بسم الله الرحمن الرحیم

بخش چهارم مبانی علم رایانه

موضوع : شبکه ی جهانی اینترنت

تهیه کنندگان:

مجید گلی

محمدرضا محمدی

حسین نیکبخت

نشانی پروتکل اینترنت

نشانی پروتکل اینترنت (به انگلیسی: Internet Protocol Address) یا به اختصار **نشانی آی‌پی** (به انگلیسی: IP Address) نشانی عددی است که به هریک از دستگاه ها و رایانه‌های متصل به شبکهٔ رایانه ای که بر مبنای نمایه TCP/IP (از جمله اینترنت) کار می‌کند، اختصاص داده می‌شوند.
پیام‌هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانهٔ عددی همراه است و راه یاب های شبکه آن را مانند «نشانی گیرنده» در نامه‌های پستی تعبیر می‌کنند، تا بالاخره پیام به رابط شبکه رایانه مورد نظر برسد.

انواع آی‌پی

دو نسخه آی‌پی درحال استفاده می باشد : آی‌پی نسخه ۴ و آی‌پی نسخه ۶ که هر یک نشانی آی‌پی را به روش متفاوتی ارائه می نمایند.

نشانی آی‌پی نسخهٔ ۴

نشانی آی‌پی نسخهٔ چهارم یک عدد ۳۲ بیتی است که برای سادگی آن را به شکل چهار بخش عددی در مبنای ده می‌نویسند که با نقطه از هم جدا می‌شوند (مانند ۱۹۹,۲۱۱,۴۵,۵). این روش نشانی‌دهی را دهدهی نقطه‌دار می‌نامند هر یک از چهار بخش را یک هشتایی (Octet) می‌گویند زیرا طول آن ۸ بیت (یا ۱ بایت) است و می‌تواند عددی از ۰ تا ۲۵۵ باشد. پس ۲ به توان ۳۲ آدرس مختلف داریم.

اصولاً هر نشانی آی‌پی ۳۲ بیتی به دو بخش تقسیم می‌شود: یک پیشوند و یک پسوند. این دو سطح به منظور ایجاد یک روش مسیریابی کارآمد طراحی شده است. پیشوند آدرس، شبکه‌ای را که رایانه به آن متصل است مشخص می‌کند (Network) در حالیکه پسوند یک رایانهٔ یکتا را روی شبکه مشخص می‌کند(Host). یعنی به هر شبکه در اینترنت یک مقدار یگانه که تحت عنوان شمارهٔ شبکه شناخته شده است، اختصاص دارد. شمارهٔ شبکه به عنوان یک پیشوند در نشانی هر رایانه‌ای که به شبکه وصل است ظاهر می‌شود. بعلاوه به هر رایانهٔ روی یک شبکه، یک پسوند نشانی یکتا تخصیص یافته است.

هر نشانی کامل، شامل یک پیشوند و یک پسوند است و طوری تخصیص داده می‌شوند که یکتا باشند، بنابراین ویژگی اول تضمین می‌گردد. اگر دو رایانه به دو شبکهٔ مختلف وصل شده باشند، نشانی‌هایشان پیشوندهای متفاوت خواهند داشت. اما اگر دو رایانه به یک شبکه وصل باشند، نشانی‌هایشان دارای پسوندهای متفاوت خواهد بود.

کلاس‌های مختلف آی‌پی نسخهٔ ۴

سه کلاسِ پایه‌ایِ مختلفِ نشانی‌دهیِ آی‌پی، برای شبکه‌های بزرگ، متوسط و کوچک وجود دارد.
کلاس A برای شبکه‌های بزرگ، کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک است. علاوه بر این سه کلاس، کلاس D برای پخش چندگانه، ارسال اطلاعات به گروهی از رایانه‌ها،

