آموزش Hack

جلسه چهارم

Whois چیست؟

تعریف کلی برای Whois نمی‌توان ارائه‌داد؛ ولی فعلاً منظور ما از Whois همان کسب اطلاعات درمورد یک سایت است (قبلاً با نوع خاصی از Whois برای تبدیل Domain به IP آشنا شدید).

کاری که امروز می‌خواهیم انجام‌دهیم، کسب اطلاعات درمورد یک شماره IP ویا یک Domain خاص (مثلاً IRIB.com) است. برای کسب این اطلاعات، باید به اینترنت وصل‌شده و به‌طریقی، به یک‌سری سایت‌های خاص که وظیفه ثبت Domain و... را دارند، متصل‌شده و اطلاعات را از آنها درخواست‌کنیم. این سایت‌های خاص، Database (بانک اطلاعاتی) ویژه این وظایف را دارند. برای کسب این اطلاعات از سایت‌ها، روش‌های زیر را می‌توان به‌کار برد :

۱- اگر ازطریق سیستم‌عامل UNIX یا Linux به اینترنت وصل شده‌اید، دستوری به‌اسم whois در آنها وجوددارد. ویا می‌توانید از نرم‌افزارهای خاصی که برای این سیستم‌های عامل وجوددارد (مثل Xwhois) استفاده‌کنید؛ ولی فعلاً بحث روی ویندوز است که این‌دستور را ندارد !!!

۲- برای Whoisکردن در ویندوز، نرم‌افزارهای زیادی وجوددارد. به‌عنوان مشهورترین این نرم‌افزارها می‌توان به NetScan Tools و SamSpade اشاره‌نمود؛ ولی فعلاً از این موارد هم صرف‌نظر می‌کنم تا شما بیشتر با جزئیات این‌کار آشنا شوید.

۳- روشی که ما در این جلسه به‌کار می‌بریم، استفاده‌از سایت‌هایی است که این جستجو را برای ما انجام می‌دهند.

Databaseهای Whois در چه سایت‌هایی وجود دارد؟

تعداد زیادی از سایت‌ها این داده‌ها را دارند که مشهورترین‌ها عبارتند از :

```
whois.internic.net (The InterNIC)
whois.onlinenic.com (The OnLineNIC)
whois.arin.net (American Registry for Internet Numbers)
whois.ripe.net (European IP Address Allocations)
whois.apnic.net (European IP Address Allocations)
whois.nic.mil (US Military)
whois.nic.gov (US Government)
```

اولین‌سایت مشهورترین سایت ثبت Domain برای .com ، .net و .org است.

توجه‌کنید که امروزه سایت‌های مختلفی عمل ثبت Domain را انجام می‌دهند و برای اینکه درمورد یک سایت خاص (که درواقع یک Domain خاص دارد)، اطلاعاتی کسب‌کنیم، باید اطلاعات مربوطه را از سایتی بگیریم که ثبت Domain را انجام داده‌است و چون این‌کار مشکل‌است، به‌جای استفاده‌از سایت‌های فوق، از سایت‌های دیگری استفاده می‌کنیم که این‌کار را برای ما ساده‌تر می‌کنند (آن سایت‌ها نیز درنهایت اطلاعاتشان را از سایت‌های اصلی می‌گیرند و فقط نقش یک واسطه را دارند که هم‌زمان برای ما در چند سایت مختلف

عمل جستجو را انجام می‌دهند تا اطلاعات موردنظر ما به‌دست آید). لازم‌به‌ذکر است که ایجاد چنین سایت‌هایی زیاد هم مشکل‌نیست).

سایت موردعلاقه من برای کسب اطلاعات، سایت زیر است :

http://samspade.org/whois/*domain*

که به‌جای *domain*، آدرس سایت ویا IP آن را می‌نویسیم و اطلاعات زیاد و ارزشمندی درباره سایت موردنظر، حاصل خواهد شد (اطلاعاتی ازقبیل آدرس ISP، شخصی که به‌عنوان Admin کار ثبت را انجام‌داده‌است و... که البته به‌طور قطعی نمی‌توان درمورد صحت اطلاعات نام اشخاص و... اظهارنظر نمود).

