FTP Siteو راه های ایمن سازی

مترجم : کیانوش مرادیان

FTP یا **File Transfer Protocol** یکی از رایج ترین و قدیمی ترین سرویسهای موجود بر روی شبکه ها و همچنین اینترنت است که برای نقل و انتقال فایلها روی شبکه بکار می رود. در حال حاضر FTP روشی استاندارد و در دسترس است که جامعیت یافته است.

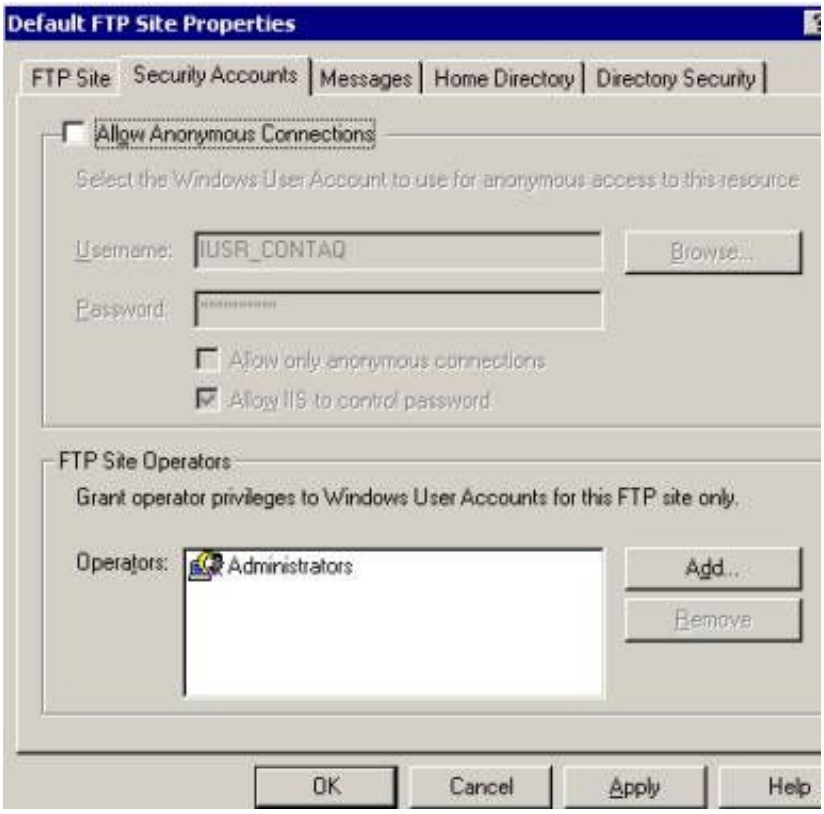
FTP Site یکی از اعضای IIS 5.0 بوده وبه همراه Windows 2000 آمده است بصورت یک Service مستقل با کارایی و امکانات فراوان می باشد. بعضی از این امکانات آشکار بوده و برخی از آنها توسط سرپرست شبکه مورد استفاده قرار می گیرند البته بعدها سرویسهای وابسته ای نظیر VPN و SSH برای امنیت رواج یافته اند.

در این نوشتار ده روش موجود در Windows 2000 توضیح داده خواهد شد تا به کمک آن بتوانید سایتهای FTP خود را بیش از پیش در اختیار گرفته ، ایمن نموده و کنترل نمائید.

۱- از دسترسیهای بی نام و نامشخص جلوگیری نمایید.

در ابتدا و پس از فعال ساختن FTP، دسترسی ها بی نام به صورت پیش فرض در سیستم به وجود می آیند. به عبارتی هرکس بدون ثبت و Autentication قادر به استفاده از FTP Site خواهد بود.

