان به دو دسته تقسیم کرد :

الف) اطلاعاتی که کاربر به صورت مستقیم از اهمیت آن آگاهی دارد، مانند انواع پرونده ها یا

حتی برنامه های کاربردی که تهیه و نصب کرده است (User Data).

ب) اطلاعاتی که کاربر به طور مستقیم با آن سروکار ندارد بلکه برای سیستم عامل مهم است

(System Data).

اغلب کاربران پس از مدت کوتاهی با نحوه تهیه پشتیبان از اطلاعات خودشان آشنا می شوند اما

کمتر کاربر عادی پیدا می شود که طی مدت کوتاهی بتواند به طور کامل از اطلاعات سیستمی نیز پشتیبان

گرفته یا بازیابی کند چرا که با توجه به پیچیدگی سیستم عامل ها، کسب آگاهی نسبت به ظرافت های

سیستم عامل در زمان کوتاه امر ساده ای نبوده و نیاز به تجربه و تخصص دارد.

چگونه می توان از اطلاعات سیستمی بدون مهارت لازم پشتیبان گرفت؟

یک راه حل مناسب آن است که سیستم عامل ابزارهای قوی و در عین حال کاربر پسند^۱ در

اختیار کاربر بگذارد تا او بتواند اولاً به راحتی اطلاعات را دسته بندی کند ثانیاً بدون داشتن تخصص

زیاد قادر به تهیه پشتیبان از اطلاعات سیستمی باشد. خوشبختانه ابزارهای تهیه پشتیبان در سیستم

عامل های ویندوز NT 5.x دارای چنین توانایی هایی بوده و کاربر می تواند در صورت داشتن مجوز،

تنها به علامت گذاری در قسمت «System State» به تهیه پشتیبان از System Data اقدام کند.

تفاوت بین ابزارهای خاص تهیه پشتیبان (مانند NTBackup در ویندوز NT 5.x) با ابزارهای

عمومی مدیریت پرونده ها که عملیاتی مانند کپی را انجام می دهند در این است که قابلیت هایی در این

ابزارها وجود دارد که در برنامه های عمومی (مانند My Computer) نیست. مهمترین این قابلیت ها

عبارتند از :

الف) به کمک ابزارهایی مانند NTBackup به راحتی از اطلاعات سیستمی نسخه پشتیبان تهیه

می شود.

ب) با این ابزارها، از پرونده هایی که در حال استفاده هستند (Open Files) می توان به راحتی

نسخه پشتیبان تهیه کرد.

ج) سیاست‌های تهیه پشتیبان (Backup Policy) در ابزارهای خاص تنوع بیشتری دارد، بدان معنی که می‌توان برای تهیه پشتیبان با معیارهایی همچون «فقط پرونده‌های تغییر یافته» و ... اقدام کرد که در ابزارهای معمولی تنوع این معیارها کمتر است.

د) با ابزارهای خاص می‌توان انجام عملیات را به طور خودکار در موعد دلخواه زمانبندی کرد (Scheduling).

ه) ابزارهای خاص می‌توانند از مجوزهای امنیتی (لیست دسترسی افراد به پرونده‌ها^۱ که به اختصار ACL خوانده می‌شود نیز پشتیبان گرفته و بازایی کنند. منظور از ACL لیستی است در فایل سیستم‌هایی مانند NTFS که تعیین می‌کند چه افرادی چه عملیاتی را با یک پرونده یا پوشه می‌توانند انجام دهند. بدیهی است که ACL در FAT یا FAT 32 وجود ندارد چرا که FAT امنیت ندارد.

فرایند پشتیبان‌گیری برای خود جزو مباحث مهم بوده و معمولاً در درس سیستم عامل پیشرفته مورد بحث قرار می‌گیرد با این حال برای تثبیت نکات یاد شده فوق، اکیداً توصیه می‌کنیم که انجام این کار باید به کمک هنرآموز درس انجام شود.

