نویسنده : میثاق یاریان

موضوع پروژه : هکرها و اینترنت

شماره همراه : 09185785257-09189809677

با تشکر از استاد عزیزم مهندس محمد هادی اردکانی

تقدیم به دستان رنج کشیده پدر

و دلواپسی های بی پایان

مادرم به گواهی سپاسی

بیکران و آکنده از مهر

مقدمه:

با یک بررسی اجمالی مشاهده می شود که سرعت رشد دانش و تکنولوژی بشر با گذشت سده های اخیر به حد چشمگیری رو به افزایش است.در طی قرن بیستم تکنولوژی اصلی در جمع آوری پردازش و توزیع اطلاعات خلاصه می شود، در کنار این نوآوری ها پدیده های دیگری نظیر: شبکه های عظیم مخابراتی رشد صنعت رایانه و توسعه روز افزون ماهواره ها از جایگاه ویژه ای برخوردارند؛ گرچه صنعت رایانه در مقایسه با دیگر تکنولوژی ها مانند:ژنتیک و روباتیک قدیمی به نظیر می رسد، ولی رایانه ها قادرند در مدت زمان کوتاهی اعمال زیادی را انجام دهند که این خود باعث کاربرد روبه رشد و موثر آن در شاخه های گوناگون علمی شده است

از تلفیق رایانه با علم ارتباطات شاخه جدیدی در علم بوجود آمد که بعدها شبکه های رایانهی نام گرفت.

متاسفانه مزایایی متعدد و بسیار شبکه ها علاوه بر کاربران عادی این امکان رابه هکرها (مهاجمان شبکه ای) داده است که در پی دستیابی به اهداف سوء خود در قالب انگیزه های گوناگون (اعم از انگیزه های مالی و روانی) فعالیتهای اخلال گرانه خود را دنبال کنند.

در فصل اول با روشها و تکنیکهای شناخته شده این تهاجمات و موثرترین شیوه های مقابله با آنها صحبت خواهیم کرد.

هکرها و انواع آنها

قبل از هر چیز بهتر است هکرها را بشناسیم؛ هکرها افراد باهوشی هستند که علاقه به شغل ثابت نداشته و در شروع این کار معمولاً انگیزه ای غیر از پول دارند، اصل اول این گروه اطلاعات رایگان برای همه بوده و استفاده از اطلاعات و برنامه های دیگران را حق مسلم خود می دانند هکرها بر اساس اصول اخلاقی خود به 3 دسته تقسیم می شوند.

گروه اول:سامورائی ها (Sumurai)

هکرهایی هستند که تنها هدفشان ورود به رایانه کاربر بوده و هیچگونه آسیبی به کامپوتر نمی رسانند مهمترین اصل این گروه آزادی اطلاعات برای عموم می باشد و هدفشان نشان دادن ضعف سیستم حفاظتی رایانه شما می باشد.

گروه دوم :کراکرها (Cracker)

در واقع هکرهایی هستند که هدفشان دزدیدن اطلاعات و خرابکاری بر روی رایانه و... می باشد و در واقع هدف آنها پنهان شدن در گوشه ای و خرابکاری بر روی رایانه می باشد.

گروه سوم :واکرها (Wacker)

نوع دیگر از هکرها هستند که هدف آنها استفاده از اطلاعات شخصی وخصوصی رایانه مورد نفوذ قرار گرفته می باشد و در واقع خطرناکترین نوع هکر از نظر میزان استفاده از اطلاعات قربانی و خرابکاری با استفاده از این اطلاعات می باشد.

ساده ترین شیوه های تهاجم هکرها

الف) هک کردن به کمک ویروس

ویروس

به طور خلاصه ویروس برنامه هایی هستندکه بدون اطلاع کاربر اجرا وبا تکثیر خود در کامپیمتر میزبان ،وارد رایانه های دیگر می شوند ودراکثر موارد با این فعالیت های نهفته خود تحت شرایط خاص باعث تخریب بخشی از اطلاعات سیستم رایانه ای میشود؛این تخریب می تواند شامل ازدست دادن بخشی از اطلاعات مهم وضروری یا کلیه اطلاعات موجود در رایانه قربانی می باشد.

خصوصیات مشترک تمام ویروس ها این است که در کلیه سیستم های که وارد می شوند،تکثیر و توزیع شده و برای رسیدن به این هدف از ابزار مختلفی مانند:دیسکت،پست الکترونیک و سی دی آلوده وغیره استفاده می کنند ؛ یک ویروس می تواند ظرف مدت کوتاهی کلیه رایانه های یک شبکه بزرگ را آلوده کند قبل از اینکه شناسایی شود اهداف مخرب خود را پیاده کند.

یکی از اعمال اولیه برای هک کردن و نفوذ به سیستم قربانی تنها راه بدست آوردن رمز عبور می باشد، یک هکر برای ورود به رایانه کاربر به دو عامل اولیه یعنی رمز عبور (Password) و اسم کاربر (User name) نیاز دارد. ابتدا هکرها یک برنامه (Virus) را درون اطلاعات درخواستی کاربر قرار داده و بدین ترتیب به رایانه کاربر نفوذ می کند.

حال برای دریافت اطلاعات یک آدرس E-mail یک کاربر شناخته شده را برای Virus تعریف کرده تا اطلاعات بدست آورده در سیستم قربانی را به محض اولین اتصال به اینترنت و به طور مخفیانه و بدون توجه وتائید قربانی را به آن آدرس تعریف شده در ویروس بفرستد; بدون اینکه هکر شناسایی شود.

ب) ارسال پیام های نهانی

گاهی می خواهند موضوعی را با مرجعی، شخصی و ... در میان بگذارند و در عین حال ناشناس بمانند برای این منظور از نرم افزاری به نام «گوست میل» (Ghost mail[1]) استفاده می کنند که در پایگاههای وب گوناگون در دسترس می باشد و قابل ردگیری وشناسایی نمی باشد.

برای پیدا کردن این نرم افزار می توانید از موتورهای جستجو مانند یاهو و گوگل استفاده کنید یا می توانید آن را از پایگاه اینترنتی زیر دریافت کنید.

http : //down load. My computer. Com / detail/ 60/14.html

راه دیگر ارسال اطلاعات به صورت خصوصی با رمز درآوردن کلمه های رمز ورود (گذر واژه ها) و نام کاربران است که باید قبل از اینکه ارسال شوند به رمز درآورده شوند؛ با این حال برای کامل شدن این حمله لازم است ویروس به صورت پنهان در سیستم مورد نظر قرار گرفته باشد، زیرا ویروس عامل نهفته شما بروی

[1] یک نوع نرم افزار ویژه هک کردن می باشد که هکر می تواند با استفاده از این نرم افزار اعمال خرابکارانه ای بر روی رایانه قربانی انجام دهد بدون اینکه قربانی متوجه او شود

رایانه مورد حمله است گذاشتن این تمهید در داخل ویروس به این معناست که ویروس را می توان احتمالاً بعد از اینکه شخص آن را به کاربرد اطلاعات مربوطه را رمز گشایی کند یعنی دستورالعمل را بخواند.

حمله پیشگویی شماره سریال TCP/ IP

حمله به IP

هر رایانه در اینترنت یک آدرس منحصربه فردی برای شناسایی در این جهان مجازی دارد که این آدرس یک سری اعداد هستند که با نقطه ازهم جدا شده که قسمتی از آن هیچ وقت تکراری نمی باشد.

صورت کلیIP این چنین است xxx.xxx.xxx.xxx مثلا: آدرس IP رایانه علی 126.254.63.69 میباشد واین یک آدرس منحصربه فرد رایانه علی هست.

در این حمله هکر کار خود را در دو مرحله انجام می دهد :

در قدم اول هکر سعی می کند آدرس IP سرویس دهنده را بدست آورد این کار معمولاً از طریق بررسی بسته های موجود در شبکه از طریق حدس زدن ترتیب شماره های میزبانها یا از طریق اتصال به یک مرورگر وب و مشاهده آدرس IP سایت در نوار وضعیت پنجره انجام می شود.

چون هکر می داند که دیگر رایانه های موجود در شبکه دارای آدرس های **IP** هستند که بخشی از این آدرس با آدرس سرویس دهنده مشترک است بنابراین او سعی می

کند یک شماره آدرس **IP** را طوری شبیه سازی کند که به هکر اجازه عبور از مسیریاب و اجازه دستیابی به سیستم را به صورت یک کاربر داخلی ارائه نماید .

به عنوان مثال اگر سیستمی دارای آدرس **192.00.15** باشد هکر با دانستن این که حداکثر 256 رایانه می تواند به یک شبکه کلاس C متصل شوند ممکن است سعی کند کلیه شماره آدرسهایی که آخرین بایت آنها در این بازه جای می گیرند را حدس بزند. می دانید که آدرسهایی که آخرین IP تعداد رایانه های متصل به یک شکبه را نشان می دهند، در این حالت مقدار دو بیت با ارزش (128+64=192) نشان می دهند که کلاس شبکه از نوع C می باشد.

در قدم دوم پس از آنکه هکر محدوده ی آدرسهای موجود در شبکه را حدس زد سعی می کند شماره سریالهای بسته های ارسالی میان رایانه های موجود در شکبه را کشف کند، با کشف مبادلات درون شبکه هکر سعی می کند شماره سریال بعدی را توسط سرویس دهنده تولید می شود حدس بزند و سپس یک شماره سریال تقلبی درج نموده و خود را میان سرویس دهنده و کاربر جای دهد با توجه به این که هکر آدرس **IP** سرویس دهنده را نیز در اختیار دارد می تواند بسته هایی با شماره سریال و آدرس **IP** صحیح تولید کرده و به مبادلات کاربر نفوذ نماید.

یک هکر پس از نفوذ به یک سیستم کلیه اطلاعات مورد مبادله با سرویس دهنده اعم از فایلهای کلمه رمز اسامی **Login**[1] و دیگر داده های حیاتی را در اختیار دارد بنابراین با کشف شماره سریال مقدمه ای برای یک حمله واقعی به سرویس دهنده فراهم می شود.

حمله به TCP

TCP

TCPمسئول چک و نظارت کردن انتقال صحیح اطلاعات از مبداء به مقصد که همان IPهای موجود در شبکه می باشد تا اگر مشکلی در میان راه اتفاق افتاد،اطلاعات دوباره ارسال شود.

شاید متداول ترین تهاجم به سرویس دهنده های مرتبط با اینترنت حمله به **TCP** باشد. هدف اصلی از حمله به**TCP** این است که هکر بتواند کنترل رایانهی را که به شبکه مورد نظر وی متصل شده است در اختیار بگیرد پس آن رایانه را از شکبه جدا سازد و سرویس دهنده را طوری فریب دهد که هکر را به عنوان یک کاربر معتبر بشناسد.

پس از انجام تهاجم هکر آدرس **IP** رایانه مقصد را با آدرس **IP** خود تعویض کرده و شماره سریالهای مقصد را جعل می نماید.حمله به **TCP** نسبت به حدس زدن **IP** کار را بسیار راحت می کند، با یک بار حمله به **TCP** یکبار برای همیشه از شر پاسخگویی

[1] عمل ورود به شبکه را Login می گویند،دراینجا به معنی رمز ورود به شبکه

به کلمه رمز در سیستم های دارای کلمه رمز راحت می شوید، از طرفی حمله به **TCP** خطرناکتر نیز می باشد، زیرا در این شیوه منابع بسیاری به صورت نا محدود در اختیار هکر قرار می گیرد.

حمله نشست TELNET[1]

هکرها می توانند تقریباً در هر نوع ارتباطات شکبه ای اختلال گری نمایند به عنوان مثال یک هکر با الگوی زیر می تواند در یک ارتباط **TELNET** اخلال کند.

1ـ قبل از شروع حمله در **TELNET** هکر مدتی مبادلات را نظاره می کند.

2ـ در زمانی مناسب هکر حجم زیادی از اطلاعات تهی را به سرویس دهنده می فرستد در نشست **TELNET** هکر بایتهای **ATR – SVR-OFFSET** را که حاوی رشته ای از بایتهای **IAC Nop** است ارسال می نماید در پروتکل **TELNET** فرمان **Nop** بصورت " **No Operation** " (عملیات تهی) تفسیر می شود به عبارت دیگر هیچ کاری انجام نشده و از این بایتها صرف نظر می شود تنها مزیت این کار ایجاد وقفه ای کوتاه برای پذیرش و پردازش دستور می باشد، پس از این مرحله سرویس دهنده زیر را دریافت می کند.

3ـ پذیرش فرمان هکر یک ارتباط ناهماهنگ بوجود می آورد.

[1] یک پروتکل یا قرارداد کاربردی اینترنت است که وظیفه برقراری ارتباط با میزبان های راه دور را دارد .

4ـ برای ایجاد یک وضعیت ناهماهنگ برای کاربر هکر همان مراحل انجام شده برای سرویس دهنده را برای کاربر تکرار می نماید.