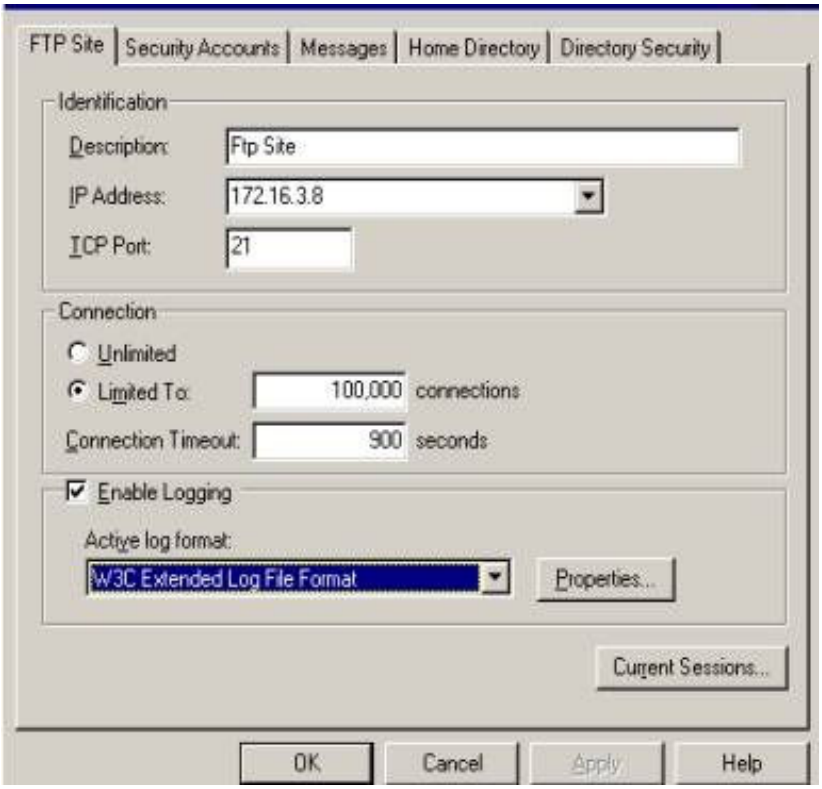
به غیر از موارد خاص از این خاصیت در اکثر اوقات استفاده غیر مجاز می شود. با حذف دسترسی Anonymous که به معنای بی نام است و استفاده از کلمه عبور و Password مختص کاربر قادر به کنترل دسترسی ها خواهیم بود. این عمل با تنظیم ACL یا (Access Control List) روی FTP Home Directory که در سیستم NTFS وجود دارد قابل انجام است.



برای محدود کردن دسترسی های ناشناس به FTP ، گزینه مربوط بـه Allow Anonymous Connection در پنجره Security Accounts واقع در FTP Property را بردارید.

۲- گزارشگیری را فعال نمایید

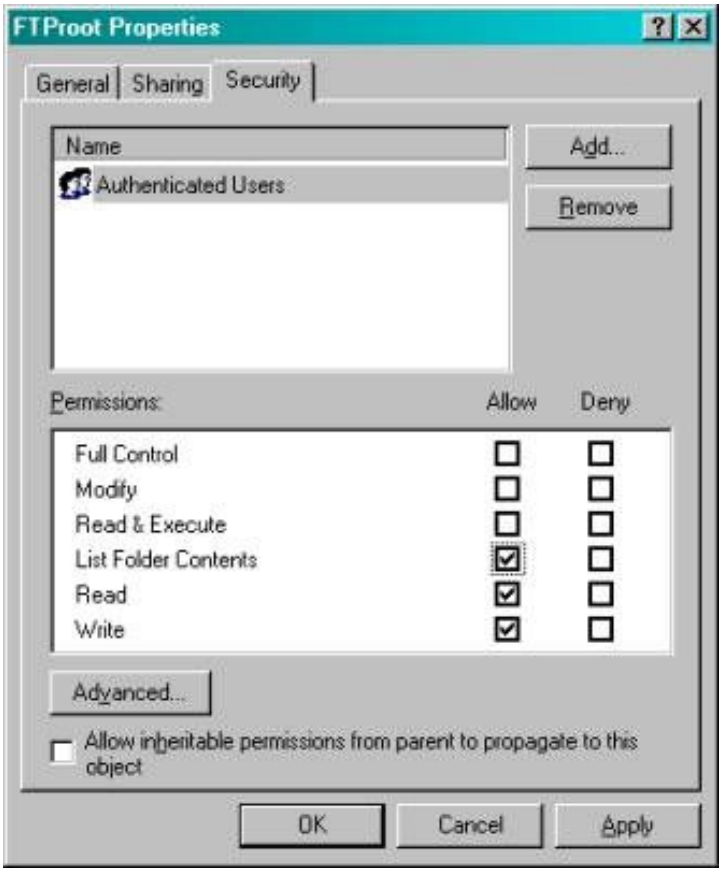
با فعال شدن گزارشگیری شما از اینکه چه کسانی با کدام آدرس شبکه (IP) به سایت شما دسترسی یافته اند آگاهی خواهید یافت . مرور گزارشها شما را قـادر مـی سـازد ترافیـک سـایت را تشـخیص داده و متوجـه تهدیـدهای امنیتـی و مشکلات شوید.



