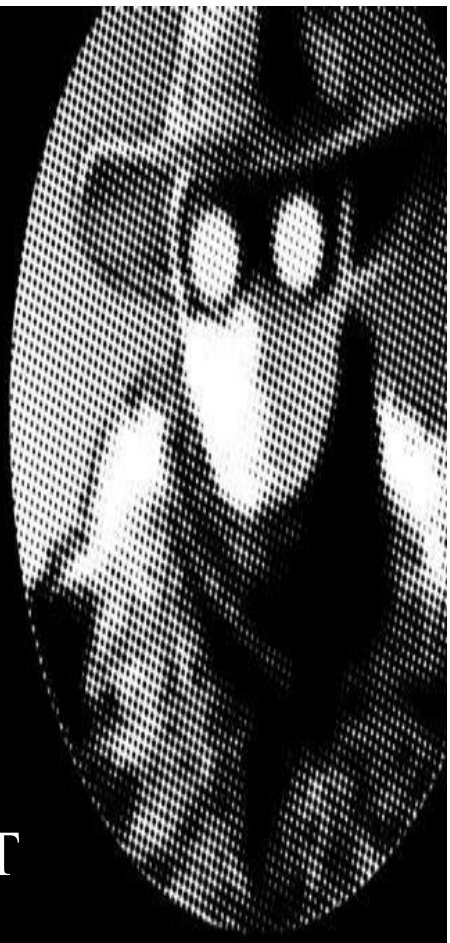
BLOG Hacking



By : Invisible Man

Invisible Team Peresent

Www.InvisibleTeam.NeT

Complete Explain About BLOG Hacking

Invisible Digital Security Team ™®

SHADOW OF THE

INVISIBLE MAN

Invisible Digital Security Team
Www.InvisibleTeam.NeT

به نام تنها خالق هستی

نام مقاله : مرجع کامل آموزش وبلاگ داری و هک آن
نام نویسنده : ساسان سیفی
سطح مقاله : مقدماتی به حرفه ای
تاریخ : 25 . 10 . 1384
منبع :

www.invisibleteam.net
Shabgard Security Group

با تشکر فراوان از دوستان :
Of Invisible Team = (Alikhoub – Hacker – Subzero – Agape – Mehrun)
Of IHS Team = (Majid NT – C0d3r – L0rd)
Of IBBH Team = (yt3m_$h4r3 – l2odon – MaX666)
Of IHC Team = (ErRoR_Sir)
Of Y! Team = (Y4ho0 – Sisil – Satanic_Soulfol)
Of Emper0r Team = (Im4n – Farhad)
Eblis_Empire & All Other Friends That Help Me To Write Journals …….

فهرست مطالب :

فهرست مطالب :

مقدمه :

در این دوره که دنیای اینترنت در حال جانشینی به جای تمام موارد می باشد عده ای تمایل به داشتن سحمی از این دنیا را دارند که بعضی افراد که از اوضاع مالی خوبی برخوردارند با تاسیس یک سایت اینترنتی و بعضی دیگر با استفاده از سرور های رایگان وبلاگ دهی بسته به علاقه خود سایتی شخصی را راه اندازی کرده و در آن شروع به فعالیت می کنند.
در این بین هم همواره و همیشه عده ای هکر برای اتمام هدف خود :
۱- رسیدن به شهرت
۲- اثبات قدرت
۳- اهداف رو کم کنی
....
ترس را بر جان صاحبان و مدیران این سایت ها و وبلاگ ها می افکنند که در این بین راهای بسیاری جهت حمله و دفاع در این بین وجود دارد.
ما در این مقاله ابتدا نحوه حمله و سپس دفاع را به شما آموزش می دهیم.
به امید روزی که به توانیم با بالاترین امنیت ممکن سایت خود را به راحتی اداره کنید.
پس وقت را از دست ندهید و دست به کار شوید.

آشنایی با چند سرور وبلاگ دهنده :

امروزه تعداد بسیاری سایت وجود دارد که به عنوان یک امکان اضافه به کاربران خود می تواند به آن ها وبلاگ شخصی بدهد مانند همین سایت تیم ما ...
www.invisibleteam.net
اما سایت های دیگری هم هستند که هدف اصلیشان وبلاگ دهی می باشد حال با نام چند تا از آن ها آشنا خواهیم شد :

1- www.blogfa.com
2- www.mihanblog.com
3- www.parsiblog.com
4- www.persianblog.com
5- www.blogsky.com
6- www.persiangig.com*

*= این سایت در واقع سرویس وبلاگ نمی باشد بلکه یک هاستینگ ۱۰۰ مگا بایتی رایگان برای ایرانیان است که می توانند برای وبلاگ هم استفاده کنند اما کاری نیست که افراد عادی و نا آشنا با امور زبان برنامه نویسی وب به آسانی انجام دهند.
خوب در ضمن بگم که بالاترین امنیت هم واسه همین سرور هست اما سایر سرورهای دیگر هم مانند بلاگفا از امنیت بالایی برخوردار هستند اما من به هیچ کس سرور پرشین بلاگ رو توصیه نمی کنم .

توضیح روش های هک :

در کل برای هک کردن یک وبلاگ ۲ روش بیشتر وجود ندارد اما بعضی ها روش های دیگری را هم می گویند اما در اصل آن ها نحوه تکامل یافته و با تغییر جزئی از همین روش های اصلی هستند.

۱- نفوذ به سرور (Server Hacking)
۲- هک کردن صاحب وبلاگ (Client Hacking)

خوب در ابتدا یه توضیح مختصر درباره هرکدام می گم تا کمی آشنا شوید.

نفوذ به سرور :

در این روش شما چند راه دارید :

۱- نفوذ مستقیم به سرور
۲- گوش دادن به سرور
۳- استفاده از اکسپلیت ها

توضیح بیشتر این ها در قسمت های بعدی مقاله می باشد در اینجا فقط هدف آشنایی با نام می باشد.

هک کردن صاحب وبلاگ :

این روش یکی از ساده ترین روش ها می باشد که نسبت به هوض هکر و صاحب وبلاگ سختی آن زیاد یا کم می شود.

در این روش شما ابتدا سیستم صاحب وبلاگ و سپس ایمیل وبلاگ او را هک می کنید و بعد از انجام این عمل و به دست آوردن اطلاعات کافی و مورد نیاز برای هک کردن وبلاگ حمله اصلی خود را آغاز می کنید و وبلاگ طرف هک می شود.

من بر اساس عادت همیشه اول روش های دفاعی را توضیح می دهم بعد روش حمله برای همین در این قسمت ابتدا با روش های دفاعی آشنا می شوید.

دفاع در برابر حملات :

عموما در تمامی سرور های وبلاگ دهی ایمیلی از شما به عنوان ایمیل پشتیبانی سوال می شود.
زمان استفاده از این ایمیل وقتی هست که شما در خواست فرستادن پسورد خود را می کنید حال امکان دارد که پسورد را فراموش کرده باشید یا ..... .
خوب هکر شما هم دقیقا از همین روش استفاده می کند.
چون عموما تمامی افراد در محل ایمیل پشتیبانی یاهو میل خودشون رو می دهند هکر هم می تواند به راحتی ایمیل یاهو آن ها را هک کرده و به سرور رفته و درخواست پسورد کند و به همین راحتی پسورد شما را به دست آورد پس شما باید جهت حفظ امنیت در آن محل ایمیلی را وارد کنید که از یک سرور نا شناخته یا کاملا امن باشد .
برای مثال Gmail – Walla - Mail از جمله بهترین گزینه ها برای انتخاب شما هستند.البته روش هایی برای هک کردن این وارد هم هست که در قسمت آموزش هکینگ توضیح داده می شوند.
در مورد دفاع در برابر حملات روی سرور هم شما هیچ کاری جز اطلاع رسانی به سرور نمی توانید انجام دهید.برای همین در انتخاب یک سرور امن دقت کنید.

