



2

## الهاكر الأخلاقي

عملية الاستطلاع (RECONNAISSANCE)

# Kabbani Books

By

Dr.Mohammed Sobhy Teba

RECONNAISSANCE

<https://www.facebook.com/tibea2004>

## CONTENTS

31	Footprinting Concepts 2.1 مفهوم فوكت برتنت
31	<b>مقدمة</b>
31	Footprinting Terminology مصطلحات فوكت برتنت
31	Open Source or Passive Information Gathering (OSINT) استخراج معلومات من المصادر المفتوحة أو التحليل النشط
31	Active Information Gathering استخراج معلومات نشط
31	Anonymous Footprinting فوكت برتنت مجهولة الهوية
31	Pseudonymous Footprinting فوكت برتنت مجهولة الهوية
32	Organizational or Private Footprinting فوكت برتنت تجارية أو خاصة
32	Internet Footprinting فوكت برتنت على الشبكة
32	ما هو الفوكت برتنت؟ ما هو فوكت برتنت؟
32	لماذا؟ لماذا فوكت برتنت؟
33	الهدف من عملية الاستطلاع (Footprinting) الهدف من عملية الاستطلاع
33	2.2 التهديدات الناتجة من عمليات الاستطلاع .Footprinting threats
33	فيما يلي مختلف التهديدات التي تكون بسبب عملية الاستطلاع (Footprinting)
34	2.3 منهجة/نظيرية عمل عملية الاستطلاع Footprinting Methodology
35	Footprinting through search engines-1 عملية الاستطلاع باستخدام محركات البحث
35	ما هو محرك البحث؟
35	ما يكون محرك البحث؟
36	Finding Company's External and Internal URLs إيجاد عناوين URL للشركة خارجياً وداخلياً
37	الموقع العامة والمقيدة (Public and Restricted Websites)
38	جمع معلومات عن الموقع الجغرافي Collect Location Information
40	البحث عن الناس People search
43	جمع المعلومات باستخدام الخدمات المالية Gather Information from Financial Services
44	عمليات الاستطلاع باستخدام موقع البحث عن العمل Footprinting through job Sites
44	رصد الأهداف عن طريق التبيهات Monitoring Targets Using Alerts
45	2. Website Footprinting-2 عملية الاستطلاع عن الموقع الإلكترونية
48	(فحص إكواز صفحة html) Examine the HTML source code
49	Mirroring an Entire Website
55	Extract Website Information from استخراج معلومات عن الموقع من خلال موقع الارشيف



56	رصد تحديثات الويب باستخدام مراقب الموقع (Monitoring Web Updates Using Website Watcher)
56	3- عمليات الاستطلاع باستخدام البريد الإلكتروني (Email Footprinting)
56	تتبع اتصالات البريد الإلكتروني [Tracking Email Communications]
57	جمع المعلومات من خلال عنوانين البريد الإلكتروني (Collection from the Email Headers)
62	4- الاستخبارات التافسية (Competitive Intelligence)
62	جمع المعلومات الاستخباراتية (Competitive Intelligence Gathering)
63	الاستخبارات التافسية - متى بدأت هذه الشركة [When Did this Company Begin] ؟ وكيف تطورت؟
63	فيما يلي بعض من الواقع التي تكون مصدراً للمعلومات التي تساعد المستخدمين الحصول على معلومات استخباراتية تافسية.
64	الاستخبارات التافسية - ما هي خطط الشركة [What Are the Company's Plans] ؟
65	الاستخبارات التافسية معرفة آراء الخبراء حول شركة ما [What Expert Opinions Say About the Company] ؟
66	5- عملية الاستطلاع باستخدام جوجل (Footprinting using google)
66	عملية الاستطلاع باستخدام تقنية قرصنة جوجل Footprinting using Google Hacking Techniques
67	ماذا يمكن أن يفعل الهاكر مع استخدام قرصنة جوجل؟
67	عمليات البحث المتقدم لمتشقني جوجل Google Advance Search Operators
68	إيجاد الموارد باستخدام عمليات جوجل للبحث المتقدم Finding Resources using Google Advance Operator
69	ما هو البيزنت " Usenet "
70	قرصنة جوجل: قاعدة بيانات قرصنة جوجل (GHDB) (Google Hacking Database)
70	الأدوات الأخرى المستخدمة في قرصنة جوجل
73	6- عمليات الاستطلاع باستخدام WHOIS
73	WHOIS Lookup (WHOIS Lookup) WHOIS بحث
74	تحليل فنائج WHOIS Lookup (SmartWhois) :WHOIS Lookup أدوات
76	WHOIS Lookup Tools
77	Whois في نظام التشغيل لينكس (كالي/ياك تراك).
78	7- عملية الاستطلاع عن معلومات DNS (DNS Footprinting)
79	Extracting DNS Information
79	الأدوات المستخدمة في إرسال طلب استعلام عن سجلات DNS record كالاتي:
87	الأدوات المستخدمة في عملية الاستطلاع عن DNS في نظام التشغيل كالي/ياك تراك فقط
94	8- Network Footprinting
94	تحديد نطاق الشبكة (Locate Network Range)



95	في كاليفورنيا تراك لينكس
98	تحديد نظام التشغيل (Determining the operating system)
99	Traceroute
101	Traceroute tools
104	9. عملية الاستطلاع من خلال الهندسة الاجتماعية (Footprinting through Social Engineering)
104	(التنصت) Eavesdropping
104	Shoulder Surfing
104	Dumpster Diving
105	10. عمليات استطلاع من خلال شبكات التواصل الاجتماعي [Footprinting through Social Networking site]
105	عملية الاستطلاع باستخدام الهندسة الاجتماعية من خلال موقع التواصل الاجتماعي
105	المعلومات المتاحة على موقع التواصل الاجتماعي (Information available in the social networking site)
106	جمع المعلومات عن طريق الفاسبوك [Collection Facebook Information]
106	جمع المعلومات عن طريق التويتر [Collection Twitter Information]
107	جمع المعلومات عن طريق لينكدين [Collection LinkedIn Information] LinkedIn
107	جمع المعلومات عن طريق يوتيوب [Collection YouTube Information]
107	Tracking Users on Social Networking Sites ( تتبع المستخدمين على موقع التواصل الاجتماعي)
108	2.4 أدوات عملية الاستطلاع Footprinting Tools
108	Footprinting Tool: Maltego
108	في نظام التشغيل ويندوز.
109	في نظام التشغيل كاليفورنيا تراك
112	Footprinting Tool: Domain Name Analyzer Pro
112	Footprinting Tool: Web Data Extractor
114	Additional Footprinting Tools
114	2.5 (الحماية من عمليات الاستطلاع) Footprinting Countermeasures
115	Footprinting Penetration Testing
115	Footprinting Pen Testing
116	Footprinting Pen Testing Report Templates ( قالب/شكل تقارير عملية اختبار الاختراق).
117	other technique of Information Gathering with kali Linux
118	2.7 Company website
119	The Harvester: Discovering and Leveraging E-mail Addresses



120	.....MetaGoofil
121	.....Threat Agent: Attack of the Drones
123	.....Darknet· Invisible WEB· Hidden WEB·Deep WEB 2.8
124	.....محتوى Deep web كالاتي:
124	.....هادين النقطتين تشكلان فنction مستقلتين للDNS:
124	.....:Tor2web
125	.....نظرة عامة على شبكات الانترنت الموجودة في الخفاء (Deep web)
125	.....شبكة TOR
125	.....شبكة I2P
126	.....شبكة Freenet
126	.....Alternative Domain Roots
127	.....فيما يلي قائمه Alternative Domain Roots الفعالة:
127	.....ما سبب أنه مخفى أو لا يمكن لمحركات البحث أن تراه؟

**Kabbani Books**



## FOOTPRINTING CONCEPTS 2.1 (مفهوم فوت برينت)

### مقدمة

المصطلح **RECONNAISSANCE** بالتعريف يأتي من استراتيجية الحرب العسكرية لاستكشاف خارج المنطقة المحتلة من قبل القوات الصديقة للحصول على معلومات عن العدو للتحليل أو لهجوم مستقبلي. أما هنا في أنظمة الكمبيوتر فإنه متاباه لذلك، وهذا يعني عادة أن مختبر الاختراق "Penetration testing" أو الهاكر سوف يحاول معرفة أكبر قدر ممكن حول البيئة الهدف وصفات النظام قبل سن الهجوم. وتعرف أيضاً هذه العملية باسم **Footprinting**. عملية الاستطلاع هو عادة في الحقيقة غير ضروري وفي كثير من الحالات (ومن ذلك، نحن لسنا محامين، ولا يمكن تقديم المساعدة القانونية) لأنك تتعامل مع نظام غير مصرح لك به. أمثلة على عملية الاستطلاع تتضمن أي شيء من البحث على مصادر عامة عن الهدف مثل جوجل، ورصد نقاط الموظفين لمعرفة أنماط التشغيل، ومسح/فحص الشبكات أو الأنظمة لجمع المعلومات، مثل نوع التصنيع، ونظام التشغيل، ومنفذ الاتصال المفتوحة. لمزيد من المعلومات التي يمكن جمعها حول هدف يجلب فرصة أفضل لتحديد أسهل وأسرع الطرق لتحقيق هدف الاختراق، فضلاً عن أفضل طريقة لتجنب النظام الأمني القائم. أيضاً، تتباه الهدف من المرجح أن يسبب بعض السبل لغلق الهجوم كرد فعل على التحضير للهجوم. ومن الأقوال القهير: "كلما كنت أكثر هدوءاً، كلما كنت قادرًا على السمع".

ينبغي أن تسجل نتائج عمليات الاستطلاع في وثائق سرية، وذلك لأن البيانات الموجودة قد تكون ذات صلة في وقت لاحق في ممارسة الاختراق. أيضاً سوف يحتاجها العملاء وذلك لأنهم يريدون أن يعرفوا كيف تم الحصول على مثل هذه البيانات، ويطلبون المراجع لها. ومن الأمثلة على ذلك الأدوات التي تستخدم للحصول على البيانات أو مورد ما، على سبيل المثال، استعلام بحث معين في محرك البحث **Google** الذي تم تقديمها للحصول على البيانات. إعلام العميل "إذن حصلت على المعلومات" ليست جيدة بما فيه الكفاية، لأن الغرض من اختبار الاختراق هو تحديد نقاط الضعف للإصلاحات في المستقبل.

## FOOTPRINTING TERMINOLOGY (مصطلحات فوت برينت)

قبل الذهاب قدمًا إلى عمق هذا المفهوم وكيفية استخدامه، سوف نتعرف أولاً على بعض المصطلحات الأساسية المستخدمة في **Footprinting**. هذه المصطلحات تساعدك على فهم مفهوم **Footprinting** و هيكلتها.

### OPEN SOURCE OR PASSIVE INFORMATION GATHERING (OSINT)

هذه الطريقة تعبر من الطرق السهلة في جمع المعلومات عن الهدف. وهي تشير إلى عملية جمع المعلومات من المصادر المفتوحة أي من المصادر العامة المتاحة وهذه المعلومات تكون متاحة للجميع. هذا النوع لا يدعم الاتصال المباشر بالهدف وقانوني. المصادر المفتوحة المجانية للمعلومات تشمل الآتي: الجرائد والتلفزيون ومواقع التواصل الاجتماعي مثل فيسبوك و **blogs** والخريط وجوجل وغيرها.

باستخدام هذا النوع يمكنك تجميع المعلومات مثل نطاق التبعة (**network range**) وعناوين IP القابلة للوصول على الإنترنت ونظام التشغيل وتطبيقات خوادم الويب التي يتم استخدامها بواسطة التبعة الهدف وبروتوكولات النقل سواء **TCP** أو **UDP** وأدوات التحكم في الوصول وبنية النظام وأنظمة كشف التسلل وهكذا.

### ACTIVE INFORMATION GATHERING

في هذا النوع من جمع المعلومات فإن المهاجمين يقومون بالتركيز أساسياً على موظفي المنظمة الهدف. بحيث يحاولون انتزاع بعض المعلومات من هؤلاء الموظفين عن طريق استخدام الهندسة الاجتماعية. هنا يتم التعامل مباشرة مع المنظمة الهدف.

### ANONYMOUS FOOTPRINTING

هذا يتشير إلى عملية جمع المعلومات من مصادر مجهولة.

### PSEUDONYMOUS FOOTPRINTING

هذا يتشير إلى عملية جمع المعلومات من مصادر تم نشرها على شبكة الإنترنت ولكن غير مرتبطة مباشرة باسم الكاتب. حيث يمكن نشر المعلومات تحت اسم مختلف أو الكاتب قد يكون له اسم مستعار مشهور أو قد يكون الكاتب مسئول في أحدى الشركات أو الجهات الحكومية

ويحظر عليه النقر تحت اسمه الحقيقي أو الأصلي. ويسمى هذا النوع بغض النظر عن السبب في إخفاء الاسم الحقيقي وجمع المعلومات من هذه المصادر يسمى **pseudonymous**.

## ORGANIZATIONAL OR PRIVATE FOOTPRINTING

هذا النوع يتضمن جمع المعلومات من تقويم المنظمات على شبكة الإنترنت ومن خلال خدمات البريد الإلكتروني.

## INTERNET FOOTPRINTING

هذا يتضمن إلى عملية جمع المعلومات من المنظمة الهدف من خلال اتصال هذه المنظمة بشبكة الإنترنت.

### ما هو الفت برتق (FOOTPRINTING)؟

**F** هو أول مرحلة من مراحل القرصنة الأخلاقية، والتي تشير إلى عملية جمع المعلومات عن القibleة الهدف والبيئة المحيطة بها. باستخدام **Footprinting** يمكنك إيجاد طرق عده للتغافل على القibleة الهدف وهو يعتبر **methodological** أي له منهجه في العمل وذلك بسبب أن سنه للمعلومات الهامة كان على أساس المنهجيات السابقة. بمجرد أن تبدأ عملية **Footprinting** بطريقة منهجه، فإنك سوف تحصل على مخطط (**blueprint**) للأمن الشخصي للمنظمة المستهدفة. هنا يتم استخدام المصطلح 'blueprint' لأن النتيجة التي سوف تحصل عليها في نهاية **Footprinting** يشير إلى وضع النظام الفريد للمنظمة الهدف.

ليس هناك منهجة واحدة لـ **Footprinting** كما أنه يمكنك تتبع المعلومات بطرق عده. ومع ذلك، فإن هذا لا يقل أهمية عن احتراজاتك لجميع المعلومات الحاسمة التي يتبعها قبل أن تبدأ عملية القرصنة. وبالتالي، يجب أن تتقى **Footprinting** بدقة وبطريقة منظمة.

يمكنك جمع المعلومات عن المنظمة المستهدفة من خلال وسائل **Footprinting** في أربع خطوات:

1. جمع المعلومات الأساسية حول الهدف وشبكتها.
2. تحديد نظام التشغيل المستخدم، ومنتجات التشغيل، وإصدارات خادم الويب، الخ.
3. يودي بعض التقنيات مثل **Whois** و **DNS** و **network and organizational queries**.
4. البحث عن التغرات الأمنية واستخدامها في الهجوم.

علاوة على ذلك، سوف نناقش لاحقاً كيفية جمع المعلومات الأساسية، وتحديد نظام التشغيل من الكمبيوتر الهدف، منتجات التشغيل، وإصدارات خادم الويب، وأساليب مختلفة من **Footprinting** ، وكيفية إيجاد واستغلال نقاط الضعف بالتفاصيل.

### لماذا FOOTPRINTING ؟

**Footprinting** يتم استخدامها من قبل المهاجمين لبناء استراتيجية القرصنة، وال الحاجة إلى جمع المعلومات عن شبكة المنظمة الهدف، حتى يتمكوا من العثور على أسهل طريقة لاقتحام محيط أمن المنظمة. كما ذكر سابقاً، **Footprinting** هو أسهل طريقة لجمع المعلومات عن المنظمة المستهدفة، وهذا يلعب دوراً حيوياً في عملية القرصنة. **Footprinting** يساعد على الآتي:

- معرفة الوضع الأمني (**know security posture**)

أداء **Footprinting** على المنظمة الهدف بطريقة منتظمة ومنهجية يعطي صورة كاملة عن الوضع الأمني للمنظمة. بحيث يمكنك تحليل هذا التقرير لمعرفة التغرات في الوضع الأمني للمنظمة التي تستهدفها وعلى ذلك يمكنك بناء خطة الهجوم.

- الحد من منطقة الهجوم (**Reduce Attack Area**)

باستخدام مجموعة من الأدوات والتكتيكات، فإن المهاجمين يمكنهم استهداف كيان غير معروف (على سبيل المثال منظمة **XYZ**) وتقليل هذا الكيان إلى مجموعة محددة من أسماء الدومنين (**domain names**)، وكل الشبكة، وعناوين **IP** الفردية للأنظمة المرتبطة مباشرة إلى شبكة الإنترنت، وكذلك العديد من التفاصيل الأخرى المتعلقة بالموقف الأمني .

- بناء قاعدة معلومات (**Build Information Database**)

يوفر **Footprinting** أقصى قدر ممكن من المعلومات التفصيلية عن المنظمة المستهدفة . حيث يقوم المهاجمين ببناء قاعدة بيانات من المعلومات الخاصة ب نقاط الضعف في نظام الأمان في المنظمة المستهدفة. تم تحليل قاعدة البيانات هذه للعثور على أسهل طريقة لاقتحام نظام الأمان لهذه المنظمة.

## - رسم خريطة للشبكة (Draw Network Map)

الجمع بين تقنيات الـ **Footprinting** وبعض الأدوات مثل ترسرت (**Tracert**) يسمح للمهاجم إنشاء مخطط للشبكة مع وجود تبكة المنظمة الهدف. فان هذه الخريطة تمثل فهم لشبكة الإنترن特 الخاصة بالهدف بواسطة **Footprint**. ويمكن لهذه الرسومات التخطيطية للشبكة توجيه الهجوم.

**(FOOTPRINTING) الهدف من عملية الاستطلاع**

الأهداف الرئيسية لـ **Footprinting** تتمثل الآتي جمع المعلومات عن الشبكة الهدف (**target's network information**) ، ومعلومات عن أنظمة التسجيل (**system information**) ، ومعلومات عن المنظمة نفسها (**Organizational information**) . من خلال تنفيذ **Footprinting** في مستويات الشبكة المختلفة، يمكنك الحصول على معلومات مثل: كل الشبكة، خدمات الشبكة والتطبيقات، وبنية النظام، وأنظمة كشف التسلل، وعنوان **IP** المحدد، وأدلة مراقبة الدخول. مع معلومات **Footprinting**، مثل أسماء الموظفين، وأرقام الهاتف وعناوين الاتصال، والخبرة في العمل، وهلم جرا من المعلومات التي يمكنك الحصول عليها.

- جمع المعلومات عن الشبكة الهدف (target's network information)

يمكن جمع المعلومات عن الشبكة الهدف عن طريق إجراء تحليل لقاعدة البيانات بواسطة **trace routing** و **Whois**، الخ ويشمل الآتي:

- اسم الدومن - اسم الدومن الداخلي - بلوکات الشبکة - عناوين IP للأنظمه التي يمكن الوصول إليها -
    - **Rogue/private websites** - **Access control mechanisms** (ACLs) وبروتوكولات النقل سواء **TCP** و **UDP** التي تحمل - آلية التحكم في الوصول (Access control mechanisms)
  - بروتوكولات الشبکة - **VPN points** - جدار الحماية **IDSes** - أرقام التليفونات سواء **digital** أو **analog** - عمليات الولوج المشفرة (system enumeration) (authentication mechanism)
    - جمع معلومات عن أنظمة التشغيل (collect system information)

- **SNMP** - (**routing table**) - جداول روتنج (**user & group name**) - أسماء المستخدمين والمجموعات التي ينتمون لها.  
هيكلة/**نوع** النظام - نوع remote system - اسم النظام - كلمات السر - system banner (نظام الإنذارات).  
- **معلومات عن المنظمة نفسها** (**Organizational information**)

بيان وأرقام التأمينات - تفاصيل عن الموظفين - مكان الشركة - دليل الشرك

الموقع الرسمي للقركة - اتجاه القركة - تشهر المنظمة - التعليقات الموجودة في الملفات المصدرية في [HTML](#)

## 2.2 التهديدات الناجمة من عمليات الاستطلاع FOOTPRINTING THREATS

كما تم سرقة سابقاً، فإن المهاجم يُؤدي عملية الاستطلاع (**Footprinting**) خطوة أولى في محاولة لاختراق المنظمة الهدف. في مرحلة عملية الاستطلاع (**Footprinting**)، فإن المهاجمون يحاولون جمع المعلومات القصيرة على مستوى النظام مثل تفاصيل الحساب، ونظام التشغيل وإصدارات البرامج الأخرى وأسماء الخادم، وتتفاصل مخطط قاعدة البيانات التي من شأنها أن تكون مفيدة في مرحلة القرصنة.

فِيمَا يُلِي مُخْتَافَ التَّهَدِيدَاتِ الَّتِي تَكُونُ يَسِيرًا عَمَلِيَّةً لِلْاسْتِطِلاعِ (FOOTPRINTING).

الهندسة الاجتماعية Social engineering .1

بدون استخدام أية من أساليب التسلل، فإن المهاجمين يعملون على جمع المعلومات مباشرة وغير مباشرة من خلال الإقناع ومختلف الوسائل الأخرى. هنا، يتم جمع المعلومات الخامسة من قبل المتسلين من خلال الموظفين دون تماقز بينهم.

System and Network Attacks .2

عملية الاستطلاع (**Footprinting**) يساعد المهاجم لتنفيذ هجمات النظام والتسلل. من خلال **Footprinting**, يمكن المهاجمين جمع معلومات ذات صلة بالمنظمة الهدف كملفات إعداد النظام, نظام التشغيل الحالى على الجهاز, وهلم جرا. باستخدام هذه المعلومات, يمكن عنور المهاجمين على نقاط الضعف الموجودة في النظام الهدف ومن ثم استغلال هذه التغيرات الأمنية. وبالتالي, يمكن المهاجمين من السيطرة على النظام الهدف. وبالتالي, يمكن للمهاجمين أيضا السيطرة على التسلل بالكامل.

### 3. تسريب المعلومات Information leakage

تسريب المعلومات يمكن أن يشكل تهديداً كبيراً لأية منظمة وغالباً ما يتم تجاهله، بحيث إذا وقعت بعض من المعلومات الحساسة الخاصة بمنظمة ما في أيدي المهاجمين، تم يقوموا ببناء خطة الهجوم على أساس هذه المعلومات، أو استخدامه للحصول على مبالغ نقدية.

### 4. فقدان الخصوصية Privacy Loss

مع مساعدة من عملية الاستطلاع **Footprinting**، فإن المهاجمين يمكنهم الوصول إلى الأنظمة والشبكات للشركة وحتى التنصيع من امتيازات تصل إلى مستويات الإدارية (**Admin privilege**)، مما كانت الخصوصية التي تحتفظ بها الشركة فإنها فقدت تماماً.