برای فعال ساختن گزارشگیری از FTP Site ، Enable Logging را در صفحه Property فعال سازید. بااین عمل فایل های گزارش با فرمت خاص قابل مرور شدن و تجزیه تحلیل خواهند بود.

۳- ACL را مقاوم سازید

برای تنظیم نه تنها لزوم دسترسی به FTP Directory با استفاده از محدودیت های موجود در ACL (در NTFS) و همچنین تنظیم آن است بلکه گروه های موجود در FTP باید از لحاظ حقوق و دسترسی تنظیم گردند.

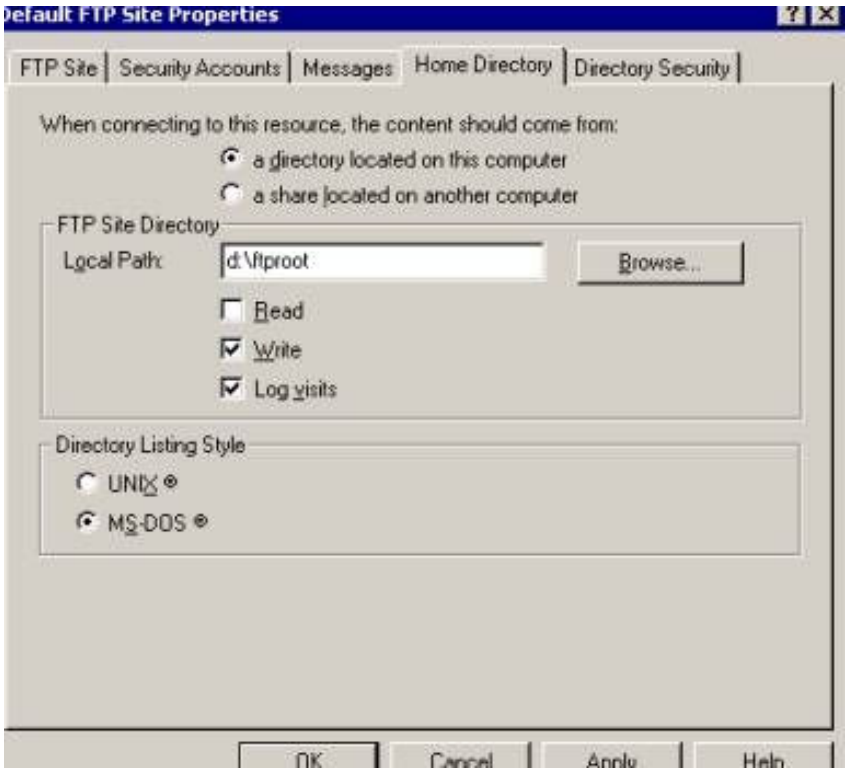


به عنوان مثال شما تنها می خواهید دسترسی Read,Write,List Folder را به این گروه بدهید بدون آنکه امکان اجرا (Execute) را فعال سازید لذا تنها سه گزینه فوق انتخاب می شود.

٤-FTP Site را بصورت یکطرفه (Blind Put) تنظیم نمایید.