دفاع در برابر حملات هکرها

دفاع در مقابل حمله های ناشی از حدس زدن شماره سریال

ساده و کارآمدترین شیوه برای محافظت در برابر حمله های ناشی از حدس زدن شماره سریال این است که مطمئن شوید مسیریاب **Fire Wall**[1] و هر یک از سرویس دهنده های موجود در سیستم شما از سیستم حفاظتی بررسی ردپا برخوردار هستند. با این نوع حفاظت هرگاه یک هکر بخواهد در میان مسیریاب یا **Fire Wall** قرار گیرد و عملیات نفوذی خود را انجام دهد می توانید حرکات وی رامشاهده نمایید.

کشف حمله نشست **TELNET** و نتایج جانبی

شما می توانید با استفاده از نقص **ACK**[2] ها ناشی از حمله پی به تهاجم ببرید در این مبحث سه شیوه شناسایی حملات بررسی می شوند.

1ـ شناسایی وضعیت نا هم زمان :

با استفاده از یک برنامه خواندن بسته های **TCP** (برنامه ای که تعداد بسته های **TCP** را خوانده و می تواند محتویات هر بسته را نشان دهد،) می توانید در هر دو طرف

[1] به معنی دیوار آتش اما در اصطلاح به دیوار امنیتی موجود در سیستم عامل گویند که از ورود هکرها و دیگر نفوذگرها جلوگیری می کند.

[2] در واقع پیام های ردو بدل شده بین سرویس دهنده و سرویس گیرنده می باشد

ارتباط شماره سریالها را مشاهده کنید با توجه به شماره سریالها می توانید تشخیص دهید آیا ارتباط غیر هم زمان شده است یا خیر با این حال تنها در حالیکه مطمئن هستید شماره سریالها توسط هکر دستکاری نمی شوند این شیوه موثر است.

2ـ شناسایی توفان ACK :

برخی اطلاعات آماری درباره ترافیک TCP در یک[1] Ethernet محلی پیش از حمله و بعد از حمله نشان دهنده وقوع حمله هستند، به عبارت بهتر در هنگام حمله تعداد بسته های ACK در بازه ای بین 1 تا 300 بسته رشد می کنند .

3- شماره درصد بسته ها :

با شمارش درصد بسته ها می توانید وضعیت ارتباط را نشان دهید از مقایسه درصد بسته های شمارش شده در وضعیت عادی در هنگام حمله وجود حمله قابل شناسایی خواهد بود.

نکاتی در مورد جعل کردن

در سرویس های TCP , UDP[2] فرض می شود که آدرسIP میزبان آدرس معتبر است و بنابراین به آن اعتماد می کنند با این حال میزبان یک هکر می تواند با مسیریابی

[1] یکی از رایج ترین مدل های شبکه های رایانه ی است که بیشتر در شبکه سازی استفاده قرار می گیرد .

2 یک پروتکل ساده و کاربردی بوده که وظیفه ی اصلی آن بررسی شماره ترتیب و ارسال پیغام های کنترلی در لایه انتقال TCP/IP می باشد .

IP خود را به عنوان یک میزبان یا کاربر معتبر جا بزند، در مثال زیر مشاهده خواهید کرد که رایانه یک هکر چگونه کاربر معتبر را جعل کند.

1-هکر آدرسIP یک میزبان را طوری جعل می کند که مطابق با آدرس یک کاربر شود

2- هکر سپس یک آدرس برای سرویس دهنده ای می سازد که مسیری مستقیم میان سرویس دهنده و آدرس هکر برقرار می کند.

3- هکر با استفاده از آدرس منبع تقاضاهای کاربر را به سرویس دهنده می فرستد.

4- سرویس دهنده در صورتی که درخواست مستقیماً از کاربر برسد می پذیرد و پاسخی برای آن می فرستد.

5- کاربر مطمئن با استفاده ازمسیر مبدا بسته را به میزبان هکر می رساند.

یک روش ساده تر برای جعل کردن یک کاربر این است که صبر کنیم تا کاربر رایانهش را خاموش کند و سپس رایانهش را جعل نماییم در بسیاری از سازمانها،اعضاء دارای رایانههای شخصی و نرم افزارهای شبکه ایTCP/IP اختصاصی هستند و از میزبانهای یونیکس به عنوان سرویس دهنده های محلی استفاده می برند رایانههای شخصی معمولاً از سیستم فایل شبکه ای یونیکس[1] (Unix) ; (NFS) برای دستیابی به شاخه ها و فایلهای سرویس دهنده استفاده می کنندیک هکر می تواند خود را جای یک کاربر واقعی جا بزند و یک رایانه شخصی را با همان

[1] یک نوع سیستم عامل قدرتمند مبتنی بر شبکه می باشد

نام و آدرس IP پیکربندی نماید و سپس یک ارتباط با میزبان یونیکس برقرار سازد یک هکر به سادگی می تواند یک حمله جعلی پیاده سازی کند.

جعل کردن E-mail

جعل کردن Email در اینترنت بسیار آسان است و غالباً نمی توان به Email های فاقد ابزار امنیتی نظیر امضای دیجیتالی اطمینان کرد، به عنوان مثالی کوتاه فرض کنید در یک مبادله اینترنتی میان میزبانها یک نام ردوبدل می شود، در این مبادله از پروتکلی مبنی بر میزان کدهای اسکی استفاده می شود با استفاده از Telnet به سادگی می توان به پورت SMTP[2] متصل شد گیرنده به مشخصات فرستنده اعتماد می کند،هکربه سادگی می تواند نامه اصلی را با الصاق آدرس متفاوت و درج آدرس خود جعل کند.

مراحل جعل کردن Emil در Nets Scap Nawigator[3]:

برای جعل کردن نامه ها از برنامه Nets Scap Nawigator مراحل زیر را دنبال کنید.

1- از منوی Option گزینه Mail و سپس News Prefrences را انتخاب نمایید.

2- در جعبه مکالمه Prefrences روی قسمت Identify کلیک کنید.

3-در این پنجره مشخصات جاری E-mail شما به چشم می خورد در قسمت نام و آدرس E-mail عبارتی دلخواه نظیر Borna66@Yahoo.com قرار دهید.

---

[2] یک پروتکل یا قرارداد کاربدی اینترنت است که برای نقل و انتقالات پست الکترونیک استفاده می شود.

[3] یک مرورگر اینترنت می باشد که قابلیت های فراوانی نسبت به دیگر مرورگرها دارد.

4-سپس روی قسمت **Servers** کلیک کرده و آدرس **POP3**[1] را حذف نمایید زیرا اگر قصد جعل کردن دارید طبیعتاً نمی خواهید کسی شاهد اعمال شما باشد پس مقادیر درون **User Name** را حذف نمایید.

5- دکمه **OK** را فشار داده و از پنجره**Perfrences** خارج شوید اکنون آماده جعل کردن نام هستید.

جعل کردن آدرسهای درون وب

هکرها پا را فراتر گذاشته و می توانند حمله ی خود را روی سایتهای ایمن و سایتهای بنا شده بر مبنای **SSL**[2] گسترش دهند در حال حاضر پروتکل **SSL** از نام **DNS** (Domain Name Server)در گواهینامه خود استفاده می کند برای مبادله ایمن داده و اعتماد کاربر به داده های دریافتی سرویس دهنده برای مرورگر کلید خصوصی ارسال می کند بنابراین در رابطه با جعل نواری آدرس ها **SSL** تقریباً هیچ مسئله ای ندارد.اما از آنجا کلیه آدرسهای موجود در یک صفحه وب قطعاً از **SSL** بهره نمی برند بنابراین جعل کردن چنین آدرسهایی امکان پذیر است.

کشف جعل گذاری

[1] یکی دیگر از پروتکل یا قراردادهای کاربردی انترنت می باشد که نقل و انتقالات پست الکترونیک استفاده می شود.

[2] به یک فناوری و تکنولوژی جدید که برای کنترل و برقراری امنیت بیشتر در شبکه های رایانهی مورد استفاده قرار می گیرند .

بر خلاف حمله های غیر هم زمان حمله های جعل گذاری به سختی کشف می شوند. اگرسایت[1] شما توانایی نمایش ترافیک شبکه راحول مسیریاب شما داشته باشد باید بار ترافیک ورودی به مسیریاب را مورد بررسی قرار دهید این بار را در قالب یک فایل ذخیره کنید با استفاده از این فایل می توانید بسته های ورودی را که آدرس مبدأ و مقصد آنها در محدوده دامنه سایت شما هستند بررسی نمایید.

اگر با بسته هایی مواجه شوید که داراری آدرس مبدأ و مقصد یکسانی بودند و از مسیریاب شما عبور کرده اند این موضوع نشان دهنده وقوع یک حمله جعل گذاری می باشد.

مقابله های ممکن در برابر جعل آدرسها

اگراز نرم افزار تأیید سرویس دهنده (نظیر سرویس دهنده های جاوا در زمینه جامعیت مبادلات) استفاده می کنید و نمی توانید برای ترمیم یک تخریب منتظر خدمات چنین نرم افزاری بمانید تنها راه حل ممکن قرار دادن نقطه شروع مرورگرهای کاربران روی سایتهای ایمن می باشد، بدین ترتیب هکرها نمی توانند عملیات تخریبی

[1] آدرس یا محل منحصربه فرد و غیر تکراری در اینترنت می باشد که به عنوان نشانی آن محل در وب جهانی می باشد.

خود را شروع کنند؛ یک صفحه ایمن صفحه ای است که به جامعیت آن می توانید اعتماد نمایید چنین صفحه ای می تواند یک فایل **HTML**[1] یا یک صفحه **SSL** باشد.

یکی از دو روش زیر را می توانید تشخیص دهید که سایت مورد نظر شما ایمن می باشد یا خیر.

1-سایت مربوطه از کلیه روشها و خدمات ایمن سازی در مقابل تهاجمات برخوردار باشد.

2- سایت تنها به صفحاتی اتصال داشته باشد که ایمن باشد.

اگر سایتها از ویژگی شماره 1 بی بهره اند در صورت تمایل برای ایمن سازی می توانید عناصر منحصر به فرد در صفحات خود درج نمایید نمونه هایی از این عناصر گواهینامه **Verisign Java** یا گواهینامه **Microsoft Aathenticode** می باشد.

روش دوم برای مقابله با چنین تهاجماتی انجام تنظیمات خاص روی مرورگر می باشد یکی از این تنظیمات باعث نمایش گواهینامه های مربوط به سایت می شود.

یک کاربر و یک سازمان می تواند سریعاً **Plug-in**[2] مربوط به یک مرورگر را طوری تنظیم کند که گواهینامه مربوط به هر سایت را که مرورگر به آن متصل می شود نمایش دهد.

---

[1] یک زبان برنامه نویسی و اسکریپ نویسی صفحات و ب اینترنت می باشد، که در واقع مبنای تمام زبان های برنامه نویسی صفحات وب می باشد.

[2] برنامه هایی الحاقی هستند که درون یک مرورگر که قرار می گیرند که موجب افزایش کارایی و ویژگی مرورگر افزونی قابلیت چند رسانه ای آن می شود

جعل کردن وب

جعل کردن وب یکی دیگر از شیوه های حمله های هکرها می باشد. در این روش یک نسخه معادل از کل وب کپی می شود وب کپی شده دارای تمام ظواهر وب اصلی است با این تفاوت که به طور کامل توسط هکر کنترل می گردد به طوری که کلیه مبادلات میان مرورگرهای کاربران و وب از زیر نظر هکر می گذرند.

اثرات جعل کردن وب

در این شیوه از تهاجم هکر می تواند کلیه داده های ارسالی از کاربر به سرویس دهنده وب را مشاهده یا دستکاری نماید علاوه بر این او می تواند کلیه داده های ارائه شده از سرویس دهنده به کاربر را نیز کنترل نماید در نتیجه هکر می تواند به روشهای گوناگون ضربه وارد نماید.

در روش جعل کردن وب هکر محتویات صفحاتی کاربر مشاهده می کند را ضبط می نماید وقتی کاربر در یک صفحه HTML فرعی را پر می کند و آن را ارسال می نماید، هکر می تواند کلیه این اطلاعات را گردآوری نماید از طرفی پاسخ سرویس دهنده به کاربر نیز توسط وی قابل دسترسی می باشد با توجه به این که در اکثر معاملات تجاری از فرم ها استفاده می شود هکر می تواند به شماره حسابها کلمات رمز دیگر اطلاعات حیاتی افراد دستیابی داشته باشد.

جعل کردن کل وب

ممکن است تصور کنید که برای هکر جعل کردن تمام"Word wide web"[1] مشکل باشد اما متاسفانه چنین نیست برای هکر ذخیره کردن تمام محتویات وب دنیا ضرورتی ندارد با توجه به این که کل وب به طور مستقیم در اختیار هکر است او می تواند در هنگام نیاز هر صفحه دلخواه را بازیابی کرده و یک کپی برای خود بسازد.

