

بسم الله الرحمن الرحيم

## رد پا ( Footprinting )

هک اخلاق مدارانه ( سلسله گزارش های فنی ، شماره ۲ )

نویسنده : مهندس علی کسرائی<sup>۱</sup>

کلید واژه ها :

رد پا ، مهندسی اجتماعی ، Whois ، هک گوگل ، Trace

چکیده :

مرحله رد پا ، اولین قسمت از فرآیند کاری ، قبل از وقوع حملات است که شامل گردآوری همه گونه اطلاعات در دسترس ، در مورد یک سازمان می باشد بطوریکه این اطلاعات می تواند در حملات علیه سازمان مربوطه ، مورد استفاده هکر قرار بگیرد . در بعضی مواقع ، اطلاعات گردآوری شده ، توسط مهندسی اجتماعی بدست می آید . بدین معنی که اطلاعات گردآوری شده ، توسط مهندسی اجتماعی نیز ، می تواند ، در نهایت ، به یک حمله ، منتهی شود . در این گزارش فنی به هر دوی این مباحث ، نظر تحلیلی می افکنیم و به تفصیل ، مهمترین موضوعات آن را که شامل موارد ذیل است مورد بررسی قرار می دهیم .

الف ) تعریف اصطلاح رد پا

ب ) تشریح متدلوژی گردآوری اطلاعات

ج ) تشریح خبرگیری یا جاسوسی ، با انگیزه ی رقابت

د ) درک ریز یا صورت اطلاعاتی ( DNS ) ها

ه ) درک جستجوهای ( Whois ) و ( ARIN )

و ) تشخیص انواع متفاوت رکوردهای ( DNS )

ز ) درک عملکرد ( E-Mail Tracking )

ح ) درک عملکرد ( Web Spider ) ها یا دام گستران وب

<sup>۱</sup> مدیر و مؤسس مرکز مهارت آموزی هزارستان ، محقق سیستم های امنیت اطلاعات و سیستم های هوشمند

## مقدمه :

### رد پا ( Footprinting ) :

رد پا ، مرحله ای است ، پیش از حمله نهایی ، که به منظور آماده سازی ابزار و اطلاعات لازم ، جهت شروع کار ، تعریف می شود . در واقع ، این مرحله ، به جمع آوری داده های لازم در خصوص محیط هدف مورد نظر اشاره داشته و همچنین به طرح ریزی ، جهت بررسی راه های ورود غیر قانونی به سیستم ها می پردازد . در این فاز ، به راحتی ، نقاط آسیب پذیر سیستم آشکار شده و به سهولت می توان ، درک کرد که با کدام ابزار ، می توان ، سیستم مزبور را مورد سوء استفاده قرار داد . این آسانترین راه ، برای هکرها ، در خصوص ، جمع آوری اطلاعات در مورد سیستم های کامپیوتری و کمپانی های استفاده کننده از آنها ، به شمار می رود . به دیگر سخن ، هدف این فاز ، ایجاد آمادگی لازم برای هکر ، بدین مفهوم که ، بتواند اطلاعاتی را در مورد سیستم های مذکور ؛ شامل توانایی های دستیابی از راه دور ، پورتهای و سرویس های اجراء شده ، بر روی سیستم های عامل شان ، و در آخر ، همه جوانب ویژه ی امنیتی سیستم های مذکور ، در اختیارش ، قرار دهد .

### تعریف اصطلاح رد پا ( Footprinting ) :

**( الف ) رد پا ؛** در واقع ، به فرآیند پیش طرحهای گرافیکی – متنی از شبکه ها و سیستم های یک سازمان ، اشاره دارد . به دیگر سخن ، ( Information gathering ) یا جمع آوری اطلاعات نیز به نوعی ، بر فرآیند مرحله ی رد پا ، دلالت می کند . پس مرحله ی رد پا ، کلیه ی مختصات هدف مورد نظر ، از قبیل سیستم های داخلی ، برنامه های کاربردی و موقعیت فیزیکی رایانه ها در شبکه ی داخلی و ... را آشکار می سازد . هنگامی که اطلاعات ویژه ی این سازمان ، جمع آوری شد ، هکر سعی در انتخاب و شناسایی روشهایی جهت نفوذ ، اما بدون فشار و از راههای مطمئن ، می نماید . به عنوان مثال ، یک سازمان ، ممکن است در یکی از صفحات وب خود ، لیستی از کارمندان ؛ همراه با معرفی شاخه ی فعالیتهای آنها را ارائه نموده باشد که عملاً ممکن است در یک حمله از نوع ( مهندسی اجتماعی ) ، برای سارقین اطلاعات ، به جهت رسیدن به اهدافشان ، مفید باشد . یک هکر ممکن است ، جمع آوری اطلاعات ، از قبیل محل اقامت کارمندان و یا دیگر اطلاعات درباره مردم را از طریق جستجوی اطلاعات در سایت ( Google ) و یا ( Yahoo ) بدست آورد . موتور جستجوی گوگل ، ممکن است که بوسیله ی روش های توأم با خلاقیت ، جهت جمع آوری اطلاعات افراد یا ... ، مورد بهره برداری قرار بگیرد . عمل برگردان اطلاعات بوسیله ی روشهای مزبور ، را ( روشهای هک گوگل ) یا ( Google hacking ) می نامند . از سایت ( <http://groups.google.com> ) نیز ، ممکن است جهت جمع آوری اطلاعات در گروههای خبری نیز ، بهره برداری شود .

در ادامه ، به دستوراتی اشاره می شود که می توانند ، موتور جستجوی گوگل را وارد نماید تا به سرعت ، اطلاعات پیرامون موارد ذیل را برگرداند :

#### \* ( Site - سایت ) :

ممکن است یک وب سایت یا ( Domain ) را سرچ نماید . پس نام وب سایت ، باید پس از دو نقطه ( : ) یا کالون ، آورده شود .

#### \* ( file type - نوع فایل ) :

در میان متون ، فقط به جستجوی نوع مخصوصی از یک فایل ، می پردازد . مواظب باشید که هیچ فاصله ای قبل از پسوند فایل قرار ندهید .

**\* (Link – لینک یا فوق متن ) :**

جستجو را بر پایه ی لینک های ( فوق متن های ) قابل تشخیص ، انجام می دهد .

**\* ( cache – حافظه پنهانی ) :**

- بوسیله ی حافظه پنهانی ، نسخه ( ورژن ) یک صفحه وب ، تشخیص داده می شود . آدرس ( URL ) سایت ، باید بعد از دو نقطه ( : ) یا کالون قرار گیرد .

**\* ( intitle – در عناوین ) :**

- هدف ، جستجوی یک اصطلاح ، در داخل عناوین متون و اسناد می باشد .