اگر تنها انتقال اطلاعات به سرور مدنظر بوده و نیاز به برداشت فایل از آن نباشد (به عبارتی انتقال اطلاعات یکطرفه است) به این حالت اصطلاحا Blind Put گفته می شود. به عبارتی امکان نوشتن (Write) را دارا می باشد بدون آنکه توانایی خواندن داشته باشد.

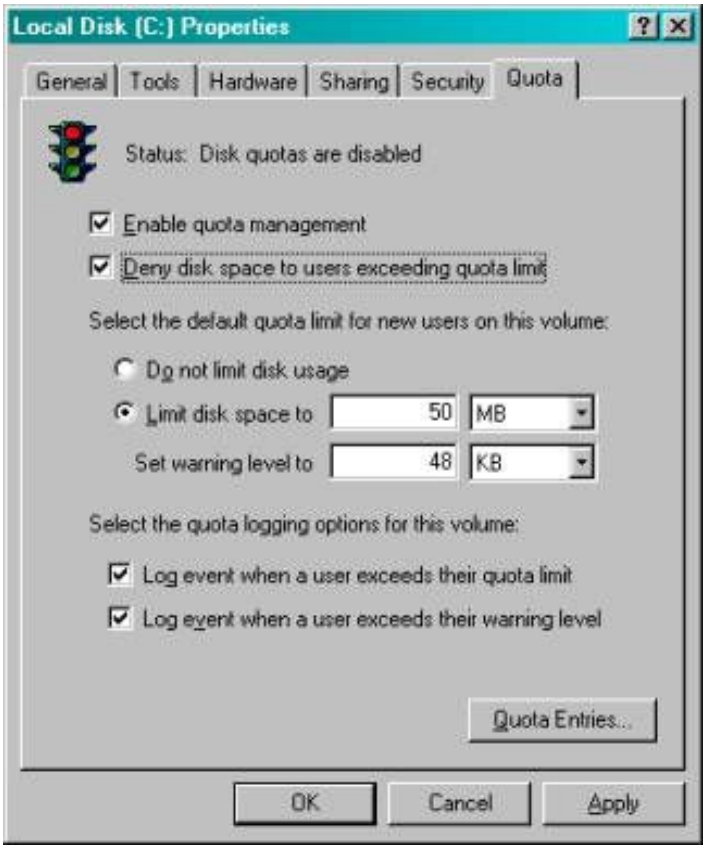
این روش یکی از روش های کنترلی برای در اختیار گرفتن دسترسی کاربران می باشد. تنظیم Blind Put در FTP Site و مجوزهای NTFS صورت می پذیرد.



شکل فوق روش حذف دسترسی خواندن رااز FTP Site نشان می دهد.

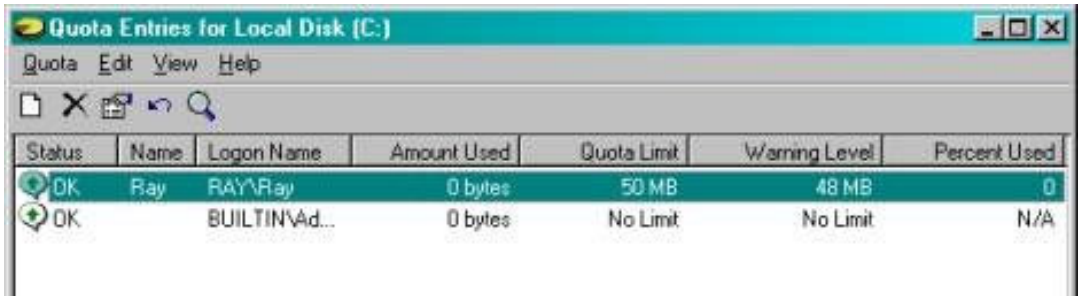
۵- فعال سازی ظرفیت حافظه مورد نیاز

Windows 2000 به همراه ابزاری دستی برای تخصیص فضای دیسک (Disk Quotas) به بازار آمد. Disk Quotas بطور مؤثر قادر به تخصیص مقدار مشخصی فضای حافظه به کاربری خاص می باشد. مقدار پیش فرض معادل فضای کل دیسک (Partition) است. با استفاده از این خاصیت شما قادر به کنترل و محدود کردن خطاهای احتمالی ناشی از کاربرها می باشید لذا سایت شما به سایتی غیر جذاب برای نفوذگران بدل خواهد شد.



