تاریخچه HACKING

در ابتدای تاریخچه HACK افرادی دیده می شوند که «برنامه نویسان واقعی»بودند. واین نـامی بود که خودشان به آن اعتقاد داشتند .آنها همچنان خود را «HACKER» ویـا چیـزی مشـابه آن می نامیدند .واین برنامه نویسان پیش زمینه تـاریخ HACKING را بوجـود آوردنـد.امـا تـاریخ آغـازHACKING رابـه وضـوح میتـوان از سـال 1961 بـه بعـد در نظـر گرفـت **آشـنایی باHACKINGودنیای مهیج HACKER هابا** گسـترش روز افـزون اینترنـت شـاهدیکپارچه شـدن اطلاعات در سراسـر جهـان هسـتیم .بـا پیوسـتن بسـیاری از سـازمانها ،دانشـگاهها و مراکـز تحقیقاتی سرویسهای دولتی و امنیتی به اینترنت ،مسئله امنیت اطلاعـت امـری ضـروری اسـت زمانی بود که اطلاعات در محیطهای بسته ومجتمع، دسترسی افراد به آنها را مشکل وحتـی در بعضی اوقات غیر ممکن می ساخت امابا پیدایش این بزرگراه اطلاعاتی یعنـی اینترنـت ، تمـامی مراکز اطلاعاتی به یکدیگر متصل شدند و از آن زمان بـود کـه دسترسـی بـه اطلاعـات در هـر گوشه دنیا با فشار دادن یک دکمه ممکن شد ولی نباید فراموش کرد که هنوز هم نه تنها مسـئله امنیت اطلاعات برای هرسازمانی به قوت خود باقیست بلکه با بازکردن راههای دسترسی افراد به اطلاعاتشان دارای اهمیت بیشتری شده است.اما این سـازمانها و مراکـز اطلاعـاتی هرگـز از مزایای اطلاعاتی در مقابل این عیب چشم پوشی نکردندو به آن متصل شدند و اکنـون بهتـر از هر زمانی میدانیم که اهمیت اینترنت به قدری است که به آن حتی لقب شاهراه اطلاعـاتی را نیـز اطلاق کرده اند و حقیقتاً نیز چنین است و به جرأت می توان گفت که اگـر روزی ایـن شـاهراه اطلاعتی قطـع شـود صـدمات غیـر قابـل جبرانـی بـه سـازمانهای اطلاعـاتی ،اداری ، تجـاری ، صنعتی، شرکتها و... وارد خواهد شد و بعد از این زمان بود که کلمه ایی تحت عنوانHACKING

به معنای آنچه که امروزه به آن اطلاق میشود به وجود آمد.

HACKING چیست و HACKER هاو CRACKER ها چه کسانی هستند؟

HACKING در لغت به معنی ((دسترسی غیر قانونی یا بدون اجازه به سیستمها می باشد .))اما واقعأنمیتوان مفهومHACKING رادرهمین یک جمله خلاصه کرد باید بیشتر روی این موضوع بحث کنیم .یکی از مشکلات موجود این است که هنوز تعریف استاندارد و مشخصی برای HACKING وجود ندارد و هر کس ، که معمولأخود از HACKER های معروف می باشند بنا به فراخورحال و درک خود تعریفی برای آن ارائه کرده است .

احساس زمانی که شما می دانید در حال دسترسی به سیستمی هستید وصف نشدنی است و HACKING بهترین راه برای امتحان کردن تواناییهایتان د رمقابل کسانی که شاید به این مطلب واقفند که شما توانا تر هستید و سیستم خود را هر چه بیشتر غیر قابل H ACK کردن می نمایند ، می باشد.

اعتقاد براین است که اگر سیستمی را می توان HACK کرد بنابراین افراد حق و این اجازه را دارند که آنرا HACK نمایید ، چرا که حفاظت و امنیت اطلاعات بر مبنای هیچ حقوقی بنا نهاده نشده است .وقتی سیستمی HACK می شود،منظور و مقصود از این کار به هیچوجه آسیب رساندن و دزدیدن چیزی نیست .حقیقت این است که اکثریت HACKERهاحتی ذره ای خرابی به بار نمی آورند.و هزینه امن تر کردن سیستم بعد از حمله یک H ACKERدر مقایسه با هزینه هایی که ممکن است واقعأتوسط حمله یکی از شرکتها ی رقیب صورت بگیرد ،مقداری نا چیز است . در نظر گرفتن این حقیقت که دستیابی چند دانش آموز به یک سیستم غیر حفاظت شده هرگز به بدی حمله توسط یک شرکت حرفه ای نیست ،بسیاری از مسائل را روشن میکند.

کلمه حمله در معناهای متفاوتی استفاده می شود .یک حمله بیشتر مواقع چیزی بیشتر از یک تلاش می تواند موفقیت آمیز یا ناموفق باشد.عمدتا منظور از حمله به هیچ وجه خسارت و خرابی به بار آوردن نیست. همچنین لازم است توجه کنید که به دلیل روابط نادرست بین شرکتها HACK کردن یک HOME PAGE توسط یک شرکت در مقابل صدماتی که HACKER ها ممکن است در هنگام HACK کردن به یک سیستم بزنند چیز ناچیزی است .H ACKING در واقع بهترین روش برای یافتن معایب سیستمها است .بسیاری از HACKER ها معتقدند که اگر افراد مسئول در سیستمها کارشان را به خوبی انجام دهند ،هیچ مشکلی پیش نخواهد آمد.شکایت این افراد از HACKER ها در واقع ناشی از ناآگاهی خودشان است.بنا بر این در سی که HACKERها به صاحبان شرکتها می دهند این است که افراد مسئول را موظف به مراقبت از سیستمها نمایند به جای آنکه دائما از HACKER ها شکایت نمایند ویا کارشان را بدست شانس بسپارند.

وقتی کلمه HACKER به میان می آید ، بیشتر در خصوص افرادی استفاده می شود که از حل مسائل لذت می برند و به محدودیتها غلبه می کنند.یک ار تباط و فرهنگ مشترک از برنامه نویسان حرفه ای و افراد با مهارت در شبکه وجود داردکه تاریخ خود را از چند دهه گذشته تااولین مینی کامپیوترهایTIME-SHIRING و آزمایشات ARPANET جستجو می کند.اعضا این فرهنگ واژه HACKER را به وجود آوردند.HACKERها اینترنت را ساختند.این HACKERها بودند که سیستم عامل یونیکس را به آنچه که امروز می بینیم تبدیل کردند.HACKERها USENET را اجرا می کنند وباعث شدند WWW(WORD WIDE WEB) راه اندازی شود.

ایده HACKER بودن تنها به فرهنگ نرم افزاری HACKER محدود نشده است افرادی هستند که فرهنگ و رفتار HACKER را در شاخه های دیگر بسط داده اند مانند الکترونیک و موزیک.گروه دیگری از افراد هستند که به طور واضح خود را HACKER می نامند، در حالی که نیستند این دسته از افراد گروهی هستند که پس از ورود به سیستمها خرابی به بار می آورند HACKER های واقعی این افراد را CRACKER می نامند وهیچ میلی برای کار کردن با این افراد ندارند .ساده ترین تفاوت میان HACKER ها و HACKER ها این است که: HACKERها باعث استحکام کامپیوتر و سازندگی میشوند ولی CRACKER ها آنها را می شکنند.

خصوصیات ورفتارهای یک HACKER

HACKE ها باعث سازندگی می شوند ومسائل را حل میکنند وبه آزادی و کمک آزادانه دو طرفه اعتقاد دارند.بعضی ها تنها برای اینکه جزء HACKERها باشند این خصوصیت را مد نظر قرار می دهند در حالی که به آنها اعتقاد ندارند و این باعث می شود که هرگز به عنوان یک HACKER مورد قبول قرار نگیرند چرا که اعتقاد داشتن به این مسائل از آنجایی اهمیت پیدا میکند که به آنها کمک می کند یاد بگیرند و باعث ایجاد انگیزه در آنها می شود حال خصوصیاتی چند از HACKER ها را ذکر میکنیم و کسانی که می خواهند به عنوان یک HACKER مورد قبول وارد شوند ،باید آنها را همواره برای خود تکرار کنند:جهان مملو از مسائل جذاب می باشد که منتظر حل شدن هستند.HACKER بودن بسیار سرگرم کننده است اما یک نوع سرگرمی است که نیاز به مرارت و سختی بیش از اندازه دارد.و این سختی نیاز به انگیزه دارد.یک HACKER از حل مسائل وحشت دارد ، بنابراین مهارتهایش را تقویت می کند و تمرین هوش میکند یک HACKER به ظرفیت یادگیری خود اعتماد دارد و عقیده دارد که

هرگز لازم نیست که برای حل یک مسئله به تمام مسائل احاطه داشته باشد و با حل کردن قسمتی از مسئله به اندازه کافی برای حل قسمت بعدی فرا می گیرد و به همین ترتیب ادامه میدهد تا مسئله را به طور کامپیوتري حل نماید.

- هیچ کس نباید یک مسئله را دوبار حل کند اندیشه های خلاق منابع با ارزش و محدودی هستند . آنها نباید برای کشف و حل مجدد چیزهایی تلف شوند که قبلا به همین منظور زمان فکر کردن HACKER های دیگر به یک مسئله بسیار با ارزش خواهد بود بنا بر این برای یک HACKER یک وظیفه خواند بود که اطلاعات خود را در اختیار دیگران قرار دهد تا آنها نیز بتوانند مسائل جدیدتر را حل کنند .

- کسالت وتنبلی ویران کننده است HACKER ها نباید هرگز از حل مسائل کسل و خسته شوند واینطور شوند یعنی اینکه آنها قادر به حل مسائل جدید نیستند .برای مانند یک HACKER رفتار کردن باید اعتقاد داشته باشند که مسائل ومشکلات هر چه بیشتر از سر راه بردارند،نه تنها برای خودشان ، بلکه حتی برای دیگر HACKER ها .

- آزادی خوب است HACKER ها به طور طبیعی ضد سلطه هستند آنها اعتقاد دارند ،هر کس که بتواند به آنها دستور دهد، می تواند آنها را از حل مسائل جالب و دلخواه آنها باز دارد . در صورت وجود سلطه، آنها مجبور هستند که مانند کارفرما خود فکر کنند و نظریات او را دنبال کنند و این نظریات ممکن است مبنای فکری سالمی نداشته باشندو با انجام آنها مسلما از اهداف HACKER ها دور خواهند شد.

- این رفتار و خصوصیات نمی توانند جایگزینی برای توانایی و قابلیت HACKER شدن باشند.برای HACKER بودن باید بیشتر روی این خصوصیات تفکر کرد برای HACKER شدن نیاز به هوش، ممارست، فداکاری و کار سخت می باشد HACKER ها وقتی برای تلف کردن ندارند اما تلاش برای موفق شدن را ستایش می کنند مخصوصا تلاش د رعرصه HACKING ، ولی تلاش در هر زمینه ای خوب است و این موارد برای HACKER شدن بسیار حیاتی هستند.

قوانین HACKING

- هرگز به سیستمی صدمه نزنید و این تنها باعث دردسر شما خواهد شد.
- هرگز فایلهای سیستم ها را تغییر ندهید ، به جزء آنهایی که باعث شناسایی شما میشوند و آنهایی که دسترسی شما به کامپیوتر را در آینده ممکن می سازند .
- هرگز در باره پروژه های HACKING خود هیچ اطلاعاتی در اختیار دیگران به جزء افراد مورد اطمینان قرار ندهید.
- هرگز از یک نام واقعی و شماره تلفن واقعی کسی در هنگام P OST در یک BBS استفاده نکنید.
- هرگز اثری از خود در سیستمی که آن را HACK کرده اید باقی نگذارید.
- هرگز کامپیوتر های دولتی را HACK نکنید.
- هرگز در باره پروژه های HACKING پشت تلفن خانگی صحبت نکنید.

PHREAKINGچیست؟

شـاید در کنـار HACKING و CRACKING بـه کلمـه PHREAKING نیـز بـر خـورده باشـید.« PHREAKING» اصولا عمل HACKING با یک تلفن مـی باشـد. بـا اسـتفاده از جعبـه هـای تلفـن وچند حقه می توان چیزهایی بدست آورد ، که دو مورد از آنها را مـی تـوان ، آگـاهی یـافتن از سیستم تلفنها و تماسهای تلفنی مجانی نام برد اما بیشترین منظـور ا زایـن کـار بدسـت آوردن اطلاعات در باره نلفنها و اجازه دسترسی مجانی به تمام اطلاعات می باشد.

کلاه قرمزی ،کلاه سفید یا کلاه خاکستری ؟

WITH HACK : معمولا به افرادی اطلاق می شود که مخصوصا بـه دلایـل منطقـی و دوسـتانه عمل HACK را انجام میدهند مثل محققان وافراد مشغول به کـار در قسـمت امنیـت شـبکه هـا و غیره.

BLACK HAT : همان هکر های بدجنس هستند که به قصد خرابکاری بـه سیسـتمها دسترسـی می یابند

و کلاه خاکستری ها افراد ی مابین این دو هستند.

چیزهاییکه یک هکر باید بداند

IP:

IP شماره ای است که به هر کامپیوتر متصل به اینتر NET BUS داده میشود تابتوان به کمک آن شماره به آن کامپیوتر ها دسترسی داشت. این عدد برای کامپیوتر هایی که حالت سرور دارند(مثل سایتها) و نیز کامپیوتر های کلاینتی که معمولا به روشی غیر ازشماره گیری (DIAL UP) به اینتر نت وصل هستند،عدد ی ثابت و برا ی دیگران عددی متغییر است مثلا هر بار که با شرکت ISP خود تماس گرفته و به اینترنت وصل میشوید عددی جدید به شما نسبت داده می شود.

آدرس ها ی IP طولشان 32بیت می باشند .از آنجایی که محدود کردن مردم به خواندن و حفظ کردن یک بلوک 32بیتی بسیار مشکل است لذا آدرس های IP به صورت نماد(DOTTED_QUAD) نوشته می شوند نماد DOTTED_QUAD هر کدام از چهار بسته های 8 بیتی ازآدرس IP را به عنوان عددی بین 0.255 که درآدرس IP به فرم W.X.Y.Z مانند10.21.41.3 نتیجه می شود را لیست می کند.

هرکدام از بسته ها ی IP آدرس IP مبداء را با تعریف سیستمی که بسته را می فرستد و آدرس IP مقصد که سیستم مقصد را برای بسته مشخص می سازد شامل می شود.

مثلا ممکن است آدرس شمابه صورت 195.217.172.69 باشد حتی اسمهایی مثل WWW.YAHOO.COM که برای اتصال استفاده می کنید در نهایت باید به یک IP تبدیل شودتاشما سایت YAHOO راببنید .

درIP معمولا XXX اولی معنای خاصی دارد که اگر به روش DIAL UP به اینترنت وصل شوید ،معمولا عددی که به عنوان XXX اولیه می گیرید مابین 192تا223 خواهد بود این توضیح برا ی تشخیص کامپیوتر ها ی کلاینت از سرو ر(حداقل در ایران)بسیار می تواند مفید باشد.

تقسیم بندی آدرس های IP :

آدرس های IP به چندکلاس تقسیم بندی می شوندکه Aتا E نام دارند ولی از این بین ،سه کلاس اول (یعنی A,B,C) کاربرد عملی دارند که به شرح زیر می باشد:

- کلاس A : اگر IP را به صورت XXX.YYY.YYY.YYY درنظر بگیرید، این کلاس تمام IP هایی را شامل میشود که XXX بین ? تا??? است .این کلاس ویژه BACKBONE های بزرگ اینترنتی است و درهنگام ثبت برای گرفتن ازآنها استفاده میشود.
- بنا بر این اکثر سایتها چنین IP هایی دارند .این کلاس را 8/ هم می گویند.
- کلاس B : این کلاس تمام IP هایی را شامل می شود که XXX بین ??? و??? است . این کلاس از جمله کلاسهای پرکاربرد است .این کلاس را 16/ هم میگویند.

