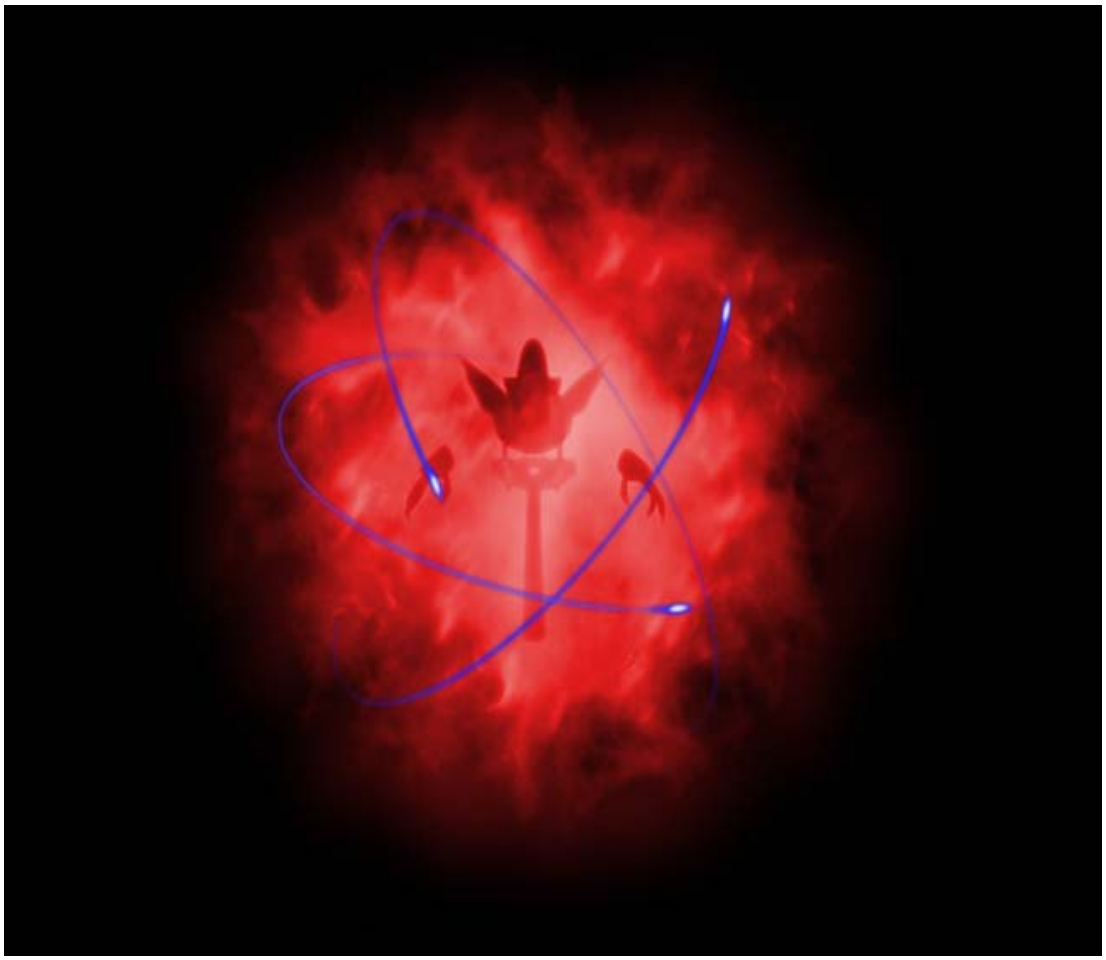
Breaking Firewalls



در هم کوبیدن دیوار آتش !!

نام و موضوع مقاله : در هم کوبیدن دیوار آتش !!

موضوع : ضد امنیت !! ، امنیت !! ، شبکه و امنیت شبکه .

نویسنده : امیر آشتیانی ..::ZXO003::..

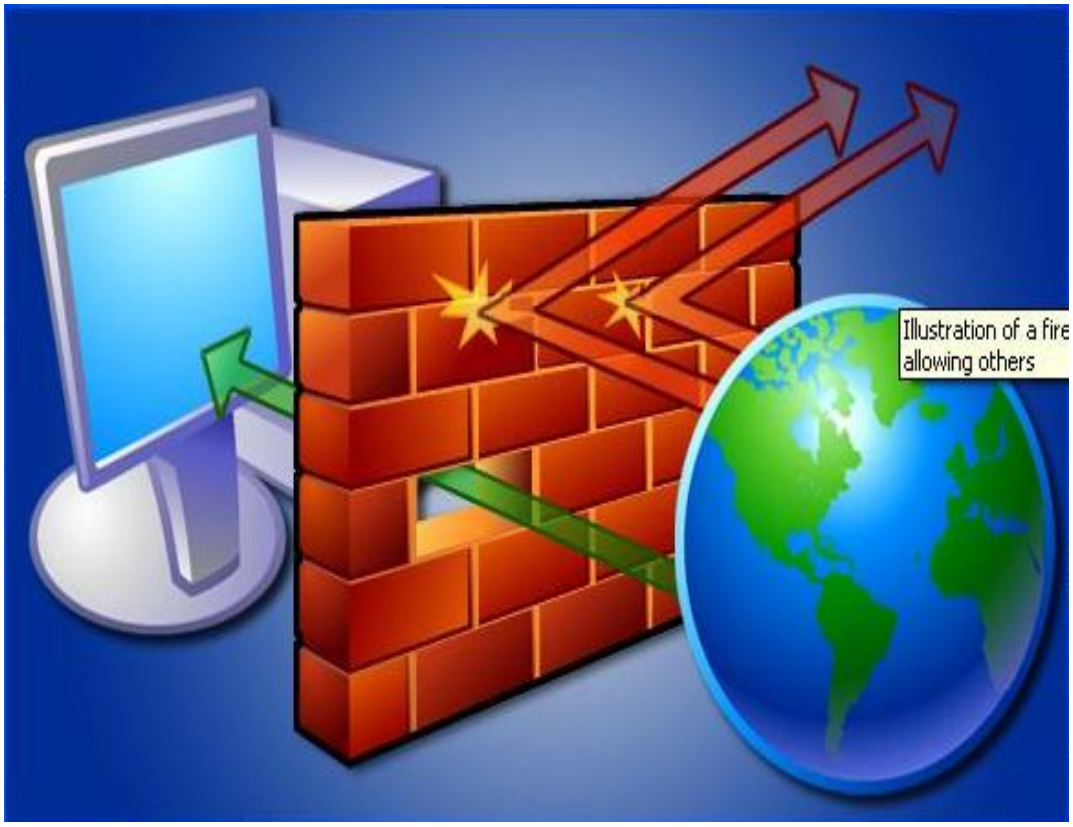
وبلاگ نویسنده :

http://blog.websecurity.ir/ & http://zxo003.blogfa.com/

پست الکترونیک { نامه برقی !! } :

zxo003@gmail.com & zxo003@noavar.com & ...