جهت فعال سازی Quotas در Property پارتیشن NTFS قادر به انجام این مهم خواهید شد.

Quotas می تواند برای یک کاربر تنظیم شود و نمی تواند به یک گروه تخصیص یابد.



مدیریت Quota برای هر کاربر تنظیم می شود و محدودیت باید روی هر User Account برای دسترسی به FTP تنظیم گردد.

٦- محدودسازی زمان Logon

این خاصیت امکان دسترسی کاربران را تنها در ساعتهای خاص فراهم می آورد. در واقع با این کار دسترسی های مجاز کاربران را محدود به زمان می کنیم. به عنوان مثال اگر از FTP Site برای مقاصد کاری استفاده می کنید زمان دسترسی می تواند به زمان شروع و پایان کار محدود شود. با Deny کردن Logon بعد از ساعات کاری شما بطور مؤثری FTP Site خود را ایمن ساخته اید.

تنظیم مربوط به زمان Logon در Windows2000 در صفحه User Property واقع در Active Directory Users می باشد.

Net user <username> /times :

Local user account برای زمان Login در Local Users و Group Console امکان پذیر نیست لذا این خاصیت در GUI دسترس نمی باشد.

٧- محدود ساختن دسترسی توسط IP

FTP Site در Windows2000 قابلیت محدود شدن توسط آدرس IP را دارد. با محدود ساختن FTP Site بطور موثری قادر به کاهش دسترسی های غیر مجاز می باشید.

با محدود ساختن دسترسی به FTP توسط IP از Directory Security Tab در صفحات Properties واقع در FTP Site از انتخاب گزینه Default Denied Access مطمئن شوید که تنها IP های مجاز در لیست موجود باشد.

٨-کنترل وضعیت Loginها

با فعال شدن ثبت وقایع Auditing of account logon ، قادر به مرور Logonهای صحیح و غیر صحیح در قسمت Security Log خواهید شد.

مرور و نظارت مداوم به این گزارشها فعالیت افراد مخرب را که تلاش به رسوخ بدون مجوز به FTP Site را دارند فاش می نماید.

گزارش های مربوط به Audit Account Logon با فعال ساختن Local Security Policy قابل تنظیم شدن هستند.

۹- استفاده از کلمه عبور مناسب

استفاده از کلمه عبور مختلط تجربه خوبی برای بالابردن امنیت است.Windows2000 امکان داشتن کلمه عبور مناسب را برای کاربرها فراهم می آورد. با فعال سازی "Password must meet complexity Requirement" در Local Security Policy یا Group Policy، User Account ها در قالب خاصی محدود می شوند که از قوانین زیر تبعیت می کنند.

- نباید شامل کل یا قسمتی از نام Account کاربر شود.
- حداقل طول شش کاراکتر باشد.
- شامل ۳ کاراکتر از ۴ گروه حروف زیر باشد
- حروف بزرگ A تا Z
- حروف کوچک a تا z
- از رقمهای ۰ تا ۹ استفاده شود
- از علامتهای استفاده شود. (بطور مثال$,@ ,# , !)

نحوه تخصیص کلمه عبور در Local Security Policy Configuration فعال می شود.

۱۰- فعال سازی Account Lock Out و Account Lock Out Threshold

Account های FTP هدفهای جالبی برای نفوذ توسط برنامه های Crack هستند. Windows administrator Policy سرپرست شبکه را قادر به کنترل و قفل کردن Loginهایی می نماید که بعد از چندبار Fail شده اند . با فعال ساختن این خاصیت فعالیت نفوذگران سیستم را محدودتر می نماییم.

Account Lockout و تنظیم تعداد دفعات مجاز در Local Security Policy Configuration Tool قابل فعال شدن می باشد. به Local Policies/Account Policies/Password Policy رفته و تنظیم خود را انجام دهید.