الف) نشان دهید که با NTBackup می‌توان به راحتی از اطلاعات سیستم پشتیبان تهیه کرد. ب) دقیقاً با کدام کاربرد سیستم شده‌اید؟ پس از پاسخ به این سؤال، برنامه My Computer را اجرا کرده سپس پارتیشن‌های را که سیستم عامل روی آن نصب شده باز کرده (مثلاً دیسک C:) و وارد پوشه Documents and Settings شوید. قاعدتاً باید یک پوشه همانم با کاربری را که با آن وارد سیستم شده‌اید ببینید. حال سعی کنید که (با استفاده از برنامه My Computer) از این پوشه کپی بگیرید. آیا امکان‌پذیر است؟ قطعاً خیر! چرا که یکی از پرونده‌های موجود در این پوشه (که البته مخفی نیز هست) به نام NTUser.dat در حال استفاده بوده (اصطلاحاً باز است) و برنامه My Computer نمی‌تواند از آن کپی تهیه کند. حال با استفاده از برنامه NTBackup از همین پوشه کپی بگیرید. نتیجه چیست؟ بلی، امکان‌پذیر است. بنابراین نشان دادید که NTBackup قدرت بیشتری نسبت به My Computer در تهیه پشتیبان از پرونده‌ها و پوشه‌ها دارد.

۶-۱-۸ — ابزارهای مدیریتی ساده، قدرتمند و یکپارچه^۲: هر سیستم عاملی هر چقدر هم که قوی باشد اما اگر بیکربندی، تنظیمات و به طور کلی مدیریت آن پیچیده باشد با عدم استقبال عامه مواجه می‌شود و این دقیقاً یکی از دلایلی است که سیستم عامل UNIX به ویژه نسخه‌های قدیمی‌تر فقط در بین متخصصین محبوبیت پیدا کرد.

آشنایی با یکی از ابزارهای مدیریتی قوی در ویندوز NT 5.x

یکی از برنامه‌های قدرتمند برای مدیریت بخش‌های مختلف، برنامه‌ای است به نام Computer Management. برای اجرای این برنامه راه‌های متفاوتی وجود دارد در اینجا دو راه را بیان می‌کنیم.

الف) روی نشانه My Computer در میز کار کلیک راست کرده، گزینه Manage را انتخاب کنید.

ب) از طریق Run تایپ کنید : Compmgmt.msc
پس از اجرای برنامه، بررسی کنید که به وسیله آن چه کارهایی را می‌توان انجام داد.

۷-۱-۸- قابلیت اطمینان و پایداری^۱: با یک مثال مفهوم این ویژگی برای ما تثبیت

می‌شود، تجربه شده است که سیستم عامل ویندوز 98 برخلاف سیستم عامل UNIX و LINUX پس از نصب چندین برنامه مختلف به هم می‌ریزد حال به نظر شما چنین سیستمی مناسب شبکه و مخصوصاً سرویس دهنده است؟!

سیستم عامل‌های ویندوز NT و مخصوصاً NT 5.x در وضعیت بسیار بهتری نسبت به خانواده ویندوز 9x قرار دارند و بدین لحاظ برای کاربرد در شبکه‌ها اعم از سرویس گیرنده یا سرویس دهنده مناسب‌ترند.

۸-۱-۸- پشتیبانی^۲: هر سیستم عاملی اعم از قوی یا ضعیف نیاز به رشد و رفع مشکلات و

نواقص دارد و این با پشتیبانی از طرف تهیه‌کنندگان آن یا تیم‌های جنبی میسر می‌شود. در زمینه محصولات مایکروسافت با وجود نقص‌های بسیار به ویژه در زمینه امنیتی، پشتیبانی آن قوی بوده و اکثراً تجربه به هنگام سازی سیستم عامل‌های ویندوز NT 5.x را از طریق برنامه Automatic Update داشته‌ایم.

۲-۸- انواع سیستم عامل‌های شبکه

شرکت مایکروسافت به طور کلی در مورد سیستم عامل، دو دسته محصول ارائه کرده است:

- سیستم عامل‌هایی برای نصب و کاربرد در سرویس گیرنده.