**\* ( inURL – در آدرس URL ) :**

- جستجو ، فقط بر اساس آدرس ( URL ) وب سایت ها انجام می شود . عنوان این نوع جستجو نیز ، باید پس از ( : ) یا کالون قرار گیرد . بعنوان نمونه ، هکر می تواند ، فرامین فوق را بشکل ذیل بکار گیرد :

**INURL: ["parameter = "]**

به همراه :

**FILETYPE: [ext]**

و همچنین :

**INURL: [Script name]**

- که این روش به طور کامل ، نوعی از انواع کاربردهای ویژه ی کشف نقاط آسیب پذیر برنامه های تحت وب را ، به نمایش می گذارد و یا حتی هکر می تواند به جهت بررسی

( Novell Border Manager Proxy/firewall servers ) ؛ به جستجو بر پایه ی متن ذیل بپردازد :

Intitle: "Boarder Manager information alert"

پس ، متوجه این نکته شده اید که ، وبلاگها ، گروههای خبری و یا حتی روزنامه ها ، همگی ، مکانهای خوبی برای یافتن اطلاعات در مورد یک کمپانی یا کارمندانش ، خواهد بود . شخصیت حقوقی مشاغل نیز برای خود ، دارای داده هایی هستند که ممکن است به راحتی ، با نفوذ به یک سرور و یا حتی به وسیله ی دسترسی به وسایل رایانه ای درون شبکه ی داخلی همان شرکت ، در دسترس ، قرار گیرند . و بدین ترتیب ، اطلاعات دیگر که شامل ، شناسائی نوع تکنولوژی بکار گرفته شده در اینترنت ، نوع سیستم عامل و سخت افزارهای بکار رفته در محیط کار شرکت مزبور ، تشخیص آدرسهای ( IP ) فعال شبکه ها ، آدرس پست الکترونیکی افراد ، شماره تلفن های آنها و همچنین عملکرد و ( Policy ) های داخلی شرکت می باشد ، همگی به سادگی قابل جمع آوری خواهند شد .

**( نکته )**

عموماً ، هکر ، ( ۹۰ ) درصد از زمان خود را صرف جمع آوری اطلاعات در مورد اهداف می نمایند و ( ۱۰ ) درصد باقیمانده از زمان را صرف حمله و بررسی روش های مختلف حمله به اهداف ، می نمایند . پس نتیجه گیری می شود که مرحله ی جمع آوری اطلاعات در مورد اهداف ، بسیار مهم است .

## اشارت مهم نگارنده :

به عنوان نمونه اگر شما این عبارت را در موتور جستجوی گوگل وارد نمایید ؛  
[[allinurl:tsweb/default.htm](http://allinurl:tsweb/default.htm)] گوگل برایتان اطلاعات مهم و زیربنایی از  
سرورهایی با ویندوز مایکروسافت همراه با داده های مربوط به [ Remote Desktop Connection ]  
برملا خواهد کرد . اضافه می شود که جهت کسب اطلاعات در مورد سیستم های هک گوگل به این منبع رجوع  
نمایید : [Google Hacking For Penetration Testers , By : Johnny Long – Syngress ۲۰۰۴]

## ب ( تشریح متدولوژی جمع آوری اطلاعات :

مرحله ی جمع آوری اطلاعات را می توان به ( ۷ ) مرحله تقسیم بندی نمود . مرحله رد پا ، فقط شامل دو مرحله  
ی اول از تقسیمات می شود ، که به نوعی می توان این مراحل را شامل حفاری آغازین ، جهت کسب اطلاعات و  
همچنین درک مقادیر و داده های علمی مربوط به شبکه مزبور ، دانست . ( شکل ۱ ، این مراحل را به تصویر  
کشیده است ) .

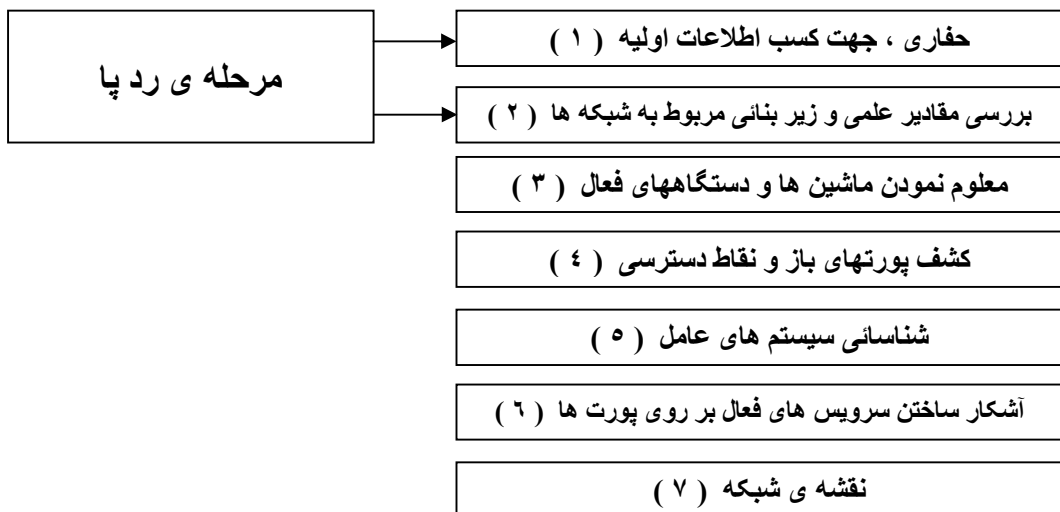
نکته ( از دیگر مراحل جمع آوری اطلاعات می توان به ( اسکن کردن - Scanning ) و ( سر شماری ، شماره  
گذاری یا Enumeration ) اشاره نمود که در گزارش فنی ( ۳ ) ، بطور کامل ، به شرح آنها ، خواهیم پرداخت .  
در ادامه بعضی از ابزارهایی را که برای جمع آوری اطلاعات از منابع معمولی ، مورد استفاده قرار می گیرند ،  
ارائه شده است :

Domain name lookup ( ۱ )

Whois ( ۲ )

Ns lookup ( ۳ )

Sam spade ( ۴ )



( شکل ۱ ) - مراحل هفتگانه جمع آوری اطلاعات

پیش از اینکه ، مباحثی را از قبیل معرفی و نحوه ی عملکرد ابزار های فوق الذکر ، مطرح نمائیم ؛ به خاطر بسیاری که اطلاعات بر پایه ی منبع باز ( open source ) ، یک ثروت واقعی برای هکر ، به جهت کسب اطلاعات در مورد اهدافش ، مانند ، آدرس ، شماره تلفن ها و ... به حساب می آید . ( Whois ) ، درخواست جستجو مبنی بر جداول ( DNS ) ، اسکن آدرسهای ( IP ) برای پورتهای باز و ... همگی ، از دیگر مصادق ( Footprinting ) یا رد پا به گونه ی ( منبع باز یا open source ) می باشند .

