موسسه غیرانتفاعی جهاد دانشگاهی همدان

گزارش کارآموزی کارشناسی ناپیوسته / گرایش نرم افزار

موضوع کارآموزی : فعالیت در بیمه توسعه

محل کارآموزی:

شرکت بیمه توسعه

نویسنده گزارش:

مسعود پارسانیا

تهیه و تنظیم :

کافی نت اسمان

آدرس :

www.asemankafinet.ir

تابستان ۱۳۹۱

فهرست مطالب :

معرفی مکان کارآموزی :

جایی که من برای گذراندن واحد کارآموزی انتخاب نمودم شرکت بیمه توسعه نهاوند بود. من در تاریخ ۱۳۹۱ /٤/۳ کارآموزی خود را شروع کردم و از گذراندن کارآموزی در آن شرکت راضی بودم.در آن شرکت تمامی فعالیت های گرافیکی و طراحی و انجام کارهای تایپ و کارهای مربوط به بایگانی اطلاعات بیمه شدگان را انجام می شد و میتوانست مکان فو ق العاده ای بر هر کسی اعم از دانشجو و .. باشد،من هم به کارهای طراحی خیلی علاقه داشتم وخیلی سعی کردم که بخش طراحی را به عنوان محل کارآموزی انتخاب کنم.و بتوانم در آنجا کارهایی یاد بگیرم و از دانش خودم که قبلا کسب کرده بودم استفاده کنم و بتوانم کم وکاستی های خود را برطرف سازم.

وظایف من در محل کارآموزی :

من در امور کارهای کامپیوتری در این شرکت فعالیت میکردم. البته گاهی اوقات نیز برای گرفتن اطلاعات از متقاضیان بیمه و بررسی اطلاعات نیز همراه سرپرست شرکت میرفتم. اما در کل ، من با تایپ نامه های شرکت و وارد کردن اطلاعات بیمه و بیمه شوندگان و کارهای کامپیوتری دیگر که برای پیشرفت امور شرکت مهم بود؛ شرکت را یاری میدادم. لازم بذکر است در کارهای شبکه و گرافیکی این شرکت نیز نقش اساسی داشتم همچنین در این دوره با بسیاری از اجرای شبکه و نحوه کار با آنها و پیکربیندی آنها آشنا شدم که این خود یک شانس و پیشرفت خوب در دوره تحصیل من بود.

فـــــــــصل دوم :

۱-۲ امنیت شبکه :

همانطور که در قسمت بالا نیز ذکر کردم شرکت گرافیکی بیمه توسعه دارای چیزی بالغ بر ۱۰ سیستم کامپیوتری می باشد که این کامپیوتر ها توسط یک سرویس دهنده سرور با همدیگر در ارتباط هستند همانطور که می دانید امنیت در یک شبکه بسیار مهم می باشد به طور کلی معنا و مفهوم امنیت شبکه جلوگیری از دسترسی کاربران غیر مجاز به شبکه بوده است در ایجاد امنیت شبکه برای هر یک از کاربران حقوق معینی در نظر گرفته می شود و کاربر هنگام اتصال به شبکه باید نام و گذرواژه خود را وارد کند سرور معتبر بودن ترکیب این نام و گذرواژه را کنترل می کند سپس با استفاده از آن و با توجه به بانک اطلاعاتی مجوزهای دسترسی کاربران که روی سرور موجود است دسترسی کاربر مورد نظر را به منابع اشتراکی قبول و یا رد می کند در محیط شبکه باید این اطمینان وجود داشته باشد که داده های حساس و مهم محفوظ باقی می ماند و فقط کاربران مجاز می توانند به آن ها دسترسی داشته باشند این کار نه تنها برای امنیت اطلاعات حساس بلکه برای حفاظت از عملیات شبکه نیز اهمیت دارد هر شبکه باید در برابر خسارات عمدی و یا غیر عمدی محفوظ نگه داشته شود به همین خاطر مدیریت محترم شرکت میگفت که امنیت در شبکه ی سیستم شرکت باید به طور متعادل صورت بگیرد و نباید امنیت را آنقدر سخت گیرانه فراهم کرد تا کاربران برای

استفاده از فایل های خودشان نیز دچار مشکل شود در اینجا من به این نتیجه رسیدم که باید امنیت شبکه به طور متعادل برقرار باشد یا در حد مورد نیاز امنیت برقرار باشد .

۱-۱-۲ مفاهیم امنیت شبکه :

امنیت شبکه یا Network Security **پردازه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند :**

۱- شناسایی بخشی که باید تحت محافظت قرار گیرد.

۲- تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.

۳- تصمیم گیری درباره چگونگی تهدیدات

٤- پیاده سازی امکاناتی که بتوانند از دارایی های شما به شیوه ای محافظت کنند که از نظر هزینه به صرفه باشد.

٥- مرور مجدد و مداوم پردازه و تقویت آن درصورت یاقتن نقطه ضعف

برای درک بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبکه می پردازیم.

۱- منابع شبکه:

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱- تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها

۲- اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

۳- منابع نامحسوس شبکه مانند عرض باند و سرعت

٤- اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

٥- ترمینالهایی که برای استفاد هاز منابع مختلف به شبکه متصل می شوند.

٦- اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

۷- خصوصی نگهداشتن عملیات کاربرن و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی های یک شبکه قلمداد می شود.

۲- حمله :

حال به تعریف حمله می پردازیم تا بدانیم که از شبکه در مقابل چه چیزی باید محافظت کنیم. حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.برای فهم بهتر بد نیست حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱- دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲- دستکاری غیرمجاز اطلاعات بر روی یک شبکه

۳- حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحا Denial of Service **نام دارند.**

کلمه کلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یک عمل مجاز یا غیرمجاز به عهده سیاست امنیتی شبکه است، اما به عبارت کلی می توان دسترسی غیرمجاز را تلاش یک کاربر جهت دیدن یا تغییر اطلاعاتی که برای وی در نظر گرفته نشده است، تعریف نمود اطلاعات روی یک شبکه نیز شامل اطلاعات موجود بر روی رایانه های متصل به شبکه مانند سرورهای پایگاه داده و وب ، اطلاعات در حال تبادل بر روی شبکه و اطلاعات مختص اجزاء شبکه جهت انجام کارها مانند

جداول مسیریابی روتر است. منابع شبکه را نیز می توان تجهیزات انتهایی مانند روتر و فایروال یا مکانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱- ثابت کردن محرمانگی داده

۲- نگهداری جامعیت داده

۳- نگهداری در دسترس بودن داده

۳- تحلیل خطر :

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱- احتمال انجام حمله

۲- خسارت وارده به شبکه درصورت انجام حمله موفق

٤- سیاست امنیتی :

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می مانند.در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱- چه و چرا باید محافظت شود.

۲- چه کسی باید مسئولیت حفاظت را به عهده بگیرد.

۳- زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

سیاستهای امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱- مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.

۲- محدود کننده (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودکننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشکلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد. المانهای دخیل در سیاست امنیتی در RFC ۲۱۹٦ لیست و ارائه شده اند.

۵- طرح امنیت شبکه :

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از :

۱- ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا بکارگیری SSH

۲- فایروالها

۳- مجتمع کننده های VPN برای دسترسی از دور

٤- تشخیص نفوذ

۵- سرورهای امنیتی AAA (Authorization and Accounting،Authentication) و سایر خدمات AAA برای شبکه

٦- مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه

٦- نواحی امنیتی :

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنابر استراتژی های اصلی ذیل تعریف می شوند.

۱- تجهیزات و دستگاههایی که بیشترین نیاز امنیتی را دارند (شبکه خصوصی) در امن ترین منطقه قرار می گیرند. معمولا اجازه دسترسی عمومی یا از شبکه های دیگر به این منطقه داده نمی شود. دسترسی با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از دور امن (SRA) کنترل می شود. کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه به شدت انجام می شود.

۲- سرورهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه ای امن ، خصوصی و مجزا قرار می گیرند. کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و دسترسی ها کاملا نظارت و ثبت می شوند.

۳- سرورهایی که باید از شبکه عمومی مورد دسترسی قرار گیرند در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار می گیرند. درصورت امکان بهتر است هر یک از این سرورها را در منطقه ای مجزا قرار داد تا درصورت مورد حمله قرار گرفتن یکی ، سایرین مورد تهدید قرار نگیرند. به این مناطق DMZ یا Demilitarized Zone می گویند.

٤- استفاده از فایروالها به شکل لایه ای و به کارگیری فایروالهای مختلف سبب می شود تا درصورت وجود یک اشکال امنیتی در یک فایروال ، کل شبکه به مخاطره نیفتد و امکان استفاده از Backdoor نیز کم شود.

علل عمده ای که می توانست امنیت شبکه را تهدید کند به شرح زیر بود :

- دسترسی غیر مجاز کاربران به اطلاعات شبکه و دستکاری اطلاعات
- سوء استفاده الکترونیکی
- سرقت رفتن اطلاعات محرمانه شبکه
- وارد شدن خسارات عمدی و یا غیر عمدی به اطلاعات شبکه

مدیر شبکه با پیاده سازی این امنیت های شبکه ای و دادن مجوز به کاربران برای ورود به شبکه تضمین می کند تا شبکه در برابر تهدیدات امنیتی همچنان محفوظ و ایمن باقی بماند در ضمن به این مساله نیز بایستی دقت داشت که برقراری امنیت و ایمنی اطلاعاتی برای تمامی شرکت ها یکسان نیست و شرکت های بزرگ همراه با سیستم های زیاد نیاز بیشتری به محافظت دارد تا یک شرکت کوچک با امکانات کمتر .

ایجاد امنیت برای محافظت از دارایی‌ها تعریف می‌گردد. روش های تعریف شده و استانداردهای متفاوتی برای حفظ دارایی‌ها موجود است.
در مورد امنیت مفاهیم مختلفی وجود دارد. امنیت می تواند شامل محافظت (protection) و یا تشخیص(detection) باشد.

- امنیت

حفظ دارایی‌ها برای جلوگیری از آسیب‌رسانی به آنهاست. یعنی ممکن است دارایی وجود داشته باشد، اما هیچ تهدیدی برایش معنی پیدا نکند. مانند تکه‌های الماسی که در کهکشان موجود است، تعریف امنیت برای این دارایی‌ها مادامی که تهدیدی برایشان نیست، معنی ندارد.

حفاظت از دارایی ها با اطلاع از اینکه این دارایی آسیب پذیری دارد و می‌تواند با سواستفاده از این آسیب‌پذیری مورد حمله قرار بگیرد، انجام می‌پذیرد. مثلا پایگاه داده‌ای که در شبکه موجود است و اطلاعات و شناسه‌های کاربران را در خود ذخیره کرده است، یک دارایی در شبکه محسوب می‌شود و باید مورد حفاظت قرار گیرد زیرا در صورت دسترسی افراد غیرمجاز، به شبکه آسیب می‌رسد. پس این آسیب‌پذیری می‌تواند مورد سواستفاده قرار گیرد.