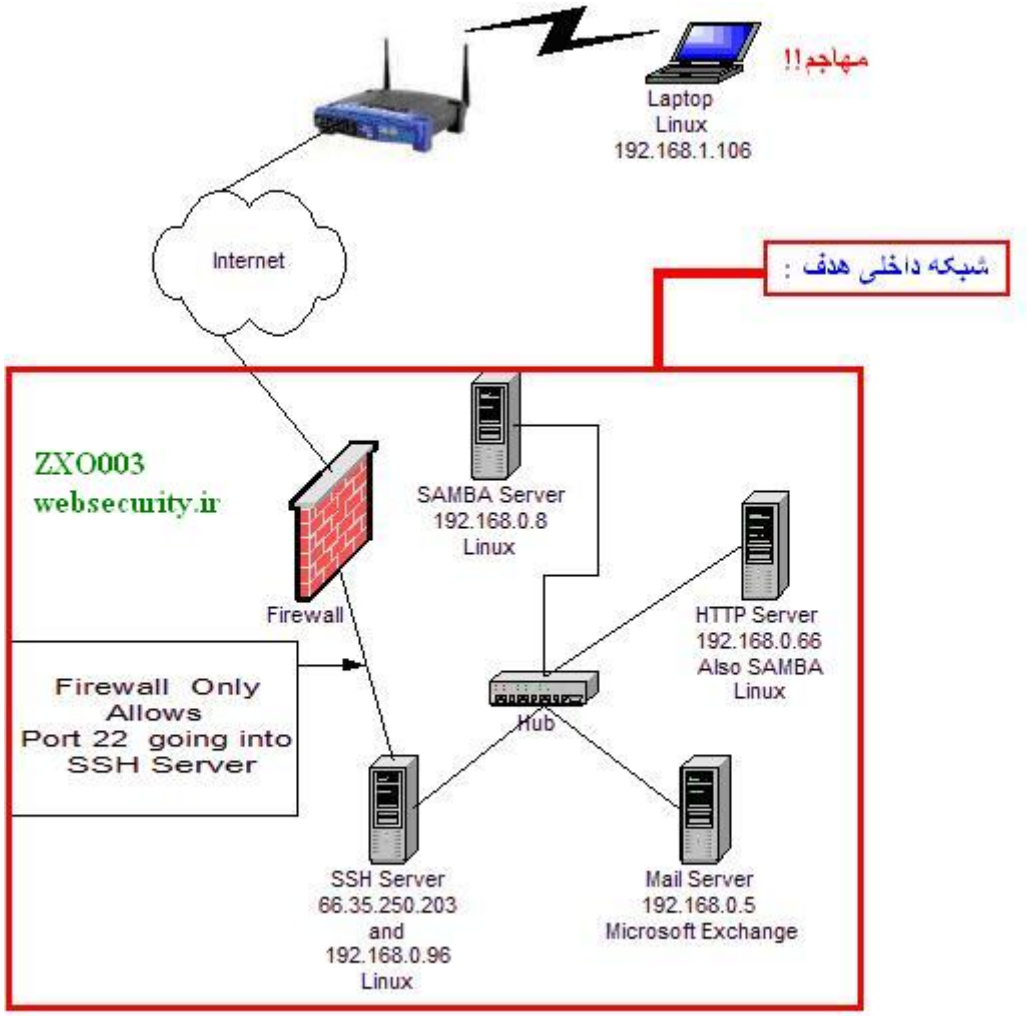
تاریخ آغاز و اتمام نگارش مقاله : ۱۳۸۴/۹/۲ تا ۱۳۸۴/۹/۴



مقدمه و شرح کلی مسئله :

بعضی مواقع پیش می آید که مدیر یک شبکه تصمیم می گیرد که برای بدست آوردن امنیت بیشتر و پیشگیری از کنجکاوی های بیش از حد کاربران دردسر ساز اینترنت (یا هر شبکه دیگری) !! تمام ترافیک ورودی از اینترنت (یا هر شبکه دیگری) به سوی شبکه داخلی را به سوی پورت ۲۲ از یک سرور خاص که توسط آن ارتباط با دنیای داخل شبکه برقرار میشود (که همان SSH است) هدایت کند . البته قبل از آن هم یک دیوار آتش جلوی هرگونه دسترسی مستقیم به داخل شبکه غیر از آن سرور خاص (SSH) را میگیرد !! که در این مواقع با توجه به سیاست سخت گیرانه مدیر شما احتمالا با محدودیت های بسیاری برخورد میکنید !! ما در این قسمت به راه حل این مشکل با توجه به نوع سیستم عامل میپردازیم ، تا مدیران از ایجاد چنین طرح های ابلهانه ای خود داری کنند و نه خود و نه ما را به زحمت بیندازند و به دنبال طراحی های امنیتی درست و کارا بروند !!

خوب ما اول یک راه حل ساده اما کاری را در ویندوز به اجرا در می آوریم و در قسمت دوم مقاله راه حلی برای لینوکس ارئه میکنیم . به شکل زیر توجه کنید ، نمای کلی مسئله :



« یک سیاست امنیتی ابلهانه !! »

خوب بعد از آشنا شدن با صورت کلی مسئله یا مشکل به ارایه راه حل میپردازیم البته در ویندوز !! برنامه های بسیار خوبی برای این کار نوشته شده است که ما فقط در اینجا به برنامه PuTTY اشاره میکنیم و از ان استفاده میکنیم ، قبل از هر چیز PuTTY را از اینجا دانلود کنید !! اگر دوست دارید plink را هم دانلود کنید (به دردتان خواهد خورد) !!

همانگونه کا در عکس بالا مشاهده کردید تنها راه ، استفاده از پورت ۲۲ برای دسترسی به میل سرور و سرویس دهنده وب و ... است ، به نظر شما ایجاد یک تونل ssh چطور است ؟

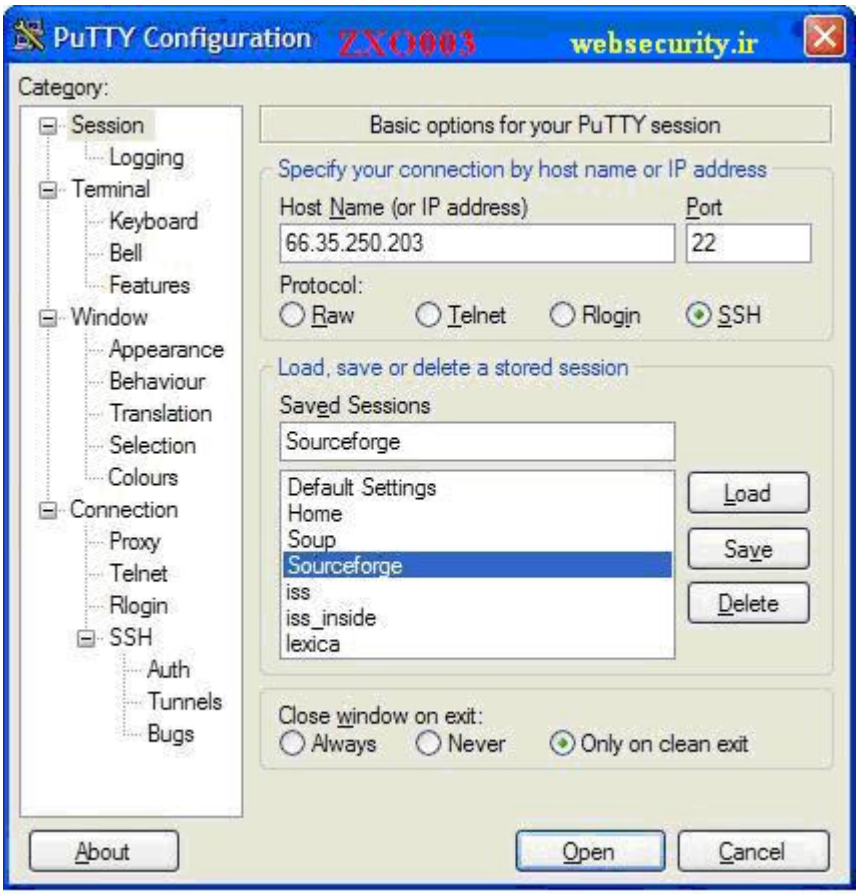
گذر از دیوار آتش و اتصال به سرویس دهنده ها .

