به نام او که هر چه دارم از اوست

DNS چیست ؟

DNS مخفف Domain Name System می باشد. ارتباط با server DNS به طور پیش فرض از طریق پورت ۵۳ ، برقرار می گردد و hostname ها به آدرسهای IP تبدیل می شوند و برعکس. قبل از DNS سیستم تبدیل نام به آدرس دیگری وجود داشت اما DNS ، جهت تکثیر آسان جدول میزبان (host table)ایجاد شد.به خاطر سپردن یک hostname بسیار راحت تر از به خاطر سپردن ۴ رقم می باشد. همان طور که احتمالا می دانید DomainName System بسیار پیچیده است. کتابهای زیادی در این رابطه نوشته شده است اما در اینجا سعی شده است خلاصه ای از DNS شرح داده شود.سیستم تبدیل نام به آدرسی که قبل از DNS استفاده می شد ، شامل فایلی به نام) host file فایل میزبان بود .این فایل حاوی جدولی از hostname ها و آدرسIP متناظر با آنها بود که توسط Stanford Research Institute's SRI-NIC(Network Information Center) ایجاد شده بود -SRI .

NICچندین بار در هفته این جدول را با افزودن hostname های جدید ، به روز می رساند و مدیران سیستم نیز جدول خود را با گرفتن جدول SRI-NIC از طریق FTP ، به روز می رساند ند. این سیستم تا مدت زیادی کارا بود اما به مرور زمان با گسترش سریع شبکه ، دیگر این سیستم کارا نبود وبدلیل اینکه به پایداری شبکه اهمیت زیادی داده می شد، نیاز به سیستمی جدید احساس می شد. در واقع نیاز به یک سیستم غیر متمرکز احساس می شد DNS .این نیاز را برآورده کرد DNS .غیر متمرکز است ، در واقع یک بانک اطلاعاتی توزیع شده می باشد که بر روی هر سروری قرار دارد و هر server DNSی می داند که کجا به دنبال اطلاعات مورد نیاز خود بگردد.(در صورتی که آن اطلاعات را در جدول محلی خود در اختیار نداشته باشد.) یک server DNS کامپیوتری

دارای سیستم عامل Unix و یا مشابه آن می باشد بنابراین معمولا از یک برنامه Unixبه نام BIND (Berkeley Internet Name Domain) استفاده می کند. برنامه های مشابهی برای ویندوز و مکینتاش نیز وجود دارد اما اکثر مردم Unix serverها را بیشتر ترجیح می دهند چرا که استوارتر بوده و قابلیت ذخیره حجم اطلاعات بالایی را دارند. یک برنامه DNS از دو قسمت تشکیل شده است : خود) name server برنامه daemon که از طریق پورت ۵۳ عمل می کند.) و جز دیگری به نام name server . resolver به درخواست مرورگرها (browsers) برای دریافت نام ، پاسخ می دهد. به عنوان مثال اگر شخصی پنجره مرورگری مانند Internet Explorer را باز کرده و www.securitywriters.org را تایپ می کند ، مرورگر از نزدیکترین server DNS (server DNSمثلا server DNS موجود در ISP خود) ، آدرس IP این hostnameرا درخواست می کند چرا که به این آدرس جهت یافتن سرور این سایت و در نتیجه نمایش این سایت نیاز دارد .DNS daemon در جدولهای محلی خود به دنبال این آدرس می گردد و در صورتی که آدرس IP متناظر را پیدا نکرد به resolver رجوع می کند تا از server DNS سطح بالاتر خود آدرس متناظر را درخواست کند. پس هر گاه server DNS محلی نتوانست آدرس IP متناظر با یک hostname را پیدا کند از server DNS سطح بالاتر خود آدرس متناظر را درخواست می کند و اگر پیدا نکرد از server DNSیک سطح بالاتر، آدرس متناظر را درخواست می کند و به همین ترتیب (به شکل یک درخت) ادامه می دهد تا آدرس متناظر پیدا شود. پس با یک درخت مواجهیم . این درخت به چه شکلی می باشد ؟

به مثال زیر توجه کنید:

فرض کنید ISP شما isp.co.uk است. طبیعتا DNS server's hostname مربوط به ISP شما ، dns.isp.co.ukخواهد بود. حالا فرض کنید که از dns.isp.co.ukآدرس IP مربوط به www.somehost.com را

درخواست کرده اید dns.isp.co.uk .چک خواهد کرد (در جدول محلی اش) که آیا کس دیگری این آدرس را درخواست کرده و این آدرس در حافظه اش وجود دارد یا نه. در صورتی که نتوانست آدرس را پیدا کند از DNS server سطح بالاتر خود ، co.ukپرس و جو می کند. این DNS server هر hostnameزیرشاخه co.uk را در بردارد که البته ممکن است IP یا www.somehost.com را نیز در بر داشته باشد چرا که ممکن است شخص دیگری تاکنون آن را درخواست کرده باشد. در صورتی که IP موردنظر در جدولهای محلیش موجود نبود از DNS server سطح بالاتر خود ، uk، پرس و جو می کند uk .دربرگیرنده تمام زیرشاخه هایuk. (از قبیل isp.co.uk ، school.edu.uk ،some-organization.org.uk،another-isp.net.uk ، university.ac.uk ،england.gov.uk، airforce.mil.uk و هر چه که به uk. منتهی می شود.) می باشد. در صورتی که باز هم نتوانست IP موردنظر را پیدا کند به DNS server بالاترین سطح به نام root. مراجعه می کند. این کامپیوتر بسیار قدرتمند بوده و جدول DNS شامل تمام hostname های موجود دریک(domainname نام حوزه) می باشد.

چه وقت و چرا DNS از کار افتاده و hang می کند ؟

فرآیند تبدیل در DNS ممکن است سریع و یا کند باشد. در صورتی که ISP شما ، آدرس IP موردنظر را داشته باشد ، در عرض چند میلی ثانیه این آدرس به دست خواهد آمد. در صورتی که نیاز به پرس و جو از DNS server سطوح بالاتر باشد ، مدت زیادی ، حدود ۱۵ ثانیه ، طول خواهد کشید. در بدترین حالت مرورگر شما dialog box ی را مبنی بر پیدا نکردن آدرس موردنظر نمایش می دهد که در دو صورت ممکن است رخ دهد : یا واقعا آدرس موردنظر شما موجود نیست یا اینکه فرآیند جستجو بسیار وقت گیر بوده و باعث time-out و به عبارتی قطع ارتباط شده است. در صورتی که حالت دوم باشد بر روی Refreshیا Reload (بسته به نوع مرورگر خود) کلیک کنید . این بار

فرآیند جستجو زمان کمتری خواهد گرفت چرا که DNS server مربوط به ISP شما را در مرحله قبل آدرس IP موردنظرتان را از سطوح بـالاتر دریافـت کرده و در جدولش ذخیره کرده است.

نویسنده : ZaiaN_Red

Special Thanks To My Friends : r00t_accs , jmxforce , blackcodewriter

*** Black Hole Network Security Team ***