

درباره IP

IP شماره ایست که به هر کامپیوتر متصل به اینترنت داده میشود تا بتوان به کمک آن شماره به آن کامپیوترها دسترسی داشت. این عدد برای کامپیوترهایی که حالت سرور دارند و نیز کامپیوترهای کلاینتی که معمولا به روشی غیر از شمارهگیری (Dial Up) به اینترنت وصل هستند، عددی ثابت و برای دیگران عددی متغیر است. و در هر بار وصل شدن به اینترنت این شماره عوض میشود یعنی هر بار که شما با شرکت ISP خود تماس گرفته و به اینترنت وصل میشوید، عددی جدید به شما نسبت داده میشود .

این عدد یک عدد ۳۲ بیتی است و برای راحتی به صورت زیر نوشته میشود :

xxx.xxx.xxx.xxx که منظور از **xxx** عددی بین **۰** تا **۲۵۵** است (البته بعضی شمارهها قابل استفاده نیست). مثلا ممکن است آدرس شما به صورت ۱۹۵,۲۱۹,۱۷۶,۶۹ باشد. حتی اسمهایی مثل <http://www.yahoo.com> که برای اتصال استفاده میکنید، در نهایت باید به یک IP تبدیل شود، تا شما سایت یاهو را ببینید .

در IP معمولا **xxx** اولی معنای خاصی دارد، که بعدا توضیح میدهم... فقط این را بگویم که اگر به روش Dial Up به اینترنت وصل شوید، معمولا عددی که به عنوان xxx اول میگیرید، مابین ۱۹۲ تا ۲۳۲ خواهد بود. این توضیح برای تشخیص کامپیوترهای کلاینت از سرور (حداقل در ایران) بسیار میتواند مفید باشد .

بعد از اتصال به اینترنت برای به دست آوردن IP خود، از دستور IPCONFIG یا در command prompt استفاده کنید .

پورت: (Port)

محلی است که دادهها وارد یا خارج میشوند. در بحث هک معمولا با پورتهای نرمافزاری سروکار داریم که به هر کدام عددی نسبت میدهیم. این اعداد بین ۱ و ۶۵۵۳۵ هستند. معمولا به یک سری از پورتهای کار خاصی را نسبت میدهند و بقیه به صورت پیشفرض برای استفاده شما هستند. پورتهای که فعال هستند، هرکدام توسط یک نرمافزار خاص مدیریت میشوند. مثلا پورت ۲۵ برای ارسال Email است، بنابراین باید توسط یک نرمافزار این کار انجام شود و این نرمافزار بر روی پورت ۲۵ منتظر (فالگوش) میماند. اینجا ممکن است شخصی از فلان نرمافزار و دیگری از بهمان نرمافزار استفاده کند ولی به هر حال پورت ۲۵ همیشه برای ارسال Email است .

و پورتی که یاهو مسنجر از آن استفاده میکند ۵۰۵۰ هست. از پورت های مهم : ۷۹, ۱۱۹, ۲۳, ۱۵, ۷, ۲۱, ۱۳۹, ۱۱۰ و... که بعد در موردشان بیشتر توضیح میدم .

اولین نکتهای که لازم است بگویم اینه که وقت خود را برای هک کردن کامپیوترهای کلاینت هدر ندهید (اگرچه برای افراد مبتدی کار با نرمافزاری مثل V Sub زیاد هم بد نیست ولی نباید زیاده روی کرد) علت هم اینه که هر بار که به اینترنت وصل میشوید ip جدیدی به آنها اختصاص پیدا میکنه و زحماتون هدر میره.

یافتن آدرس IP

با وجود اینکه به احتمال قوی این مقاله نه تنها کاملترین نوشته در مورد روشهای یافتن IP به زبان فارسی، بلکه به طور کلی کاملترین نوشته در این زمینه بر روی اینترنت می باشد، فراموش نکنید که روشهای یافتن IP به این موارد محدود نمی شوند و به همین دلیل در زیر ابتدا مقدمه ای در مورد کلیت روشهای یافتن IP و مجاز یا غیرمجاز بودن آنها آورده ایم و سپس به چند روش مهم اشاره کرده ایم .