انتخاب سرور :

برای انتخاب یک سرور شما باید تعدادی معیار برای خود در نظر بگیرید و سپس در قسمت امکانات آن سرور به مطالعه بپردازید تا مطلع شوید که آیا امکانات شما را دارند یا خیر.

امکانات برتر :

۱- بالاترین سرعت در بار گذاری صفحات
۲- امکان مدیریت ساده
۳- ایمیل پشتیبانی و امور بازدید مجزا
۴- امکان تغییرات ساده در قالب بندی صفحات
۵- امکان داشتن وبلاگ گروهی
۶- امکان موضوع بندی مقالات

هم اکنون بهترین سرور که کاملا دارای این موارد باشد سرور بلاگفا می باشد که از جمله برترین سرورهای وبلاگ دهی می باشد اما این چند روزه اخیر به علت کشف تعداد زیادی باگ بر روی این سرور درجه اطمینان آن کاهش یافته و هم اکنون گزینه اول انتخاب کاربران سرور میهن بلاگ می باشد که من خودم تا الان باگی رو این سرور ندیده ام.

نحوه هک کردن یک وبلاگ :

یک وبلاگ در حالت کلی به این صورت هک می شود که پسورد آن کشف یا لو می رود و سپس هکر در قسمت ورود به مدیریت وبلاگ مشخصات را وارد کرده و وارد قسمت مدیریت می شود سپس در قسمت عوض کردن قالب , قالب های صحفه اصلی و قسمت آرشیو را با قالبی که برای صحفات هک خود طراحی کرده است عوض می کند و در انتها با تعویض مشخصات پیش فرض و تعویض رمز عبور آن وبلاک را به طور کامل هک می کند.

نکته برای هکرهای حرفه ای :
بعضی سرورهای وبلاگ مانند میهن بلاگ هنوز به طور رسمی در سایت جهانی Zone – H شناخته نشده اند که شما می توانید با هک آن ها درجه خود را افزایش دهید.

حالا که این رو گفتم جا داره از دوست خوبم Alir9 که این نکته جالب رو به من گفتن تشکر کنم اما چه فایده دیگه Zone – H هم مارو بنیده و ما بی خیال درجه شدیم.

آموزش روش شماره ۱ :

خوب در این روش شما یاد خواهید گرفت که چگونه سیستم صاحب وبلاگ رو هک کنید.
در ابتدا باید ایمیل ادمین رو بدست بیارید (اگر یاهو باشه خیلی خیلی بهتر هست) .
خوب اگر ایمیل دیگری هم بود می توانید یه میل بزنید و توش بهش بگید که با یاهو آیدیش شما رو Add کنه.
خوب بعد از بدست آوردن ایمیل شما باید سرور اون میل رو شناسایی کنید ما در اینجا فقط پیرامون سرور یاهو صحبت می کنیم.
بر فرض اینکه ایمیل طرف روی سرور یاهو باشد شما باید با استفاده از یکی از روش های مربوطه اون شخص رو هک کنید.
بهترین و کاربردی ترین روش استفاده از تروجان هست که من به شما (IHZ PS Ver 1.2) توصیه می کنم چون خودش کی لاگر هم داره و اصلا کار خیلی راحت تر می شه اما با تروجان های خیلی ساده تر هم مثل مجیک می شه چون هدف اصلی پسورد و رمز عبور ایمیل یاهو می باشد.البته من بیشتر یه تروجان پیشرفته رو توصیه می کنم چون یه کی لاگر قوی می تونه خیلی کمک ها به شما بکنه تا راحت تر اون رو هک کنید.

خوب حالا وقتی پسورد قربانی برای شما ارسال شد باید در اولین قدم آدرس سرور و نام کاربری رو پیدا کنید . به مثال زیر توجه کنید :

Blog Url : www.X.persianblog.com
User Name : X
Password :
E-mail : You Find In Hack + Password

حالا این امر در سرورهای مختلف فرق می کنه برای اینکه بیشتر متوجه بشید یه مثال تو میهن بلاگ :

Blog Url : www.X.mihanblog.com
User Name :
First See Blog In It You Will See That

نوشته شده توسط Sasan

Here Sasan Is Your User Name
Pass & E-mail You Will Find

خوب امیدوارم متوجه شده باشید سعی کردم تاجی که می شه واضح بگم.

بعد از پیدا کردن نام کاربری به قسمت ورود به مدیریت وبلاگ می روید و در آن قسمت بر روی فراموش کردن رمز عبور یا رمز عبورم را فراموش کرده ام (هر چی ممکن هست باشه یه چیزی که تو این مایه ها بود بزنید چون این قسمت به سرور ربط داره) خوب در قسمت بعدی از شما یا فقط ایمیل رو می خواد یا نام کاربری رو هم می خواد که شما هر دوتا رو دارید با خیال راحت می توانید اون هارو وارد کنید و منتظر دریافت ایمیل حاوی اطلاعات از سرور باشید.

در اینجا ممکن هست شما به ۲ تا مشکل برخورید :

۱- اگر وبلاگ رو سرور بلاگ اسکای باشه اصلا برای فراموش رمز عبور چیزهایی رو که می خواد به هیچ وجه نمی شه بدست آورد.
۲- شاید پسورد طرف جوری باشد که شما نتوانید تو میل اون را کامل بخوانید یا اصلا نشه بخوانید.
مثل اینکه بین پسورد از Space استفاده شده باشه که در ایمیل نمی یفته.
خوب حالا چی کنیم ؟!؟!؟
هر کدام را در محل مورد نظر توضیح می دم اما باز هم می گم که اگر از یه تروجان کامل استفاده کنید خیلی بهتر از این هست که بخواید خودتون رو خسته کنید ولی نکته مهم این هست که آخرش هک می شه !!

در آوردن پسوردها از ایمیل :

همان طور که می دانید پسوردهایی هستند که در صحفه هایی که با کد HTML طراحی شده اند نشان داده نمی شوند.این پسورد ها ۲ دسته هستند دسته اول بر اثر تکرار بالا دیده نمی شوند و دسته دوم از خود تگ های HTML می باشند.
برای دیدن این مدل پسوردها کافی هست که مدل صحفه میل خود را به حالت < Basic > در بیاورید.
در حالت تگ ها از کار می افتند در صورتی که باز هم پسورد کامل نشان داده نشد مدل های دیگر را امتحان کنید اما معمولا در همین حالت اکثر پسوردها دیده می شوند.
برای عوض کردن مدل صحفه در سرور Gmail می توانید از قسمت Option استفاده کنید و برای سرور Yahoo از گزینه Mail Option استفاده کنید.
فقط دقت کنید که در این میان بعضی وقت ها ایمیل های فرستاده شده به جای قسمت Inbox به قسمت Bulk می روند و گاهی اوقات هم با حدود ۱۲ ساعت تاخیر بر اثر شلوغی سرور یا به هم ریختن آن می رسند برای همین بیشترین دقت را به خرج بدهید.