۱. قدم اول (دریافت و نصب) »

قدم اول دانلود این دو ابزار است که گفتم از کجا دریافت کنید !! ابزار PuTTY را در درایوی که سیستم عامل را نصب کرده اید و در پوشه ای به نام bin قرار بدهید (البته این یک توصیه تجربی از من است) !!

۲. **قدم دوم** (پیکر بندی برنامه) »

به قسمت Session (نشست) بروید در اینجا شما مطابق شکل نام ssh Server یا شماره IP آن را بعلاوه پورت مورد استفاده این ماشین سرویس دهنده SSH به برنامه میدهید و در قسمت پروتکل ، پروتکل SSH را انتخاب نمایید ، در قسمت ... Load , save هم یک نام برای این عملیات انتخاب کنید ، تنظیمات خود را ذخیره کنید (تنظیمات را تا مرحله سوم انجام دهید و آنگاه در اینجا ذخیره کنید) البته ما نام Source forge را انتخاب کرده ایم ولی شما مختار هستید هر نام دل خواهی را انتخاب نمایید . دیگر تنظیمات را هم مشابه تصویر انتخاب نمایید .



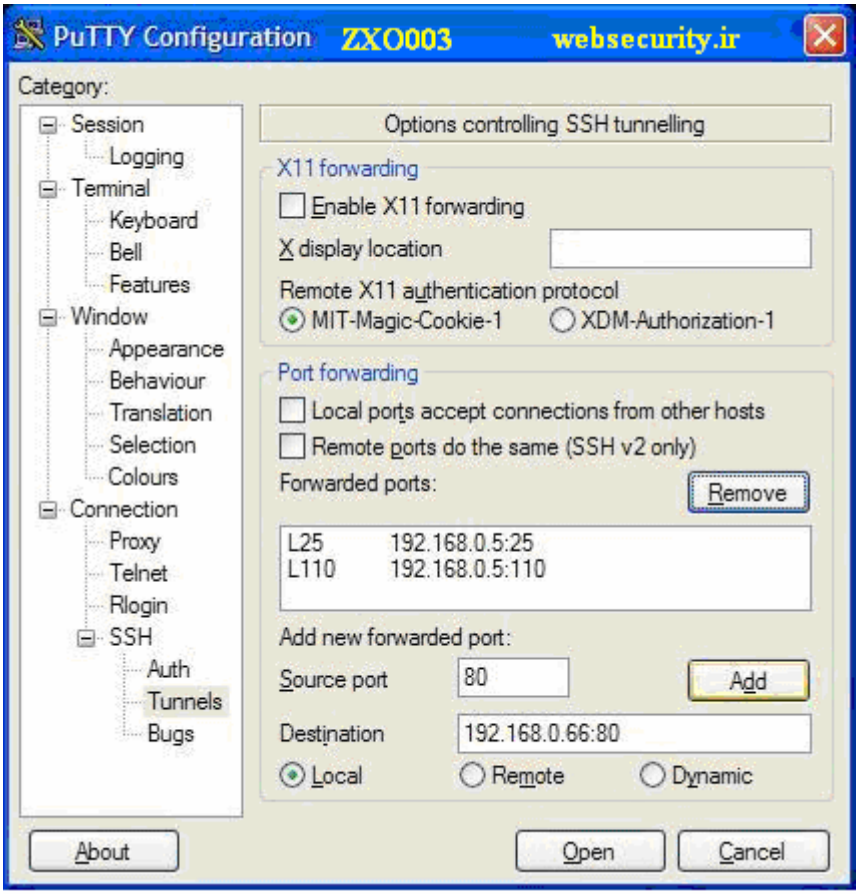
« مرحله دوم »

۳. **قدم سوم** (ایجاد تونل با سرویس دهنده های مورد نظر) »

در ستون سمت راست بر روی SSH کلید کنید و قسمت Tunnlels را انتخاب نمایید ، در این مرحله شما باید سرور های که میخواهید به آن ها دسترسی پیدا کنید باید به برنامه اضافه کنید . **همین جا بگم که شما برای هر سرویس دهنده باید کل مراحل را یک بار تکرار کنید .**

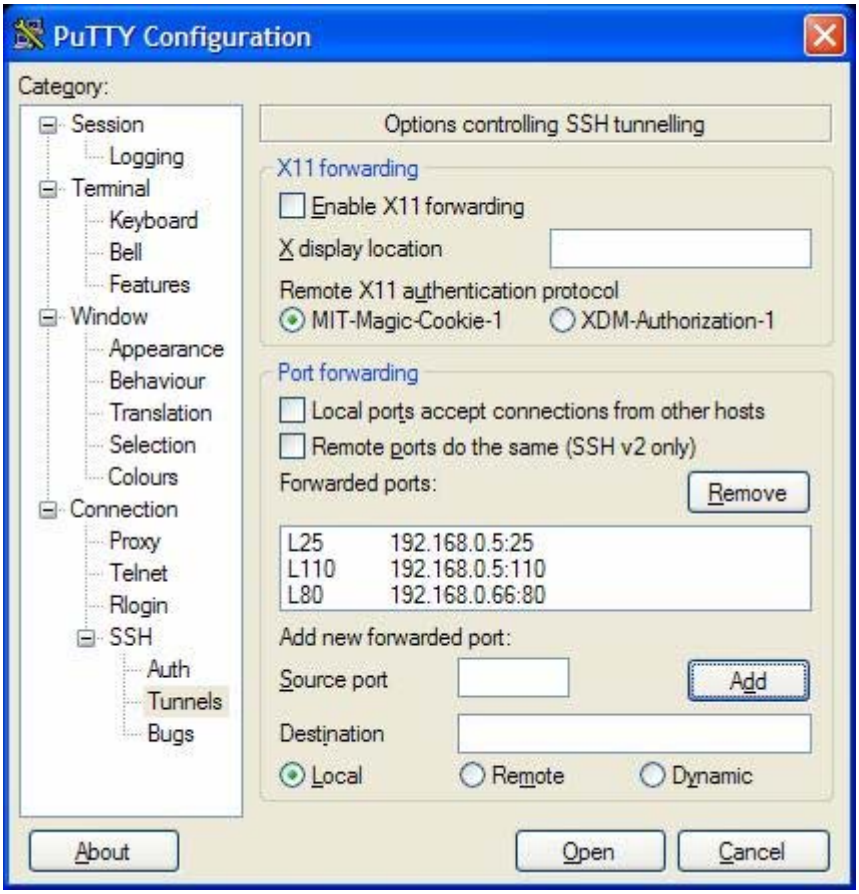
در فرضیات مسله ما سه تا سرویس دهنده داریم یکی از آنها را در اینجا در نظر میگیریم که میل سرور است که آن هم IP برابر با ۱۹۲,۱۶۸,۰,۵ دارد و شماره پورت آن هم ۱۱۰ است که برای POP3 استاندارد است ولی چون یک پورت استاندارد دیگر هم SMTP دارد که استفاده میشود و آن هم پورت ۲۵ است که آن را نیز وارد میکنیم و بعد شماره IP و پورت سرویس دهنده وب را هم وارد میکنیم . آن یکی سرویس دهنده (SAMBA) را جدا توضیح میدهم به علت یک سری خورده کاری ها !!