تعدادی از مهم‌ترین اطلاعات را درقسمت DNS Servers یا Domain Servers خواهید دید. بعداً درمورد این آدرس‌ها توضیح کامل‌تری خواهم‌داد ولی فعلاً باید بگویم که به‌کمک همین چند آدرسی که در انتها به‌دست می‌آید، می‌توانیم به‌وسیله دستوری به‌نام nslookup اطلاعات باارزش‌تری به‌دست‌آوریم که به‌زودی یاد خواهید گرفت.

ادامه بحث Whois :

قبلاً درمورد IP Whois و DNS Whois صحبت‌کردم. دراینجا بحث DNS Whois (کسب اطلاعات درمورد یک Domain خاص) را ادامه می‌دهیم.

اگر کمی بیشتر از سایت SamSpade استفاده‌کنید، متوجه می‌شوید که برای یک‌سری از Domainها جواب نمی‌دهد. مثلاً آن سایت‌هایی که دارای دامنه جغرافیایی (مثلاً ایران) هستند. درمورد دامنه‌های جغرافیایی ایران باید گفت که به ir. ختم می‌شوند (مثل www.ncis.ir). مثال دیگری که در Whois سایت SamSpade کار نمی‌کند، تعدادی از دامنه‌های com. ، net. و org. هستند که در InterNIC.net ثبت نشده‌اند، بلکه در DomainPeople.com ثبت‌شده‌اند (مثلاً www.sanjesh.org). چند سال قبل، ثبت Domainهایی که در گروه com. ، net. و org. بودند، مختص InterNIC.net بود ولی الآن دیگر این‌طور نیست.

حال به شما می‌گویم که برای Whoisکردن Domainهای مختلف از چه سایت‌هایی استفاده‌کنید :

۱- InterNIC.net : برای com. ، net. ، org. و edu. عالی است. برای aero. ، arpa. ، biz. ، coop. ، info. ، int. و museum. هم می‌توانید از آن استفاده‌کنید. صفحه Web مربوطه در آدرس http://www.internic.net/whois.html قرار دارد؛ یا می‌توانید مستقیماً در آدرس مرورگر خود بنویسید :

http://reports.internic.net/cgi/whois?whois_nic=*domain*&type=domain

و به‌جای *domain* آدرس سایت موردنظر خودتان را بنویسید (مثلاً google.com یا yahoo.com).

۲- NIC.ir : برای ir. استفاده می‌شود. صفحه Web مربوطه عبارت‌است از http://whois.nic.ir یا می‌توانید مستقیماً در آدرس مرورگر خود بنویسید :

http://whois.nic.ir/cgi-bin/whois.pl?name=*domain*

و به‌جای *domain* آدرس سایت موردنظر خودتان را بنویسید (مثلاً ncis.ir).

۳- ChannelME.tv : برای tv. مورداستفاده قرار می‌گیرد. صفحه Web مربوطه عبارت‌است از http://www.channelme.tv یا می‌توانید مستقیماً در آدرس مرورگر خود بنویسید :

http://domains.channelme.tv/searchresults.aspx?searchsld=*domain*

و به‌جای *domain* آدرس سایت موردنظر خودتان را بنویسید (مثلاً channelme.tv).

۴- DomainPeople.com : برای .biz ، .name ، .com ، .net ، .org و .info. عالی است. صفحه Web مربوطه عبارت‌است از http://whois.domainpeople.com و باید بگویم که این سایت، آدرس مستقیم جهت تایپ کردن، ندارد!

همان‌طور که ملاحظه می‌فرمایید، .com ، .net و .org. در ۱ و ۴ مشترک هستند. علت آن‌است که بعضی‌ها در اولی و بعضی‌ها در چهارمی ثبت شده‌اند؛ ولی برای Whoisکردن فرقی ندارد که شما از اولی استفاده‌کنید یا از چهارمی چون یکدیگر را پشتیبانی می‌کنند.

