چهار شنبه 19 فروردین 1388 - 11:26

IP و Port چیست وچگونه آنها را بدست بیاوریم؟

IP چیست ؟

هر کامپیوتر در اینترنت با یک IP شناسایی می شود که نمای ظاهری آن به صورت A.A.A.A است که بجای هر یک از این A ها عددی بین صفر تا 255 قرار می گیرد. بسته به اینکه چه عددی باشد موقعیت جغرافیایی (شهر(ISP اینترنت شما تعیین می شود. منظور از ISP همان شرکتی است که به شما خدمات اینترنت ارائه می نماید. اکنون به یک IP توجه کنید:

69.147.102.73

عدد 69 مربوط به ISP می شود. و عدد 73 مربوط به شخص کاربر می شود. در هر شبکه ، چه اینترنت باشد و چه چند کامپیوتر به صورت مدار بسته (Share) به هم متصل باشند برای هر یک از آنها باید یک IP Address تعریف شود که سایر کامپیوتر ها طبق آن IP آن کامپیوتر را پیدا و به آن وصل شوند.

اینترنت چندین سرویس خاص دارد. همان طور که می دانید DialUp اینترنت کم سرعت و ADSLاینترنت پر سرعت سرویس های اینترنتی رایج هستند. کسانی که Modem آن ها به صورت شماره گیر ار طریق سرویس DialUp به اینترنت متصل می شود در هر بار وصل شدن به اینترنت عدد سمت راست IP آنها عوض نمی شود. مثلا اگر در مثالی که زده شد در این اتصال به اینترنت ، شماره سمت راست IP کاربر 73 است در اتصال بعدی عدد دیگری است مثلاً 69. اما کسانی که Modem آنها ویژه اتصال به اینترنت پر سرعت است (ADSL) در هر بار که سیستم را ShutDown می کنند و مدتی مودم را از برق خارج می سازند یکبار عدد سمت راست IP آن ها عوض می شود. بدیهی است که DialUp کمی خطرناک است. زیرا Hacker ها که عموماً از طریق IP به سیستم قربانی حمله می کنند به چنین سرویس های اینترنتی که IP آنها در طول ماه ثابت است راحت تر نفوذ می کنند. برای اینکه متوجه شوید IP شما چیست می توانید بدین روش عمل کنید:

هنگامی که به اینترنت متصل هستید به منوی Start رفته و گزینه Run را کلیک کنید. در پنجره باز شده تایپ کنید: cmd و سپس Enter را بزنید. پنجره مشکی رنگی باز می شود. در آن تایپ کنید: ipconfig و سپس Enter کنید. با یک سری اطلاعات مواجه می شوید که می توانید در مقابل عبارت IP Address شماره IP خود را بخوانید.

بدست آوردن IP دیگران بدون نیاز به برنامه

اگر در چت روم با شخصی در حال چت کردن هستید از او بخواهید یک فایل(عکس) برای شما بفرستد در هنگام دانلود فایل به منوی start رفته و بر روی گزینه run کلیک کنید ودر کادر باز شده (دستور Cmd را تایپ کنید) یک صفحه مانند داس برای شما باز می شود که مانند دستور روبرو عمل کنید:

C:\>netstat -n

تایپ کنید می بینید در دو ردیف به شما تعدادی شماره نشان خواهد داد که در ردیف اول IP خود شماست ودر ردیف دوم IP طرف مقابل است . البته این هم گفته باشم که بعضی از آن شماره ها IP سایتها یست که باز کردیت . در بخش آموزش نرم افزارها روش های ساده تری را آموزش می دهم.

بدست آوردن IP سایت

برای بد ست اوردن ip سایت می توانیم در همان command prampt از دستور ping استفاده کنیم مانند مثال اگر بخواهیم ip سایت yahoo را پیدا کنیم مانند دستور زیر عمل می کنیم.

C:\> ping tebyan-tabriz.ir می بینید که براحتی IP سایت تبیان تبریز را به شما نشان خواهد داد.

