مشخصه و ویژگیهای آدرس شبکه (آی پی) را بطور کامل توضیح دهید

تعریف : یک آدرس آی پی ، آدرس منحصر به فردی است که برای آدرس دهی تجهیزات شبکه بکار میرود .

مشخصه ها :

یک آدرس کامل آی پی از ۳۲ بیت تشکیل شده است .

این آدرس از ۴ قسمت ۸ بیتی تشکیل شده که با نقطه از هم جدا میشوند .

دارای ۵ کلاس به شرح زیر میباشد :

نام کلاس	رنج آی پی	Subnet Mask	Net ID	Host ID	پرارزشترین بیت سمت چپ	توضیحات
A	۰ ~ ۱۲۷	255.0.0.0	2^8	2^{24}	**0**	برای شهرهای بزرگ استفاده میشود
B	۱۲۸ ~ ۱۹۱	255.255.0.0	2^{16}	2^{16}	**10**	برای شهرهای متوسط استفاده میشود
C	۱۹۲ ~ ۲۲۳	255.255.255.0	2^{24}	2^8	**110**	برای شهرهای کوچک استفاده میشود
D	224 ~ 239	N/A	-	-	**1110**	Multicast
E	240 ~ 247	N/A	-	-	**11110**	Reserved

دیوار آتش را تعریف کرده و لایه های آن را بنویسید .

سیستمی است که بین کاربران یک شبکه محلی و یک شبکه خارجی مانند اینترنت قرار میگیرد و بر ورودی و خروجی اطلاعات و داده ها نظارت میکند . به عبارت دیگر دیوار آتش کلیه ترافیک ها را کنترل و ورودی و خروجی را با استاندارد امنیتی خود مطابقت داده و به سه روش زیر عمل میکند :

الف) بسته اجازه ورود میگیرد Accept Mode

ب) بسته حذف میشود Blocking Mode

ج) بسته حذف شده و به مبدا (فرستنده بسته) پاسخ مناسبی ارسال میشود . Response Mode

بطور کلی دو نوع دیوار آتش وجود دارد : الف) دیوار آتش لایه کاربردی Application Layer Firewall

ب) دیوار آتش فیلتر بسته ای Packet Filtering Firewall

لایه ها در دیوار آتش :

بطور کلی در دیوار آتش ۳ لایه وجود دارد .

لایه اول) براساس تحلیل بسته آی پی و فیلدهای سرآیند کارمیکند .که بخش زیر را بررسی میکند :

الف) برسی آدرس آی پی مبدا و مقصد ب) شماره شناسایی بسته اطلاعاتی Data Gram ج) شماره قراردادProtocol د) زمان حیات بسته

لایه دوم) فیلدهای سرآیند لایه انتقال برای تحلیل بسته استفاده میشود . که موارد زیر را بررسی میکند :

الف) شماره پورت و پروسه مبدا و مقصد Port And Process

ب) فیلد شماره ترتیب Field

لایه سوم) فیلدهای سرآیند همچنین محتوای بسته اطلاعاتی بررسی میشود ، مثلاً محتوای نامه الکترونیکیE-mail

اجرای تشکیل دهنده یک دیوار آتش : الف) واسط محاوره ای و ساده ورود و خروج ب)سیستم ثبت ج) سیستم هشدار دهنده

وی پی ان را تعریف کرده و انواع آنرا بیان و مزایای استفاده از وی پی ان را بنویسید .

شبکه اختصاصی از خطوط اجاره ای بصورت خط تلفن گرفته میشود ، ساخته میشود . این خطوط از نوع نقطه به نقطه بوده و بیت های اطلاعاتی که روی این خطوط جابجا میشوند از ترافیک های دیگر تفکیک شده است زیرا خطوط اجاره مداری واقعی بین دو سایت ایجاد میکنند .

انواع وی پی ان : الف) وی پی ان سایتی ب) وی پی ان کاربری

الف) وی پی ان کاربری : شبکه اختصاصی بین دو کامپیوتر کاربر و شبکه سازمان میباشد . این نوع وی پی ان اغلب برای پرسنلی استفاده میشود که زیاد سفر یا در خانه کار میکنند .

ب) وی پی ان سایتی : سازمانها برای ارتباط یافتن به سایتهای دور دست بدون نیاز به خطوط اجاره ای گران یا برای ارتباط دو سازمان متفاوت که میخواهند اهداف تجاری و باهم تبادل اطلاعات داشته باشند ، از وی پی ان سایتی استفاده میشود . در واقع وی پی ان سایتی برای ارتباط دو سازمان یا سایت بکار میرود .

مزایای استفاده از وی پی ان :

الف) ترافیک رمز شده تا از استراق سمع جلوگیری شود .

ب) سایتهای دور دست اعتبار سنجی میشوند .

ج) پروتکل های متعددی روی وی پی ان حمایت میشوند .

د) ارتباط از نوع نقطه به نقطه می باشد .

ه) کاربر احساس مجزا بودن نمیکند .