هر بار که یک کامپیوتر به کامپیوتر دیگری متصل می شود، حداقل اطلاعاتی که باید به آن بدهد آدرس IP خود است؛ بنابراین یافتن IP کسی که به دلیلی قصد اتصال به رایانه شما را داشته است نه تنها غیر قانونی نیست بلکه یک موضوع کاملاً طبیعی است . تمامی روشهای یافتن IP به نوعی به این اصل کلی برمی گردند. شاید به نظرتان بیاید که هنگامی که با کسی روی مسنجر صحبت می کنید باید کامپیوترهای شما به هم متصل باشند و بنابر این به سادگی بتوان IP فرد مقابل را به دست آورد، اما مسنجرهای معتبر مانند Yahoo یا MSN در حقیقت میزبان خود را بین شما و فرد مقابل قرار می دهند به این صورت که شما و دوستان هر دو به سرور مسنجر متصل می شوید و همه پیامها از آن عبور می کنند. پس پیامی که شما می نویسید وارد سرور مسنجر می شود و سپس از طریق سرور مسنجر به فرد مقابلتان می رسد و بالعکس. اما نگذارید این موضوع شما را ناامید کند! هنگامی که شما و دوستان در یک بازی مسنجر شرکت کنید یا فایلی را به طور مستقیم برای او بفرستید دو کامپیوتر به طور مستقیم به هم متصل هستند! این روش یکی از مناسبترین روشهاست. در زیر چند روش مناسب یافتن IP را برای شما توضیح می دهیم، اما قبل از آن، نکته مهمی را یادآوری می کنیم: اگر کسی از اینترنت قطع شود، IP او عوض می شود! پس اگر شما امروز IP کسی را به دست آورید که با خط تلفن و مودم به اینترنت وصل می شود، ممکن است ۳۰ ثانیه بعد او Disconnect کند و دوباره Connect شود که در این شرایط قاعدتاً IP دیگری خواهد داشت که این موضوع اطلاع قبلی شما را بی فایده می کند! اما اگر کسی به هر دلیل قصد حمله و آزار شما را داشت، بلافاصله IP او را به دست آورید که از طریق آن بتوانید به طور قانونی از وی شکایت کنید. تمامی مدارک را نگه دارید. من حاضرم به محض دریافت IP آنها و مدارکی که دلالت به مهاجم بودن آنها کند، اطلاعات کامل مربوط به صاحب IP شامل شماره تلفن و آدرس ایمیل او را برای شما ارسال کنم تا از این طریق و با دادن زمان دقیقی که فردی با آن IP قصد آزار شما را داشته است به صاحب IP، وی را به دام بیندازید. از طرف دیگر اگر کسی از Proxy استفاده کند، به دست آوردن IP او بسیار دشوار می شود (اگر فرد Java Script را از کار نینداخته باشد با استفاده از آن می توانید IP را به دست آورید !)

خواندن IP از طریق ایمیل :