- تشخیص

زمانی که تشخیص مد نظر ما باشد، باید ابزار و تمهیداتی در شبکه تعریف کنیم تا قابلیت تشخیص حمله‌ها (attack) را داشته باشد. ابزاری که وضعیت شبکه را آمارگیری نموده و در هر زمان از وضعیت ابزار شبکه، نودهای ارتباطی، ترافیک بین مسیریابها، نوع ترافیک انتقالی، زمان پیام‌ها و بسیاری از پارامترهای شبکه آگاهی دارد.

این ابزار وضعیت شبکه را همچون موجود زنده‌ای گزارش می‌دهند و در صورت ایجاد هر گونه وضعیت مشکوک در شبکه اقدامات امنیتی لازم را انجام می‌دهند.

محافظت و تشخیص نقشی همانند پیشگیری و درمان در مقابل بیماریها را دارند. تشخیص حمله در صورتی که از آن جلوگیری نماید، یک تشخیص فعال(active detection) نامیده می‌شود.

دسته دیگر تشخیص را تشخیص منفعل(passive detection) می نامیم. در این تشخیص بعد از وقوع حمله، گزارشی از وضعیت شبکه داده می‌شود و توانایی پیش‌بینی و پیشگیری از حمله‌ها وجود ندارد.

ایمن سازی ارتباطات در شبکه طبق استانداردهای تعریف شده دارای بخش‌ها و مفاهیم متفاوتی است.

هراستانداردی بخش‌هایی را برای امنیت تعیین می‌کند وحفظ امنیت هر داده‌ای بعضی از این بخش‌ها را شامل می‌شود. در ادامه به بخش‌های اساسی مفهوم حفظ امنیت می پردازیم.

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

برخی مفاهیم ضروری هستند. حفظ محرمانگی داده از ضروریات اولیه است. داده ارسالی که در شبکه تنها باید برای گیرنده و مقصد مفهوم و قابل استفاده باشد و بقیه گیرندگان غیر مجاز قابلیت بهره بردن از آن را نداشته باشند.
بجز محرمانگی , احراز هویت فرستنده پیام هم ارزشمند است.

فصـــــــل سوم :

۳–۱ نصب Fire Wall برای جلوگیری از ورود غیر مجاز به سیستم های کاربران :

این نرم افزار به عنوان مهمترین بخش برای کنترل حملات اینترنتی در شرکتی که در آن فعالیت می کردم بود و در آن تمامی سیستم ها دارای نرم افزار ذکر شده بودند تا سیستم ها را در برابر حملات اینترنتی محفوظ نگه دارد دیوارهای آتش به صورت نرم افزاری و سخت افزری موجود است که اطلاعات ارسالی به وسیله دو شبکه ارسالی را کنترل و فیلتر می کند در شرکت برای اتصال به اینترنت از یک دیوار آتش برای دسترسی به اطلاعات استفاده می کردیم بدون استفاده از دیوار آتش تمامی کامپیوتر های موجود در شبکه داخلی قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت بوده و از طرف دیگر کامپیوتر های دیگر نیز به راحتی قادر خواهند بود به رایانه های شخصی و شبکه های کامپیوتری دیگر به راحتی وارد شوند و دزدی اطلاعات انجام دهند بنابر این تمامی سیستم ها را تک به تک چک کردم تا همگی فایر وال آن ها فعال باشد تا از بروز این مشکلات در شبکه

شرکت مربوطه جلوگیری به عمل آید . در صورتی که بخواهید از فایر وال موجود بر روی ویندوز سیستم خود استفاده کنیم و آن را فعال کنیم می توانیم مراحل زیر را برای فعال کردن آن انتخاب کنیم .

Start >> Control Panel >> Windows Fire Wall

۳-۲ آشنایی با DNS (Domain Name System) :

در این شرکت نرم افزاری چون عمده کاری بر روی شبکه انجام می گرفت با تکنولوژی دیگری نیز به نام DNS آشنا شدم و برداشتی که درباره این مورد داشتم فهمیدم که DNS ها در واقع یکی از پروتوکل های TCP\IP می باشد که برای تبدیل اسامی به آدرس های IP در اینترنت بکار می رود هرگاه سیستمی از یک نام FQDN استفاده کند از سرور DNS تقاضا می کند آدرس IP معادل آن اسم را معین کند تا بتواند به وسیله آن آدرس در شبکه به آن دسترسی پیدا کند .

۳-۳ آشنایی با DHCP (Dynamic Host Configuration Protocol) :

این سرویس یکی از قابلیت های TCP/IP بوده و سرور ۲۰۰۳ می تواند این سرویس را ارایه کند در واقع این سرور در یک شبکه وظیفه دارد به سرویس گیرنده ها یک آدرس IP اختصاص دهد تا آن ها نیز بتوانند از شبکه استفاده کند این سرویس امکان پیکره بندی خودکاربه سرویس گیرنده ها را در لحظه ی شروع می دهد این سرور روش توزیع این قابلیت را به صورت اجاره ای انجام می دهد یعنی برای مدت معینی IP در اختیار Client قرار می گیرد و پس از پایان مدت اجاره لازم است دوباره تقاضای IP از Client صادر شده تا DHCP یک آدرس IP خالی را به آن اختصاص دهد در ویندوز ۲۰۰۳ سرور به طور پیش فرض ٦ روز یا ١٤٤ ساعت مدت اجاره یک IP می باشد .

۳-۴ آشنایی با مفهوم Domain در شبکه و کاربرد آن :

یکی از مهمترین مسایل در شبکه درک مفهوم دامنه یا Domain می باشد در واقع یک دامین گروهی است متشکل از یک یا چند سرور و ایستگاه های کاری که موافقت خود را برای متمرکز کردن کاربران و حساب های کاربری آن ها در یک بانک اطلاعاتی مشترک اعلام داشته اند و به همین دلیل اجازه می دهد یک کاربر دارای یک نام کاربری و یک رمز عبور بوده و در یک Domain سازماندهی شده قابل استفاده باشد .

در شرکت مدیر شرکت وقتی می خواهد که یک کارمند را استخدام کند اول محل کار و نوع کار و نوع ارتباط های کاری این کارمند را تعیین می کند یا میزان دسترسی و مجوز دسترسی به منابع سیستم را برای آن تعیین می کند Domain یکی از بهترین راه های تمرکز و مدیریت کاربران است در ویندوز ۳,۵۱ NT مدیریت به کمک یک user Profile انجام می شد که در واقع ابزاری بود برای مدیریت دسکتاپ و تنظیمات لازم هنگام ورود Log In به سیستم . در ٤ NT بحث دامین به وجود آمد که در واقع مکانی بود برای مدیریت تمرکز و سیاست های سیستم به منظور کنترل بیشتر کاربران . در ویندوز ۲۰۰۰ سرور یک Domain می توانست اطلاعات یک DNS را نیز متمرکز کند و سیاست های سیستم را نیز بهتر مدیریت کند که این بخش به Group Policies معروف گردیده است حال در پایین با توجه به بحث گفته شده در بخش بالا می خواهیم با نحوه ساختن Domain آشنا شویم من در طی این مدت کارآموزی خود چیزی بالغ بر ٥ Domain را ساختم که در زیر به نحوه ساختن یک Active Directory Domain به منظور ساخت Domain پردازیم .:

۱-اول فرمان dcpromo را در زیر منوی Runاز منوی Start نوشته و اجرا می کنیم برنامه نصب Active Directory Domain نمایش می یابد

۲- در این ویزارد یک سری سوالات برای نصب می پرسد و در نهایت یک ساختار درختی را ایجاد می کند .

۳- روی دکمه Next کلیک کنید تا کادر بعدی نمایان شود .

٤- این پنجره پیغام میدهد که اگر شما یک دامین تحت ۲۰۰۳ سرور ساختید بدلیل افزایش امنیت نمی توانید از ویندوز ۹۵ یا DOS استفاده کنید و این به دلیل استفاده از قرارداد SMB ماکروسافت به جهت جلوگیری از هک شدن Active Directory می باشد . در ضمن نیاز به یک ارتباط کامل بین سرویس گیرنده و Domain بوده و بایستی اطمینان داشته باشید که این ارتباط قطع نمی شود از طرف دیگر برای برقراری ارتباط ویندوز ۹۸ با سرور ۲۰۰۳ لازم است که قبل از ارتباط توسط CD مربوط به ۲۰۰۳ سرور بخش ۹۸ Active Directory Client For Windows نیز نصب بکنید .

٥- پس از کلیک بر روی دکمه Next پنجره دیگری نمایش داده می شود که دارای دو بخش می باشد انتخاب بخش اول به این معنا است که می خواهید یک Domain Controller جدید ایجاد نمایید و بخش دوم نیز به این معنا می باشد که می خواهید یک Domain Controllerجدید تحت یک دامین موجود ایجاد نمایید بخش اول را انتخاب کرده و بر روی گزینه Nextکلیک کنید و در پنجره ظاهر شده مجددا Nextرا کلیک کنید .

٦- در پنجره بعدی دو گزینه وجود دارد گزینه اول به این معنا می باشد که Dns روی این دستگاه تنظیم نشده است و لازم است ابتدا آن را تنظیم کنید و در صورتی که این گزینه انتخاب شود در پنجره بعدی دوباره پیغام تنظیم DNS را می دهد که البته با انتخاب View Help می توان از راهنمای تنظیم DNS آن را انتخاب کرد و در اینجا گزینه دوم بدین معناست که آیا مایل هستید

کار ادامه یابد و DNSنیز پس از نصب Active Directory بر روی سیستم نصب شود بدین صورت که DNSرا انتخاب نکرده اید گزینه دوم را انتخاب کنید و روی NEXT کلیک کنید

۷-در پنجره بعدی لازم است نام کامل دامین خود را وارد کنید در این بخش نام دامین خود را My Domain.Edu قرار داده و روی Nextکلیک کنید .

۸-در پنجره بعدی از شما دو آدرس پرسیده می شود مسیر اول برای ذخیره سازی بانک اطلاعاتی مربوطه Active Directory بوده و لازم است پارتیشنی با سیستم فایل NTFS انتخاب شود مسیر دوم هم برای ذخیره Logفایل یا به عبارتی گزارش های Active Directory می باشد . و برای بازیابی و توانایی بازیابی بهتر داده ها بهتر است که این دو فایل در درایو فیزیکی نا برابر و یا مجزا از هم ذخیره شود آدرس این دو مسیر را بر روی دو درایو با سیستم فایل NTFS ذخیره کنید و بر روی NEXT کلیک کنید .