### 5. تجسس الشركات corporate espionage

تجسس الشركات هي واحدة من التهديدات الرئيسية للشركات كمنافسين يمكنهم التجسس ومحاولة سرقة البيانات الحساسة من خلال **Footprinting**. بسبب هذا النوع من التجسس، فإن المنافسين قادرين على إطلاق منتجات مماثلة في السوق، مما يؤثر على الموقف السوقي للشركة.

### 6. الخسائر التجارية Business Loss

عملية الاستطلاع (**Footprinting**) له تأثير كبير على الشركات مثل شركات الإنترنت والمواقع الإلكترونية الأخرى، والأعمال المصرفيّة والشركات المالية ذات الصلة، وما إلى ذلك. المليارات من الدولارات يتم خسارتها كل عام بسبب الهجمات الصارمة من قبل قراصنة.

## 2.3 منهجية/نظريّة عمل عملية الاستطلاع FOOTPRINTING METHODOLOGY

منهجية **Footprinting** هي وسيلة إجرائية لجمع المعلومات عن المنظمة الهدف من جميع المصادر المتاحة، إنها تتعامل مع جمع المعلومات عن المنظمة المستهدفة، وتحديد **URL** والموقع وتفاصيل إنشاء، وعدد الموظفين، ومجموعة محددة من أسماء الدومن، ومعلومات الاتصال. يمكن جمع هذه المعلومات من مصادر مختلفة مثل محركات البحث وقواعد البيانات **Whois**، الخ. محركات البحث (**search engines**) هي مصادر المعلومات الرئيسية حيث يمكنك العثور على معلومات قيمة عن المنظمة التي تستهدفها، لذا، أولاً سوف نناقش **Footprinting** عن طريق محركات البحث. هنا نحن ذاهبون لمناقشة كيف وماذا يمكننا فعله من جمع المعلومات من خلال محركات البحث فيما يلي العمليات التي يمكن القيام بها لجمع المعلومات والتي سوف نتحدث عنها في هذا الجزء.



## FOOTPRINTING THROUGH SEARCH ENGINES-1 عملية الاستطلاع باستخدام محركات البحث

تم تصميم محركات البحث (**search engine**) على شبكة الإنترنت للبحث عن المعلومات على شبكة الويب العالمية. يتم عرض نتائج البحث بشكل عام في خط من النتائج ويشار إليها بصفحات نتائج محرك البحث (**Search Engine Result Pages SERPs**). في العالم الحاضر، العديد من محركات البحث تسمح لك بانتزاع المعلومات عن المنظمة الهدف مثل منصات التكنولوجيا وتفاصيل الموظفين، صفحات تسجيل الدخول، وهكذا. باستخدام هذه المعلومات، فإن المهاجم يقوم ببناء استراتيجية القرصنة لاقتحام شبكة المنظمة المستهدفة ومن الممكن تنفيذ أنواع أخرى من هجمات النظام المتقدمة. محرك البحث جوجل يمكنه أن يكتف لك عن تقارير من قبل أفراد الأمان التي تكشف العلامات التجارية لجدران الحماية (**firewall**) أو برامج مكافحة الفيروسات المستخدمة في المنظمات الهدف. في بعض الأحيان يوفر لك مخططات الشبكة التي يمكن عن طريقها توجيه الهجوم.

### ما هو محرك البحث؟

محرك البحث (الباحث) هو برنامج حاسوبي مصمم للمساعدة في العثور على مستندات مخزنة على شبكات المعلومات (شبكة الانترنت) أو على حاسوب شخصي. بنى محركات البحث الأولى اعتماداً على التقنيات المستعملة في إدارة المكتبات الكلاسيكية. حيث يتم بناء فهارس للمستندات تشكل قاعدة للبيانات تقييد في البحث عن أي معلومة. يسمح محرك البحث للمستخدم أن يطلب المحتوى الذي يقابل معايير محددة (والقاعدة فيها تلك التي تحتوي على كلمة أو عبارة ما) ويستدعي قائمةً بالمراجع توافق تلك المعايير. تستخدم محركات البحث مؤشرات/فهارس/مساردة متقطعة التحديث لتنشغل بسرعة وفعالية.

تعرض النتائج على شكل قائمة بعناوين المستندات التي توافق الطلب. يرتفع بالعناوين في الغالب مختصر عن المستند المhtar إليه أو مقتطف منه للدالة على موافقته للبحث. عناصر قائمة البحث ترتب على حسب معايير خاصة (قد تختلف من محرك لأخر) من أهمها مدى موافقة كل عنصر للطلب.

عند الحديث عن محركات البحث فغالباً ما يقصد محركات البحث على شبكة الانترنت ومحركات الويب بالخصوص. محركات البحث في الويب تبحث عن المعلومات على الشبكة العنكبوتية العالمية، ومنها يستعمل على نطاق ضيق يتضمن البحث داخل الشبكات المحلية للمؤسسات أي إنترانet. أما محركات البحث الشخصية فتبحث في الحواسيب الشخصية الفردية.

بعض محركات البحث أيضاً تحفر في البيانات المتاحة على المجموعات الإخبارية، وقواعد البيانات الضخمة، أو أدلة موقع الويب. تشنغل محركات البحث عن طريق الخوارزميات، على عكس أدلة الموقع، والتي يقوم عليها محررون يسر.

### ما يتكون محرك البحث؟

نجد ان محرك البحث يتكون من ثلاثة أشياء اساسية كالتالي:

- **برنامجه العنكبوت (crawler/spider/robot)**:

تُستخدم محركات البحث برنامجه العنكبوت (**spider**) لإيجاد صفحات جديدة على الويب بالإضافة، ويسمى هذا البرنامج أيضاً الزاحف (**crawler**) لأنّه يتحرّك في الإنترنّت بهدوء لزيارة صفحات الويب والاطلاع على محتوياتها، ويأخذ هذا البرنامج مؤشرات المواقع من عنوان الصفحة (**title**) ، والكلمات المفتاحية (**keywords**) التي تحوّلها، إضافة إلى محتويات موحدات الميتا (**Meta tags**) فيها. ولا تقتصر زيارة برنامجه العنكبوت على الصفحة الأولى للموقع بل يتتابع البرنامج تَعَّقب الروابط (**links**) الموجودة فيها لزيارة صفحات أخرى. أما الغاية من هذه الزيارات فهي وضع النصوص المنتقاة في نظام الفهارس لمحرك البحث، ليتمكن المحرك من العودة إليها فيما بعد، ولم تغ فكرة تغيير المحتوى في الموقع عن بال مصممي محرك البحث، إذ ينظم محرك البحث زيارات ذيوريّة للمواقع الموجودة في الفهارس للتأكد من التعديلات التي تصيب الموقع المفهرسة.

- **برنامجه المفهرس**

يُمثل برنامجه المفهرس (**index program**) ، الكatalog أحياناً، قاعدة بيانات ضخمة تُوصيّف صفحات الويب، وتعتمد في هذا التوصيف على المعلومات التي حصلت عليها من برنامجه العنكبوت (**spider**) كما تعتمد على بعض المعايير مثل الكلمات الأكثر تكراراً من غيرها، وتختلف محركات البحث عن بعضها في هذه المعايير، إضافة إلى اختلافها في خوارزميات المطابقة (**ranking algorithms**) .

- **برنامجه محرك البحث**

يبدأ دور برنامجه محرك البحث عند كتابة كلمة مفتاحية (**keyword**) في مربع البحث (**search box**)؛ إذ يأخذ هذا البرنامج الكلمة المفتاحية ويعمل عن صفحات الويب التي تحقق الاستعلام الذي كونه برنامجه المفهرس في قاعدة بيانات الفهارس (**index database**)، ثم تُعرض نتيجة البحث المتمثلة بصفحات الويب التي طلبها المستخدم في نافذة المستعرض (**browser window**) .

مثال على محركات البحث ما يلي:

[www.google.com](http://www.google.com) – [www.yahoo.com](http://www.yahoo.com) – [www.bing.com](http://www.bing.com)

الموقع التالي يحتوي على قائمه بجميع محركات البحث كالتالي:

[http://en.wikipedia.org/wiki/List\\_of\\_search\\_engines](http://en.wikipedia.org/wiki/List_of_search_engines)

إذا كنت تريد أن تقوم بعملية استطلاع (Footprint) عن المنظمة المستهدفة، على سبيل المثال (XYZ pvt ltd)، فقم بكتابة هذا (XYZ pvt ltd) في مربع البحث في محرك البحث تم اضغط على [Enter](#). فهذا سوف يعرض جميع نتائج البحث التي تحتوي على الكلمات الرئيسية (XYZ pvt ltd). يمكنك أيضا تصبيط النتائج بإضافة كلمة محددة أثناء البحث. وعلاوة على ذلك، سوف تناقش تقنيات [Email Footprinting](#) و [Website Footprinting](#) أخرى مثل [Footprinting](#).

على سبيل المثال، بالنظر في المنظمات، وربما مايكروسوفت. قم بكتابة Microsoft في مربع البحث لمحرك البحث واضغط على [Enter](#)، فإن هذا سيتم عرض جميع النتائج التي تحتوي على معلومات حول مايكروسوفت. تصفح النتائج قد يوفر معلومات حاسمة مثل الموقع الجغرافي، عناوين الاتصال، والخدمات المقدمة، وعدد الموظفين، وهكذا. والتي قد تكون مصدرا قيما لبناء استراتيجية الهجوم.

The screenshot shows a Microsoft search result page on Wikipedia. The left sidebar includes the Wikipedia logo, main page, contents, featured content, current events, random article, donate to Wikipedia, and various interaction and tools links. The main content area displays the Microsoft article, which describes it as an American multinational corporation headquartered in Redmond, Washington, developing, manufacturing, licensing, supporting, and selling computer software, consumer electronics, and personal computers and services. It lists its best-known products like Windows, Office, Xbox, and Surface. The sidebar on the right provides company details: Microsoft Corporation, founded by Bill Gates and Paul Allen in 1975, traded on Nasdaq and NYSE, and headquartered in Albuquerque, New Mexico. It also features a photo of the company's headquarters building.

باعتبارك هاكر أخلاقي، إذا وجدت أي من المعلومات الحساسة للشركة الخاصة بك في صفحات نتائج البحث، فإنه يجب عليك إزالة تلك المعلومات. وعلى الرغم من إنك قمت بإزالة هذه المعلومات الحساسة، فإنها قد تكون لا تزال متاحة في ذاكرة التخزين المؤقت لمحرك البحث. لذلك، يجب عليك أيضا التحقق من ذاكرة التخزين المؤقت الخاصة بمحرك البحث للتأكد من أنه تم إزالة البيانات الحساسة بشكل دائم.

## FINDING COMPANY'S EXTERNAL AND INTERNAL URLs

عناوين URL للشركة خارجيا وداخليا توفر الكثير من المعلومات المقيدة إلى المهاجم. هذه العناوين تصف الشركة وتقدم تفاصيل عنها مثل مهمة الشركة ورؤيتها الشركة، وتاريخ ومنتجات الشركة أو الخدمات التي تقدمها، وما إلى ذلك.

عناوين URL التي يتم استخدامها خارج شبكة الشركة للوصول إلى خادم الشركة عبر جدار الحماية تسمى عنوان URL الخارجي (External URL). هذه العناوين تعمل على الرابط المباشر إلى صفحة الويب الخارجية للشركة. يمكنك تحديد URL الخارجي للشركة المستهدفة مع مساعدة من محركات البحث مثل غوغل أو بنسج (google or Bing).

إذا كنت ترغب في العثور على عناوين URL الخارجية للشركة، اتبع الخطوات التالية:

1. افتح أي من محركات البحث، مثل غوغل أو بنسج.
2. اكتب اسم الشركة المستهدفة في مربع البحث واضغط على [Enter](#).

يتم استخدام عناوين URL الداخلية للوصول إلى خادم الشركة مباشرة داخل شبكة الشركات. عنوان URL الداخلي يساعد على الوصول إلى الوظائف الداخلية للشركة. معظم الشركات تستخدم أشكال متعددة لعناوين الموقع الداخلية. لذا، إذا كنت تعرف عنوان URL الخارجي



للشركة، فإنه يمكنك التنبؤ بعنوان URL الداخلي من خلال التجربة والخطأ. توفر هذه العناوين الداخلية نظرة تافية عن مختلف الإدارات ووحدات الأعمال في المؤسسة. يمكنك أيضاً العثور على عناوين الموقع الداخلية للمنظمة الهدف باستخدام أدوات مثل NetCraft.

### أدوات البحث عن عناوين الموقع الداخلية كالتالي:

#### - NetCraft

المصدر: <http://news.netcraft.com>

تتيكرافت يتعامل مع خادم الويب، موقع استضافة تحليل حصة السوق، والكشف عن نظام التشغيل. ويتوفر شريط أدوات مجاني لمكافحة الاحتيال (Net craft toolbar) لفايرفوكس وكذلك متصفحات الإنترنت إكسيلورر. شريط أدوات تتيكرافت يتتجنب هجمات لتصيد المعلومات، ويحمي مستخدمي الإنترنت من المحتالين. فإنه يتحقق من معدل المخاطر وأيضاً من موقع استضافة الموقع التي تزورها.

#### - Link Extractor

المصدر: <http://www.webmaster-a.com/link-extractor-internal.php>

Link Extractor هي أداة استخراج الروابط (links) التي تسمح لك أن تختار بين عناوين URL الداخلية والخارجية، تم تعود لك بقائمة من العناوين المرتبطة في صورة URL أو قائمة HTML. يمكنك استخدام هذه الأداة المساعدة في المواقع المنافسة. مثال على ذلك موقع URL الداخلية لميكروسوف特 كالتالي:

-  support.microsoft.com
-  office.microsoft.com
-  search.microsoft.com
-  msdn.microsoft.com
-  update.microsoft.com
-  technet.microsoft.com
-  windows.microsoft.com

### (PUBLIC AND RESTRICTED WEBSITES) المواقع العامة والمقيدة

الموقع العام (Public website) هو موقع مصمم لإظهار وجود المنظمة على شبكة الإنترنت. أنها مصممة لجذب العملاء والشركاء. أنها تحتوي على معلومات مثل تاريخ الشركة والخدمات والمنتجات، ومعلومات الاتصال للمنظمة.

الصورة التالية هي مثال على موقع على شبكة الإنترنت العامة:

المصدر: <http://www.microsoft.com>



الموقع المقيد (**restricted website**) هو موقع على شبكة الإنترنت التي توفر لعدد قليل من الناس. هؤلاء الناس قد يكونوا العاملين في المؤسسة، أو أعضاء قسم ما، وهكذا. القيد (**restriction**) يمكن تطبيقها على أساس رقم IP، الدومن أو الشبكة الفرعية (**subnet**، واسم المستخدم، وكلمة المرور).

الموقع الخاصة أو المقيدة لميكروسوفت تشمل الآتي:

<http://technet.microsoft.com> - <http://windows.microsoft.com> - <http://office.microsoft.com>

<http://answers.microsoft.com>



## 搜集地理信息

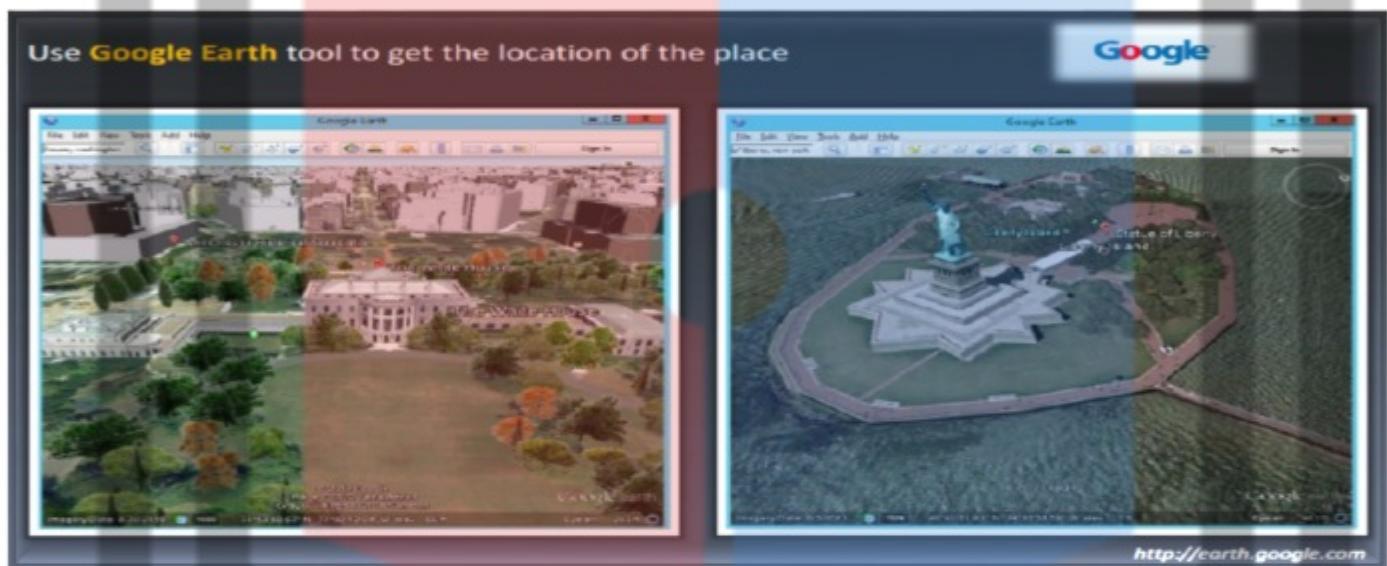
معلومات مثل الموقع الجغرافي للمنظمة تلعب دوراً حيوياً في عملية القرصنة. ويمكن الحصول على هذه المعلومات باستخدام تقنية **Footprinting**. بالإضافة إلى الموقع الجغرافي، فإنه يمكننا أيضاً جمع المعلومات مثل شبكة الواي فاي المحيطة (**Wi-Fi hotspots**) التي قد تكون وسيلة لاختراق شبكة المنظمة الهدف.

المهاجمين مع العلم بموقع المنظمة الهدف قد يحاولون التفتيش في قاعدة هذه المنظمة، والمراقبة، الهندسة الاجتماعية، والهجمات غير الفنية الأخرى لجمع المزيد من المعلومات عن المنظمة المستهدفة. وبمجرد معرفة موقع الهدف، فإن صور الأقمار الصناعية المفصلة

للموقع يمكن الحصول عليها باستخدام مصادر مختلفة متاحة على شبكة الإنترنت مثل <http://www.google.com/earth> و <https://maps.google.com>. حيث يمكن استخدام هذه المعلومات من قبل القراءة للوصول الغير مصرح به إلى المباني والشبكات السلكية واللاسلكية، والنظم، وهلم جرا.

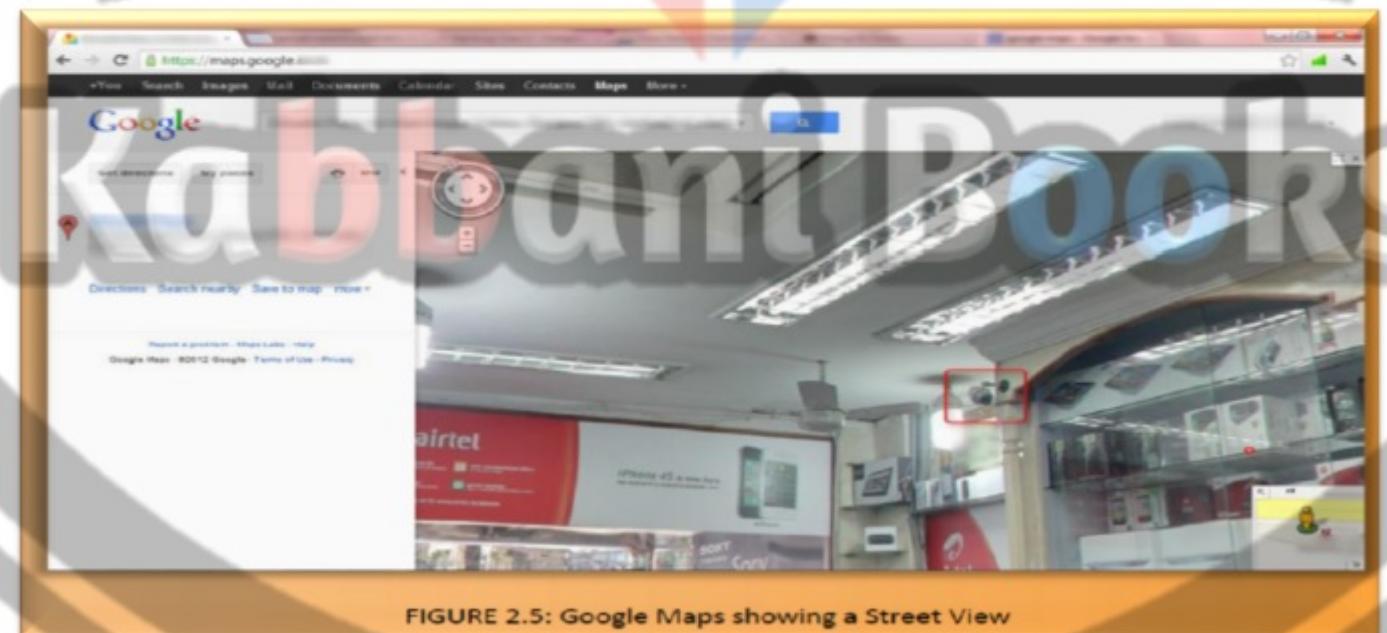
#### **earth.google.com**

جوجل ايرث هو أداة قيمة للتراصنة التي تسمح لك بإيجاد المكان، والإشارة إليه، والتكيير في هذا الموقع لاستكشاف. يمكنك حتى الوصول إلى صور **3D** التي تصور معظم الأرض بتفاصيل عالية الجودة.



#### **maps.google.com**

يتوفر خرائط جوجل ميزة عرض **(View)** التسuar التي توفر لك مجموعة من الصور عن المبني، وكذلك المناطق المحيطة بها، بما في ذلك شبكات الواي فاي. يستخدم المهاجمون خرائط **Google** للتحور على أو تحديد مداخل المبني، الكاميرات الأمنية، البوابات، أماكن الاختباء، نقاط الضعف في الأسوار المحيطة، الموارد ذات الفائدة مثل الاتصالات الكهربائية، لقياس المسافة بين الأهداف المختلفة، وهكذا.



## البحث عن الناس PEOPLE SEARCH

يمكنك استخدام موقع السجل العام للعثور على معلومات حول عناوين البريد الإلكتروني للأشخاص وأرقام الهاتف وعنوان المنازل، وغيرها من المعلومات. باستخدام هذه المعلومات يمكنك المحاولة للحصول على التفاصيل المصرفية وتفاصيل بطاقة الائتمان، وأرقام الهاتف النقالة، والتاريخ الماضي، وما إلى ذلك. هناك العديد من خدمات البحث عن الأشخاص المتاحة في الإنترنت التي تساعدك في إيجاد الناس. <http://www.spokeo.com> و <http://pipl.com> أمثلة على خدمات البحث عن الأشخاص التي تسمح لك بالبحث عن الأشخاص باستخدام الاسم، والبريد الإلكتروني، واسم المستخدم، والهاتف، أو عنوان.