هنگامی که شما یک ایمیل از فردی می گیرید، معمولاً آدرس IP وی در آن نامه وجود دارد. ابتدا باید با رفتن به قسمت تنظیمات ایمیل خود آن را در حالتی قرار دهید که تمامی Header نامه را به شما نشان دهد که با کمی گردش در قسمت تنظیمات ایمیل خود آن را پیدا خواهید کرد. حال به بالای ایمیل دقت کنید و به دنبال عبارت **Received: from** باشید. شما معمولاً دو یا چند بار عبارت **"Received: from"** را در بالای ایمیل خواهید دید که ما فقط با پایینی کار داریم که معمولاً کمی با بالاییها فاصله دارد و بعد از **Message ID** قرار می گیرد. آدرس IP فرستنده ایمیل درست در ابتدای این عبارت قرار می گیرد. دادن روش دقیق غیر ممکن است، اما معمولاً همانطور که گفتیم در پایینترین Received باید به دنبال IP باشید. با این حال در شرایطی که فقط در بالاترین Received عددی شبیه IP مشاهده کنید، IP همان است. از سوی دیگر بسیاری از میزبانان ایمیل، راه آسانتری هم برای کمک به شما در نظر می گیرند به این صورت که قسمتی با نامی شبیه به **X-Originating-IP** برای شما قرار می دهند و IP فرستنده نامه را در آن می نویسند. به مثالهای زیر توجه کنید که IP فرستنده به رنگ قرمز مشخص شده است :

```
Received: from [farsiedu@farsiedu.com] by server۶۲,۱۴۵,۶۱,۱ [۴ pfs
۰۷۰۰ -۰۰:۳۸:۴۳ ۲۰۰۳ Jun ۳۰E; Mon, ۹۰۳۱۳۰۱۸] id A۳۲-V,۱۲(SMTPD
@farsiedu@farsiedu.com> ۰۱۲۱۲.SM۲۰۰۳۰۶۳۰۰۱۰۴۵۰۰Message-Id: <
```

farsiedu@farsiedu.com From:
۰۷۰۰ -۰۱:۰۶:۳۸ ۲۰۰۳ Jun ۲ Date: Mon,
farsiedu@farsiedu.com X-RCPT-TO:
Status: U
۳۴۷۷۳۱۲۳۷X-UIDL:
pfs ۴] by server۲۰۵,۱۵۸,۶۲,۱۵۸.us.outblaze.com [۱Received: from spf
۰۷۰۰ -۰۹:۰۲:۳۸ ۲۰۰۳ Jun ۰۷EA; Sat, ۵۴۰۰E۹) id AC۲۲-V, ۱۲(SMTPD
۰۰۰۰ -۱۶:۰۳:۳۹ ۲۰۰۳ Jun ۷ invoked from network); ۳۱۰۶۸Received: (gmail
) ۲۰۵,۱۵۸,۶۲,۶۸Received: from unknown (
۰۰۰۰ -۱۶:۰۳:۳۹ ۲۰۰۳ Jun ۷.us.outblaze.com with QMQP; ۱by spf
۰۰۰۰ -۱۶:۰۳:۳۷ ۲۰۰۳ Jun ۷ invoked from network); ۶۱۶۱۱Received: (gmail
) ۲۰۵,۱۵۸,۶۲,۵۷.us.outblaze.com (۴.us۱-VReceived: from unknown (HELO ws
۰۰۰۰ -۱۶:۰۳:۳۷ ۲۰۰۳ Jun ۷.us.outblaze.com with SMTP; ۲۰۵-۱۵۸-۶۲-۱۵۳by
۰۰۰۰ -۱۶:۰۳:۳۵ ۲۰۰۳ Jun ۷); ۱۰۰۱ invoked by uid ۵۴۸۹۱Received: (gmail
.gmail@mail.com> ۲۰۰۳۰۶۰۷۱۶۰۳۳۵,۵۴۸۸۹Message-ID: <
" ۱۰۵۵۰۰۱۸۰۹-۵۴۳۷۰۰۰Content-Type: multipart/mixed; boundary="-----=
bit VContent-Transfer-Encoding:
۱,۰MIME-Version:
) ۵,۴۰۴ (Entity ۵,۴۱X-Mailer: MIME-tools
.outblaze.com with http for ۴.us۱-V] by ws۲۱۷,۲۱۸,۵۷,۵۵Received: from [
۰۵۰۰ -۱۱:۰۳:۲۹ ۲۰۰۳ Jun ۰۷; Sat, farsiedu@farsiedu.com
From: "Reza"
farsiedu@farsiedu.com To:
۰۵۰۰ -۱۱:۰۳:۲۹ ۲۰۰۳ Jun ۰۷Date: Sat,
Subject: The Interactive Matrix
۲۱۷,۲۱۸,۵۷,۵۵X-Originating-Ip:
.outblaze.com ۴.us۱-VX-Originating-Server: ws
X-RCPT-TO:
Status: U
۳۴۴۳۹۳۳۵۰X-UIDL:

اما یک استثنا: اگر فرد برای فرستادن ایمیل از فرمهای موجود در برخی سایتها مانند سایتهایی که اجازه ارسال یک خبر یا کارت را می دهند یا سایتهایی که ادعای ارسال ایمیل فارسی را دارند (هرچند واقعاً فارسی تایپ کردن در یاهو از اکثر آنها بهتر است) یا فرمهای "تماس با ما" در سایتها استفاده کنند، بعید است IP آنها در ایمیل شما باشد و معمولاً IP سرور خود سایت را در آن می بینید. در مثال زیر که ایمیلی است که با استفاده از فرم "تماس با ما" سایت همسفر برای مدیر آن ارسال شده بوده است، فقط IP خود همسفر را مشاهده می کنید :

] by farsiedu.com with ESMTP ۳۸,۱۱۸,۱۴۳,۹۸pfs [۴Received: from server
۰۷۰۰ -۰۶:۱۶:۵۳ ۲۰۰۳ Jun ۰۷VDC; Sat, ۵۴۴۰۰C۵) id A۳۲-V, ۱۲(SMTPD
From:
To:
Subject: farsiedu
۰۷۰۰ -۰۶:۱۶:۵۳ ۲۰۰۳ Jun ۷Date: Sat,
pfs> ۴@server۷۶۲۶۷۴۰\$۶۲۸b۷\$۱۰۴۶cf۳۲c۰۰۰۳۰۱Message-ID: <
۱,۰MIME-Version:
Content-Type: text/plain;
" ۸۸۵۹-۱charset="iso-

bit VContent-Transfer-Encoding:
۲۰۰۰X-Mailer: Microsoft CDO for Windows
vhkQ== ۶WTby۱B/RZms۵z۵xBGKda۹Thread-Index: AcMs
Content-Class: urn:content-classes:message
۶,۰۰,۲۸۰۰,۱۱۶۵X-MimeOLE: Produced By Microsoft MimeOLE V
X-RCPT-TO:
Status: U
۳۴۷۷۳۰۷۵۳X-UIDL:

به دست آوردن IP از طریق سایت خودتان :

اگر سایت یا وبلاگی دارید، راههای بسیاری برای به دست آوردن IP بازدیدکنندگان دارید و با دادن آدرس سایت یا وبلاگتان به یکی از دوستان می توانید IP او را به دست آورید. از آنجایی که در یک لحظه ممکن است چندین بازدید کننده داشته باشید، بهتر است صفحه زیبایی مخصوص این کار بسازید که هیچ لینکی به آن نباشد و آن را برای به دست آوردن IP مورد استفاده قرار دهید .

برای این کار دو روش اصلی داریم :

۱ - برنامه نویسی: با کمی جستجو در اینترنت کدهای بسیار کوتاهی را می یابید که IP را به دست می دهند و به سادگی می توانید آن را به همراه تاریخ و ساعت در یک فایل متنی یا پایگاه داده ذخیره کنید .

۲ - استفاده از سایتها دیگر: اکثر شمارنده ها این امکان را به شما می دهند که IP بازدید کنندگان صفحات خود (حداقل چند بازدید کننده اخیر) را ببینید. پس با نصب یک شمارنده روی آن صفحه ای که گفتیم، IP به دست آمده است .

به دست آوردن IP از طریق مسنجرها :