۹- در پنجره باز شده آدرس پوشه ای به نام SYSVOL پرسیده می شود در واقع یک آدرس برای نگهداری یک کپی از فایل های عمومی از دامنه هاست در NT٤ اطلاعات مهم کاربران و اطلاعات کنترلی آن ها در پوشه ای به نام NETLOGON در ۲۰۰۳ سرور همین کار را انجام می دهد NEXT را کلیک کنید

۱۰- دو گزنه دیگر در اینجا وجود دارد : انتخاب اول یعنی سرویس گیرنده ها از ویندوزی قبل از ۲۰۰۰ استفاده می کنند انتخاب دوم یعنی سرویس گیرنده ها از ویندوزی بعد از ۲۰۰۰ استفاده می کنند پس بهتر است گزینه دوم که پیش فرض است را انتخاب کنیم

۱۱- در این قسمت لازم است رمزی را برای وضعیت Restore Mode حساب کاربری Administrator تعریف کنید و در واقع این رمز هیچ ارتباطی با رمز اصلی ادمین شما ندارد و می تواند کاملا متفاوت باشد مثلا رمز ۱۲۳٤ را وادر کرده و پس از تایید بر روی NEXT کلیک کنید .

۱۲-در صورت موافقت با آن ها بر روی NEXT کلیک کرده تا مراحل نصب نرم افزار انجام شود و در صورتی که نرم افزار شما به صورت صحیح نصب شده باشد حتما بعد از اتمام نصب سیستم شما Restartمی شود اگر نشد جایی از مراحل نصب را اشتباه انجام داده اید به این صورت می تون دامین برای استفاده در شبکه های شازمان یا شرکت های نرم افزاری را ساخت .

۵-۳ آشنایی با زیرساختهای Active Directory :

یک دایرکتوری (Directory) مجموعهای ذخیره‌شده از اطلاعات درباره‌ی اشیایی است که به نوعی با یکدیگر مرتبطند. یک سرویس دایرکتوری (Directory Service) تمامی‌اطلاعاتی را که برای استفاده و مدیریت این اشیا لازم است، در یک محل متمرکز ذخیره نموده و بدین ترتیب نحوه‌ی یافتن و مدیریت این منابع را تسهیل می‌بخشد. یک Directory Service زمینه‌ای را

فراهم می‌آورد تا دسترسی به منابع در سطح شبکه به بهترین نحو ممکن سازمان یابد . کاربران و مدیران ممکن است که نام دقیق یک شئ مورد نیاز را ندانند، اما با دانستن یک یا چند ویژگی از یک شئ و با استفاده از Directory Service می‌توانند لیستی از اشیا با ویژگی مورد نظر خود را جستجو کنند.

۱-۵-۳ چرا Service Directory؟:

نیاز به یک Active Directory قوی و شفاف، از رشد انفجاری شبکه ها ناشی می شود. همان طور که شبکه ها رشد می کنند و پیچیده تر می شوند و برنامه های کاربردی که نیاز به شبکه و سیستم های دیگر در اینترنت دارند افزایش می یابند، به همان میزان نیاز فراوانی به Service Directory احساس می شود .دایرکتوری سرویس یکی از مهمترین ابزارهای سیستم های پیشرفته کامپیوتری است که در این جا بد نیست مزایای این سرویس را با هم مرور می کنیم:

۱- فراهم کردن یک مرکز واحد و یکنواخت مدیریتی برای کاربران، برنامه های کاربردی و دستگاه ها.

۲- فراهم کردن یک نقطه ورود جهت دسترسی به منابع شبکه و همچنین فراهم کردن ابزارهای قوی و یکنواخت مدیریتی برای مدیریت سرویس های ایمنی برای کاربران داخلی و نیز کاربرانی که از راه دور و توسط تلفن ارتباط برقرار می کنند.

۳- مهیا کردن دسترسی استاندارد و یکسان به همه امکانات اکتیو دایرکتوری.

اکتیو دایرکتوری یک جزء اصلی از معماری شبکه ویندوز ۲۰۰۰ و هسته های مشابه است. Active Directoryبه سازمان ها اجازه می دهد که اطلاعات خود را در شبکه، شامل منابع موجود در شبکه و کاربران شبکه به اشتراک بگذارند و مدیریت کنند. اکتیو دایرکتوری همچنین به عنوان یک مرکز اصلی برای امنیت شبکه عمل می کند. به طوری که اجازه می دهد سیستم عامل به طور شفاف هویت کاربر را تعیین نماید و همچنین دسترسی به منابع شبکه را توسط آن کاربر کنترل نماید .نکته مهمتر این است که Active Directoryبه عنوان نقطه ای برای گردآوری تعمیم ها و مدیریت آنها عمل می کند. این قابلیت ها به سازمان ها اجازه می دهند که قوانین کاری استانداردی را برای برنامه های کاربردی توزیع شده و منابع شبکه به کار ببرند، بدون اینکه نیازی به مدیرانی داشته باشند که توانایی نگهداری دایرکتوری های مخصوصی را داشته باشند. در عین حال Active Directory یک نقطه مرکزی را برای مدیریت حساب های کاربران و سرورها و برنامه های کاربردی در محیط ویندوز فراهم می کند که با برنامه های کاربردی تحت ویندوز و دستگاه های سازگار با ویندوز ارتباط برقرار کنند. به این ترتیب Active Directory باعث توسعه سرمایه گذاری در شبکه می شود. همچنین باعث کم شدن هزینه استفاده از کامپیوتر از طریق افزایش مدیریت بیشتر و راحت تر شبکه، افزایش ایمنی شبکه و افزایش قابلیت همکاری بین شبکه ها می شود. استراتژی Directory Service شرکت مایکروسافت سبب می شود که بسیاری از فروشنده ها و مراکز، Service Directoryهای خاصی را در برنامه های کاربردی یا دستگاه هایشان

تعبیه نمایند تا بتوانند درخواست ها و عملیات هایی را که مورد نیاز مشتریان است برآورده سازند. برای مثال سرویس E-mail شامل Directory Service هایی است که به کاربران اجازه می دهد تا صندوق پست خود را جست وجو کنند. سیستم عامل های سرور نیز می توانند از Directory Serviceها برای امکاناتی نظیر مدیریت حساب کاربران، ذخیره کردن اطلاعات و پیکربندی برای برنامه های کاربردی استفاده کنند **Active** Directory .اولین Director Service کامل و جامع است که اندازه پذیر بوده و از اندازه های کوچک شروع می شود و به اندازه های بسیار بزرگ می رسد و نیز براساس تکنولوژی اینترنتی ساخته شده و کاملاً با سیستم عامل هماهنگ است ...علاوه بر این جهت برنامه های کاربردی تحت ویندوز، Active Directoryطوری طراحی شده که برای کاربران، محیط های ایزوله و محیط های انتقال، محیط مدیریت متمرکز را با حداقل Directory Service مورد نیاز شرکت ها فراهم می کند و این توانایی Active Directory را برای مدت طولانی به عنوان پایه و ستون اصلی جهت اشتراک گذاشتن اطلاعات و مدیریت مشترک منابع شبکه، شامل استفاده از برنامه های کاربردی، سیستم عامل های شبکه و سرویس های وابسته به دایرکتوری مطرح می کند.

۲-۵-۳ اکتیو دایرکتوری چگونه کار میکند ؟ :

اکتیو دایرکتوری به سازمان ها اجازه می دهد تا اطلاعات را به صورت سلسله مراتبی طبقه بندی کنند و برای پشتیبانی محیط های شبکه ای توزیع شده، مدل تکثیر اطلاعات در سرورهای متناظر را ارائه می کند. اکتیو دایرکتوری از اشیا برای نمایش منابع شبکه استفاده می کند. کاربران، گروه ها، ماشین ها، دستگاه ها و برنامه های کاربردی از بسته ها برای نشان دادن سازمان ها استفاده می کنند مثل بخش بازاریابی و یا مجموعه ای از اشیای وابسته به هم مانند پرینترها. این اطلاعات در ساختارهای درختی که از این اشیا ایجاد می شوند سازماندهی می شوند و همانند روشی است که سیستم عامل های ویندوز برای فایل ها و شاخه ها جهت سازماندهی اطلاعات در کامپیوتر استفاده می کنند. علاوه بر این اکتیو دایرکتوری روابط بین اشیا و بسته ها را فراهم می کند تا یک دید متمرکز و جامع را نشان دهد و این باعث می شود که درک و کنترل منابع راحت تر شده و مدیریت آنها بهینه شود. ساختار سلسله مراتبی اکتیو دایرکتوری که یک ساختار انعطاف پذیر و قابل پیکربندی است باعث می شود که سازمان ها منابع را آن طور که به آن نیازمند هستند سازماندهی کنند .گروه بندی اشیا در داخل دایرکتوری اجازه می دهد که مدیران اشیا را در سطح ماکرو مدیریت کنند. این کار کارایی، دقت و مدیریت را افزایش می دهد، به طوری که سازمان ها مدیریت شبکه را با نیازهای تجاری خودشان انجام می دهند.

برای فراهم کردن قابلیت اجرایی بالا، دسترسی بهتر و قابلیت انعطاف در محیط های توزیع شده، اکتیو دایرکتوری از تکثیر اطلاعات در سرورهای متناظر استفاده می کند و این به سازمان ها اجازه می دهد که نسخه های گوناگون از دایرکتوری ها ایجاد کنند. در نتیجه، تعویض ها و تغییراتی که در هر جای شبکه صورت بگیرد به طور اتوماتیک در سراسر شبکه کپی می شوند. از سوی دیگر اکتیو دایرکتوری از تکثیر اطلاعات در سرورهای متناظر برای قابلیت انعطاف، جهت افزایش و بالا بردن میزان دسترسی و اجرا پشتیبانی می کند. برای مثال کپی دایرکتوری Syncron می تواند از هر موقعیت و مکانی در شبکه مورد استفاده قرار گیرد.

چنین پردازشی می تواند اجرای سریع تر را در اختیار کاربر بگذارد. به این دلیل که کاربران برای دسترسی به منابع مورد نیازشان به جای جست وجو در شبکه ، آن را از طریق جست وجو در دایرکتوری سرور محلی خود پیدا می کنند. این دایرکتوری ها بسته به منابع مدیریتی که در دسترس است می توانند به طور محلی یا از راه دور مدیریت شوند.