خدمات البحث عن الأشخاص قد توفر لك بعض المعلومات مثل الآتي:

1. عنوان السكن وعنوان البريد الإلكتروني.
2. أرقام الاتصال وتاريخ الميلاد.
3. صور والملف الخاص به في الشبكات الاجتماعية.
4. عناوين المدونة الخاصة به (Blog URLs).
5. صور الأقمار الصناعية من المساكن الخاصة.



FIGURE 2.6: Examples of People search online service websites

### خدمات البحث عن الأشخاص أونلاين People Search Online Services

في الوقت الحاضر، العديد من مستخدمي الإنترنت يستخدمون محركات البحث عن الأشخاص للعثور عن معلومات عن آخرين. غالباً ما تقوم محركات البحث عن الأشخاص بتوفير أسماء الناس، والعناوين، وتفاصيل الاتصال، وتفاصيل الشخصية. بعض محركات البحث عن الأشخاص تكشف أيضاً عن نوع عمل الفرد، والشركات المملوكة من قبل الشخص، وأرقام الاتصال، وعناوين البريد الإلكتروني للشركة، وأرقام الهاتف النقال وأرقام الفاكس، وتاريخ الميلاد، وعناوين البريد الإلكتروني الشخصية، الخ. هذه المعلومات تبرهن على أن تكون مفيدة للغاية للمهاجمين لشن الهجمات.

#### • بعض من محركات البحث عن الأشخاص كالاتي:

**ZABA®SEARCH**

المصدر: <http://www.zabasearch.com>

**Zaba Search** هو محرك بحث عن الأشخاص الذي توفر المعلومات مثل العنوان ورقم الهاتف والموقع الحالي، وما إلى ذلك من الناس في الولايات المتحدة. فإنه يسمح لك للبحث عن الناس باستخدام أسمائهم.





المصدر: <http://www.zoominfo.com>

**ZoomInfo** هو دليل استخدام رجال الأعمال والتي يمكنك أن تجد الاتصالات التجارية ، وملامح الناس المهنية ، والسير الذاتية ، وتاريخها المهني ، والانتصارات ، ووصلات لملفات الموظف مع معلومات الاتصال التحقق ، وأكثر من ذلك.



المصدر: <http://wink.com>

**Wink People Search** هو محرك بحث عن الأشخاص التي توفر معلومات عن الأشخاص بالاسم والموقع. أنه يعطي رقم الهاتف والعنوان، والموقع، والصور، العمل، المدرسة، الخ.



المصدر: <http://www.anywho.com>

**Any who** هو موقع يساعدك في العثور على معلومات عن الأشخاص والشركات الخاصة بهم ، و مواقعها على الإنترنت. مع مساعدة من رقم الهاتف، يمكنك الحصول على جميع التفاصيل للفرد.



المصدر: <https://www.peoplelookup.com>

**People Lookup** هو محرك بحث عن الأشخاص التي تسمح لك بالعثور على الأشخاص، و مواقعهم، ومن تم التواصل معهم. كما أنه يسمح لك بالبحث عن رقم هاتف، البحث عن أرقام الهواتف المحمولة، العثور على عنوان أو رقم الهاتف، البحث عن الأشخاص في الولايات المتحدة. يستخدم قاعدة بيانات هذه المعلومات من السجلات العامة.



المصدر: <http://www.123people.com>

**123 People Search** هي أداة بحث عن الأشخاص التي تسمح لك بالعثور على المعلومات مثل السجلات العامة ، وأرقام الهاتف والعنوان و الصور، والفيديو ، و عناوين البريد الإلكتروني.



المصدر: <http://www.peekyou.com>

**PeekYou** هو محرك بحث عن الأشخاص التي تسمح لك بالبحث عن ملامح ومعلومات عن الأشخاص في الهند وبعض المدن الكبرى المكتظة بالموظفين والمدارس. فإنه يسمح لك للبحث عن الأشخاص بأسمائهم أو أسماء المستخدمين.



المصدر: <http://www.intelius.com>

**Intelius** هو ملفات سجلات عامة التي تقدم خدمة المعلومات. فإنه يسمح لك بالبحث عن الأشخاص في الولايات المتحدة عن طريق الاسم والعنوان والهاتف، أو البريد الإلكتروني.



المصدر: <http://www.peoplesmart.com>

**PeopleSmart** عبارة عن خدمة بحث عن الأشخاص. تسمح لك بالعثور على المعلومات عن الأشخاص مع اسمائهم، المدينة، الدولة. بالإضافة إلى ذلك، فإنه يسمح لك لتنفيذ عمليات البحث العكسى للهاتف، بحث البريد الإلكتروني، البحث عن طريق العنوان، والبحث الإقليمي.



المصدر: <http://www.whitepages.com>

**WhitePages** هو محرك بحث عن الأشخاص. يعمل على تزويدك بكثير من المعلومات عن الأشخاص عن طريق أسمائهم وأماكنهم. باستخدام أرقام telephones يمكنك إيجاد عنوان الشخص.

### عملية البحث عن الأشخاص في الشبكات الاجتماعية

البحث عن الأشخاص على موقع الشبكات الاجتماعية يتميز بالسهولة واليسر. خدمات الشبكات الاجتماعية هي خدمات أونلاين، أو منصات، أو موقع تركز على تسهيل بناء الشبكات الاجتماعية أو العلاقات الاجتماعية بين الناس. توفر هذه المواقع المعلومات التي يتم توفيرها من قبل المستخدمين. هنا الناس سواء بصورة مباشرة أو غير مباشرة مرتبطين مع بعضهم البعض عن طريق الاهتمام المشترك، أو نفس مكان العمل، أو المجتمع التعليمية، الخ

موقع الشبكات الاجتماعية تسمح للناس لتبادل المعلومات بسرعة وفعالية كما يتم تحديث هذه المواقع في الوقت الحقيقي. لأنها تتيح استكمال الحقائق حول الأحداث القائمة أو الحالية، والإعلانات والدعوات، وهكذا. وبالتالي، فإن موقع الشبكات الاجتماعية يغير منصة كبيرة للبحث عن الأشخاص والمعلومات المتعلقة بهم. من خلال البحث عن الأشخاص على خدمات الشبكات الاجتماعية، فإنه يمكنك جمع المعلومات الهامة التي من شأنها أن تكون مفيدة في أداء الهندسة الاجتماعية أو أنواع أخرى من الهمجات.

العديد من مواقع الشبكات الاجتماعية تسمح للزوار للبحث عن أشخاص من دون تسجيل، وهذا يجعل البحث عن الأشخاص على موقع الشبكات الاجتماعية مهمة سهلة بالنسبة لك. يمكنك البحث باستخدام اسم الشخص، والبريد الإلكتروني، أو العنوان. بعض المواقع تسمح لك للتحقق ما إذا كان الحساب هو حالياً قيد الاستخدام أم لا. هذا يسمح لك للتحقق من حالة الشخص الذي تبحث عنه.

**فيما يلى قائمه بأهم موقع الشبكة الاجتماعية كالتالي:**

#### Facebook



المصدر: <https://www.facebook.com>

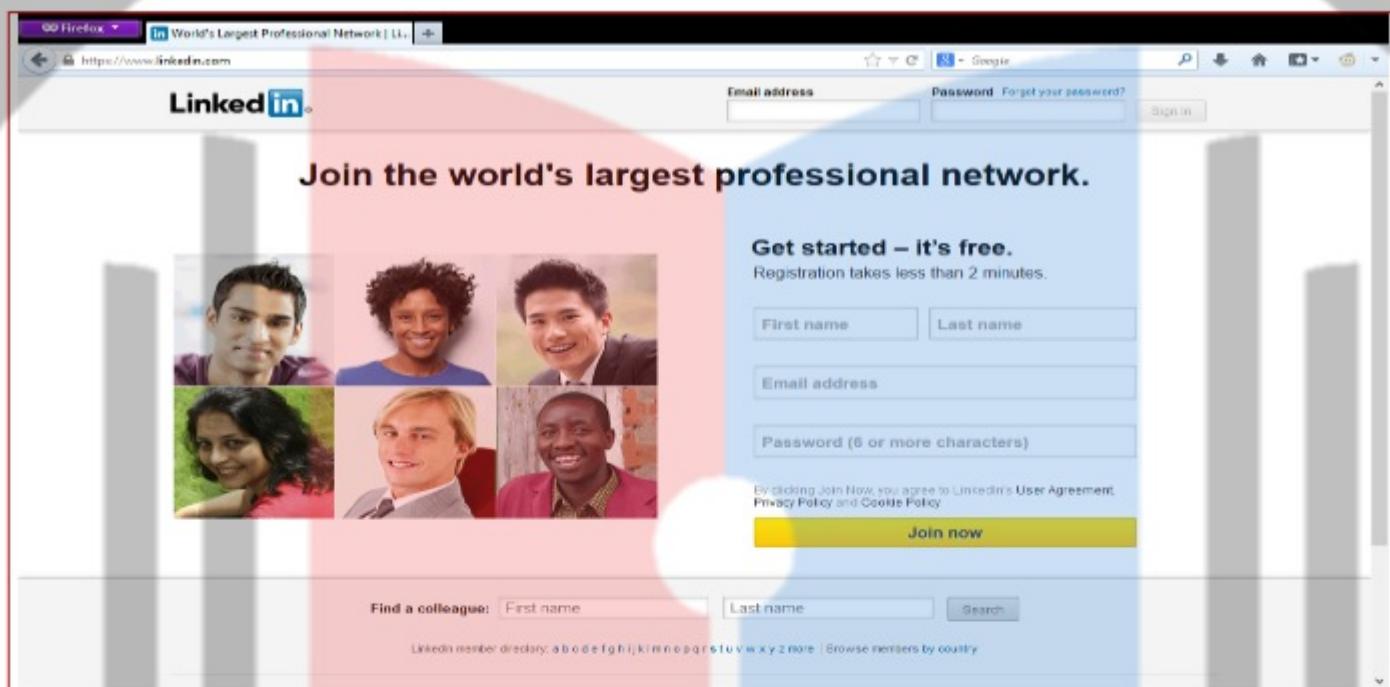
الفاسبوك يسمح لك بالبحث عن الأشخاص، وأصدقائهم، وزملائهم والأشخاص الذين يعيشون حولهم والآخرين الذين كانوا ينتمون لهم. بالإضافة إلى ذلك يمكن أيضاً إيجاد المعلومات الشخصية عن الشخص الهدف مثل الشركة التي يعمل بها وماذا يعمل والمكان الذي يعيش فيه حالياً وأرقام telephones والبريد الإلكتروني وبعض الصور الشخصية وبعض الفيديوهات وهكذا. الفاسبوك يمكنك من البحث عن الأشخاص باستخدام أسمائهم أو البريد الإلكتروني الذي يخصهم.

#### LinkedIn



المصدر: <https://www.linkedin.com>

هو عيارة عن موقع للتواصل الاجتماعي للأشخاص المحترفين حيث يسمح لك بإيجاد الأشخاص عن طريق الاسم، بعض الكلمات، الشركة التي يعمل بها، اسم المدرسة وهكذا. البحث عن الأشخاص في LinkedIn يعطيك الكثير من المعلومات مثل الاسم، التعيين، اسم الشركة التي يعمل بها، موقع الشخص الحالي، والدرجة التعليمية ولكن لكي تستخدم LinkedIn يجب أن تكون مسجلًا فيه.



### Twitter

[المصدر:](https://twitter.com)

هو عبارة عن شبكة اجتماعية التي تسمح بإرسال رسائل نصية للقراءة وتسمى تويت tweets. حتى الأشخاص غير مسجلين يمكنهم قراءة هذه الرسائل.

### Google+

[المصدر:](https://plus.google.com)

هو موقع تواصل اجتماعي يهدف إلى جعل عملية المشاركة على الموقع يشبه كثيراً المشاركة في الحياة الحقيقة. من خلال هذا الموقع يمكن جمع المعلومات المهمة عن المستخدمين واستخدام هذه المعلومات لقرصنة على أنظمة تسخيلهم.

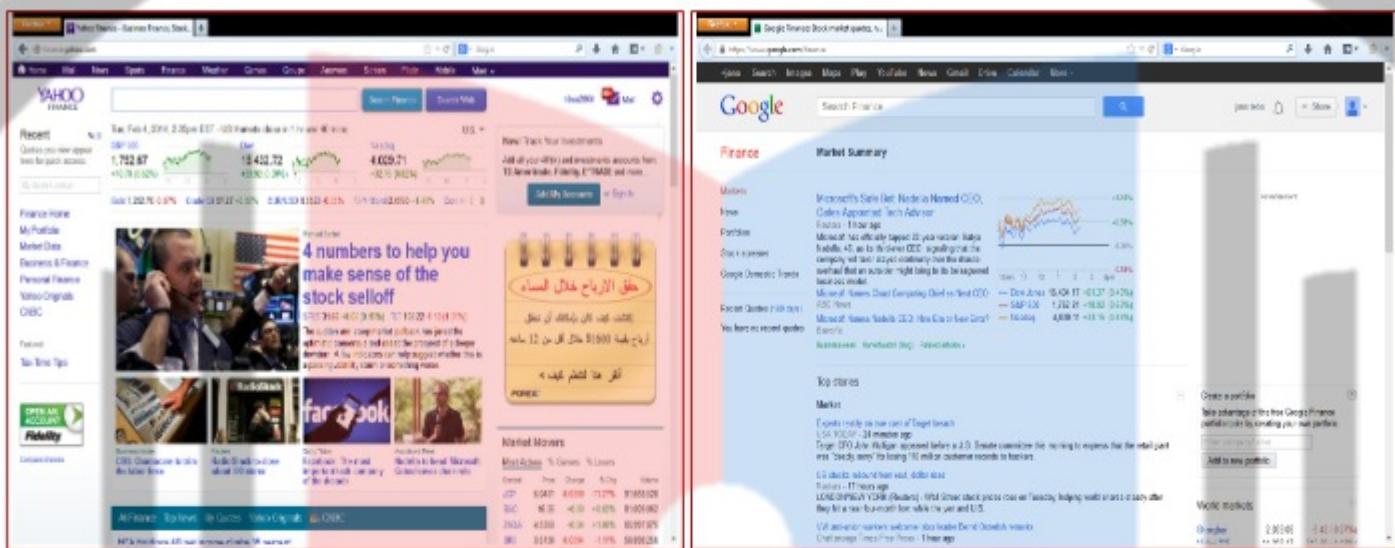
## GATHER INFORMATION FROM FINANCIAL SERVICES

الخدمات المالية (Financial services) مثل **Yahoo! Finance**، **Google Finance**، والذى توفر الكثير من المعلومات المقيدة مثل القيمة السوقية لأسهم الشركة، نبذة عن الشركة وبعض التفاصيل الأخرى عن المنافسين، وهكذا. هذه المعلومات تختلف من سيرفر إلى آخر. من أجل الاستفادة من هذه الخدمات مثل تطبيقات البريد الإلكتروني وتطبيقات الهاتف، فإن المستخدمون يحتاجون للتسجيل في الخدمات المالية. وهذا يعطي قرصنة للمهاجمين لانتزاع معلومات مفيدة لعملية القرصنة.

العديد من الشركات المالية تعتمد على الوصول إلى شبكة الإنترنت، وأداء المعاملات، ووصول المستخدمين إلى حساباتهم. القرصنة يمكنهم الحصول على معلومات حساسة وخاصة من المستخدمين عن طريق سرقة المعلومات، **key loggers**، وهكذا. المهاجمون أيضاً يمكنهم الاستيلاء على هذه المعلومات من خلال تنفيذ جرائم الإنترنت، واستغلال ذلك من خلال المساعدة من قبل التهديدات الغير ضعيفة (تصميم برمجيات على سبيل المثال؛ تعمل على كسر آلية المصادقة).

و فيما يلي بعض من التهديدات الغير ضعيفة (non-vulnerable threats)

- قيضات الخدمة (Service flooding)
- هجوم القوة الخامسة (Brute force attack)
- الخداع (Phishing)



## عمليات الاستطلاع باستخدام موقع البحث عن العمل

المهاجمين يمكنهم جمع المعلومات القيمة مثل نظام التشغيل، إصدارات البرامج وتفاصيل البنية التحتية للشركة، ومخطط قاعدة البيانات للمنظمة، وذلك من خلال **Footprinting** لموقع العمل المختلفة باستخدام تقنيات مختلفة. تبعاً لمتطلبات التقرير لفرص العمل، فإن المهاجمين يكونوا قادرين على دراسة الأجهزة والمعلومات المتعلقة بالشبكة، والتقنيات المستخدمة من قبل الشركة. معظم موقع الشركة لديها قائمة من الموظفين الرئيسيين مع عنوان بريد إلكتروني. هذه المعلومات قد تكون مفيدة للمهاجمين. على سبيل المثال، إذا كانت الشركة تزيد استئجار شخص لوظيفة إدارة الشبكة، فإنه تعلم على نشر متطلبات العمل المتعلقة بوظيفة إدارة الشبكات.

باستخدام موقع البحث عن عمل (**Footprinting through job sites**) فإن المهاجمين يمكنهم الحصول على المعلومات الآتية:

- متطلبات العمل – ملفات الموظفين – معلومات عن الأجهزة لديهم – معلومات عن التطبيقات لديهم.

فيما يلي قائمة بمواقع العمل المشهورة:

<http://www.monster.com>

<http://www.careerbuilder.com>

<http://www.dice.com>

<http://www.simplyhired.com>

<http://www.indeed.com>

<http://www.usajobs.gov>

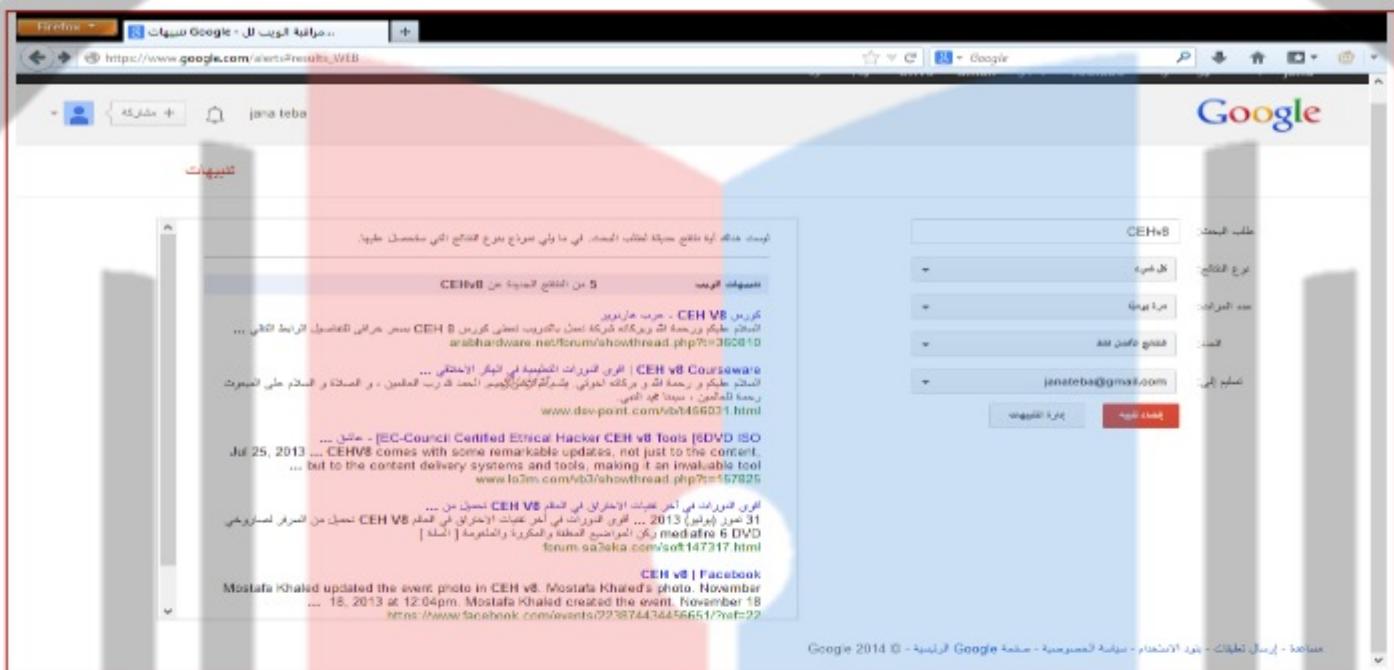
## رصد الأهداف عن طريق التبيهات

ال**التبيهات** هي محظى خدمات الرصد الآلي (**Monitoring services**) والتي تقدم معلومات محدثة إلى تاريخ اليوم على أساس التقديم الخاص بك، عادة يتم عرض المعلومات عن طريق البريد الإلكتروني أو الرسائل القصيرة. من أجل الحصول على هذه التبيهات، فإنك تحتاج إلى التسجيل في الموقع، ولكي تقوم بالتسجيل فإنك أيضاً تحتاج إلى تسجيل البريد الإلكتروني أو رقم الهاتف الخاص بك في الخدمة. هنا يأتي دور الفراغنة حيث يمكنهم جمع هذه المعلومات الحساسة من خدمات التبيه واستخدامها لمزيد من عمليات الهجوم.

### Google Alerts

المصدر: <https://www.google.com/alerts>

تبيهات جوجل هي محظى خدمة المراقبة الذي يقوم بطريقة تلقائيه بإعلام المستخدمين عن موضوع معين حسب اختيار المستخدم وذلك عند وجود محتوى جديد من الأخبار، أو على شبكة الإنترنت، أو المدونات (**Blogs**)، والفيديو، وأو مواضيع للمناقشة من قبل مجموعة تقابل الموضوع الذي يبحث عنه المستخدم ويتم تخزينها بواسطة خدمة تبيهات جوجل.



بعض مواقع التبيهات الأخرى كالتالي:

(<http://alerts.yahoo.com>) Yahoo! Alerts-1

(<http://www.gigaalert.com>) Giga Alert-2

## WEBSITE FOOTPRINTING-2 عملية الاستطلاع عن الموقع الإلكترونية

فيما سبق قمنا بشرح أول خطوه في منهجه عملية الاستطلاع (**Footprinting methodology**) من خلال محركات البحث. أما الأن سوف نقوم بشرح عملية الاستطلاع عن الموقع الإلكتروني.

من الممكن أن يقوم المهاجمين ببناء خريطة تفصيلية لبنية وعممارية الموقع الإلكتروني بدون تشغيل **IDS** أو بدون إثارة أي شكوك من قبل مسؤولي الأنظمة(**admin**). ويمكن تحقيق ذلك إما بمساعدة أدوات متطرفة لـ **Footprinting** أو مع الأدوات الأساسية التي تأتي جنبا إلى جنب مع نظام التشغيل، مثل **browser** و **telnet**. باستخدام أداة **Nmap** يمكنك جمع معلومات عن الموقع مثل عنوان **IP** ، الاسم المسجل وعنوان مالك الدومن، اسم الدومن، المضيف المرتبطين بالموقع (**host of the site**) وتفاصيل نظام التشغيل، وغيرها من المعلومات. ولكن هذه الأداة قد لا تطيق كل هذه التفاصيل عن كل الموقع. في مثل هذه الحالات، يجب تصفح الموقع المستهدف.