بد نیست که بدانید ، اکثر این اطلاعات نسبتاً آسان و قانونی بدست می آیند . شایان ذکر است که جزئیات اینکه ، ( DNS ) چگونه عمل می کند و همچنین تفسیر جزئیات مربوط به روش های نگهداری رکوردهای نامگذاری ( DNS ) ، از دامنه ی مورد بحث در کتاب حاضر ، بیرون است و ما فقط اشارتی گذرا نمودیم که بهانه ای باشد تا بطور مجزا ، توسط شما ، مورد مطالعه و تحقیق قرار گیرد . پس تنها مهمترین عناوینی که مربوط به جمع آوری اطلاعات است ، در راستای کار ما قرار دارد . لذا توصیه می شود که همه علاقمندان به شرکت در آزمون ( CEH ) و یا دیگر مدارج امنیتی ، جهت درک کامل از نحوه ی عملکرد ( DNS ) در اینترنت ، مطالعات دقیق و برنامه ریزی شده ای را انجام دهند .

## ابزار هک :

( Sam spade ) به آدرس ( <http://www.samspace.org> ) ، یکی از مجموعه ابزارهایی که جهت ( Whois ) کردن ، مورد استفاده قرار می گیرد را ارائه کرده است . همچنین ابزارهایی چون ( nslookup ) و ( traceroute ) . شایان ذکر است که این ابزارها ، بر روی هر سیستم عاملی کار می کنند و به راحتی ، اطلاعات مورد نیاز هکر را از طریق وب سایت یک سازمان ، فراهم می کنند .

## ج ( تشریح خبرگیری یا جاسوسی با انگیزه ی رقابت :

خبرگیری رقابتی ، به مفهوم جمع آوری اطلاعات ، درباره محصولات تولیدی رقبا ، داد و ستد آنها و همچنین تکنولوژیهای مورد استفاده ی آنها ، می باشد . این نوع از جاسوسی ، بی خطر است و فقط برای مقایسه ی آمار فروش ، ساخت و غیره ی محصولات تولیدی شرکتها ، با یکدیگر کاربرد دارد و مشخص می کند که رقبا ، چگونه محصولاتشان را می فروشند و همچنین اطلاعاتی در مورد بازار کار و ... ابزارهای متفاوتی وجود دارند که جهت خبرگیری رقابتی ، مورد بهره گیری قرار می گیرند و یا حتی ، می تواند ، توسط یک هکر به کار گرفته شوند ، جهت کسب اطلاعات در مورد پتانسیل های امنیتی یک هدف خاص .

## د ( درک ریز ، سرشماری و یا صورت اطلاعاتی ( DNS ) ها :

( DNS Enumeration ) ، فرآیندی تعیین کننده برای همه سرورهای ( DNS ) و همچنین رکوردهای متناظرشان برای یک سازمان ، بشمار می آید . یک کمپانی ممکن است ، هر دوی سرورهای ( DNS ) داخلی یا خارجی را داشته باشد ، تا بتواند اطلاعات مهمی ، از قبیل نام کاربران ، نام رایانه های داخلی ، آدرسهای ( IP ) و در نهایت پتانسیل سیستمهای هدف را مدیریت نماید . ( NSlookup ) ، ( DNSstuff ) و ( the American Registry for Internet Numbers = ARIN ) و ( Whois ) می توانند ، همه ی آن اطلاعاتی که جهت ( DNS Enumeration ) است را ، فراهم نمایند .

## ( Nslookup and DNSstuff ) :

یکی از ابزارهای قدرتمندی که باید به آن آشنا باشید ، ( nslookup ) است . ( به شکل ۲ نگاه کنید ) . این ابزارها ، در حقیقت ، ابزارهای جستجوگر سرورهای ( DNS ) ، بر اساس کوئری ( Queries ) ، برای استخراج رکوردهای اطلاعات ، می باشند و در سیستمهای عامل یونیکس ، لینوکس و ویندوز وجود دارند . شایان ذکر است که در ابزارهای هک کردن ، مانند ( Sam spade ) نیز ، ( nslookup ) تعبیه شده است .

```
C:\WINDOWS\system32\cmd.exe

C:\>nslookup www.eccouncil.org
Server:
Address:

Non-authoritative answer:
Name:      www.eccouncil.org
Address:  64.90.176.10
```

( شکل ۲ ) – nslookup

همانند مکانیزم جمع آوری اطلاعات در ( Whois ) ، شما می توانید ، از ( nslookup ) ، برای یافتن آدرسهای ( IP ) اضافی ، برای سرورهای دیگر میزبانان ( hosts ) ، استفاده نمایید ؛ همچنین در کنار یافتن اطلاعاتی درباره ی نامهای معتبر سرورها در ( Whois ) مانند ( AUTH1.NS.NYI.NET ) میتوانید ، آدرسهای ( IP ) سرورهای پست الکترونیک ( سرویس دهنده های پستی ) را نیز ، کشف کنید . صدای انفجاری که در کاربرد آسان این گونه ابزار ، به گوش می رسد ، حاکی از آن است که در عمل هکینگ ، بسیار ساده جلوه نموده ؛ در صورتیکه شما ، عملکرد این وسایل را بشناسید . ( DNS stuff ) نیز از دیگر وسایل هک کردن است . به جای استفاده از خط فرمان ( nslookup ) با کلید های مشکل برای کار با آن ، جهت جمع آوری اطلاعاتی در مورد رکوردهای ( DNS ) ، فقط کافیست که به وب سایت ( http://www.dnsstuff.com ) دسترسی داشته باشید . آری ؛ شما به یک موتور جستجوی قدرتمند رکوردهای ( DNS ) آنلاین ( online ) ، وصل شده اید . شکل شماره ( ۳ ) نمونه ای از جستجوی رکورد های ( DNS ) روی وب سایت ( www.eccouncil.org ) را به وسیله ی وب سایت فوق الذکر ، نشان می دهد .

## DNS Lookup: eccouncil.org A record

Generated by [www.DNSstuff.com](http://www.DNSstuff.com) at 13:01:51 GMT on 12 Apr 2006.

Now I am searching:  
Searching for eccouncil.org A record at 1.root-servers.net [198.32.54.12]: Got referral to TLD4.ULTRADNS.org. [took 94 ms]  
Searching for eccouncil.org A record at TLD4.ULTRADNS.org. [199.7.67.1]: Got referral to AUTH2.NS.NYI.NET. [took 7 ms]  
Searching for eccouncil.org A record at AUTH2.NS.NYI.NET. [66.111.15.154]: Report: eccouncil.org. [took 9 ms]

Answer:

Domain	Type	Class	TTL	Answer
eccouncil.org.	A	IN	3600	64.90.176.10
eccouncil.org.	NS	IN	3600	auth2.ns.nyi.net
eccouncil.org.	NS	IN	3600	auth1.ns.nyi.net
auth2.ns.nyi.net.	A	IN	7765	66.111.15.154

There is no need to *refresh* the page -- to see the DNS traversal, to make sure that all DNS servers are reporting the same results, you can [Click Here](#).