- کلاس C : این کلاس تمام IP هایی راشامل می شودکهXXX بین ??? و??? است . این کلاس معمولا به ISP هایی که خدمات DIAL UP ارائه میدهند،تعلق میگرد.بنابراین اگر به صورت DIAL UP به اینترنت متصل شوید ،چنین IP می گیدید.این کلاس را 24/ هم می گویند.

آشنایی با انواع پورتهای فیزیکی و مجاز ی یک کامپیوتر

هر کامپیوتری عموما دو پورت سریال دارد که در بیشتر موارد یکی به ماوس و دیگری احتمالا به یک دستگاه مودم خارجی (EXTERNAL MODEM) وصل می شوند . (البته در مادر بوردهای پنتیوم چهار امروزی موس به پورت USBوصل شده و اکثر مودمها هم از نوع داخلی INTERNAL و در داخل CASE کامپیوتر بر روی شکافهای توسعه از نوع PCI یا ISA نصب می شوند). همچنین اسکنر ها و چاپگر ها نیز از طریق پورت موازی (PARALLEL) به کامپیوتر وصل می شوند .امروزه در کامپیوتر های جدید از 2 تا 6 پورت USB نیز استفاده می شود که می توانند به دوربینهای دیجیتالی ، ماوس ، کیبرد ، WEB کمپ، اسکنر و دستگاه های بسیار دیگری وصل شوند . اینها همه پورتهای سخت افزاری یا بهتر بگوییم فیزیکی کامپیوتر شما هستند.

PORT های مجازی :

هر لایه درTCP/IP اطلاعاتی را درجلوی داده ای که از لایه بالایی می گیرد اضافه میکند. این اطلاعات که به جلوی داده افزوده شده است ،هدر (HEADER) نام دارد وشامل اطلاعات مفیدی برای داده میباشد تا وظیفه اش را انجام دهد.

برنامه کاربردی پیامی را تهیه می کند که می تواندقسمتی از درخواست WEB ،قطعه ای از EMAIL ،ویا سایر داده هایی باشد که می توانند عبور داده شوند.لایه انتقال ، هدری را به این داده می افزاید که احتمالا شامل اطلاعاتی در باره اینکه پیام روی ماشین نهایی به کجا باید برود ،میباشد.

اگر TCP مورد استفاده قرارگیرد، هدر حاصل و المان داده قطعه TCP(TCP SEGMENT) نامیده می شود.قطعه TCP از درون شبکه، جایی که هدر دیگری افزوده می گردد عبور داده می شود.لایه شبکه اطلاعاتی درمورد آدرس مقصد و مبداء را در هدر IP که به پیام افزوده میشود قرار میدهد.پیام حاصل ،IP DATA GRAM نامیده می شود.این بسته به لایه پیوند داده ها و لایه های فیزیکی یعنی جایی که هدربرای ایجاد قاب افزوده می گردد،فرستاده میشود.بنابر این داده میتواند درطول پیوند ارسال شود.

هدرهربسته TCP شامل دو عدد درگاه می باشد .پورت مبداء و پورت مقصد .

این اعداد 16 بیتی همانند درها ی کوچکی برروی سیستم یعنی جایی که داده میتواند فرستاده و یا دریافت شودمیباشد.درگاهها درها ی فیزیکی نیستند.آنها واحدها ی منطقی هستند .65535پورت TCP مختلف روی هر ماشین وجوددارد.پورت صفر TCP رزرو شده و استفاده نمی شود.هر بسته TCP از میان یکی از این درهااز ماشین مبداء بیرون می آید(عددپورت TCP مبداء) وپورت دیگر روی ماشین مقصدمشخص شده است .وقتی که یک برنامه کاربردی سرویس دهنده مبتنی بر TCP روی سیستم کار میکند ،به درگاه خاصی برای بسته های TCP که از یک سرویس گیرنده می آید ،گوش می دهد.به یک پورت با سرویس شنوایی ، پورت باز و به جایی که چیزی برای شنیدن وجودندارد پورت بسته گفته می شود.سرویس دهنده های گوناگون برنامه کاربردی به پورتهای مشهور گوش می دهند.

پورتها یTCP مورد استفاده اغلب به صورت زیر می باشد:

- TCP PORT 21- پروتکل ارسالی فایل (FTP)
- TCP PORT 23- TELNET
- TCP PORT 25- پروتکل ارسالی پستی ساده (SMTP)
- TCP PORT 80- WORD WIDE WEB (HTTP)
- TCP PORT 666- DOOM (... ID بازی از نرم افزار)

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

- دسته اول پورتهای با شماره های از 0 تا 1023 :

که قبلا سرویس خاصی برای آنها تعریف شده است .برای مثال پروتوکل H TTP که به NET BUS انتقال صفحات WEB دارایند این NET BUS اختصاص دارند به ترتیب از پورتهای 21 و 80 استفاده میکنند.

دسته دوم پورتهای با شمارههای از 1024 تا 49151 هستند که به هیچ سرویس یا پروتکل خاصی اختصاص ندارند بلکه عموما تمامی برنامه های تحت شبکه مثل مرور گر هایی چون پویشگر اینتر نت مایکروسافت یا برنامه پست الکترونیکی یا هر برنامه دیگری از این دست بطور تصادفی پورتی از این محدوده را انتخاب کرده و از آن برای برقراری ارتباط با دنیای خار ج استفاده می کنند در حقیقت اگر این محدوده از پورتهای مجازی برروی کامپیوتر ها وجودنمی داشتند شماهرگز نمی توانستید در محیط WEB گردش کرده یا اینکه پیامهای پست الکترونیک د ریافتی رااز روی جعبه پستی خود به روی کامپیوترتان منتقل کرده و آنها را بخوانید.اما مسئله به اینجا ختم نمی شود زیرا بسیاری از TROJANها هم برای HACK کردن کامپیوتر ها از همین محدوده استفاده می کنند از مشهورترین TROJANهای فعلی می توان SUBSEVEN ، NETBUS و BACK ORIFICE اشاره کرد که در حالت پیش گزیده به ترتیب از مجموعه پورتهای :

‹6711و6776›،‹12345و12346›،‹31337› استفاده می شود.

- دسته سوم پورتهای با شماره های 49152و65535 هستند که غالبا توسط TROJANها مورد استفاده قرار گرفته و کمتر به مصارف دیگری می رسند . البته در موارد نادری هم بعضی از شرکتها در محصولات و تکنولوژی خود از آنها استفاده می کنند .

نحـــوه بـدسـت آوردن IP

چگونه می توان آدرسIPای خود را پیدا کرد ؟

برا ی این کار کافیست پس از شماره گیری از طریق خط تلفن(DIAL-UP) و بر قراری اتصالتان به ISPو نهایتا حضور د راینترنت مراحل زیر را دنبال کنید:

1. برروی گزینه RUN در منوی شروع ویندوز کلیک کنید.
2. کادر محاوره ای RUNظاهر می شود .فرمان WINIPCFG را در داخل کادر متن تایپ کرده دکمه OK را کلیک کنید.
3. کادر محاوره ای با عنوان IP CONFIGURATION ظاهر شده ، و آدرس IP فعلی شما در آن اعلام می شود.

چگونه میتوانید آدرس IP ی متناظر با سایت وبی را پیدا کنید ؟

با حضور پیدا کردن هر کامپیوتری د راینتر نت ، آدرسIP منحصر به فردی به آن تعلق می گیرد .از آنجایی که بخاطر سپردن آدرس چهاربخشی عددی I P برای ذهن آدمی کمی دشوار است عموما به جای آن از یک آدرس اسمی یا اصطلاحا آدرس U RL استفاده می شود . برای مثال سایت مشهور یاهو (YAHOO): WWW.YAHOO.COMاست .بطور قطع این آدرس با یک آدرس عددی IP متناظر است که شما به راحتی می تنوانید آنرا پیداکنید .برای این کار راههای بسیاری وجود دارد ،یکی استفاده از برنامه ها ی کمکی و سودمندی است که د رهک کردن کامپیوترها از راه دور استفاده می شوند.

آشنایی و کار با فرمان PING :

پینگ کردن یکی از کارها و دستورات پرکاربرداست بدین معنا که به وسیله ویندوز یا داس یا برنامه دیگر یک بسته کوچک D ATA یا اطلاعات فرستاده می شود . این بسته مانندرادار عمل می کند بدین معنا که وقتی ماIP یا سایتی را پینگ میکنیم رایانه سرعت رفت و برگشت این بسته را حساب می کند وسرعت سرور یا سایت را به ما نشان میدهد. حال مامیتوانیم این بسته ها ی نرمال را آنطور که می خواهیم تغییر دهیم و مثلا برای مودم فرد دستورات دلخواه راارسال کنیم .به عنوان مثال :

مودم را قطع میکند ⟵ +++ ATH

راه دیگر پیدا کردن آدرس عددی IP متناظر با هرآدرس اسمی URLای ، استفاده از فرمان سودمند و مشهور PIN است این فرمان اساسا استفاده های بسیار دیگری به غیراز فقط پیدا کردن آدرس IP دارد .

این فرمان بخشی از پروتکل ICMP(INTERNET CONTROL NESSAGE PROTOCOL) است ککه د راشکال زدایی شبکه هایی که تحت پروتکل TCP/IP کار می کنند مورد استفاده قرار می گیرد.

به زبان ساده تر فرمانی است که شما به کمک آن میتوانید بسته های حاوی اطلاعات یرا به کامپیوتری د ریک شبکه فرستاده و از کامپیوتر مذکور ربخواهید تا در صورت ONLINE بودن د رشبکه ،همان بسته ها یدریافت یحاوی اطلاعات اولیه یا هر جوابیه دیگری را که صلاح می داند برای شما پس فرستاده از این طریق شما را بز وضعیت ONLINE و حضور فعالش در شبکه مطلع سازد .به عبارت دیگر از طریق فرمان PING شما می توانید چک کنید که آیا کامپیوتری در آن لحظه خاص در مخیط شبکه ای حضوری فعال داردیا خیر.

ا زآنجا که اولین گام در HACK کردن هرکامپیوتری در اینترنت کسب اطلاع از وضعیت ONLIN و حضور فعال آن د راینترنت است ،که از این رو فرمان PINGیکی از فرامین کلیدی هکرها به حساب می آید .بدین ترتیب که هکرها ابتدا با اجرای فرمان PING یا اصطلاحا PING کردن به یک کامپیوتر از حضورآن در اینترنت اطمینان حا صل کرده ،سپس افدام به برنامه ریزی برای HACK کردن سیستم قربانی خود می کنند .

شیوه کار فرمان PING که در محیط DOS اجرا میشود اینگونه است که وقتی شما آنرا اجرا می کنید یا همانطور که گفتم اصطلاحا به کامپیوتری PING میکنید ،کامپیوتر شما چهار بسته حاوی اطلاعات را به کامپیوترمورد نظر ارسال کرده و منتظر می ماند تاد رصورت ONLIN بودن کامپیوتر مذکور دراینترنت ،حداقل یکی از بسته های ارسالی برگشت داده شده و دریافت شود.البته د راکثر موارد در صورت ONLIN بودن کامپیوتر را ه دور هر چهار بسته ارسالی بر گشت داده می شوند .

مراحل اجرا ی آن به صورت زیر است :

1. گزینه MS-PROMPT را در زیر پوشه PROGRAMS از منوی شروع انتخاب می کنیم.
2. اتصال خود به اینترنت را بر قرارنموده ،سپس فرمان PING YAHOO.COM را تایپ کرده و کلید ENTER را بفشارید.

چگونه می توانید آدرس IP ی فردی را پیدا کنیم ؟

اولین و ابتدایی ترین گام د رهک کردن کامپیوتردانستن آدرس IP آن است .که در زیر به آنها اشاره می کنیم :

استفاده و کار با فرمان NETSTAT

این فرمان یکی از فرمانهای تحت داس است که شما از طریق آن می توانیدعلاوه بر آدرس IP ی هر کامپیوتر دیگری را از راه دور پیدا کنید .همچنین می توانید پورتهایی که هم اکنون بر روی کامپیوتر مذکور HACK کشده است یا خیر .

فرمان NETSTAT هم مثل هرفرمان تحت DOS دیگری سویچهای بسیاری دارد که عبارتند از:

NETSTAT[-A][-E][-N][-S][-P PROTO][-R][INTERVAL]

کارایی هر یک از این سویچها د رجدول زیر آمده است:

سویچ	کارایی
-A	تمامی پورتهایی که د رو ضعیت شنود به سر میبرند را بهمراه بقیه اتصالات نشان می دهد.
-E	آمار اترنت را نشان می دهد.
-N	آدرسها و اعداد پورتها را به فرم عددی نشان می دهد.
-P PROTO	تمامی اتصالات مربوط به پروتکلی که توسطPROTO مشخص شده را نشان میدهد
-R	تمامی محتویات جدول مسیریابی را نشان می دهد.
-S	آمارهرپروتکل را نشان میدهد .درحالت پیش گزیده آمارپروتکلهای UDP،TCP وهح نشان داده می شوند
- INTERV AL	آمار انتخابی را مجددا به نمایش درمی آورد.

از میان تمامی سویچهای بالا ما از همه بیشتراز سویچ [-N] که در HACK کردن هم کارایی بیشتری دارد استفاده می نماییم

این سویچ برای نمایش دادن آدرسها و اعداد پورتهای باز شده بر روی کامپیوتر مورد استفاده قرار می گیرد .

مراحل استفاده از آن به صورت زیر است :

1. اتصال خود را به اینترنت برقرار کرده سپس یکبار دیگر برروی گزینه MS-DOS PROMPT که درزیر منوی PROGRAM از منوی شروع آمده کلیک کنید.

2. فرمان NETSTAT-N را تایپ کرده و کلید ENTER را بفشارید.البته این کار را پس از وارد شدن به نرم افزار YAHOO MASENGER انجام دهید

در سطر اول عباراتی ظاهر می شود که ابتدا به توضیح آن می پردازیم :

PORT : معرف نام پرو تکلی است که مورد استفاده قرار می گیرد

LOCAL ADDRESS: در این بخش آدرس IP ی کامپیوتر شما ذکر می شود.که شامل آدرس IP و پورت آزاد سیستم را یه شما نمایش می دهد

FOREIGN ADDRESS : در این بخش آدرس IPای کامپیوتر طرف مقابل ذکر می شود.

STATE : دراین بخش وضعیت خط اتصال اعلام می شود.یکاتصال حالات مختلفی می تواند داشته باشد که در جدول زیر آمده است.

وضعیت	به معنای آن است که
CLOSE	هیچ اتصالی میان کامپیوترپسوترشماو کامپیوتر راه دور وجود ندارد
CLOSING	هیچ اتصالی میان کامپیوترپسوترشماو کامپیوتر راه دورهر د و موافق هستند تا این اتصال خاتمه یابد
CLOSE WATE	کامپیوتر راه دور اقدام به بستن اتصالش با شما کرده است
ESTABLISHED	اتصال پایداری برقرار شد ه است
FIN WATE1	نرم افزاری که از این اتصال استفاده می کرده
FIN WATE2	کامپیوتر راه دور نیز موافق بسته شدن این اتصال است
LAST ACK	اتصال منتظر از بین رفتن تمامی بسته های اطلاعات است.
LISTEN	کامپیوتر شما د روضعیت شنود قرار گرفته است تا پذیرای اتصالی از خارج باشد.