و کلاس E برای کارهای جستجو وجود دارند. برای شرکت در پخش چندگانهٔ آی‌پی، مجموعه‌ای از رایانه‌های میزبان باید بر سر استفاده از آدرس پخش چندگانه، به طور مشترک توافق داشته باشند. پس از تشکیل گروه پخش چندگانه یک کپی از هر بستهٔ اطلاعاتی فرستاده شده به نشانی پخش چندگانه به هر رایانهٔ میزبان در مجموعه تحویل می‌گیرد. بنابراین نخستین ۴ بیت (از سمت چپ) آدرس IP کلاس آن را مشخص می‌کند. همچنین اگر نمایش نقطه‌دار را در نظر بگیریم از روی مقدار دهدهی بایت اول کلاس آن تشخیص داده می‌شود

کلاس	شروع	پایان
Class A	0.0.0.0	127.255.255.255
Class B	128.0.0.0	191.255.255.255
Class C	192.0.0.0	223.255.255.255
Class D	224.0.0.0	239.255.255.255
Class E	240.0.0.0	255.255.255.255

اصولاً در سامانهٔ آی‌پی‌دهی به مشترکان، آی‌پی‌ها به صورت تعدادی که توانی از عدد ۲ باشد (۲، ۴، ۸، ۱۶، ۳۲، ۶۴ و ۱۲۸) دسته‌بندی می‌شوند. لازم به ذکر است که در هر دستهٔ آی‌پی اختصاص داده شده به مشترک آی‌پی‌های اول و آخر بر اساس استاندارد معمولاً غیر قابل استفاده است و از باقیماندهٔ آی‌پی‌ها می‌توان در شبکهٔ محصورشده استفاده کرد. به عنوان مثال در یک کلاس هشت‌تایی، حداکثر شش نشانی آی‌پی قابل استفاده است.

آی‌پی ایستا و پویا

آی‌پی پویا با هر بار وصل‌شدن به شبکهٔ داخلی و یا اینترنت تغییر می‌کند. اما آی‌پی ایستا (Static) اینطور نیست. آی‌پی پویا (Dynamic) در هر شبکه توسط کارساز پروتکل پیکربندی پویای میزبان (DHCP Server) به رایانه‌ها در شبکه اختصاص داده می‌شود. یعنی وقتی شما به اینترنت و یا شبکهٔ داخلی وصل می‌شوید، کارساز پروتکل پیکربندی پویای میزبان به شما یک نشانی آی‌پی اختصاص می‌دهد.

آی پی نسخهٔ ۶

گسترش روز افزون اینترنت و نیاز به آدرس های بسیار بیشتر تیم Internet Engineering Task Force را برآن داشت تا به فکر تکنولوژی های جدیدی باشند تا امکان تعریف آدرس های آی پی بیشتری فرآهم گردد. بهترین راه ساخت مجدد نشانی پروتکل اینترنت بود . در سال ۱۹۹۵ میلادی نسخه جدید نشانی پروتکل اینترنت با نام آی پی نسخه ۶ معرفی گردید . اندازه آدرس از ۳۲ بیت به ۱۲۸ بیت افزایش یافت وامکان آدرس دهی تا ۲به توان ۱۲۸ آدرس افزایش یافت. این کار تنها تعداد آدرس های اینترنتی را گسترش نداد، بلکه باعث خواهد شد جدول مسیریاب های اینترنتی (روترها) کوچکتر شود . کلیه سیستم‌عامل‌های جدید سرور و خانگی از جمله ویندوز ویستا به طور کامل پشیبانی می‌شود ولی متاسفانه هنوز توسط بسیاری از مسیریاب های شبکه های خانگی و تجهیزات شبکه عادی پشتیبانی نشده است.

۹ راه برای حفاظت از اطلاعات در برابر هکرها

۱. استفاده از فایروال

هکرهایی که دسترسی مستقیم به کامپیوتر شما ندارند، از طریق ارتباط اینترنتی به سیستم شما نفوذ می کنند. یکی از راه های ورود آنها استفاده از پورت های شبکه ای باز است. فایروال همه ترافیک اینترنتی شما را که در طول پورت های شبکه ای وجود دارند، در هر دو حالت ورودی و خروجی کنترل می کند. این نرم افزار همچون یک دربان عمل می کند و به کاربر اجازه می دهد تا انتخاب کند کدام برنامه، اطلاعات را دریافت یا ارسال کند.