Note that these results are obtained in real-time, meaning that these are *not* cached results.  
These results are what DNS resolvers all over the world will see right now (unless they have cached information).

( شکل ۳ ) – جستجوی رکوردهای DNS از سایت www.eccouncil.org

این جستجو ، تمامی رکوردهای مربوط به نامهای ساختگی و اصلی وب سایت مورد نظر را و همچنین آدرسهای ( IP ) سرورهای وب آنرا نیز ، آشکار می سازد . بدین مفهوم که می توانیم ، همه ی نامهای سرورها و آدرسهای ( IP ) مختص به آنها را کشف نمائیم و این برای هکر ، یعنی همه چیز ... .

#### یادداشت )

این اکسپلویت ، برای شما در گزارش فنی شماره ی ( ۴ و ۵ ) ، تحت عنوان ( سیستمهای هکینگ ) به تفصیل ، تشریح شده است .

#### ه ) درک جستجوهای ( Whois ) و ( ARIN ) :

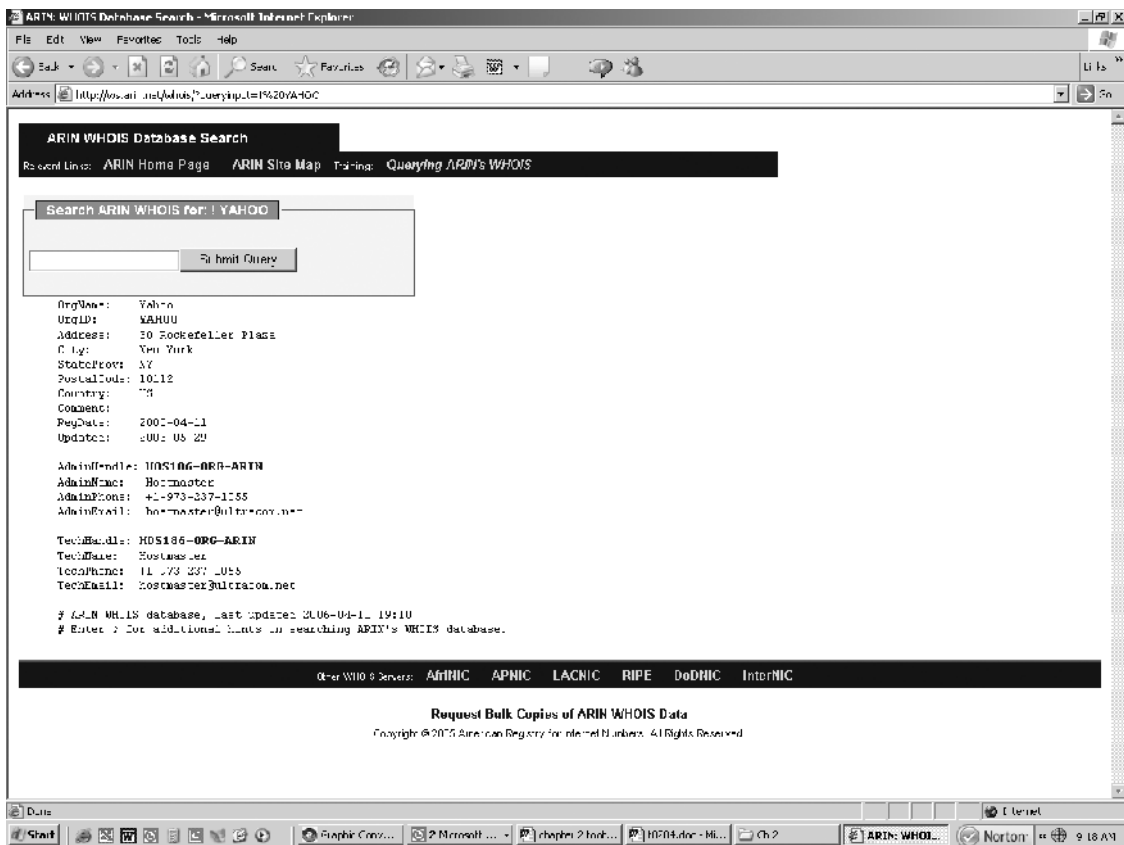
( Whois ) ، راه تکامل و کاربرد خود را از سیستم عامل یونیکس پیدا کرد ولی امروزه در بسیاری از سیستمهای عامل دیگر نیز ، می تواند ، وجود داشته باشد و می تواند ، به عنوان ابزاری ، برای هک در اینترنت ، مورد بهره برداری قرار گیرد . این ابزار می تواند تشخیص دهد که چه کسی ، یک نام ثبت شده ، برای ( Domain ) خود دارد که از آن در وب سایت و ( E-Mail ) های خود ، استفاده می نماید . یک آدرس URL ( uniform resource locator ) ، مانند ( www.Microsoft.com ) ، شامل نام ( Domain ) یعنی ( Microsoft.com ) با عملکرد تجاری ، همچنین نام یک میزبان ( host ) یا نام های مستعاری با خاصیت ( www ) می باشد .

در شرکت ( ICANN ) ؛ ( Internet Corporation for Assigned Names and NUMBERS ) در خصوص ثبت نام ( Domain ) تصویب شده است که یک نام ( Domain ) فقط متعلق به یک کمپانی ویژه باشد . ابزارهای ( Whois ) ، در واقع ، حاصل پرسش هایی را برمی گردانند که بازایی اطلاعات مربوط به اشخاص یا سازمان ها ، در خصوص ثبت ( Domain ) و... در بانک اطلاعاتی مربوطه را شامل شود .

#### ابزار هک :

یک ( Whois ) هوشمند ، در واقع برنامه ی گرد آوری اطلاعاتی است که اجازه می دهد تا شما ، به همه ی اطلاعات ، درباره ی یک آدرس ( IP ) ، نام میزبان ( host name ) و یا ( Domain ) ، در حیطه ی کشور ، استان ، شهر و همچنین نام تامین کننده ی شبکه ها ، ( Administrator ) ها و تلفن های مربوط به بخش پشتیبانی فنی ( Technical - supports ) ، دسترسی پیدا نمائید .