تصفح الموقع المستهدف سوف يوفر لك المعلومات التالية:

- 1) البرمجيات المستخدمة وإصدارها: حيث يمكنك أن تجد ليس فقط البرنامج المستخدم ولكن أيضاً إصدار النسخة بسهولة على الموقع المستندة إلى البرامج الجاهزة.
- 2) نظام التشغيل المستخدمة: عادة نظام التشغيل يمكن تحديده.
- 3) المجلدات الفرعية والمعاملات (**sub-directories and parameters**): حيث يمكنك أن تكتشف المجلدات الفرعية والمعاملات عن طريق جعل ملاحظة على كافة عنوانين الموقع URLs أثناء تصفح الموقع المستهدف.
- 4) اسم الملف، المسار، أسماء الحقول في قاعدة البيانات، أو استعلام: يجب تحليل أي شيء يكتبه اسم الملف، المسار، أسماء الحقول في قاعدة البيانات بعد الاستعلام أو الاستعلام بعثة للتحقق ما إذا كان يوفر فرصة للحقن **SQL injection**.
- 5) منصة الأسكريبت: مع مساعدة من اسم امتداد ملف الأسكريبت مثل (.php), (.asp), (.jsp), الخ. فإنه يمكنك بسهولة تحديد منصة الأسكريبت الذي يستخدمه الموقع المستهدف.
- 6) بيانات الاتصال وتفاصيل **CMS**: عادة ما تقدم صفحات تفاصيل الاتصال بعض المعلومات مثل أسماء وأرقام الهاتف وعنوان البريد الإلكتروني، وموقع المشرف أو مدعي الناس. يمكنك استخدام هذه التفاصيل لتنفيذ هجوم الهندسة الاجتماعية.

**برنامجه(CMS):** يسمح لعنوان **URL** من إعادة كتابتها من أجل إخفاء أسماء امتدادات ملفات الأسكريبت. في هذه الحالة، تحتاج إلىبذل المزيد من الجهد القليل لتحديد منصة ملف الأسكريبت.

يمكن استخدام كل من (Zaproxy، Owasp، Firebug، Brup Suite، Paros Proxy، etc) لعرض العناوين التي تزودك بالمعلومات التالية:

حالة الاتصال ونوع الاتصال (**connection status and connection-type**)

المناطق المقبولة (**Accept-ranges**)

المعلومات الأخيرة المحدثة (**Last-Modified information**)

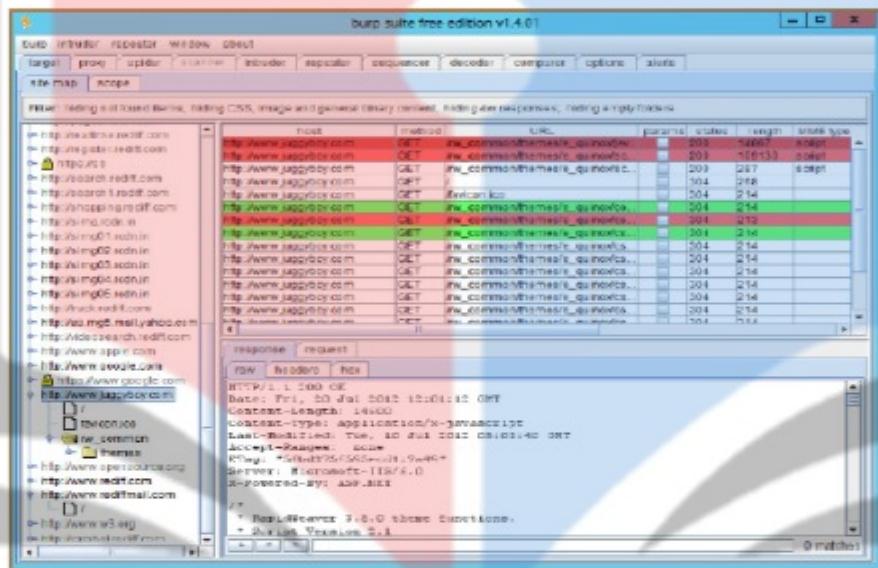
**X-Powered-By information**

خوادم الويب المستخدمة وإصداراتها (**Web server in use and its version**)

### Burp suite

المصدر: <http://portswigger.net>

ملحوظه هذا التطبيق يحتاج إلى منصة الجافا لكي يعمل ويتم إعداده لكي يعمل بالتناوب مع المتصفح الخاص بك ولرؤيه طريقة إعداده مع المتصفح الخاص بك فيمكن زيارة موقع هذا التطبيق والذي يوضح طريقة إعداده مع المتصفح وكيفية عمله وفيما يلي screenshot كالاتي:



### Firebug

المصدر: <http://getfirebug.com/>

تحمل هذه الأداة مع متصفح الويب **فایرفوکس** تدعيمه بمجموعة من أدوات التطوير والتي تمكنه من CSS monitor و editing و debug و HTML و JavaScript الموجودة في أي صفحة ويب.

ملحوظه: هذا التطبيق يعمل على جميع أنظمة التشغيل لأنه يعتمد في عمله على متصفح الويب فقط وليس نظام التشغيل.

كما تعلمون جميعاً، إن البريد الإلكتروني هو واحد من أهم الأدوات التي تم إنشاؤها. ولكن لسوء الحظ قد يساء استخدامه من قبل المهاجمين عن طريق إرسال رسائل البريد المزعجة (**spam emails**) وذلك للتواصل سراً وإخفاء أنفسهم وراء هذه الرسائل المزعجة (**spam**)، أثناء محاولته لتقويض بعض التعاملات التجارية. في مثل هذه الحالات، يصبح من الضروري للمهندس المسؤول عن اختبار معدلات الأمان تتبع البريد الكتروني للعثور على مصدر البريد الإلكتروني وخاصة الذي استخدم في ارتكاب عملية القرصنة باستخدام البريد الإلكتروني. وهذا ما سوف نتطرق إليه لاحقاً والذي قد يساعد أيضاً في كيفية العثور على الموقع (**location**) عن طريق تتبع البريد الكتروني باستخدام **MailTrackerPro** والذي يمكنه أيضاً توفير بعض المعلومات مثل المدينة والولاية والدولة، وما إلى ذلك. غالبية المسؤولين عن اختبار الاختراق يستخدموا متصفح موزيلا فایرفوکس كمسحورض ويب لأنشطتهم. هنا سوف نتعلم استخدام **Firebug** لاختبار اختراق تطبيقات الويب وجمع معلومات كاملة.

1- أولاً نعمل على تحميل هذه الأداة وذلك بفتح متصفح الويب فایرفوکس وذلك لأن هذه الأداة لا تعمل إلا مع هذا المتصفح فقط تم تقوم بالذهاب إلى الموقع التالي [<https://getfirebug.com>] كالاتي:



The most popular and powerful web development tool

- Inspect HTML and modify style and layout in real-time
- Use the most advanced JavaScript debugger available for any browser
- Accurately analyze network usage and performance
- Extend Firebug and add features to make Firebug even more powerful
- Get the information you need to get it done with Firebug.

[More Features...](#)

Transfering data from [getfirebug.com...](http://getfirebug.com)

**What is Firebug?** Introduction and Features    **Documentation** FAQ and Wiki    **Community** Discussion forums and lots    **Get Involved** Hack the code, create extensions

**Install Firebug** for Firefox, IE8+, Fire and open source  
Source Firebug Lite Extensions

**Introduction to Firebug** firebug.oceanconservancy.org/kb Campbell gives a quick introduction to Firebug. Watch now...

[More Screencasts...](#)

- 2- تم اختيار **Install Firebug** والذي يعمل على توجيهك الى صفحة الويب الذي من خلاله سوق تختار الإصدار الذي يناسبك لتنزيله كالتالي:

**Download Firebug**

**Firebug for Firefox**

**Firebug 1.12.6 for Firefox 27: Recommended**

Compatible with: Firefox 23-29  
[Download](#), [Release Notes](#), [New Features](#)

**Firebug 1.11.4**  
Compatible with: Firefox 17-22  
[Download](#), [Release Notes](#), [New Features](#)

**Firebug 1.10.6**

- 3- بمجرد الضغط على الإصدار الذي تريد تحميله يبدأ على توجيهه الى صفحة **download add-on** الخاصة بفایرفاکس والذي من خلالها نضغط على **install now** تم تثبيت التطبيق **Add to Firefox** حتى يتم تثبيت التطبيق كالتالي:

**ADD-ONS** EXTENSIONS | THEMES | COLLECTIONS | MORE...

Welcome to Firefox Add-ons. Choose from thousands of extra features and styles to make Firefox your own.

**Firebug** 1.12.6 NO RESTORE by Joe Hewitt, Jan Odvarko, robecc, FirebugWorkingGroup

Firebug integrates with Firefox to put a wealth of development tools at your fingertips while you browse. You can edit, debug, and monitor CSS, HTML, and JavaScript live in any web page...

[+ Add to Firefox](#)

5 ★★★★★ 1,611 user reviews, 2,064,005 users all

[Add to collection](#) [Share this Add-on](#)



4- بعد الانتهاء من التثبيت نلاحظ وجود الأيقونة الخاصة بالـ **Firebug** في الجانب الأيمن من شريط الأدوات باللون الرمادي كالاتي:



5- نقوم بالضغط عليها للتحول إلى اللون الأصفر حتى يظهر شريط الأدوات الخاص بها كالتالي:

6- نجد أن شريط الأدوات يحتوي على العديد من الأدوات مثل **Console** و **CSS** و **html** و **script** و **Net** وغيرها.

7- هنا سوف نذهب إلى موقع مايكروسوفت [http://www.microsoft.com/ar-EG/default.aspx] وتنطيل **Firebug** عليه.

8- **Console panel** يقدم لك سطر الأوامر الخاص بالجافا سكريبت، يسرد كافة أنواع الرسائل ويقدم التعريف لأوامر جافا سكريبت.

9- **HTML panel** تقدم لك صفحة **HTML/XML** الذي تم إنشاؤه من الصفحة المفتوحة حالياً. وهو يختلف عن طريقة العرض التقليدي للـ **source code** لأنها تعرض أيضاً جميع المعالجات على شجرة **DOM**. على الجانب الأيمن فإنه يعرف أنماط

المحددة حالياً والأساليب المحسوبة لذلك، ومعلومات التخطيط ومتغيرات **DOM** المسندة إليه انظر إلى التكمل السائق أو بمعنى آخر أن هذه **panel** تقدم لك بعض المعلومات مثل اكواد الائتمان (**source code**) والعنوانين الداخلية (**internal URLs**) وغيرها من المعلومات.

10- الغرض الرئيسي من هذه هو مراقبة حركة المرور لا **HTTP** التي بدأتها صفحة ويب على شبكة الإنترنت. ببساطة هي ت تقديم جميع المعلومات التي تم جمعها وتجميعها للمستخدم. ويكون محتواه من قائمة إدخالات حيث يمثل كل إدخال واحد من الآتي **request** و **round trip respond** و **cookies** يسمح بعرض ومعالجة ملفات **cookies** التي وضعتها الصفحة الحالية.

يمكن الاطلاع على تفاصيل أكثر وجميع الأوامر المستخدمة لهذه الأداة عن طريق الاطلاع على الصفحة التالية:

<https://getfirebug.com/wiki/index.php/>

ملحوظه هذه الأداة تم تطويرها الان لتسخدم مع مستعرضي الويب الآخرين مثل جوجل كروم وغيره.

## (HTML) EXAMINE THE HTML SOURCE CODE (فحص اكواد صفحة HTML)

عن طريق متابعة التعليقات (**comments**) التي يتم إنشاؤها إما عن طريق نظام **CMS** أو إدراجها يدوياً. قد توفر هذه التعليقات القرائن لمساعدتك على فهم ما يحمل في الخلية. حتى هذا قد يوفر تفاصيل الاتصال الخاصة بمشرف شبكة الإنترنت (**web admin**) أو المطور (**developer**). مراقبة جميع الروابط (**links**) وعلامات الصورة (**image tags**) ، من أجل تعين بنية نظام الملفات. هذا يسمح لك بالاكتشاف عن المجلدات والملفات المخفية. إدخال بيانات وهمية لتحديد الكيفية التي يحمل البرنامج النصي (**script**).

فحص ملفات الكوكيز (**cookies**) التي تم وضعها بواسطة الملقن/الخادم (**server**) لتحديد البرنامج التي تم تضليلها وسلوكها. يمكنك أيضا تحديد البرنامج النصي (**script**) في المنتصات من خلال مراقبة الدورات (**sessions**) وغيرها من ملفات الكوكيز.



## MIRRORING AN ENTIRE WEBSITE

**مرآءة الموقع (Website Mirror):** هو عملية إنشاء نسخة طبق الأصل من الموقع الأصلي. ويمكن أن يتم ذلك مع مساعدة من مجموعة من الأدوات. هذه الأدوات تسمح لك بتحميل موقع على شبكة الإنترنت إلى المجلد المحلي الخاص بك، وبناء كافة المجلدات، صفحات HTML، الصور، الفلاشات، ملفات الفيديو وغيرها من الملفات من الخادم/الملقم إلى جهاز الكمبيوتر الخاص بك.

هذه العملية (Website Mirror) يحتوي على العديد من الفوائد كالتالي:

- (1) من المقيد تصفح الموقع في الوضع اوفلاين (**offline**).
  - (2) يساعد في إنشاء موقع احتياطي نسخة أصلية من الموقع الأصلي.
  - (3) يمكن عمل استنساخ للموقع ما (**website clone**).
  - (4) مفید في اختبار موقع ما في الوقت الذي يتم فيه تصميم وتطوير الموقع.
  - (5) من الممكن توزيعها على خوادم/ملفات متعددة بدلاً من استخدام في ملقم واحد فقط.



FIGURE 2.17: JuggyBoy's Original and Mirrored website

## (الأدوات المستخدمة في استنساخ المواقع) Website Mirroring Tools

### HTTrack Web Site Copier

[المصدر:](http://www.httrack.com)

هو أداة لنسخ موقع ويب من على شبكة الانترنت هذه الأداة تسهل على مختبرى الاختراق عمله حيث تعطيه الفرصة لإلقاء نظره على المحتوى الكامل لهذا الموقع وجميع صفحاته وملفاته وفي بيئه أخرى تسسيطر عليها بنفسك. هذه الأداة تتبع لك تحميل موقع ويب كامل من على الإنترنت إلى مجلد محلي، وبناء كافة المجلدات، والحصول على صفحات **HTML** والصور وغيرها من الملفات من الخادم إلى جهاز الكمبيوتر الخاص بك. **HTTrack** يرتب هيكل روابط الموقع الأصلي (**Site's relative link structure**). افتح صفحة من الموقع الذي قمت بتحميله **website mirror** على المتصفح الخاص بك، وتتصفح الموقع من رابط إلى رابط، ويمكنك عرض الموقع كما لو كنت موجود على الإنترنت. **HTTrack** يمكنه أيضاً تحديث الموقع الذي قمت بتحميله حالياً، وأيضاً استئناف انقطاع التحميل.

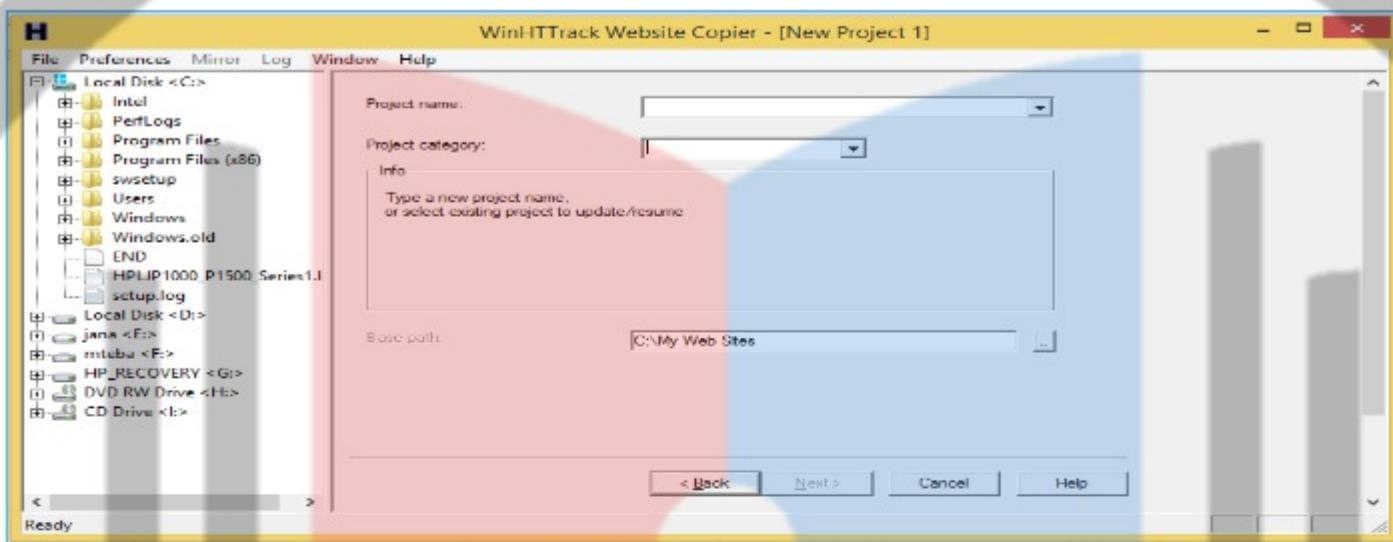
هذا سوف تتعلم نسخ موقع كامل من على شبكة الانترنت باستخدام أداة النسخ **HTTrack** والتي تمكنت منع هجوم **D-DOS**.

#### - في نظام التشغيل ويندوز

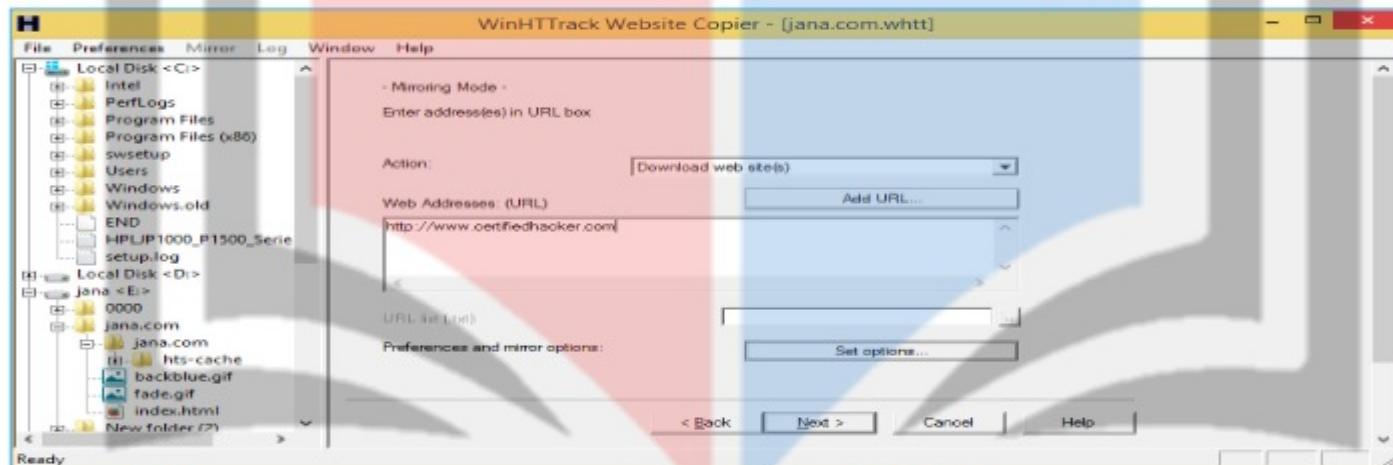
- 1- تعمل على تحميل هذه الأداة ثم تقوم بتثبيتها عن طريق اتباع **wizard** الخاص به
- 2- تقوم بتشغيل البرنامج من خلال الأيقونة الخاصة به
- 3- بعد الضغط عليه تظهر الشاشة التالية:



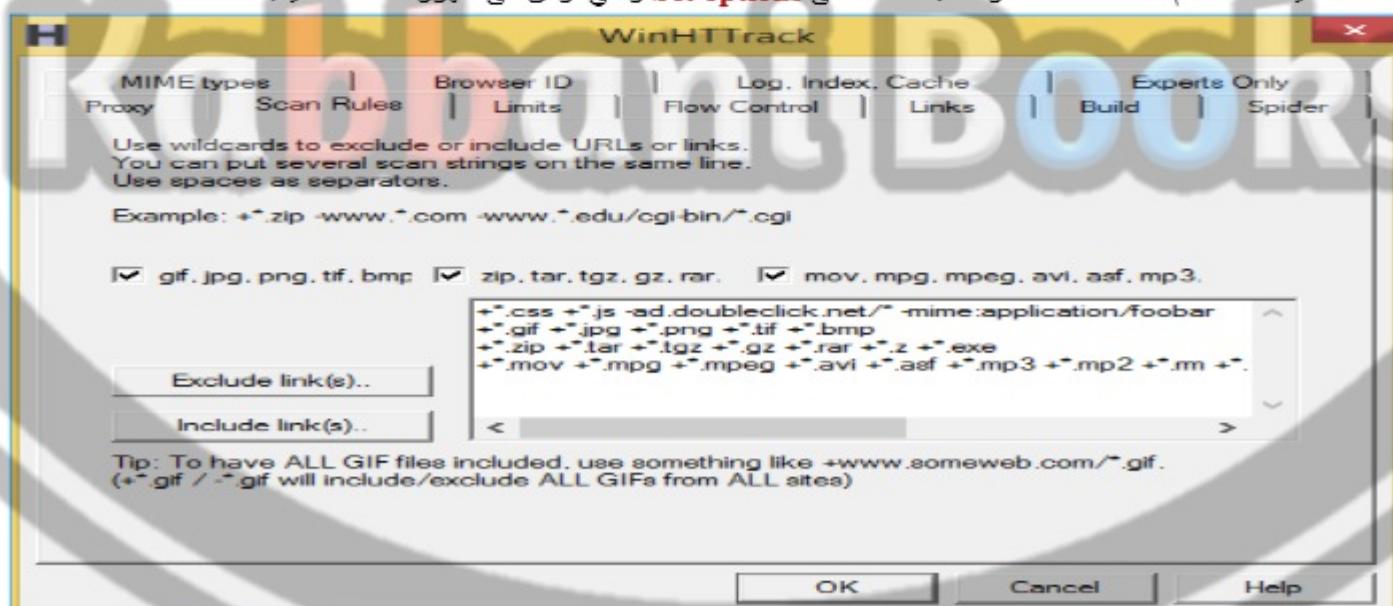
- 4- تقوم بالضغط على **next** لإنشاء مشروع جديد **new project** تم تحديد اسم هذا المشروع.