ویندوز به صورت پیش فرض فایروالی ابتدایی دارد. در ویندوز ۷ می توانید با رفتن به استارت، کنترل پنل و سپس قسمت System and Security فایروال دستگاه را با انتخاب Windows Firewall پیدا کنید. نرم افزاری که به شما کمک می کند تا فایروال خود را مدیریت و کنترل کنید، Windows 7 Firewall Control است.

البته باید توجه داشته باشید که فایروال‌های پیشرفته تری را نیز در اینترنت می توانید پیدا و به جای فایروال پیش فرض ویندوز از آنها استفاده کنید. فایروال های دیگر امکانات بیشتر و پیشرفته تری نیز دارند.

۲. امنیت شبکه

اگر فردی به شبکه کامپیوتری شما دسترسی داشته باشد می تواند به ترافیک شبکه شما نفوذ کند و به اطلاعات حساس و محرمانه شما دسترسی پیدا کند. به همین دلیل بسیار مهم و ضروری است که تنظیمات روتر را از حالت پیش فرض تغییر دهید و برای شبکه وای‌فای خود رمز عبور تعیین کنید.

۳. استفاده از نرم افزار ضد بدافزار

احتمالا ساده ترین راه برای هکرها به منظور نفوذ به سیستم یک کاربر، استفاده از نصب نرم افزارهای مخرب یا نصب شده توسط کاربران ساده و بی تجربه است. در برخی موارد، کاربر حتی به تایید چیزی نیاز ندارد زیرا به محض اینکه فایل موردنظر توسط کاربر باز شد جاسوس افزار به طور خودکار اجرا می شود و خودش را نصب و راه اندازی می کند. به همین دلیل داشتن یک نرم افزار امنیتی برای محافظت از امنیت سیستم بسیار لازم و ضروری است. نرم افزارهای ضد بدافزار، هر گونه فعالیت مخربی که در کامپیوتر صورت می گیرد را ردیابی و متوقف می کنند.

۴. کار کردن با حساب های کاربری استاندارد یا محدود شده

بیشتر کاربران تمایل دارند تا از اکانت Administrator استفاده کنند زیرا استفاده راحت تری دارد. شما به راحتی می توانید بدون نیاز به سوئیچ کردن بین اکانت ها یا اجرای یک فایل نصب با قوانین Administrator، یک برنامه را نصب و راه اندازی کنید. می دانید این کار تا چه اندازه مورد استقبال هکرهاست؟

ویندوز ۷ و ویستا امنیت بیشتری دارند زیرا هنگامی که برنامه ای می خواهد در سیستم تغییری ایجاد کند، این سیستم‌عامل ها به تایید یا اطلاعات لاگین نیاز دارند. اگر از کاربران ویندوز XP هستید، اکانت پیش فرض خود را یک اکانت غیر ادمین تعیین کنید. شما در این حالت نیز می توانید کارهای سیستم را به عنوان Administrator از اکانت مذکور اجرا کنید.

همچنین برای حساب کاربری ادمین رمز عبور تعیین کنید. بیشتر اوقات حساب کاربری ادمینستریتور رمز عبور ندارد. به این معنا که به راحتی می توان به سیستم نفوذ کرد. بنابراین، بهتر است کامپیوتر را قفل کنید.