SYN RCVD	کامپیوترپیوتدراه دور د رخواست یرا برای برقرار شدن اتصال می فرستد.
SYN SEND	کامپیوترپیو تر شما برای باز شدن اتصالی اقدام کرده است.
TIMED WAIT	همان کارایی LAST ACKرا دارد

پیدا کردن آدرس IP ی کامپیوتر راه دور

- **روش اول : دعوت به گپ زنی از طریق ICQ**

از میان تمام یرنامه های پیام رسان مشهوری نظیر :YAHOO MASANGER و MSN MESENGER نرم افزار ICQ که یکی از پر طرفداراترین نرم افزارهای گپ زنی در سالهای اخیر به حساب می آید و بیش از 110 میلیون کاربر از سراسر دنیا دارد یکی از آندسته پیام رسانهایی است که شما از طریق آن می توانید به را حتی و فوق العاده آسا ن به آدرس IP ی کامپیوتر راه دور و طرف مقابلی که با آن در حال گپ زدن هستید دسترسی پیدا کنید.برای پیدا کردن آدرس IP ی کامپیوترپیوت را ه دوری از این طریق کافیست از فرد مورد نظرتان دعوت تکنید تا در ICQ حضور پیدا کرده و با شما شروع به گپ زدن کند ،سپس در حین گپ زنی فرمان NETSTAT-N را اجرا کرده و آدرس IP ی شخص مذکور را بدست آورید .آزمایش این روش آسان از آنجایی که احتیاج به اطلاعاتی در باره کارکردن با برم افزار ICQ و چگونگی گپ زدن با این نرم افزار چگونگی DOWNLOAD کردن و نصب آن ،قابلیتهای فراوانش که ا زآن جمله می توان به ارسال پیامی از نوع S M S به تلفن ها ی موبایل کشورهای سراسر دنیا اشاره کرد.

- **روش دوم: فرستادن یک فایل یا گپ زنی صوتی (VOICE CHAT) از طریق یک پیام رسان**

بر خلاف نرم افزار ICQ که تنها لا شروع به گپ زنی و اجرای فرمان NETSTAT-N می توان به آدرس IP ی طرف مقابل دست پیدا کرد ،در پیام رسانهای متداول و مشهوری چون MSN MESENGERو YAHOO MESENGER دیگر تنها با گپ زدن نمی توان آدرس IP ی طرفق مقابل را بدست آورد.بلکه لازم است تا ابتدا فایلی را ارسال کرده و یا اینکه یه گپ زنی از طریق صوت پرداخته بعد فرمان NETSTAT را برای پیدا کردن آدرس IP ی طرف مقا بل به اجرا رد آورد .

مراحل زیر را انجام دهید:

1. اتصال خود به اینترنت را بر قرار نموده ،سپس یک یاز برنامه های پیام رسان مثل YAHOO MESENGER را بر روی کامپیوترتان اجرا کرده و از طریق آن شروع به گپ زدن با یکی از دوستان خود کنید .سپس درهمین حین فرمان-NETATATرا اجرا کنید.در ستون FOREIGN ADDRESS به دنبال آدرس IP ی باشید که دوویژکی زیر را دارد:
   - وضعیت اتصال آن ESTABLISHED است.
   - در همان سطر و در زیرستون مخزشم ADDRESS ، آدرس IP ی شما بهمراه پورت باز شده 80 آمده باشد.

در حقیقت زمانی که شما از طریق YAHOO MASENGER با فردی گپ می زنید ، سرور گپ زنی یاهومیان شما و طرف مقابل قرار گرفته و دیگر اجاز دسترسی به آدرس IP ی طرف مقابل را به شما نمیدهد. در چنین مواقعی شما فقط به آدرس IP ی سرور گپ زنی یاهو دسترسی پیدا خواهید کرد. اما زماینکه شما اقدام به انتقال فایلی می کنید دیگر سرور گپ زنی یاهو کنار رفته و ارتباط مستقیم میان شما و فرد مقابل برقرار می شود.

بدین ترتیب است که شما می توانید با برقراری یک ارتباط جدید و مستقیم به آدرس IP ی کامپیوتر طرف مقابل خود دسترسی پیدا کنید.

- **روش سوم: دعوت برای بازدید از یک صفحه WEB**

یکی از مشکلاتی که عمدتا این دسته از هکرها با آن روبرو هستند آتست که طرف مقابل یا اصلا به نرم افزار ICQ دسترسی نداشته و از آن استفاده نمی کند یا اینکه تمایلی از خود برای دریافت فایلی ا زطریق پیام رسانهایی چونYAHOO MESENGER وMSN MESENGER نشان نداده و اصلا درخواست ارسال فایل شما رد می کند زیرا بسیاری تصور میکنند که با رد کردندر خواست دریافت هر گونه فایلی میتوانند خود را ازدست شما خلا ص کنند حال آنکه قضیه به همین جاختم نمی شود،زیرا شما می توانید با ترفند دیگری که از عدم اگاهی اکثر کاربران اینترنت از قابلیتهای یک صفحه WEB ساده نشأت می گیرد. حمله را از جایی دیگر آغاز کنید.شما می توانید در سایت خود یک شمارشگر قرار داده و از کاربر کامپیوتر قربانی بخواهید که به سایت شما سری بزند که دراین صورت شمارشگر صفحه WEB شما IP ی فرد مذکور را اسکن کرده سپس بر طبق قراری که شما در زمان راه اندازی شمارشگر بااو گذاشته اید که مثلا آدرس IP ی تمامی بازدیدکنندگان سایت را به آدرس پست الکترونیکی شما ارسال کندشما نهایتا به آدرس I P ی طرف مقابل خوددسترسی پیدامی کنید.

- **روش چهارم :دریافت نامه پست الکترونیک از طرف مقابل**

درابتدای هر نامه پست الکترونیکی یک سری اطلاعات فنی می آیند که اغلب از سوی بخش عظیمی از کاربران مورد چشم پوشی قرار گرفته وبه آن توجهی نمی شود ،حال آنکه در این بخش اطلاعات بسیار مقیدی را می توان یافت .یکی از این اطلاعات آدرس IP ی فرستنده نامه می باشد.

➢ روش پنجم: استفاده از یک برنامه IP SINFFER

SINFFER برنامه هایی هستند که با نظاره کردن بسته های اطلاعات موجـود د ریـک شـیکه اطلاعات مفیدی را رد اختیار شما قرار میدهندبرای مثـال میتواننـدکلمات عبـور اشـتراکهای کاربری ،اعداد کارتهای اعتباری ،اطلاعات بانکها وعیره را کشف رمز و فـاش کننـد .یکـی از انواع ساده این برنامه ها IP SNIFFER است که وظیفه پیدا کردن آدرسهای IP را با ردگیـری بسته های اطلاعات بر عهده دارد.همچنین برنامه AIM BLACKOUT نیـز بـاخودIP SNIFFER ای را با قابلیتهای بسیار بالایی بهمراه داردکه شما یم توانیدآنها را به خدمت بگیرید.

آشنایی با مفهوم و تاریخچه TROJANها

یکی از راهها ی HACK کردن کامپیوتری از راه دو ر،استفاده کردناز برنامه هـایی بـاعنوان TROJAN HORSES(اسبهای تراوا)است که مختصرا TROJAN (تراوا) نیز نامیده مـی شـوند .اینکه جرا این نوع برنامه ها TROJAN HORSES نامیده می شـوند داسـتان شـنیدنی داردکـه قطعا به شما دردرک بیشتر مسئله کمک خواهد کرد .قضیه از اینجا آغاز می شـودکه در 12 قرن پیش از میلاد دو گروه با عنوان TROY وGREEK به مدت 10 سال با هـم مـی جنگیدنـد ولی هیچ یک موفق به شکست دیگری نمی شدند.این بیشتر از این بابت بود که گـروه TROY صاحب قله هایی بودند که شکست ناپذیر لقـب گرفتـه بـودولی سـرانجام گـروه GREEK بـا بکار بردن حقه ساده ای به قلعه TROY نفوذ کرده وبر آنها مسلط شدند .(درست بـه همـان صورتی که شما قرار است به کامپیوتر قربانی خود نفوذ کرده وبر آن مسلط شوید.)

GREEK ها تندیس فوق العاده بزرگی از چوب به شکل یک اسب ساختند و گروهی از سربازانشان را در آن قرار دادند.سپس این مجسمه غول پیکر را به کمک چرخهایی که د رزیر آن تعبیه کرده بودند تا نزدیکی دربهای قلعه TROY آورده و بعد از آنجا گریختند . TROYها یساده لوح به گمان اینکه این یک هدیه از طرف GREEK ها است پس از فرار آنان مجسمه بزرگ اسب چوبی را به داخل قلعه خود وارد کردند غافل از اینکه د رهنگام شب زبده ترین سربازان GREEK از داخل آن بیرون خواهند آمند و در های قلعه را برای ورود بقیه سربازان GREEKخواهند گشود .دقیقا همین مسئله بر روی کامپیوتر قرباین اتفاق خواهد افتاد .بدین ترتیب که شما فایلی را برای فرد قربانی (همان اسب چوبی غول پیکر را)می فرستید و وی به گمان آنکه این فایل مثلا تصویری از شما یا موزیکی دلتشین است

آنرا بر روی کامپیوترش اجر امی کند.(یعنی همان اسب تراوا را به قلعه خود داخل میکند.) که در اینصورت از این لحظه به بعد هر زمان به محض ورود کامپیوتر قربانی به اینترنت دربهای کامپیوتر وی (همچون دربهای قلعه TROY ها)برروی شما باز خواهد شد و شما این امکان را پیدا خواهید کرد تا هر بلایی که مایل بودید به سر فرد قربانی و کامپیوترش بیاورید.

ساختار برنامه ها یTROJAN HORSE

TROJANها اغلب از سه فایل اجرایی با پسوند EXEتشکیل شده اند.اینها عمومانامهایی نظیرSERVER.EXE،EDITSERVER.EXEوCLIENT.EXE را دارا هستند .

معرفی فایل اجرایی SERVER.EXE

این فایل همان فایلی است که شما بریا فرد قربانی می فرستید تا آنرابر بـروی کـامپیوترش نصب کند.با اجراشدن این فایل بر روی هر کامپیوتر خانگی REJISTRY ویـنـدوز ان مـورد حمله قرار گرفته و تنظیمـات لازمـه بـر روی آن اعمـال مـی شـود.همچنـین بسـته بـه نـوع TROJAN ممکن است در موقعیتهای کلیدی دیگری د رویندوز نظیر : پوشه PROGRAMS یـا دیگر پوشه های سیستمی نیز فایلهایی ذخیره شوند تا کنترل کـامپیوتر قربـاین د راینترنـت دربهایی را بر رو ی کامپیوتروی به بیرون بـاز کننـد.بـه ایـن دربهـا کـه راههـای ارتبـاطی کامپیوتر با دنیای خارج هستنداصطلاحا پورت گفته می شود. دقـت کنیـد کـه ایـن پورتهـا مجازی بوده و با پورتها ی سخت افزاری متفاوت هستند.

معرفی فایل اجرایی EDITSERVER.EXE

برای HACK کـردن کـامپیوتری از راه دور بـه وسـیله یـک TROJAN شـما ابتـدا بایـد فایـل اجرایی سرور HACK مربـوط بـه آن TROJAN را بـر روی کامپیوترقربـانی نصـب و اجـرا کنید.اما همیشه پیش از ارسال کردن فایل اجرایی سرور HACK لازمست که تنظیمات مـورد نظرتان را برروی آن اعمال کنید.

برای این کار عموما از فایل اجرایی دیگری استفاده می شود کـه اغلـب EDITSERVER.EXE نامیده می شود.در حقیقت با اجرا کردن این فایل اجرایی بر روی کامپیوتر خودتـان پنجـره ای باز شده و این اجاره را به شما می دهد تا تمامی گزینه هـا و امکانـات مـورد نظرتـان را درفایل سرور HACK ذخیره کنید.

معرفی فایل اجرایی CLIENT.EXE

شما پس از آنکه سرور HACK مورد نظرتان را به کمک فایل اجرایی EDITSERVER.EXE تنظیم کرده ونهایتا آنرا بر روی کامپیوتر قربانی خود نصب و اجرا کردید،نهایتا نوبت به آن می رسدکه منتظر بمانیدتا کامپیوتر قرباینONLINE شده و بعد حمله خود را آغاز کنید.این حمله که برنامه ریزی آن از طریق کامپیوتر شما صورت میگیرد از طریق فایل اجرایی CLIENT.EXE عملی می شود . در حقیقت وقتی شما این فایل اجرایی را بر روی کامپیوترتان اجرا می کنید پنجره ای باز شده و به شما این امکان را می دهد تا هر بلایی که مایل بودید به سر کامپیوتر قربانی خود بیاورید .

ویژگیهای متداولی که TROJANها دارند

- تعیین نحوه کسب خبر از وضعیت ONLINE کامپیوتر قربانی

برای مثا ل شمامی توایند سرور HACK را به گونه ای تنظیم کنید که به محض ONLIN شدن کامپیوتر قربانی از طریق

دریافت نامه پست الکترونیکی یا پیغام فوری در ICQ یا هر روش دیگری شما از آن مطلع شوید.

- تعیین شماره پورتی برای باز شدن بر روی کامپیوتر قربانی. در اغلب TROJANها شما می توانید سرور HACK را بگونه ای تنظیم کنید که مثلا به محض حضور فرد قرباین در اینترنت پورت خاصی بر روی کامپیوتر وی باز شده و درحالت شنود قرار گیرد .از طریق شما هر زمان که مایل بودید می توانید حمله به کامپیوتر قربانی را آغاز کنید.

- تعیین کلمه عبوری برای دسترسی به کامپیوتر از طریق پورت باز شده .در بعضی از TROJANهای پیشرفته حتی این امکان نیز وجود دارد که شما کلمه عبورر اجهت تنظیم شرور HACK از راه دور تعیین کنید تا این فقط خود شما با شید که امکان دسترسی و اعمال تنظیمات را داشته باشید.

امکاناتی که TROJANها در اختیار ما قرارمی دهند

- امکان دسترسی کامپیوتر به اطلاعات روی دیسک سخت و امکان کپی یا پاک کردن آنها
- امکان دنبال کردن تمامی اعمال شخص در هنگام استفاده از رایانه
- امکان خواندن تمامی پسوردهای ذخیره شده در رایانه هدف
- امکان کنترل برخی از اجزاء رایانه مانندCD ROM
- امکان مدیریت کامپیوترل ویندوز و تغییر آن به صورت دلخواه برای رایانه هدف
- امکان دیدن تمامی CHAT هایی که فرد انجام می دهد

معرفی مشهورترین TROJANها ی دنیا ی WEB

- از آنجایی که هر روز TROJANهای بیشتر و جدیدتری به دنیای هکرها معرفی می شوند ، از این رو همیشه باید سعی کنیداطلاعات خود را بروز نگاه دارید .

- ACKCMD
- CRAZZYNET 3.71
- ALDINO SERVER 0.6
- ARCTIC 6.0
- ACID BATTERY 1.O
- ADMIN.TROJ.KIKZYURASE

همچنین از تروجاها ی مشهور قدیمی نیز می توان به موارد زیر اشاره کرد.