چگونه سوالات امنیتی را رد کنیم :

همان طور که می دانید در سرور < BlogSky > وقتی بر روی گزینه ((رمز عبور را فراموش کردم)) کلیک می کنید سوالات امنیتی از شما پرسیده می شود که هیچ کس به جز فردی که وبلاگ را ساخته است نمی داند و در هیچ محلی هم نمی توان آن را تغییر داد . البته این اطلاعات برای سرور قدیم است هم اکنون این سرور تغییرات زیادی را انجام داده است.

مدیریت جدید بر روی این سرور بسیار سخت شده است البته نکته ای که به آن اضافه شده است که شما می توانید مقداری فایل بر روی FTP وبلاگ خود بگذارید که اگر خیلی حرفه ای باشید با قرار دادن یک فایل که با آن بتوان از سرور شل گرفت می توانید کل سرور را بدست بگیرید و به طور کامل هک کنید.

من در اینجا این روش رو توضیح نمی دم.

اما برای رد کردن سوالات امنیتی ۲ راه است :

۱- با حقه از زیر زبون صاحب وبلاگ بکشید بیرون.

۲- با یه ایمیل دروغی از طرف همون ایمیل که هک کردید به سرور بگید که فراموش کردید تا بهتون بده.

توضیح روش شماره ۲ :

این روش با نام مهندسی اجتماعی معروف است.
این روش مخصوص آدم های الاف هست اما اگر نتوانستید از روش های دیگر هک کنید دیگر باید به این روش رو بیارید.لازم به ذکر هست که این روش رو همه چیز حتی سایت ها حتی سایت ما و حتی سایت های خیلی بزرگتر در حد یاهو هم عمل می کنه اما چی مهم این هست که ادمین خام نشه که یه ادمین کار کشته هرگز تن به این خطر نمی ده.
این روش خیلی ساده هست و عموما پسرها راحت گول می خورند.خلاصه روش این هست که ادمین گول می خوره و یوزر و پسورد رو به شما می ده.
خوب اگر شما با یه آیدی دختر به یه پسر بگید که مثلا می خواهید که با او همکاری کنید یا می خواهید قالب را عوض کنید یه ذره هم بتونی خوب نقش بازی کنی می تونی خیلی راحت گولش بزنی و پسورد رو بگیری.البته این روش رو وبلاگ های گروهی کمتر جواب می ده چون طرف امکان داره بیاد یه مدیر دیه با دست رسی کمتر تعریف کنه اگر باز هم خوب نقش بازی کنی پسره خام می شه پسورد رو می ده.یادش به خیر من خودم یه بار از این روش حدود ۴ سال پیش وبلاگم هک شد.

روش هک شماره ۳ :

این روش یکی از موثرترین روش های هک کردن وبلاگ می باشد چون شما با این روش به طور مستقیم به خود سرور نفوذ می کنید و می توانید هر آنچه را که بخواهید بدست آورید حال اگر اطلاعات شما پسورد باشد تا سایر اطلاعات محرمانه روی سرور می باشد که بعد از نفوذ شما کاملا به همه چیز دست رسی دارید اما این نکته را به یاد داشته باشید که همواره باید جنبه آموزش دیدن رو داشت نه این که اگر روش رو کامل یاد گرفتید و می توانستید برید کل دنیا رو سرور وبلاگ رو هک کنید بله به شهرت می رسید اما چه فایده کلی دشمن تراشی هم کردی باور کنید نصفشون هم باورتون نمی کنند چون می گند سرور ضعف داشت در ضمن اگر خیلی هک شاخی برو با اونو که واست شاخ هست در بیفت نه اینکه با یه عده که حتی شاید ندونند هک چی هست !! خیلی شاخ بودی بده شاختو برات بتراشن !! همیشه یادت باشه فقط گاو شاخ دار می شه !! دیگه توضیح ندم چون فهمیدی منظورم چیه !! آخه واقعا این کارها عاقبت ندارد .....

خوب بریم سر اصل مطلب اون هم اینکه چه جوری به سرور نفوذ کنیم ؟!؟!؟

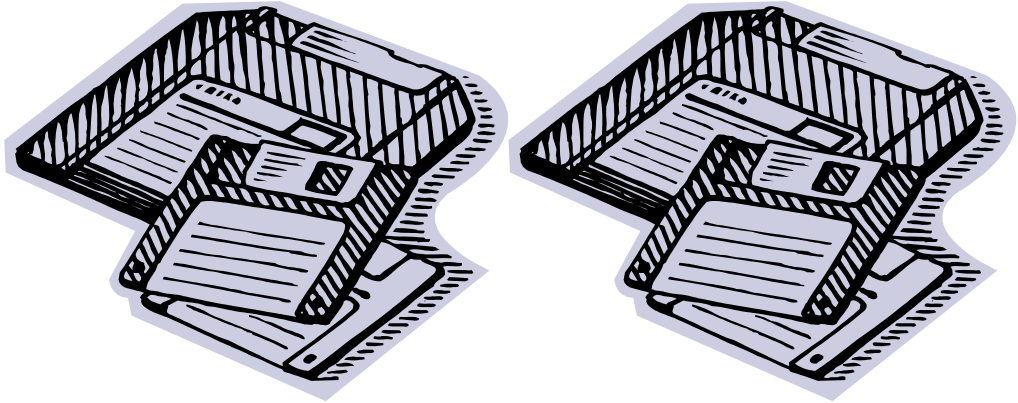
خوب برای نفوذ به سرور شما ابتدا باید به چند نکته دقت کنید :

۱- هدف از نفوذ چیست ؟
۲- جمع آوری اطلاعات از هدف معلوم شده !!
۳- نفوذ به سرور و انجام و دریافت موارد لازم !!
۴- پاک کردن رد پا ها و خروج و اطلاعیه پایان کار !

خوب حالا شروع به توضیح هر قسمت می کنم :

هدف از نفوذ چیست ؟؟

شما باید معلوم کنید که به چه علتی می خواهید نفوذ کنید مثلا هک کردن فقط یک وبلاگ یا تست امنیت سرور یا خدا نکرده هک کردن کل سرور که این قدم واقعا مهم هست بعضی وقت ها طرف بعد از ۴ ساعت به سرور نفوذ می کنه تازه می فهمه که چی < ای وای این سرور نبود > !!!!!!



جمع آوری اطلاعات از هدف ؟؟

خوب شما قبل از انجام هرکاری باید با هدف خود کاملا آشنا شوید و از آن به طور کامل اطلاعات جمع آوری کنید.
از جمله مهم ترین نکات می توان به موارد زیر اشاره کرد که قبل از شروع حمله باید معلوم شود :

۱- سرور از چه پرتالی استفاده می کند ؟!؟
۲- نقاط ضعف این پرتال چیست ؟!؟
۳- نحوه عملکرد با این پرتال چگونه هست ؟!؟
۴- آدرس سرور اصلی چیست ؟!؟
۵- نحوه سرویس دهی این سرور چگونه است ؟!؟
۶- نام کاربری قربانی چیست ؟!؟
۷- ایمیل به کار رفته چیست ؟!؟
۸- آخرین زمان به روز کردن کی بوده است ؟!؟

این موارد از جمله مهمترین گزینه ها هستند که شما باید از آن مطلع شوید.
حال به توضیح هر کدام که چگونه اطلاعات را بدست بیاوریم می پردازم ...