همانطور که در مقدمه گفتیم، فقط هنگامی که شما در حال ارسال یا دریافت فایلی به طور مستقیم (با در برخی بازیهای مسنجر) (باشید می توانید از این روش استفاده کنید. این روش که به روش Netstat معروف است، از همه روشها معروفتر است ولی به نظر من به خوبی روشهای بالا نیست. با کمی Social Engineering می توان هر کسی را راضی به دریافت یک فایل یا عکس کرد. بهتر است حجم فایل کم نباشد که فرصت کافی داشته باشید. البته اگر از AOL مسنجر استفاده می کنید، در منوهای آن گزینه ای برای برقراری Direct connection خواهید دید که مناسبتر است. هنگامی که فردی در حال دریافت یا فرستادن فایل به شما به طور مستقیم (نه روش فرستادن فایل با استفاده از Upload در یاهو مسنجر) باشد، با استفاده از Netstat می توانید IP او را ببینید. با توجه به شلوغ بودن خروجی Netstat یکبار قبل از آغاز به گرفتن/فرستادن فایل و بار دیگر بعد از آن این خروجی را بگیرید تا IP فرد را که به تازگی به لیست اضافه شده تشخیص دهید. برای ساده شدن کار بهتر است تمامی برنامه هایی که به هر طریق از اینترنت استفاده می کنند را ببندید که از شلوغی لیست کم شود. اگرچه در بیشتر راهنماها گفته می شود از پسوند n- استفاده کنید، به طور معمول در ایران استفاده نکردن از آن بهتر است. تنها تاثیر n- این است که تمام آدرسها را به طور عددی نشان می دهد و این کار یافتن آدرس IP ایرانیها را که به طور معمول به هر حال به شکل عددی است، در میان عددهای دیگر دشوارتر می کند .

برای اجرای netstat کافی است cmd.exe را از run اجرا کنید و به سادگی در آن تایپ کنید gnetstat و enter را فشار دهید. لیستی از تمامی اتصالهای موجود بین کامپیوتر شما و کامپیوترهای دیگر را مشاهده خواهید کرد. حال پس از برقراری ارتباط، دوباره این کار را تکرار کنید، آدرس جدید آدرس IP فرد مورد نظر است. اگر در لیست آدرسهای عددی ندیدید، از netstat -n استفاده کنید. با کمی تمرین این روش برایتان آسان می شود. یک روش کمکی استفاده از روش رو به رو است netstat > temp '۱: '۱.txt که این کار خروجی netstat را به درون فایل temp ۱.txt می ریزد. (که اگر وجود نداشته باشد ساخته می شود و اگر از قبل موجود باشد اطلاعات قبلی آن پاک می شود!) و سپس پس از برقراری اتصال، netstat > temp '۲: '۲.txt را وارد می کنید و سر

فرصت تفاوت فایلها را بررسی می کنید .

• به دست آوردن IP از طریق دادن IP خودتان :

مسخره ترین روش به دست آوردن IP آدرس این است که اول IP خودتان را به آنها بدهید تا شاید روی آن کلیک کنند و IP آنها به دست شما بیفتد! متاسفانه برنامه هایی که برای به دست آوردن IP از اینترنت می گیرید یا روی CD های بی ارزشی که به قیمت زیادی از بازار می خرید پیدا می کنید، از این روش استفاده می کنند IP شما را به طور واضح یا کمی کد شده به فرد می دهند یا از شما می خواهند که خودتان آن لینک را که چیزی جز IP شما نیست به او بدهید تا اگر روی آن کلیک کرد IP او را به شما بدهد! شکی نیست که این روش غیر منطقی ترین روش است و بهتر است از خیر چنین برنامه هایی بگذرید! کار پیچیده ای هم نمی کنند، Port خاصی را زیر نظر می گیرند (کاری که با Netstat خودتان هم می توانستید انجام دهید) و لینکی می سازند که با کلیک روی آن فرد به آن port شما متصل شود. جدای از خطرات این روش و مشکلات آن با Firewallها، این کار به طور کلی صحیح نیست اما روشی بسیار مشابه آن وجود دارد که کمی بهتر است. اگر از web server یا ftp server موجود در IIS (ویندوز) یا هر میزبان دیگری استفاده کنید و به این شکل سایتی به راه بیندازید، باز هم با دادن IP خودتان این شانس را دارید که IP آنها را هم به دست آورید .

<http://www.denaboy.persianblog.ir>

وبلاگ کرانه گمنام

<http://www.et4ir.blogfa.com>

وبلاگ آموزش های کاربردی

<http://denaboy.parsaspace.com>

وبسایت فرزند دنا

=====

مدیر سایت و وبلاگ ها : فرید نیک اقبالی