- BACK ORIFICE
- DEEP BACK ORIFIC
- NET BUS
- SUB7
- NET SPHERE
- HACK ATTACK
- EXPLORERZIP TROJAN HORSE

SUBSEVEN

آشنایی با SUB7 :

SUB7 توسط شخصی به نام MOBMANنوشته شد و تا کنون نسخه های2.2,1.0.92.1,1.1,1.2,1.3,1.4,1.5,1.6,1.7,1.8,1.9,2.0, GOLD,2.1 BONUS,2.1 B ازاین TROJAN معرفی شده اند .

خطرناکترین نسخه این TROJAN تا این لحظه SUB7 2.2 است که بررو ینسخه های ویندوز 95و98وMR و NT و2000بخوبی کار می کند.

همچون بسیاری از TROJANها ،SUB7 هم فایل اجرایی سرور هکی دارد که بـر روی کـامپیوتر قربانی نصب می شود.این فایل هر اسمی می تواند داشته با شد اما درحالت پـیش گزیـده یکـی از اسامی SYSTRAY.DLL و RUNDLL16.EXE وSERVER.EXE و یا TASK_BAR.EXE را داشـته ،و حدودا 328 کیلو بایت هم حجم دارد همنچنین عـلا وه بـر فـایلی کـه د ردایرکتـوری اصـلی ویندوز قرارمی گیرد فایل دویم نیز با هر اسم دلخـواهی یـا د رحالـت پـیش گزیـده بـا یکـی از اسامی NODLL.EXE وMVOKH-32.DLL و FAVPNMCFEE.DLL و حجم تقریبی 35 کیلـو بایـت در داخل دایرکتوری \WINDOWS\SYSTEM قرار خواهد گرفت

قابلیتهای SUB7

امروزه SUB7 یکی از توانمندترین TROJANها ی دنیای WEB به SUB7 می آید . زیرا قابلیت انجام کارهای فراوانی را دارد که ما در ادامه به تعدادی از آنها اشاره می کنیم :

- مشاهده تمامی فرایندهایی که برروی کامپیوترد رحال اجراهسـتند(حتـی اگرفراینـد مخفـی اجراشده باشدهم فاش خواهد شد).
- کسب اطلاع ا زوضعیت ONLINE فرد قربانی از طریق د ریافت یک نامه پست الکترونیـک یـا پیامی د رICQ
- روشن کردن WEBCAM کامپیوتر قربانی و مشـاهده آنچـه د رمعـرض دیـد دوربـین قـرار دارد.
- دریافت تمامی کلمات عبور دخیره شده بر روی کامپیوتر و حافظه نهان آن
- خاموش و روشن کردن مانیتور کامپیوتر قربانی
- باز کردن و بستن دربCD-ROM

- ضبط کردن صدا از از طریق میکرو فن متصل به کامپیوتر قربانی و بعد پخش آن
- وارون کردن دوران دادن و آینه ای ساختن محتویات صفحه مانیتور کامپیوتر قربانی

تنظیم سرور SUB7 HACK

1. پس از DOWNLOAD کردن فایل ZIP شده از روی سایت WWW.SHFHACKER.COM و خارج کردن آن از حالت فشرده و زیپ شده به ترتیب اعمال زیر را انجام دهید .
2. برروی EDITSERVER دابل کلیک کند تا کادر محاوره ای .SELECT FI KLHDA NVHDN
3. قویا پیشنهاد می کنم که همیشه بر رو ی عبارت RUN IN NORMAL MODE کلیک کنید تا کاد رمحاوره ای EDIT SERVER به نمایش د رآید.

این کاد راز 8 برگه تشکیل شده که د رستون سمت چپ کادر قرار گرفته اند که با آن تنظیمات مورد نظر را اعمال می نماییم.

4. درحالت پیش گزیده محتویات برگه اول یعنی SERVER SETTING به نمایش د رمی آید .

برگه SERVER SETTING:

PORT

در این بخش شماره پورتی که بر روی کامپیوتر قربانی باز خواهد شد آورده می شود.در حالت پیش گزیده شماره این پورت 27374است .البته شما می توانید هر شماره پورت دیگری که مایل بودید تا از آن استفاده کنید را در این کادر متن تایپ کنید.

PASWORD

در صورت تایپ کلمه عبوری در این بخش ، دیگر استفاده از پورتی که بر روی کامپیوتر قربانی باز می شود تنها محدود به کسانی می شود که این کلمه عبور را می دانند . به عبارت دیگر اگر شخص ثالث یا ه رهکری بخواهد تا با استفاده از برنامه IP SCANNER ای از باز بودن پورتی بر روی کامپیوترپیوتد قربانی شما می توانید استفاده از آنرا برای خود انحصاری کنید .البته این به نوعی هم لطفی است که شما د رحق کامپیوتر و فرد قربانی خود می کنید زیرا د رغیر اینصورت بسیاری از هکرها این فرصت را پیدا خواهند کرد تا به کامپیوتر قربانی شما حمله کنند که این امری فوق العاده ناخوشایناست.

RE-ENTER PASSWORD

اگر در قسمت قبل در کادر متن جلویی عبارت PASSWORD کلمه عبوری را برای پورتی که قرار است برروی کامپیوترپیوتد قربانی باز شود تایپ کرده باشید اکنون یکبار دیگر باید برای تایید شدنش آنرا در کادرمتن این قسمت نیز تایپ کنید.

VICTEM NAME د ر کادر متن این قسمت باید نامی که مایل هستید تا بررو یکامپیوترپیوتد فرد قربانی بگذارید را وارد کنید بر حذر باشید که همیشه نباید اسم را MY VICTEM(قربانی من)انتخاب کیند ،بلکه توصیه می شودتا د رانتخاب این نام کمی دقت کنید تا تشخیص قرد قربانی برایتان آسانتر شود.زیرا فرض کنید که مثلا شما کامپیوترپیوتد 10 نفر را HACK کرده باشید .حال اگر در زمانیکه در وضعیت ONLINE به سر می بریدپیامی دریافت کنید مبتنی بر اینکه یکی از قربانیان شما ONLINE شده ،تنها اگر برای ه ر10 نفر نام درستی را تغیین کرده باشید قاد رخواهید بود تا آنها را از هم تفکیک کرده و متوجه شوید که منظو رچه کسی است.اما هر10 نفر را MY VICTEM نامیده باشید که دیگر کار خیلی دشوار خواهد شد .برای نام گذاری هرکامپیوتراز نام فرا قربانی استفاده کنید.مثلا نام کامپیوتر قرباین متعلق به فردی که اسم او حسن است را HASAN-VICTEM انتخاب کنید .همینطور الی آخر .البته اگر حدس می زنید که چندین HASAN در آینده وجود خواهند داشت پس بهتر است تا از نام فامیلی یا هر نشانه دیگری نیز استفاده کنید.

PROTECT PASSWORD

در کادر متناین قسمت شما با ید کلمه عبوری را وارد کنیدکه هر کسی برای بروز کردن (UPDATE) و دست کاری سرور HACK ب رروی کامپیوتر قرباین باید آنرا بداند . به عبارت دیگر این کلمه عبوری که انتخاب یم کنید قفلی برا ی فایب اجرایی سرور هکی است که شاید در آینده مایل با شید تا از را ه دور تنظیمات آنرا بر روی کامپیوتر قربانی تغییر دهید.

USE RANDOM PORT

در صورتیکه کادرعلامت کناری این عبارت را کلیک کرده و آنرا علامت بزنید از این به بعد هر بار با ONLINE شدن کامپیوترقربانی و حضور آن دراینترنت به شکلی تصادفی شماره پورتی انتخاب شده و بر روی کامپیوتر قربانی باز می شود .سپس شما با دریافت پیامی از طریق نامه پست الکترونیک یا یک پیام فوری در ICQ از این شماره پورت جدید ،نام کامپیوتر قربانی و شماره IP ی و ی مطلع خواهید شد.

MELT SERVER AFTER INATALITION

با انتخاب این گزینه پس از قرار دادن سرور HACK بر روی کامپیوتر قربانی و به محض اجرا و نصب شدن آن بر رو ی کامپیوتر مذکور فایل سرور هم نیز ناپدیدمی شود.انتخاب این گزینه کار درستی نمی باشد زیرا ممکن است کاربر کامپیوتر هدف با نا پدید شدن آن به موضوع پی ببرد.

WAIT FOR REBOOT

با انتخاب این گزینه با کلیک کردن بر رو ی سروراین فایل بلا فاصله نا پدید نمی شودبلکه پس از یکبا ر راه اندازی مجدد سیستم این فا یل ناپدید می گردد.انتخاب این گزینه بسیار توصیه می گردد زیرا فرد با یک با ر را ه اندازی سیستم خود دیگر به فایل شما دسترسی ندارد.

SERVER FILENAME

نام سرور هکی که قرار است برروی کامپیوتر قربانی قرار گرفته و اجرا شودرا تعیین می کند.

RANDOM FILE NAME

با انتخاب این گزینه پس از دابل کلیک کردن بر رو ی سرور HACK بـه طـو رتصـادفی اسـمی برای فایلهای اجرایی هکی کـه قراراسـت بـر رو ی کـامپیوتر قربـانی در دایرکتـوری خاصـی قرارگیرند انتخاب می شود.انتخاب این گزینه قویا پیشنهاد می شود ،زیـرا از ایـن طریـق اکثـر ضد ویروسها گمراه شده و از دور خارج می شوند.

SPECIFY

نام سرور HACK را می توانید در آن انتخاب نمایید.

برگه START UP METTHODS

ا زطریق این برگه شما می توایندتعیین کیند که هربارسرور HACK چگونـه بـر روی کـامپیوتر قربانی شروع بکار کرده و اجرا شود .

REJISTRY RUN

با انتخاب آن برای هربار شروع سـرور HACK و فعـال شـدنش بـرروی کـامپیوتر قربـانی از قسمت RUN در REJISTRY ویندوز استفاده خواهد شد.

REJISTRY RUN SERVICES

با انتخاب آن برا ی هر بار شروع شدن سرور HACK و فعال شدنش بر روی کامپیوتر قربانی ،از قسمت RUN SERVICES در REJISTRY ویندوز استفاده خواهدشد.

KEY NAME

با انتخاب یکی از دو گزینه قبلی شما می توانیددرکادر مـتن ایـن قسـمت نـام فایـل کلیـدی کـه قرارست تاسرور HACK در REJISTRYویندوز کامپیوتر قربانی با آن ثبت شود را تعیین کنید.

WIN.INIبا انتخاب آن برا ی هر با ر شروع شدن سرور HACK و فعال شدنش بر روی کامپیوتر قربانی ،از داخل فایل WIN.INI ویندوز اقدام خواهدشد.این ویژگی تنها بر رو ینسخه های ویندوز 95و98 کار می کند.

SYSTEM.INI

با انتخاب آن برای هر بار شروع شدن سرور HACK و فعال شدنش بر روی کامپیوتر قربانی ،از داخل فا یل SYSTEM.INI ویندوز اقدام خواهد شد .این ویژگی تنها برا ی نسخه های ویندو ز 95و98 کار می کند.

NEW METHOD#1

با انتخاب این برای هر با ر شروع شدن سرور HACK و فعال شدنش بر روی کامپیوتر قربانی ، ا زدو قسمت دررجبستری ویندوز اقدام خواهد شد .

این روش فایلی به عنوان RUN.EXE مسئولیت اجرای سرور HACK را درصورتی که قبلا در حافظه با رگذاری شده باشدبر عهده دارد .همچنین خود فایل RUN.EXE نیز هر بار که برنامه کاربردی در ویندوز اجرا شود شروع به کار می کند.

NET METHOD #2 [EXPLORER]

با انتخاب این گزینه برای هر بارشروع شدن سرورهک وفعال شدنش بر روی کامپیوتر قربانی از قسمت HKEY_CURRENT_USER SOFT WARE\MICROSOFT\INTERNETEXPLORER\EXPLORER BARS\{C4EE31F3-4768-11D2-BE5C-20AOC9A83DA1}\FILES NAMED MAU

دررجیستری ویندوز اقدام خواهد کرد.

METHOD #3 MARK LORD

با انتخاب این گزینه برای هر بار شرو ع شدن سرور HACK وفعال شدنش بر روی کامپیوتر قربانی ازقسمت

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ACTIV SETUP\INESTAL COMPONENTS

در ویندوز اقدام میکند.

برگهNOTIFICATION

از طریق گزینه های موجوددراین برگه شما می توانید نحوه کسب خبر از وضعیت ONLINE کامپیوتر قربانی خودرا تعیین کنید.

گزینه ها عبارتند از :

ADD ICQ NOTIFY

شما می توانید از این گزینه برا ی کسب خبر از طریق پیام رسان (ICQ)استفاده می گردد.

ADD E-MAIL NOTIFY

از این گزینه برای کسب خبر از طریق پست الکترونیکی استفاده می گردد.

ADD IRG NOTIFY

از این گزینه برا ی کسب خبر از طریق IRC (INTERNET RELAY CHAT) استفاده می گردد.

ADD SIN NOTIFY

از این گزینه برا ی کسب خبر از طریق برنامه SIN (STATIC IP NOTIFICATION) مورد استفاده قرار می گیرد.

اگر SUB7 را بر روی سیستم خود DOWN LOAD کنید و سپس آن را از حالت فشرده خارج کنید به پنجره SIN.EXE برخورد خواهید کرد که اگر شماره پورتی که برا ی سرور HACK نصب شده برروی کامپیوتر قربانی خود وار دکرده اید یکسان باشد در اینصورت به محض وارد شدن کامپیوتر قربانی به اینترنت آیکن مربوط به سرور مورد نظر در لیست برنامه SIN به رنگ سبز خواهد آمد اما اگر کامپیوتر مذکور OFFLINE باشد آیکن به رنگ قرمز در خواهد آمد و پس از گذشت 2دقیقه نیز از لیست حذف خواهد شد .

ADD CGI NOTIFY

اگر مایل به کسب اطلاعات و خبر از طریق CGI (COMMOM CATA WAY INTERFACE)

هستید بر رو ی این گزینه کلیک کنید.

MORE INFO

با کلیک کردن بر رو ی این دکمه کادری ظاهرمی شود که درآن اطلاعات راهنمایی آمده است.

برگه BINDED FILES

از طریق این برگه شما می توانیدهر فایل دیگری را به فایل اجرایی سرور HACK خود پیوند (BIND)بزنید تا از این طریق فردقربانی دیگر هرگز متوجه دریافت سرور HACK نشود برای مثال :شما می توانید قطعه کوچکی ا زیک موسیقی با پسوند WAV یا MP3 را به سرود HACK خود پیوند زده و برای فرد قربانی بفرستید تا به محض اجرا شده فایل سرور HACK بروی کامپیوترپییوتر قربانی علاوه بر اجرا شدن سرور HACK ،به طور همزمان موزیکی نیز پخش شود.در این صورت دیگر فرد قربانی هرگز بویی از مسئله نخواهد برد.

ADD EXE CTUDE FILE

شما می توانید فایلی را که مایل هستید به سرور HACK پیوند بزنید.

DELETE

از این گزینه برا ی پاک کردن یک فایل پیوند زده شده استفاده می شود

EDIT NAME

از این گزینه برای تغییر دادن نام فایل استفاده می گردد.

برگه PLUGINS :

این برگه یکی از مهمترین برگه های پنجره EDIT SERVER است شما از طریق این برگه می توانید PLUGINهای مربوط به اتفاقات و بلاهایی که مایل هستید تا بر سر کامپیوتر قربانی خود بیاورید را بر روی سرور HACK موردنظرتان نصب کنید .یک PLUGIN ماهیتا فایلی با پسوندDLL است .