برای اینکه بهفهمیم سرور از چه پرتالی استفاده می کند در ابتدا باید با مفهوم پرتال آشنا شوید :
< پرتال یک نرم افزار مدیریتی می باشد که برای اداره سایت ها به کار می رود و در هر سایتی بنا به خواست مدیر سایت و نوع کار آن فرق می کند >
از جمله پر مصرف ترین پرتال ها می توان به :
< PHP – ASP – HTML – Vbulltion >
اشاره کرد.که بیشترین حفره های کشف شده برای پرتال PHP می باشد اما هنوز هم این پرتال به عنوان پر کاربرد ترین پرتال می باشد.زیرا مدیریت آن بسیار ساده است و دارای عناصر گرافیکی جالبی می باشد.
عموما سرورهای وبلاگ از پرتال ASP استفاده می کنند اما این که بفهمیم کار ساده ای است.مثال ها را با دقت بخوانید و دقت کنید :

www.X.com/Index.php <=== PHP Portal
www.X.com/search.asp <=== ASP Portal

خوب گمون کنم فهمیده باشید اما باز هم یه توضیح می دم که اون هم این هست که اگر در هر صحفه ای از سایت نام پسوند یکی از دو مورد بالا باشد یعنی پرتال اون سایت هم از همین می باشد اما راه دیگری هم می باشد که خیلی ساده است.

اگر در آخر صحفه اصلی سایت یکی از موارد زیر بود نشان دهنده پرتال آن سایت است :

Powered By PHP-Nuke
PHPBB ===> PHP Portal

اگر تو عنوان صحفه اصلی سایت مانند زیر باشد یعنی پرتال آن هم از همین می باشد :

X – Powered By VBulltion => VB Portal

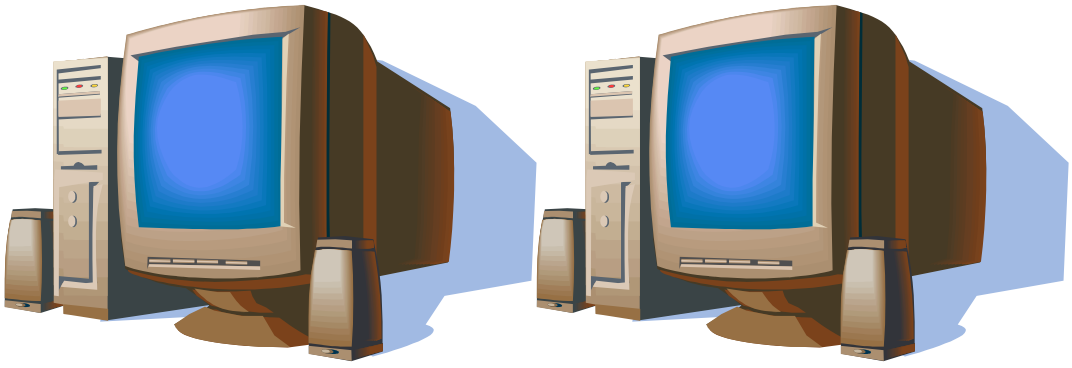
حال اگر هیچ یک از موارد بالا در سایت نبود یعنی اینکه سایت از پرتال < HTML > است.
به همین راحتی شما پرتال سایت رو بدست آوردید.
حالا این که نوع پرتال رو بدست آوردید خیلی مفید هست چون می تونید دونبال باگ هایی که از قبل کشف شده اند هم استفاده کنید.
برای اطلاع این آخرین باگ های کشف شده باید به سایت هایی مراجعه کنید که این باگ هارو پخش می کنند.چند تا سایت بزرگ رو براتون مثال می زنم :

www.SecurityFocus.com
www.SecurityFocus.net

خوب حالا وارد قسمت سوم می شویم که باید نحوه کارکردن با آن سرور رو بلد باشید وگرنه زمانی که داخل مدیریت سایت شوید هیچ کاری نمی توانید انجام دهید . البته این نکته رو بدونید که اون هایی هم که زبان انگلیسی بلد باشند هم در مقابل این موارد کم میارند چون از یک سری اصطلاحات خاص در این میان استفاده می شود که فقط نیاز به تمرین و آشنایی با موارد آن دارد.
برای این کار شما چند راه دارید :

۱- سوال از دوستان و بزرگان آشنا با پرتال ها
۲- خواندن مقالات مربوط به آن پرتال
۳- استفاده از یک سرور رایگان

از همه بهتر شماره ۳ هست که شما بر روی یک سرور رایگان که اون پرتال را در اختیار کاربران قرار می دهد می توانید به طور کامل با آشنا شوید .



بعضی وقت ها شما برای هک کردن یک سرور نیاز دارید تا با سرور اصلی که این سرور بر روی آن هاست شده است را بدست آورید و مقداری اطلاعات از روی آن سرور جمع آوری کنید.
من در اول مفهوم هاست و هاستینگ را برای شما توضیح می دهم :
هاست : مقداری فضای اینترنتی که شما از یک سرور خریداری می کنید
هاستینگ : به سایتی که این خدمات هاست می دهد یک هاستینگ می گویند
دومین : یا دامنه یک نام است که بعدا به عنوان سایت شناخته می شود مثلا

www.InvisibleTeam.net
Domain : invisibleteam.net

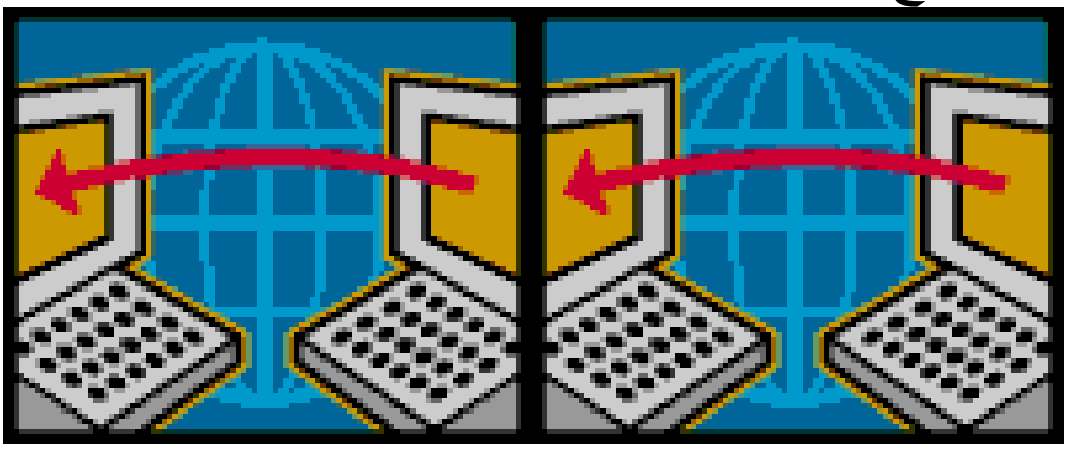
ساببدومین : یا همان وبلاگ که نام دلخواه شما به دنباله اسم سایت اصلی می آید . برای مثال :

www.Invisible.InvisibleTeam.net
SubDomain : Invisible
Domain : invisibleteam.net

خوب ما تا ۳ مرحله آخر پیش رفتیم و فقط مراحل جمع آوری اطلاعات از هدف کوچک مانده که این ۳ مرحله برای حملات مخصوص هک کردن یک وبلاگ است.
برای پیدا کردن نام کاربری صاحب وبلاگ در مباحث قبلی توضیح دادیم و نحوه بدست آوردن ایمیل وی را هم گفتیم اما اینجا تنها یک نکته باقی می ماند آن هم این که اگر هیچ جا ایمیلی نذاشته بود چه کنیم ؟!؟!
خوب شما می توانید باز هم از روش مهندسی اجتماعی استفاده کرده و با یک دروغ در بخش نظرات ایمیل وی را درخواست کنید.
تنها نکته غیر آشنا آخرین زمان بروز کردن بوده است که اگر هدف یک وبلاگ است زمان آخرین وبلاگ را برمی داریم و اگر هدف سرور است زمان آخرین ارسال بر روی وبلاگ مدیران را بدست می آوریم.