شکار هکرها

مشاهده می شود که تنها عامل بازمانده هکرها از تهاجمات جعلی پیدا کردن و گوش مالی دادن آنهاست؛ طبیعت یک تهاجم طوری است که ازطریق سرویس دهنده هکر می تواند جایگاه وی را شناسایی کرد، اگر کاربری پی یک حمله برد می تواند با کمی هوشمندی موقعیت حمله کننده را شناسایی کنند، باز در این جا لازم به ذکر است که هکر های حرفه ای تهاجمات خود را ازطریق رایانه ها و تلفنهای ضروری انجام می دهد

راه حل هایی برای جلوگیری از حمله به وب

[1] به معنی تور جهان گستر است که در واقع همان اینترنت جهانی می باشد.

تاکون دریافتید که جعل کردن وب ها حمله بسیار خطرناک و تقریبا غیر قابل کشف می باشد اما با استفاده از استراتژی[1] سه مرحله ای زیر می توانید حداقل دفاعی مناسب ازخود ارائه دهید.

1 ـ در مرور گر خود قابلیت (**Java , Java Script , Vb Script**[2]) را غیر فعال نمایید تا هکر نتواند ردپای خود را محو نماید.

2 ـ مطمئن شوید که خط آدرس مرور گر شما فعال است.

3 ـ همواره به خط آدرس توجه نمایئد تا مطمئن شوید که مرورگر شمابه آنجایی که منظور شماست متصل شده است روش فوق در واقع یک راه حل ساده و کو.تاه مدت می باشد .

این استراتژی ساده و سه مرحله ای و تا حد زیادی از تهاجمات جعلی جلوگیری خواهد کرد اما در صورت لزوم به راه حلهای بلند مدت وپایداری برای مقابله با تهاجمات باید مرورگرهایی اختصاصی طراحی نمود که در مقابل جعل کردن خط منوها و نوار وضعیت مقاوم باشد و همواره کاربر را از اتصال به وب مورد نظر وی مطلع سازد.

---

[1] یک روش یا هدف کوتاه مدت در یک گروه می باشد که در صورت موفقیت در اجراء به هدف یا نتیجه ی نهایی آن گروه رهنمون می شود .

[2] هر یک زبان برنامه نویسی و اسکریپت نویسی برای طراحی صفحات وب می باشد.

مقدمه ای درباه ی امنیت و اینترنت

اینترنت همه روزه افراد بیشتری را با یکدیگر ارتباط می دهد و دسترسی به مکانهای گسترده تری را امکان پذیر می سازد.با استفاده هر چه بیشتر از اینترنت و پست الکترونیک،دانستن وبکاربردن مسائل امنیتی مهمتر و واجب تر می شود؛ ممکن است تصور کنید که وارد شدن به رایانه شما ،برای کسی اهمیت چندانی ندارد ،ولی واقعیت این است که نفوذگران انسانی و ماشینی به صورت ماهرانه نشانه های IP اینترنت راجستجو واسکن کرده تا شبکه ها و رایانههای ناامن را پیدا کنند و سپس کرمها و ویروس ها بصورت پست الکترونیک را مثل شعله های خشمگین گسترش دهند،بدون اینکه بدانند یا اهمیت بدهندکه به چه کسی آسیب می رسانند.

بسیاری ازمردم برای تجهیز کردن رایانه خود به دیوار آتش (Fire Wall) و حفاظت ازآن،به دنبال یک راه حل عملی وکارا در محیط سیستم عامل خود هستند.

کاربران ویندوز(Windows)باید نکاتی را جهت حفظ و برقراری امنیت مراعات کنندوبه مظور درک بعضی از موارد مربوط به امنیت شبکه ،شناخت ساده ای از تکنولوژی مرتبط با این علم را داشته باشیم .

بنابراین در فصل دوم با چند مفهوم پایه و اساسی امنیتی آشنا می شویم،سپس درفصل سوم به معرفی و بررسی چند نرم افزار ویژه هرایانه می پردازیم، بالاخره در فصل چهارم آموزش نرم افزاز امنیتی Zone Alarm Pro می پردازیم ودر پایان در فصل پنجم با چند مفهوم پایه و کاربردی اینترنت آشنا و به معرفی آن می پردازیم.

فصل دوم

آشنایی به چند مفهوم پایه و اساسی امنیتی

Active Content Monitoting

عبارت مزبور در مورد فرآیند بررسی ورود داده ها به شبکه یا رایانه که به خاطر جلوگیری از خرابکاری انجام می شود،بکار می رود.

Access Control

فرآیند تعیین و شناسایی شخصی است که می خواهیم از منابع و اطلاعات سیستم شما استفاده کند.

ویروس (Virus)

برنامه هایی هستندکه بدون اطلاع کاربر اجرا وبا تکثیر خود در رایانه میزبان ،وارد رایانههای دیگر می شوند ودراکثر موارد با این فعالیت های نهفته خود تحت شرایط خاص باعث تخریب بخشی از اطلاعات سیستم رایانهی میشود؛این تخریب می تواند شامل ازدست دادن بخشی از اطلاعات مهم وضروری یا کلیه اطلاعات موجود در رایانه قربانی می باشد.

خصوصیات مشترک تمام ویروس ها این است که در کلیه سیستم های که وارد می شوند،تکثیر و توزیع شده و برای رسیدن به این اهدف از ابزار مختلفی مانند:دیسکت،پست الکترونیک و سی دی آلوده وغیره استفاده می کنند ؛ یک ویروس

می تواند ظرف مدت کوتاهی کلیه رایانه های یک شبکه بزرگ را آلوده کند قبل از اینکه شناسایی شود اهداف مخرب خو را پیاده کند.

با این وجود باید در نظر داشت که عناصری نیز وجود دارند که ویروس محسوب نمی شوند؛این عناصر کرمها و اسبهای تروا نامیده می شوند.

اسب تروا(Trogan Horse)

برنامه هایی هستند که مخفیانه خود را وارد سیستم کده و دور از چشم کاربر،فعالیتهای خاصی را انجام می دهند؛این فعالیتها معمولابرای سیستم مضر نیستند ،بلکه بخشی از اطلاعات مهم ومحرمانه کاربر را به نقاط دیگری ازجهان می فرستند ویا زمانی که اجرا می شوتد حفره ها ی امنیتی در سیستم عامل ایجاد می کنند.

کرمها (Worm)

برنامه هایی هستند که صرفا به تکثیر خود می پردازند،این عمل علاوه بر مشکل اشباع شدن حافظه و هارد دیسک ،می تواند به دلیل تکثیر مداوم ،پهنای باند سیستم را بلوکه کرده و بازده کاری آنرا به حداقل ممکن برساند.

البته بایددرنظر داشت که امروزه با روش های ویروس نویسی جدید و ارتباطات کنون ،عملا مرز بین ویروس ها،اسب تروواها ،کرمها تا حدودی برداشته شده است ؛ به این معنی که یک اسب تروا می تواند بصورت یک کرم وارد سیستم شده و عملیات تخریبی ویروسی را در سیستم انجام دهد.

IP

در اینترنت هر رایانهی دارای یک شماره خاص خود یعنی نشانیIP_ است که از 4 بایت تشکیل می شود(هر بایت متشکل از هشت بیت بوده و هر بیت می تواند مقداری بین 0تا255 در مبنای دهدهی به خود بگیرد)،این 4 بایت بصورت دهدهی به وسیله نقطه از هم جدا می شود.به عبارت دیگر هر رایانه در اینترنت یک آدرس منحصربه فردی برای شناسایی در این جهان مجازی دارد که این آدرس یک سری اعداد هستند که با نقطه ازهم جدا شده که قسمتی از آن هیچ وقت تکراری نمی باشد.

صورت کلی IP این چنین است xxx.xxx.xxx.xxx مثلا آدرس IP رایانه رضا 126.254.63.69 می باشد واین یک آدرس منحصربه فرد رایانه رضا هست.

TCP

TCPمسئول چک و نظارت کردن انتقال صحیح اطلاعات از مبداءبه مقصد که همان IPهای موجود در شبکه می باشد تا اگر مشکلی در میان راه اتفاق بیافتد،اطلاعات دوباره ارسال شود.

Spyware

در واقع Spyware یک ویروس نیستند،بلکه به هر فناوری که هدفش جمع آوری اطلاعات از یک شخص یا سازمان بدون اطلاع آن باشد Spyware گفته می شود.

بـر روی اینترنـت گـاهی اوقـات بـه آن Spywbot گفتـه میشـود؛بطورکلی Spyware نـرم افزاری است که روی رایانه یـک شـخص بـه منظـور جمـع آوری اطلاعـات راجـع بـه کاربران آن با مقاصد و اهداف مختلف (مثلا:تجاری،مالی،سیاسی و...) و بـدون اطـلاع آنها قرار می گیرند. Spyware می تواند در قالب یک ویروس، کرم، اسب تروا یا هر نـرم افزار دیگری باشد؛این گونه برنامه ها ممکن است به وسیله یک نرم افـزار کـه خودبـه خود روی رایانه شما بارگذاری شده است یا کلید روی یک پنجره Pup-up[1] و تبلیغاتی و بسیاری موارد دیگر روی رایانه اجرا شود.

Spam (نامه های مزاحم ناخواسته)

اسپم ها نامه های الکترونیکی ناخواسته و مزاحمی هستند که به شکل انبوه توسط شرکت ها تبلیغاتی برای کابران اینترنت فرسـتاده مـی شـود،بدون اینکـه درخواسـتی مبتنی بر دریافت آنها از سوی کابران ارائه شود.

اسپم ها برای اینکه بتوانند در سراسر اینترنت پایگاههـایی بـرای ارسـال ایمیـل هـای مزاحم داشته باشند از رایانه ها کابران تازه کار برای Spamer (ارسال کننـدگان نامـه ها الکترونیکی مزاح و ناخواسته)استفاده می کنند.آنها براحتـی رایانـه هـای کـاربران ساده لوح را با روش های گوناگون هک کرده و از سـخت افـزار و منـابع شـبکه آنهـا برای ارسال اسپم استفاده می کنند.

[1]: نوع پنجره های تبلیغاتی آلوده به ویروس هستند که هنگام کار با اینترنت به یکباره ظاهر شده و کاربر با توجه به ظاهر و نمای زیبای و جذاب آن و بدون آگاهی جواب آن را تائید می کند.

Cookie (کوکی)

وقتی در حال مشاهده برخی از سایتهای اینترنتی هستید، اطلاعاتی روی رایانه شما ذخیره می شود،که به این اطلاعات ذخیره شده توشط سایت ها بر روی رایانه شما Cookie(کوکی یا کلوچه)می گویند .

سایت های که شما ازآن بازدید کرده و فرم و اطلاعات شخصی خود(مانند:نام کاربری و پسورد دیگر مشخصات) را پر کرده اید، اطلاعات را در یک فایل متنی روی رایانه شما ذخیره می کنند تا در آینده برای شناسایی شما به هنگام ورود به آن سایت استفاده کنند؛بیشتر مرورگرها بطور پیش فرض به کارگزاران وب اجازه می دهند که فایل های کوچک کوکی را برای شناسایی شما در سایتشان بر روی رایانه شما ذخیره کنند؛اما شما می توانید جلوی این کار را بگیرید.

در واقع وقتی شما برای نخستین بار به برخی از سایتها مراجعه می کنید از شما می خواهند که یک فرم ثبت نام را پر کنید ،در این فرم اطلاعات چون :نام،نام خانوادگی،کلمه عبور و نشانی پست الکترونیک خود را در صورت تمایل وارد و فرم را پر می کنید،اینها نخستین اطلاعات موجود در کوکی بوده و بسیاری از اطلاعات دیگری را که حتی شما فکرشان هم نمی کنید در فایل کوکی قرار می گیرد.

با این وصف وقتی برای بار دوم با این سایت مراجعه کنید ،کارگزار وب آن سایت سراغ آن فایل کوکی موجود در رایانه شما می رود و آنرا می خوانند،بدین ترتیب شما را می شناسد و صفحات سایت را برای شما نتظیم می کند،مثلا :در صفحه اول

سایت شما را با نام کاربری خطاب می کرده و به شما خوش آمدگویی می کند،شما فقط یک بار در این سایت ثبت نام کرده باشید و فرم پر کرده اید، در ملاقات های بعدی از سایت مذکور،خود سایت شما را به جا می آورد و نیازی نیست که مجدد ثبت نام وفرم پر کنید.

Fire Wall (دیوار آتش)

فایروال در لغت به معنای دیواری است که برای جلو گیری از گسترش آتش بنا شده باشد بکار می رود،اما فایروال های رایانه و اینترنت برای جلوگیری از ورود سرزده و غیرمجاز از اینترنت به رایانه ی شما ساخته شده است.