راستی شما شماره پورت مبدا (پورتی که روی سیستم شما باز میشود برای راه اندازی تونل) را در قسمت Source port می نویسید و بعد در قسمت destination (مقصد) شماره IP بعلاوه شماره پورتی که آن سرویس دهنده از آن استفاده میکند مشخص میکنیم . در آخر کار هم باید روی دکمه Add کلید می کنید تا تنظیمات شما ثبت شود !! (قابل ذکر است در نسخ جدید برنامه بخش X11 به صورت جداگانه در یک قسمت مجزا قرار دارد و با این شکل اندکی تفاوت دارد !!)



« مرحله سوم »

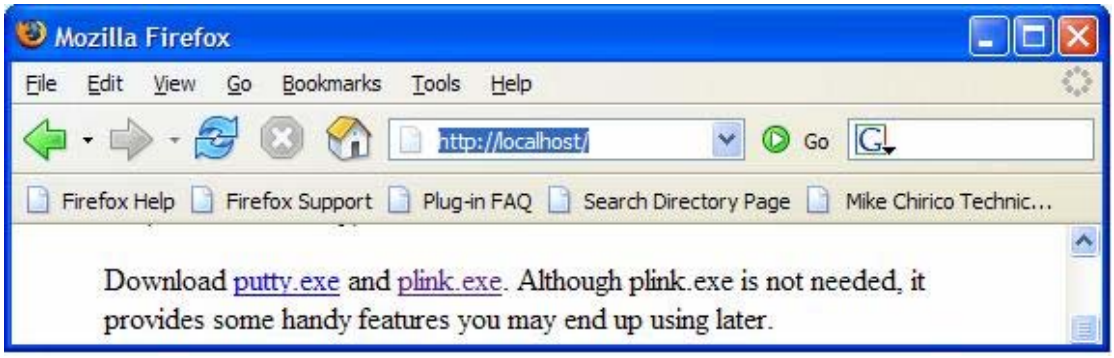
توجه کنید که لیست باید همانند این شرح باشد !! باید قبل از هر سطر کلمه L درج شده باشد که به معنی این است که در سیستم شما مثلا پورت ۲۵ باز شده و در حال قصد کردن به پورت ۲۵ از میل سرور است و به همچنین برای موارد دیگر ....



« تصویر نهایی مرحله سوم »

۴. قدم چهارم (امتحان و اتصال) »

اگر حالا شما اتصال را که در مراحل قبل ایجاد کرده اید و با نام دل خواهی (Sourceforge) ذخیره کرده اید انتخاب کنید و روی دکمه Open کلید کنید میتوانید بدون دیوار آتش به آن سرویس دهنده ها اتصال بیابید . برای مشاهده اطلاعات سرویس دهنده وب کافی است یک مرورگر اینترنت مثل Fire fox را اجرا کنید و در نوار آدرس آن عبارت Local host را بنویسید . حال میتوانید به آن دسترسی یابید !! به شکل زیر توجه کنید :

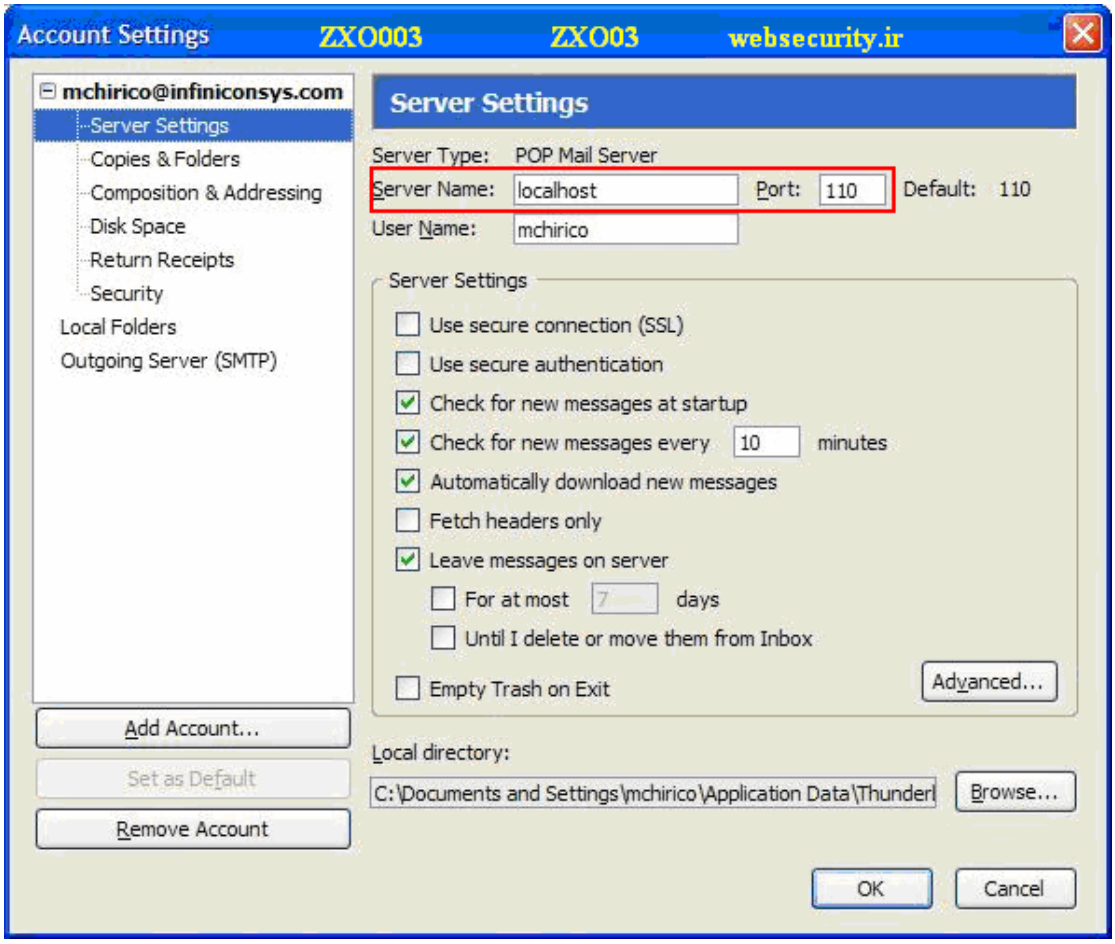


« مرحله چهارم »