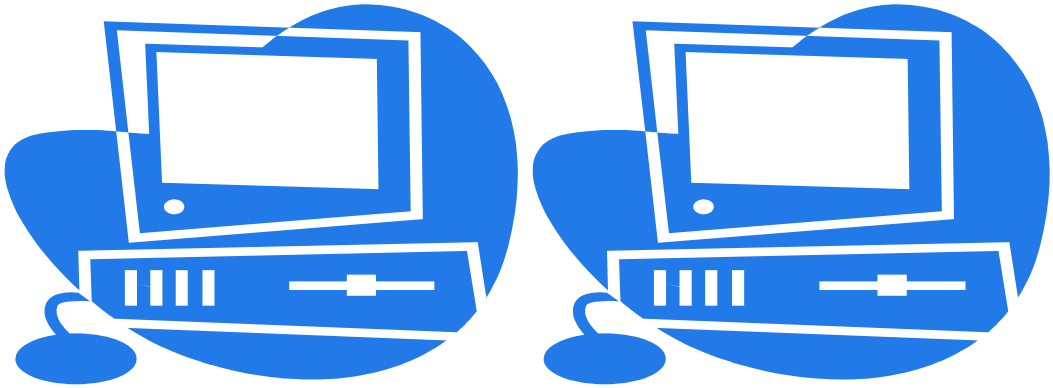

نفوذ به سرور :

خوب هم اکنون خودتون رو برای جذاب ترین و مهم ترین قسمت مقاله آماده کنید .
مبحث سرور هکینگ واقعا مبحث گسترده و بزرگی می باشد که نمی توان آن را براحتی توضیح داد و حتی تعداد افراد معدودی هم هستند که با تمام روش های آن و به طور کامل با عمل < نفوذ به سرور > آشنا باشند.
این نفوذ به سروری که ما در این قسمت به شما آموزش می دهیم یک نفوذ به سرور کاملا ساده و مبتدی (از نظرمقایسه با سایر روش ها) اما باز هم درک و فهم آن نیاز به آشنایی زیادی به سایر موارد دارد.
در این مدل نفوذ که بیشتر به معنای فال گوش ایستادن می باشد شما باید با استفاده از نرم افزارهای خاصی خود را برای آن آماده کنید و بعد به سرور وصل شده و شروع به گوش دادن کنید تا به نتیجه دلخواه برسید.



مواد لازم :

برای انجام عمل گوش ایستادن شما نیاز به نرم افزارهای مخصوص این کار دارید که از بهترین آن ها می توان به Sniffer ها اشاره کرد.
در ضمن شما به تعدادی برنامه Cracker نیز نیاز دارید.
من در ابتدا شما را با نحوه عمل کرد این نرم فزارها آشنا می کنم و سپس با نحوه گوش دادن به سرور آشنا می شوید.
یکی از بهترین نرم افزارهایی که شاید وجود آن برای شما باعث راحتی انجام کار شود وجود یک باگ اسکنر هست که می تواند شما را در راحتر وصل شدن به سرور کمک کند.
البته این نرم افزار برای مبتدیان می باشد افراد حرفه ای دیگر نقاط ضعف را بر اثر تجربه می دانند و نیازی به اسکن دوباره سرور ندارند.



Sniffer :

کار اصلی این نرم افزار ها چک کردن تمام ردوبدل های انجام شده بر روی سرور شامل پاکت ها و نامه ها و ..... که سرور برای کاربران می فرستد و یا کاربران برای سرور می فرستند می باشد.
این نوع برنامه ها تمام این رد و بدل ها را ثبت کرده و برای هکر می فرستند.
این رد و بدل ها عموما شامل پاکت ها می باشد که این پاکت ها درخواست های مدیران وبلاگ ها می باشد که برای ورود به وبلاگ خود به سرور فرستاده می شود و حاوی اطلاعات آن وبلاگ < نام کاربری – رمز عبور و ... > می باشد.
اما نکته مهم این پاکت ها این می باشد که به صورت رمز شده هستند و به حالت عادی قابل استفاده نمی باشند و یک هکر با پاکت های رمز شده نمی تواند هیچ کاری انجام دهد.
با این برنامه می توان بر روی تمام ورودی ها و خروجی ها نظارت داشت و آن ها را ثبت کرد.

: Cracker

کراکر (یا کرکر) ها برنامه هایی هستند که جهت اهداف مختلفی می باشند.
۱- بدست آوردن رمز عبور
۲- به کد تبدیل کردن یا بر عکس

ما در اینجا از کراکر هایی استفاده می کنیم که برای ما فایل های کد شده (پاکت های رمزی شده) را ترجمه کرده و کلمات اصلی را به ما می دهند.
این کار بنابر امنیت سرور و سایت در ضمینه Encode کردن پاکت ها از ۱ دقیقه تا ۱ ساعت طول می کشد . اما پسورد وبلاگها عموما در زیر ۱ دقیقه Decode می شوند.

Encode: زمانی که یک کلمه یا رمز عبور جهت ارسال به سرور رمزی می شود را گویند.
Decode: زمانی که یک کلمه رمزی شده به همان کلمه اصلی تبدیل شود را گویند.

عموما از این روش ها برای افزایش رد و بدل اطلاعات استفاده می شود که اکثر برنامه این تبدیل گر ها را دارند.

: Scanner

اسکنر ها همان طوری که از اسمشان بر می آید برنامه هایی هستند که یک سایت یا یک سرور یا ..... را اسکن (مورد بررسی) می کنند.
این اسکنر ها انواع مختلفی دارند که ما در اینجا از < BUG Scanner > , < Security Scanner > استفاده می کنیم.
با استفاده از این برنامه ها ما قادر خواهیم بود که نقاط ضعف و قوت هدف خود را بسنجیم و در صورت پیدا شدن نقطه ضعفی با استفاده از آن حفره امنیتی به هدف خود حمله کنیم و کار های اصلی خود را انجام دهیم.

بهترین و قویترین برنامه های نام برده شده که در این نفوذ برای ما مفید هستند در بخش دانلود سایت ((گروه امنیتی مردان نامریی)) وجود دارد.