به زبان ساده فایروال یک برنامه یا قطعه سخت افزاری است که در محل اتصال شبکه شما به اینترنت قرار می گیرد و اطلاعاتی که میان رایانه شما و اینترنت ردوبدل می شود کنترل می کند،مثلا فرض کنید که شبکه شما بدون استفاده از فایروال به اینترنت وصل می شود،در این صورت هر کسی می تواند به هر یک از رایانه های دست یابد و آنرا وارسی و جستجو کند و با آن اتصال FTP یاTelNet برقرار کند،درآن صورت فکرش را بکنید که شبکه شما چه وضعیتی خواهد داشت!؟

ولی با نصب یک فایروال در محل مناسب اوضاع کامل عوض می شود ،در این صورت شما می توانید با تنظیم فیلترهای فایروال،قوانین موردنظرتان را روی شبکه اعمال کنیدو تعیین کنید که کاربران شبکه به چه سایتهایی می توانند متصل شوند

واجازه دارند چه فایل هـایی را بـه اینترنـت بفرسـتند و یـا دریافـت کنند،بـدین ترتیـب براحتی می توان شبکه را با نصب یک فایرول خوب در محل مناسب مدیریت کرد.

TCP/IP

شماره IP یک نشـانی 4 بـایتی اسـت کـه در حقیقـت نشـانی هـر رایانـه در شـبکه محسوب می شود؛

این پروتکل اینترنت وظیفه انتقـال الکترونیک بسته های اطلاعاتی شـبکه را بـه شـماره هـــای IP موردنظر در شبکه را دارد.

TCP مسئول چک و نظارت کردن انتقال صحیح بسته های اطلاعاتی از مبدا بـه مقصـد که همان IP ها می باشد تا اگر مشکلی در میان را افتاد مشکل را رفع کند تـا اطلاعـات را دوباره ارسال شوند.

به طور کلی TCP/IP به قوانین و قراردادهای موجود در شبکه اینترنت برای دریافت یـا ارســال اطلاعــات گفتــه مــی شــود و در حقیقـت اینترنــت از پروتکـل یــا قــرارداد کاربردی TCP/IP استفاده می کند.

IP Port

تمام وسایل و تجهیزات جانبی رایانه برای برقـراری ارتبـاط و ردوبـدل اطلاعـات بین رایانه و خود بوسیله قسمتی کوچک در خود رایانـه متصـل هسـتند اسـتفاده مـی کنند که به آن دراصطلاح رایانه پورت (Port) می گویند.

هر رایانهی عموما دو پورت سریال دارد که در بیشتر موارد یکی به ماوس و دیگری احتمالا به یک دستگا مودم خارجی وصل می شود،همچنین اسکنرها ،چابگرها نیز از طریق پورت موازی به رایانه وصل می شوند.امروزه در رایانههای جدیداز 2تا6 پورت USB[1] استفتده می شود؛دوربین های دیجیتالی،ماوس،صفحه کلید،اسکنر،WebCam و بیشتر تجهیزات جانبی رایانه برای اتصال به رایانه از پورت USB استفاده می کنند.

اینها همه پورت های سخت افزاری یا بهتر بگوییم پورت های فیزیکی رایانه هستند؛اما به واقع امر هر رایانه علاوه بر پورتهای سخت افزاری یا فیزیکی،دارا ی 65535 پورت مجازی نرم افزاری می باشد که می توانند به عنوان کانالی برای ارتباط با دنیای خارج استفاده شوند.

این قبیل پورت های مجازی عموما به سه دسته تقسیم می شوند که عبارتنداز:

دسته اول:

پورت هایی باشماره های 0تا1023 هستند که قبلا سرویسی خاص برای آن تعریف شده بود،برای مثال :پرونتکل FTP که انتقال فایل ها را بر روی شبکه جهانی

[1] یکی از پورت های ورودی و خروجی رایانه می باشد ، در واقع usp نوعی دیگر از پورهای سریال با سرعت نقل و انتقال اطلاعات بالاتر بین وسیله جانبی و رایانه می باشد .

اینترنت و پروتکل HTTP که به انتقال صفحات وب در اینترنت اختصاص دارند به ترتیب از پورت های 21و80 استفاده می کنند.

دسته دوم:پورت هایی می باشند از شماره 1024 تا 49151 هستند که به هیچ سرویس یا پروتکل خاصی اختصاص ندارند،بلکه عموما تمامی برنامه های تحت شبکه مثل مرورگرهایی چون: Intetnet Explorer یا برنامه های مدیریت پست الکترونیک رایانه نظیر OutLook Express یا هر برنامه ی دیگری ازاین دسته بطور تصادف از پورتی ار این محدوده را انتخاب کرده و برای برقراری ارتباط با دنیای خارج استفاده می کنند؛در حقیقت اگراین محدوده از پورتهای مجازی بر روی رایانهها وجود نداشت،شما هرگز نمی توانستید در محیط وب گردش و سیر کنید،یا اینکه پیام های پستی الکترونیکی دریافتی ا از جعبه ی پستی خود به روی رایانهتان منتقل کنید و آنها را بازبینی و یا بخوانید.

دسته سوم:

پورت هایی با شماره 46151تا65535 هستند که غالبا توسط Trojan ها یا اسب تروا‌ها مورد استفاده قرا گرفته و به مصارف دیگری می رسند؛در واقع این دسته از پورتها شاهراه ورود نفوذگران مختلف به رایانه می باشد.البته در موارد خاصی هم بعضی از شرکت ها در محصولات و تکنولوژی های جدید خود از این پورت ها استفاده می کنند،برای مثال:SVN پورت های PRC خود را از شماره 32768 آغاز می کند

فصل سوم

معرفی و بررسی چند نرم افزار ویژه هک

در حال حاضر نرم افرارهای گوناگون و متعددی در زمینه ی هک از سوی شرکت های مختلف نرم افزاری ارائه شده است که معروف ترین و پرکاربردترین این گونه نرم افزارها به صورت ذیل می باشد.

NetBus **Sub7**

Back Orifice **Deep Back Orifice**

Hack Attack **Net Sphere**

از آنجا که معرفی تمامی این نرم افزارها طولانی و خارج از بحث بوده ،فقط به معرفی و بررسی سه مورد ازمشهورترین و پر کاربرد ترین آنها می پردازیم.

NetBus

آشنایی ومعرفی NetBus

NetBus در سال 1998 توسط یک برنامه نویس سوئدی به نام Cerd Fredrik Neikter نوشته شد؛ولی از این نرم افزار برای سربه سر گذاشتن دوستان خود و شوخی با آنان استفاده می کرد.دیری نگذشت که این نرم افزار در میان بسیاری از کاربران

اینترنت پخش گشته وموردااستفاده قرار گرفت تا امروز که یکی از مشهورترین نرم افزارهای هک وب به حساب می آید.

تاکنون 10 نسخه متفاوت از NetBus عرضه شده که بر روی ویندوز های 2000,ME,NT,98,95 کارمی کند.همچون بسیاری از نرم افزارهای هک NetBus یک فایل اجرایی سرور هک دارد که باید بر روی رایانه قربانی نصب شود.

در نسخه 1.7 این نرم افزار،این فایل در حالت پیش فرض Path.exe نام داشته و حدود 470KB هم حجم دارد،فایل اجرایی Client نسخه NetBus 1.7 که قرار است شما آنرا روی رایانه خود اجرا کنید و از طریق آن رایانه قربانی را مورد هدف قراردهید NetBus.exe نام داشته و حدود 585KB حجم دارد.

معرفی قابلیت های NetBus

- بازوبسته کردن درب CD-Drive برای یکبار یا در بازه های زمانی مشخص.
- به نمایش درآوردن هر تصویری با پسوند BMP یاJPG در رایانه قربانی.
- جابه جا کردن عمکرد دکمه های چپ و راست ماوس در رایانه قربانی.
- اجرا کردن هر نوع فایل صوتی دلخوا ه با پسوند Wave در رایانه قربانی.
- هدایت اشاره گرماوس فرد قربانی به موقعیت دلخواه بر روب مانیتور رایانهش.
- به نمایش درآوردن پیغامی بر روی صفحه نمایش رایانه قربانی جهت ارسال و دریافت پیامهای دیگر.

◄ Shut down کردن یاخاموش کردن رایانه قربانی یـا Log Off کـردن آن فـرد قربـانی اشتراک کاربریش از روی شبکه.

◄ باز کردن پنجره مرورگر پیش فرض رایانه که اکثرا Internet Explorer است و نمایش صفحه وب تحت آدرس سایت خاصی.

◄ ارسال ضربه کلیدهایی به رایانـه قربـانی،برای مثـال در صـورتی کـه فـرد قربـانی برنامه واژه پرداز Word را باز کرده باشد،شما می توانید از راه دور مـتن خـود را در داخل این پنجره فعال تاپ کنید.

◄ دریافت ضربه کلیدهای به رایانه قربانی،شما با این روش می توانیـد کلمـات عبـور (Password) رایانه قربانی را کشف و پیدا کنید.

◄ دریافت محتویات صفحه نمـایش رایانـه قربانی؛بـا ایـن روش مثـل دوربـین مخفـی جاسازی شده است، تا محتوات صفحه نمایش را نشان دهد.

◄ دریافت اطلاعات درباره رایانه قربانی.

◄ امکان Upload کردن و نشاندن هر فایلی از رایانه شما به روی رایانه قربانی.

◄ اضافه یا کم کردن میزان صدای بلنگوی رایانه قربانی.

◄ ضبط کردن صدای اتاق رایانه قربانی از طریق میکروفن متصل به رایانه.

◄ درآوردن صدای کلید ماوس با هر بار زدن کلیدی از صفحه کلید رایانه قربانی.

◄ حذف،اضافه و تغییر فایلی در رایانه قربانی.

◄ غیر فعال کردن کلیدهایی از صفحه کلید رایانه قربانی .

◄ به نمایش درآوردن و بستن هر پنجره اینترنت بر روی رایانه قربانی.

◄ امکان خواندن کلمات عبور(Password)ذخیره شده در حافظه ی نهان رایانه قربانی.

◄ اجازه دادن به IPهای خاصی برای برقراری اتصال.

◄ چاپ کردن یک یا چند فایل بر روی چاپگر رایانه قربانی.

◄ زمان بندی کردن برنامه هایی که قرار است پشت سرهم در رایانه قربانی اجرا شود.

◄ گپ یا گفتگو زدن(Chat)با سرور بصورت بلادرنگ و همزمان.

◄ و...

Back Orifice

آشنایی با Back Orifice

Back Orifice توسط گروهی که خود را The Cult Of The Dead Cow می نامند برنامه ریزی شد و در سال 1998 برای استفاده همگان در اینترنت منتشر شد.

درطراحی Back Orifice که اصطلاحا BO نیز نامیده می شود، آشکار ساختن خلاء و حفره های امنیتی سیستم عاملهایی نظیر ویندوز(Windows)از شرکت مایکروسافت را به خوبی انجام می دهد.خطرناکترن نسخه این نرم افزار هک تا این لحظه زمانی Back Orifice 2000 یا مختصرا BO2K است که بر روی ویندوز های 2000,ME,NT,98,95 کارمی کند.همچون بسیاری از نرم افزارهای هک Back Orifice یک فایل اجرایی سرور هک دارد که باید بر روی رایانه قربانی نصب شود.

در نسخه BO2K این نرم افزار،این فایل در حالت پیش فرض UMGR32.EXE نـام دارد و حدود 122 KB حجم دارد،فایل اجرایی Client[1] درنسخه BO2K که قرار است شما آنـرا روی رایانـــه خـــود اجـــرا کنیـــد و از طریـــق آن رایانـــه قربـــانی را مـــورد هـــدف قراردهیدBO2KGUI.EXE نام داشته و حدود 175KB حجم دارد.

Back Orifice همچـون NetBus اغلـب بـه بیشـتر بازیهـای رایگـان، فایلهـای موزیـک از نوع:MP3، عکسهای زیبا رایگان بر روی اینترنت پیوند زده شده و پس از اجـرا کـردن فایل اصلی به طور کاملا مخفی و پنهانی بدون اینکه از خود اثری بر جـای بگـذارد بـر روی رایانه قربانی نصب می شود.

همچنـین از آنجاییکـهBack Orifice اسـتفاده کـردن از هـر پـورتی را بـر روی رایانـه داردحتی پورت های HTTP و FTP)بنابراین براحتی مـی توانـد اغلـب دیوارهـای آتـش (Fire Wall)را فریب داده و از آنها بگذرد.

معرفی قابلیت های Back Orifice 2000

◄ ارسال و دریافت ضـربه کلیـدها(Keystroke)بـرای مثـال شـما مـی توانیـد از طریـق خواندن کلیدهای رایانهقربـانی کلمـات عبـوری (Password)وی را بـرای وارد شـدن بـه اشتراک(Account)پست الکترونیک را کشف وپیدا کنید.

◄ قابلیت انتقال و مرور سیستم فایل HTTP .

[1] رایانه یا نرم افزار دریافت کننده اطلاعات در هر شبکه ای را سرویس گیرنده یا Client گویند.

◄ در دست گرفتن مدیریت ویژگی اشتراک فایل و چاپگر (File and Print Saring) در صورت فعال کردن این ویژگی حتی با پاک کردن BO2K از روی رایانه هم قادر خواهد بود که تا به تمامی محتویات درایوهای رایانه دسترسی داشته باشد.

◄ امکان ویرایش مستقیم Registry (رجیستری)ویندوز از راه دور.

◄ قابلیت مدیریت، تبادل و مرور کردن رایانه فایل از راه دور.