۳-۵-۳ مـــــــزایای اکتیو دایرکتوری :

به علت ارتباط تنگاتنگ و کاملاً مجتمع اکتیو دایرکتوری با ویندوز ۲۰۰۰ این قابلیت در اختیار مدیران شبکه، برنامه نویسان و کاربران قرار گرفته که به Service Directory **زیر دسترسی داشته باشند:**

۱-آسان تر کردن کارهای مدیریت

۲-افزایش امنیت شبکه

۳-قابلیت استفاده از سیستم های موجود در محیط شبکه های مختلف و آسان کردن مدیریت سیستم های توزیع شده که اغلب منجر به اشتراک زمانی می شوند. در عین حال زمانی که شرکت ها برنامه های کاربردی را به زیرساخت و شالوده خود اضافه کنند و یا پرسنل خود را بازنشسته می کنند و همچنین نیاز به توزیع نرم افزار بر روی کامپیوترهای خود و همچنین مدیریت دایرکتوری های برنامه های کاربردی دارند، اکتیو دایرکتوری به شرکت ها اجازه می دهد که هزینه های خود را با استفاده از کنترل مرکزی کاربران، گروه ها و منابع شبکه به همراه نرم افزار توزیع شده و مدیریت پیکربندی کامپیوترهای کاربران کاهش دهند. اکتیو دایرکتوری از سوی دیگر به شرکت ها کمک می کند که مدیریت آسان تر و راحت تری داشته باشند. این سرویس با سازماندهی کاربران و منابع شبکه به طور سلسله مراتبی به مدیران اجازه می دهد تا یک مرکز واحد مدیریت را برای حساب های کاربران و سرورها و برنامه های کاربردی داشته باشند .اکتیو دایرکتوری مدیریت منابع شبکه را آسان می کند. در واقع اکتیو دایرکتوری با تعویض اختیار وظایف مدیریتی به افراد یا گروه های خاص، انجام کارهای مدیریتی منابع شبکه را ارتقا می دهد. اکتیو دایرکتوری یک مزیت بزرگ دیگر نیز دارد و آن هم بالا بردن امنیت است.

Active Directory مدیریت را متمرکز می کند و نقش هایی که دارای امنیت مستحکم و استوار هستند را به وسیله پردازش قوانین جاری در سازمان ها اجرا می کند. Active Directory امنیت رمزها و مدیریت را بالا می برد. انجام این کار با فراهم آوردن نقطه ورود یکسان در منابع شبکه با کار گروهی و سرویس های امنیتی با قدرت بالا مقدور می شود. Active Directory عملکرد کامپیوتر را نیز تثبیت می کند. این سرویس این کار را با قفل کردن پیکربندی کامپیوتر و جلوگیری از دسترسی عملیات در سطح کامپیوتر

مشتریان انجام می دهد و با فراهم کردن ساختارهای پشتیبانی کننده ایجاد امنیت در پروتکل های استاندارد اینترنت و سنجش تصدیق ورود مکانیسم ها سرعت تجارت الکترونیکی را بالا می برد. یکی دیگر از مزایای Active Directoryکنترل امنیت و سیستم های ایمنی است که با تنظیم کردن امتیازات دسترسی بر روی اشیای دایرکتوری و عنصرهای فردی اطلاعات که آنها را ایجاد می کند این کار را انجام می دهد.

۶-۳ پروتکل‌های امنیتی شبکه ها :

پروتکل، مجموعه قوانینی برای ارتباط طرفین و یا دو موجودیت نظیر(peer entity) می‌باشد. مجموعه قوانینی که برای انتقال پیام بین دو طرف ارتباط در یک شبکه وجود دارد. پروتکل‌های مختلفی در لایه های مختلف شبکه ها تعریف شده‌اند. این پروتکل‌ها اهداف مختلفی را دنبال می‌نمایند. پروتکل‌های تعریف شده در لایه کاربرد ارتباط بین دو نهاد به صورت انتها به انتها را برقرار می‌نمایند. یعنی دو کاربرد در دو انتهای ارتباط به صورت امن رابطه برقرار می‌نمایند.

پروتکل‌های امنیتی در لایه های پایین‌تر با ارتباط کاربردی، کاری ندارند و امنیت در حد واسطها و دیتا گرام و یا امنیت بسته را برقرار می‌نمایند.

پروتکل‌های امنیتی در ابتدا کار احراز هویت را انجام می‌دهند. احراز هویت به صورت یکطرفه و دو طرفه انجام می‌پذیرد. احراز هویت یک طرفه یعنی کاربر و یا نهادی که می‌خواهد از شبکه ارتباط بگیرد، باید ابتدا خود را معرفی نماید.

معرفی یک کاربر به شبکه، بسته به اینکه پروتکل امنیتی مربوط به کدام لایه باشد، فرق می‌کند. پروتکل امنیتی لایه سه، آدرس IP او را بررسی نموده و تصدیق می‌نماید. پروتکل امنیتی لایه کاربرد، آدرس پورت‌ها، شماره نشست و بقیه مشخصه‌ها را بررسی می‌نماید. بقیه مشخصه‌ها می‌تواند شامل شماره ترتیبی(Sequent Number) نیز باشد.

در احراز هویت دوطرفه شبکه سرویس‌دهنده هم باید خود را به کاربر معرفی نموده و خود را احراز نماید. بعد از معرفی اولیه دو طرف و توافق بر کیفیت ارتباط ؛ امکان ایجاد ارتباط ، تعریف شده و شروع می‌شود.

توافق‌های اولیه راجع به الگوریتم‌های رمزنگاری مورد استفاده، کلیدهای عمومی، کلیدهای خصوصی و بقیه مشخصه‌ها می‌باشد. پس از این مرحله هر دو طرف ارتباط می‌دانند که از چه کلیدی استفاده کنند تا طرف مقابل قادر به رمزگشایی باشد،از چه الگوریتمی برای رمزنمودن داده استفاده نمایند و بقیه اطلاعات لازم را از طرف دیگر بدست می‌آورند.

این توافق‌ها در بخشی به نام hand shaking و یا دست‌داد انجام می‌پذیرد. دستداد در ابتدای هر ارتباط انجام می‌پذیرد.

در مورد احراز هویت و روش‌های مختلف آن در مقاله‌های بعدی توضیح خواهیم داد.

از پروتکل‌های امنیتی می‌توانم به IPsec، SSL، SSH، TLS، WTLS اشاره کنم. هر کدام از این پروتکل‌ها می‌توانند به همراه پروتکل‌های شبکه و در کنار آنها، وظیفه اجرا و پیاده‌سازی مکانیزم‌های امنیتی را به منظور حفظ ابعاد هشت‌گانه امنیتی برعهده داشته باشند.

این مکانیزم‌ها از بروز حمله‌ها جلوگیری می‌نمایند. پیاده‌سازی برخی از این پروتکل‌ها به صورت اجباری در پروتکل‌ها تعریف شده است. به عنوان مثال پیاده‌سازی پروتکلIPsec در پروتکل IPv٦ اجباری می‌باشد. پروتکلIPsec مربوط به لایه شبکه و بقیه پروتکل‌های گفته شده مربوط به لایه کاربرد و یا انتقال می‌باشند.

سازگاری این پروتکل‌ها در کنار بقیه استانداردهای شبکه منجر به افزایش استفاده از آنها می‌گردد. برخی از آنها نیز همانند WTLS به منظور خاصی تعریف می‌گردد.

پروتکلWTLS یک پروتکل امنیتی لایه انتقال است که در شبکه‌های سیار برای حفظ امنیت لایه کاربرد ارتباط انتها به انتهای کاربران شبکه تعریف شده است.

پروتکل‌های دیگر لایه انتقال TLS،SSL می‌باشند و پروتکلSSH مربوط به ارتباط در لایه کاربرد می‌باشد. با وجودی که پروتکل‌های TLS،SSL شباهت زیادی دارند، به طور همزمان و در دو طرف یک ارتباط قابل استفاده نیستند. هدف این دو پروتکل صحت داده و محرمانگی ارتباط بین طرفین ارتباط می‌باشد.

SSL بیشتر توسطWEB browser ها و کارهای مربوط به شبکه که امنیت در آنها مهم می‌باشد، به کار گرفته می‌شود. یکی از این کاربردهای مهم تجارت الکترونیک می‌باشد.SSL بر روی TCP اجرا می‌گردد.

هر چه پروتکل امنیتی استفاده شده در لایه‌های پایین‌تر باشد نیازی به تغییر برنامه ها نخواهیم داشت. به عنوان مثال در صورت استفاده از IPsec نیازی به تغییرات در برنامه‌های کاربر نیست اما در صورتی که بخواهیم از SSL و یا TLS استفاده نماییم، باید برنامه کاربردی تا حدودی تغییر یابد و از پیاده‌سازی پروتکل امن مربوطه آگاه باشد.

۱-۶-۳ پروتکل امنیتی IPsec :

این پروتکل مسیریابی مطمینی در شبکه موجب می‌گردد و از بسیاری از حملاتی که ناشی از مسیریابی جعلی است ممانعت می‌نماید.

این پروتکل در دو مد transport و tunnel مورد بهره‌برداری قرار می‌گیرد. در مد انتقال، از payload یا همان داده و قسمتی از سرآیند IP که این پروتکل به آن اضافه شده است، محافظت می‌شود و سرآیندهای مربوط به IP محافظت نمی‌شوند.

مد تونل‌زنیIPSec بر روی دروازه‌ها و یا گره‌هایی که توسط آنها اطلاعات از زیرشبکه خارج می‌گردد، اعمال می‌گردد و در زمان خروج بسته‌ها ایمنی بر روی آن‌ها اضافه می‌شود و از payload محافظت می‌گردد.

کل داده به همراه بخش‌های ایمنی، به عنوان داده جدید برای datagram جدید درنظر گرفته شده و سرآیند مربوط به datagram نیز محافظت می‌شود. به این معنی که یک سرآیند خارجی امنیتی به کل بسته IP شامل داده و سرآیند آن اضافه می‌گردد.

ممانعت می‌کند و به علت تعریف شماره‌های توالی در خود از حمله تکرار نیز IPSpoofing از حملاتی نظیر IPsec پروتکل جلوگیری می‌کند. در حمله تکرار مهاجم بسته فرستاده شده در شبکه را دریافت نموده و دوباره آن را ارسال می‌کند. در صورت در یک بسته وقتی دوباره بسته‌ای فرستاده باشد، این شماره توالی در شبکه sequence Numberیا داشتن شماره توالی و می‌کند. در صورتی که بسته‌ای نیز از شبکه حذف شود، dropتکراری خواهد بود و گیرنده با دریافت این موضوع بسته را ٠شماره توالی مربوط به آن حذف شده است و شبکه متوجه مفقود شدن یک بسته خواهد شد
نوشتن شماره توالی و time stamp و یا مهر زمانی برای جلوگیری از حمله تکرار می‌باشد.

هر کدام از این دو مد کاری پروتکلIPSec، می‌توانند در دو نوع حالت پیاده‌سازی شوند. پیاده‌سازی این پروتکل با دو روش AH,ESP مورد اجرا قرار می‌گیرد. سرویس‌های پروتکل AH شامل احراز هویت، یکپارچگی داده و کنترل دسترسی است.

روش ESP با رمزنگاری، شامل سرویس‌های محرمانگی داده، کنترل دسترسی و محرمانگی جریان داده می‌باشد.

هر دو روش از ایجاد حمله تکرار بسته‌ها با استفاده از یک مقدار شماره توالی سی و دو بیتی، ممانعت می‌کنند.