( ARIN ) ، در حقیقت ، یک بانک اطلاعاتی از داده هاست که شامل اطلاعاتی در خصوص صاحبان آدرسهای ( IP ) استاتیک می باشد . بانک های اطلاعاتی ( ARIN ) نیز می توانند ، توسط پرسش های ( query ) ابزارهای ( Whois ) ، مورد بهره برداری قرار گیرند . به عنوان نمونه به آدرس (<http://www.arin.net/whois>) مراجعه نمائید. ( شکل ۴ ) ، جستجوی ARIN با استفاده از ابزار ( Whois ) را برای آدرس (<http://www.yahoo.com>) نشان می دهد . توجه کنید که آدرسها ، پست های الکترونیک و اطلاعات تلفنی ؛ همگی در حاصل جستجوی ( Whois ) ، نهفته است . این اطلاعات می تواند به وسیله ی یک هکر اخلاق مدار مورد استفاده قرار گیرد که بفهمد ، یک آدرس ( IP ) ، مربوط به کدام سازمان بوده و... و همچنین می تواند به وسیله ی یک هکر بدخیم ، مورد استفاده قرار گیرد که حداقل صدمات ناشی از این اتفاق ، می تواند ، به شکل یک حمله ی ( مهندسی اجتماعی ) عظیم ، بر ضد یک سازمان ، جلوه کند . به هر صورت ، به عنوان یک حرفه ای امنیت ، احتیاج دارید که توسط ابزارهای جستجویی از قبیل ( ARIN ) ، به بانک های اطلاعاتی شامل داده های مردم و ... دسترسی داشته باشید ؛ ولی مطمئن باشید که سارقان بدخیم ، از این اطلاعات ، به جهت آماده سازی حملات ، بر ضد شبکه های رایانه ای ، استفاده خواهند کرد .



( شکل ۴ ) – خروجی ARIN برای آدرس <http://www.yahoo.com>

## یادداشت :

آگاه باشید که دیگر مناطق جغرافیایی بیرون از آمریکای شمالی ، دفاتر ثبت اینترنتی مخصوص به خودشان را دارند . از قبیل ( RIRE NCC ) اروپا ، خاورمیانه ، و قسمتهایی از آسیای مرکزی [ همچنین ( LACNIC ) آمریکای لاتین و آدرس های اینترنتی ثبت شده ی مربوط به کارائیب [ و ( APNIC ) مرکز اطلاعات شبکه ای آسیا پاسیفیک ] .

## تجزیه و تحلیل خروجی Whois :

یک راه ساده برای اجرای عمل ( Whois ) ، اینست که به وب سایتی که این خدمات را ارائه می دهد ، متصل شوید ( برای مثال : [www.networksolutions.com](http://www.networksolutions.com) ) و جستجوی ( Whois ) را انجام دهید . در ذیل ، نتیجه ی یک ( Whois ) ، روی سایت ( [www.eccouncil.org](http://www.eccouncil.org) ) ، ارائه می شود .



## یادداشت :

کلیه ی نامهای افراد و سرورها ، در نتایج حاصل از جستجوی این ابزارها ، در این گزارش فنی ، به لحاظ رعایت مسائل امنیتی ، تغییر یافته اند .

Domain ID:D۸۱۱۸۰۱۲۷-LROR  
Domain Name:ECCOUNCIL.ORG  
Created On:۱۴-Dec-۲۰۰۱ ۱۰:۱۳:۰۶ UTC  
Last Updated On:۱۹-Aug-۲۰۰۴ ۰۳:۴۹:۵۳ UTC  
Expiration Date:۱۴-Dec-۲۰۰۶ ۱۰:۱۳:۰۶ UTC  
Sponsoring Registrar:Tucows Inc. (R۱۱-LROR)  
Status:OK  
Registrant ID:tuTv۲ltRZBMNd۴IA  
**Registrant Name: Ali Kasraei**  
Registrant Organization:International Council of E-Commerce Consultants  
Registrant Street۱:۶۷ Wall Street, ۲۲nd Floor  
Registrant Street۲:  
Registrant Street۳:  
Registrant City:New York  
Registrant State/Province:NY  
Registrant Postal Code:۱۰۰۰۵-۳۱۹۸  
Registrant Country:US  
Registrant Phone:+۱.۲۱۲۷۰۹۸۲۵۳  
Registrant Phone Ext.:  
Registrant FAX:+۱.۲۱۲۹۴۳۲۳۰۰  
Registrant FAX Ext.:  
Registrant Email:forum@eccouncil.org  
Admin ID:tus۹DYvpp۵mrbLNd  
**Admin Name: Ali Kasraei**  
Admin Organization:International Council of E-Commerce Consultants  
Admin Street۱:۶۷ Wall Street, ۲۲nd Floor  
Admin Street۲:  
Admin Street۳:  
Admin City:New York  
Admin State/Province:NY  
Admin Postal Code:۱۰۰۰۵-۳۱۹۸  
Admin Country:US  
Admin Phone:+۱.۲۱۲۷۰۹۸۲۵۳  
Admin Phone Ext.:  
Admin FAX:+۱.۲۱۲۹۴۳۲۳۰۰  
Admin FAX Ext.:  
Admin Email:ethan@eccouncil.org  
Tech ID:tuE۱cgAfi۱VnFkpu  
Tech Name:Jacob Eckel  
Tech Organization:International Council of E-Commerce Consultants  
Tech Street۱:۶۷ Wall Street, ۲۲nd Floor  
Tech Street۲:  
Tech Street۳:  
Tech City:New York  
Tech State/Province:NY  
Tech Postal Code:۱۰۰۰۵-۳۱۹۸  
Tech Country:US  
Tech Phone:+۱.۲۱۲۷۰۹۸۲۵۳  
Tech Phone Ext.:  
Tech FAX:+۱.۲۱۲۹۴۳۲۳۰۰  
Tech FAX Ext.:  
Tech Email:forum@eccouncil.org  
**Name Server: ns۱.xyz.net**  
**Name Server: ns۲.xyz.net**

به چهار ردیف درشت و سیاه ، در این متون توجه نمایند . اولین سطر ، هدف را نشان می دهد که می تواند یک کمپانی یا شخص باشد . ( همچنین آدرس فیزیکی شان ، آدرس پست الکترونیکی ، شماره تلفن و به همین ترتیب ) . دومین سطر ، به اطلاعاتی چون تلفن تماسهای بخش فنی یا اداره ی خاص اشاره دارد و دو سطر آخر نیز ، به نامهای سرورهای ( Domain ) [ domain name servers ] اشاره دارند .