◄ قابلیت توسعه عملکردها و قابلیتهای سرور هک با اضافه کردن Plug-in از راه دور.

◄ قابلیت ارتقا، نصب، ویا از نصب خارج کردن BO2K از راه دور.

◄ دسترسی به برنامه های همراه کنسول مثل TelNet.

◄ امکان نمایش اعلانات وپیامها به شکل گرافیکی.

◄ امکان راه اندازی مجدد رایانه (Reset)از راه دور.

◄ قابلیت نمایان ساختن DNS

◄ و...

Sub7

آشنایی با Sub7

Sub7 (Sub Seven) توسط شخصی بنام Mobman طراحی و نوشته شده است و تاکنون 18 نسخه از این نرم افزار هک عرضه شده. خطرناکترن نسخه این نرم افزارهک رایانه تا این لحظه Sub7 2.2 که بر روی تمای ویندوزها کارمی

کند.همچون بسیاری از نرم افزارهای هک Sub7 یک فایل اجرایی سرور هک دارد که باید بر روی رایانه قربانی نصب شود.

در نسخه 2.2 این نرم افزار،این فایل می تواند هر اسمی به خود بگیرد اما در حالت پیش فرض Server.exe,rundll.exe,Systemtry.dll نام دارد و حدود 328 KB حجم دارد،علاوه بر فایلی که در دایرکتوری اصلی ویندوز قرار می گیرد،فایل دومی نیز با هر اسم دلخواهی یا در حالت پیش فرض بایکی از اسامی زیر و حجم تقریبی 35KB در داخل دایرکتوری سیستم قرار می گیرد C:\Windows\System\ Windows\system\

nodll.exe---MVKH-32.dll ---facpnmcfee.dll--watching.dll

معرفی قابلیت های Sub7

امروزه Sub7 یکی از قدرتمندترین و توامندترین نرم افزارهای ویژه هک می باشد زیرا قابلیت های انجام کار فراوانی را دارد که ما در ادامه به تعدادی از آنها اشاره می کنیم

◄ تغییر دادن درجه وضوح(Resolation) صفحه نمایش رایانه قربانی.

◄ کسب اطلاع از وضعیت Online فرد قربانی از طریق یرایانه نامه پست الکترونیک(E-mail) یا پیامی د ر ICQ .

◄ مشاهده تمامی فرایندهای که بر روی رایانه در خال اجرا هستند، حتی اگر فرایند مخفی اجرا شده یاشد، فاش خواهد شد..

◄ چاپ کردن متن یا فایلی بر روی چابگر رایانه قربانی.

◄ ویرایش Registry(رجیستری) ویندوز رایانه قربانی از راه دور.

◄ برخورداری از ویژگی جستجوی فایل های موردنظر در رایانه قربانی.

◄ خاموش و روشن کردن هریک از چراغ هـای کلیـدهای Caps Lock, Scorll Lock, Num Lock بر روی صفحه کلید رایانه قربانی

◄ قطع کردن اتصال فرد قربانی به اینترنت .

◄ امکان مشاهده آنچه بر روی مانیتور رایانه قربانی به نمایش درمی آید.

◄ معکوس کردن ،دوران کردن و آینـه ای سـاختن محتویـات صـفحه نمـایش رایانـه قربانی.

◄ پنهان و نهـان سـاختن آیکـون هـای موجـود بـر روی Desktop (دسـکتاپ) رایانـه قربانی.

◄ استفاده از سرور FTP برای Download و upload کردن فایل ها در رایانه قربانی.

◄ باز کردن کادر متنی بر روی Desktop (دسکتاپ) رایانه قربانی و گپ زدن اجبـاری با فرد قربانی

◄ فعال یا غیر فعال کردن عملکرد دکمه های Ctrl+Alt+Delete در رایانه قربانی.

◄ تایپ کردن در داخل کادرها و پنجـره هـایی کـه بـر روی دسـکتاپ ویـندوز رایانـه قربانی.

◄ باز کردن مرورگر پیش فرض رایانه قربانی و رفتن به صفحات خـاص مـدنظر هـک است

◄ پنهان و نهان ساختن دکمه شروع و نوار وظیفه(Task bar) دسکتاپ ویندوز رایانه قربانی.

◄ از کار انداختن صفحه کلید رایانه قربانی بطور کامل .

◄ ضبط کردن صدا از طریق میکروفن متصل به رایانه قربانی و بعد پخش آن.

◄ خاموش و روشن کردن بلندگوی رایانه قربانی.

◄ شروع بکار کردن مجدد(Reset) ویندوز رایانه قربانی.

◄ روشن کردن Webcam رایانه قربانی و مشاهده آنچه که در معرض دید دوربین قرار دارد.

◄ باز و بسته کردن درب CD-Rom.

◄ اضافه کردن وکاستن به دنباله اشاره گر ماوس.

◄ کار با پنجره های باز شده بر روی دسکتاپ رایانه قربانی برای مثال:بستن یک پنجره خاص،فعال یا غیر فعال کردن یک پنجره، فعال یا غیر فعال کردن بستن(Close) یک پنجره،نهان یا پنهان ساختن یک پنجره خاص.

◄ دریافت لیستی از تمامی درایوهای موجود بر روی رایانه قربانی .

◄ خاموش و روشن کردن صفحه نمایش رایانه قربانی.

◄ دریافت اطلاعاتی در باره رایانه قربانی نظیر:نسخه ویندوز،نام کابری،نام شرکت،درجه وضوح نمایش و غیره.

◄ خواندن ضربه کلید های رایانه قربانی چه در وضعیت Online وختی در وضعیت Offline .

◄ دریافت تمامی کلمات عبور(Password) ذخیره شده بر روی حافظه نهان (Cache) رایانه قربانی.

◄ و...

فصل چهارم

معرفی و آموزش نرم افزار امنیتی Zone Alarm Pro

معرفی نرم افزار Zone Alarm Pro

Zone Alarm Pro یک نرم افزار امنیتی و حفاظتی رایانه در برابر نفوذ گران و هکران می باشد و با هوشیاری تمام از رایانه شما در مقابل نفوذ گران و برنامه های trojanمخفی شده در سیستم مقابله می کند ، کوکی ها (Cookies) و تبلیغات ظاهر شونده در مرور گر را بلوکه می کند . این نرم افزار امنیتی چهار عمل مهم را انجام می دهد :

1 _ نصب ، پیکر بندی و مدیریت یک فایروال (د یوار ایمنی یا آتش)

2 _ نظارت دقیق بر دستیابی نرم افزارهای رایانه به اینترنت

3_ کنترل کوکی ها (Cookies) و بلوکه کردن تبلیغات

4_ امکاناتی برای قرنتینه کردن پیوست های خطرناک و ویروسی نامه های الکترونیکی

نحوه اجرا و نصب برنا مه :

پس از کلیک کردن بر روی آیکن برنامه ی نصب و پس از باز شدن پنجره خوش آمد گویی ، نام کاربری و آدرس پست الکترونیک خود را وارد نمایید . البته در پایین همین پنجره دو عبارت وجود دارد که توسط خود برنامه علامت گذاری شده است؛ مضنون گزینه اول این است که : اگر در این برنامه ثبت نام کنید ، خواهید توانست برنامه های ضمیمه و کمکی را از شبکه دریافت کنید ،اما چون پرداخت وجه فقط از طریق حساب اینترنتی میسر است و این مسئله ممکن است برای همه افرادی که در ایران از این برنامه استفاده می کنند امکان پذیر نباشد بهتر است این گزینه را غیر فعال کنید .

علامت دار بودن گزینه دوم این امکان را به شما می دهد که اخبار جدیدی در خصوص نسخه های جدید برنا مه و اطلاعات دیگر را به طور خودکار از طریق اینترنت در یافت کنید .اگردرقسمت قبلا درصندوق پستی را درست وارد کرده باشید تمامی اخبار به آدرس پستی شما ارسال می شود سپس با زدن کلید Next برنامه را دنبال کرده تا به پنجره configure your browser نام دارد بوسیله این برنامه برای ساده تر کردن کار شما ، می تواند نوع مرور گرتان را تشخیص داده و خود را از نظر امنیتی با آن تطبیق دهد ،بنابراین بهتراست علامت این قسمت را بر ندارید ، بعد از این مرحله برنامه شروع به نصب درمرحله که شما مشخص کرده اید می کند . پس از نصب پنجره ای باز می شود از شما می خواهد که به پرسش های آن پاسخ دهید . این پرسش شامل: نوع

ارتباط شما با اینترنت ، طریقه آشنا یی شما با این نرم افزار ، تعداد رایانههای استفاده شده و غیره می باشد . توجه داشته باشید حتما باید به سه پرسش اول پاسخ دهید در غیر این صورت ، برنامه از حا لت نصب خارج می شود .

پس از انجام مراحل فوق ، برنا مه طی 7 مرحله به صورت تصویری ، توضیحا ت مختصری در مورد نحوه کار کرد نرم افزار نمایش می دهد . پس از آن برنامه اجرا شده و از شما درخواست راه انداری مجدد رایانه را می کند که بهتر است به آن پاسخ مثبت دهید ، پس از وارد شدن مجدد به ویندوز ، برنامه آیکن خود را به نوار وظیفه قرار می دهد .

معرفی و آموزش کلیدهای اصلی برنامه

پنجره اصلی شامل شش کلید ا ست که با قسمت ساده و جامع خود که کار را برای کاربران بسیار ساده کرده است .

از این قسمت ، نحوه راه اندازی برنامه شروع می شود و در مورد آن و تک تک کلید ها توضیح خواهیم داد.

دکمه Stop

این د کمه در قسمت اصلی برنا مه، امکان قطع کلیه ارتباطات رایانه با شبکه را می دهد و می توان در صورت لزوم ، با فشردن این دکمه ، ارتباط رایانه را با تمامی

اعضای شبکه قطع کرد . در این حا لت علامت قفل به صورت بسته در مـی آیـد و ایـن حاکی مسدود و قطع ارتباط شدن رایانه است .

دکمه Alerts

در صورتی که رایانهی بخواهد با رایانه شما ارتباط بر قرار کند ، ایـن بخـش ، بـا بـاز کردن چند پنجره ، به شما پیغام می دهد که کدام IP در خواست ارتبـاط بـر روی کـدام درگاه را دارد .تمامی این پیغام ها برروی یک فایلی که امکـان بـازبینی و دسترسـی بـه آن وجود دارد ثبت می شود و شما می توانید در این قسمت پیغام ها را باز بینی کـرده و آنها را پاک کنید و یا مسیر فایل توضیح را تغییر دهید و یا اصلا از برنا مه بخواهیـد که در صورت مشاهده ارتباط هیچ گونه پنجره یا پیغامی به شما نما یش ندهد.

دکمه Lock:

این کلید وضعیت جاری تماس اینترنت شما را نشا ن می دهـد شـما مـی توانیـد بـا فعال کردن قسمت ترتیبی دهید که اگر مثلا بیش از 10 دقیقه از اینترنـت اسـتفاده کنیـد برنامه به صورت خودکار حالت قطع ارتباط را فعال کند .

دکمه Security:

توسط این دکمه می توان شبکه داخلی را تعریف کرد و برای اعضـای آن امکانـا ت خاصی قائل شد . در واقع سطوح امنیتی در این نرم افزار بـر روی دو شـبکه داخلـی و سراسری بطور مجزا تعریف می شوند. لذا می توان امکا نات خاصی را بـرای اعضـای شبکه تعریف کرد که برای عموم قدغن وممنوع است . مثلا استفاده از چابگر شبکه و یا

فایل ها و فهرست ها و برنامه های به اشتراک گذاشته را می توان در شبکه داخلی مجاز کرد ولی در سطح شبکه سراسری مجاز ندانست . برای هر یک از دو شبکه داخلی و سراسری به سطح امنیتی High(بالا)،Medium(متوسط)وlow(کم)تعریف شده است .

در سطح امنیتی Low ، محدودیت در اجرای برنامه ها رعایت می شود و رایانه شما توسط دیگر اعضای شبکه قابل مشاهده است . اشتراک فایل ها ، هارد دیسک ها و چاپگرها بلوکه نمی شود و رایانه های خارج از شبکه مورد نظر هم می توانند از فایل هارد دیسک شبکه استفاده کنند و بالعکس .

در سطح امنیت متوسط یا Medium ، رایانه شما توسط سایر اعضای شبکه قابل رؤیت است اما اشتراک فایل ها ، هارد دیسک و چاپگرها فقط برای اعضای شبکه قابل استفاده است و نه برای رایانه های خارج از شبکه ، در این سطح امنیتی قفل خودکار که تمامی درگاهها را بلوکه می کند نیز وجود دارد .

در سطح امنیت بالا یا High رایانه شما در حا لت خفا به سر می برد ، یعنی از د ید سا یر اعضای شبکه مخفی است و تمام درگاههای آزاد آن ، درگاهها یی که در حال حاضر توسط یک برنامه در حال استفاده نیستند بلوکه می شود .