امضای دیجیتال را بطور کامل توضیح داده و نقش آنرا در امنیت بنویسید و الگوریتم های آنرا با توضیح شرح دهید .

يكي ديگر از راه هاي تائيد صحّت فايل ارسال شده به مقصد ، استفاده از امضاي ديجيتال مي باشد.كاربر با ساختن يك امضاي ديجيتال مي تواند هر نامه اي را به اين وسيله مورد تائيد قرار دهد . اگر اين نامه در بين راه توسط يك هكر مورد حمله قرار گيرد ، امضاي آن نامه از بين مي رود و هكر قادر به برگرداندن آن امضا نيست ، در اين صورت گيرنده نامه متوجه مي شود كه اين نامه معتبر نبوده و توسط يك هكر مورد استفاده قرار گرفته است .

الگوریتم های امضای دیجیتال

چک سام: كنترل نهايي ممكن است هيچ اهميت خارجي نداشته باشد اما براي اهداف كنترلي مورد استفاده قرار مي گيرد اگر حاصل جمع رياضي (خردكننده) قبل و پس از ارسال شدن بسته هاي اطلاعاتي با هم ، هم خواني نداشته باشد خطائي در انتقال داده ها و اطلاعات صورت گرفته است با روش چك سام مي توان كشف خطا نمود و به روش كد همينگ اصلاح خطا نمود .

هشینگ : يعني در هم يا قطعه قطعه يا حاصل جمع كنترل كننده اي كه در آن كسي نمي تواند بلوكي از داده ها را توليد نمايد كه مجموع كنترلي از پيش تعيين شده يا مقدار هش ديگري را ايجاد نمايد .

کلید اختصاصی : اين كليد در اختيار كاربران مي باشد و هر كاربر كليد اختصاصي مختص خود را دارد و رمز گزاري توسط اين كليد انجام مي شود. براي امنيت بيشتر نبايد اين كليد دست هر كسي بيفتد .

کلید عمومی : از کلید عمومی برای ارسال اطلاعات رمز شده استفاده میشود که هر طرف باید از کلید مطلع باشند .

انواع ویروس ها را شرح داده و عواملی که باعث تخریب در شبکه میشود را بنویسید.

الف) ویروس های قطاع بوت : این ویروس ها خود را در اولین قطاع دیسک مخفی میکنند و بدلیل کم حجم بودن ، این مکان برای جایگیری آنها کافی است . این ویروس ها به هنگام راه اندازی یک سیستم پیش از تشخیص توسط ویروس یاب وارد حافظه شده و در آنجا مخفی میشوند و با راه اندازی مجدد یا اجرای یک برنامه فعال شده و باعث آلودگی سیستم میشوند .

ب) ویروس های نرم افزاری : این ویروس ها فایل های اجرایی را آلوده می کنند ، با اجرای فایل آلوده ویروس فعال شده و باعث افزایش حجم یکی از داده ها میگردد . اما ویروس های جدید به فایل های آلوده حمله نمیکنند بنابراین باعث افزایش زیاد فایل ها نمی گردد .

ج) ویروس های مقیم در حافظه : در حافظه موقت قرار گرفته و کنترل سیستم را در دست میگیرند . آنها برآیندهای ورودی و خروجی را در ترجمه فایل ها و غیره را تحت کنترل دارند و مورد تاثیر خود قرار می دهند .

د) ویروس های نسل جدید : بگونه ای طراحی شده اند که قابل شناسایی و نابودی توسط ویروس یاب نباشد .

مراحل زندگی ویروس ها :

الف) مراحله خوابیده و بی حرکت : که بستگی به نوع ویروس دارد و مدت زمانی است که ویروس از زمان نوشته شدن تا زمان انتقال به محیط خارج لازم دارد .

ب) مرحله انتشار : که در این مرحله آلوده سازی سیستم صورت می گیرد .

ج) مرحله فعال شدن : که در اثر یک رویداد خاص تعیین شده توسط برنامه نویس ویروس این حالت رخ می دهد

د) مرحله صدمه زدن : بستگی به وظیفه ویروس دارد که چه صدماتی را به برنامه های کاربر وارد خواهد ساخت .

خسارتهای ناشی از ویروس ها

خسارتهای نرم افزاری : بهم ریختن و یا پاک شدن داده های موجود در فایلها ، از بین بردن ارتباط بین فایلها و تغییر در اجرای فایل ها ، افزایش حجم و کپی کردن فایل هل در محل دیگر و تغییر کد های کامپیوتر و نمایش اطلاعات بصورت دیگر .

خسارتهای سخت افزاری : در این نوع حمله ویروس ها ، اگر سیستم قادر به هدایت و کنترل قطعات نباشد ، برای ویروس ها بسیار ساده است که آنها را از کار بیندازند . اگر فرمان یک شیاری که وجود نداشته باشد را به هارد دیسک بدهیم ، هِد دیسک خوان با دیواره دیسک برخورد کرده و از بین میرود . و یا اگر به بیت های آی سی سی پی یو ولتاژ اضافی بدهیم باید با این قطعه خداحافظی کرد .