5- ندخل اسم المشروع في الخانة **Project name** وفي الخانة **Base path** نعمل على تحديد المكان الذي سوف يتم فيه تخزين الملفات. تم نضغط **next** فتظهر الشاشة التالية:

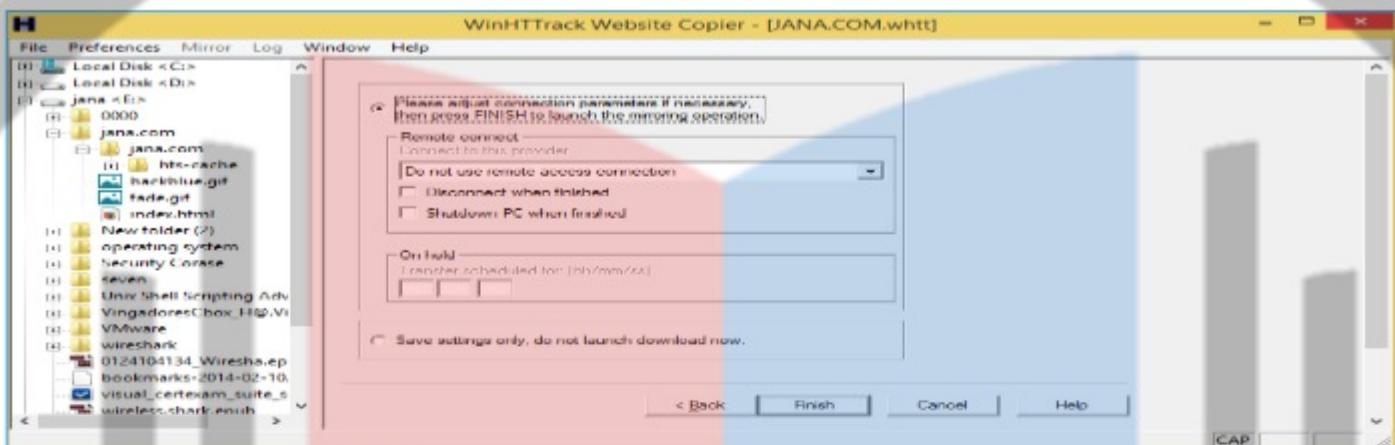


6- ندخل ايم الموقع باستخدام الزر **Add URL** ويمكن أيضا تحديد طبيعة موقع الويب المراد تحميله عن طريق **Action** ويمكن أيضا استخدام اعدادات متقدمة وذلك بالضغط على **Set options** والتي تؤدي الى ظهور الشاشة التالية:

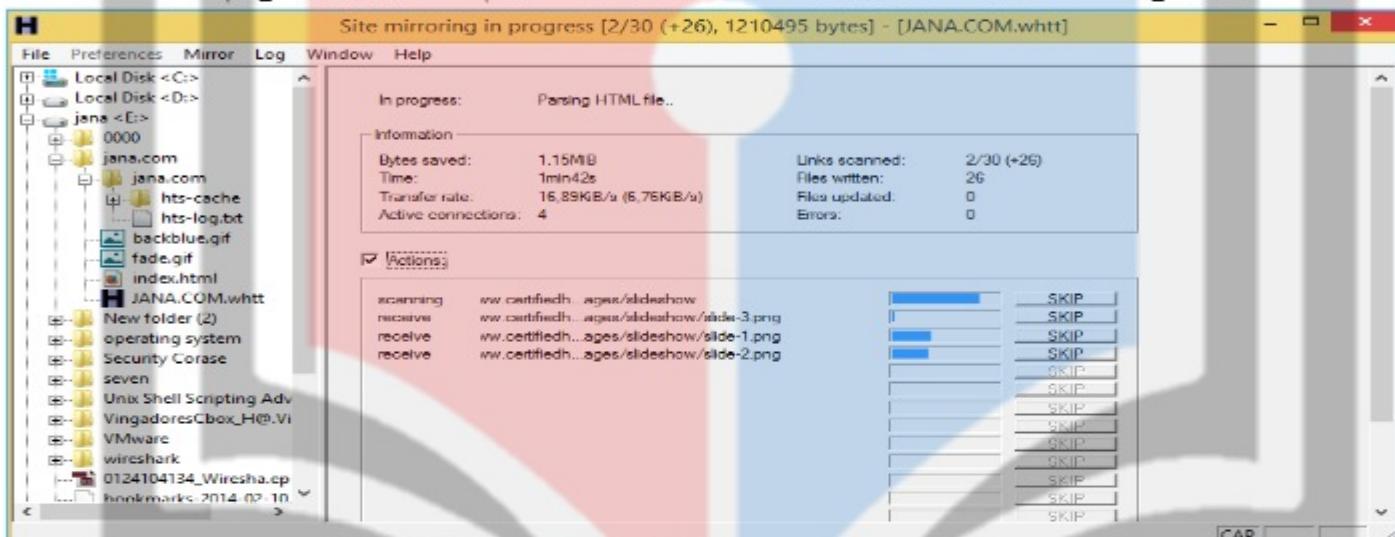


7- نجد هنا الكثير من الاعداد المتقدمة مثل البروكسي وتحديد الحجم المسموح به للتحميل (**Limits**) وغيرها ما ليها هنا هو **NEXT** والتي تحدد أنواع الملفات التي نريد تحميلها وهنا نختار جميع الأنواع المتاحة تم نضغط **ok** تم نضغط **Scan Rules**

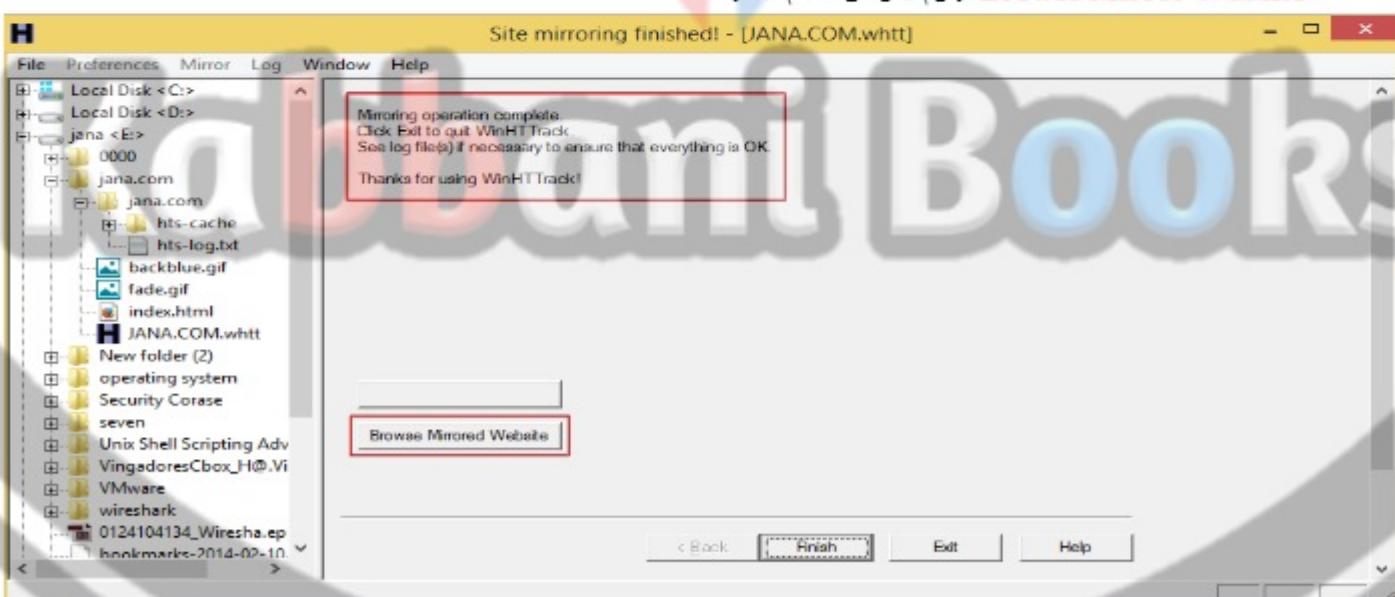




8- عند الوصول الى هذه الشاشة تكون قد انتهينا ونترك الاعدادات الافتراضية فيها كما هي تم نضغط **FINISH** حتى يتم عملية التحميل.



9- بعد الانتهاء من التحميل يعطيك رسالة انه قد أنهى التحميل **Mirror Operation complete** ويوجد في اخر الشاشة زر اسمه **Browse Mirror Website**.



- في نظام التشغيل جنو/لينكس

هذه الأداة مدمجة في بعض نسخ التوزيعة كالى ولكن للأسف غير مدمجة في نسخ أخرى من كالى وغير مدمجة في نسخة **باك تراك** لذلك سوف تحتاج إلى تثبيتها في حالة عدم توفرها على النسخة الخاصة بك كالاتي:

```
root@jana:~# apt-get install httrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libhttrack2
Suggested packages:
  webhttrack httrack-doc
The following NEW packages will be installed:
  httrack libhttrack2
0 upgraded, 2 newly installed, 0 to remove and 574 not upgraded.
Need to get 415 kB of archives.
After this operation, 1,095 kB of additional disk space will be used.
Do you want to continue [Y/n]? ■
```

سوف تحتاج إلى إنشاء مجلد لتخزين ملفات موقع الويب الذي قمت بنسخه، ويتم ذلك عن طريق استخدام الامر **mkdir** ولكن اسم المجلد تم تقوم بالانتقال إلى داخل المجلد كالاتي:

```
root@jana:~# mkdir mywebsites
root@jana:~# cd mywebsites/
root@jana:~/mywebsites# ■
```

ان عملية **HTTrack** تتم في الوضع **non-interactive mode** او في الوضع **interactive mode**. لتشغيل **HTTrack** في الوضع **interactive mode** ويتم ذلك عن طريق كتابة الامر **httrack** بدون أي صيغة والذي يؤدي إلى الدخول إلى الأمر. تم بيدا بسؤالك بعض الأسئلة لتحديد موقع الويب الذي تريد نسخه. اما لتشغيله في الوضع **non-interactive mode** فيتم ذلك عن طريق كتابة الامر **httrack** تم بتنعيم أي من الصيغ اختيارية الخاصة به.

تم تشغيل **httrack** في الوضع **interactive mode** كالاتي:

```
root@jana:~/mywebsites# httrack
Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhttplib.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help
```

Enter project name : ■

نجد ان الخطوة الأولى يطلب منك اسم لهذا المشروع تقوم بإدخال اسم للمشروع **[Enter project name]** ولكن مثلا تم **janateba** نضغط **Enter** كالاتي:

Enter project name :janateba

Base path (return=/root/websites/) : ■

الخطوة التالية هو اختيار المجلد الذي سوف يتم نسخ موقع الويب بداخله. قد كنا انتقائنا من قبل المجلد **mywebsites** سوف نختار هذا المجلد في هذا المثال كالاتي:

Base path (return=/root/websites/) :/root/mywebsites

Enter URLs (separated by commas or blank spaces) : ■

الخطوة التالية يطلب منك اسم موقع الويب الذي تريد ان تقوم بنسخه ولكن مثلا **www.certifiedhacker.com** كالاتي:

Enter URLs (separated by commas or blank spaces) :www.certifiedhacker.com

Action:

- (enter) 1 Mirror Web Site(s)
- 2 Mirror Web Site(s) with Wizard
- 3 Just Get Files Indicated
- 4 Mirror ALL links in URLs (Multiple Mirror)
- 5 Test Links In URLs (Bookmark Test)
- 0 Quit

: ■

بعد إدخال اسم الموقع يعطيك خمس اقتراحات ويطلب منك ان تختار واحدا منها. يعتبر الاختيار الثاني أسهل واحد تقوم بكتابته 2 تم الضغط على **Enter** كالتالي:

Proxy (return=none) :

You can define wildcards, like: -\*.gif +www.\*.com/\*zip -\*img\_\*zip  
Wildcards (return=none) :\*

You can define additional options, such as recurse level (-r<number>), separated by blank spaces

To see the option list, type help

Additional options (return=none) :

بعد ذلك يخبرك بمجموعه من الخيارات مثل نوع البروكسي الذي تريده استخدامه إذا كنت تريده استخدام بروكسي تدخل عنوانه اما إذا كنت لا تريده تقوم بالضغط على **Enter** بدون ادخال أي شيء.

بعد ذلك يريدك تحديد نوع الملفات التي تريده تحميلها هنا نكتب التعبير \* والتي تعنى جميع أنواع الملفات تم **Enter**. بعد ذلك إذا كنت تريده إدخال إعدادات اضافيه ام لا تم **Enter**.

Additional options (return=none) :

---> Wizard command line: httrack www.certifiedhacker.com -W -o "/root/mywebsites/janateba" -%v \*

Ready to launch the mirror? (Y/n) :

الآن بعد الضغط على **Enter** يقوم بإخبارك بلخص بالعمليات التي سوف يقوم بها ولديه عملية النسخ نختار Y تم **Enter** فيبدأ النسخ كالتالي:

Ready to launch the mirror? (Y/n) :Y

WARNING! You are running this program as root!

It might be a good idea to use the -%U option to change the userid:

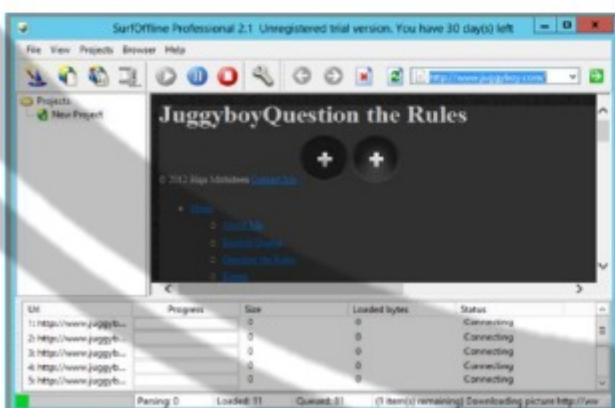
Example: -%U smith

Mirror launched on Thu, 06 Mar 2014 19:43:06 by HTTrack Website Copier/3.46+libhttplib.java.so.2 [XR&CO'2010]

mirroring www.certifiedhacker.com \* with the wizard help..

بعد الانتهاء من عملية النسخ نذهب الى المجلد الذي تم نسخ الموقع اليه ونجد انه يحتوي على ملفات الموقع كالتالي:

```
root@jana:~# ls mywebsites/janateba/
backblue.gif          hts-cache
certifiedhacker.com   hts-in_progress.lock
fade.gif              hts-log.txt
index.html            parallel.us
root@jana:~#
```



### SurfOffline ▪

المصدر: <http://www.surfoffline.com>

**SurfOffline** هو برنامج لتحميل موقع الويب. البرنامج يسمح لك بتحميل الموقع بالكامل وتحميل صفحات الويب إلى القرص الثابت الخاص بك. بعد تحميله للموقع المستهدف، يمكنك استخدام **SurfOffline** باعتباره المتصفح حالياً وعرض صفحات الويب التي تم تحميلها في ذلك. إذا كنت تقضي عرض صفحات الويب التي تم تحميلها في متصفح آخر، يمكنك استخدام معالج التصدير(**Export Wizard**). معالج التصدير يسمح لك بنسخ الموقع بعد تحميلها إلى أجهزة الكمبيوتر الأخرى من أجل عرضها في وقت لاحق، وإعداد الموقع لحرقها لاحقاً على قرص مضغوط أو قرص DVD.



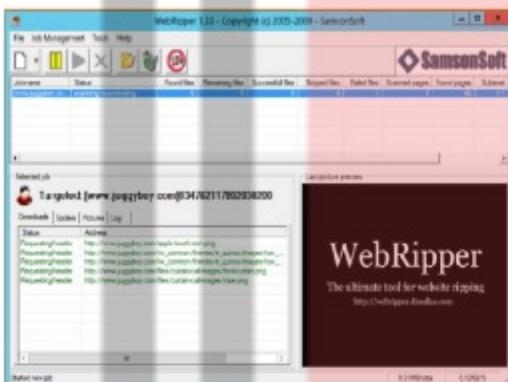
## BlackWidow ▪

[المصدر:](http://softbytelabs.com)

(الأرملة السوداء) هو ماسح ضوئي للموقع على الإنترنت لكلا من الخبراء والمبتدئين. فإنه يفحص الموقع (انه سفاح الموقع). فإنه يمكن تحميل موقع كامل أو جزء من موقع على شبكة الإنترنت. فإنه يقوم ببناء هيكل الموقع أولاً، ثم تحميله. انه يسمح لك لاختيار ما تريد تحميله من الموقع.

## WebRipper ▪

[المصدر:](http://www.calluna-software.com)



هو ماسح محمل لموقع الإنترنت (**Internet scanner and downloader**). هذا يعمل على تحميل كمية هائلة من الصور، والفيديو، وملفات الصوت، والوثائق القابلة للتنفيذ من أي موقع. يستخدم **WebRipper** تكنولوجيا العنكبوت (**spider-technology**) لتنبيه الروابط في كل الاتجاهات بدءاً بالعنوان. يتم ذلك بتصنفي الملفات المتيرة للاهتمام، ويضيفها إلى قائمة انتظار التحميل. يمكنك تعيين العناصر التي تم تنزيلها حسب نوع الملف، والحد الأدنى لحجم الملف، والحد الأقصى لحجم الملف، وحجم الصورة. ويمكن أيضاً تحميل جميع الروابط التي تكون مقيدة للكلمات الرئيسية لتجنب إضاعة **bandwidth** الخاص بك (حجم التبعة).

بالإضافة إلى الأدوات التي سبق شرحها فيما يلي بعض الأدوات الأخرى:

Website Ripper Copier available at <http://www.tensons.com>

Teleport Pro available at <http://www.tenmax.com>

Portable Offline Browser available at <http://www.metaproducts.com>

Proxy Offline Browser available at <http://www.proxy-offline-browser.com>

iMiser available at <http://internetresearchtool.com>

PageNest available at <http://www.pagenest.com>

Backstreet Browser available at <http://www.spadixbd.com>

Offline Explorer Enterprise available at <http://www.metaproducts.com>

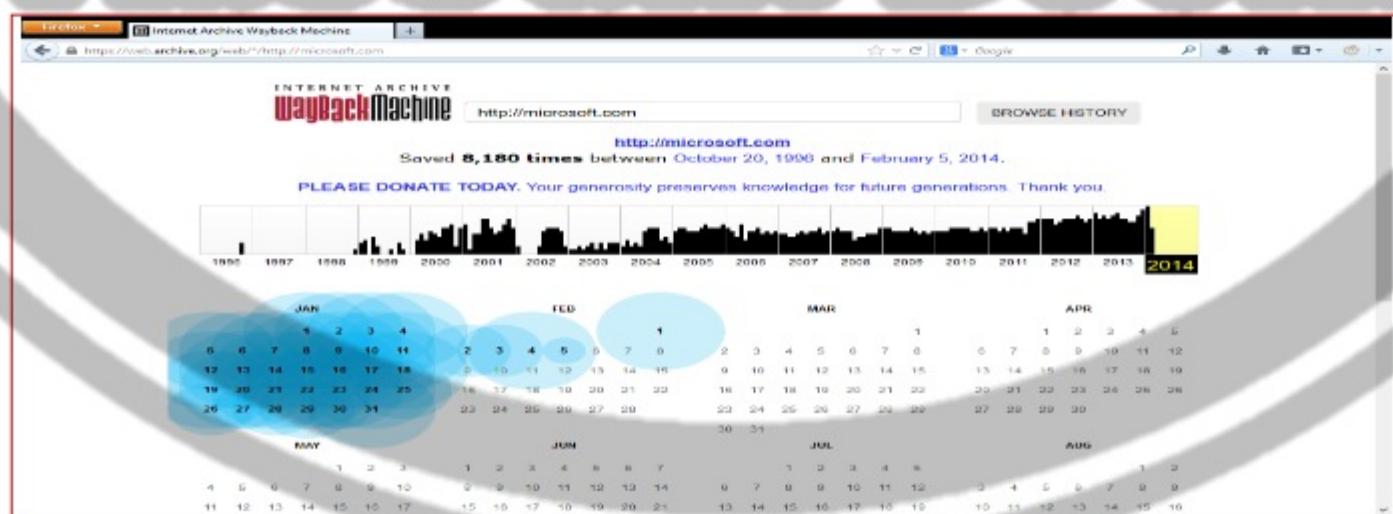
GNU Wget available at <http://www.gnu.org>

Hooeey Webprint available at <http://www.hooeeywebprint.com>

## استخراج معلومات عن الموقع من خلال موقع الأرشيف EXTRACT WEBSITE INFORMATION FROM

<https://archive.org/>

**الأرشيف (Archive)** هو عبارة عن مخزن لملفات الإنترنت (**Internet Archive Wayback Machine**). يسمح لك بزيارة الإصدارات المؤرشفة عن موقع ما. يسمح لك بجمع بعض المعلومات عن صفحات الويب الخاصة بالقرارات منذ إنشائها. يقوم الموقع [www.archive.org](http://www.archive.org) بتتبع صفحات الويب من وقت بدايتها، يمكنك استرداد حتى المعلومات التي تم إزالتها من الموقع الهدف.



## رصد تحديثات الويب باستخدام مراقب الموقع (MONITORING WEB UPDATES USING WEBSITE WATCHER)

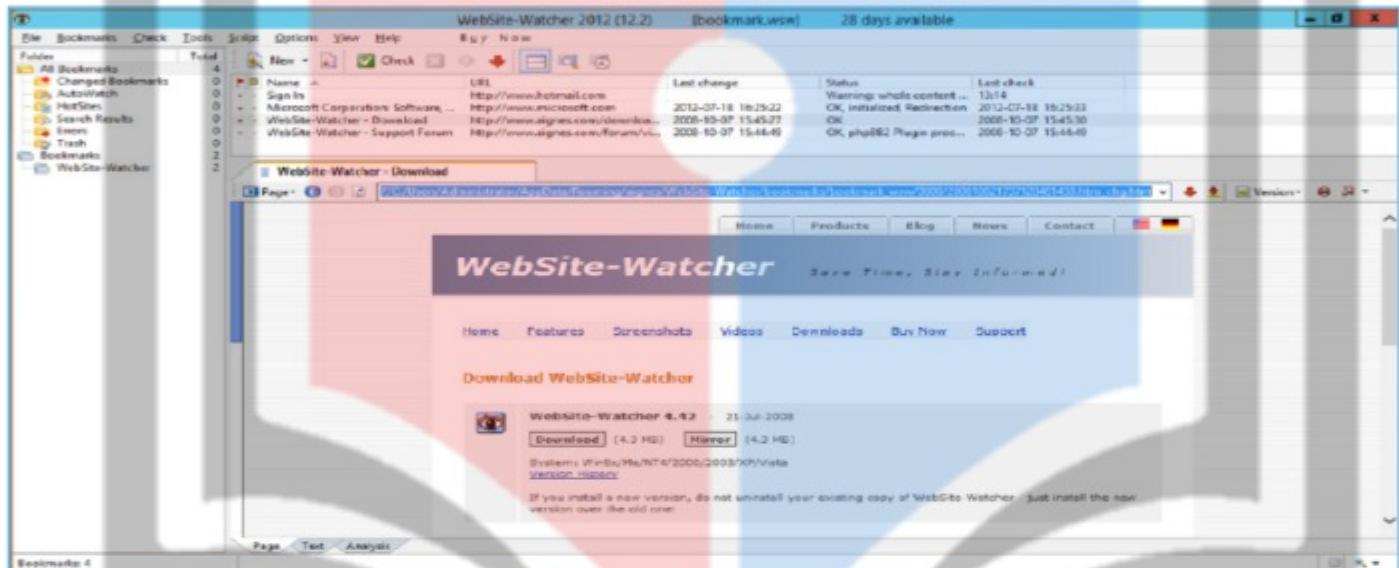
المصدر: <http://www.aignes.com>

يستخدم مراقب الموقع (**Website Watcher**) لتنبيح الموقع للحصول على التحديثات والتغييرات التلقائية. عندما يحدث أي من تحدث أو تغير، فإن مراقب الموقع تلقائياً يقوم بالكتف عنه ثم حفظ آخر إصدارين على القرص الخاص بك، ويسلط الضوء على التغييرات التي حدثت في الملف النصي. هو أداة مفيدة لرصد الموقع لاكتساب ميزة تلقائية.