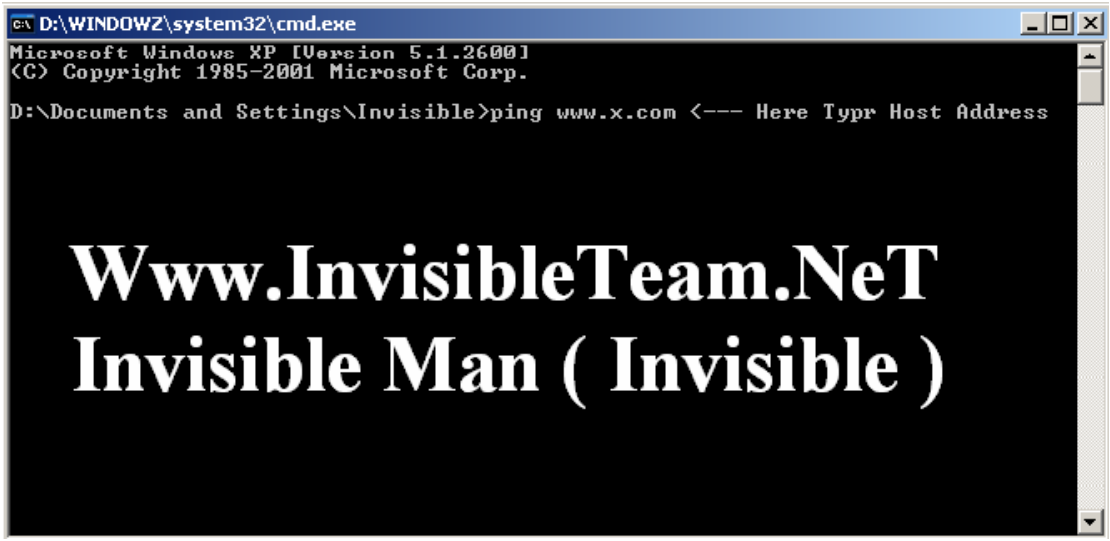
Link Address : Www.InvisibleTeam.Net
Go To Download Area ……..
Hack Tools ←

نفوذ مدل ۱ :

خوب برای انجام این کار شما ابتدا باید < IP > سرور مورد نظر خود را بیابید برای این کار می توانید از یکی از دستورهای داس استفاده کنید :
ابتدا با استفاده از یکی از روش ها داخل برنامه شوید :

1- Start → Run → Cmd / Command
2- Start → Program Files → Accessorios → Command Prompt

پنجره ای برای شما باز می شود با استفاده از دستور <Ping Hostaddress> شما می توانید به اطلاعات مورد نظر خود برسید :



خوب بعد از بدست آوردن IP هدف خود آن را در برنامه Sniffer خود وارد کنید :

البته این یکی از مبتدی ترین Sniffer ها می باشد ولی هدف آشنایی شما با حالت کلی برنامه می باشد که در چه محلی اطلاعات را وارد کنید و در کجا دریافت کنید و چگونه شروع به کار کنید.

خوب بعد از جمع آوری پاکت های مخصوص شما باید آن ها را باز کنید و داخل با استفاده از برنامه کراکر خود آن ها را از حالت کد شده خارج کنید و به حالت قابل استفاده در بیارید.
خوب بعد از بدست آوردن پسورد و یوزر شما دیگر هیچ اطلاعات دیگری را نمی خواهید و همانند قبل وارد مدیریت وبلاگ شده و قالب مخصوص هک خود را قرار داده و کار تمام شد.خسته نباشید.

نکته خیلی خیلی مهم :
اگر IP که شما در برنامه Sniffer خود وارد می کنید برای سرور وبلاگ دهی باشد پاکت هایی که دریافت می کنید برای وبلاگ هایی هست که در همان لحظه وارد مدیریت وبلاگ خود شده اند.

با استفاده از این روش بر روی یک سرور و انتخاب زمان مناسب می توان با شانس خوب یکجا حدود ۵۰ وبلاگ را هک کرد.برای یک بار و بار اول رکورد خیلی خوبی می باشد.

نفوذ مدل ۲ :

در این روش شما با استفاده از یکی از برنامه های اسکنر که برای پیدا کردن ضعف ها (حفره های) امنیتی روی سایت ها و سرورها طراحی شده اند شروع به اسکن کردن یک هاست می کنید.

نکته : در انتخاب اسکنر خیلی دقت کنید زیرا یک اسکنر قوی موجب افزایش درصد شما می شود اما یک اسکنر ضعیف امکان دارد درصد شما را به حد ۰ برساند.

جا داره از دوست خیلی خوبم < HULK > که یه اسکنر واقعا قوی را در اختیار من گذاشت تشکر به عمل بیاورم.

اسکنرها نیز همانند سایر برنامه های لازم در بخش دانلود سایت ((گروه امنیتی مردان نامریی)) قرار گرفته است .

Link Address : Www.InvisibleTeam.NeT
Go To Download Area → Hack Tools

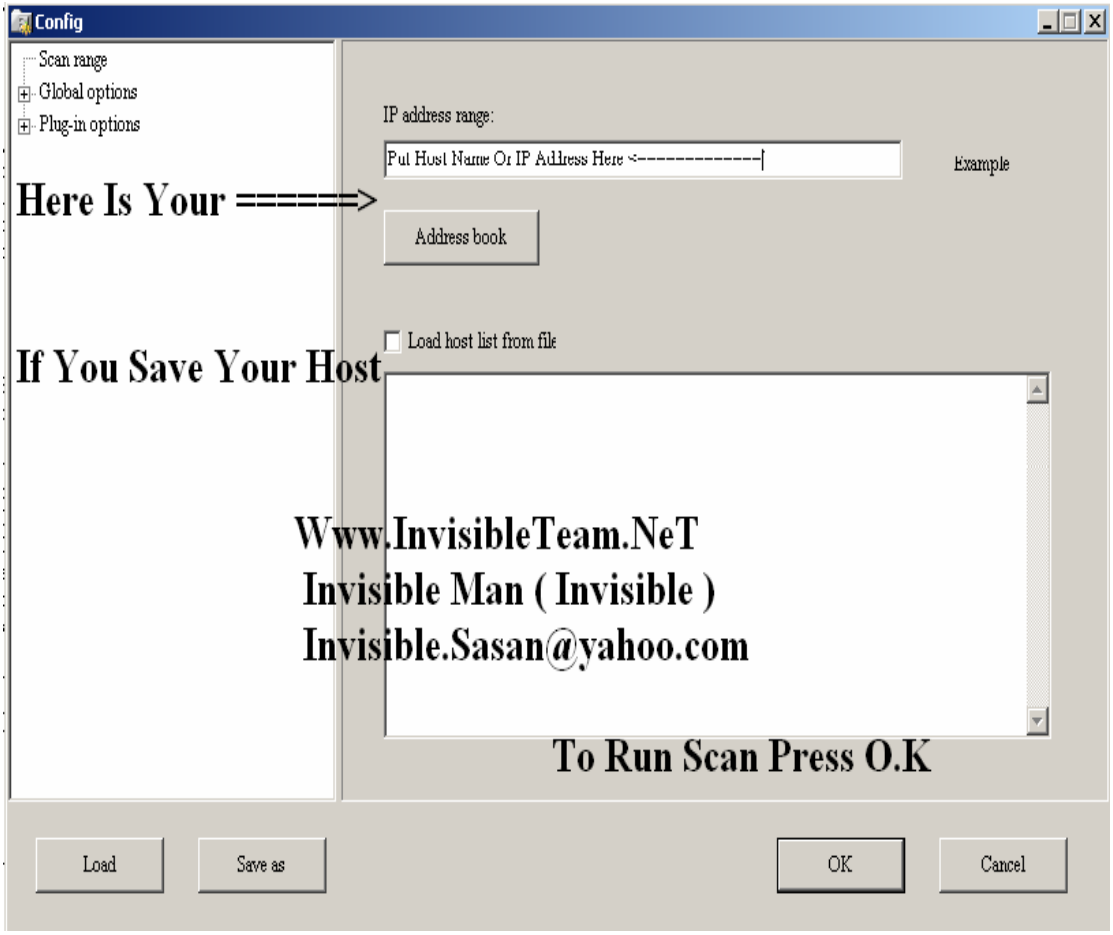
اسکنرها و طرز کار :