زمان انتقال ترافیک، وقتی که بستهIP، به هر گره‌ای که بر روی آن IPSec نصب شده است، برخورد کند، بر اساس آدرس مقصد می‌تواند تشخیص دهد که این گره، کاربر نهایی، مسیریاب و یا یک دیواره آتش است.

۲-۶-۳ پروتکل امنیتی Transport Layer Security(TLS) :

این پروتکل امنیتی ، در لایه انتقال و بسیار نزدیک به پروتکل امنیتی(Secure Socket Layer)SSL تعریف شده است، تا ارتباطات روی شبکه را همانند شبکه اینترنت ایمن نماید. پروتکل‌های امنیتی TLS و SSL، پروتکل‌های امنیتی استفاده شده در لایه انتقال شبکه‌ها می‌باشند و در شبکه‌های سیار و سیمی می‌توانند پیاده‌سازی شوند. این پروتکل یک ارتباط انتها به انتها را رمزنگاری می‌نماید. موسسه IETF آن را در RFC۵۲٤٦ استاندارد نموده است.

هدف از تعریف و اجرای TLS در لایه انتقال، ایمن نمودن تراکنش‌های ارتباطی در لایه کاربرد می‌باشد. این پروتکل امنیتی می‌تواند در کنار پروتکل‌های ارتباطی، همانندHTTP،FTP،SMTP،NNTP مورد استفاده قرار گیرد. به عنوان مثال، مفهوم HTTPS یادآور این مطلب است که در ارتباط HTTP از پروتکل ارتباطی TLS در لایه انتقال بهره برده‌ایم.

به این ترتیب پروتکل‌های لایه بالاتر به همراه این پروتکل یک ارتباط ایمن را به همراه مکانیزم‌های موجود در TLS پدید می‌آورد. مکانیزم‌های درنظر گرفته شده این پروتکل، شامل رمزنگاری به منظور ایجاد محرمانگی در ارتباط و الگوریتم‌های صحت به منظور ایجاد یکپارچگی و تضمین حفظ صحت داده در روند انتقال آن به مقصد می‌باشد.

علاوه بر مکانیزم‌های گفته شده، تایید هویت نهادهایی که قصد شرکت در ارتباط را دارند، نیز در این پروتکل منظور شده است. پروتکل TLS تایید هویت یک‌طرفه یا دوطرفه (تایید هویت کاربر به شبکه و تایید هویت شبکه به کاربر) را برای دسترسی رمزشده به شبکه‌ها فراهم می‌نماید. این عمل با استفاده از الگوریتمی صورت می‌گیرد که کاربر و شبکه، هردو در مورد آن توافق نموده‌اند. بخش‌هایی همچون حفاظت از بسته داده، محدود نمودن و بهینه نمودن اندازه بسته و انتخاب یک الگوریتم سریع، به استاندارد TLS افزوده شده‌است.

کیفیت ارتباط بین دو طرف بستگی به نوع الگوریتم‌های توافق شده بین آنها دارد. این توافق قبل از اجرای TLS، و با تبادل پیام بین دو طرف بوجود می‌آید.

الگوریتم و روش انتخابی شبکه، در پیام ارسالی به اطلاع کاربر می‌رسد. الگوریتم‌ها شامل، الگوریتم‌هایی می‌باشد که قرار است در محاسبه چکیده پیام(MAC) مورد استفاده قرار گیرد.

علاوه بر آن الگوریتم‌ها و روش‌های انتخابی برای رمزنگاری نیز در این پیام ارسال می‌شود.به این ترتیب کاربر متوجه می‌شود از چه نوع الگوریتم و از چه تنظیماتی در ارتباط خود با شبکه بهره ببرد. تست صحت داده در این پروتکل، توسط الگوریتم‌های عمومی تعریف شده، انجام می‌پذیرد.

این پروتکل برای محافظت از پروتکل کاربردی SIP استفاده می‌شود. پروتکل SIP، در بحثVoIP و یا تلفن مبتنی بر IP کاربرد دارد. انتقال صوت بر روی شبکه اینترنت می‌تواند نمونه‌ای از VoIP باشد.

در لایه انتقال برای تعریف کانال‌های ارتباطی، مفهومی به نام نشست (Session) وجود دارد. نشست‌هایی که لایه انتقال در ارتباط با شبکه IP تعریف می‌نماید، دارای زمان اعتبار می‌باشد.

هر نشست تعریف شده، با استفاده از Sequence Number ها و یا همان شماره توالی مشخص می‌شود.

یک نشست علاوه بر شماره توالی دارای یک مدت اعتبار نیز می‌باشد. مدت اعتبار نشست نشان می‌دهد که تا چه زمان، ارتباط بین کاربر و شبکه IP می‌تواند طول بکشد.

قابلیت دیگری که در TLS وجود دارد، امکان تعلیق یک نشست و اجرای دوباره آن در زمانی دیگر می‌باشد.

به این طریق یک نشست می‌تواند در مدت زمان طولانی، به صورت باز، ولی غیرفعال باقی بماند. این قابلیت باعث می‌شود تا یک حمله‌کننده از مشخصه‌های ارتباط که در زمان طولانی معتبر باقی مانده است، سو استفاده نماید.

در طول مدت معتبر بودن یک نشست، کلیدهای امنیتی آن معتبر می‌باشند و این موضوع احتمال کشف کلیدهای رمزنگاری را توسط یک مهاجم افزایش می‌دهد.

۷-۳ انواع حملات :

حملات در شبکه‌های کامپیوتری جزو جدانشدنی دنیای اینترنت شده اند. حملات به دلایل متفاوتی همانند منافع تجاری، دلایل کینه‌جویانه، حیله‌گری و تقلب، جنگ و منافع اقتصادی انجام می‌پذیرند.

حمله‌ها در نتیجه نقص یکی از ابعاد امنیتی همانند محرمانگی، یکپارچگی و یا دسترس‌پذیری در شبکه و منابع آن انجام می‌پذیرند.

تقسیم بندیهای مختلفی برای انواع حملات تعریف شده است. شما هر کتاب و مرجعی را که ببینید نوعی گروه‌بندی را انجام داده‌اند. در مجموع حملات را به گروه‌های زیر تقسیم می‌نماییم.

- Modification Attacks (تغییر غیرمجاز اطلاعات)
- Repudiation Attacks (جلوگیری از وقوع یک اتفاق و یا تراکنش)
- Denial of service attacks (عملی که مانع می‌شود از اینکه منابع شبکه بتوانند سرویس‌های درخواستی را به موقع ارایه دهند.)
- Access attacks (دسترسی غیرمجاز به منابع شبکه و اطلاعات)

به طور عام هر عملی که باعث می‌شود تا عملکرد شبکه ناخواسته گردد، حمله نامیده می‌شود. ممکن است این عمل تغییر رفتار مشهودی در سیستم شبکه نباشد.

حمله غیرفعال: وقتی فرد غیرمجاز در حال شنود ترافیک ارسالی می‌باشد، تغییر مشهودی در رفتار سیستم نداریم. این حمله، حمله غیرفعال است. در صورتی که شنودکننده موفق به رمزگشایی گردد، اطلاعات مفیدی به دست آورده است.

حمله فعال: حمله‌ای که محتوای پیام را اصلاح نماید، فرستنده و یا گیرنده پیام را تغییر دهد و یا هر ترفندی که پاسخ مجموعه را تغییر دهد، حمله فعال نامیده می‌شود.

در ادامه به معرفی حملات معروف شبکه و راه‌های مقابله با آن خواهیم پرداخت.

: Denial of Service (DOS)/ Distributed DOS

درحمله DOS ، منابع یک سیستم اشغال می‌شود تا آن منبع توانایی پاسخگویی به درخواست‌ها را نداشته باشد. این حمله با بمباران سیل آسای یک سرور با تعداد زیادی از درخواست‌ها مواجه می‌نماید که نمی‌توان به همه آنها به صورت کارآمد پاسخ گفت. مورد دیگر فرستادن مجموعه درخواست‌ها به هارد درایو یک سیستم است که تمام منابع آن را درگیر نماید.

نوع دیگر DOS توزیع شده است که از طریق تعداد زیادی از host ها انجام می‌پذیرد. برنامه حمله بدون اطلاع مالکان، بر روی این سیستم‌ها نصب و در رابطه با اجرای حمله به سوی هدف، فعال می‌گردند.

مثال‌های زیر را می‌توان برایDOS **نام برد.**

Buffer overflow **(دریافت حجم زیادی از داده‌ها در پاسخ یک درخواست مانند دریافت حجم زیادی از پاسخ‌ها در مقابل دستور** echo **در پروتکل** ICMP**)**

SYN attack **(بهره‌برداری از فضای بافر در** handshake **پروتکل** TCP**)**

Teardrop Attack **(تغییر فیلد** offset **در بسته** IP**)**

Smurf **(فرستادن** Broadcast **یک دستور** PING **– ارسال پاسخ کلیه آنها به سمت هدف حمله– ایجاد ترافیک اشباع شده در سمت هدف)**

: Back door

حمله در مخفی از طریق مودم‌های dial up **و غیره انجام می‌گردد. سناریو آن دسترسی به شبکه از طریق کنار گذاشتن مکانیزم‌های کنترلی با استفاده از راه‌های مخفی می‌باشد.**

: IP Spoofing

در این حمله قربانی متقاعد می‌گردد که به یک سیستم شناخته شده و قابل اطمینان متصل شده است. این حمله در لایه TCP **انجام می‌پذیرد و آدرس یک مبدا مجاز (به جای مبدا غیرمجاز) داده می‌شود و مقصد این بسته را گرفته و دستورات بسته را پذیرفته، اعمال می‌نماید.**

۱-۷-۳ حمله های لایه کاربرد(virus, worm):

حمله های مربوط به لایه کاربردی شامل انواع ویروس‌ها و کرم‌ها می‌باشد. یکی از روش های انتشار ویروس‌ها ، قرار گرفتن در boot sector است که با هر بار روش شدن و بالا آمدن سیستم، ویروس فعال می‌گردد و در جاهای مختلف نظیرDVD,CD و ... قرار می گیرد.

یک ویروس روش های متفاوت تکثیر را در شبکه دارد. ویروس برای تکثیر نیازمند یک برنامه میزبان می باشد که در کامپیوتر میزبان نصب می‌گردد و از طریق اجرای این برنامه ، فعالیت خود را آغاز می‌نماید.

یک ویروس فایل‌های داده را آلوده نمی‌کند، چون فایلهای داده اجرا نمی‌شوند و قسمت اجرایی هم ندارند که بتوانند به ویروس کمک کنند.

گاهی ویروس‌ها به صورت رمزشده در شبکه منتقل می‌شوند. هدف از رمز کردن یک ویروس، ایجاد محرمانگی برای داده نمی‌باشد، بلکه هدف تغییر شکل ویروس است تا در شبکه توسط ابزار امنیتی مانند دیوار آتش و یا IDS ها قابل تشخیص نباشند و در مقصد توسط برنامه رمزگشایی که دارند، بازیابی شده و اجرا گردند.