سایر برنامه های مخرب : اینگونه برنامه ها قابلیت انتشار و تکثیر خود را مانند ویروس ها ندارند و بر سه قسم است .

الف) کرم ها : برنامه هایی که با خزیدن در حافظه کامپیوتر ، دیسک و ... داده های موجود در آنها را تغییر میدهند .

ب) بمبهای منطقی : برنامه ای بسیار کوتاه است که به یک برنامه کاربردی اضافه شده و در زمانی که شرایط مناسب برای او باشد شروع به تخریب داده ها میکند .

د) اسب های تراوا : برنامه های مخربی هستند که میتوانند سیستم را از راه دور کنترل کنند در ضمن این اسبها مورد علاقه هکر ها هستند . به ظاهر برنامه ساده اما در درون محتوای شروری دارند .

DMZ چیست و چه کاربردی در امنیت شبکه دارد .

با ايجاد ناحيه اي شبه حفاظت شده روي شبكه ، دي ام زد ايجاد مي شود و در حالت عادي اين ناحيه با كنترل دسترسي به شبكه توسط فايروال يا روتر با امكان فيلتر كردن بالا طراحي و ايجاد مي شود . اين كنترل سياست را به گونه اي تنظيم مي كند كه تعيين مي كند كه كدام ترافيك اجازه ورود به دي ام زد را دارد و كدام ترافيك مي تواند از دي ام زد خارج شود عموماً هر سيستمي كه بتوان به وسيله ي كاربر خارجي مستقيماً به آن وصل شد بايد در دي ام زد قرار گيرد . در حالت كلي به بخشهايي از شبكه اشاره مي شود كه كاملا قابل اطمينان نيست ، دي ام زد مكاني را روي شبكه ايجاد مي كند تا سيستم هايي كه توسط عموم مردم و از طريق اينترنت قابل دسترسي است از سيستم هايي كه فقط توسط پرسنل سازمان قابل استفاده است ، تفكيك شود .

انواع هکر ها را بنویسید و پس از تقسیم بندی آنها ، انواع حملات را نیز بنویسید .

الف) کلاه سفید ها : این گروه از هکر ها در واقع همان دانشجویان و اساتید هستند که هدفشان نشان دادن ضعف سیستم های امنیتی شبکه های کامپیوتری می باشد . این گروه از هکر ها به هکرهای خوب معروفند .

ب) کلاه سیاه ها : نام دیگر این گروه " کراکر ها " می باشد ، کراکر ها خراب کارانه ترین نوع هکر ها می باشند که بطور پنهانی اقدام به عملیات خرابکارانه میکنند . اولین چیزی که به فکرشان میرسد نفوذ به سیستم قربانی است . کلاه سیاه ها ویروس نویس هستند که با ارسال آن به سیستم قربانی نفوذ میکنند . در واقع یک جاسوس بر روی سیستم قربانی ارسال کرده و همیشه هویتشان پنهان است .

ج) کلاه خاکستری ها : نام دیگر این گروه " واکرها " می باشد ، هدف اصلی واکر ها استفاده از اطلاعات سایر کامپیوتر ها به منظور و مقاصد خواص بوده و صدمه ای به کاپیوتر وارد نمی کنند . این گروه کد های ورود به سیستم امنیتی را پیدا کرده و به داخل آن نفوذ میکنند اما سرقت و خرابکاری جزو کارهای کلاه خاکستری نمی باشد ، بلکه اطلاعات سرقت کرده اشان را در اختیار عموم قرار میدهند .

د) کلاه صورتی ها : نام دیگر این گروه " بوتر ها " می باشند . بوتر ها افراد لوس و بی سوادی هستند که فقط قادرند در سیستم اختلال بوجود آورند و یا مزاحم سایر کاربران در محیط چت شوند . آنها جوانان عصبی و جسوری هستند که خود سواد برنامه نویسی نداشته و از نرم افزارهای دیگران استفاده میکنند . ولی گاهی اوقات این هکر های کم سواد میتوانند خطرهای جدی برای امنیت ایجاد کنند .

انواع حملات هکر ها :

الف) دسترسی ب) دستکاری ج) جلوگیری از سرویس دهی د) حملات انکار

الف) دسترسی : در این حمله مهاجم میکوشد تا به اطلاعاتی که او مجاز به دسترسی به آنها نیست ، دست یابد .

ب) دستکاری : در این حمله مهاجم میکوشد تا به اطلاعاتی که او مجاز به تغییر نمی باشد ، تغییر دهد .

ج) جلوگیری از سرویس دهی : در این حملات باعث میشود که کاربرِ مجاز ، نتواند به منابع سیستم و قابلیت ها و اطلاعات آن سیستم دستبابی پیدا کند .

د) حملات انکار : در این نوع حملات اطلاعات بطور نادرست داده میشوند ، به عبارتی یک واقعیه حقیقی یا معامله ای انجام شده است ، انکار میشود .

Hparvini.blog.ir