۵. قدم پنجم (اتصال به سرویس دهنده پست الکترونیک) »

شما حتما متوجه شدید که برای اتصال به سرویس دهنده چاپار برقی E-Mail هم باید مثل مرحله قبل تنظیمات را اندکی تغییر بدهیم ، ون من از بیلی و محصولات آن بدم می اید یک برنامه معروف و کار درست از رقیبش به نام Thunderbird را به شما معرفی میکنم ، و پیکربندی

ها را با توجه به این ابزار به پیش میبریم ، البته به حد توصیه میکنم شما از این ابزار به جای هر ابزار دیگری برای این کار استفاده کنید ، البته شیوه کلی همه یک جور است و شما هم میتوانید از Outlook Express ه استفاده کنید ولی من خوشم نمیاید از آن ، بگذریم !! شما از هر برنامه ای که استفاده می کنید باید تنظیمات آن را به Local host باید تغییر بدهید !! (البته فرض کلی مسئله در ای است که این سرویس دهنده وب POP3 را به شما ارئه بدهد) ، به قسمت پیکربندی Account وارد شوید و Server Name را به طور مناسبی تغییر بدهید البته شما میتوانید به جای عبارت Localhost شماره IP معدل آن که عبارت است از ۱۲۷,۰,۰,۱ را استفاده کنید که توصیه نمیکنم !! حال کار تمام است لذت ببرید .....



« مرحله پنجم »

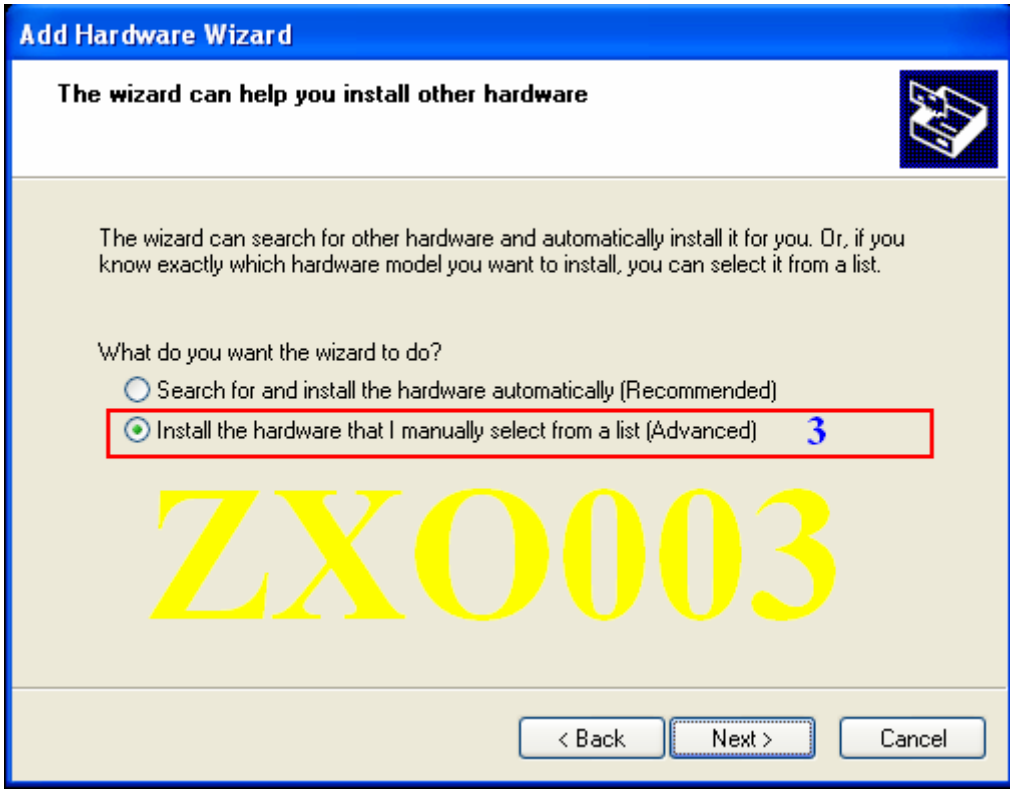
۶. قدم ششم (دسترسی به SAMBA با استفاده از آداپتور Loop back) »

خوب برای اینکه در ویندوز XP به توانیم به Share ها دست رسی پیدا کنیم باید Loopback را باید نصب کنیم ، که بدین منظور به control panel میرویم و بعد Add Hardware را اجرا میکنید بعد آنگاه روی Next میزنید

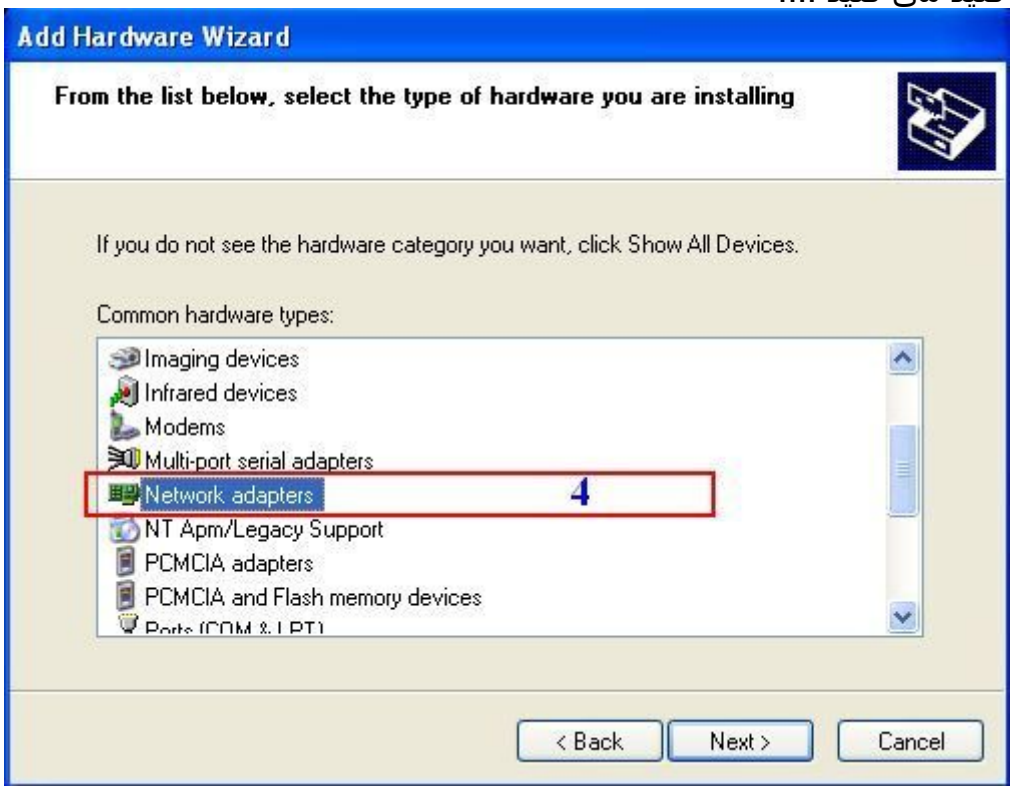
۱- بیلی یک خورده ای با خودش کلنجار میرود یک سوال میکنه و دو تا جواب را به شما میده !! که شما Yes, I already connected the hardware را انتخاب میکنید و دوباره روی Next کلید می کنید ...