ویروس ها بر اساس یک برنامه HOST و بر اساس تحریکی که ممکن است کاربر به آن پاسخ دهد(مثل کلیک کردن توسط کاربر) به سیستم وارد شده و منتشر می‌گردند. گاهی برنامه های نامربوطی به صورت دادن پیغام از ما می خواهند یکی از گزینه های YES/NO را انتخاب کنیم تا آنها اجازه داشته باشند که نصب شوند و ما غافل از اینکه هر دو گزینه YES/NOدر باطن یکی هستند گزینه NO را انتخاب می نماییم!! و به این ترتیب به برنامه ویروس اجازه می دهیم تا در کامپیوتر ما نصب شوند!!

علاوه بر ویروس‌ها که در لایه کاربرد شبکه فعال هستند، کرم ها نیز وجود دارند. کرم‌ها (worm) به صورت خودکار منتشر می‌شوند و نیاز به تحریکی از طرف کاربر ندارند. عملکرد کرم‌ها مستقل است و نیازی به استفاده از برنامه میزبان ندارند.

برای جلوگیری از نفوذ کرم‌ها و ویروس‌ها در شبکه اینترنتDARPA **یک گروه به نام گروه** CERT

Computer Emergency Response Team **را تشکیل داد که هنوز هم در زمینه امنیت فعال است.**

یک مدیر شبکه خوب باید اطلاعات کافی از مهاجمین داشته باشد و بتواند تشخیص دهد که مهاجم از لحاظ داشتن امکانات و نیز اطلاعات راجع به حمله، درچه سطحی قرار دارد.

اسب های تراوا نوع دیگری از حمله‌های لایه کاربرد می‌باشد. به اسب های تراوا که در سطح سیستم عامل عمل می‌کنندRootkit گفته می شود.

با توجه به حمله‌های لایه کاربرد، بررسی و تشخیص نقاط ضعف شبکه به جلوگیری و کشف حمله‌ها کمک موثری نماید. این روش ها شامل موارد زیر است:

- تعیین پورت های باز
- تعیین ماشین های فعال
- به دست آوردن نقشه شبکه
- تعیین موقعیت مسیریاب‌ها و دیواره آتش
- تعیین سیستم عامل
- تجزیه و تحلیل دیواره آتش و نقاط ضعف و قوت آن

علاوه بر اطلاعات بالا می توان از نرم افزارهای قوی که برایscan نمودن و تشخیص وضعیت شبکه نوشته شده‌اند، بهره برد. نرم افزارهایی مانند NESUS, ethereal و.... که البته دو نوع مورد استفاده مفید و مضر می توانند داشته باشند.

می توان از طریق نصب برنامه Nesus نقاط آسیب‌پذیر را یافت. این نوع نرم افزارها برای استفاده معمولی در شبکه طراحی شده‌اند تا مدیر شبکه نقاط آسیب‌پذیر شبکه را بیابد.

۲-۷-۳ راههای مقابله با چند حمله :

: File Extensions

سیستم عامل ویندوز قابلیتی دارد که اجازه می‌دهد تا پسوند یک برنامه در مقابل کاربر مخفی باقی بماند که ظاهرا باعث راحتی در کار است، اما باعث می‌شود برخی کدهای مخرب در ظاهری آشنا، مخفی شوند. مثلا فایلی با نام readme.txt در ظاهر یک

فایل متنی بی آزار است، در حالی که می تواند نام آن readme.txt.bat باشد! و پسوند واقعی.bat به علت خاصیت ویندوز مخفی شده باشد.

راه مقابله: شما می توانید خاصیت مخفی بودن پسوند فایل را در ویندوز غیرفعال نمایید.

Packet Sniffing :

ترافیک ایستگاه کاری شبکه‌های LAN ، در مقابل شنود توسط بقیه ایستگاه‌های کاری، در یک hub آسیب‌پذیر است. در این محیط، کاربر ترافیک دیگران را بدون اینکه آشکار شود و به صورت off lineگوش می‌دهد. ابزار شنود در این محیط، حمله را انجام داده ، ترافیک را شنود کرده، کپی نموده و سپس به مقصد نفوذکننده می‌فرستند. شنود شامل تمام ترافیک اینترنت مانند پست الکترونیکی، instant message و ترافیک web خواهد بود. در زمان شنود ترافیک web،تمام عملیاتی که کاربر انجام می‌دهد، توسط شنودکننده دیده می‌شود.

راه مقابله: بهترین روش محافظتی در مقابل این حمله، رمزگذاری پیام‌های انتقالی است تا در صورت شنود نیز نتوان استفاده‌ای از پیام‌ها نمود.

Hijacking and Session Replay :

Hijacking : **به معنی دزدی در حین انتقال به منظور انتقال به مقصد جدید است.**

Session Hijacking : **وقتی رخ می‌دهد که یک session پروتکل TCP/IP توسط یک شنودکننده شبکه برداشت شود. به این معنی که در حال انتقال یک پیام بین فرستنده و گیرنده، تغییرات لازم در وضع و حالت پیام داده شده و پیام اصلاح شده دوباره در جریان ترافیک شبکه قرار می‌گیرد. با این تغییرات، نفوذکننده به عنوان مقصد پیام تعریف می‌شود.**

تمام پیام‌های بعدی تعریف شده در آن session، بین مبدا اصلی و نفوذکننده(به عنوان مقصد جدید) در جریان خواهد بود و ترافیک به سمت مقصد مورد نظر حمله‌کننده، تغییر مسیر می‌دهد و تمامی پیام‌های بعدی آن session به حمله کننده می‌رسد.

راه مقابله: کاربردهای مبتنی بر web ، برای حمله‌های hijacking مناسب هستند. استفاده از پروتکل SSL از حملات hijacking و replay جلوگیری می‌نماید. این پروتکل بر روی TCP/IP و قبل از پروتکل‌های HTTP,IMAP استفاده می‌گردد و به صورت client- Server اجرا می‌شود. سرور خود را برای Client احراز هویت نموده و اجازه می‌دهد client نیز خود را به سرور معرفی نماید پس از احراز هویت دو سویه، یک ارتباط رمز شده بین دو طرف برقرار می‌شود.

۸-۳ اعمـــــال سیاست با Group Policy :

Group policy به سرورها و مدیران شبکه قدرت تنظیم و اعمال اجباری سیاست های خود روی کاربران و کامپیوترهایی که بعنوان کلاینت در شبکه قرار دارند را می دهد. برخی از سیاست ها که توسط Group Policy روی کامپیوتری ، کاربری یا گروهی خاص و بدون دخالت کاربر و از روی سرور انجام می شود عبارتند از :

نصب برنامه های کاربردی روی سیستم

تنظیم اجباری رجیستری به تفکیک کاربر یا به تفکیک کامپیوتر (منظور دستگاه کلاینتی که به شبکه Login میکند)

تنظیم موارد امنیتی (Security setting)

اجرای اسکریپت هایی هنگام بالا آمدن یا خاموش شدن سیستم

حذف و اضافه نمودن گزینه ای Taskbar و Start Menu وکنترل پانل

برخی تنظیمات برای سرویس هایی که از راه دور نصب می گردند

به عبارت دیگر یک مدیر شبکه با این امکان به جای اینکه روی تک تک سیستم ها تنظیماتی را انجام دهد می تواند از طریق سرور و برای گروه های مختلف سیاست های گوناگون را تنظیم و اعمال نماید طوری کاربر هیچگونه دخالتی در این خصوص نداشته باشد.

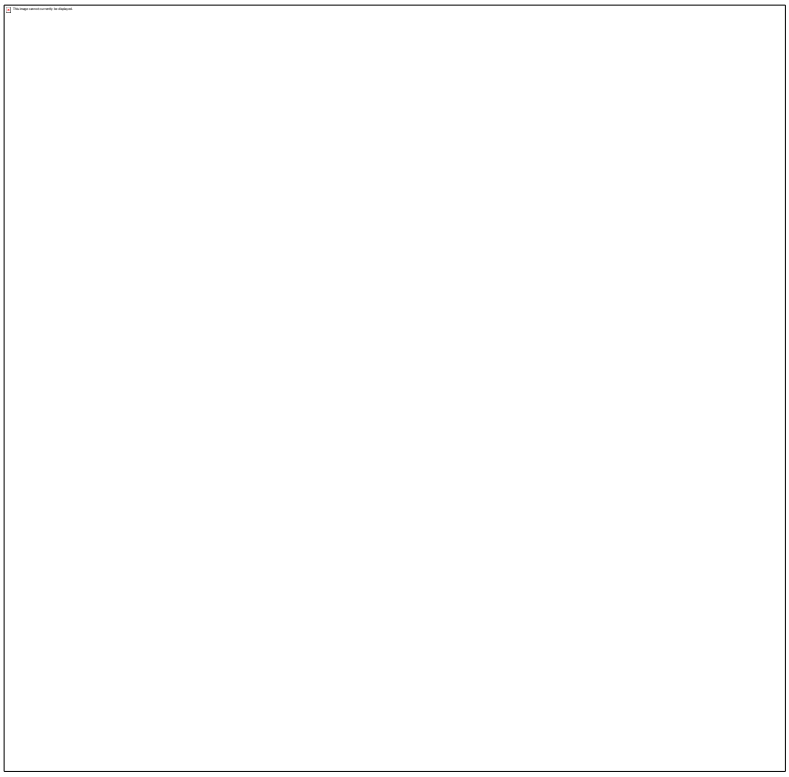
برخی از تنظیمات Group Policy مخصوص کاربر و برخی دیگر از تنظیمات مخصوص کامپیوتر است. یعنی اگر تنظیمات روی کاربر اعمال گردد ، آن کاربر از هر کامپیوتر وارد شبکه گردد آن سیاست ها و تنظیمات روی نام کاربری (Username) وی اعمال می شود و به کامپیوتر بستگی ندارد و برخی از سیاست ها (Policy ها) که روی کامپیوتر اعمال می شود به کاربر بستگی ندارد.

امروزه با توجه به گسترش و افزایش تعداد کاربران و کامپیوترها در شبکه ، یک مدیر تنظیمات لازم را برای یک فرد یا یک کامپیوتر انجام نمی دهد بلکه مدیر شبکه ابتدا گروه هایی ساخته و کاربران را عضو این گروه ها می کند و در این حالت می تواند سیاست ها و تنظیمات را روی این گروه ها اعمال کند. در این مقاله بر اساس امکانی که در ویندوز ۲۰۰۳ وجود دارد قصد داریم یک Organization Unit بسازیم و تنظیمات را روی آن اعمال نماییم. پس ابتدا روش ساخت یک Organization Unit را شرح می دهیم.