■ سیستم عامل هایی برای نصب و کاربرد در سرویس دهنده.
در متن زیر طبقه بندی این سیستم عامل ها نشان داده شده است :

1- Client Operating Systems:

DOS Family: DOS (v1,..., v6.2, v6.22, v7.0)

Windows 3.x Family: Windows 3.1, 3.11 (Windows for Workgroups)

Windows 9x Family: Windows 95, 97 (95 OSR2), 98, 98 SE, ME

Windows NT Family:

NT 3.51 Workstation

NT 4.0 Workstation

NT 5.0: 2000 Professional

NT 5.1: XP (Home, Professional, Media center, Tablet PC)

NT 6.0 Windows Vista

NT 6.1 Windows 7

2- Server Operating Systems:

NT 3.51 Server

NT 4.0 Server

NT 5.0: 2000 Server Family: (Server, Advanced Server, Data center)

NT 5.2: 2003 Server family: (Standard, Enterprise Data Center,
Web edition)

NT 6.D: Window 2008 server

NT 6.1 Windows 2008 server (R2)

همان طور که مشاهده می کنید ویندوز 2000 به نام ویندوز NT5.0، XP به نام NT 5.1 و 2003 به نام NT 5.2 نیز خوانده می شوند. در کل به هر سه سیستم عامل، خانواده ویندوز NT 5.x گفته می شود. ویندوز اکس بی فقط در گروه سرویس گیرنده و ویندوز 2003 فقط در گروه سرویس دهنده قرار گرفته است. به عبارت دیگر ویندوز اکس بی نسخه سرویس دهنده نداشته و ویندوز 2003 نیز نسخه

سرویس گیرنده ندارد.

هر چند خانواده ویندوز 9x و XP جایی در گروه سرویس دهنده‌ها ندارند اما خیلی از کاربران تجربه به اشتراک گذاری پوشه‌ها و چاپگرهای خود را در آنها داشته‌اند، یعنی رایانه‌ای که مثلاً سیستم عامل آن ویندوز 98 است تبدیل به فایل سرور یا سرویس دهنده چاپ می‌شود. این موضوع نقض کننده طبقه‌بندی فوق نیست، به عبارتی هر چند ویندوز اکس پی هم می‌تواند در مواردی تبدیل به سرویس دهنده شود اما قرار نگرفتن آن در گروه سرویس دهنده‌ها به معنی آن است که این سیستم عامل عمده‌تاً برای کاربرد در ایستگاه‌ها طراحی شده است.

مایکروسافت فقط خانواده ویندوز NT را برای کاربرد در سرویس دهنده‌ها پیشنهاد داده است. نام برخی از محصولات شرکت‌های دیگر در زمینه سیستم عامل‌ها (که عمده‌تاً برای کار در سرویس دهنده‌ها استفاده می‌شوند) عبارتند از:

- UNIX (SCO , Solaris, BSD, Free BSD, AIX, HP, Linux, ...)
- Novell Netware
- IBM OS/2, IBM LAN Server
- Apple Macintosh (Used in Graphic Stations)

خانواده UNIX تقریباً در همه زمینه‌ها کاربرد دارد. امروزه در ایران شبکه‌های بانکی، شرکت نفت، شهرداری، بیمه و ... همگی از این خانواده به عنوان سیستم عامل اصلی در سرویس دهنده‌ها بهره می‌برند.

فعالیت کارگاهی

۳-۸- ویندوز ۲۰۰۸ سرور

ویندوز ۲۰۰۸ سرور از جدیدترین نسخه‌های سیستم عامل سروری برای شبکه، توسط شرکت مایکروسافت به بازار عرضه شده است. ویندوز ۲۰۰۸ سرور با نام کد شده Longhorn نوشته شده است و محیطی شبیه ویندوز ویستا یا ویندوز ۷ دارد و در دو گروه ۳۲ و ۶۴ بیتی ارائه می‌شود که معماری x86 آن از نوع ۳۲ بیتی می‌باشد و معماری x64

برای ۶۴ بیتی مورد استفاده قرار می‌گیرد و دارای ویرایش‌های زیر است :

۱- ویرایش وب (Web Edition) : ساده‌ترین ویرایش Windows Server

2008 بوده و برای ایجاد یک سرویس دهنده وب مورد استفاده که سرویس IIS نسخه ۷ را برای رایانه سرویس دهنده فراهم می‌کند. این نسخه حداکثر از چهار پردازنده و چهار گیگا بایت RAM برای ۳۲ بیتی و ۳۲ گیگا بایت RAM برای ۶۴ بیتی پشتیبانی می‌کند.