۲- بعد از این انتخاب یک منو به شما نمایش میدهد که شما از آن منو آخرین گزینه که نوشته Add a new hardware device را انتخاب میکنید و دوباره Next را میزنید ...

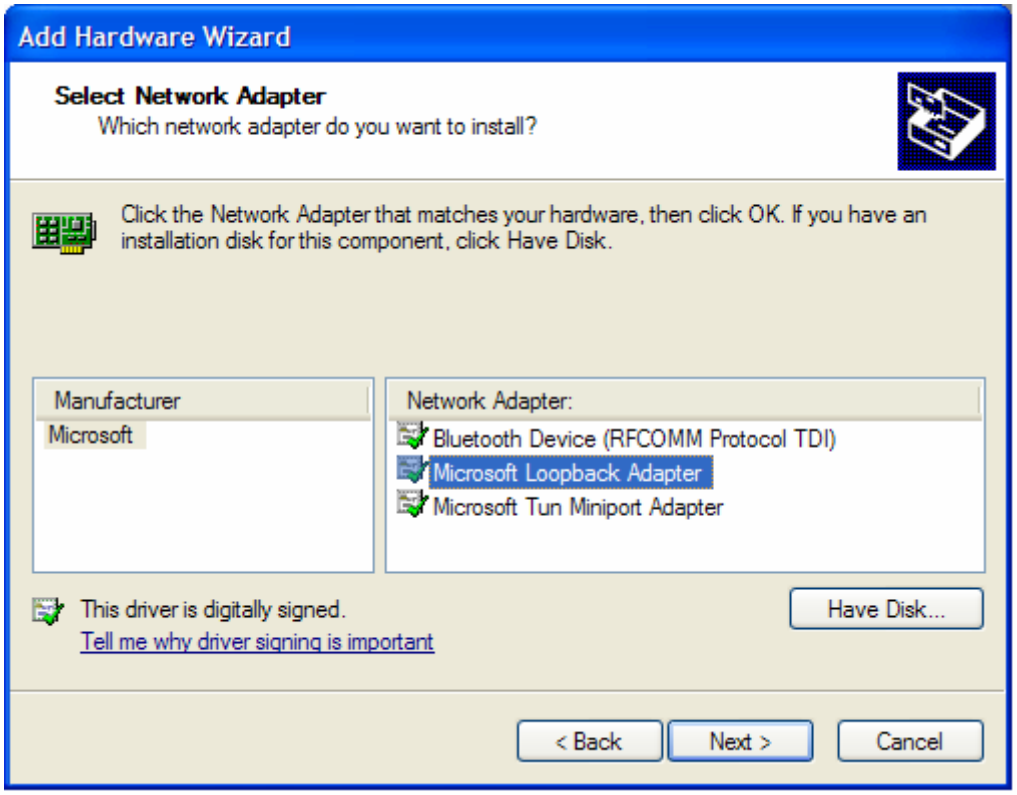
۳- در این مرحله شما گزینه ای را که خودش پیشنهاد نمی کند را انتخاب میکنید !!! یعنی : Install the hardware that I manually select from a list (Advanced) و بروی دکمه Next کلید می کنید ....



۴- سپس از منوی که دوباره می آید Network Adapters را انتخاب میکنید و بر روی Next کلید می کنید ....



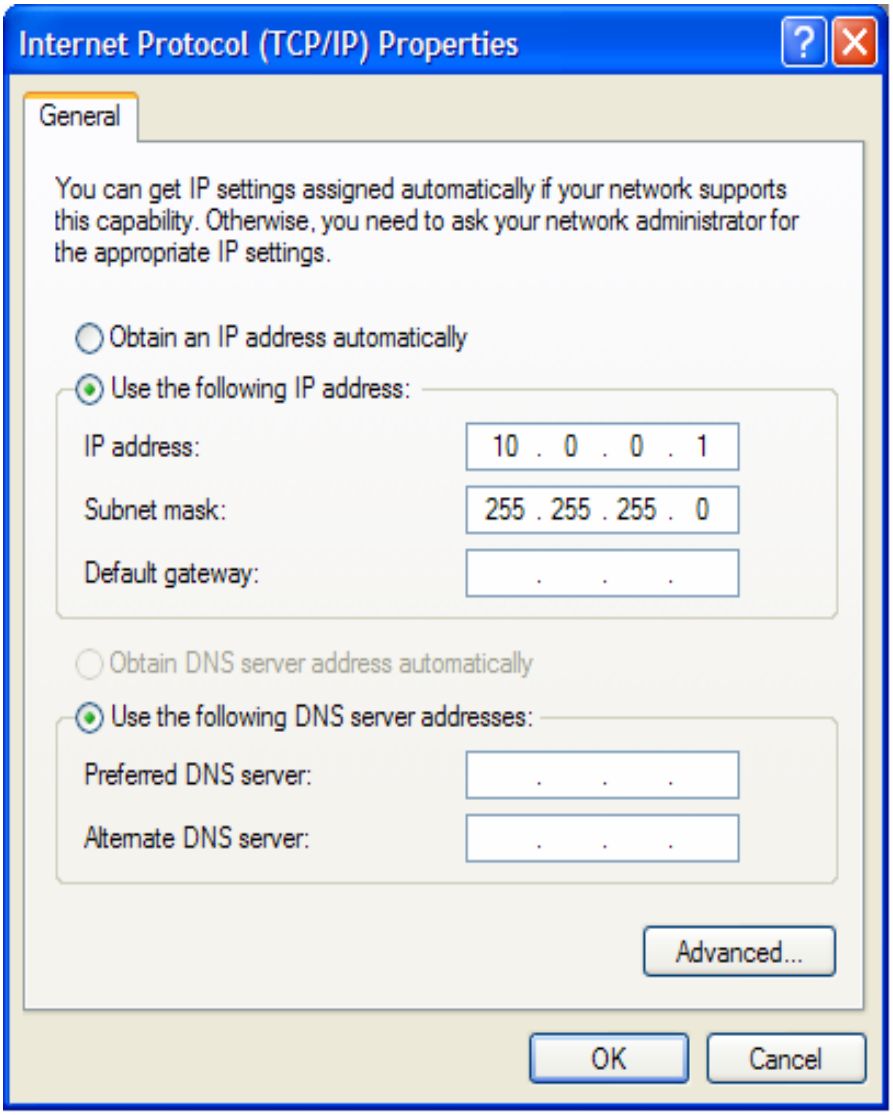
۵- در این قسمت گزینه Microsoft Loopback Adapter را انتخاب کرده و روی Next کلید می کنید ....