چگونگی استفاده از nslookup :

وقتی که DNS Server یک سایت را به‌دست آورده‌باشیم (ازطریق Whois)، به‌کمک دستور nslookup می‌توان اطلاعات اضافی درمورد آن‌سایت پیدا کرد. طریقه استفاده از این دستور را توضیح می‌دهم. فرض‌کنید که می‌خواهم از Domain Server سایت 404.ir اطلاعاتی به‌دست بیاورم. اگر به این سایت Whois کنم (ازطریق NIC.ir - مورد ۲ در بالا)، می‌بینم که دو عدد Name Server یا DNS Server دارد :

```
ns1.irandns.net
ns2.irandns.net
```

حالا دیگر آدرس DNS Server مربوط‌به 404.ir را دارم و می‌توانم شروع کنم.

۱- درداخل Command Prompt دستور nslookup را نوشته و اجرا می‌کنم و خروجی زیر را مشاهده می‌کنم :

```
*** Can't find server name for address 192.168.15.254: Non-existent domain
Default Server:  vnsc-pri-dsl.genuity.net
Address:  4.2.2.4

>
```

هیچ‌کدام از اطلاعات فوق مهم نیستند. مهم علامت > است که به‌معنی ورود به nslookup است. درجلوی این علامت، می‌توانید دستورات nslookup را بنویسید.

۲- دستور زیر را می‌نویسم :

server *dns_server*

که به‌جای *dns_server* باید آدرس DNS Server سایت موردنظر را بنویسم. پس دراینجا، از یکی‌از دو گزینه ns1.irandns.net و ns2.irandns.net به‌دلخواه، استفاده می‌کنم :

```
> server ns1.irandns.net
Default Server:  ns1.irandns.net
Address:  69.16.242.170

>
```

اگر در این مرحله، پیغام خطا دریافت نمودید، مجدداً دستور را تایپ کنید یا اینکه از DNS Server دیگر دراینجا، ns2.irandns.net) استفاده‌کنید. حال که به Server موردنظر متصل‌شدم، از دستور زیر استفاده می‌کنم تا مشخص کنم که در گزارش من، باید همه اطلاعات ذکر شوند :

```
> set type=any
>
```

این دستور، خروجی ندارد و دوباره اعلان مربوطه ظاهر می‌شود.

۴- حالا به‌کمک دستور زیر، اطلاعات را به‌دست می‌آورم :

```
> ls -d site_name.
```

که برای 404.ir می‌شود :

```
> ls -d 404.ir.
```

دقت‌کنید که اسم سایت، یک نقطه (dot) گذاشته‌ام. شما هم بهتر است این‌طوری بنویسید (بعداً علت آنرا خواهید فهمید). نتایج زیر حاصل می‌شود :

```
[ns1.irandns.net]
 404.ir.                    SOA    ns1.irandns.net xeekor@googlemail.com.404.ir. (2007112100 86400 7200 3600000 86400)
 404.ir.                    MX     0    404.ir
 404.ir.                    NS     ns1.irandns.net
 404.ir.                    NS     ns2.irandns.net
 404.ir.                    A      69.16.242.170
 domain                     A      67.15.47.4
 domains                    A      67.15.47.4
 ftp                        A      69.16.242.111
 localhost                  A      127.0.0.1
 mail                       CNAME  404.ir
 www                        CNAME  404.ir
 xeekor                     A      69.16.242.170
 www.xeekor                 A      69.16.242.170
 404.ir.                    SOA    ns1.irandns.net xeekor@googlemail.com.404.ir. (2007112100 86400 7200 3600000 86400)
```

بعداً درمورد کاربرد تک‌تک این موارد صحبت خواهم‌کرد؛ ولی بعضی‌از آنها اطلاعات واضحی دارند (می‌توانید آنها را بیابید؟). برای راهنمایی و دریافت لیست دستورات nslookup، از دستور help درجلوی اعلان آن (>) استفاده کنید.

۵- دستور exit را مقابل اعلان تایپ‌کرده و اجرا می‌کنم تا از nslookup خارج‌شوم.

می‌توانید برای تمرین، چند سایت دلخواه را امتحان‌کنید.