برنامه های اسکنر نیز مانند Sniffer ها براساس IP هاست مورد نظر کار می کنند.اسکنری که من استفاده می کنم با لینک خود سایت هم اسکن می کنه اما همه جا اگرIP بدید همواره بهتر کار می کنه.
اسکنرها با اتصال به سایت تمامی صحفات آن را لیست می کنند و سپس بر اساس تشخیص پرتال آن سایت شروع به اسکن آن سایت می کنند و نتایجی را بدست می آورند.
این نتایج بر اساس تنظیم بندی خود برنامه چند قسمت مختلف می شوند که تمام سعی و تلاش ما بر روی قسمت < Vulnerability > می باشد.
بعد از اینکه اسکنر شما کار خود را تمام کند در صورتی که باگی در آن سایت وجود داشته باشد آن را در این قسمت مشاهده می کنید که باید با استفاده از راهنمایی های خود برنامه در جهت پیدا کردن کد مربوط به آن باگ تلاش کنید یا می توانید از سایت هایی که قبلا گفته بودیم استفاده کنید.
البته به یاد داشته باشید که همیشه جدیدترین باگ ها حالت خصوصی دارند و همواره باگ های خصوصی هم هست که می توان از آن استفاده کرد.

: Error

در اکثر اسکنر های جدید قسمت با نام < Error >
وجود دارد که در آن بعد از اسکن نکاتی نوشته می
شود.
این موارد هم جزو ضعف های سایت اسکن شده می
باشد اما نحوه استفاده از آن ها کمی فرق می کند زیرا
اینجا صحفاتی می باشد که بر اثر یک < Error >
موجب به هنگ و هک شدن سایت یا آن صحفه می
شود.
عموما افرادی که با زبان های برنامه نویسی
<HTML> , < Java Script >
به خوبی آشنا نباشند نمی تواند از این موارد استفاده
کنند و سایت مورد نظر خود را هک کنند.
اکثر این مدل صحفات بر اساس ضعف در برنامه
نویسی پرتال استفاده شده در سایت به وجود می آید که
در این موارد با دست کاری مقدار داده که با لینک می
دهید می توانید حد اکثر را پیدا کرده و بعد از عبور از
آن شروع به تزریق کدهای مخرب کنید.
این مدل حملات با نام < SQL – Injcetion >
معرفی شده اند که بیشترین کاربرد را در اکسپلیت ها
دارند . (چون خیلی راحت استفاده می شوند)

نمایی از صحفه اول یک باگ اسکنر و لیست های موجود در آن :



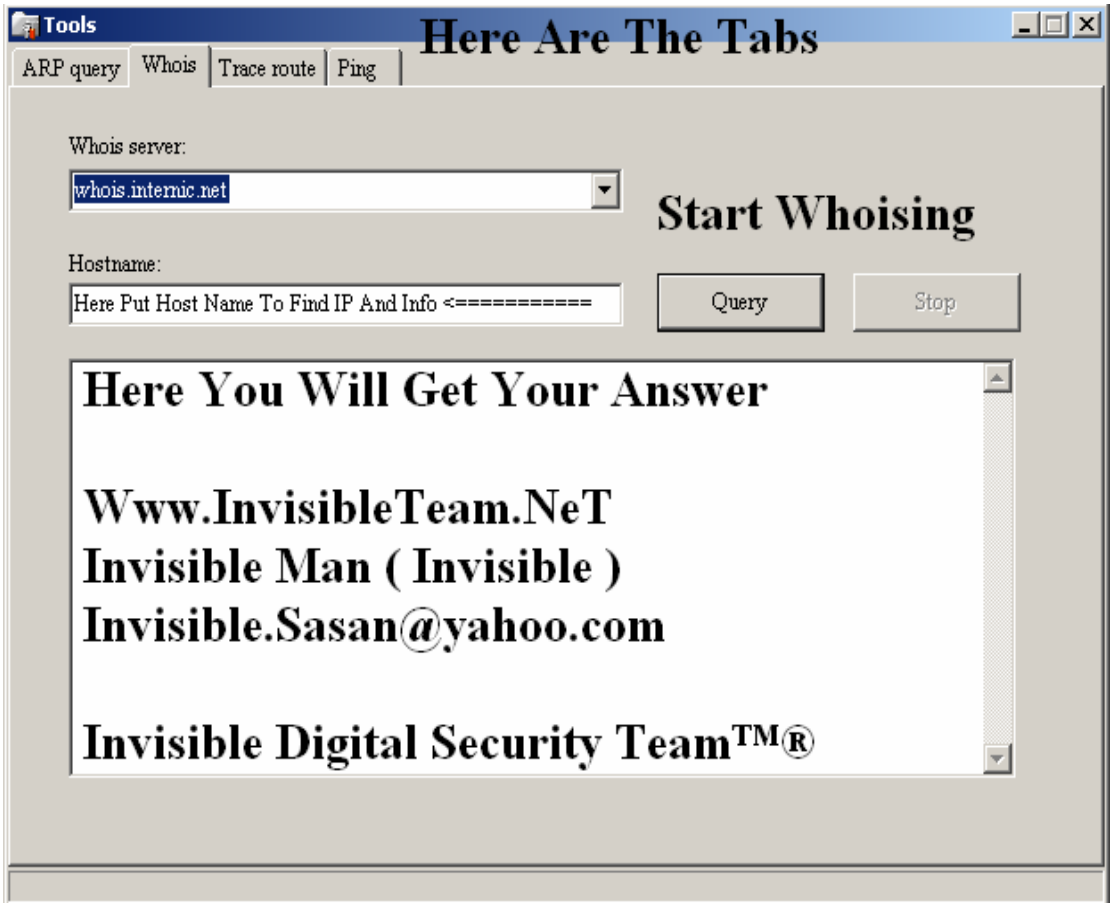
البته برای بدست آوردن IP یک سایت روش موثر دیگری هم وجود دارد که با نام روش Whois معروف است.