۱-۸-۳ ایجاد Organization Unit :

قبل از اینکه بخواهید Policy هایی را برای کاربران تعیین و اعمال نمایید و به منظور صرفه جویی در زمان یک Organization Unit ایجاد نمایید و کاربران مورد نظر را به عضویت آن در آورید تا نیاز نباشد برای هر کاربر جداگانه Group Policy تعریف و تنظیم شود. برای ساخت Unit Organization مراحل زیر را انجام دهید:

- در قسمت Start بر روی Administrative Tools کلیک و سپس گزینه Users and Computers Active Directory را انتخاب نمائید.
- مطابق شکل ۱ روی نام سرور راست کلیک کرده و از منوی New گزینه Organization Unite را انتخاب نمایید سپس یک نام (مانند MizbananUsers) برای آن در نظر بگیرید.



شکل - ۱

در ویندوز ۲۰۰۳ هر کاربری که جدید ساخته شود بصورت پیش فرض در گروه Users قرار می گیرد پس برای اینکه بتوانید User ایجاد شده را عضو گروه جدید کنید آن را توسط موس داخل گروه ساخته شده (این در مثال MizbananUsers) بیاندازید. در صورتیکه کاربری ایجاد نکرده اید بر روی Unit Organization ساخته شده راست کلیک کرده و از آنجا یک کاربر جدید بسازید تا از همان ابتدا عضو آن گروه قرار گیرد.

اکنون Organization Unit ساخته شده و اعضای آن نیز مشخص می باشند حال باید برای آنها Group Policy تعریف گردد.

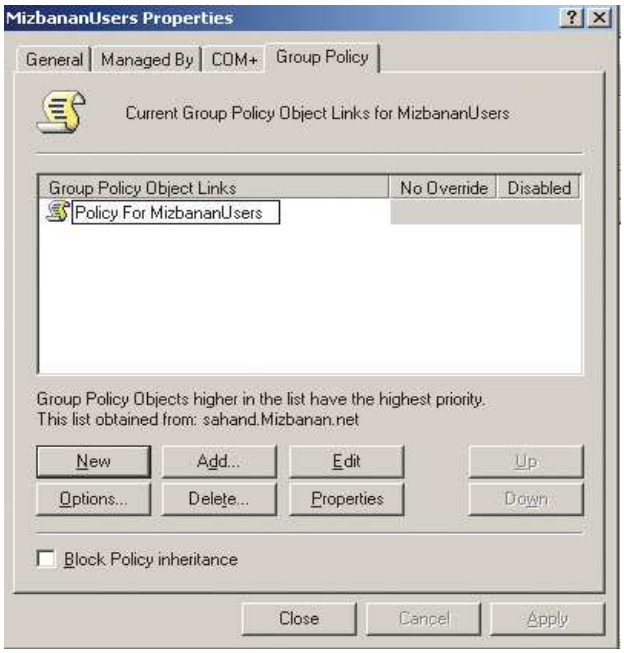
برای درک مفهوم Group Policy و آشنایی عملی با آن ، چند مثال را بطور عملی توضیح می دهیم.

۲-۸-۳ تنظیم Proxy برای کاربران بصورت گروهی :

فرض کنید در شبکه محلی (LAN) اداره یا سازمان مطبوع خود اینترنت راه اندازی کرده اید و می خواهید فقط برای گروهی از کاربران و با استفاده از قابلیت Group Policy ، پروکسی (Proxy) تنظیم نمایید. اگر شبکه شما دارای یک DC Domain Controller باشد و همچنین Active Directory راه اندازی کرده اید از این پس نیازی نیست برای تک تک کاربران پروکسی تنظیم کنید. بلکه مراحل زیر را طی کنید:

- روی Organization Unit ساخته شده راست کلیک و گزینه Properties را انتخاب نمایید.

- در صفحه ظاهر شده (در این مثال MizbananUsers Properties) به قسمت Group Policy بروید.
- در این قسمت و مطابق شکل ۲ دکمه New را بزنید و یک نام (مانند Policy For MizbananUsers) برای آن تعیین کنید.



شکل - ۲

اکنون وقت تنظیم پروکسی می باشد. برای این منظور مراحل را به ترتیب زیر ادامه دهید:

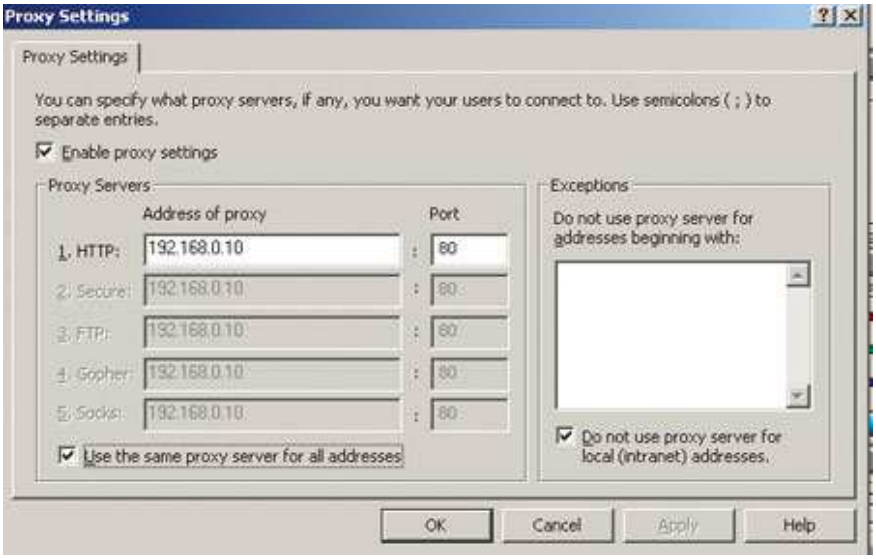
•در همان صفحه (مطابق شکل ۲) Policy تعریف شده را انتخاب و گزینه Edit را بزنید.

• در صفحه Group Policy Object Editor به مسیر زیر بروید.

Users Configuration Windows Setting Internet Explorer maintenance Connection

•در صفحه سمت راست گزینه Proxy Setting را انتخاب نمائید.

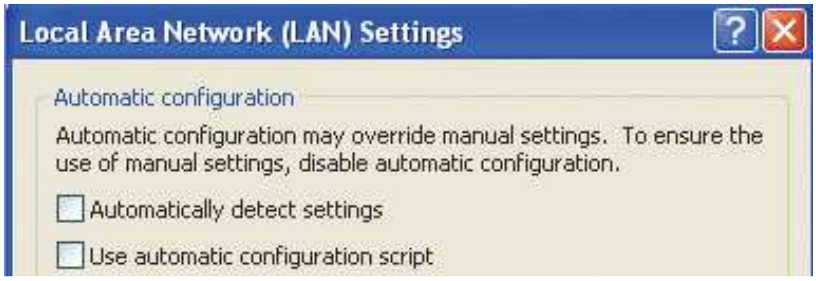
•در صفحه Proxy Setting ابتدا تیک Enable Proxy Setting را بزنید (به شکل ۳ توجه کنید).
•سپس مطابق شکل ۳ در قسمت HTTP آدرسی که قرار است کاربران به آن متصل شوند و اینترنت را از آنجا دریافت کنند را وارد کنید.

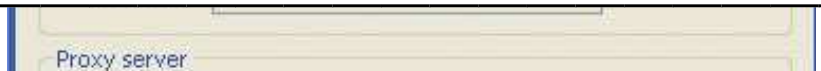


شکل – ۳

همانطور که در شکل ٤ ملاحظه می کنید از این پس ، کاربرانی که با نام کاربری و پسوردی که در Domain موجود باشد به شبکه Login کنند و عضو Organization Unit ساخته شده توسط شما نیز باشند ، بصورت اتوماتیک در اینترنت اکسپلور خود در قسمت Proxy Server آدرس ۱۹۲,۱٦۸,۰,۱۰ با پورت ۸۰ وارد شده است.

(Internet Options > Connection > LAN Setting > Proxy Server **)**





شکل – ٤

۳–۸–۳ تنظیمات و حذف و اضافه گزینه های مربوط به Control Panel :

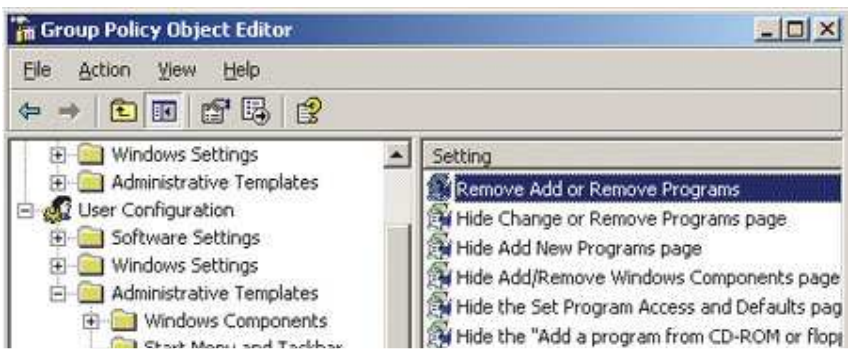
با توجه به تکرار مراحل قبلی که چندین بار به آن اشاره شد یعنی با ادیت کردن Group Policy ساخته شده و در صفحه Group Policy Object Editor از طریق مسیر :

User Configuration Administrative Templates Control Panel می توان کلیه تنظیمات و محدودیت های مربوط به کنترل پانل را برای کاربران انجام داد.

به عنوان مثال اگر بخواهید دکمه Add Remove Program از داخل کنترل پانل سیستم های موجود در شبکه حذف نمایید مراحل زیر را انجام دهید. به مسیر زیر بروید:

User Configuration Administrative Templates Control Panel Add or Remove Program

از صفحه سمت راست همانطور که در شکل ۸ مشاهده می کنید گزینه Add or Remove Program را با دوبار کلیک انتخاب کنید و سپس در پنجره‌ای که باز می شود گزینه Enable را بزنید.



شکل – ۵

بعد از این تنظیم اگر کاربری که جزء گروه ایجاد شده (در این مثال (MizbananUsers)) باشد وارد کنترل پانل سیستم خود شود با توجه Policy که در این مثال تعریف شده نمی تواند گزینه Add or Remove Program را اجرا نماید و صورت اجرای آن با پیغامی که در شکل ٦ مشاهده می کنید مواجه می گردد.