### الفوائد:

التحقق اليدوي المتكرر عن التحديثات ليس مطلوباً. مراقب الموقع يمكنه تلقائياً كشف وإعلام المستخدمين عن التحديثات:

- هو يتبع لك أن تعرف ما يقوم به منافسيك عن طريق فحص موقع منافسيك.
- الموقع يمكنه تتبع إصدارات البرامج الجديدة أو تحدثات برامج التشغيل.
- يخزن الصور من الموقع المعدلة إلى القرص.



## 3- عمليات الاستطلاع باستخدام البريد الإلكتروني (EMAIL FOOTPRINTING)

يصف هذا القسم كيفية تعقب الاتصالات عبر البريد الإلكتروني، وكيفية جمع المعلومات من رؤوس البريد الإلكتروني، وأدوات تعقب البريد الإلكتروني.

### [TRACKING EMAIL COMMUNICATIONS]

تعقب البريد الإلكتروني (**Email tracking**) هو الأسلوب الذي يساعدك على مراقبة وكذلك تعقب رسائل البريد الإلكتروني لمسخدم معين. هذا النوع من التتبع يمكن من خلال سجلات **digitally time stamped** للكشف عن وقت و تاريخ تلقي أو فتح رسالة بريد إلكتروني بواسطة الهدف. هناك الكثير من أدوات تعقب البريد الإلكتروني متوفرة بسهولة في السوق، وذلك باستخدام ما يمكنك جمعه من المعلومات مثل الآتي: عناوين IP، خدمة البريد، ومزود الخدمة الذي تم إرسال البريد عن طريقه. المهاجمين يمكنهم استخدام هذه المعلومات لبناء استراتيجية القرصنة.

**أمثلة على أدوات تعقب البريد الإلكتروني ما يلي:** **Paraben E-mail Examiner** و **eMailTrackerPro** . باستخدام أدوات تتبع البريد الإلكتروني يمكنك جمع المعلومات التالية حول الضحية:

- الموقع الجغرافي: تقدير وعرض موقع المتلقي على الخريطة، وربما حتى حساب المسافة من موقعك.
- قراءة الفترة الزمنية: مدة الوقت الذي يقضيه المتلقي على قراءة البريد المرسل من قبل المرسل.
- كشف الوكيل **proxy detection**: يوفر معلومات حول نوع الخادم المستخدم من قبل المستلم.
- وصلات: يسمح لك بالتحقق ما إذا كان قد تم فحص الروابط المرسلة إلى المتلقي من خلال البريد الإلكتروني أو لا.
- نظام التشغيل: هذا يعطيك معلومات عن نظام التشغيل المستخدم من قبل المستلم. المهاجم يمكنه استخدام المعلومات لبدء عملية الهجوم من خلال بعض التعرّفات في نظام التشغيل الحالي.
- توجيه البريد الإلكتروني (**Forward Email**): البريد الإلكتروني الذي يتم إرساله إليك يتم توجيهه إلى شخص آخر والذي يتم تحديده بسهولة عن طريق هذه الأدوات.

## جمع المعلومات من خلال عناوين البريد الإلكتروني (COLLECTION FORM THE EMAIL HEADERS)

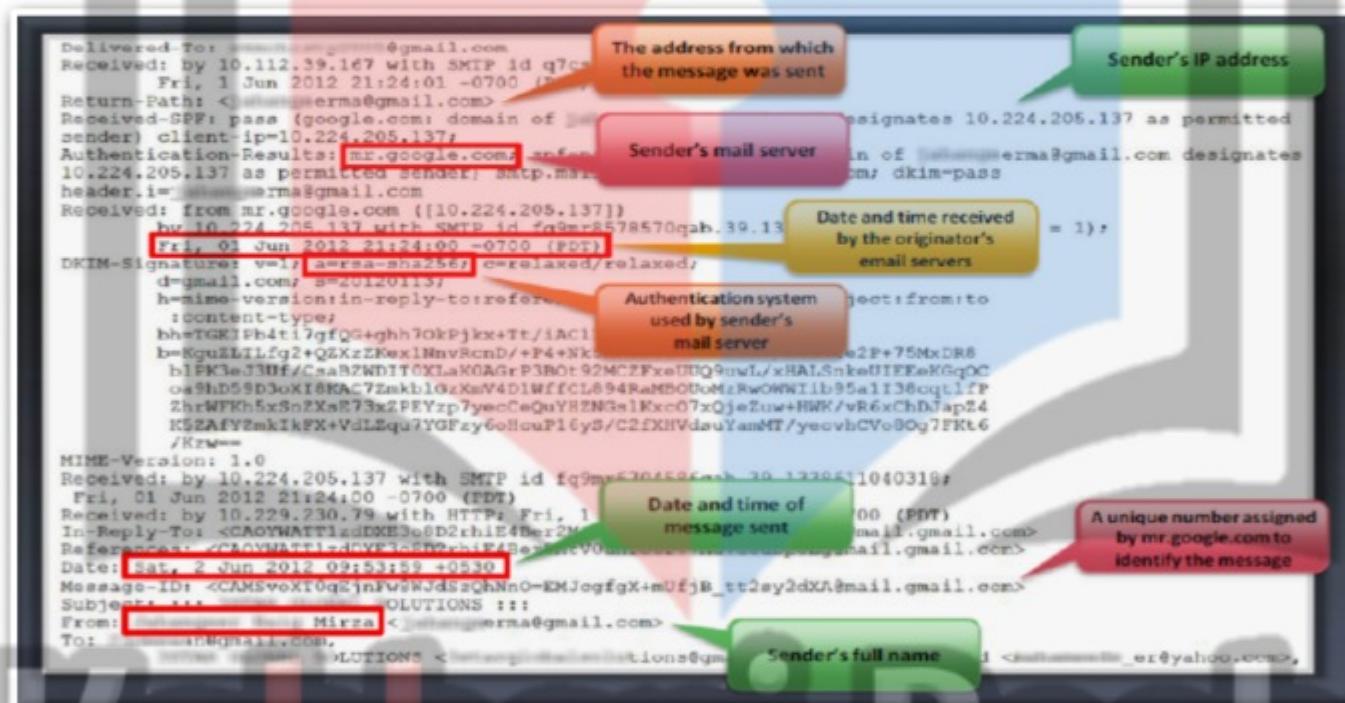
هذه الأيام أصبح البريد الإلكتروني هو أسرع وسيلة للاتصال، ونستخدم على نطاق واسع عبر البريد الإلكتروني، لأغراض شخصية ولأغراض تجارية، الآن لديك المقدرة لتحديد موقع الشخص الذي يرسل لك رسالة البريد الإلكتروني ولكن كيف يمكنك أن تفعل هذا. يمكنك تتبع البريد الكتروني باستخدام رأس رسالة البريد الإلكتروني، والسؤال المطروح الآن هو ماذا يوجد في رأس البريد الإلكتروني، وكيف نستخدمه لتتبع موقع المرسل.

**رأس/عناوين البريد الإلكتروني** هي المعلومات التي تosopher مع كل رسالة بريد إلكتروني. هذه العناوين تحتوي على تفاصيل المرسل، معلومات التوجيه، التاريخ، الموضوع، والمستقبل. عملية عرض رأس البريد الإلكتروني يختلف مع برامج البريد المختلفة. أكثر برامج البريد الإلكتروني استخداماً:

**SmarterMail Webmail – Outlook Express 4-6 – Outlook 2000-2003 – Outlook 2007 – Eudora 4.3/5.0**

**Entourage – Netscape Messenger 4.7 – MacMail**

فيما يلي لقطة لرأس/عنوان البريد الإلكتروني والمعلومات التي تحتويها:



المهاجم يمكنه تتبع وجمع هذه المعلومات عن طريق التحليل بالتفاصيل لعناوين البريد الإلكتروني.

### أدوات تتبع البريد الإلكتروني (Email Tracking Tools)

أدوات تعقب البريد الإلكتروني تسمح لك بتعقب البريد الإلكتروني واستخراج المعلومات منه مثل هوية المرسل (**Sender identity**) ، خادم البريد (**IP**) ، عنوان **mail server** ، وما إلى ذلك. يمكنك استخدام هذه المعلومات لمهاجمة أنظمة المستهدفة عن طريق إرسال رسائل البريد الإلكتروني الخبيثة. تتوفر العديد من أدوات تعقب البريد الإلكتروني بسهولة في السوق. وفيما يلي عدد قليل من الأدوات التي تستخدم عادة لتعقب البريد الإلكتروني:

#### eMailTrackerPro

المصدر: <http://www.emailtrackerpro.com>

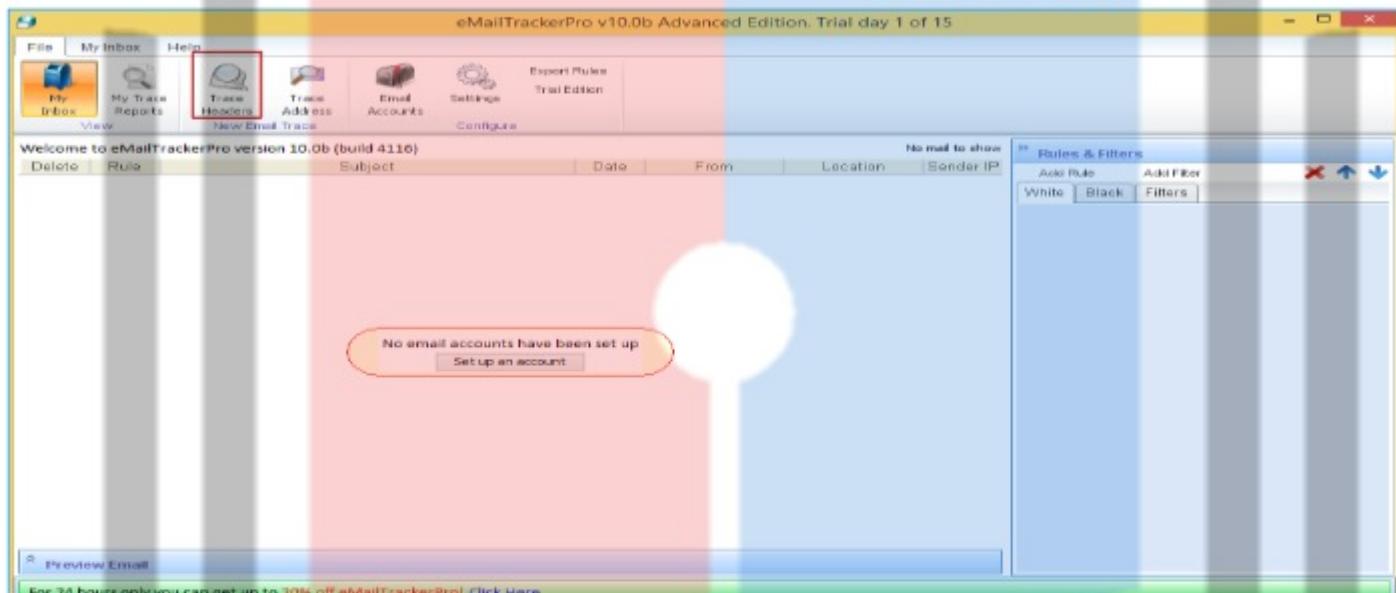
**eMailTrackerPro** هو أداة تتعقب البريد الإلكتروني الذي يحلل رؤوس البريد الإلكتروني ويكتفى عن بعض المعلومات مثل الموقع الجغرافي للمرسل وعنوان **IP** ، وما إلى ذلك. يسمح لك أيضاً باستعراض آثار في وقت لاحق عن طريق حفظ كل آثار الماضي. **تعقب البريد الإلكتروني [email tracking]** هو وسيلة لرصد أو تجسس على بريد إلكتروني يتم تسليمها إلى المستلم الهدف. **eMailTrackerPro** يتيح لك تتبع البريد الإلكتروني إلى مصدره، وأيضاً يستخدم لتصفيقة الرسائل الغير المرغوب فيها والحملات الضارة (**SPAM EMAIL**). وعن طريق استخدام المعلومات الواردة في رأس البريد الإلكتروني (**Email header**) ، فيمكنه تحديد المدينة



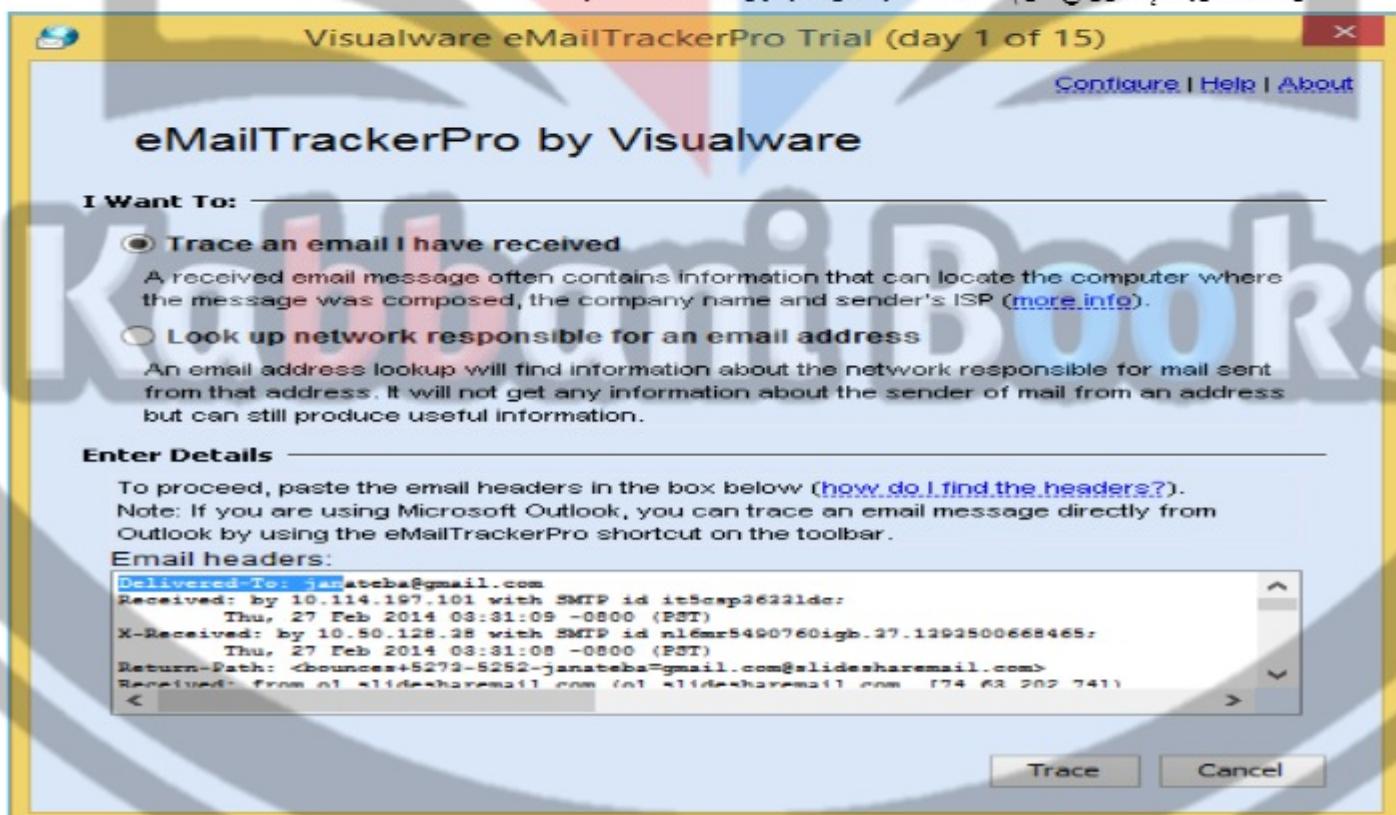
أو البلد التي نسأ منها البريد الكتروني، بما في ذلك معلومات **Whois** التي يمكنك استخدامها للإبلاغ عن سوء المعاملة وإغلاقها نهائياً.  
1. يتم تثبيت هذه الأداة باتباع **wizard** الخاص بعملية التثبيت ونلاحظ أيضاً أنه خلال هذه العملية يتم تثبيت **java runtime** أيضاً معه.

2. ملحوظه عند تثبيت البرنامج فإنه يحتاج إلى حساب للبريد الإلكتروني سواء من مقدمي الخدمة مثل ياهو أو هوتميل أو خادم خاص بك. هنا سو نتعامل مع النسخة العاشرة أما النسخة الذي تم ترجمتها في **CEH** هي النسخة التاسعة.

3. بعد تثبيت تطبيق **eMailTrackerPro** يتم تشغيله فتظهر الشاشة التالية:



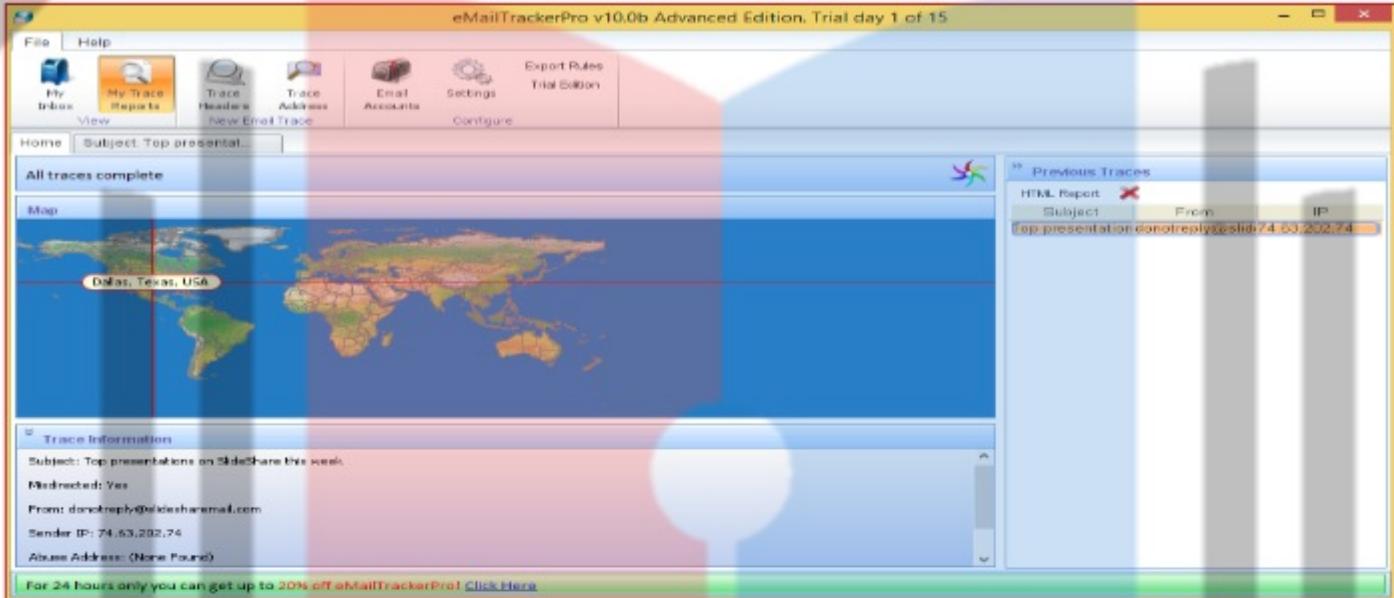
4. نلاحظ هنا انه يحتاج الى وضع بيانات الخاصة بالحساب الخاص بك في البريد الإلكتروني (**set up an account**) والتي سوف تنترق اليه لاحقاً. هنا سوف نلاحظ في شريط الأدوات وجود زر يسمى **Trace Headers** والذي يستخدم في تحليل رؤوس رسائل البريد الإلكتروني تقوم بالضغط عليه سوف يظهر لنا الشاشة التالية:



5. نختار **Trace an email I have received** ونضع رأس البريد الذي استلمته في المربع الخاص **Enter Details** ثم نضغط على **Trace**.



6. بعد الضغط عليه نلاحظ انه اعطى جميع البيانات عن الذي قام بارسال هذا البريد الإلكتروني وموقعه الجغرافي وعنوان IP الخاصة به كالتالي:



### PoliteMail ▪

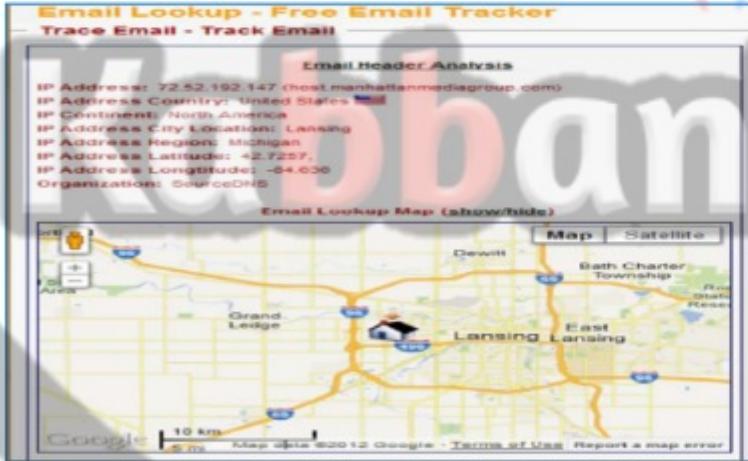
[المصدر](http://www.politemail.com)

**PoliteMail** هو أداة تُتبع البريد الإلكتروني لبرنامج **Outlook**. وهو يتتابع ويقدم تفاصيل كاملة حول من قام بفتح البريد الخاص بك وأي من الوثيقة التي تم فتحها، وكذلك أي من الروابط التي تم النقر عليها وقراءتها. فإنه يوفر دمج المراسلات، اختبار الانقسام، وقائمة كاملة للإدارء بما في ذلك التجزئة. يمكنك إنشاء رسالة البريد الإلكتروني تحتوي على وصلات خبيثة وإرسالها إلى موظفي المنظمة المستهدفة وتتبع هذا البريد الإلكتروني. إذا قام الموظف بالنقر على الرابط، فإنه يصبح مصاباً وسيتم إعلامك بذلك. وبالتالي، يمكنك السيطرة على النظام مع مساعدة من هذه الأداة.