قابلیتهای PLUGIN با نام S7FUN1 :این PLUGIN ویژگی های زیر را با خود دارد

- FLIP SCREEN : این گزینه با عث چرخش و دوران صفحه می گردد.
- SHOW PICTURE : این گزینه باعث به نمایش درآوردن عکس میشود.
- TEXT 2 SPEECH : این گزینه باعث خوانده شدن متن می شود.
- TIC_TAC_TOE : این گزینه سبب می شود که بتوانید باکامپیوتر قربانی بازی کنید.

قابلیت های PLUGIN با نام S7FUN2

این PLUGIN ویژگیهای زیر را دارد :

- OPEN BROWSER : این گزینه باعث بازکردن پنجره مرورگر و بازدید کردن از یک صفحه WEB خاص را می شود
- MOUSE : با انتخاب این گزینه می توان عمل سوییچ کردن دکمه ها و حرکت دادن موس و همچنین قرار دادن دنباله ای برای اشاره گر موس می گردد.

- TIME/DATE : با انتخاب این گزینه می توان تاریخ و زمان سیستم را تغییر داد و همچنین آن را تنظیم کرد.

قابلیتها یS7KEYS PLUGIN: این PLUGIN ویژگیهای زیر را باخوددارد.

- KEY LOGGER : از این گزینه برای ارسال ضرب کلید استفاده می شود.
- LOGGED KEY : از این گزینه برای خواندن ضرب کلید می توان استفاده نمود.
- KEY LOGGER E-MAIL REPORT : با استفاده از این گزینه ارسال ضرب کلید از طریق پست الکترونیکی انجام می گیرد.

قابلیتهای PLUGIN با نام S7PASSSWOD : این PLUGIN ویژگی ها ی زیر را باخوددارد.

- CACHED : انتخاب این گزینه سبب خواندن کلمات عبور و اطلاعات حافظه نهانی می شود.
- RAS : انتخاب این گزینه موجب کسب اطلاع از طریق سرویس RAS می گردد.
- AIM : انتخاب این گزینه موجب کسب اطلاع از طریق سرویس AIM می شود.
- E_MAILLING PASSWORD : انتخاب این گزینه سبب ویژگی دریافت کلمه عبور از طریق پست الکترونیکی می شود.

قابلیتها یPLUGIN با نام S7CAPTURE : این PLUGIN ویژگی ها ی زیر را دارد

- SCREEN CAPTURE : انتخاب این گزینه سبب دریافت تصویری ا زصفحه نمایش کامپیوتر قربانی می شود.
- MOUSE CLICKS : انتخاب این گزینه سبب انتقال کلیک های موس می گردد.

- WEB CAM CAPTURE : انتخاب این گزینه سبب دریافت تصاویری ازWEB CAM می شود.

قابلیتها یPLUGIN با نام S7ADVANCED :

این PLUGIN ویژگی های زیر را با خود دارد

- PROCESS MANEGER : انتخاب این گزینه سبب مدیریت فرایندها می شود.
- REGISTRY EDITOR : با انتخاب این گزینه می توان از ویژگی ویرایش رجیستری ویندوز از را ه دور استفاده می گردد.

برگه RESTRICTION :

از طریق این برگه می توان تنها تعدادی از قابلیتها ی مورد نظرتان رابرروی یک سرور HACK فعال کنید.این ویژگی زمانی مفید است که شما به هکر های دیگر هم امکان استفاده از سرور HACK روی سیستم قربانی رابدهید.اگر برای پورت باز قربانی پسورد و نامی را انتخاب نکنید سایر هکر ها هم می توانندبه سیستم دست پیدا کنندااما دراینبین شما میخواهید که این هکر ها یکسری کارها ی بی خطر را روی سیستم قربانی انجام دهنددرنتیجه می توان از این گزینه استفاده کرد.

برگه E_MAIL :

از طریق این برگه شما می توانید از سرور HACK بخواهید تا تمامی کلمات عبور ذخیره شده برروی کامپیوتر قربانی و نیز تمامی کلیدهای رزرو شده برروی صفحه کلید (PASSED KEYS) آنرا به آدرس پست الکترونیکی شما بفرستد که شامل گزینه های زیرمی باشد:

- E_MAIL ALL PASSED KEYS TO : با کلیک کردن آن و وارد کردن آدرس پست الکترونیکی خود به محض حضور کامپیوتر قربانی دراینترنت سرور HACK تمامی کلیدهای فشرده شده از آن جمله کلمه عبور اشتراک اینترنت کامپیوتر قربانی را به آدرس پست الکترونیکی شما ارسال خواهد کرد
- E_MAIL ALL PASSWORDS TO : با کلیک کردن آن ووارد کردن آدرس پست الکترونیکی آن به محض نصب شدن سرور HACK برروی کامپیوتر قربانی تمامی کلمات عبور اشتراکهای فرد قربانی اعم از اشتراک YAHOO ،MSN ،ICQو بسیاری دیگر به آدرس پست الکترونیکی شما ارسال خواهدشد .
- E_MAIL RECORDED PASSWORD TO : با کلیک کردن آن و وارد کردن آدرس پست الکترونیکی خود با هر بار وارد شدن کامپیوتر قربانی به اینترنت تمامی کلمات عبور ذخیره شده برروی کامپیوتر قربانی به آدرس پست الکترونیکی شما ارسال خواهدشد.

برگه EXE ICON/OTHER :

از طریق این برگه شمامی توانید آیکن فایل اجرایی سرور HACK خود را تغییردهیدتا کمتر از سوی فرد قربانی موردشک قرار گیرید.همچنین این امکان وجوددارد‌که پیغام خطایی را طراحی کرده تا درزمان اجرا ی فایل سرور HACK برروی صفحه نمایش کامپیوترقربانی ظاهر شده و فرد قربانی را گمراه کند.این درحالی است که فایل سرور HACK تواما با ظاهر شدن این پیغام به طور مخفیانه اجرا می گردد.

گزینه های SUB SEVEN برای حمله

استفاده از گزینه های مختلف پنجره SUB7 برای حمله به کامپیوتر قربانی

باوارد کردن IP و پورت باز قربانی دکمه کانکت را فشار دهید تا به کامپیوتر متصل گردید پس از اتصال شما می توانید از امکانات زیر استفاده نمایید.

بررسی امکانات گزینه SHURTCUTS :

دراین قسمت میانبر هایی به برنامه ها و فعالیتهای بسیاردیگری آمده است که خود شامل امکانات زیر می باشند.

1. LOCAL SHURTCUTS : روی آن کلیک کنید تا زیرمنوهای آن ظاهر شود:

- IP TOOLS : به وسیله آن شما می توانیدهر یک از کارهای زیر را انجام دهید

أ به کامپیوتری PING کنید

ب آدرس IPمتناظر باهر اسم URL را دراینترنت پیدا کنید

ت آدرس IP کامپیوتری که کاربرآن باشماره ICQ خاصی مشغول گپ زنی است را پیدا کنید

- ADDRESS BOOK : شما از طریق این کادرکه نقش یک دفتر جه آدرس را دارد می توانیدمشخصاتی در باره کامپیوتر قربانی خوددسترسی پیدا کنید
- CONSOLE : در این کادر محاوره ایی آن دسته از فرمانهایی که قبلا توسط شما صاد رشده اند ولی به هر دلیلی موفق به اجرا نگردیده اند می آیند .
- SETTING : این کادر به تنظیمات ظاهری بخش کلاینت برنامه SUB7 که هم اکنون درحال کار با آن هستید اختصاص دارد

2. MISC SHORTCUT : با کلیک کردن روی آن زیر منوهای آن ظاهر می گردد

- FILE MANAGER : از طریق این کادر محاوره ایی شما می توانید د رصورت اتصال به کامپیوتر قربانی تمامی محتویات هارد دیسک کامپیوتروی را مشاهده کنید همچنین از طریق دکمه هایی که درسمت راست این پنجره آمده اند شما می توانیدهر بلایی را بر سر هارددیسک قربانی خود بیاورید
  - REFRESH CURRENT PATH : در صورت مایل بودن به دیدن نتیجه تغییرات داده شده توسط شماروی کامپیوتر قربانی از این گزینه استفاده نمایید
  - UPLOAD FILE : از طریق این گزینه شما می توانیدفایلهای مورد نظرتان را بر روی کامپیوتر قربانی UPLOAD کنید
  - RUN SELSCT FILE : با این گزینه می توانید فایلهایی را بررو ی کامپیوتر قربانی خوداجرا کنید.
  - DELETE SELECTED FILES OR FOLDER :با این گزینه شما می توانید فایلهایی را بر رو ی کامپیوتر قربانی خودحذف کنید.

- CREATE A NEW FOLDER IN THE CURRENT PATH : با این گزینه می توانید پوشه جدیدی را به هر اسمی که مایل بودید برروی کامپیوتر قربانی خودایجاد کنید.
- PLAY WAV FILE ON THE REMOTE COMPUTER : با این گزینه می توانید فایلهای صوتی با پسوند WAV را برروی کامپیوتر قربانی خود به اجرا درآورده و پخش کنید.
- SELECTED FILE AS WALLPAPER ON THE REMOT COMPUTER :با استفاده از این گزینه شما می توانید عکسی را به عنوان کاغذدیواری کامپیوتر قربانی خود انتخاب کنید.
- REMOT FILE OR FOLDER : با این گزینه می توانیدهر فایل یا فولدری را برروی کامپیوتر قربانی تغییر نام دهید.
  - SEARCH FILE :با استفاذه از این گزینه به دنبال فایل مورد نظرتان جستجویی ر ابرروی کامپیوتر قربانی به اجرا درآورید.
  - QUEUE : با استفاده از این گزینه شما میتوانید به ترتیب میزان پیشرفت عملیات انتقال فایل میان کامپیوتر خودتان و کامپیوتر قربانی نظارت کنید.
  - WINDOWS MANEGER : با استفاده از این گزینه شما می توانیدتمامی پنجره ها یباز شده بر رو ی کامپیوتر قربانی را مدیریت کنید.مثلا پنجره ایی که در زیر پنجره های دیگر قرارگرفته است را بر روی بقیه بیندازید،پنجره ای را فعال یا غیر فعال کنید.

- SCREEN CAPTURE : با استفاده از این گزینه شما می توانید صفحه نمایش کامپیوتر قربانی را برروی کامپیوتر خودتان مشاهده کنیدشیوه کار به این صورت است که شما باز زمانی را بر حسب ثانیه تعیین می کنیدکه با گذشت آن ا ز صفحه نمایش کامپیوتر قربانی عکسی گرفته شده و برای شما فرستاده شود. این کار از طریق اهرم کشویی که د رروبروی عبارت INTERVAL آمده صورت می گیرد.
- PROGRESS WINDOWS : از طریق این کاد رمحاوره ای شما می توانید شاهد و ناظر سرعت تبادل اطلاعات میان کامپیوترخود و کامپیوتر قربانی باشید.
- PLUGIN MANEGER : با استفاده از این گزینه شما می توانید تمامی PLUGIN های که برروی یک سرور HACK نصب شده اند را مدیریت می کنید

3. OPEN : این گزینه دارای زیر منوها ی زیر است :

- SUB7 WEB SITE : باکلیک کردن رو ی آن پنجره ایی با ز شده و مرورگر WEB کامپیوترتان باز می شود و شما به سایت WWW.SUBSEVEN.SLAK.ORG رهنمون می شوید.
- NOTEPAD.EXE : برنامه NOTEPAD اجرا می گردد.
- TELNET : پنجره خالی TELNET اجرا می گردد.

بررسی امکانات CONNECTION : این منو دارای گزینه های زیر است:

1. PROXIES : درصورتی که بر روی خط اینتر نتی که از آن استفاده می کنیدیک PROXIES نصب شده باشد آن را پشت سر بگذارید برای این کار کافیست مختصات PROXIES خود را که آن را از مدیر ISP خود دریافت می کنید در داخل کادرهای متن مربوطه وارد کنید .
2. PC INFO : اگر شما به کامپیوترراه دوری که قبلا سرور هکی را بر رو ی آن نصب کرده ایدوصل شده باشید در این کادرمحاوره ای تمامی مشخصات اولیه کامپیوتر مورد نظر لیست خواهد شد.
3. MORE PC INFO : اطلاعات بیشتر و پیشرفته تری درباره کامپیوتر قربانی می دهد.
4. NAME INFO : اطلاعات شخصی صاحب کامپیوتر قربانی را به ما می دهد.
5. SERVER OPTION : برای مدیریت سرور HACK بر رو ی کامپیوترقربانی آمده است و دارای دکمه ها ی زیرمی باشد:

- CHANGE PORT : این دکمه شماره پورتی را تعیین می کند که قرار است تا سرور HACK به محض وارد شدن کامپیوتر قربانی به اینترنت آن را بر رو ی کامپیوترمذکور باز کنددر حالت پیش فرض این شماره 27374 می باشد.
- REMOVE SERVER : فرمان دهید تا سرور HACK از روی کامپیوتر قربانی پاک شود.
- SET PASSWORD :شما می توانید کلمه عبوری را برای دسترسی به سرور HACK بر روی کامپیوتر قربانی تعیین کنید.
- REMOVE PASSWORD : شما میتوانید کلمه عبوری را که قبلا برای دسترسی قرار داده اید حذف کنید.

- RESTART SERVER : با انتخاب این دکمه شما می توانیدپس از اعمال تغییرا ت یکبار سرور HACK را RESTART کنید تا تغییرات اعمال شود.
- CLOSE SERVER : شما می توانیددریک جلسه کاری استفاده هر شخص از کامپیوتر قربانی راتعیین کرده و سرور HACK را از کاربیندازید.
- UPDATE SERVER FROM URL : شمامی توانیداین امکان را به سرور HACK بدهیدکه خودرابه طوراتوماتیک بروز کند.

6. CONNECT COMMANDS : این گزینه دارای زیر منوهای زیر می باشد:

- OPEN ON CONNECT : تعیین نحوه با خبر شدن از وضعیت ONLINE کامپیوترقربانی که شامل دکمه ها ی زیر میباشد.
- GET SERVER ON CONNECT COMMANDS : تمامی روشهایی که قبلا برروی سرو رهک کامپیوتر قربانی تنظیم کرده اید تا از طریق آنهااز وضعیت ONLINE وی مطلع شوید را دریافت کنید.
- SAVE ON CONNECT COMMANDS TO SERVER : تمامی روشهای جدیدی که صلاح می دانید تا از این به بعد از طریق آنها از وضعیت ONLINE کامپیوتر قربانی خود مطلع شوید را بر روی سرو رهک کامپیوتر راه دور و قربانی خود ذخیره کنید.
- SET/CHANG PASSWORD : برای تغییر دادن نحوه با خبر شدن از وضعیت ONLINE کامپیوتر قربانی کلمه عبوری را تعیین کرده یا اینکه کلمه عبور قبلی خودتان را تغییر دهید.

- ADD ICQ NOTIFICATION : از سرور HACK بخواهید تا وضعیت ONLINE کامپیوتر قربانی ر ابا ارسال پیامی از طریق سرویس گپ زنی ICQ به استحضار شما برساند.
- ADD EMAIL NOTIFICATION : از طریق این دو دکمه شما می توانید ازسرور HACK بخواهید تا وضعیت ONLINE کامپیوتر قربانی را باارسال نامه پست الکترونیکی به استحضار شما برساند.
- ADD IRC NITIFICATION : تاوضعیت ONLINE کامپیوترقربانی را با ارسال پیامی از طریق سرویس گپ زنی IRC (INTERNET RELAY CHAT) به استحضار شما برساند.
- ADD CGI NITIFICATION : از طریق این دکمه شما میتوانیداز سرور HACK بخواهید تا وضعیت ONLINE بودن کامپیوتر قربانی را با ارسال اطلاعیه ای به CGI ای که بر روی سایت وبی راه اندازی کرده اید به استحضار شما برساند
- ADD STATIC IP NOTIFICATION : این گزینه سبب میشودتاوضعیت ONLINE کامپیوترقربانی راباختصار آدرس IP ثابتی که قربانی مذکور دارد را به اطلاع شما برساند.