۵. استفاده از رمزهای بسیار قوی و تغییر هر چند وقت یک بار آنها

شاید بتوان گفت تنها راه برای محافظت از حساب های کاربری آنلاین همچون ایمیل یا حساب های بانکی، استفاده از رمزهای عبور بسیار قوی است. باید از رمزهایی استفاده کنید که به راحتی نتوان آنها را پیدا کرد. برای هر کدام از حساب های کاربری نیز رمزی جداگانه باید در نظر گرفت. همچنین باید توجه داشته باشید که هر چند وقت یک بار رمز عبور خود را تغییر بدهید. شاید این تغییرات مداوم چندان جالب به نظر نرسد و مشکل باشد ولی برای حفظ امنیت اطلاعات فردی و حساس حساب های بانکی باید این سختی را بر خود هموار کرد.

۶. رمزگذاری اطلاعات حساس

هنگامی که اطلاعات بسیار حساس را روی هارد درایو یا هارد اکسترنال خود ذخیره می کنید، حتما آن را رمزدار کنید. به این ترتیب دسترسی به آن دشوار می شود. حتی زمانیکه یک هکر به سیستم کامپیوتری شما نفوذ می کند نیز اگر اطلاعات رمزگذاری شده باشند دسترسی به آنها برایش مشکل خواهد بود. یکی از بهترین ابزارهای رایگان و منبع باز برای رمزگذاری اطلاعات، TrueCrypt است.

۷. استفاده از اتصال امن برای ارسال اطلاعات

استفاده از اینترنت برای انجام یک سری امور بسیار مناسب است. ساختن یک حساب کاربری جدید، جالب و آسان است، به راحتی می توان از فروشگاه های اینترنتی خرید کرد، برای سفر خود برنامه ریزی کرد یا در بحث های آنلاین شرکت کرد.

هنگام استفاده از هر کدام از این سرویس ها، بخشی از اطلاعات شخصی خود همچون نام، نشانی، علاقه مندی های شخصی و جزئیات حساب بانکی را فاش می کنید. لطفا در نظر داشته باشید که این اطلاعات بسیار ارزشمند هستند.

برای محافظت از اطلاعات شخصی هنگام استفاده از سرویس های اینترنتی، اطمینان حاصل کنید که اطلاعاتتان را در طول اتصال امن رمزگذاری شده (SSL/TLS protocol) ارسال و دریافت می کنید. استفاده از یو.آر.ال https:// به جای http://. بسیار مطمئن تر و امن تر است. در حال حاضر می توانید برای دسترسی به بسیاری از سرویس های مهم از ارتباط امن HTTPS استفاده کنید که امنیت بالایی دارد.

۸. به روزرسانی سیستم‌عامل و نرم افزارها

بیشتر برنامه ها، باگ و حفره های امنیتی دارند. برای بر طرف کردن باگ ها، برنامه نویس ها آپدیت هایی برای به روز رسانی نرم افزارها می نویسند. آپدیت کردن سیستم‌عامل، درایورها و نرم افزارهای نصب شده حتی اگر قابلیت جدیدی به آنها اضافه نکند این مزیت را دارد که سیستم شما را تا به طور قابل توجهی در برابر بدافزارهای اینترنتی محافظت می کند.

۹. پاک کردن و بازنویسی روی حافظه های داخلی و خارجی

پیش از هر گونه اقدامی در رابطه با تعویض یا تغییر ابزارهای ذخیره سازی اطلاعات همچون هارد درایوها، یواس‌بی فلش ها، کارت حافظه یا دی‌وی‌دی، ابتدا همه اطلاعات موجود روی آنها را پاک کنید و برای اطمینان، دوباره روی آنها اطلاعات بی ارزشی ذخیره کنید و دوباره پاک کنید. به این ترتیب دیگر امکان بازگرداندن اطلاعات دستگاه های ذخیره سازی بسیار اندک است. فقط پاک کردن اطلاعات از روی هارد ضامن امنیت اطلاعات نیست. باید برای اطمینان حتما فضای ذخیره را با اطلاعات متفرقه پر کنید. اگر هم اطلاعات حساسی دارید که حذف دقیق آنها برایتان اهمیت دارد این مطلب نگهبان را در مورد پاک کردن امن اطلاعات از دست ندهید.