• **اشارات مهم نگارنده :**

با عنایت به ذکر این مطلب که کلیه ی اطلاعات مذکور در این سلسله مقالات جنبه ی علمی داشته و هر گونه سو استفاده از آنها به عهده ی شخص خاطی می باشد به معرفی آدرس های اینترنتی سازمان های ممیز و ابزارهای مورد استفاده در مباحث ( Whois ) می پردازیم :

- ICANN – [www.icann.org](http://www.icann.org) ( شروع عملکرد از سال ۱۹۹۸ )
- IANA – [www.iana.org](http://www.iana.org)
- ASO – [www.aso.icann.org](http://www.aso.icann.org)
- GNSO – [www.gnso.icann.org](http://www.gnso.icann.org)
- CCNSO – [www.ccnso.icann.org](http://www.ccnso.icann.org)
- APNIC – [www.apnic.net](http://www.apnic.net)
- ARIN – [www.arin.net](http://www.arin.net)
- LACNIC – [www.lacnic.net](http://www.lacnic.net)
- RIPE – [www.ripe.net](http://www.ripe.net)
- AfriNIC – [www.afrinic.net](http://www.afrinic.net)

## **Whois :**

- [www.allwhois.com](http://www.allwhois.com)
- [www.uwhois.com](http://www.uwhois.com)
- [www.internic.net/whois.html](http://www.internic.net/whois.html)

• ابزارها :

مکانیزم	منبع	پلاتفرم
Web Interface	<a href="http://www.whois.iana.org">www.whois.iana.org</a> <a href="http://www.arin.net">www.arin.net</a> <a href="http://www.allwhois.com">www.allwhois.com</a>	سازگار با همه نوع سیستم عامل همراه با ساپورت سرویس گیرندگان وب
Whois Client	این برنامه در کلیه ی نسخ سیستم عامل یونیکس قابل استفاده است	یونیکس
Ws_ping pro pack	<a href="http://www.ipswitch.com">www.ipswitch.com</a>	ویندوز های ۹۵ XP / ۲۰۰۰ / NT
Sam Spade	<a href="http://www.samspade.org/ssw">www.samspade.org/ssw</a>	ویندوز های ۹۵ XP / ۲۰۰۰ / NT
Sam Spade Web Interface	<a href="http://www.samspade.org">www.samspade.org</a>	سازگار با همه نوع سیستم عامل همراه با ساپورت سرویس گیرندگان وب
Netscan Tools	<a href="http://www.netscantools.com/nstpromain.html">www.netscantools.com/nstpromain.html</a>	ویندوز های ۹۵ XP / ۲۰۰۰ / NT
Xwhois	<a href="http://www.c۴۴.org/&lt;۱۲۶&gt;nr/xwhois">www.c۴۴.org/&lt;۱۲۶&gt;nr/xwhois</a>	همراه با Unix GTK و X GUI
Jwhois	<a href="http://www.gnu.org/software/jwhois/jwhois.html">www.gnu.org/software/jwhois/jwhois.html</a>	یونیکس

## یافتن دامنه ی آدرسهای یک شبکه :

هر هکر اخلاق مدار ، احتیاج دارد تا بفهمد ، که چگونه ، دامنه ی مقادیر شبکه ای یا ( Subnet mask ) سیستم هدف را پیدا کند . آدرسهای ( IP ) ، قابل اسکن شدن هستند و جهت اتصال به سیستم های هدف ، مورد استفاده قرار می گیرند . شما می توانید ، آدرسهای ( IP ) را در دفاتر ثبت اینترنتی از قبیل ، ( ARIN ) و یا یک مرجع صلاحیت دار انتصاب اعداد یکتا ، نظیر ( IANA ) ، پیدا کنید . همچنین یک هکر اخلاق مدار ، ممکن است به اطلاعاتی نظیر نوع شبکه ها و یا حتی ، مکان جغرافیائی سیستمهای مورد نظرشان ، احتیاج پیدا نماید . این کار را می تواند ، بوسیله ی ردیابی آدرسهای ( IP ) فرستنده ی یک پیغام ، انجام دهد . شما نیز می توانید از ابزارهایی چون ، ( trace route ) ، ( visualroute ) و ( Neotrace ) ، جهت شناسائی اینگونه راههای ورود به اهداف ، استفاده نمائید . مضافاً اینکه شما می توانید شبکه های هدفشان را ( trace ) نمائید و به دیگر اطلاعات مفید ، دسترسی پیدا کنید . بطور مثال ، شما می توانید آدرسهای ( IP ) رایانه های میزبان داخلی ( host machines ) را بدست آورید ؛ همچنین می توانید ، آدرس ( IP ) دروازه اینترنتی یک سازمان [ Internet ip gateway ] را بیابید . بنابراین ، این آدرسها ، می توانند در یک حمله بکار گرفته شوند و یا فرآیند اسکن رایانه های هدف را تقویت بخشند .

## و ( تشخیص انواع متفاوت رکوردهای ( DNS ) :

فهرست زیر ، انواع رکوردهای ( DNS ) را بطور معمول نشان می دهد و به شرح مختصر کاربریشان ، اشاره می نماید :

### ۱ ( A ) ( آدرس - address ) :

- نگاشت نام میزبان به یک آدرس .

### ۲ ( SOA ) ( آغاز اعتبار سنجی – start of Authority ) :

- تشخیص سرور ( DNS ) پاسخگو برای اطلاعات ( Domain ) .

### ۳ ( CNAME ) ( نام استاندارد و قانونی – Canonical name ) :

- نام سازی نامهای اضافی و یا مستعار برای رکوردهای آدرس .

### ۴ ( MX ) ( تبادل پستی – mail exchange ) :

- تشخیص سرورهای پست الکترونیک برای ( Domain ) .

### ۵ ( SRV ) ( سرویس - service ) :

- شناسائی سرویس هایی از قبیل ( directory services ) .

### ۶ ( PTR ) ( اشاره گر - pointer ) :

- نگاشت آدرسهای ( IP ) به نامهای میزبان ( host names ) .

### ۷ ( NS ) ( سرویس دهنده ی نام – name server ) :

- شناسائی دیگر سرویس دهنده های نام برای ( Domain ) .

## درک چگونگی عملکرد ( Trace route ) در مرحله ی رد پا ( Footprinting ) :

( Trace route ) یک ابزار ردیاب بسته یا ( Packet - tracking ) می باشد که در اکثر سیستم ها ی عامل ، موجود است . عملکرد آن ناشی از آنالیز انعکاسی است ، که حاصل فرستادن یک پیغام به اسلوب پروتکل کنترل پیامهای اینترنتی یا ( ICMP ) بر روی هر ( hop ) مانند [ مسیر یابها یا دروازه ها – router or gateway ] و در امتداد همان مسیر ، تا رسیدن به آدرس یا نشانی مقصد ، می باشد . پس از آنکه ( ICMP ) بوسیله ی مسیر یاب ، بازپس فرستاده شد ، زمان ( time to live - TTL ) بوسیله ی هر مسیر یابی که در امتداد مسیر وجود داشته باشد ، کاهش پیدا خواهد کرد ) و این نکته به هکر ، اجازه می دهد ، تا معلوم سازد که چند ( hop ) یا ( مسیر یاب ) ، در امتداد مسیر بین فرستنده تا گیرنده ، موجود می باشد . اما مشکلی که برای استفاده از ابزار ( trace route ) وجود دارد ، آنست که هنگام برخورد با یک فایروال ( firewall ) و یا سیستم فیلترینگ یک مسیر یاب ( packet – filtering router ) ؛ مدت زمان انجام عمل ( times out ) ، بصورت کاراکتر ستاره ، نمایش داده می شود . اگرچه یک فایروال ، از کشف میزبانان داخلی در یک شبکه ، توسط ابزار ( trace route ) جلوگیری می کند ولی برای یک هکر اخلاق مدار ، نوعی هشدار است و نشان از حضور یک فایروال دارد ؛ بنابراین ، می تواند ذهنیت ایشان را معطوف این نکته نماید که ممکن است ، از تکنیک های مشابه ، جهت گریز از فایروال ، استفاده شده باشد .