۲- ویرایش استاندارد (Standard Edition) : برای شرکت‌های کوچک

تا متوسط طراحی شده است که ۱۰۰ تا ۵۰۰ رایانه را در شبکه می‌تواند پشتیبانی نماید و برای به اشتراک گذاشتن فایل و چاپگر مورد استفاده قرار می‌گیرد، همچنین از ۴ پردازنده پشتیبانی می‌کند.

۳- ویرایش مرکز داده (Datacenter Edition) : بالاترین نسخه ویندوز

۲۰۰۸ سرور می‌باشد برای برنامه‌های خیلی پیچیده با محاسبات خیلی زیاد مورد استفاده قرار می‌گیرد و تا ۶۴ پردازنده و ۵۱۲ گیگا بایت RAM را پشتیبانی می‌کند. ضمناً می‌توانید کلاسترهایی با ۸ رایانه را در آن ایجاد نمایید (کلاستر یعنی چنانچه یکی از رایانه‌ها خراب شد، رایانه دیگری به طور خودکار ادامه کار سرویس دهی در شبکه را انجام دهد). از مجازی سازی^۱ نیز پشتیبانی می‌کند یعنی می‌توان چند سیستم عامل را روی رایانه سرویس دهنده نصب کرده و به طور همزمان از آنها استفاده نمود (مجازی سازی از امکانات جدید ویندوز ۲۰۰۸ سرور می‌باشد)

۴- ویرایش مؤسسات (Enterprise Edition) : مدلی بین ویرایش استاندارد

و مرکز داده می‌باشد که برای شرکت‌هایی که بین ۵۰۰ تا ۲۰۰۰ کاربر دارند مورد استفاده قرار می‌گیرد. این نسخه تا ۸ پردازنده و تا ۶۴ گیگابایت RAM را پشتیبانی می‌کند. در اینجا نیز می‌توان کلاسترهایی با ۸ رایانه در آن ایجاد نمود و از مجازی سازی نیز پشتیبانی می‌کند.

۵- ویرایش ذخیره سازی (Windows Storage Server 2008) :

ویرایش‌های جدید ویندوز ۲۰۰۸ سرور می‌باشد و برای کارهای به اشتراک گذاری فایل و چاپگر بهینه‌سازی شده است.

۶- ویرایشی بر پایه پردازنده‌های ایتانیوم (Windows Server 2008 for Itanium Based System): از ویرایش‌های جدید ویندوز ۲۰۰۸ سرور بر اساس پردازنده‌های ۶۴ بیتی ایتانیوم می‌باشد.

۱-۳-۸- دلایل استفاده از ویندوز ۲۰۰۸ سرور

الف) وجود ابزارهای خود تشخیص^۱ و کنترل از راه دور^۲

ب) مدیریت کنسول سرور جدید

ج) انعطاف بیشتر در تنظیمات اختصاصی

د) پشتیبانی از مجازی سازی^۳

ح) وجود ابزار جدید PowerShell

و) حفاظت قوی تر از درایوها مانند BitLocker Drive Encryption

ز) بهبود TCP/IP (اضافه شدن TCP/IPv6)

ه) امکان نصب هسته سرور^۴ در محیط متنی به طور مستقل با ۸۶ فرمان

ط) پشتیبانی از سرور خوشه‌ای (سرور کلاستر)

ویندوز ۲۰۰۸ سرور را در دو حالت کاری می‌توان مورد استفاده قرار داد:

۱- Workgroup

۲- Domain

بعضی از نقش‌ها^۵ در هر دو حالت کاری قابل استفاده می‌باشند و بعضی از نقش‌ها (Roles) نیز فقط در Domain قابل استفاده می‌باشند.

در موقع خاموش کردن ویندوز ۲۰۰۸ سرور باید دلیلی داشت و آن دلیل را باید در کادر Comment در پنجره Shut Down مشخص نمود زیرا معمولاً سرورها به طور دائم مشغول سرویس دهی هستند و به ندرت خاموش یا راه اندازی مجدد می‌شوند.