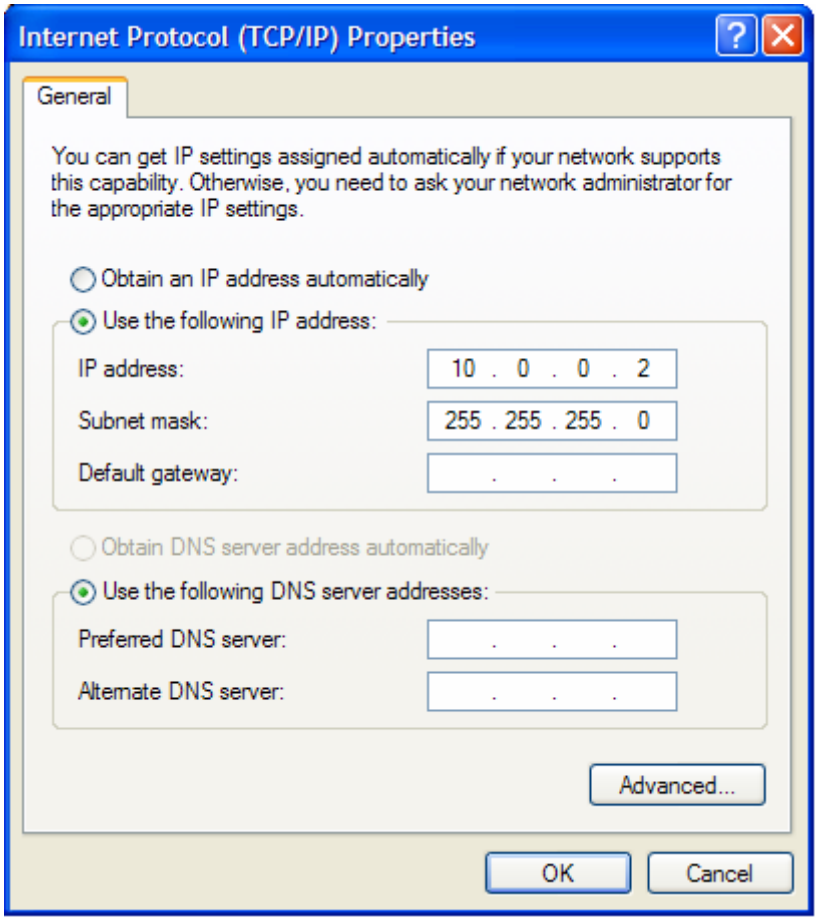
دقت کنید که فقط همین آداپتور را باید نصب کنید نه چیزی دیگر را (این کار را دو بار انجام میدهید)، البته شما نیاز دارید که آن را پیکر بندی کنید و به هیچ وجه از Default gateway استفاده نکنید . بعد از این که نصب را کامل شد کنار ساعت ویندوز تصویر آیکون " دو تا کامپیوتر " را مشاهده میکنید !

در این موقع به control panel ویندوز دوباره برمیگردیم و به قسمت Network Connections ، در این جا دو اتصال جدیدی را که ایجاد کرده اید مشاهده میکنید !! از آن Properties میگیرید و در بخش General گزینه Internet Protocol را انتخاب میکنید و بر روی دکمه Properties موجود در آن صفحه کلید میکنید . حال شما باید به این دو آداپتور یک آدرس IP اختصاص بدهید ، من برای اولین کارت آدرس ۱۰,۰,۰,۱ و برای دومین ۱۰,۰,۰,۲ و به همین ترتیب برای بقیه آدرس اختصاص میدهم برای ماسک شبکه هم که مشخص است .

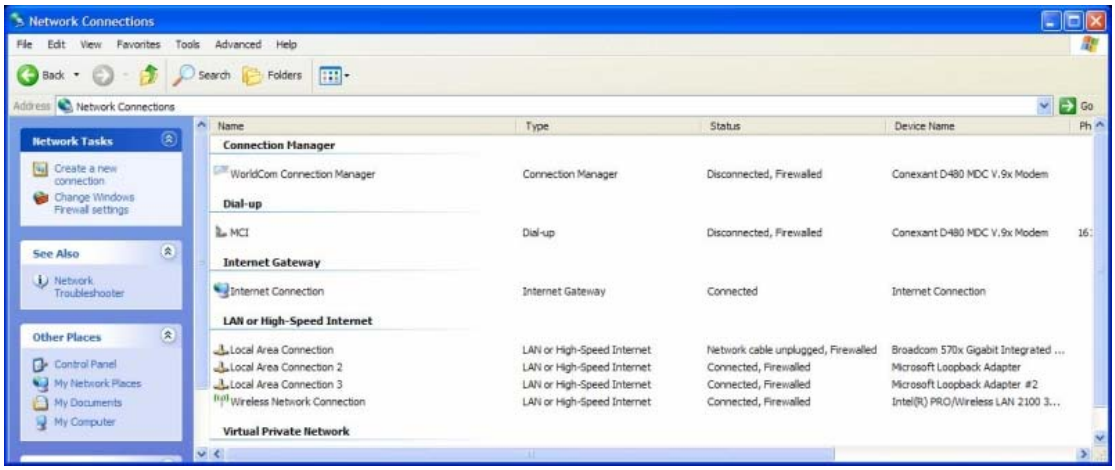
لازم به ذکر است که به هیچ وجه هیچ چیزی برای Default gateway وارد نکنید !! به شکل زیر توجه کنید :



دومین آداپتور را همانگونه که گفتم IP معادل با ۱۰,۰,۰,۲ قرار میدهیم ...