### یادداشت :

این تکنیکها ( منظور ، تکنیکهای گریز از فایروال است ) ، همگی از بخشهای هک سیستم هستند که به تفصیل ، در گزارش های فنی ( ۴ و ۵ ) ، تحت عنوان ( سیستم های هکینگ ) به شرح مفصل آن پرداخته شده است .

( Sam spade ) و بسیاری از ابزار هک کردن ، یک نسخه از ( Trace route ) را در خود دارند . سیستم عامل ویندوز نیز همچنین و با دستور [ tracert < host name > ] عمل ( Trace ) انجام می پذیرد. شکل ( ۵ ) ، بعنوان یک مثال ، نتیجه ی ( Trace route ) را برای آدرس [ www.yahoo.com ] نشان می دهد . در شکل ( ۵ ) به پیام هایی که در حال خروج از ( ISP ) یاهو است ، توجه نمائید ، که در نهایت آدرس ( IP ) سرور که ( ۶۸.۱۴۲.۲۲۶.۴۲ ) است را آشکار می سازد . دانستن این آدرس ، برای هکر اخلاق مدار ، حکم اعلام خطری را دارد که در پس انجام اسکن های عمیق و بیشتر ، بتواند ، نسبت به اقدامات پیش گیرانه ، سریعاً ، اهتمام ورزد .

```

C:\>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [68.142.226.42]
over a maximum of 30 hops:

  0  1 ms    1 ms    1 ms    192.168.1.1
  1  55 ms   32 ms   10 ms   192.168.1.1
  2  27 ms    9 ms    9 ms   192.168.1.1
  3  30 ms    9 ms    9 ms   mrfdsrj02gex070003.rd.dc.cox.net [68.100.0.149]
  4  22 ms   11 ms   11 ms   mrfdbbrj02-ge020.rd.dc.cox.net [68.1.1.6]
  5  12 ms   11 ms   12 ms   ashbbbrj01-pos020100.r2.as.cox.net [68.1.1.232]
  6  14 ms   11 ms   13 ms   68.105.30.98
  7  43 ms   12 ms   12 ms   vlan260-msr2.re1.yahoo.com [216.115.96.173]
  8  28 ms   11 ms   10 ms   t-2-1.bas2.re2.yahoo.com [206.190.33.93]
  9  28 ms   11 ms   11 ms   p11.www.re2.yahoo.com [68.142.226.42]

Trace complete.
```

شکل ( ۵ ) - ( Trace route ) برای آدرس www.yahoo.com

( Tracert ) ، مکان روترها ( مسیر یاب ها ) را در مسیر خود ، تا شبکه ی مقصد ، شناسائی می کند . چرا که عموماً ، روترها ، بر اساس مکان فیزیکشان نامگذاری می شوند و این مطلب به ( Tracert ) ، کمک می نماید تا هکر ، بتواند ، این وسایل را شناسائی کند .

#### ابزار هک کردن :

برنامه های ( Neotrace ) ، ( Visual Route ) و ( Visual Lookout ) ، همگی از وسایل ردیابی بسته ها [ Packet - tracking ] با یک ( GUI ) یا رابط گرافیکی کاربر ، به مفهوم ویژوال بشمار می روند . آنها مسیر جابجائی بسته ها را روی یک نقشه ، ترسیم می کنند و محل روترها و [ Internet Works ] را به شکل بصری ، قابل تشخیص می سازند . این وسایل ، همگی به طور یکسان ( Tracert ) را انجام داده و در جمع آوری اطلاعات بسان هم ، عمل می نمایند . به هر حال آنها یک نمایش بصری از آنچه جمع آوری می نمایند ، نشان می دهند .

#### ز ( درک عملکرد ( E-mail Tracking ) :

برنامه های ( E-mail Tracking ) به فرستنده یک ایمیل ، اجازه می دهد تا بداند که آیا ؛ گیرنده ی آن ایمیل ، آنرا خوانده ، آنرا برای کسانی دیگر ، ارسال نموده ، آنرا تغییر داده و یا آنرا حذف کرده است . بیشتر برنامه های ( E-mail Tracking ) به وسیله ی افزودن ( domain name ) به آدرس ایمیل ، عمل می نمایند ؛ بطور مثال [ readnotify.com ] . بدین مفهوم که فایل گرافیکی ، حاوی یک پیکسل گرافیکی که عموماً ، برای گیرنده ، غیر قابل توجه است ، به لیست الکترونیکی ، ضمیمه می شود . بنابراین ، وقتی که عمل ، روی یک ایمیل ، انجام می شود ، این فایل گرافیکی ، به سرورهای خصوصی ، متصل شده و عملکرد مربوطه را برای فرستنده آن ایمیل ، مخابره می نماید .

#### ابزار هک کردن :

( E-mail Tracking pro ) و ( MailTracking.com ) همگی ، ابزارهایی هستند که به هکرها ی اخلاق مدار ، اجازه می دهند تا به ردیابی و تعقیب ، پست های الکترونیکی ، بپردازند . بطوریکه ، پس از استفاده از این ابزار ، می تواند به اطلاعاتی دست یابند که عبارتند از :

۱ ( یک ایمیل ، چه موقع فرستاده می شود ؟

۲ ( آیا یک ایمیل ، ( forward ) شده است یا نه ؟

۳ ( آیا ایمیل مذکور ، تغییر یافته است یا خیر ؟

۴ ( و در نهایت نتیجه حاصل ردیابی و اینکه آیا مالک اصلی میل باکس به ایمیل باکس ، ( Log ) کرده است

۵ ( و ...