۱- Self diagnosis

۲- Remote Control

۳- Virtualization

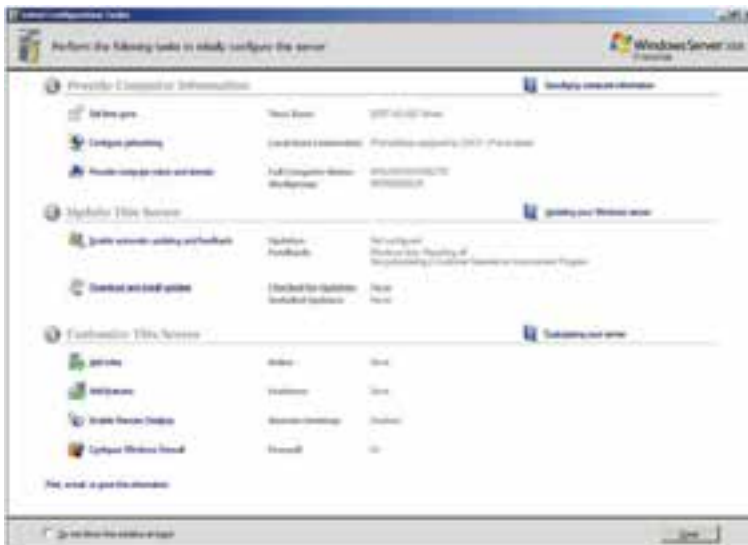
۴- Server Core

۵- Roles



شکل ۸-۱

بعد از اینکه اولین بار با کاربر مدیر وارد محیط ویندوز می شوید صفحه پیکربندی اولیه وظایف^۱ ظاهر می شود. که در شکل ۸-۲ نمایش داده شده است.



شکل ۸-۲- صفحه پیکربندی اولیه ویندوز ۲۰۰۸ سرور

در این صفحه شما می‌توانید تنظیماتی چون منطقه زمانی، اضافه کردن آدرس‌های IP و پیکربندی آنها، نامگذاری رایانه و اتصال آن به گروه کاری یا دامنه^۱، به روز رسانی ویندوز، اضافه کردن نقش‌ها^۲ و اضافه کردن اجزای ویندوز^۳ و غیره را انجام دهید. بعد از نصب ویندوز ۲۰۰۸ سرور، باید آن را فعال^۴ کنید. چون ویندوزی را که شما نصب کرده‌اید ۳۰ روزه می‌باشد و بعد ۳۰ روز شما فقط می‌توانید آن را فعال نمایید و امکان وارد شدن به محیط اصلی را نخواهید داشت (البته این کار با کراک کردن غیر فعال خواهد شد).

۲-۳-۸- نصب سرویس‌ها در ویندوز ۲۰۰۸ سرور

برای نصب سرویس‌ها ابتدا باید برنامه Server Manager (مدیریت سرویس دهنده) را از مسیر زیر اجرا نمود

Start → Administrative Tools → Server Manager



شکل ۳-۸

در پنجره Server Manager در سمت چپ بر روی Roles برای کار با سرویس‌ها کلیک نمایید. سپس از منوی Action گزینه Add Role را انتخاب نمایید

۱- Domain

۲- Roles

۳- Features

۴- Activate

و یا از کادر سمت راست بر روی گزینه Add Role کلیک نمایید تا بتوانید سرویس جدیدی را نصب کنید.

۳-۳-۸- انواع سرویس‌ها در ویندوز ۲۰۰۸ سرور

۱- File Services

۲- Active Directory Domain Services

۳- Print Services

۴- و ...

که در فصل‌های بعدی سرویس‌های مذکور تشریح خواهد شد.

خودآزمایی و پژوهش

- ۱- ویژگی‌های مهم سیستم عامل‌های سرویس دهنده را نام ببرید.
 - ۲- امنیت در سیستم عامل‌های شبکه‌ای در چه حوزه‌هایی بررسی می‌شود؟
 - ۳- User Data و System Data را تعریف کنید.
 - ۴- تفاوت چند وظیفه‌ای و چند برنامه‌ای را بنویسید.
- پژوهش کنید که حداقل سخت افزار لازم برای نصب هر یک از سیستم عامل‌های محصول مایکروسافت چیست و آنها را با هم مقایسه کنید.