Portچیست ؟

در ساده ترین تعریف، محلی است که داده‌ها وارد یا خارج می‌شوند. در مبحث هک معمولا با پورت‌های نرم‌افزاری سروکار داریم که به هر کدام عددی نسبت می‌دهیم. این اعداد بین ۱ و ۶۵۵۳۵ هستند. معمولا به یک سری از پورت‌ها کار خاصی را نسبت می‌دهند و بقیه به‌صورت پیش‌فرض برای استفاده شما هستند. پورت‌های که فعال هستند، هرکدام توسط یک نرم‌افزار خاص مدیریت می‌شوند. مثلا پورت ۲۵ برای ارسال Email است، بنابراین باید توسط یک نرم‌افزار این کار انجام شود و این نرم‌افزار بر روی پورت ۲۵ منتظر (فال‌گوش) می‌ماند. اینجا ممکن است شخصی از فلان نرم‌افزار و دیگری از بهمان نرم‌افزار استفاده کند ولی به‌هر حال پورت ۲۵ همیشه برای ارسال Email است.

روش بدست اوردن پورتهای باز :

شما میتوانید با استفاده از IPeye و داشتن IP طرف مقابل پورتهای باز آن سیستم را پیدا کنید ابتدا وارد Cmd شده و مسیر IPeye را فعال کنید یعنی اینکه اگر IPeye درون درایوی C: وجود دارد ابتدا وارد درایو C: شده ودستور زیر را تایپ کنید. مثال میخواهیم پورتهای باز این ip10.0.0.50 را بدست بیا وریم.

C:\>ipeye 10.0.0.50 -syn -p 1 2000

این دستور از پورت ۱ تا ۲۰۰۰ را scan می کند وبه شما نشان می دهد که کدام پورت باز و کدام بسته است.

TCP/IP چیست؟

برنامه نویسان برای تضمین این‌که انواع متفاوتی از کامپیوترها بتوانند با یکدیگر کارکنند، برنامه‌های خود را با استفاده از پروتکل‌های استاندارد می‌نویسند. پروتکل مجموعه‌ای از قوانین است که با اصطلاحات فنی چگونگی انجام گرفتن کاری را توصیف می‌کند. به عنوان مثال، پروتکلی وجود دارد که به طور دقیق قالبی را که بایستی برای ارسال پیام‌های پستی استفاده شود، توضیح می‌دهد. تمام برنامه‌های پستی اینترنت در هنگام آماده ساختن پیامی برای تحویل از این پروتکل پیروی می‌کنند.
TCP/IP نام متداولی برای مجموعه‌اي بیش از ۱۰۰ پروتکل می‌باشد که برای متصل ساختن کامپیوترها و شبکه‌ها استفاده می‌شود. نام واقعی TCP/IP از دو پروتکل مهم می‌آید:

۱) TCP(Transmission Control Protocol)

۲) IP(Internet Protocol)