- CLEAR COMMAND : تمامی شیوه ها ی مختلفی که برای کسب اطلاع از وضعیت ONLINE کامپیوتر قربانی تعیین شده بودپاک می شوند.
- ADD COMMAND : با این گزینه می توان فرامین را برای تعیین شیوه ها ی مختلف کسب اطلاع از وضعیت ONLINE کامپیوتر قربانی خود اجرا کنید.

7. OTHERS : این گزینه داراری زیر منوهای زیر است:

- WEB STATUS :با انتخاب این گزینه شما می توانید ازوضعیت سرور HACK بررو ی کامپیوتر قربانی خودکسب اطلاع کنید.
- WEB DOWNLOAD : شما می توانیدباواردکردن آدرس سایت WEB موردنظرتان درداخل کادرمتن روبروی عبارت URL و همچنین تعیین موقعیت فایل موردنظر بررو ی سایت WEB مربوطه د رداخل کادرمتن با عبارت DESTIMTION از سرور HACK نصب شده بر رو ی کامپیوتر قربانی بخواهید تا فایل موردنظر شما را روی سایت WEB به روی کامپیوتر قربانی DOWNLOAD کرده و آنر ا نصب کیند.

8. SCANNER : این منو زیر منوهای زیررا دارا می باشد:

- REMOT SCANNER : از طریق گزینه های این کادر که شباهت زیادی به یک اسکنر آدرس IP دارد ،کامپیوتر هایی که توسط خود شما یا هر وسیله دیگری HACK شده و هم اکنون در وضعیت ONLINE هستند را پیدا کنید.

بررسی امکانات KEY/MESSENGER

این منو دارای گزینه های زیراست:

1. KEYBORD : این گزینه شامل زیر منوهای زیر است:

- OPEN KEY LOGGER : میتوانیدفعالیتها یKEYBORD کامپیوتر قربانی خود را مدیریت کنید.و شامل گزینه های زیر میباشد:
  - ENABLE /DISABLE KEY LOGGER : میتوانیدویژگی KEY LOGGER را فعال یا غیر فعال کنید.
  - CLEAR LOGG : میتوانیدصفحه KEY LOGGERرا پاک کنید.

- DISABLE KEYS : شما می توانیدتعدادی از دکمه های صفحه کلید کامپیوتر قربانی را از کار بیندازید.
- REPLASE KEYS : شما میتوانید دکمه های صفحه کلید کامپیوتر قربانی خودرا باهم تعویض کنید.

- OPEN LOGGED KEYS : تمامی کلیدهایی که برروی کامپیوترقربانی زده شده د رسرور HACK ذخیره شده اند را بر اساس روز ،ماه وسال وقوع آنها مشاهده کنید.ومی توان اعمال زیر را با آن انجام داد:
  - GET LOGED KEYS :شما میتوانید تمام دکمه ها ی ذخیره شده در داخل سرور HACK نصب شده برر و ی کامپیوتر قربانی را دریافت کنید.
  - DELETE ALL LOGGED KEYS : محتویات کادر LOGGED KEY که شامل تمامی دکمه هایی است که توسط فرد قربانی برروی صفحه کلیدکامپیوترش زده شده اندرا پاک می کنند.
  - SAVE ALL LOGGED KEYS TO A TEXT FILE : تمامی کلیدهای زده شده را برای آنالیز آن درفرصتی مناسب درداخل فایل متنی ذخیره می کند.
- SEND KEYS : کلیدهایی راکه برر و ی صفحه کلید خود تایپ کرده میتوانیدآنها را برای کامپیوتر قربانی بفرستید.
- DISABLE ALL KEYS :شمامیتوانید تمامی کلیدهای صفحه کلیدکامپیوتر قربانی خودرا ازکار بیندازید.

- RE ENABLE ALL KEYS : تمامی کلیدهای صفحه کلید کامپیوتر قربـانی خـود را کـه از کا رانداخته بودید فعال می کند.

2. MATRIX : میتوانیدکادری را برروی کامپیوتر قربانی خود بـاز کـرده وا ز طریـق آن بـه گپ زنی بافردقربانی بپردازید.

3. MESSAGE MANAGER : میتوانید کادرهای مشابه با همان کادرهای معمـول ویـندوز کـه درمواقع بروز ایرادی به نمایش درمـی آیـدرا بـرروی مـانیتور کـامپیوتر قربـانی خودظـاهر سازید.

4. SPY MANAGER : می توانیدکلمات عبور اشتراکهای(ACCOUNTS) کـاربری هـر یـک از سرویسهای MSN، YAHOO وICQ و AIMموجودروی کامپیوتر قربانی را برباییید.

5. ICQ TAKE OVER : میتوانیدتمامی URL های موجود در پانل نرم افـزار ICQ فـرد قربـانی خود را صاحب شوید.

بررسی امکانات ADVANCE

این منوشامل گزینه های زیر است :

1. FTP SERVER : میتوانیدکامپیوتر قربانی خودرابه یک سرور HACK بدل کنیـد سـپس از طریق هر یک از برنامه ها یFTP نظیر CUTEFTP یا هربرنامه دیگری کـه بـا آن کارمیکنیـد آدرس IP کامپیوتر قربانی و شماره پورتی را که درحالت پیش گزیده می باشدواردکرده و نهایتا CONNECT را کلیک کنید.

2. FIND FILES : دارای دوزیرمنو است :

- FILED FILES : دنبال فایلهای موردنظرتان می گردد.

- SHOW FOUND FILES : تمامی فایلهای جواب جستجورا نمایش میدهد.

3. PACKET SNIFFER : دارای زیر منو های زیر می باشد:

- ENABLE /DISABLE : بسته های اطلاعاتی که میان سرور و کلاینت کامپیوترقربانی مبادله می شوندرا به مونیتور داده از این طریق به اطلاعات نابی چون شماره کارتهای اعتباری یا اطلاعاتی از این دست که کامپیوتر قربانی با کامپیوتر شبکه های بانکی یا هر مرکز دیگری مبادله می کنددسترسی پیداکنید.
- LOGG WINDOW : تمامی بسته های حاو ی اطلاعاتی که به آنها LOGGکرده اید را مشاهده می کنید.

4. PASSWORD :این گزینه شامل زیر منوهای زیر است:

- SCREEN SAVER : دارای کلمه عبور مربوط به محافظ صفحه نمایش کامپیوتر قربانی است که میتوانید آن را کشف کنید.
- CACHED : تمامی کلمات عبوری که د رحافظه نهان کامپیوتر ذخیره شده اند را بر ملا می سازند.
- RAS PASSWORD : تمامی کلمات عبور سرور های دسترسی از راه دور که برای دسترسی به فایلها و چاپگر های به اشتراک گذاشته شده در یک شبکه قرار میگیرند را کشف کنید .
- ICQPASSWORDS : تمامی کلمات عبور سرویس ICQ نصب شده روی کامپیوتر قربان یرا کشف میکند.

- AIM PASSWORD : کلمات عبوری سرویس AIM نصب شده بر روی کـامپیوتر قربـانی کشف میشود.
- RECORDED : تمامی کلمات عمومی که از داخل پنجره ها یا کادر های باز شده بـرروی کامپیوترقربانی ذخیره شده است را می بینید.
- ICQ PASS STEALER : شما می توانید تمامی کلمات عبور ICQ را بربایید.

5. REGISTRY EDITOR : رجیستری ویندوز قربانی خود را ویرایش کنید .
6. NET WORK BROWSER : درصورتی که قربانی بـه عنـوان سـرور دریـک شـبکه مـور داستفاده قرار گرفته بودتمامی دیواره های موجود درشبکه را نگاشت (MAP) نمود.
7. PROCCES MANEGER : تمامی پروسه هـایی کـه بـرروی کـامپیوتر قربـانی درجریـان هستند را مشاهده کرده و درصورت تمایل به کار یا عملکرد پروسه ای پایان دهید.
8. PORT REDIRECT : بابازکردن پورتی برروی کـامپیوتر قربـانی از سرویسـهایی نظیـر IRC وFTPوHTTP و بسیاری دیگر بهره مند می شویم .
9. ADD REDIRECT : پورتی بر روی کـامپیوتر قربـانی خـود بـاز کـرده و بعـد از طریـق سرویس تلنت به آن نفوذ کنید.
10. NET STATE : شاهد تمامی ارتباطات کامپیوترقربانی خودبادیگرکامپیوتر ها باشید.

بررسی امکانات MISCELLANEOUS

این منو دارای گزینه های زیر می باشد.

1. FILE MANAGER :در MISC SHORTCUT درمورداین کادرقبلا صحبت شده است .

2. WINDOWSE MANAGER : در MISC SHORTCUT مفصلا درباره آن توضیح داده شده است.

3. TEXT 2 SPEECH : پس از تایپ متن مورد نظر درداخل کادرمتن زیرین عبار ت TEXTو کلیک برروی SAY IT! متن مورد نظرتان را برروی کامپیوتر قربانی پخش کنید.

4. CLIP BORD MANAGER :میتوان متن موجود در کلیپ بوردرا مشاهده وتنظیم کرد.

5. PRINT MANAGER :متن موردنظر را تایپ کرده سپس آن را روی چاپگر کامپیوتر قربانی خودچاپ کنید.

بررسی امکانات FUN MANAGER

این منو شامل گزینه های زیر است:

1. SCREEN CAPTURE : در MISC SHORTCUT گفته شد.

2. WEB CAM : در صورت استفاده کامپیوتر قربانی از WEB CAM یا دوربین WEB می توانیدآنرا روشن کرده و اتاق وی را دیدبزنید.

3. FILP SCREEN : صفحه نمایش کامپیوتر قربانی را بچرخانید.

4. PRINT MANAGER : قبلا توضیح داده شده است.

5. OPEN BROWSER : میتوانیدپنجره مرورگری را روی کامپیوترقربانی باز کرده و صفحه WEB خاصی را درآن به نمایش درآورید.

6. RESOLUTION :شما می توانید درجه وضوح مونیتور را تغییر دهید.

7. WINDOWSE COLORSE : شمامیتوانیدرنگ صفحات ویندوز را تغییر دهید.

8. TIC-TAC-TOE : پنجره ایی را برای کامپیوتر قربانی باز کرده و شروع به بازی کنید.

9. REALISTIC MATRIX : می توانیدکادری روی صفحه مانیتور قربانی باز کـرده و بـا وی گپ بزنید.

بررسی امکانات *FUN OTHER*

این منو شامل گزینه ها ی زیر می باشد :

1. RESTART COMPUTER : با انتخاب این گزینه می توان کامپیوتر را خاموش یا به حالت خواب برد.
2. MOUSE : با موس کامپیوتر قربانی بازی کنید.
3. VOLUME SETTING : می توان ولوم صدای کامپیوتر قربانی را زیادیاکم کرد .
4. RECORD MIC : درصورت اتصال میکروفون یا هد ستی بـه کـامپیوتر قربـانی صـدای مکانی که کامپیوتر قربانی در آنجا می باشد را ضبط کرده و مجددا آنرا بـرای فردقربـانی پخش کنیم.
5. TIME/DATE : این گزینه برای تغییر ساعت و تاریخ سیستم است .
6. EXTRA FUN : شامل گزینه های زیراست:
   - HIDE/ SHOW DESKTOP ICON
   - HIDE/SHOW START BOTTOM
   - OPEN/CLOSE CD-ROM
   - SHOW /HIDE CLOCK
   - START/STOP SPEKER
   - HIDE/SHOW TASKBAR
   - TURN MONITOR ON/OFF
7. KEY FUN : این گزینه شامل زیر منوهای زیر می باشد:
   - NUMLOCK ON/OFF
   - CAPS LOCK ON/OFF
   - SCROLL LOCK ON/OFF

- DISABLE/ENABLE ALT+CTRL+DEL

بررسی امکانات PLUGIN

دارای امکانات زیر است

1. LIST PLUGIN: با استفاده از این گزینه می توانیدPLUGIN هایی رابه سرور اضافه یاکم کنید.که خود شامل قسمتهای زیر میباشد:
   - REFRESH PLUGIN LIST باعث تازه سازی PLUGIN هامی شود.
   - UNINSTALL PLUGIN : تعدادی از PLUGIN هارا از حالت نصب خارج میکند.
   - UPLOAD AND INSTALL PLUG : PLUGIN روی کامپیوتر قربانی خودDOWNLOADکرده ونصب وراه اندازی میکنیم.
   - MENUALLY INSTALL A PLUGIN : شما مسیر PLUGIN ای که قبلا به روی کامپیوتر قربانی خود UPLOAD کرده بودید راواردکرده از این طریق آنرا بر روی سرور HACK کامپیوتر قربانی نصب و راه اندازی می کنید.
   - DOWN LOAD PLUGIN FROM THE WEB : آدرس URL سایت وبی که PLUGIN های موردنظرتان رابرروی آن قرار داده اید واردکرده سپس از سرور HACK بخواهیدتاآنهارابر روی کامپیوتر قربانیDOWNLOAD کرده ونصب کند.
2. GET COMMAND : توسط این گزینه شمامیتوانیدفرمانهای صادره را دریافت کنید.
3. PLUGIN : قبلا توضیح داده شده است.

بررسی امکانات LOCAL OPTION

دارای گزینه های زیر می باشد:

1. IP TOOLS : قبلا توضیح داده شده است.

2. ADDRESS BOOK : قبلا توضیح داده شده است.

3. PROXIES : قبلا توضیح داده شده است.

4. PERFERENCE : قبلا توضیح داده شده است.

5. INSTALL PLUGIN :توسط این گزینه می توانید PLUGIN موردنظرتان را سوار نمایید.

6. ADVANCED :که خودشامل گزینه های زیر است:

- COMMAND :کادرمحاوره ای نمایش داده می شودکه شما میتوانید فرامینیبرای اجراشدن آن واردنمایید.
- SCRIPT EDITOR : توسط این گزینه شمامی توانید فرامین نوشته شده را تست نمایید.

NET BUS

آشنایی با NET BUS

NET BUS در سال 1998 توسط یک برنامه نویس سوئدی به نـام CARD-FREDRIK NIEKTER نوشته شد .وی از این تروجان برای سر بـه سـر گذاشـتن دوسـتان خـود وشـوخی بـا آنـان استفاده می کرد.دیری نگذشت که این TROJAN درمیـان بسـیاری از کـاربران اینترنـت پخـش گشت و مورد استفاده آنان قرار گرفت تا امروز که یکـی از مشـهورترین TROJAN هـای WEB به حساب می آید.

تـا کنـون نسـخه 1.2،1.53،1.60،1.70،00 BETA،2 PRO، PRO 2.00، PRO 2.10از NET BUS عرضـه شده اندکه برروی نسخه ها ی ویندوز 98،95،NT ،MEو 2000 کار می کنندالبته ایـن دلیـل نـم یشود که ویندوز XP را کنار بگذاریم زیرا نسخه ایی برای تاثیر گذاری بر ویـنـدوز XP عرضـه خواهد شد .

همچون بسیاری ازTROJAN ها NET BUS هم یـک فایـل اجرایـی سـرور HACK دارد کـه بایـد بـررو ی کـامپیوتر قربـانی نصـب شـود در نسـخه نـت1.70 ایـن فایـل درحالـت پـیش فـرض PATCH.EXE نام داشته و حدود 470 KB هم حجم دارد.