## ح) درک عملکرد ( web spider )ها یا دام گستران وب :

فرستنده های هرزنامه ( spammers ) و هر شخص دیگری که علاقمند به جمع آوری پست های الکترونیک از اینترنت باشد ، می تواند از روشهایی موسوم به دام گستری وب یا ( web spider ) استفاده نماید . یک دام گستر وب ، علاقمند است که اطلاعات بخصوصی را از قبیل پست الکترونیک و ... جمع آوری نماید ؛ بطوریکه از روشهای شناسائی علامت ( @ ) که در پست های الکترونیک مرسوم است بهره جسته و فهرستی از آنها را یافته و کپی برداری می نماید . گاهی ، این فهرست ، در یک پایگاه داده ، نهفته است که عمل جستجوی ( @ ) را از میان رکوردهای موجود ، آسانتر می نماید . بنابراین ، می توان نتیجه گرفت که دام گستران وب ، به هر نوع داده ای در اینترنت ، حتی اگر به حمله ، منجر نگردد ، علاقمندند . یک هکر بدخیم ، به راحتی می تواند ، عملکرد دام گستری وب را به حالت خودکار ، تبدیل نموده و به جمع آوری اتوماتیک اطلاعات ، بپردازد . روشی که برای پیشگیری از ( web spidering ) وب سایت شما توسط نگارنده پیشنهاد می شود ، اینست که یک فایل با عنوان [ robots.txt ] را در قسمت ( root ) وب سایت خود ، قرار دهید ، بطوریکه ، فهرستی از همه ی دایرکتوری هایی ( directories ) که می خواهید از آن محافظت به عمل آید ، در آن ذکر شده باشد .

## نتیجه گیری :

۱) از تحلیل یک سازمان ، در خصوص ساختار پست های شغلی – داخلی آن ، اطلاع حاصل نمائید .  
- هکر ها به راحتی ، می توانند با استفاده از جستجوهای چون ( google hacking ) و ... به اطلاعات حیاتی از قبیل فایروال ها و سیستم های کشف نفوذ ( IDS ) و انواع سرورها ، اطلاع یابند .

۲) از روشهای جستجوی اطلاعات در خصوص ، اخبار سازمانها ، در وبلاگها و گروههای خبری و ... آگاه باشید .  
- از همه ی منابع عمومی در دسترس ، جهت کشف اطلاعات در مورد شرکت هدف ، شبکه های داخلی ، همچنین اوضاع امنیتی سیستم هایش ، استفاده نمائید .

۳) درک نمائید که چگونه می توان درباره کارمندان یک سازمان ، به جمع آوری اطلاعات پرداخت .  
- از سایت ( yahoo ) و ( People Search ) و یا هر موتور جستجوی دیگر ، برای یافتن کارمندان یک سازمان ، به عنوان یک هدف ، استفاده نمائید .

۴) از روشهای ویژه ی کسب اطلاع ، بوسیله ی ( query DNS ) آگاه باشید .  
- بدانید که چگونه از ( DNS stuff ) ، ( nslookup ) و یا ( Sam spade ) بوسیله یک پرس و جو در میان رکوردهای سرورهای ( DNS ) ، به جمع آوری اطلاعاتی درباره ی ( host )ها و آدرسهای ( IP )شان ، استفاده بعمل می آید .

۵) از عملکرد ( Whois ) به جهت کسب اطلاعات اشخاص یا سازمان ها ، با خبر باشید .  
- بدانید که چگونه می توان از ( ARIN ) ، ( LACNIC ) ، ( RIPE NCC ) ، ( APNIC ) و ( Whois ) پایگاه های داده ی مکان های ثبت شده و داده های تماس های سازمان ها ، برای جمع آوری اطلاعات ، بهره جست .

۶) بدانید که چگونه می توان نامهای داخلی و خارجی ( Domain ) یک سازمان را پیدا نمود .  
- شما باید قادر باشید که بوسیله ابزاری چون ( Whois ) و ( sam spade ) ، اطلاعات مربوط به ( Domain ) یک سازمان را بیابید ؛ همچنین آگاهی از پایگاه داده ( ARIN ) و روشهای بهره جویی از آن نیز ، توصیه میشود .

۷) بدانید که چگونه می توان از زیر ساخت های فیزیکی شبکه و سرورهای وب یک سازمان ، آگاه باشید .  
- از ابزارهایی چون ( Neo trace ) ، ( Visual Route ) و یا ( Visual Lookout ) برای داشتن یک دید گرافیکی از مسیرهای داخلی یک شبکه ، استفاده نمائید . این ابزار ، مختصات فیزیکی سرورهای یک سازمان را به شما ، نشان می دهند .

۸) بدانید که چگونه می توان پست های الکترونیکی یک سازمان را مورد ردیابی یا تعقیب قرار داد .  
- شما باید قادر باشید که بوسیله برنامه های ( e-mail Tracking ) به ردیابی و تعقیب پست های الکترونیک سازمانهای هدف ، پرداخته و به جهت کسب اطلاعات بیشتر در خصوص نقاط آسیب پذیری از این دست ، تلاش نمائید .

## منابع :

بمنظور نگارش سلسله گزارشات فنی ، برای تبادل اطلاعات و اخذ مآخذ به روز امنیتی ، با موسسات ، محققان و سازمان های بسیاری مکاتبه شده است که جهت آشنایی و اطلاع محققان گرامی ، به ذکر نامشان اکتفا می گردد :

- **Frank Abagnale** – Abagnale and Associates  
Author of 'Catch Me if You Can', Lecturer, Consultant, National Cyber Security Alliance spokesman
- **Prof. Matt Bishop** – University of California Davis  
Computer Security Professor, Author of 'Computer Security: Art and Science'
- **LTC Dr. Andrew Glen** – United States Military Academy  
Associate Professor, Department of Mathematical Sciences
- **Dr. Simon Jackman** – Stanford University  
Political Science and Statistics Professor
- **Dr. Nimrod Kozlovski** – Yale University,  
Computer Science Department, Adjunct Professor of Law at New York Law School,  
Author of 'The Computer and the Legal Process'
- **Kevin Mitnick** – Mitnick Security Consulting  
Author, Public Speaker, Consultant, and Former Computer Hacker
- **Dr. Tom Piazza** – University of California Berkeley  
Senior Sampling Statistician, Survey Research Center
- **Dr. Sam Sander** – Clemson University  
Computer Engineering Professor
- **Dr. Eugene Spafford** – Purdue University  
Computer Security Professor, CISSP, ISSA Hall of Fame,  
security advisor to Presidents Bill Clinton and George W Bush
- **Paul Williams** – Gray Hat Research  
Chief Technology Officer, MCSE, NSA IAM and IEM
- **Ray Yepes** – Computer Security Consultant  
CISSP, MCSE, MCP, NSA IAM and IEM, Homeland Security level ۲, CCNP, CCSP

- تشکر ویژه اینجانب از عزیزانی که کمک هایشان ، روشنگر راهمان شد :

- سرکار خانم سپیده وحیدی
- سرکار خانم فهیمه جرجانی