این سطح امنیتی تنها زما نی یک درگاه را باز می کند که یک برنامه ی مجاز به آن نیاز داشته با شد . طبق پیش فرض برنامه ، سطح امنیتی شبکه داخلی ، در حا لت Medium و سطح امنیتی شبکه سراسری یا اینترنت در حا لت High قرار دارد . شما با توجه به

حساسیت و نوع فعا لیت خود می توانید با بالا و پایین بردن یک انتخا بگر، هر سطحی که مایل هستید ، انتخاب کنید . همچنین به کمک د کمه Security می توانید از برنامه بخواهید که تمامی پیوست ها و پیغام ها ی الکترونیکی را کنترل کند تا دارای VB Script های مخرب نباشد . این قسمت بسیار مهم و مفید است و در قسمت پا یین همین پنجره با عنوان mailsate email protection قابل دسترسی است.

دکمه Programs :

هر برنامه ای که بخواهد برای اولین بار با شبکه ارتباط برقرار کند ، باید دارای مجوز باشد و نام آن در این قسمت آمده باشد . در زمان درخواست ارتباط هر برنامه باشید که به شما اعلام می شود که چه برنامه ای می خواهد به شبکه وارد شود و شما می توانید یک اجازه دائم یا موقت به آن برنامه بدهید . شما می توانید اجازه را محدود به شبکه سراسری یا محلی کنید . با زدن علامت چک مارک سبز رنگ ، به برنامه این مجوز را می دهید که بدون سؤال از شما در هر زمان بتوانید با شبکه ارتباط داشته باشید . با زدن علامت ضربدر قرمز ، شما مجوز ارتباط با شبکه را از برنامه مورد نظر می گیرید ، تا وقتی که در مورد این تصمیم تجدید نظر کنید . با زدن علامت سؤال (؟) سبز رنگ ، شما مجوز ورود را مشروط به کسب اجازه ی خودتان بلا مانع می کنید . یعنی هر گاه برنامه ای که لیست این قسمت وجود دارد خواست با اینترنت ارتباط برقرار کنند ابتدا از شما سؤال می کند در صورتی که با پاسخ مثبت

شما مواجه شود ، می تواند از این دروازه ی مستحکم و امنیتی عبور کند و با اینترنت ارتباط برقرار کند .

دکمه Configure :

توسط این دکمه می توانید تنظیمات مربوط به اینکه آیا این نرم افزار با هر بار بالا آمدن سیستم اجرا شود یا خیر . فعال یا غیر فعال کنید . اگر شما عضوی از یک شبکه داخلی نیستید ، بهتر است از اجرا شدن این برنامه در هر بار بالا آمدن سیستم جلوگیری کنید و در عوض با زدن یک میانبر به روی دسکتاپ خود ، هر بار که خواستید وارد اینترنت شوید ابتدا آن را اجرا کرده ، سپس اقدام به شماره گیری کنید.

از دیگر نکات جا لب این برنامه ،آیکن آن دو نوار وظیفه ویندوز است که دارای دو قسمت سبز و قرمز است که در زمان Online بودن فعال می شود ، قسمت سبز نشان دهنده ی اطلاعاتی است که به رایانه شما download می شود مثلا موقع باز شدن یک سا یت توسط مرورگر ، شما می توانید حرکت چراغ های سبز را ببنید و قسمت قرمز رنگ نشانگر اطلاعاتی هستند که توسط بعضی از برنامه ها از رایانه شما خارج می شوند ، مثل Cookie که با ورود خود اطلاعاتی را از رایانه و کاربر برای سایتی که قبلا کاربر ثبت نام و فرم اطلاعاتی پر کرده است می فرستد ، مثلا با هر بار اتصال به سایت Yahooمی توانید در خواست برنامه را برای مجوز خروج اطلاعات ببیند که البته با توجه به نوع این نرم افزار که خود یک دیوار آتش (Fire Wall) است و با تنظیمات زیادش ، نگران این موضوع نباشید.

آشنایی با مفا هیم پایه و اساسی اینترنت :

اینترنت

اینترنت از لحاظ فیزیکی، تعداد زیادی رایانه محلی است که بوسیله ی خطوط کابلی نوری ماهواره ای سیمی (مدام و غیر مدام) به هم متصل شده اند و به یک زبان یا قرار داد مشترک با هم ارتباط برقرار می کنند .این قرارداد به نام TCP\IP پروتکل کنترل انتقال پروتکل اینترنت موسوم است .

در این الگو اساسا اختلافی با دیگر انواع شبکه های کامپوتری ما نند شبکه ی رایانهی یونیکس مرجود در دانشگاه یا هر رایانه شخصی متصل به هم وجود ندارد.

همین که دو یا چند رایانه با یک زبان مشترک ارتباط برقرار کنند کافی است تا بتوانند به رد و بدل اطلاعات بپردازند و این همان اساس پیدایش اینترنت است یعنی تبادل اطلاعات .

به عبارت دیگر اینترنت یک جامعه بین المللی است که از اتصال رایانه های در اندازه شکل و فرم های مختلف بوجود آمده است.

اینترنت گسترده ترین تلاش دسته جمعی است که بدون همکاری و مشارکت داوطلبانه هزاران نفر در سراسر جهان ابدا قادر به ادامه حیاتش نیست.محور اصلی در اینترنت

ارتباطات است و انتقال نظرات و تجربیات و هر چیز دیگر وسیله است به سوی این هدف.

بطور کلی در یک کلام اینترنت مجموعه ای از هزاران شبکه رایانهی دهها هزار رایانه و بیش از ده میلیون کاربر است که همگی از واسطه ی سازگار جهت ارتباط برقرار کردن با یکدیگر و تبادل داده های دیجیتال استفاده می کنند .

کار برد های اینترنت

عمده کاربردهای اینترنت را می توان به صورت ذیل نام برد:

- مبادله پیام و ارسال أن (E-mail)
- گفتگو با افراد مختلف (Chat)
- شرکت در کنفرانس های گروه های خبری
- مطالعه اخبار
- کاوش در کتابخا نه ها اینترنتی
- خرید کالاهای مورد نیاز
- گرفتن نرم افزارهای رایانهی
- مطالعه مجلات و روز نامه ها
- دیدن از موزه ها و دیگر مکان ها
- تما شای تلویزیون و گوش دادن به رادیو

- بدست آوردن اطلاعات در زمینه های متفاوت
- بازی , سر گرمی و...

سرویس های مهم و کاربری اینترنت :

عمده سرویس های محلی و کار برد های اینترنتی بدین نام است:

- ♦ (www) وب جها نی
- ♦ FTP
- ♦ گروه های پستی (Maling lists)
- ♦ TelNet(تل نت)
- ♦ Archie (آرجی)
- ♦ Gopher (گوفر)
- ♦ Veronica(ورونیکا)
- ♦ Usenet(یوزنت)
- ♦ Finger (فینگر)
- ♦ قابلیت مکالمه یا Talk
- ♦ قابلیت مکالمه دسته جمعی یا IRC
- ♦ WAIS (ویز)
- ♦ Web Directory (فهرست وب)

♦ Motor Engine (موتور جستجوگر)

Word Wide Web (www)

آن چیزی که مردم عادی به نام اینترنت می شناسند. تنها یکی از سرویس هایی اینترنت یا به عبارتی پر طرفدارترین سرویس اینترنت به نام سرویس وب جهانی (www) می باشد .

وب جدیدترین ابزار روی اینترنت است که با سرعت زیادی در حال رشد می باشد وب ابزاری است مبنی بر Hypertext که به شما اجازه می دهد تا به اطلاعات مورد نظرتان از طریق جستجو بر مبنای کلمات کلیدی دستیابی کنید . آنچه www را تا این حد قدرتمند ساخته است .ایده ارتباط گسترده متون یا همان Hypertext می باشد .

Hypertext به یک سیستم گفته می شود که ارتباطی Click-And-Pointبین اطلاعات ایجاد کرده یعنی به استفاده کننده اجازه می دهد که یک منبع اطلاعاتی به منبع اطلاعات دیگری تنها با اشاره کردن به آن و فعال نمودن اش با ماوس منتقل گردد برای مثال: در حالی که مشغول مطالعه اطلاعاتی هستید متوجه می شوید که بعضی از کلمات یا عبارت به شیوه ی مخصوص معیین و یبان شده اند ،شما می توانید از www بخواهید که به یکی از مداخل لطلاعات وارد شوید،بدین صورت www اطلاعات موجود و مرتبط با این کلمه را در سراسر شبکه در اختیار شما می گذارد،بلاخره به دنبال ارتباط منطق داده ها ،شما از نقطه ای به نقطه ی دیگر حرکت خواهید کرد.در این سیستم تمام مراحل و مسائل تکنیکی حرکت بین رایانهها و منابع

مختلف از چشم کاربر مخفی می ماند و کاربر براحتی و بدون دغدغه به جستجو می پردازد.

وجه تسمیه این ابزار اینترنت که در لغت به معنای تارعنکبوتی است که در سرتاسر جهان گسترده شده است که آن است که پرونده هایی که در رایانه های مختلف قرار گرفته اند . به گونه ای از طریق ابر پیوندها با یکدیگر مرتبط شده و مجموعه ای درهم تنیده تشکیل داده اند به هنگام استفاده از وب از لحاظ دسترسی هیچ تفاوتی با یکدیگر ندارد و گونه ای به یکدیگر مرتبط شده اند که هزاران نقطه دیگر بر روی اینترنت نیز ب همین شکل قابل بازیابی هست این نکته تدبیری دیگری از توزیعی بودن اطلاعات میزبان آن وب می باشد .

پست الکترونیک (E-mail)

مخفف کلمات Electornic Mail است و به سرویسی در شبکه اینترنت گفته می شود که به وسیله آن افراد می تواند برای یکدیگر در نقاط مختلف دنیا پیام , ارسال یا دریافت کند.این سرویس عمل پست را بصورت الکترونیکی و از طریق شبکه اینترنت انجام می دهد .

پست الکترونیک یا E_ mail زیر بنای آن چیزی است که در اینترنت انجام می گیرد،به عبارت دیگر سرویس ساده ای است که به دو نفر اجازه می دهد تا پیامشان را در یک زمان بسیار کوتاه به هم برسانند، تمام امکاناتی که برای ارسال یک پیغام الکترونیکی لازم دارید عبارتند از: یک رایانه،یک توع اتصال به اینترنت و نرم افزاری

برای این کار طراحی شده است مانند(OutLook,Edura) بـرای اینکـه مطـالبی اعـم از فایل نوشتاری،تصویری،صوتی و حتی ویدوئی برای مخاطب خود بفرستید کافیست تـا نشانی الکترونیکی اورا بدانید،واضح است که شما مطالبی را که مـی فرسـتید بصـورت دجیتال تبدیل شده باشد, زیرا ایت تنها قالب است که رایانه می تواننـد آنـرا بفهمد،البتـه خود نرم افزار پست الکترونیک مطالب شـما را بـدون هـیچ نگرانـی و مشـکل بـه قالـب دیجیتال تبدیل می کند.البته با پست الکترونیک ارسال پیام محدود به یک نفر نیست بلکه می توان پیام را برای تعداد زیادی از مخاطبان مورد نظر فرستاد و به پیام خود یک یـا جند فایل صوتی یا تصویری ضمیمه کرد.

کاربران برای تبادل پیـام در شـبکه اینترنـت نیـاز بـه یـک آدرس صـندوق پسـت الکترونیکی دارند، این آدرس منحصـربه فـرد و غیـر تکـراری بـوده ومیـان علامـت ات ساین @ قرار میگیرد

مانند Borna66@yahoo.com قسمت اول آدرس های پسـت الکترونیکـی نشـان دهنده ی نام کاریر و قسمت دوم آن بیانگر نام سـرویس دهنـده پسـت الکترونیـک مـی باشد.

گروهای پستی (Mailing Lists)

یک گروه پستی، یک سیستم سازمان یافتـه مـی باشـد کـه در آن افـراد عضـو مـی توانند به یکدیگر پیام هایی درباره یک موضوع خاص ارسال کنند که البتـه پیـام هـا در چارچوب موضوعات مصوب گروه پستی است.پیام ها می تواننـد مقاله،پیشـنهاد،یا هـر

چیز متناسب با گروه باشد.شما می توانید با یک دستورارسال،پیام خود را به افراد گروه ارسال کنید،همچنین شما میتوانید از طریق فرستادن پیامی به آدرس خادم یک گروه پستی به عضویت آن گروه درآیید یا عضویت خود در آن گروه را لغو کنید و یا حتی برای فرستادن آرشیو پیام های رد وبدل شده در روز وماهای گذشته را از خادم درخواست کنید.

نمونه از این گروه های پستی می توان به گروهای پستی در موضوعات علمی،تجاری،ورزشی،خبری و اقتصادی نام برد که خادم گروه اطلاعات به روز هر یک از موضوعات فوق را برای کلیه افراد عضو ارسال می کند.