در این روش اگر شما سایت بزرگی را می خواهید مورد تست قرار دهید اینکه دومین باشد یا کل لینک فرق دارد . برای این کار از لینک زیر استفاده کنید:

http://www.samspade.org/t/ipwhois?a=Here Put Site Name

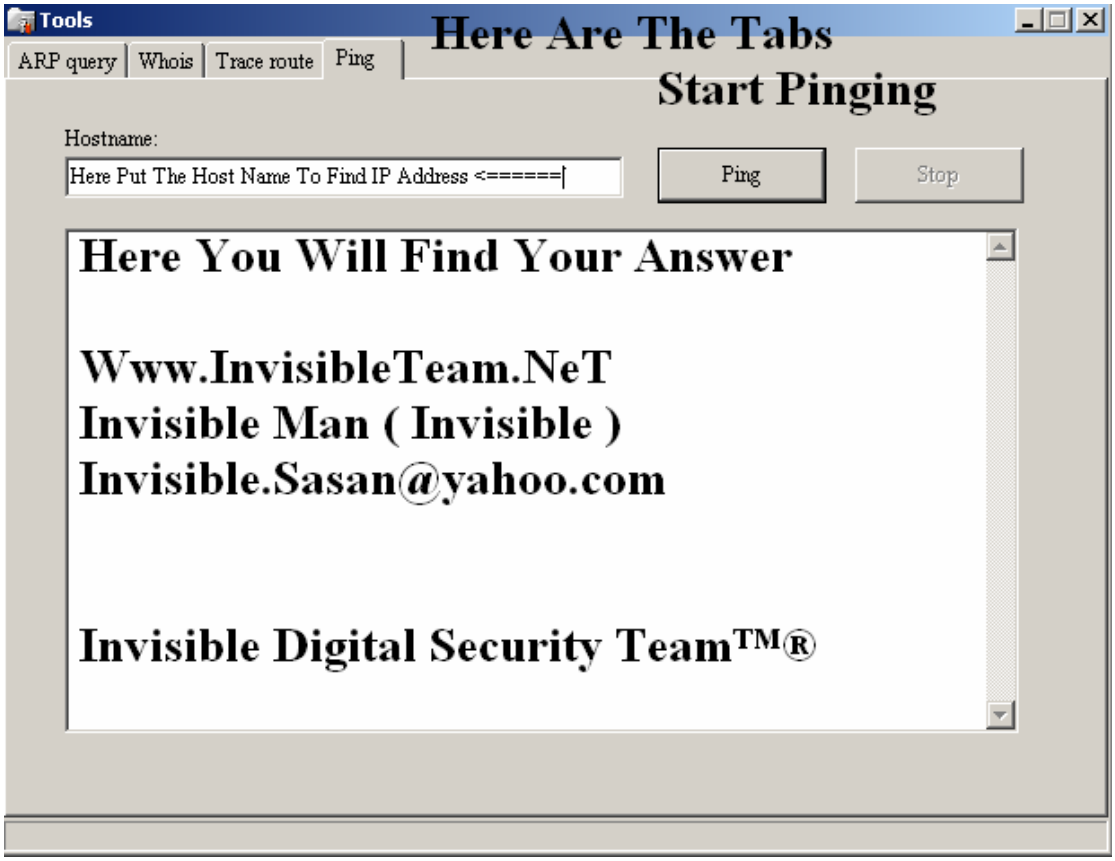
سایت هایی زیادی هستند که Whois برای شما می گیرند اما اینکه می گم در انتخاب اسکنر دقت کافی را داشته باشید برا این مواقع است :

((اسکنر مورد استفاده من همچنین برای بدست آوردن IP دارای گزینه Whois می باشد توسط خود برنامه می باشد.))



با استفاده از این دستوراطلاعات بیشتری از قبیل آدرس سرور و نام مدیر و تلفن او و سایر اطلاعات داده شده را بدست خواهید آورد.

قبلا روشی را نیز در مورد بدست آوردن آدرس IP یک سایت یا سرور در داخل داس به شما یاد دادیم اما لازم هست که یک نکته را در اینجا به شما بگم که این روش دارای چند حالت است اگر در آخر بگه ۱۰۰ % از دست رفت یعنی ول معطلی اما اگر ۰% یعنی به یه جایی رسیدی اما اسکنری که من دارم این کار رو هم برام انجام می ده (خیلی تو انتخاب دقت کنید !!)



خوب پس حتما تا حالا به این نتیجه رسیدید که یک انتخاب خوب در اول یک عمر راحتی در آسایش ...

خوب این مقاله در اینجا به پایان اما باز هم چند نکته هست که در کل متن به طور پراکنده گفتم حالا هم دوباره تکرار می کنم :

۱- هرگز از شکست دل سرد نشو
۲- هرگز با صلح راضی نشو
۳- هرگز از کارت خسته نشو
۴- هرگز برای کسی شاخ نشو
۵- هرگز زیادی هک نکن (هرچیزی به اندازه)
۶- سعی کن بیشتر یه پیش کسوت باشی
۷- همیشه به زیر دستات توجه کن
۸- کسی که به تو یک کلمه یاد دهد تورا بنده خود کرده است هرگز به او بدی نکن
۹- با هیچ کسی دشمنی نکن تا دشمنی ندیدی
۱۰- با هم دوست باش کارت راه می یفته
۱۱- تمرین – تمرین – تمرین یادت نره
۱۲- کار نشد نداره
۱۳- سوال داری بپرس ننگت نیاد

امیدوارم با رعایت موارد بالا یه هکر خوب بشید....
با امیدرضایت شما از این مقاله .....
← گروه امنیتی مردان نامریی →

جا داره یک بار دیگر از تمام دوستان که مارا در تهیه این مقاله یا جمع آوری مطلب یاری کردند تشکر و قدر دانی به عمل بیاوریم :

Persons :

Alikhoub – Hacker_Boy – Subzero
Mehrun – Agape – Betrayed – Mr Sisil
SiaHacker – Netquard – Error_Sir
System_Share – l2odon – MaX666
Y4ho0 Emper0r – Im4n Emper0r
Majid NT – C0d3r – Th3 L0rd – Magic
Satanic Soulfol – S Haroo Z – Eblis
Little Hacker – Dangerous Hacker
Port – Alir9 – Soba Nucker - Hulk

Teams :

IHZ Team – IHS Team – IHC Team
IBBH Team – Shabgard Security Group
Satanic Digital Security Team
Y!Underground Team – Emperor Team
Black Devils Boys Security Team
White Hat Hackers – Virangar Team
Invisible Digital Security Team

منابع و مآخذ :

گروه امنیتی مردان نامریی
گروه امنیتی شبگرد
گروه امنیتی دلتا هکینگ
گروه امنیتی کروز
گروه امنیتی جهنم شیطانی
گروه امنیتی فورس (چین)
گروه امنیتی هکران شرقی (آسیایی و اروپایی)
گروه امنیتی آشیانه
گروه امنیتی سیمرغ
گروه امنیتی هکران سایبریا ایرانی
گروه امنیتی شیران طلایی
گروه امنیتی هکران کوچ نشین
گروه امنیتی پسران شیطان
گروه امنیتی هکران کلاه سفید جهان (آمریکا شمالی)
گروه امنیتی هکران زیر زمینی (آمریکا شمالی)
گروه امنیتی هکران کلاه سیاه بین المللی (جهانی)
گروه امنیتی نیروهای مخرب
گروه امنیتی گروه هکران بی کلاه
گروه مشورت
و سایت و وبلاگهای چند تن از دوستان .....

Invisible Man
Invisible Digital Security Team
Www.InvisibleTeam.NeT

We Are :
Invisible – Alikhoub – Hacker_Boy – Subzero
Mehrun – Agape

Yahoo ID : Invisible.Sasan
E-mail : Sasan.Seyfi@gmail.com
Upload Center : Www.Invisible.Persiangig.coM

!~! My Dreams Always Is A Girl Standing In The Sun !~!