در داخل اینترنت، اطلاعات به صورت جریان ثابتی از میزبان به میزبان(کامپیوترهایی که با هم ارتباط دارند) منتقل نمی‌شود. در عوض، داده‌ها به بسته‌های کوچکی به نام بسته(packet) شکسته می‌شوند.
به عنوان مثال، در نظر بگیرید که پیامی پستی را برای دوستی در اینترنت می‌فرستید. TCP آن را به تعدادی بسته تقسیم خواهد کرد. هر بسته با شماره سریال ، نشانی گیرنده و نشانی فرستنده علامت گذاری می‌شود. TCP اطلاعات مربوط به کنترل خطا را نیز در بسته درج می‌کند.
سپس بسته‌ها از طریق شبکه فرستاده می‌شوند، در اینجا کار IP است که آنها را به میزبان راه دور منتقل کند. TCP در انتهای دیگر، بسته‌ها را دریافت و وجود خطاها را بررسی می‌کند.اگر خطایی رخ داده‌باشد، TCP می‌تواند درخواست ارسال مجدد این بسته به خصوص را نماید.
بعد ازاین‌که تمام بسته‌ها دریافت شدند،TCP از شماره سریال بسته‌ها، آنها را به ترتیب به هم وصل می‌کند تا پیام پستی اصلی در طرف دوم ساخته شود.
به عبارت دیگر ، کار IP گرفتن داده‌های خام-بسته‌ها- از یک مکان به مکان دیگر است و کار TCP اداره جریان و تضمین صحت داده‌ها می‌باشد.
شکستن داده‌ها به بسته‌ها فواید مهم بسیاری دارد. اول این‌کهبه اینترنت اجازه می‌دهد در یک زمان از همان خطوط ارتباطی برای کاربران متفاوت بسیاری استفاده کند. از آن‌جایی که بسته‌ها مجبور نیستند با یکدیگر سفر کنند، خط ارتباطی می‌تواند تمام انواع بسته‌ها را همان‌طوری که در راه خود از مکانی به مکان دیگر می‌روندؤ حمل کند. بزرگراهی را در نظر بگیرید که در آن ماشینهای مجزا با وجود اینکه مقصدهای متفاوتی دارند، همگی در راه مشترکی سفر می‌کنند.
همان‌طوری که بسته‌ها سفر می‌کنند، تا زمانی که به مقصد نهایی خودشان برسند، از میزبانی به میزبان دیگر فرستاده می‌شوند(مسیر واقعی توسط کامپیوترهایی با استفاده خاص به نام مسیریابانتخاب می‌شود). این این موضوع یعنی اینترنت دارای انعطاف‌پذیری بسیار زیادی می‌باشد. اگر اتصال به‌خصوصی خراب شود، کامپیوترهایی که جریان داده را کنترل می‌کنند می‌توانند معمولاً مسیر جایگزینی را پیدا کنند. در حقیقت امکان دارد که در داخل انتقال واحدی از داده‌ها، بسته‌های مختلف در مسیرهای مختلفی به یک مقصد جریان پیدا کنند.
همچنین شبکه می‌تواند از بهترین مسیر در شرایط مختلف استفاده کند. به عنوان مثال، هنگامی که بار بخشی از حد متعارف می‌شود بسته‌ها می‌توانند از طریق خطوطی که بار کمتری دارند، فرستاده شوند.
مزیت دیگر استفاده از بسته‌ها این است که در هنگام رخ‌دادن خطایی کوچک در انتقال، به جای انتقال کل پیام فقط نیاز به ارسال مجدد بسته‌ای منفرد خواهد بود. این مزیت سرعت کلی اینترنت را افزایش می‌دهد.
تمام این انعطاف‌پذیری کمک می‌کند تا قابیت اطمینان بالا امکان‌پذیر شود، TCP/IP به هر صورت تضمین می‌کند که داده با موفقیت عبور می‌نماید. در حقیقت، حتی با وجود این‌که ممکن است میزبانها صدها کیلومتر دور از یکدیگر باشند و تمام بسته‌ها مجبور به عبور از چندین کامپیوتر میانی باشند، اینترنت آن‌قدر خوب عمل می‌کند که ارسال پرونده‌ای از یک میزبان به میزبان دیگر فقط چند ثانیه طول می‌کشد.
بنابراین دو جواب برای «TCP/IP چیست؟» وجود دارد. جواب فنی این است که TCP/IP خانواده‌ای بزرگ از پروتکل‌هایی است که برای سازمان‌دهی کامپیوترها و ابزارهای ارتباطی در شبکه، استفاده می‌شوند. و مهمترین پروتکل‌های آن TCP و IP هستند. IP داده‌ها را از مکانی به مکان دیگر منتقل می‌کند، در حالی که TCP از صورت‌گرفتن صحیح تمام کارها مطمئن می‌شود.
با وجود این، بهترین پاسخ این است که اینترنت وابسته به هزاران شبکه و میلیونها کامپیوتر است، و TCP/IP چسبی است که این شبکه‌ها و کامپیوترها را در کنار یکدیگر نگه می‌دارد.

تهیه و تنظیم : امیر محمد زارع مجتهدي
کارشناس فناوري اطلاعات اداره کل تبلیغات اسلامي