TelNet(تل نت)

اصطلاحی است که به وارد شدن از راه دور اطلاق می شود و ابزاری است که دسترسی وکنترل رایانهی را در اینترنت ممکن می سازد.با این قابلیتها شما می توانید وارد رایانه دیگری شوید و از نرم افزار آن رایانه استفاده کنید.این سرویس بیشتر برای جستجو در اطلاعات آرشیوی بانکهای اطلاعاتی همگانی یا منابع کتابخانه ای مورد استفاده قرار می گیرد.اکثر شبکه ها در اینترنت از طریق یک حساب رایانهی مخصوص میهمان،به تمام افراد اجازه ورود می دهند،بعنوان مثال: در ایالات متحده آمریکا سیستمی وجود دارد که گزارشی از وضعیت آب وهوای تمام نقاط کشور را در اختیار کاربران می گذارد،هر شخصی می تواند به این سیستم وارد شده و از وضعیت آب و هوای منطقه ی خود اطلاع یابد.

.شما همچنین می توانید با استفاده TelNet از هر رایانهی متصل به اینترنت وارد رایانه خودتان شوید،برای مثال:وقتی شما در کنفرانس در شهر دیگری شرکت دارید ،می توانید با هر رایانه متصل به اینترنت وارد حساب رایانهی (Account) اینترنت خود شده پیغام ها الکترونیکی خود را بررسی و بازبینی کنید.

FTP

پروتکل انتقال پرونده (File Transfer Protocol) یا FTP به ابزاری در اینترنت گفته می شود که به شما اجازه می دهد که فایلی را از جایی به جای دیگر منتقل کنید .فایل شامل هر نوع اطلاعات دیجیتالی از قبیل:متن ساده،تصویر، یک کار هنری ، فیلم، صوت و نرم افزار (برنامه رایانهی) می باشد.هر چیزی که شما بتوانید در رایانهتان نگهداری کنید را می توان با FTP انتقال داد، رایانههای زیادی در اینترنت وجود دارند که آرشیوهای FTPهمگانی داشته و اطلاعات متنوعی را در معرض استفاده عموم قرار می دهند و شما می توانید با تایپ شناسه (Anonymous) ناشناس بدون اینکه کد یا کلمه خاصی را نیاز داشته باشید ، به چنین رایانههایی دستیابی داشته و به عنوان یک کاربرتازه کار اینترنت از اطلاعات مفیدFTP ناشناس استفاده کنید و آنها را بر روی رایانه خودتان کپی وذخیره کنید

Archie(آرچی)

هزاران خادمFTP به طور ناشناس حجم وسیعی از فایل ها را در سرتاسر دنیا ارائه می کنند.نقش خادم های Archie ارائه سیسنم مدیریتی است تا شما را در مسیر پیدا کردن آنچه که نیاز دارید کمک نماید.مثلا فرض کنید که شما دنبال فایلی هستید که مطلبی درباره آن شنیده اید اما از آدر آن بی خبر هستید.با استفاده از سرویس Archie می توانید نام سایت های FTP را که دارنده این فایل می باشند پیدا کنید.اگر شما دنیای FTP را کتابخانه عظیمی در پهنه کره زمین که مدام در حال تغییر می باشد در نظر بگیرید،Archie مانند کاتالوگ های این کتابها خواهد بود.مطمئنا بدون خادم هایArchie اکثر منابع FTP دنیا پنهان و غیر قابل دسترس خواهد ماند.

نامArchie از ایده خادمهای بایگانی Archive Server اقتباس شده است.برخلاف ایده ای که در بکارگیری رایانهها متداول می باشد؛ ما معمولا بهArchie مانند یک شخصیت انسانی نگاه می کنیم.مثلا شما ممکن است از کسی سئوال کنید که کدام سایت FTP حامل اخبار الکترونیکی Uplastic News می باشد دوست شما پاسخ می دهد:مطمئن نیستم، چرا از Archie نمی پرسی ؟ سرویس Archie هم با TelNet و هم با E-mail قابل دستیابی است.همچنین با نرم افزارهای موجود دیگر چون Gopher (در ادامه توضیح داده می شود) و یا وب که می توانید برای استفاده از اینترنت روی رایانهتان نصب کنید، نیز می توان به Archie دست یافت .Archie ابزار خوبی است برای پیدا کردن محل فایلی که یک قسمت یا تمامی نام آنرا میدانید.

Gopher (گوفر)

گوفر از یک سری فهرست ها ی پیاپی تشکیل شده است که به واسطه آن بـه کلیـه اطلاعات دستیابی خواهید داشت.گوفرهای بسیاری در سرتاسر اینترنـت وجـود دارنـد که به صورت محلی اداره می شوند و هر یک شامل لطلاعاتی است کـه اعضـای محلـی آن تصمیم به ارائه ی آن مـی گیرنـد، در حـالی کـه بعضـی از سیسـتم هـای گـوفر بـه صورت مستقل عمل می کنند، اکثـر گوفرهـای موجـود مـی تواننـد بـه دیگـر گوفرهـای اینترنت متصـل شـوند.یرای مثـال فـرض کنیـد شـما در حـال اسـتفاده ار گـوفر مرکـز تحقیقات فیزیک نظری هستید و روبه روی خود یک صفحه فهرسـت سـاده را مشـاهده می کنید.تنها با استفاده از کلیدهای مکانما شما می توانید به گوفر دیگری در اروپـا تـا جنوب آمریکا وصل شوید.

آنچه گوفر را یک ابزار قدرتمند می سازد،این است که بدون توجه بـه اینکـه شـما از کدامین گوفر استفاده می کنید یا اینکه با چه نوع اطلاعاتی سروکار دارید، همواره رابـط شما یک سیستم فهرست ساده می باشد.

گوفر ابتدا در دانشگاه مینوسوتا آمریکا به عنوان یک سیستم اطلاعـاتی در محـدوده ی دانشـگاه بوجـود آمـد، امـا سـریعا توسـط افـراد مختلـف بـرای انتشـار اطلاعـات و سازماندهی منابع شبکه مورد استفاده قرار گرفت و در مدت کوتاهی متداول و همه گیر شد.

Veronica(ورونیکا) : هیچ کس نمی تواند چند گوفر روی شبگه وجود دارد ، فقط می دانیم که تعداد آنها بسیار زیاد است و هر کدام از طریق یک سری فهرست ساده ،انبوهی از اطلاعات و سرویس های مختلف را ارایه می کند .

Veronica ابزاری است که محتوی بسیاری از فهرست گوفرهای موجود را نگه داری می کند .توسط Veronicaشما می توانید تمام عنوان فهرستها یی را که شامل کلمه یا کلمات انتخابی شما هستند ،جستجو کنید . روند کار بدین صورت است که شما کلمه یا رشته کلماتی را که مایلید جستجو دوباره روی آن ها صورت گیرد را در محل مخصوص تایپ می کنید و شروع جستجو را تایید می کنید . نتیجه لیستی از عناوین که کلمه یا کلمات مورد نظر را در بردارد . با انتخاب هر عنوان ، شما به طور خودکار به گوفر مناسب جهت کسب اطلاعات بیشتر وصل خواهید شد و شگفت آور اینکه تا زمانی که خود مایل نبا شید ، شما نمی دانید که به کدامین کشور متصل هستید یا از کدامین رایانه استفاده می کنید.

Usent (یوزنت)

Usenet یک تابلو اعلانات الکتریکی عمومی است که از اینترنت به عنوان وسیله انتقال خود استفاده می کند . از هزاران گروه مو ضوعی تشکیل شده و شما می توانید با اشتراک در این گروه ها در جریان بحث ها و اخبار این گروهها قرار گیرید . پیغامی که به یک گروه خبری فرستاده می شود ، می تواند خوانده شده و به افرادی دیگر

برای مطا لعه منتقل می شود و یا پیغامی پیرو آن به همه مشترکان فرستاده می شود . به یک سری پیغام با موضوع مشابه the read گفته می شود .

با گذشت چند سال گروههای خبری زیادی به شکل کامل سازماندهی و بازبینی شده و بر اساس اصولی روی چارچوب بحث ها و اهداف گروهها توافق حا صل شده است . این مطا لب که FAQ[1] نا میده می شوند ، سعی می کنند با سؤالاتی که در ذهن یک فرد تازه وارده مطرح می شود ، پا سخ گویند تا از جوابگویی به سؤالات تکراری در گروه اجتناب گردد . ابزار بسیار خوبی برای متخصصان علوم می با شد. از آن جا که پایه Usenet از مجموعه افراد فوق شکل می گیرد لذا این گروه ها با متخصصان جهان در رشته های مختلف نیز در ارتباط هستند . بنابراین جای مناسبی برای گرفتن پاسخ سؤالات و یا آگاهی از موضوع عای روز در تمام سطوح و رشته های علمی از آسیب شناسی تا هواشنا سی می باشد .

در هرسا یت اینترنت ، مدیر شبکه تعیین می کند که تا چه حد سیستم می تواند بار گروه های خبری را تحمل کند . پس استفاده از Usenet همه جا امکان پذیر نیست و حتی لزومی ندارد سایت ها یی که این گروه ها را ارایه می دهند تمام آن ها را در اختیار کاربران خود قرار دهند .

---

1 مخفف Freguenriy Asked Question ((پرسش های مطرح شده)) می باشد . بیشتر اوقات تازه واردهای یک گروه خبری پرسش هایی مطرح می کنند که قدیمی ها با آنها را شنیده اند ، FAQ در خواص زمانی مشخص پرسش ها را می کند تا تعداد پرسش های اضافی را کاهش دهد

Finger(فینگر)

اکثر رایانه های اینترنت ، سیستم ها یی را کـه جهـت کسـب اطلاعـات دربـاره یـک کاربر خاص را ارایه می کنند .این سرویس ها به نام Finger شناخته می شود . همـان گونه که خواهید دید در محیط اینترنت مردم با نـام شناسـه کـاربر خـود شـناخته مـی شوند و شما خواهید توانست برای دستیا بی به نـام شخصـی کـه ورای ایـن شـنا سـه کـاربر قـرار دارد از تسـهیلات Finger اسـتفاده کنیـد . بسـته بـه اینکـه چـه نـوعی از سرویس Finger روی کامپوتر شما نصب شده باشـد ، شـما مـی توانیـد بـه اطلاعـات دیگری درباره شخص مورد نظر دسترسی داشـته باشـید . اطلاعـاتی از قبیـل شـماره تلفن ، آدرس محل کار و ... حتی بعضی از ایـن سـرویس هـا بـه شـما مـی گوینـد کـه شخص مورد نظر در چه تاریخ و ساعتی برای آخرین بار با رایانـه خـود کـار کـرده و آیا پیام الکترونیکی خوانده نشده دارد یا نه .

این موضوع می تواند در موارد بسـیاری کارسـاز واقـع شـود. همچنـین شـما مـی توانید به دلخواه خود قسمتی از اطلاعات را که موقع استفاده در مورد شنا سـه کـاربر شما مشاهده می شود تغییر دهید . به عنوان مثال یک استاد دانشگاه می توانـد سـاعات کار خود را در این قسمت قرار دهد تا کلیه افراد با اعمال Finger به شناسه را به جـای استفاده در مورد یک شناسه استفاده در مورد یک شناسه به یک رایانه اعمال کنید . در این حا لت ، آن رایانه لیستی از تمام شناسه کاربرها یی را که در آن لحظه مشغول کار با رایانه هستند نشان می دهد ودر نهایت اینکه بعضی از سیسـتم هـا از Finger بـرای

جواب دادن یک سری درخواستهای معین استفاده می کنند برای مثال در دانشگاه واشنگتن واقع در سیاتل در آمریکا یک شناسه مخصوص وجود دارد که شما می توانید برای آگاهی از زمین لرزه های اخیر از اعمال Finger به این شناسه استفاده نما ید گفتنی است که این کاربرد Finger روز به روز متداول می شود.

قابلیت مکا لمه یا Talk :

امکان مکا لمه ارتباط مستقیمی بین رایانه شما و رایانه دیگری بر قرار می کند . در این حالت شما قادر به مکالمه از طریق اینترنت خواهید بود .مطلب قابل توجه در اینجا آن است که هر چند هم که دو نفر از بعد مکانی به یکدیگر دور با شند ، قابلیت مکالمه برای رایانه های آن ها وجود دارد . پس از برقرار شدن ارتباط و ورود به محیط مکالمه شخص نشا نی آنچه را که شما تایپ می کنید تقریبا در همان لحظه می بینید و هر دوی شما می توانید پیام های خودتان را بدون آنکه مخلوط شوند ، در نیمی از صفحه که به شما تعلق می یا بد وارد نما یید.

قابلیت مکا لمه دسته جمعی یا IRC :

قابلیت مکالمه گروهی امکان مکالمه را برای چند نفر به طور همزمان بر قرار می کند . همان طور که حدس می زنید استفاده **IRC** [1] به مراتب بیش از مکا لمات ساده دو

[1] : شبکه ارائه کننده گان خدمات Chat بوده در سراسر دنیا قرار دارد هر سروری که متصل به شبکه ات ، برای کاربران اضافی پیلم محاوره بلاورنگ را فراهم می نمود پیغام کاربر توسط سایر اعضای آن کانال بلافاضله ملاحضه می شود .