### Email Lookup – Free Email Tracker ▪

[المصدر](http://www.ipaddresslocation.org)

**Email Lookup** هو أداة تُتبع البريد الإلكتروني الذي يحدد عنوان IP الخاص بالمرسل عن طريق تحليل رأس البريد الإلكتروني. يمكنك نسخ ولصق رأس البريد الإلكتروني إلى هذه الأداة والبدء في البحث في البريد الإلكتروني عن المعلومات التي تريدها.



### Read Notify ▪

[المصدر](http://www.readnotify.com)

**Read Notify** يوفر لك خدمة تتبع البريد الإلكتروني. وذلك بإعلامك إذا حدث فتح البريد الإلكتروني الذي تتحبه، أو إعادة الفتح أو إعادة إرسالها. تقارير **Read Notify** لتتبع البريد الإلكتروني تتبع لك بعض المعلومات مثل تفاصيل كاملة عن محتوى الرسالة، وتاريخ ووقت فتح الرسالة والموقع الجغرافي للمنتقى، خريطة تصور الموقع، عنوان IP الخاص بالمنتقى وتتفاصيل المرجع.

### DidTheyReadIt ▪

[المصدر](http://www.didtheyreadit.com)

**DidTheyReadIt** هو أداة تتبع البريد الإلكتروني. من أجل استخدام هذه الأداة تحتاج إلى الاشتراك **sign up** للحصول على حساب.



تم تحتاج إلى إضافة "DidTheyReadIt.com". إلى نهاية عنوان البريد الإلكتروني للمستلم. على سبيل المثال، إذا كنت تريد أن ترسل رسالة بريد إلكتروني إلى [ellen@aol.com](mailto:ellen@aol.com).**DidTheyReadIt.com**، فإنك تكتب العنوان كالتالي ([ellen@aol.com.DidTheyReadIt.com](mailto:ellen@aol.com.DidTheyReadIt.com))، ومستقل هذه الرسالة [ellen@aol.com](mailto:ellen@aol.com) لن يرى ما قمت بإضافته ([DidTheyReadIt.com](mailto:DidTheyReadIt.com)). إلى عنوان البريد الإلكتروني. هذه الأداة تعمل على تتبع كل البريد الإلكتروني التي ترسلها بالخلفاء، دون تنبيه المتنقى. إذا يفتح المستخدم البريد الخاص بك، فإنه يخبرك عن طريق البريد الإلكتروني الخاص بك أنه تم فتح الرسالة، وكم من الوقت استغرق والرسالة مفتوحة، تم تحديد لك الموقع الجغرافي للمكان الذي حدث فتح الرسالة فيه.

#### TraceEmail ▪

المصدر: <http://whatismyipaddress.com>

تحاول الأداة **TraceEmail** لتحديد عنوان IP المصدر من البريد الإلكتروني استناداً إلى رؤوس البريد الإلكتروني. تحتاج فقط إلى نسخ ولصق الرؤوس بالكامل من البريد الإلكتروني المستهدف في مربع الرؤوس ثم انقر فوق ([Get Source](#)) للحصول عليه بيان تحليل رأس البريد الإلكتروني والنتائج. لا تملك أداة تحليل رأس البريد الإلكتروني القدرة على الكشف عن رسائل البريد الإلكتروني ذات الرؤوس المزورة. هذه الرؤوس المزورة للبريد الإلكتروني شائعة في البريد الإلكتروني الخبيث والبريد المزعج. هذه الأداة تفترض أن جميع خوادم/ملقمات البريد وعملاء البريد الإلكتروني في مسار الانتقال جديرة بالثقة.

#### MSGTAG ▪

المصدر: <http://www.msgtag.com>

**MSGTAG** هو أداة ذات بيئة ويندوز تعمل على تتبع البريد الإلكتروني والتي تستخدم تكنولوجيا ([read receipt](#)) والتي تخبرك عندما يتم فتح رسائل البريد الإلكتروني الخاصة بك وخاصة عندما يتم قراءة رسائل البريد الإلكتروني الخاصة بك فعلاً. هذا البرنامج يضيف المسار والتتبع التي هي فريدة من نوعها إلى كل البريد الإلكتروني التي تحتاج إليها لتأكيد التسلل. عند فتح البريد الإلكتروني يتم إرسال رمز تعقب البريد الإلكتروني إلى نظام تتبع البريد الإلكتروني **MSGTAG** ويتم تسليم رسالة بريد إلكتروني إليك تخبرك بذلك. **MSGTAG** سوف يخبرك عندما يتم قراءة الرسالة عبر التأكيد عبر البريد الإلكتروني، رسالة منتبقة، أو رسالة نصية قصيرة [SMS](#).

#### Zendio ▪

المصدر: <http://www.zendio.com>

**Zendio**، هو تطبيق تعقب البريد الإلكتروني وهو عبارة عن إضافة لـ [Outlook](#). يقوم بإعلامك بمجرد أن يقوم المتنقى بقراءة البريد الإلكتروني، حتى تتمكن من متابعته، بمجرد قراءة الرسالة فإنك تعرف بذلك وإذا قام بالتنقل على أي من الروابط أيضاً المدرجة في البريد الإلكتروني.

#### Pointofmail ▪

المصدر: <http://www.pointofmail.com>

**Pointofmail.com** هو دليل لخدمة استلام وقراءة البريد الإلكتروني. فإنه يضمن قراءة المستلم للرسالة، ويتيح الملحقات، ويتيح لك تعديل أو حذف الرسائل المرسلة. فإنه يوفر معلومات مفصلة عن المتنقى، والتاريخ الكامل عن البريد الإلكتروني الذي قام بالقراءة والتوجيه، والروابط ومرفقات التتبع، والبريد الإلكتروني، والويب والرسائل [SMS](#) الإخطارات.

#### Super Email Marketing Software ▪

المصدر: <http://www.bulk-email-marketing-software.net>

هو برنامج ذات مستوى احترافي ومستقل لمجموعه من برامج الإيميل (البريد الإلكتروني). فهو لديه القدرة على إرسال رسائل إلى قائمة عناوين. وهو يدعم كل من النص وكذا رسائل البريد الإلكتروني بتنسيق [HTML](#). يتم إزالة كافة عناوين البريد الإلكتروني المكررة تلقائياً باستخدام هذا التطبيق. يتم إرسال كل رسالة بريد إلكتروني بشكل فردي إلى المتنقى لذلك فإن المتنقى يرى البريد الإلكتروني فقط في رأس البريد الإلكتروني. يحفظ عناوين البريد الإلكتروني للرسائل المرسلة بنجاح فضلاً عن الرسائل التي فشلت في الإرسال إلى ملف نص،

[.Microsoft Excel](#), [CSV](#), [TSV](#) أو ملف

#### WhoReadMe ▪

المصدر: <http://whoreadme.com>

**WhoReadMe** هو أداة تتبع البريد الإلكتروني. ويكون غير مرئي تماماً بالنسبة للمتنقى. المتنقون لن يكون لديهم أي فكرة أن رسائل البريد الإلكتروني المرسلة إليهم يجري تعقبها. يتم إخطار المرسل في كل مرة يقوم المستلم بفتح البريد المرسل من قبل المرسل. انه يقوم بتنبيه المعلومات مثل نوع نظام التشغيل والمتصفح الذي تستخدمه، نسخة [CSS](#), [Active X controls](#) ، والمدة بين إرسال الرسائل وقراءتها، الخ.

#### GetNotify ▪

المصدر: <http://www.getnotify.com>

أداة تعقب البريد الإلكتروني التي ترسل إخطارات عندما يقوم المتنقل بفتح وقراءة البريد. يرسل الإخطارات دون علم المستلم.

### G-Lock Analytics ▪

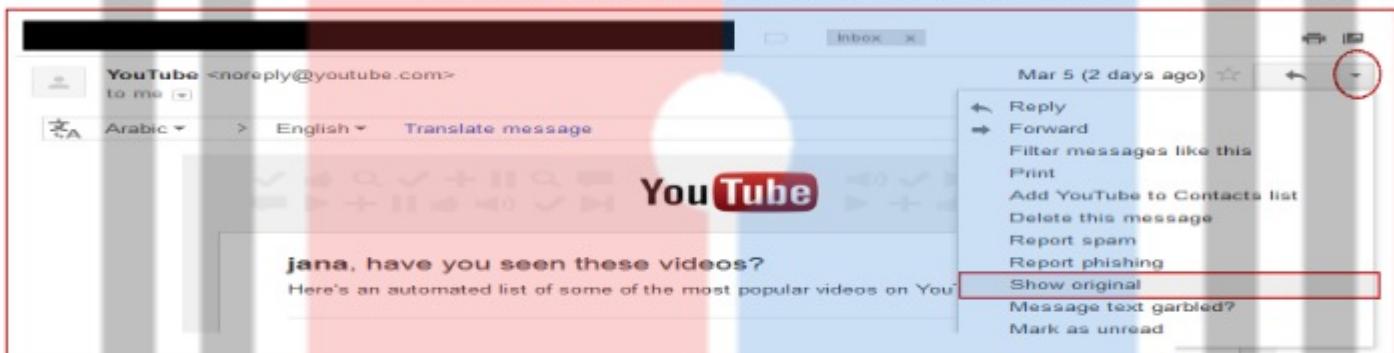
[المصدر:](http://glockanalytics.com)

**G-Lock Analytics** هي خدمة تتبع البريد الإلكتروني. هذا يسمح لك أن تعرف ما يحدث لرسائل البريد الإلكتروني بعد إرسالها. تقارير هذه الأداة بالنسبة لك هو كم مرة تم طباعة البريد الإلكتروني وإرسالها.

كيفية الحصول على بيانات رفوس البريد الإلكتروني:

### In Gmail -

ندخل على الحساب الخاص بنا، تم نذهب إلى **Inbox**، تم نضغط على الرسالة التي تزيد تعقبها. فتنتقل إلى سائمه أخرى تحتوي على مضمون الرسالة. بعد الدخول إلى الرسالة نضغط على الآتي ونختار **Show Original** كالاتى:

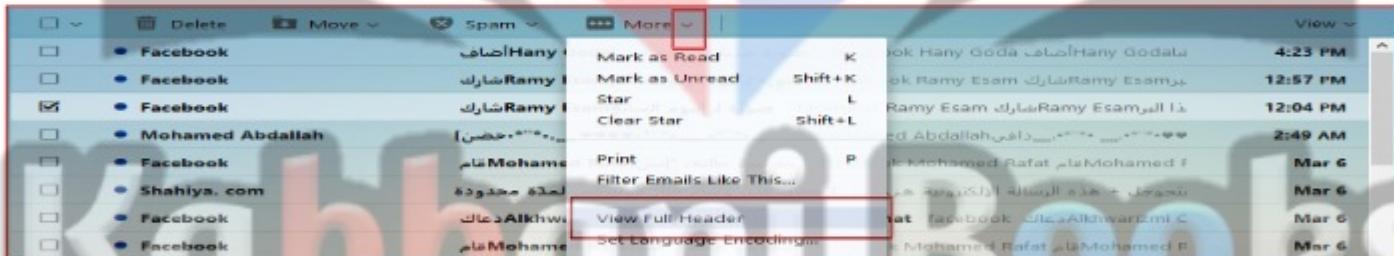


### In Hotmail -

تفعل مثل ما حدث مع **Gmail** ولكن بدلاً من الدخول على مضمون الرسالة تقوم بالضغط بالزر اليمين للماوس على الرسالة فتظهر قائمه نختار منها **view message source**.

### In yahoo -

ندخل على الحساب الخاص بنا، تم نذهب إلى **Inbox** ، تم نضغط على الرسالة التي تزيد تعقبها تم نذهب إلى القائمة العلوية توجد علامة **More** نضغط عليها فتظهر قائمه نختار منها **view Full Header** كالاتى:



### Online Email Tracer ▪

[المصدر:](http://www.cyberforensics.in/OnlineEmailTracer/index.aspx)

**Email Tracer** هو أداة تعقب البريد الإلكتروني لهوية المرسل. يحل رأس البريد الإلكتروني ويعطي تفاصيل كاملة عن المرسل مثل عنوان IP، والتي هي النقطة الأساسية للعثور على المرسل والمسار الذي اتبّعه البريد، خاتم البريد، وتفاصيل مقدم الخدمة الخ يتابع البريد الإلكتروني إلى ما يصل إلى مستوى موقـر خـدمـة إـنـترـنـت.

يمكن لخوادم/ملقمات (البريد الإلكتروني) البريد الإلكتروني ان توفر ترورة من المعلومات للمتسللين ومختربي الاختراق. في نواح كثيرة، البريد الإلكتروني يتبعه الباب الدوار للمنظمة المستهدفة الخاصة بك. على افتراض ان الهدف يملك ملقم/خادم للبريد الإلكتروني الخاص به، هذا هو في كثير من الأحيان مكانا رائعا للهجوم. من المهم أن نتنذكر، " لا يمكنك منع ما يجب أن تسمح به" بعبارة أخرى، لإعداد البريد الإلكتروني بشكل صحيح، فان حركة المرور الخارجية (**external traffic**) يجب أن تمر من الأجهزة الخاصة بك مثل جدران الحماية والموجهات (**routers**)، إلى الجهاز الداخلي، وعادة ما يكون داخل الشبكات المحمية الخاصة بك. نتيجة لهذا، نحن غالبا ما يمكن جمع قطع كبيرة من المعلومات من خلال التفاعل المباشر مع ملقم/خادم البريد الإلكتروني. واحد من أول الأشياء التي يجب القيام به عند محاولة خداع خادم البريد الإلكتروني هو إرسال رسالة بريد الإلكتروني تحتوي على ملف فارغ غير ضار سواء (.bat) أو (.exe). مثل (.calc.exe). إن الهدف من هذه الحالة هو إرسال رسالة إلى خادم البريد الإلكتروني المستهدف الموجود داخل المنظمة الهدف على أمل أنها تملك خادم البريد الإلكتروني، ومن تم يتم رفض الرسالة.

بمجرد رفض الرسالة يتم إرجاعها إليك، وهذا يمكننا محاولة انتزاع معلومات حول ملقم البريد الإلكتروني الهدف. في كثير من الحالات، يكون نص الرسالة التي تم رفضها وإرجاعها إليك هو أن الملقم لا يقبل رسائل البريد الإلكتروني مع ملحقات يحتمل أن تكون خطيرة. غالبا ما تتغير هذه الرسالة بمورد محدد ونسخة مضاد الفيروسات التي تم استخدامها لفحص البريد الإلكتروني. هذه قطعة كبيرة من المعلومات. وجود رسالة الرد من خادم البريد الإلكتروني المستهدفة يسمح لنا أيضا بتقد رؤوس البريد الإلكتروني. والتي تسمح لنا لاستخراج بعض المعلومات الأساسية حول خدمة البريد الإلكتروني، بما في ذلك عنوان IP وإصدارات برامج معينة أو العلامة التجارية من خادم البريد الإلكتروني. معرفة عنوان IP واصدارات البرمجيات تكون مفيدة بشكل لا يصدق عندما ننتقل إلى مرحلة **exploitation phase**.

## COMPETITIVE INTELLIGENCE-4 (الاستخبارات التنافسية)

الاستخبارات التنافسية هي عملية تجميع وتحليل، وتوزيع المعلومات الاستخبارية حول المنتجات والعملاء والمنافسين، والتكنولوجيات باستخدام الإنترنت. هذه المعلومات يمكن أن تساعد المديرين والمسؤولين التنفيذيين في شركة ما من اتخاذ قرارات استراتيجية. هذا القسم هو عبارة عن جمع المعلومات الاستخبارية التنافسية والمصادر حيث يمكنك الحصول على معلومات قيمة.

### COMPETITIVE INTELLIGENCE GATHERING (جمع المعلومات الاستخباراتية)

يوجد العديد من الأدوات المختلفة المتوفرة في السوق لعرض جمع المعلومات الاستخبارية التنافسية.

يعرف هذا بالحصول على معلومات حول المنتجات، المنافسين، وتقنيات الشركة باستخدام الإنترنت كوسيلة الاستخبارات التنافسية. الاستخبارات التنافسية ليس فقط عن تحليل المنافسين ولكن أيضا عن تحليل منتجاتها و العملاء والموردين، الخ التي تؤثر على المنظمة. هذه العملية تكون دقيقة ومن غير تدخل في طبيعتها مقارنة بسرقة الملكية الفكرية مباشرة والتي نفذت من خلال القرصنة أو التجسس الصناعي. هذه العملية تركز بشكل رئيسي على بيئة الأعمال الخارجية. إنها تعمل على تجميع المعلومات بطريقه أخلاقية وقانونيه بدلا من جمعها سرا. وفقا لـ **CI professionals**، بأنه إذا كانت المعلومات الاستخباراتية التي جمعت ليست مفيدة، فإنه لا يسمى **Intelligence**. يتم تنفيذ الاستخبارات التنافسية لتحديد:

- ما يفعله المنافسين.
- كيف يقوم المنافسين بوضع منتجاتهم وخدماتهم.

#### مصادر الاستخبارات التنافسية:

- الواقع الإلكتروني للشركة وإعلانات التوظيف.
- محركات البحث، الإنترنت، وقواعد البيانات على الإنترنت.
- البيانات الصحفية والتقارير السنوية.
- المجالات التجارية، المؤتمرات، والصحف.
- براءات الاختراع والعلامات التجارية.
- الهندسة الاجتماعية.
- كتالوجات المنتجات ومنافذ البيع بالتجزئة.
- المحل والتقارير التنظيمية.
- مقابلات العملاء والموردين.
- الوكلاء والموزعين والموردين.

يمكن أن تتم عملية الاستخبارات التنافسية إما عن طريق توظيف الناس للبحث عن المعلومات أو من خلال الاستفادة من خدمة قاعدة البيانات التجارية، والتي تتطلب أقل تكلفة من توظيف أفراد لتقليل التكلفة.

## الاستخبارات التنافسية - متى بدأت هذه الشركة [WHEN DID THIS COMPANY BEGIN] ؟ وكيف تطورت؟

جمع الوثائق والسجلات الخاصة بالمنافسين التي تم جمعها تساعد على تحسين الإنتاجية والربحية وتحفيز النمو. فإنه يساعد على تحديد إجابات لما يلي:



### - متى بدأت الشركة (When did it begin)؟

من خلال الاستخبارات التنافسية، وتاريخ الشركة التي يمكن جمعها، مثل متى تأسست شركة معينة. في بعض الأحيان، المعلومات الهامة الغير متوفرة عادة للأخرين يمكن أيضاً جمعها.

### - كيف تطورت الشركة (How did it develop)؟

من المفيد جداً المعرفة حول كيفية تطور شركة معينة. ما هي الاستراتيجيات المختلفة التي تم استخدامها من قبل هذه الشركة؟ سياسة الإعلان عنها، إدارة العلاقات العامة، وغيرها من الاستراتيجيات التي يمكن تعلمها.

### - من الذي يقود هذا (Who leads it)؟

تساعد هذه المعلومات شركة ما في تعلم التفاصيل عن الشخص الرائد (صانع القرار) في الشركة المنافسة.

### - أين تقع الشركة (Where is it located)؟

موقع الشركة والمعلومات ذات الصلة لمختلف فروعها وعملياتها يمكن جمعها من خلال الاستخبارات التنافسية. يمكنك استخدام هذه المعلومات التي تم جمعها من خلال الاستخبارات التنافسية لبناء استراتيجية القرصنة.

فيما يلي بعض من المواقع التي تكون مصدراً للمعلومات التي تساعد المستخدمين الحصول على معلومات استخباراتية تنافسية.

### EDGAR ▪

المصدر: <http://www.sec.gov/edgar.shtml>

جميع الشركات، الأجنبية والمحلي، تحتاج إلى تقديم بيانات التسجيل، التقارير الدورية، وأشكال أخرى إلكترونياً من خلال EDGAR. بحيث يمكن لأي شخص رؤية قاعدة بيانات EDGAR بحرية من خلال شبكة الإنترنت (الويب أو FTP). جميع الوثائق التي قدمت إلى اللجنة من قبل الشركات العامة قد لا تكون متاحة على EDGAR.

### Hoovers ▪

المصدر: <http://www.hoovers.com>

**Hoovers** هي شركة للبحوث التجارية التي توفر تفاصيل كاملة عن الشركات والصناعات في جميع أنحاء العالم. يوفر Hoovers المعلومات المتعلقة بالأعمال التجارية من خلال الإنترنت، البيانات(data feeds)، الأجهزة اللاسلكية(wireless)، الاتفاقيات العالمية التجارية المتتركة مع الخدمات الأخرى عبر الإنترنت. أنه يعطي معلومات كاملة عن المنظمات، والصناعات، والناس التي تدفع الاقتصاد. توفر الأدوات لربط الأشخاص المناسبين أيضاً، من أجل الحصول على العمل المنجز.

### LexisNexis ▪

المصدر: <http://lexisnexis.com>

**LexisNexis** هو المزود العالمي لتمكين المحتوى وحلول مصممة خصيصاً للمهنيين العاملين في القانون، إدارة المخاطر، الشركات، الحكومة، متقدي القانون، المحاسبة، والأسواق الأكاديمية. فإنه يحافظ على قاعدة بيانات إلكترونية من خلالها يمكنك الحصول على السجلات العامة القانونية والمعلومات ذات الصلة. الوثائق والسجلات، والأخبار، ومصادر الأعمال تكون في متناول العملاء.



## Business Wire ▪

**المصدر:** <http://www.businesswire.com>

**Business Wire** هي الشركة التي تركز على توزيع النشرات الصحفية والإفصاح التنظيمي. توزع النشرات الإخبارية كاملة النص، والصور، ومحظى الوسائط المتعددة الأخرى عن آلاف الشركات والمنظمات من قبل هذه الشركة في جميع أنحاء العالم على الصحفيين ووسائل الإعلام، والأسواق المالية، والمستثمرين، والمعلومات على شبكة الإنترنت، وقواعد البيانات، والجمهور العام. هذه الشركة لديها تسلكها الإلكترونية الخاصة والتي من خلالها يتم تصدير النشرات الإخبارية.

**الاستخبارات التنافسية - ما هي خطط الشركة؟ (WHAT ARE THE COMPANY'S PLANS) ?**

فيما يلي بعض الأمثلة لموقع الويب المفيدة في جمع المعلومات المهمة عن العيد من الشركات وخططهم:



**المصدر:** <http://www.marketwatch.com>

**MarketWatch** يقيس نسب الأسوق. يوفر الموقع أخبار الأعمال، المعلومات الشخصية والمالية، الأدوات والبيانات الاستثمارية، مع العديد من الصحفيين المختصين يمكنهم توليد المئات من الملايين والقصص، أسرطة الفيديو، وموجزات السوق يوميا.



**المصدر:** <http://www.twst.com>

**Wall Street Transcript** هو موقع ويب ينشر تقارير الصناعة يحتاج إلى دفع الاشتراك للنشر. أنه يعبر عن وجهات نظر مديرى المال ومحطى الأسهم في قطاعات الصناعة المختلفة. وتتعدد مقابلات مع كبار المديرين التنفيذيين من الشركات.