شکل – ٦

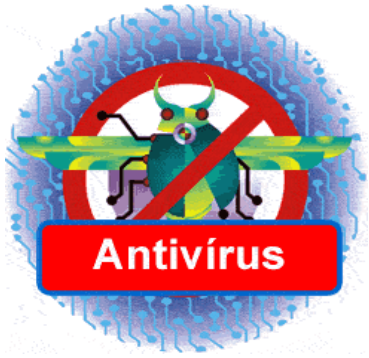
۹–۳ ۱۰نکته برای حفظ امنیت :

هر روزه اخبار جدیدی در مورد حملات و تهدیدات کامپیوتری در رسانه های مختلف انتشار می یابد. این تهدیدات شامل ویروس های جدید و یا انواع هک و نفوذ در سیستم های کامپیوتری است. انتشار این گونه اخبار باعث شیوع اضطراب و نگرانی در بین کاربرانی می شود که به صورت مستمر از کامپیوتر بهره می گیرند و یا اطلاعاتی ارزشمند بر روی کامپیوترهای خود دارند.در این مقاله سعی شده چند نکته که در رابطه با امنیت کامپیوتر اهمیت اساسی دارند به صورت مختصر شرح داده شوند. یک کاربر در صورت رعایت این نکات می تواند تا حدود زیادی از حفظ امنیت سیستم کامپیوتری خود مطمئن باشد. در رابطه با بعضی از نکات که توضیحات بیشتری لازم بوده، مقالات جامع تری معرفی گردیده اند.

استفاده از نرم افزارهای محافظتی (مانند ضدویروس ها) و به روز نگه داشتن آنها :

از وجود ضدویروس بر روی دستگاه خود اطمینان حاصل کنید. این نرم افزارها برای محافظت از کامپیوتر در برابر ویروس های شناخته شده به کارمی روند و در صورت استفاده از آنها کاربر نیاز به نگرانی در مورد ویروس ها نخواهد داشت. در شرایطی که روزانه ویروس های جدید تولید شده و توزیع می شوند، نرم افزارهای ضدویروس برای تشخیص و از بین بردن آنها باید به صورت منظم به روز شوند. برای این کار می توان به سایت شرکت تولید کننده ضدویروس مراجعه کرد و اطلاعات لازم در

مورد نحوه به روز رسانی و نیز فایل های جدید را دریافت نمود. عموما نرم افزارهای ضدویروس ابزار های به روز رسانی و زمان بندی این فرایند را در خود دارند. برای مطالعه بیشتر در مورد ویروس ها و آشنایی با طرز کار و قابلیت های ضدویروس ها به سایت گروه امداد امنیت کامپیوتری ایران مراجعه نمایید.



باز نکردن نامه های دریافتی از منابع ناشناس :

این قانون ساده را پیروی کنید، «اگر فرستنده نامه را نمی شناسید، نسبت به نامه و پیوست های آن بسیار با دقت عمل نمایید».

هرگاه یک نامه مشکوک دریافت کردید، بهترین عمل حذف کل نامه همراه با پیوست های آن است.

برای امنیت بیشتر حتی اگر فرستنده نامه آشنا باشد هم باید با احتیاط بود. اگر عنوان نامه نا آشنا و عجیب باشد، و بالاخص در صورتی که نامه حاوی لینک های غیرمعمول باشد باید با دقت عمل کرد. ممکن است دوست شما به صورت تصادفی ویروسی را برای شما فرستاده باشد. ویروس "I Love You" دقیقا به همین صورت میلیون ها کامپیوتر را در سراسر دنیا آلوده نمود.

تردید نکنید، نامه های مشکوک را پاک نمایید.

مقالات محافظت در برابر خطرات ایمیل ۱ و ۲ به صورت مفصل در رابطه با این موضوع نگاشته شده است

استفاده از گذرواژه های مناسب :

گذرواژه تنها در صورتی دسترسی غریبه ها به منابع موجود را محدود می کند که حدس زدن آن به سادگی امکان پذیر نباشد.

گذرواژه های خود را در اختیار دیگران قرار ندهید و از یک گذرواژه در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت. قانون طلایی برای انتخاب گذرواژه شامل موارد زیر است:

گذرواژه باید حداقل شامل ۸ حرف بوده، حتی الامکان کلمه ای بی معنا باشد. در انتخاب این کلمه اگر از حروف کوچک، بزرگ و اعداد استفاده شود (مانند xk۲۷D۸Fy) ضریب امنیت بالا تر خواهد رفت.

به صورت منظم گذرواژه های قبلی را عوض نمایید.

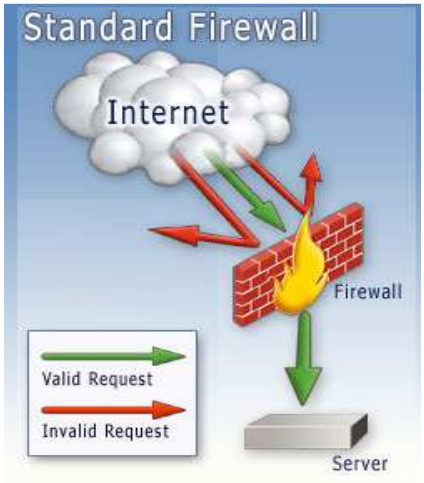
گذرواژه خود را در اختیار دیگران قرار ندهید.

در مقاله انتخاب و محافظت از کلمات عبور نکات دقیق تری در این رابطه بیان شده است.

محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظ(Firewall) :

حفاظ دیواری مجازی بین سیستم کامپیوتری و دنیای بیرون ایجاد می کند. این محصول به دو صورت نرم افزاری و سخت افزاری تولید می شود و برای حفاظت کامپیوترهای شخصی و نیز شبکه ها به کار می رود. حفاظ داده های غیر مجاز و یا داده هایی که به صورت بالقوه خطرناک می باشند را فیلتر کرده و سایر اطلاعات را عبور می دهد. علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است، مانع دسترسی افراد غیرمجاز به کامپیوتر می شود.

مقاله مقدمه ای بر فایروال به معرفی نحوه عملکرد حفاظ ها می پردازد و یکی از رایج ترین حفاظ های شخصی در مقاله حفاظ شخصی Zone Alarm معرفی شده است.



خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه :

سیستم های عامل این امکان را برای کاربران خود فراهم می آورند که با هدف به اشتراک گذاری فایل، دسترسی دیگران را از طریق شبکه و یا اینترنت به دیسک سخت محلی فراهم آورند. این قابلیت امکان انتقال ویروس از طریق شبکه را فراهم می

آورد. از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک گذاشتن فایل ها به عمل نیاورد، امکان مشاهده فایل های خود را به دیگرانی که مجاز نیستند ایجاد می کند. بنابراین درصورتی که نیاز واقعی به این قابلیت ندارید، به اشتراک گذاری فایل را متوقف نمایید.

قطع اتصال به اینترنت در مواقع عدم استفاده :

به خاطر داشته باشید که بزرگ راه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند. قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد.

تهیه پشتیبان از داده های موجود بر روی کامپیوتر :

همواره برای از بین رفتن اطلاعات ذخیره شده بر روی حافظه دستگاه خود آمادگی داشته باشید. امروزه تجهیزات سخت افزاری و نرم افزاری متنوعی برای تهیه نسخه های پشتیبان توسعه یافته اند که با توجه به نوع داده و اهمیت آن می توان از آنها بهره گرفت. بسته به اهمیت داده باید سیاست گذاری های لازم انجام شود. در این فرایند تجهیزات مورد نیاز و زمان های مناسب برای تهیه پشتیبان مشخص می شوند. علاوه بر این باید همواره دیسک های Start up در دسترس داشته باشید تا در صورت وقوع اتفاقات نامطلوب بتوانید در اسرع وقت سیستم را بازیابی نمایید.

گرفتن منظم وصله های امنیتی(Patches) :

بیشتر شرکت های تولید کننده نرم افزار هر از چند گاهی نرم افزارهای به روز رسان و وصله های امنیتی جدیدی را برای محصولات خود ارائه می نمایند. با گذر زمان اشکالات جدید در نرم افزارهای مختلف شناسایی می شوند که امکان سوءاستفاده را برای هکرها بوجود می آورند. پس از شناسایی هر اشکالی شرکت تولید کننده محصول اقدام به نوشتن وصله های مناسب برای افزایش امنیت و از بین بردن راه های نفوذ به سیستم می کنند. این وصله ها بر روی سایت های وب شرکت ها عرضه می شود و کاربران باید برای تامین امنیت سیستم خود همواره آخرین نسخه های وصله ها را گرفته و بر روی سیستم خود نصب کنند. برای راحتی کاربران ابزارهایی توسعه داده شده اند که به صورت اتوماتیک به سایت های شرکت های تولید کننده محصولات وصل شده، لیست آخرین وصله ها را دریافت می نمایند. سپس با بررسی سیستم موجود نقاط ضعف آن شناسایی و به کاربر اعلام می شود. به این ترتیب کاربر از وجود آخرین نسخه های به روز رسان آگاه می شود.

بررسی منظم امنیت کامپیوتر :

در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید. انجام این کار در هر سال حداقل دو بار توصیه می شود. بررسی پیکربندی امنیتی نرم افزارهای مختلف شامل مرورگرها و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فرایند انجام می شوند.

حصول اطمینان از آگاهی اعضای خانواده و یا کارمندان از نحوه برخورد با کامپیوترهای آلوده :

هر کسی که از کامپیوتر استفاده می کند باید اطلاعات کافی در مورد امنیت داشته باشد. چگونگی استفاده از ضدویروس ها و به روز رسانی آنها، روش گرفتن وصله های امنیتی و نصب آنها و چگونگی انتخاب گذرواژه مناسب از جمله موارد ضروری می باشد.

۱۰-۳ خلاصه مطالب :

***آشنایی با شبکه و انواع سرویس های آن**

*** انواع روش های دسترسی به خط انتقال اطلاعات در شبکه**

***کابل به کار برده در شبکه و استاندارد به کار رفته در اتصال سیم های شبکه شرکت**

***آشنایی با آرایش ستاره ای سیستم ها و نحوه ارتباط سیستم ها در این شرکت**

***نصب سیستم عامل Windows Server بر روی سیستم هایی که دچار مشکلات ویروسی**

شده بودند و برای راه اندازی مجدد شبکه نیاز به نصب این نرم افزار و تنظیمات دیگر داشتند .

***آشنایی با امنیت شبکه و مواردی که امنیت شبکه را تهدید می کند**

***نصب نرم افزار Fire Wall بر روی تک تک سیستم ها برای محافظت در برابر حملات و نفوذ در سیستم های شرکت**

***آشنایی با DNS و DHCP**

***آشنایی با دامین و طریقه ساختن یک Active Directory Domain**

(در پایان از استاد راهنما جناب مهندس شیرزاد بیات که مرا در هرچه بهتر کردن این گزارش یاری کردند کمال تشکر را دارم.)

منابع:

۱-کتاب شبکه های کامپیوتری اندرو اس تنن بام (ترجمه دکتر پدرام)

۲-کتاب شبکه های کامپیوتری سال سوم هنرستان رشته کامپیوتر (فنی) چاپ ۸۵

۳- چند سایت اینترنتی منجمله :

http://www.ircert.com

http://www.prozhe.com

http://www.srco.ir

http://computer۲۲٤.persianblog.com

pctips.javanblog.com

foxttm.pib.ir