قابلیتهای NET BUS

1. غیر فعال کردن کلیدهای صفحه کلید.
2. بنمایش درآوردن هر تصویری با پسوند BMP یا JPG .
3. SHUTDOWN کردن کامپیوتر قربانی .
4. اجازه دادن تنها به IP های خاصی برای برقراری اتصال .
5. گپ زدن با سرور به صورت بلادرنگ وهمزمان.
6. راه اندازی کنترلگرهای مدیریتی چون: حذف کردن و بستن سرور HACK یا حتی تنظیم کرده کلمه عبور برای دسترسی به آن

BACK ORI FICE

آشنایی با BACK ORI FICE

BACK ORI FICE توسط گروهی که خودرا THE CULT OF THE DEAD COW می نامندبرنامه ریزی شده و در سال 1998 برای استفاده همگان در اینترنت پخش گردید . قصد اینگروه درطراحی BACK ORI FICE که اصطلاحا BC نیز نامیده می شود آشکار ساختن خلاء های امنیتی سیستم عاملی نظیر ویندوز از شرکت MICROSOFT.

خطرناکترین نسخه این TROJAN تا این لحظه BACK ORI FICE 2000 (یا مختصرا BO2K) است که بررو ی نسخه های ویندوز 95 ،98، NT ، ME و 2000 به خوبی کار می کنند.

همچون بسیاری از TROJAN ها BACK ORI FICE هم فایل اجرای سرور هکی دارد که باید بررو ی کامپیوتر قربانی نصب شود.در نسخه BO2K د رحالت پیش گزیده این فایل UMGR32.EXE نام دارد(حجم سرور های HACK مختلف یک حدودا 122کیلو بایت است) همچنین فابل اجرایی کلاینت درنسخه BO2K نیز BO2KGUL.EXE نام دارد .

BACK ORI FICE هم چون NET BUS اغلب به بیشتر بازیهای (GAME) رایگان ،فایلهای موزیک از نوع MP3 ،عکسهای زیبای رایگان بر روی اینترنت پیوند زده شده و پس از اجرا کردن فایل اصلی به طور کاملا مخفی و پنهان بدون اینکه اثری از خود برجای بگذارد برروی کامپیوتر قربانی نصب می شود.همچنین از آنجایی که BACK ORI FICE قابلیت استفاده کردن از هر پورتی را برروی کامپیوتر دارد (حتی پورتهای HTTPوFTP) بنا براین به راحتی می تواندغلب دیوارهای آتش را فریب دهد و از آنها بگذرد.

قابلیتهای BACK ORI FICE

این نرم افزار قابلیتهای زیر را دارا می باشد:

1. ارسال و دریافت ضربه های کلید .
2. قابلیت انتقال و مرور مستقیم فایل HTTP.
3. دردست گرفتن مدیریت ویژگی اشتراک فایل و چاپگر .
4. امکان ویرایش مستقیم رجیستری ویندوز از راه دور .
5. قابلیت توسعه عملکردها و قابلیتهای سرور HACK با اضافه کرده بر P L UGIN ها .

WIN CRASH

این نرم افزار یکی از پرطرفدارترین نرم افزار هایی است که توسط کرکرها مورد استفاده قرارمی گیرد .این برنامه دارای یک رابط گرافیکی بسیار ساده است .به طوری که استفاده از آن حتی از برنامه PAINT ویندوز هم راحتتر است همین امر دلیل محبوبیت این نرم افزار در میان کرکر ها شده است .

برنامــه ویــن مانندداکثر برنامــه هــای مشــابه خودازقبیــل GINFRIEND SUB7 و NETBUS PROو...به یک فایل سرویس دهنده به نام SERVER.EXE بـرروی کـامپیوتر میزبـان احتیـاج دارد.

برای استفاده ازاین برنامه ابتدا باید آن را برروی کـامپیوتر خودنصـب کنیـد.بعـد از انجـام مراحـــل نصـــب وراه انـــدازی برنامـــه ،دو فایـــل اصـــلی برنامـــه بانامهـــای SERVER.EXEوCLIENT.EXE در اختیار شما قرارمی گیرد.

فایل SERVER.EXE همان فایلی است که باید به کامپیوتر موردنظر انتقال یابدو یک بـار نیـز اجرا شود.معمول ترین روش برای ارسال این فایل که یک فایل تروجان است انتقـال آن بـه کـامپیوتر میزبــان توســط یــک برنامــه (IM(IMSTANT MESSENGER از قبیــل YAHOO MESSENGER،MESSENGER، MSN MESSENGER،ODIGO،ICQ و...است اگر این فایـل بـه صـورت پیوسـت یک نامه الکترونیکی ارسال شود.

اکثر سرور های پستی (MAILE SERVER) دارای یک نرم افزار شناسایی ویـروس هسـتندکه قبل از DOWN LOAD کردن فایل ، امکان بازرسی آن را بـه کـاربر مـی دهنـد.در ایـن حالـت فایل توسط نرم افزار ضد ویروس به عنوان یک فایل آلوده یااسب تراواشناسایی می شود.

اما می توان به راحتی درهنگام استفاده از نرم افزار های IM فایل SERVER.EXE را تغییر نام داد (بدون اینکه در عملکر د فایل تغییری حاصل شود)وبه عنوان یک فایل گرافیکی مثل تصویر خودتان و یا به جای فایل درخواست شده توسط طرف مقابل معرفی کرده و آن را به کامپیوتر او منتقل کرد.این فایل که خود حدود330کیلو بایت حجم دارد به وسیله نرم افزارIM و بدون هیچگونه بازرسی ،به کامپیوتر مقابل DOWN LOAD شده و به محض اجرا

کامپیوتر نصب می شوداین فایل به محض اینکه اجرا شـو د.یـک کپـی از خـودرا در شـاخه اصلی ویندوز قرار می دهد.و به منظور اجرا شدن خودکـار فایـل در هـر مرتبـه بـالا آمـدن سیستم عامل ،مسیر خود را درمکانهای گوناگون مانند فایل WIN.INI در شـاخه وینـدوز در دستور RUN و یا دررجیستری ویندوز در آدرس زیر :

HKEY_LOCAL_MACHINE\SOFT WARE\MICROSOFT WINDOWSE CURRENT VERSUON\ HACK RUN می کند .که البته تمامی این عملیات بسیار سریع و کاملا در پشت صحنه اتفـاق می افتد بدون اینکه کاربر کوچکترین نشانه ای از این عملیات را مشاهده کنـد .حتـی جـالبتر اینکـه وقتـی کـاربر توسـط کـادر CLOSE PROGRAM (بـا زدن کلیـدهای ALT+CTRL_DEL) برنامه های باز درسیستم عامل را مشاهده می کند هیچ نشانی از اجرا شدن این فایـل نمـی یابد.دراین مرحله کامپیوتر سرویس دهنده آماده استفاده است .

اکنون بایدارتباط برقرار شود .برای ایـن عمـل بـه آدرس IP دسـتگاه مقابـل احتیـاج داریـم .باوجودی که آدرس IP درهر مرتبه اتصال دستگاه به اینترنت متفاوت است ولی درمجمـوع یافتن آن کا ربسیار ساده ایست.فقط به ذکر همین نکتـه اشـاره مـی کنـیم کـه بـا ایجادیـک ارتباط مستقیم (DIRECT CONNETION) به راحتی می تـوان از طریـق اجـرا ی فرمـان NET START درخط فرمان ویندوز به FOREIGN IP ADDRESS که آدرس IP کـامپیوتر طـرف دوم است دست پیدا کرد.

این فرمان معمولا درارتباط هایی که درپورتهای 5050و یا در این حدود برقرار شده است ،دقیق ترین آدرس IP را از کامپیوتر سرور نمایش می دهد.

هم اکنون همه چیز آماده است برای وارد شدن به کامپیوتر سرور و زیر و روکردن داده ها و برنامه ها ی آن کافیست برنامه کلاینت WINCRASH (فایل CLIENT.EXE) را اجرا کنید ودر کادر TARGET IP ، آدرس IP کامپیوتر سرور راوارد کنیدوسپس دکمه CONNECT TO HOST را فشار دهید پس از چند لحظه تامل ارتباط شما با کامپیوتر سرور برقرار شده و کنترل آن دردست شما قرار می گیرد و شما به تمامی منابع آن دسترسی خواهید داشت .

توجه داشته باشیدکه به وسیله دکمه DISCONNECT FROM HOST می توانید ارتباط خودرا با سرور قطع کنید.

اطلاعات مختصری راجع به هک سایت

در هک یک سایت اصل بر این است که شما بر روی **FTP** آن کار کنید یعنی **IP** مربوط به**FTP** را پیدا کر ده وتست یک مجموعه از **USER NAME** ها و پسوردها که از یک فایل بانک اطلاعاتی کلمه ها ساخته و استخراج می شود استفاده کنید .

در بعضی از مواقع یک سایت **PORT** ها وآدرسهای بازی دارد که می توان به آن وارد شد که در اینصورت نشان داده می شودکه آن پورت یک **IP** دارد و بدون اسم رمز و نام کاربری می توان به آن وارد شد.

می توانیم با استفاده از **IP TOOLS** و پینگ و **IP DETECT**، **IP** آن سایت راپیدا کنید و با استفاده از نرم افزارهایی مانند :

- **WEB CRACER 2000**
- **BRUTUSA2**
- **WEB HAKER**

می توان اسم رمز و کد کاربر رابیدا کرد و با برنامه ها ی**FTP**مانند **CUTEFTP** به آن وارد شد.با در نظر داشتن پورتها ی مربوط به این سرویسها :

http ⟶ port ⟶ 80

ftp ⟶ port ⟶ 21

pop3 ⟶ port ⟶ 110

این سرویسها که پورت 110 مربوط به ایمیل می باشد.

بهترین برنامه برای کار با**FTP** :

tel ftp/pop password trier می باشد.

Nmap scanner

معرفی برنامه NMAP SCANNER

برنامه NMAP SCANNER برا ی بدست آوردن IP و پورتها ی متعلق بـه یـک کلاینـت و یایـک ISP اس است مورداستفاده قرار می گیرد اگر سیستم عامل مورد استفاده شـما ویـنـدوز اسـت می توانید از این برنامه با نام NMAP WIN V1.3.0 که یک نسخه از این برنامـه اسـت و توسـط تیم EEYE نوشته شده است را مورد استفاده قرار دهید. ولی باید به این نکته توجه کـرد کـه از NMAP WIN فقط درویندوز XP و2000 وNT می توان استفاده کرد.و نسـخه ایـی از ایـن برنامـه برای ویندوز های دیگر نوشته نشده است .

برنامه NMAP SCANNER بیشتر از خط فرمان استفاده می کندولی یکGUI خـوب هـم بـرایش ساخته شده است که NMAP FRONT END نامیده می شود.البتـه NMAP SCANNER نسـبت بـه نسخه گرافیکی اش کاملتر و بهتر اسـت و گزینـه هـای بیشـتری دارد کـه حتـی مـی تـوان یـک سیستم را به وسیله فرستادن بسته ها ی زیـادFLOOD کـرد و موجـب CRASH شـدن سیسـتم قربانی شد.ولی با NMAP WIN نیز می توان این کارها را به صورت کمی محدودتر انجام داد .

هنگامی که برنامه NMAP WIN باز می شودباگزینه ها ی زیادی مواجه می شویم :

HOST : دراین قسمت باید IP کامپیوتر هدف را واردکردکه هم میتواند یک IP متعلق به یک کلاینت باشد و هم می تواند تعداد زیادی IP متعلق به یک ISP و یا چندین سرور باشد.

اگر می خواهید تعدادی IP برای اسکن شدن به برنامه بدهید چندین راه وجود دارد.

برای مثال می توان یک رنج IP را بدین شکل وارد کرد 217,218.*.* که در نتیجه تمام IP هایی که با 217و218 شروع می شود توسط برنامه مور داسکن قرارمی گیردویا اگر رنج رابه صورت215-217,218,12,102 وارد کرد تعداد IP هایی که بین دو عدد آخر وجود دارد اسکن می شودو درمورد هر IP درصورت فعال بودن و تنظیم سریع برنامه اطلاعات زیادی دراختیار ما قرار میگیرد.

بخش SCAN:این قسمت مهمترین قسمت برنامه NMAP WIN می باشدکه خود به دو بخش MODE وSCAN OPTION تقسیم شده است .درقسمت MODE نوع پویش و حالت اسکنینگ رامشخص می کنید چون همانطور که می دانیدماچند نوع پروتکل در TCP/IP داریم مثل پروتکل پیام کنترل اینترنت (TCP) و یا پروتکل UDP و یا پروتکل اینترنت یا همان پروتکل IP و همچنین پروتکل پیام کنترل اینترنت (ICMP) و در این قسمت و قسمت DISCOVERاز برنامه نیز شما می توانید اسکن مختلفی درهر کدام از این پروتکل ها داشته باشید درکل کاری که پورت اسکنرها انجام می دهنداین است که بسته هایی به سمت سیستم هدف که همان IP داده شده به برنامه است و تمام پورتهای آن می فرستند و امتحان میکنند تابفهمند چه پورت هایی روی آن سیستم باز هستند واطلاعات بدست آمده را در اختیار هکر قرار میدهند.

در پورت اسکنرهای قوی نوع بسته های که فرستاده می شوند را مـی تـوان انتخـاب کـرد کـه NMAP WIN درقسمت FOLDER OPTION قسمت SCANEو گزینه MODE این امکان را به وجـود می آورد.

گزینه CONNECT :

این گزینه یک نوع اسکن و پویش از نوع TCP است که سعی میکند تا HAND SHAKE سه طرفـه TCP را با هر پورت هدف روی سیستمی که اسکن می شود را کامل کند.

برای انجام HAND SHAKE درابتدا کامپیوتر ما که یک کلاینت است به سمت سـرور یـک بسـته SYN می فرستد که یک درخواست برای اتصال است بعـداگر سـرور ایـن درخواسـت را قبـول کندبرای سیستم ما یک بسته SYN/ACK می فرستد که پاسخی است برای درخواست ما .

گزینه SYN STEALTH : این نوع اسکن که به آن پورت اسکن TCP SYN هم گفتـه میشـود پـیش فرض اسکنینگ هـا در برنامـه NMAP WIN مـی باشـدکه چنـدویژگی نسـبت بـه گزینـه کانکـت دارداول اینکه این نوع اسکن مخفی تر از پویش کانکت است به ایـن دلیـل کـه اسـکن TCP SYN فقط بسته SYN اولیه را به سمت پورت هدف می فرستدو منتظر جواب SYN_ACK می مانـد تـا بفهمد که پورت باز است یا نه ؟

اگر پورت باز باشد و سیستم قربانی بسته SYN ACKرا برا ی سیستم ما بفرستد برنامه NMAP WIN و این گزینه سریع یک بسته RESET برا ی سیستم قربانی می فرستد تا قبل از اینکه اتصال کامل شود آن را قطع کند پس دراین صورت دیگر کامپیوتر ما برا ی سرور بسته ACK نمی فرستد . اگر از طرف سرو ریک بسته SYN ACK برای ما فرستاده شودیعنی آن پورت باز است و اگر یک بسته REST یا RST/ACK برسد یعنی آن پورت بسته است.SYNسرعت این نوع اسکنینگ چون دو سوم HANDSHKE را انجام می دهد به همین دلیل از نوع اسکن کانکت سریعتر به نتیجه می رسدچون دیگر بسته ACKبه سمت

سمت سرور با این نوع اسکن و فرستادن بسته های SYNشود به احتمال زیاد (بستگی به قدرت آن سرور و هماهنگ بودن هکر ها) آن سرور DOMAINمی شود .