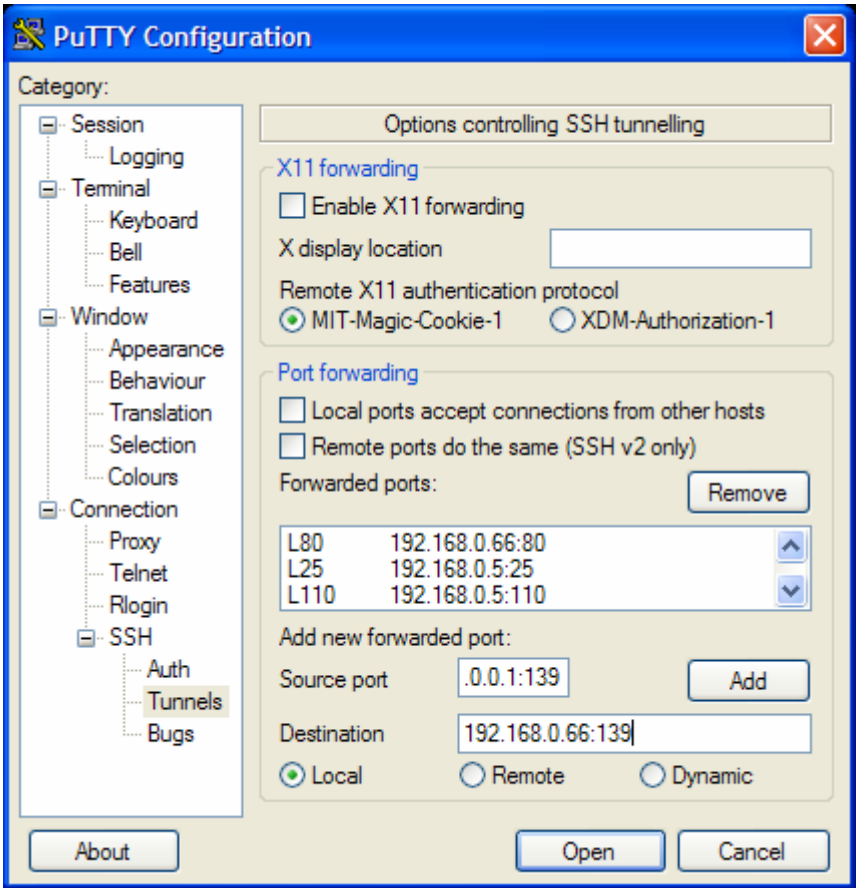
دو آداپتوری که شما نصب کردید در Network Connections باید به این صورت باشند :



۷. **قدم هفتم** (دسترسی به Samba و تنظیم پیکربندی SSH) »

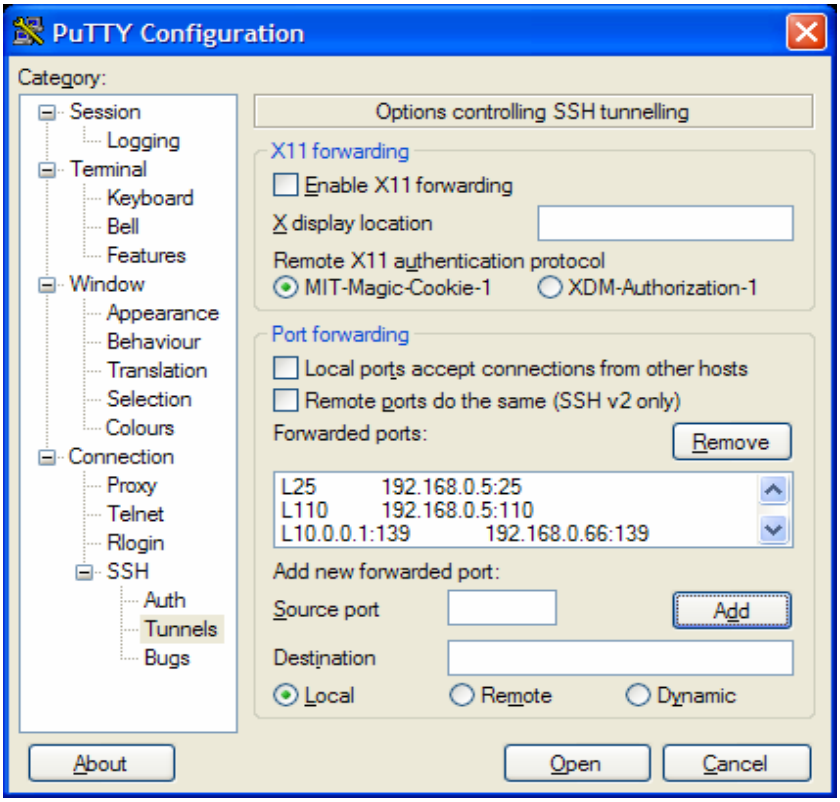
خوب حالا بر میگردیم به ابزار مان (PuTTY) و پیکربندی آن را برای کار با این تنظیمات اصلاح میکنیم !! به **قدم سوم** بر میگردیم (امیدوارم یادتان مانده باشد) در قسمت Source port چون ما یک کارت شبکه را پیکر بندی کردیم و به آن یک IP اختصاص دادیم (دیگر اینجا Localhost نیست) ، پس مینویسیم ۱۰,۰,۰,۱:۱۳۹ ، بعد در قسمت destination (که باید مقصد را مشخص کنیم) همان سیستمی را که میخواهیم به آن متصل بشویم مینویسیم بعلاوه شماره

پورت آن که در اینجا ۱۹۲,۱۶۸,۰,۶۶:۱۳۹ است و در آخر هم روی دکمه Add کلید میکنید تا این اطلاعات وارد شود . (بهتر است آن را ذخیره نیز بکنید) .



« در این تصویر نوشته های Source port کامل نیست که دلیل آن بزرگتر بودن عبارت از اندازه BOX است »

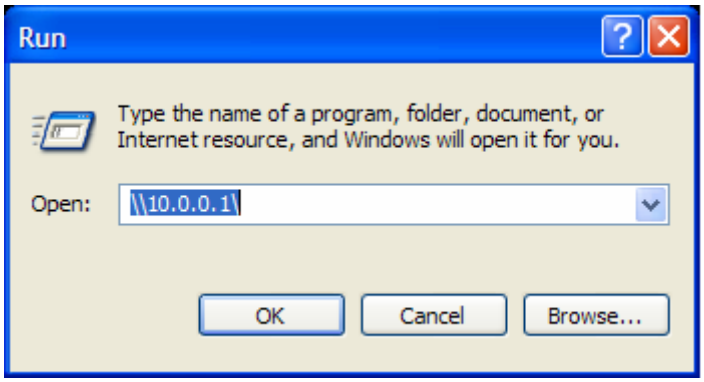
بعد از کلید کردن بر روی دکمه Add یک همچین تصویر داریم :



« تصویر نهایی قدم هفتم »

۸. قدم هشتم (دسترسی به Samba و مشاهده نتیجه) **»**

برای مشاهده فایل های Share میتوانید در باکس Run بنویسید \\10.0.0.1\ ، حال به آنچه خواسته بودید دسترسی پیدا کردید ...



- **نکات مهم :**

اگر با انجام این کار سیستم شما ریستارت شد !! و یا File and Printer Sharing از کار افتاد در شبکه بدانید که این از دسته گل های بیلی است ، البته میتوانید بسته اصلاحی بیلی را از اینجا دریافت کنید !!

اگر NetBIOS over TCP/IP پکید مطمئن بشوید که LMHosts فعال است !! قابل ذکر است که این ابزار قابلیت ها بسیاری دارد و لی ما در این مقاله فقط به آنچه که نیاز داشتیم (حداقل ها) پرداختیم شما با کمی پشتکار به تمام این قابلیت ها و قابلیت های ترکیبی این برنامه مسلط خواهید شد !!

Amir Ashtiani

Mr. Amir Hossein Sharifi
info@Websecurity.ir

..::ZXO003::..

For More Information visit : Zxo003.blogfa.com ; Blog.websecurity.ir

White Hat Nomads : Breaking Firewalls : Bay ZoXO003