نفری می باشد . شما می توانید در مکالمه های عمومی با گروه زیادی از مردم شرکت کنید . این گونه مکالمات اغلب پیرامون ایده ها یا عناوین مختلف روی می دهد گاهی اوقات از **IRC** برای مکا لمات خصوصی نیز استفاده می شود که این مورد بیشتر شبیه یک کنفرانس از راه دور می باشد .

WAIS(ویز)

WAIS مخفف Wide Area Information Services می با شد و تلفظ آن ویز می باشد . سرویس دهندگان WAIS روش دیگری را برای دستیابی به اطلاعات اینترنت مهیا می کنند .WAIS قادر است به تعداد بسیار زیادی از بانکهای اطلاعاتی دستیابی داشته باشد . در ابتدا تعیین می نما ید که جستجو در کدامیک از بانکهای اطلاعاتی صورت گیرد پس کلمات کلیدی را در اختیار WAISمی گذارید و تمام کلمات را در مقالات کلیه بانکهای اطلاعا تی که معین کرده اید ، جستجو می نما ید .

محصول جستجوی WAIS لیستی از مقالات خواهد بود که از بانکهای اطلاعاتی مختلفی جمع آوری شده است .WAIS این مقالات را فهرست وار به ترتیب از بیشترین تعداد رویداد کلید واژه ها نمایش می دهد. از طریق این لیست شما می توانید از WAIS بخواهید تا مقا له مورد علاقه شما را نما یش دهد .

آشنایی بر برخی از اصطلاحات کاربردی اینترنت

Web directory (فهرست وب)

وب سایتهای بزرگی هستند که اطلاعات روی آنها بوسیله یک سری افراد خاصی جمع آوری شده و حاوی نشانی تعداد زیادی از سایت های اینترنتی بصورت طبقه بندی شده هستند، سایت یا هو یکی از اولین و پرکاربردترین دایرکتوری یا رمز اینترنت هست .

Search Engine (موتور جسنوجوکر)

موتور جستجو برنامه ای است که می تواند داده های خاص که توسط کاربر وارد می شود را در یک پایگاه داده های عظیم جستجو کند و نتایج جستجو را برای کاربر به نمایش بگذارد .

موتورهای جستجو بلعکس دایرکتوری ها به وسیله ی افراد خاصی تهیه نمی شوند ، بلکه توسط برنامه های رایانه ای مشخص که سعی در جمع آوری همه ی اطلاعات روی اینترنت دارند ، اما چگونه می تواند نشانی همه یا قسمت اعظم سایت های اینترنت را جمع آوری کند . کلید دنیای مجازی اینترنت لینک های موجود در صفحات اینترنتی

می باشد که به عنوان شناسه ی برای برنامه های جستجو که مورد استفاده قرار می گیرند .

سایت های مثل یاهو(Yahoo) و آلتاویستا(Altavista) جزء اولین سایت هایی بودند که خدمات موتور جستجو را ارائه می کردند، اما پاسخ های آنها دقیق نبود و گهگاه باعث سردردگمی در کاربران می شد، در همین حال دو دانشجوی دکترای دانشگاه استفورد آمریکا به هنگام کارکردن روی پایان نامه خود به فکر ساختن موتور جستجوی جدید افتادند که امروزه آن را گوگل (Google) می نمایم که یکی از مشهورترین سایت های اینترنت در این دهه می باشند .

Web Site (وب سایت)

یک پایگاه اطلاعاتی نرم افزاری است که بر روی یک سرویس دهنده اینترنت (server)[1] قرار دارد و کاربران می توانند از آن اطلاعات استفاده نمایند . مانند وب سایت صداوسیما که اطلاعاتی در مورد فعالیت های این سازمان در اختیار کاربران قرار می دهد . http://www.irib.com/

web Page (صفحه وب)

وقتی با وب سایت تماس می گیرد تا از اطلاعات آن استفاده نمایید . اطلاعات اصلی سرویس دهنده آن سایت بر روی صفحه نمایش رایانه نمایش داده می شود .این

[1] در محیط شبکه رایانه ای که به دیگر کاربران شبکه خدمات مختلفی ارائه می کند؛ به عبارت دیگر ارسال کننده ی اطلاعات برای سرویس گیرندگان می باشد.

صفحه اطلاعات خاص را صفحه وب گویند در نتیجه تمامی صفحاتی که در مراجعه به سایت های گوناگون مشاهده می کنید و قبلا به آن صفحه اینترنت می گوئیم ، صفحه وب گویند.

Web Browser(مرور گر وب)

برای انجام هر عملی با استفاده از رایانه نیاز به نرم افزار خاصی می باشد. نرم افزار مشاهده و استفاده از صفحات وب را web browser می گویند. از معروف ترین نرم افزار های مرورگر اینترنت می توان Internet Explorer و Netscape Navigator رانام برد سایر مرورگرها عبارتنداز: Opera-Mozila -Mosaic

Online/ Offline

هنگامی که رایانه شما دارای یک ارتباط زنده و باز به اینترنت است و می توانید از آن برای انجام کاری در اینترنت استفاده کنید اصطلاحا گفته می شود که شما (کامپیوتان) Online هستید. اما هنگامی که ارتباط اینترنت قطع می شود شما Offline می باشید.

Update

شبکه اینترنت شامل میلیون ها صفحه وب در انواع موضوعات می باشد که هر کدام از این صفحات نیز دارای اطلاعاتی خاص می باشد. اما چنانچه این اطلاعات همواره ثابت بوده و هیچ نگرش مجدد و تغییری بر روی آنها صورت نگیرد.در هر زمان به مطالبی کهنه و قدیمی تبدیل می شوند که هیچ استفاده کنندهای ندارد . در

نتیجه این اطلاعات باید همواره جدید و تازه کردند که اصطلاحا این عمل به روز رسانی یا Updateگویند. نمونه بارز آن Update صفحات اخبار می باشد که هر روز مطالب آن تغییر کرده و جدید می شوند. واژه Up to date نیز به همین مفهوم است.

Link (پیوند)

یک لینک یا پیوند به یک شی در صفحه وب است که شما را به قسمت دیگری از همان صفحات یا صفحه دیگری متصل می کند. پیوند ها معمولا با رنگ خاصی ظاهر می شوند و مشخصه آنها که پیکان ماوس بر روی آنها به شکل دست کوچکی در می آیند. یک Link می تواند به صورت یک کلمه یک عبارت چند کلمه ای و یا یک تصویر باشد.

URL

مخفف عبارت (Unifrom Resource Locator)می باشد و عبارت است از نام رسمی قالب آدرسی که به مرورگروب می دهد تا شما را به آن سایت متصل کند. URL همانندآدرس وب سایت است، اما شامل نوع پرونکل نیز می باشد.

روش ذخیره سازی اطلاعات در رایانه سرویس دهنده را پروتکل نامیده می شود . به عنوان مثال در ذیل به URL متفاوت به ترتیب از پروتکل های http. Gpher. ftp استفاده می کنند. آمده شده است:

http://www.irib.ir

ftp://ftp.winsite.edu

gopher://gopher.asbsite.com

Download

عمل کپی یا ذخیره کردن یک فایل رایانهی از یک سرویس دهنده(Server) از طریق شبکه اینترنت بر روی رایانه شما را دانلود گویند، به نحوی که آن فایل کاملا در اختیار شما بوده و بتوانید از آن استفاده کنید. مثل اینکه آنرا از یک دیسکت یا سی دی روی رایانه تان کپی باشید.

درواقع همواره در حال بار گذاری می باشید زیرا وقتی صفحه ی وبی را باز می کنید فایل های آن صفحه بطور موقتی از سرویس دهنده به رایانه شما کپی می شوند. اما منظور از download نوع آگاهانه ترآن است یعنی خود شما به دنبال بارگذاری یک فایل از سرویس دهنده باشید .

Upload

عکس حالت download می باشد یعنی زمانی که شما فایلی را از رایانهتان برای یک سرویس دهنده ی وب از طریق شبکه ارسال کنید Upload گویند .

در این عرصه زندگی با رشد روز افزون دانش و تکنولوژی در زمینه های مختلف علمی به خصوص در زمینه ی علم و صنعت رایانه مواجه هستیم و با افزایش نیاز مندی های جامعه به این علم و فناوری برای انجام امور مختلف پس باید جامعه بستر مناسبی و ایده آل را برای افراد و کاربران جامعه آماده و مهیا کند تا آنها بتوانند در انجام امور کاری خود با تیکه بر علم و دانش خود با سهولت و سرعت بیشتر همت گمارند. البته باید علم و دانش عمومی کاربران باید به حدی باشد که توانایی درک و استنباط مفاهیم و اصول پایه و اساس آن علم را داشته باشند. تا همگام و هم قدم با پیشرفت علم و دانش آنها در زندگی روزمره اشان رشد و نمو کنند .

اما یکی از فناوری های بسیار جالب و روبه رشد امروز دنیای مجازی و شبکه جهانی اینترنت می باشد که دنیای وسیع و انبوه اطلاعات و گوناگون در زمینه های مختلف علمی می باشد. اما کاربران جامعه باید نحوه بکار گیری درست و مناسب از این ابزار جهانی را بطور قابل روشنی درک و بیاموزند و از جنبه های مثبت و

کاربردی این منبع جهانی دانش و فناوری روز در زمینه های کاری مختلف استفاده و بهره ببرند.

"" که در تحقیق به معرفی و توضیح کاربردهای مختلف اینترنت و سرویس های مهم و کاربردی اینترنت پرداختیم.""

اما در هر زمینه ی علمی تعداد عدید ی نفوذ گر و مهاجم وجود دارد که سعی آنها در این است که از رشد و پیشرفت سریع این علم در عرضه جهانی بکاهند و جهت بهبود و افزایش منافع مالی خود اقدامی بلند و نهادینه بگذارند .

در اینترنت مهاجمان و نفوذ گران خطرناکی و مهلکی وجود دارند که در صورت مقابله نکردن با آنها ضرر و زیان های جبران ناپذیر مالی و اطلاعاتی به کاربران وارد می کند. بدین معنی که هر کاربر بعد از آشنایی با آن علم و دانش باید با اصول و راههای مقابله و دفع مهاجمان و نفوذ گران آن علم آشنا و آگاه شدند.

مثلا: بدانند نفوذ گران از چه قسمتی و چگونه به آنان حمله می کنند و چگونه می توانند در مقابل حملات آنان عکس العمل مناسب و درست و به جا را نشان و انجام دهید یعنی منظور این نیست ما با وجود نفوذ گران و مهاجمان سر سخت و خطرناک نمی توانیم از علم و فناوری روز جهان بدرستی استفاده کنیم؛ بلکه ما می توانم با آگاهی و بصیرت از راههای مقابله با این موجودات خطرناکی راه خود را امر حرکت و پیشرفت در مسیر دانش و تکنولوژی همواره و صاف کنیم .

"" که ما در این تحقیق به معرفی و بررسی انواع مهاجمان ونفوذگران اینترنتی و راههای مختلف نفوذ آنها به سیستم های رایانه و روشهای مقابله با آنها پرداختیم.""

به امید آن زمانی که ایران مهد تمدن چند هزار ساله جهان همیشه در مسیر پیشرفت و ترقی علم و دانش و فناوری روز جهان در زمینه های گوناگون علمی باشد .

فهرست منابع و ماخذ

الف) منابع کتبی

نام کتاب :راهنمای جامع اینترنت نویسنده :هارلی هان Harley Han

مترجم :محمدرضا آیت زاده شیرازی محل نشر:تهران ناشر:انتشارات ناقوس

نوبت چاپ :چاپ سوم سال چاپ :تابستان 81 جلد :ج1

صفحه :ص 720

نام کتاب :خودآموز هک با Sub7 نویسنده :اردوان علی اکبری نائینی

مترجم : _____ محل نشر:تهران ناشر:انتشارات خانیزان

نوبت چاپ :چاپ اول سال چاپ : 81 جلد :ج1 صفحه :ص 286

نام کتاب :آموزش سریع اینترنت نویسنده :نئول استابورک Neol Estabrook

مترجم :مهندس علی رضا جباریه محل نشر:تهران ناشر:انتشارات جهان نو

نوبت چاپ :چاپ چهارم سال چاپ :1380 جلد :ج1 صفحه :ص 468

ب)منابع روزنامه و مجلات

1- روزنامه جام جم ضمیمه کاشف

2- روزنامه جام جم ضمیمه کلیک

3- هفته نامه عصر ارتباط

4- هفته نامه عصر شبکه

5- مجله رایانه جوان

6- مجله دانش و رایانه

ج)منابع اینترنتی

1) **http://www.majiconline.com**

1) سایت تحقیقاتی و پژوهشی و آموزشی مجیک آن لاین به بان فارسی

2) **http://www.tebyan.net**

2)سایت علمی و آموزشی و اجتماعی تبیان به زبان فارسی

3) http://www.hideway.net

3)سایت آموزشی و تحقیقاتی هک و هکر به زبان انگلیسی

4) **http://www.internet.com**

4)سایت علمی و پژوهشی مطالب خاص انترنت به زبان انگلیسی