گزینه های NULL SCANE وXMAS TREE وFIN STEALTH این نوع پویش ها واسکن ها برای سیستم ها ی ویندوز نوشته نشده است چون سیستم های ویندوز از RFC ها درمورد اینکه اگر بسته هاNULL ی وXMAS TREE و FIN STEALTH وارد شوند چه زمانی بایدRESETفرستاد پیروی نمی کنند ،برا ی مثال کاری که گزینه FIN STEALTH می کند به این صورت است که یک بسته FIN به هر پورت می فرستدکه اگر درپاسخ بسته RESETنشان داده شود یعنی اینکه پورت بسته است و اگر پاسخی دریافت نشود یعنی اینکه ممکن است پورت باز باشد ولی درکل این چندگزینه برای اسکن کردن کلاینت ها و سرور هایی که از سیستم عاملهایی غیر از ویندوز استفاده میکنندبکار میروندو خیلی هم سودمنداست.

گزینه PING SWEEP : این نوع اسکن نیز IP های فعال دریک شبکه و درآن رنج IP داده شده را پیدامیکندومیشود گفت این گزینه همان کار IPای اسکنینگها را انجام میدهد و برای این کار برنامه NMAP WIN یک بسته درخواست ICMP ECHOرا به تمام آن IP ها می فرستد تا مشخص شود که کدام سیستمها درآن لحظه فعال هستند،درهرصورت از این گزینه نیز می توانید برا ی پیدا کردن IP های فعال دریک ISP استفاده کنیدوسپس به وسیله توضیحاتی که داده شدهر کدام از آن IP هارا برای پیداکردنپورتهای باز اسکن کنید.

گزینه UDP SCAN : همانطور که از اسمش پیداست این گزینه برا یاسکن کردن پورتهای UDP

میخواهند توسط پورتهای UDPبه سیستم قربانی متصل شونداین گزینه مناسب میباشد.

گزینه IP PROTOCOL SCAN & ACK SCAN : این گزینه برای اسکنینگ IP ها ومشخص کردن IP ها ی فعال ودادن اطلاعاتی درموردهر IP به کارمیروندکه تقریبا این گزینه همان کار گزینه PING SWEEP انجام میدهند ولی این گزینه ASK SCANکه بیشتر برای تشخیص FIRE WALLها استفاده می شودوطرز کارش به اینصورت است که یک بسته با کدبیت ACKرا به تمام پورتها ی موجوددرسیستم قربانی میفرستدوامکان فیلترکردن بسته ها را دراتصالهای برقرار شده می دهد و نتایج بدست آمده اطلاعات ارزشمندی را دراختیا رهکر قرار می دهد از جمله لیستی از پورتهایی که به اتصالها ی برقرار شده اجازه ورودبه شبکه را می دهد که درنهایت به ما کمک می کندکه مسیریابها و دیواره ها ی آتش یک سرور را پیدا کنیم .

گزینه WINDOW SCAN : این نوع اسکن تقریبا مثل اسکن ACKاست ولی برای فهمیدن باز یا بسته بودن پورت روی چندین سیستم عامل ،روی اندازه TCP ویندوز تمرکز می کند وکلا این نوع اسکن کاملتر از پویش ACKاست .

گزینه LIST SCAN & ORCP SCAN : اسکن از نوع LIST SCANتقریبا همان کار اسکن PING SWEEPرا انجام میدهدولی به صورت مخفیانه تر و می توان با استفاده از این قابلیت یک اسکن NMAP TCPرا از یک سرور FTPعبور داد تامبدا ءحمله را مخفی کردولی اسکن از طریقه RCPیکی از کاملترین نوع اسکنینگ و سرویسها یRPCرا اسکن می کند وبرای فرستادن دستورهایش ازتمام پورتها یTCP و UDPبان درسیستم قربانی استفاده میکنده

گزینه POTR RANGE : با انتخاب این گزینه وفعال کردن آن می توان رنج پورتهایی که لازم است درآن سیستم اسکن شود واردکردتاپورتهای باز در آن سیستم و درآن رنج پورت را نشان دهد و اگر این قسمت خالی گذاشته شود درآن سیستم هایی که درIPHOST هایشان نوشته شده است تمام پورتها اسکن می شودو اگر فقط یک شماره پورت دراین قسمت وارد شود فقط آن پورت درآن سیستم اسکن خواهد شد.

بخش DISCOVER : این بخش نیز یکی دیگر از قسمتها ی OPTIN FOLDER برنامه NMAP WINاست که به چند گزینه تقسیم میشود:

گزینه TCP PING : این گزینه برا ی پینگ در TCPبکار میرودوبافرستادن پینگ که به آن پیام ECHO ICMPهم گفته میشودبرای IP هاوسیستم ها ی مشخص شده دربرنامه می توان فهمید که کدام یک از سیستمها فعال هستند وپس از این کا ر می توان پورتهای آن سیستم های فعال را اسکن کرد.

گزینهTCP+ICMP : این گزینه که پیش فرض قسمت DISCOVER هم هست برای پین گ کردن سیستمها درهر پروتکل TCP وICMPبکار می رودو دربخش DISCOVER یکی از بهترین گزینه ها همین است.

گزینه ICMP PING : این گزینه برای پینگ کردن سیستمها در پروتکل کنترل پیام اینترنت (I CMP) بکار می رود وفقط مخصوص این پروتکل می باشد.

گزینه DON'T PING :بافعال کردن این گزینه برنامه هیچ نوع پینگی انجام نمی دهد و کلا بخش DISCOVER از اسکن برنامه حذف و غیر فعال می شود.

بخش OPTION :

گزینه FRAGMENTATION : این گزینه زمانی برای ما مفید است که مخفی اسکن کردن از تنیجه اسکن برای ما اهمیت بیشتریداشته باشد، این گزینه از IP های مبداءبرای اسکن استفاده میکندوبه وسیله روشهایی IP هکر وکلا هر اطلاعاتی را جع به شخص اسکن کننده را پنهان میکند و بیشتر این گزینه زمانی مفیداست که اسکنی از نوع S YN-FIN XMAS ویا NULL صورت بگیرد ولی درهرصورت با انتخاب این گزینه کمی از کارایی برنامه و نتیجه پایانی اسکن هم کم می شود.

گزینه GET INDENT INFO :این گزنه نیز برای زمانی مفید است که بخواهیم سیستمی را از نوع پویش CONNECT اسکن کنیم و میشود گفت این گزینه مکمل اسکن CONNECT بشمار میرود و باانتخاب این گزینه بهمراه پویش اسکن اطلاعات ارزشمندی میشود از یک سرور بدست آورد.

گزینه RESOLVE ALL : از این گزینه نیز شما میتوانید برای پیدا کردن DNS(DOMAIN NAME (SERVER ها درسیستمها و IP های داده شده به برنامه استفاده کنید،البته این گزینه بر روی تمام آیپی های داده شده به برنامه عمل REVERSE WHOIS را انجام میدهدو برایش فرقی نمیکند آن IP فعال هست یا نه و از همه WHOIS میگیردو این گزینه نیز برای پیدا کردن سرور ها و DSN ها خیلی مفیداست.

گزینه DON'T RESOLVE : این گزینه نیز همانطور که از اسمش مشخص است عمل REVERSE WHOIS را رو ی هیچ کدام از سیستمها انجام نمیدهد و از هیچ RESOLVE IP نمیگیرد وبیشتر برای زمانی خوب هست که شما برای اسکنتان احتیاج به سرعت دارید که دراینصورت میتوانیداز این گزینه استفاده کنید.

گزینه FAST SCAN : با انتخاب این گزینه سرعت اسکن بیشتر می شود ولی وقتی که سرعت بیشتر باشد نتیجه اسکن ضعیفتر از حالت عادی اسکن هست ولی اگر شمابه سرعت احتیاج دارید میتوانیداز این گزینه استفاده کنید.

گزینه OS DETECTION : این گزینه که گزینه پیش فرض قسمت OPTIN هم هست یکی از مهمترین گزینه های برنامه است که کارش حدس زدن و فهمیدن سیستم عامل سیستم درحال اسکن است .NMAP WIN تنها با داشتن IP می تواند نوع سیستم عامل را شناسایی کند،برا یاین کارانم از یک تکنیک به نام کپی برداری از پشته TCP/IP استفاده می کند وبا کمک گرفتن از RFC ها بسته هایی را به پورتها ی مختلفی رو ی سیستم هدف میفرستدوچگونگی تغییر شماره سریال دربسته SYN ACK را بررسی میکندو درنهایت نوع سیستم عامل ر احدس می زند.

گزینه RANDOM HOST : این گزینه نیز به IP هـای داده شـده درقسـمت HOST برنامـه توجـه نمیکند و IP هایی را به صورت اتفاقی انتخاب میکند و سپس اسکن می نماید.

قسمت DEBUG وگزینهDEBUG : این گزینه اولین گزینه قسمت DEBUG که درقسـمت OPTION قرار داردکه برای DEBUG کردن به کار میرود و با انتخاب این گزینه نتایج DEBUGرا شما می توانید درقسمت OUTPUT برنامه ببینید.

گزینهVERBOSE & VERY VERBOSE : این دو گزینه نیز جزئیات و مراحل اسکن و DEBUG را نشان میدهد.یک نکته قابل توجه این است که مکمل ایـن اسـکن گزینـه V E RY VERBOSE می باشد.چون این گزینه نسبت به گزینه VERBOSE کـارایی بیشـتری داردو مراحـل اسـکن و DEBUG را دقیق تر نشان میدهد.

بخش TIMING : این بخش خود چندقسمت دارد که بـه توضـیح قسـمت اول آن (THROTTLE) می پردازیم :

هکر ها باتوجه به نوع اسکن وزمانی که دارندسرعتهای اسکن مختلفی را انتخاب میکنند که بستگی به سرعت وقدرت سیستم قربانی هم دارد. برای مثال اگر سرعت سیستم قربانی کند باشدو یا ما یک نوع اسکن سریع را انتخاب کنیم ممکن است بعضی از پورتهای باز را از دست بدهیم و یاممکن است که آن سیستم به خاطر بسته های زیادی که برایش فرستاده می شود هنگ و CRASH کند . این قسمت ا زبرنامه NMAP WIN برای تنظیم سرعت اسکن به کار می رو د که گزینه نرمال بهترین انتخاب برا ی این کا راست و اگر سیستم شما ضعیف بودو درحال اسکن با این سرعت هنگ کرداز گزینه POLITE استفاده نماییدکه سرعت کمتری داردو هر بسته را تقریبا درچهارثانیه برای سیستم ها ی قربانی می فرستد و بیشتر برای زمانی خوب است که شما وقت کافی برای اسکن دارید.

قسمت TIME OUTS : این قسمت بیشتر برای زمانبندی هر اسکن وپویش به کار می رود و قابلیت سفارشی کردن زمان اسکن را به شما می دهد.

بخش FILES : این بخش نیز خودچندقسمت دارد که بیشتر برای ذخیره کردن نتایج اسکن به کار میرود:

قسمت INPUT FILE : این قسمت تقریبا کار یک PASS LIST دربرنامه ها ی کراکر و B RUTB FORCE رامی کندو برای سریعتر کردن کادر اسکن میشود از این قسمت استفاده کردکه دراین حالت ورودی از فایلی که انتخاب کرده ایم خوانده می شود.

قسمت OUTPUT :با انتخاب این گزینه می توان نتایج بدست آمده از اسکن را که در OUTPUT نشان داده می شوددریک فایل با فرمت های مختلف ذخیره کردتا بتوان از روی فرصت پورتها و حفره ها ی باز روی آن سیستم را موردبررسی قرار داد. با انتخاب گزینه نرمال نتایج بدست آمده به صورت ROG و.TXT ذخیره میشودو میتوان فرمتهای دیگری مثل XMLیا GREP را انتخاب کرد.

بخش SERVICE : این قسمت هم برای سفارشی کردن زمان و روز اسکن IP های مشخص به کار می رودو برا ی مثال میتوان یک IP را دراین قسمت ثبت کردو یک روز رامشخص کرد و برنامه درصورت انتخاب گزینه AUTOSTART درآن روز مشخص خودبه خودآن IP و سیستم را اسکن میکندو حتی میتوان دقیقه و ثانیه شروع عملیات اسکن را دراین قسمت مشخص کرد.

بخش WIN32 : این بخش نیز که قسمت آخر برنامه NMAP WIN است برا ی تنظیم بهتر برنامه درویندوزهای XPو...می باشدکه خودچندقسمت داردچون قسمت COMMAND برا ی کسانی مفیداست که با NMAP WIN تحت LINUX کار کرده اندو با خط فرمان آن آشنایی دارند پس به توضیح آن می پردازیم.

گزینهNO PCAP : موقع نصب برنامه PCAP NMAP WIN هم به همراه آن نصب می شودکه برای ویندوزهای 2000وXP نوشته شده است و دراین ویندوزها میتواندمکمل NMAP WIN کارها ی پویش را انجام دهد،باانتخاب این گزینه برنامه دیگر از PCAP استفاده نمیکند وPCAP غیر فعال می شودو اگر این گزینه را انتخاب کنیم برنامه به جای PCAP ا زRAW SOCKET به صورت پیش فرض استفاده می کندواز آن کمک می گیرد.

گزینه NO RAW SOKET : اگر این گزینه انتخاب شودRAW SOKET غیر فعال میشودوتوسط برنامه دیگری استفاده نمیشودو اگر گزینه NO PCAP انتخاب نشده باشدبرنامه از PCAP به عنوان مکمل و البته درویندوز های XPو...استفاده میکند.

گزینه FORCE RAW SOKET :اگر این گزینه را انتخاب کینددیگر PCAP غیر فعال میشود وفقط RAW SOKET توسط برنامه استفاده میشود.

گزینه NT4ROUTE : این گزینه نیز برای کاربران سیستم NT 4.0 است که این نسخه NMAP WIN را در ویندوزشان استفاده میکنند و با انتخاب این گزینه درصورت استفاده از ویندوز NT مسشوداطلاعات ارزشمندی درموردانواع فایروالهای روی سرورها و کلاینتها بدست آورد.

گزینه WIN TRACE : این گزینه نیز یکی از بهترین گزنه های برنامه NMAP WIN است که کارش استفاده از تکنیک TRACE ROUTE برای پیداکردن روترهاوGATEWAY های یک سرور وبا انتخاب این گزینه برنامه برای هر IP عمل TRACE را انجام میدهدواطلاعات اززشمندی درباره ه رسیستم دراختیار شما قرارمیدهد البته این گزینه کمی از سرعت اسکن رامیگیردولی به نظرمن ارزش این را داردوشما نیز سعی کنید از این گزینه به عنوان مکمل برنامه واسکنتان استفاده کنید.

Filename:	MEDYA SOFT.doc
Directory:	C:\My Documents
Template:	D:\Documents and Settings\SMN\Application Data\Microsoft\Templates\Normal.dot
Title:	تاریخچه hacking
Subject:	
Author:	ara
Keywords:	
Comments:	
Creation Date:	12/22/2003 9:09 AM
Change Number:	85
Last Saved On:	5/29/2003 9:48 PM
Last Saved By:	kavan haddadian
Total Editing Time:	2,122 Minutes
Last Printed On:	6/17/2003 7:16 PM
As of Last Complete Printing	
Number of Pages:	77
Number of Words:	11,377 (approx.)
Number of Characters:	64,855 (approx.)