**المصدر:** <http://www.lippermarketplace.com>

**LipperMarketplace** تقدم حلولاً على شبكة الإنترنت التي هي مقدمة لتحديد القيمة السوقية للشركة. السوق يساعد في تأهيل و توفير الاستخبارات التنافسية اللازمة لتحويل هذه الآفاق إلى العملاء. حلولها تسمح للمستخدمين لتحديد صافي التدفقات وتتبع الاتجاهات المؤسسية.



**المصدر:** <http://www.euromonitor.com>

**Enuromonitor** يوفر البحوث الاستراتيجية بالنسبة للأسوق الاستهلاكية. وهي تنشر تقارير عن الصناعات والمستهلكين، والعوامل الديموغرافية. أنه يوفر أبحاث السوق والدراسات الاستقصائية التي تركز على احتياجات مؤسستك.



**المصدر:** <http://www.faganfinder.com>

**FaganFinder** هو عبارة عن مجموعة من أدوات الإنترنت. بل هو دليل لمواقع المدونات (blog sites)، ومواقع الأخبار، ومحركات البحث، و مواقع مشاركة الصور، و مواقع العلوم والتعليم، الخ. يحتوي على أدوات متخصصة مثل الترجمة ومعالج المعلومات URL والتي توفر للعمور على معلومات حول مختلف الإجراءات مع صفحة الويب.



**المصدر:** <http://www.secinfo.com>

**SEC Info** يقدم خدمة قاعدة البيانات عن المعلومات عن الأوراق المالية والبورصات الأمريكية (SEC) على شبكة الإنترنت، مع المليارات من الروابط التي تصف إلى وثائق SEC. لأنها تتيح لك البحث عن طريق الاسم، الصناعة، والأعمال التجارية، و SIC رمز، رمز المنطقة، رقم الملف، CIK، الموضع، الرمز البريدي، الخ.



**المصدر:** <http://www.thesearchmonitor.com>

**The Search Monitor** يوفر الاستخبارات التنافسية في الوقت الحالي لمراقبة عدد من الأمور. فإنه يسمح لك بمراقبة الحصص السوقية، رتبة الصفحة، نسخة الإعلانية، صفحات الهبوط، وميزانية منافسيك. مع رصد العلامات التجارية، يمكنك مراقبة شركتك وكذلك العلامة التجارية لمنافسك ومع جهاز العرض التابع لها، يمكنك مشاهدة الشاشة الإعلانية ونسخة من الصفحة المقصودة.

## الاستخبارات التنافسية معرفة آراء الخبراء حول شركة ما (WHAT EXPERT OPINIONS SAY ABOUT THE COMPANY?)



**المصدر: Copernic** هو تطبيق لتنبيه البرمجيات. تعمل على مراقبة مواقع الويب الخاصة بالمنافسين بشكل مستمر وبلغتك بأي تغييرات في المحتوى عبر البريد الإلكتروني، إن وجدت. يسلط الضوء على الصفحات التي تم تحديدها فضلاً عن التغييرات التي أدخلت على الموقع حسب ما تريده. يمكنك مشاهدة الكلمات الرئيسية المحددة، لمعرفة التغييرات التي تم إجراؤها على موقع منافسيك.

### SEMRush

**المصدر: SEMRush** هو موقع ويب للبحث عن الشركات المنافسة. لأي موقع، يمكنك الحصول على قائمة من الكلمات الرئيسية المسجلة لموقع جوجل وAdWords، أما هنا يمكنك الحصول على قائمة المنافسين في نتائج بحث جوجل. الوسائل الضرورية لاكتساب المعرفة المتعمقة حول ما يقوم به المنافسين من الدعاية وتخصيص ميزانية لتكلّبات التسويق عبر الإنترنت يتم توفيرها من قبل SEMRush.

### Jobitorial

**المصدر: Jobitorial** يسمح للموظفين المجهولين من رؤية ما تم نشره عن الوظائف لآلاف الشركات ويسمح لك أيضاً بمراجعة الشركة.

### AttentionMeter

**المصدر: AttentionMeter** هو أداة تستخدم لمقارنة أي موقع تريده (traffic) باستخدام compete، Alexa، QuantCast، وQuantCast. أنها تعطيك لقطة عن حركة البيانات وكذلك الرسوم البيانية من Compete، Alexa، QuantCast، وQuantCast.

### ABI/INFORM Global

**المصدر: ABI/INFORM Global** هو قاعدة بيانات الأعمال. يقدم أحدث المعلومات التجارية والمالية للباحثين على جميع المستويات. مع ABI/INFORM Global، يمكن للمستخدمين تحديد ظروف العمل، تقييمات الإدارة، الاتجاهات التجارية، ممارسة الإدارة ونظرية واستراتيجية وتكلّبات الشركات، والمتهد التفاصي.

### Compete PRO

**المصدر: Compete PRO** يوفر خدمة الاستخبارات التنافسية على الإنترنت. فهو يجمع بين كل موقع، وبحث، وتحليل في منتج واحد.



## 5-عملية الاستطلاع باستخدام جوجل(FOOTPRINTING USING GOOGLE)

على الرغم من أن جوجل هو عبارة عن محرك بحث، فإن عملية الاستطلاع (**Footprinting**) باستخدام جوجل ليست متابعة لعملية الاستطلاع (**Footprinting**) من خلال محركات البحث. لقد أتيت جوجل ليكون واحداً من أفضل وأشمل محركات البحث حتى الآن. حيث أصبح **violently spider websites**، وذلك لعرضه معلومات حساسة من غير قصد عن موقع ما على شبكة الإنترنت وذلك نتيجة الاعداد الخاطئ لمختلف خوادم/ملفات الويب (مثل فهرسة الدليل). مثل هذه النتائج تعرض كميات هائلة من البيانات التي تسرب إلى شبكة الإنترنت، وأسواً من ذلك، أنا هذه النتائج تخزن في **google cache**. في أوائل عام 2000، أُنجب حقل جديد، وهو قرصنة جوجل. قرصنة جوجل [**google hack**] قدم للمرة الأولى من قبل جوني لونج، الذي نشر بضعة كتب حول هذا الموضوع، مثل كتاب **Google Hacking for Penetration Testers** للكاتب جوني لونج [**Johnny Long**]. الفكرة العامة وراء قرصنة جوجل هو استخدام معاملات بحث متقدمة في محرك البحث جوجل لتضييق نتائج البحث والعنور على ملفات محددة للغاية، وعادةً مع صيغة معروفة. يمكنك أن تجد معلومات الاستخدامات الأساسية هنا:

<https://support.google.com/websearch/answer/134479?hl=en>

**ملحوظة:** يقوم جوجل بفلترة الاستخدام المفرط لمتغل البحث المتقدم ويقوم بخفض الطلبات (**request**) بمساعدة نظام الوقاية من الاختراق.

### عملية الاستطلاع باستخدام تقنية قرصنة جوجل FOOTPRINTING USING GOOGLE HACKING TECHNIQUES

قرصنة جوجل (**Google Hacking**) هو فن إنشاء عمليات بحث متقدم من خلال محرك البحث جوجل عن طريق استخدام صيغ محددة (**google operator**) وذلك للعثور على التغيرات الأمنية في ملفات الإعداد وأكواد الكمبيوتر التي تستخدمها المواقع. إذا استطعت بناء الاستعلامات المناسبة، فإنه يمكنك الحصول على بيانات قيمة حول الشركة المستهدفة من نتائج بحث جوجل. من خلال عملية قرصنة جوجل، فأنت المهاجم يحاول العثور على الموقع الذي هي عرضة للعديد من الماكر ومواطن الصحف. هذا يمكن أن يتحقق مع مساعدة من قواعد بيانات قرصنة جوجل (**GHDB**)، وقواعد البيانات الخاصة بالاستعلام لتحديد البيانات الحساسة. متغلب جوجل تساعده في العثور على النص المطلوب وتتجنب البيانات التي لا صلة لها بالموضوع. باستخدام متغلب جوجل المتقدم، فأنت المهاجمين يمكنهم تحديد موقع جملة محددة من النص مثل إصدارات معينة من تطبيقات الويب الصحفية.

#### متغلب جوجل المتقدم [**advanced google operator**]:

لحسن الحظ بالنسبة لنا، يوفر جوجل بعض التعبيرات التي هي سهلة الاستخدام والتي تساعدنا في الحصول على أقصى استفادة من عملية البحث. هذه التوجيهات هي الكلمات الرئيسية التي تمكنا من استخراج معلومات أكثر دقة من فهرس جوجل.

متغلب البحث المتقدم تسمح لك بتضييق عملية البحث الخاص بك حتى تصل إلى النقطة التي يتم فيها تحديد الهدف الذي كنت تبحث عنه بالضبط، ويمكن الاطلاع على قائمة متغلب جوجل في جوجل:

<http://support.google.com/websearch/bin/answer.py?hl=en&answer=136861>

باستخدام هذه العوامل، يمكنك البحث عن المعلومات المحددة التي قد تكون ذات قيمة خلال اختبار الاختراق. دعونا نحاول في بعض الأمثلة البسيطة للحصول على نتائج دقيقة.

**النظر في المثال التالي:** افترض أنك تبحث عن معلومات عن موقع جامعة ولاية داكوتا (**dsu.edu**) عن شخص ما. أبسط طريقة لأداء هذا البحث هو إدخال المصطلحات التالية (دون أي علامات اقتباس) في مربع البحث جوجل: **[pat engebretson dsu]** هذا البحث سوف يسفر عن عدد لا يأس به من النتائج. لكن تجد من خلال أول 50 نتائج بحث يوجد أربعة نتائج فقط تم انتقالها من موقع (**dsu.edu**) مبابرة. من خلال الاستفادة من **متغلب جوجل (توجيهات "directive")**، فنحن يمكن أن نجبر مؤشر جوجل للقيام بالخطوات التي تريدها. في المثال أعلاه نحن نعرف كل من الموقع الهدف والكلمات الرئيسية التي تريدها. بشكل أكثر تحديداً، نحن مهتمون بإيجار جوجل بالعودة بالنتائج الوحيدة التي يتم سحبها مباشرةً من الموقع الهدف (**dsu.edu**). في هذه الحالة، أفضل خيار لدينا هو الاستفادة من التوجيه/التعبير [**site:**]. باستخدام هذا التعبير فنحن نجبر جوجل على العودة فقط بالنتائج التي تحتوي على الكلمات الرئيسية التي استخدمناها وتأتي مباشرةً من الموقع المحدد.

لاستخدام توجيهات/توجيهات متغلب جوجل بشكل صحيح، تحتاج إلى ثلاثة أشياء:

1. اسم التوجيه الذي تريده استخدامه.

2. **القولون (:).**

3. المصطلح الذي تريده استخدامه في التوجيه.

بعد إدخال الثلاث قطع من المعلومات الواردة أعلاه، يمكنك البحث كما تفعل عادةً لاستخدام التوجيه "**site:**"، فنحن بحاجة إلى إدخال ما يلى في مربع بحث جوجل:

**site:dsu.edu pat engebretson**

نلاحظ أنه لا توجد مسافة بين التوجيه والقولون، واسم الدومنين. في مثالنا السابق أردنا إجراء بحث عن **pat engebretson** في موقع الويب **dsu.edu**. لإنجاز هذا، فإننا ندخل الأمر السابق في سريط البحث جوجل.

### ماذا يمكن أن يفعل الهاكر مع استخدام قرصنة جوجل؟

إذا كان الموقع المستهدف هو عرضة للقرصنة جوجل، فإن المهاجم يجد المعلومات التالية مع مساعدة من الاستعلامات في قاعدة بيانات قرصنة جوجل:

- رسائل الخطأ التي تحتوي على معلومات حساسة
- الملفات التي تحتوي على كلمات السر
- المجلدات الحساسة
- الصفحات التي تحتوي على بوابات الدخول
- الصفحات التي تحتوي على بيانات التباكي أو الضعف
- تحذيرات ونقاط الضغط الخادم

## GOOGLE ADVANCE SEARCH OPERATORS

المصدر: <http://www.googleguide.com>

[استعلام **cache**:] يعرض نسخة جوجل (**Google's cached version**) من صفحة الويب، بدلاً من الإصدار الحالي من الصفحة. يعني آخر للحد من نتائج البحث ويظهر المعلومات فقط التي سحبها مباشرةً من ذاكرة التخزين المؤقت لجوجل. على سبيل المثال: [cache:www.eff.org](http://cache:www.eff.org).

**ملاحظة:** لا تضع مسافة بين عنوان URL وبين (cache:).

[**link**:] يعمل على سرد صفحات الويب التي تحتوي على الروابط المحددة لصفحة الويب. على سبيل المثال، للبحث عن الصفحات التي تشير إلى الصفحة الرئيسية ل **Google Guide's**، أدخل الآتي: [link:www.googleguide.com](http://link:www.googleguide.com). هذا يعني أنه سوف يسرد لك جميع صفحات الويب الذي تحتوي على لينكات أو روابط للموقع [www.googleguide.com](http://www.googleguide.com).

**ملاحظة:** ووفقاً لتوصي غوغل، "لا يمكنك الجمع بين بحث (**link**) مع كلمات البحث العادية". نلاحظ أيضاً أنه عند الجمع بين (**link**) مع معاملات البحث المتقدم الأخرى، فإن جوجل قد لا ترجع كافة الصفحات التي تتطابق. الاستعلامات التالية يجب أن تعود بالكثير من النتائج، إذا قمت بإزالة المعامل (**-site:**) من هذه الاستعلامات.

[**related:**] إذا قمت بتشغيل الاستعلام الخاص بك مع "**related:**" ، فإن جوجل يعرض الموقع المماثلة إلى الموقع المذكور في استعلام البحث. مثال: [related:www.microsoft.com](http://related:www.microsoft.com).

[**info:**] سوف يقدم لك بعض المعلومات عن صفحة الويب. على سبيل المثال، [info:gothotel.com](http://info:gothotel.com) سوف تظهر معلومات حول دليل الفنادق للصفحة الرئيسية [GotHotel.com](http://GotHotel.com).

**ملاحظة:** يجب ألا يكون هناك مسافة بين (**info**) و URL صفحة ويب. كما يمكن الحصول على هذه الوظيفة عن طريق كتابة URL في صفحة الويب مباشرةً في مربع البحث جوجل.

[**site:**] إذا قمت باستخدام (**site:**) في الاستعلام الخاص بك ، فإن جوجل سوف تعمل على تقييد نتائج البحث للموقع أو الدومنين الذي تحدده على سبيل المثال، [site:www.lse.ac.uk](http://site:www.lse.ac.uk) هذا سوف يظهر لك معلومات القبول في كلية لندن للاقتصاد و [peace site:gov](http://peace site:gov) سوف يجد الصفحات عن السلام داخل الدومنين (**gov**). يمكنك تحديد الدومنين مع أو بدون **period**، على سبيل المثال، إما (**gov.**) أو (**gov.**) .

**ملاحظة:** لا تضع مسافة بين "site:" والدومنين.

[**allintitle:**] إذا قمت بتشغيل الاستعلام الخاص بك مع **allintitle** ، فإن جوجل يقود النتائج إلى تلك التي تحتوي على كل سروط الاستعلام الذي تم تحديده في العنوان.

على سبيل المثال، (**allintitle: detect plagiarism**) فإن هذا سوف يعود بالنتائج الوحيدة التي تحتوي على الكلمات **detect** و **plagiarism** في العنوان. كما يمكن الحصول على هذه الوظيفة من خلال صفحة الويب للبحث المتقدم، ضمن **Occurrences**.

[**inttitle:**] على سبيل المثال (**inttitle:term**) فإن هذا سوف يقود النتائج إلى المستندات التي تحتوي على المصطلح **term** في العنوان.

**ملاحظة:** يجب ألا يكون هناك مسافة بين **inttitle:** والكلمة التالية.

[**allinurl:**] إذا قمت بتشغيل الاستعلام الخاص بك مع **allinurl**: فإن جوجل يقود النتائج إلى تلك التي تحتوي على كل مصطلحات الاستعلام الذي تحدده في URL .

على سبيل المثال، (**allinurl: google faq**) فان هذا سوف يعود إليك بالوثائق الوحيدة التي تحتوي على الكلمات "google" و "faq" في عنوان URL ، مثل ([www.google.com/help/faq.html](http://www.google.com/help/faq.html)) هذه الوظيفة يمكن أيضا الحصول عليها من خلال صفحة الويب للبحث المتقدم، ضمن الموارد (Occurrences).

في عذريين الموقع **URL** ، غالبا ما يتم تشغيل الكلمات معا. ولكن لا تحتاج أن تدار معا عندما تستخدم **allinurl:[inurl:]** إذا قمت بتضمين **inurl:** في طلب الاستعلام الخاص بك ، فإن جوجل سوف تقييد النتائج إلى المستندات التي تحتوي على تلك الكلمة في عنوان **URL** .

على سبيل المثال، (**inurl:print site:www.googleguide.com**) فان هذا سوف يبحث عن الصفحات في موقع **googleguide** على العنوانين التي تحتوي على كلمة "print". إنها تحد ملفات **PDF** التي هي في الدليل أو في المجلد المسمى "print" على موقع الويب **googleguide**. [ **inurl:healthy eating**] أن عملية الاستعلام هذه سوف تعود إليك بالوثائق التي تحتوي على الكلمة **healthy** في عنوانها والتي تحتوي على الكلمة **eating** في أي مكان داخل الورقة. ملحوظة: لا يوجد مسافة بين المصطلح **inurl:** والكلمة التي تليها.

[**filetype:**] يمكننا الاستفادة من هذا التوجيه في البحث عن ملف معين داخل موقع الويب. هذا مفید للغاية للعثور على أنواع معينة من الملفات على موقع الويب الخاصة بالهدف. على سبيل المثال، للعودة الفاعلة بالنتائج الوحيدة التي تحتوي على وثائق **PDF** ، ويوجد تغيير آخر مشابه له وهو [**ext:**] بحيث يوضع بعده الامتداد المطلوب البحث عنه. ونستخدم التغيير التالي:

**filetype:pdf ext:pdf**

[**intext:**] هذه تقييد إلى تقييد نتائج البحث بحيث تحتوي على الكلمات الرئيسية الموجودة في **.txt**. هناك العديد من أنواع التوجيهات الأخرى الخاصة بقرصنة جوجل التي يجب عليك أن تصبح معهاداً عليها. جنباً إلى جنب مع جوجل، فمن المهم أن تصبح فعالة مع العديد من محركات البحث الأخرى أيضاً في كثير من الأحيان، فإن محركات البحث المختلفة تحطى نتائج مختلفة حتى عند البحث عن نفس الكلمات الرئيسية. تجدر الإشارة إلى أن عمليات البحث هذه تكون في الوضع **Passive Footprinting** فقط طالما كانت تبحث عنه. بمجرد إجراء اتصال مع النظام الهدف (من خلال النقر على أي من الروابط)، تعود إلى الوضع **active**. يجب أن تكون على علم بأن استطلاع الأنشطة دون إذن مسبق من المرجح أنه غير قانوني.

## FINDING RESOURCES USING GOOGLE ADVANCE OPERATOR

باستخدام تغييرات جوجل المتقدمة مثل [**intitle:intranet inurl:intranet +intext:"human resources"**] فان المهاجم يمكنه العثور على معلومات خاصة عن الشركة المستهدفة وفي بعض الأحيان معلومات حساسة حول موظفي تلك الشركة بالذات. المعلومات التي تم جمعها من قبل المهاجمين يمكن استخدامها لتنفيذ هجمات الهندسة الاجتماعية. إن محرك جوجل سوف يعمل على فلترة الاستخدام المفرط للمتغلب البحث المتقدم وسوف ينخفض الطبيات بمساعدة نظام منع الاختراق.

الشكل التالي يظهر صفحة نتائج محرك البحث جوجل المتقدم بعرض نتائج الاستعلام التي سبق ذكرها:

The screenshot shows a Google search results page with the query **[intitle:intranet inurl:intranet +intext:"human resources"]**. The results are as follows:

- Kellogg Faculty & Staff Intranet - Kellogg School of Management**: A link to [www.kellogg.northwestern.edu/intranet/facstaff.htm](http://www.kellogg.northwestern.edu/intranet/facstaff.htm). Description: "Human Resources & Benefits · Staff Resources · Onboarding Resources · Kellogg @ Work Quarterly staff newsletter · Directions & Maps · Fitness & Recreation".
- Human Resources Intranet**: A link to [hr.intranet.unchealthcare.org/](http://hr.intranet.unchealthcare.org/). Description: "This section of the Human Resources website is for UNC Health Care employees only. Employees must enter their system userid and password to continue."
- HR Intranet | Human Resources | Vanderbilt University**: A link to [hr.vanderbilt.edu/hr.intranet](http://hr.vanderbilt.edu/hr.intranet). Description: "Vanderbilt University Human Resources ... SharePoint Links · Human Resources · JCAHO · Service Delivery Teams · Helpful Links · Don't like your middle initial ...".
- Human Resources : CLA Intranet - University of Minnesota**: A link to [cla.umn.edu/intranet/](http://cla.umn.edu/intranet/). Description: "... Resources · Who Do I Contact in CLA HR? 2013/14 Deadlines in Faculty & Human Resources · OHR Manager's Toolkit · CLA NOW Blog · CLA NOW Calendar ...".
- Human Resources | Intranet - University of Hawaii**: A link to [www.hawaii.edu/intranet/](http://www.hawaii.edu/intranet/).

بمجرد الوصول الى صفحة الويب الهدف عن طريق إجراء عمليات تفتيش شاملة باستخدام جوجل ومحركات البحث الأخرى، فمن المهم استكشاف زوايا أخرى من الإنترنت. مجموعات الأخبار ونظام لوحة الإعلانات **Bulletin Board Systems** [BBS] مثل **UseNet** و**Google Group** يمكن أن تكون مفيدة جداً في جمع المعلومات عن الهدف.

**ملحوظة: نظام لوحة الإعلانات (BBS)** هو نظام حاسوبي يعمل من خلال برنامجه يمكن المستخدمين من الاتصال والدخول إلى النظام باستخدام المحطة الطرفية. عند الدخول إلى النظام، يستطيع المستخدم تنفيذ عمليات مثل تحميل وارسال البرامج أو البيانات كذلك يستطيع المستخدم قراءة الأخبار والنشرات وتبادل الرسائل مع المستخدمين الآخرين.

ليس من المأثور للناس استخدام مجالس المناقشة هذه لإرسال وتلقي المساعدة في المسائل التقنية. لأسف (أو لحسن الحظ، اعتماداً على أي جانب من العملة تبحث فيها)، حيث في كثير من الأحيان يقوم الموظفين بإضافة أسئلة مفصلة جداً بما في ذلك المعلومات الحساسة والسرية. على سبيل المثال، وضع في الاعتبار مسؤول الشبكة [admin] الذي وجود صعوبة في إعداد جدار الحماية بشكل صحيح. حيث ليس من المأثور أن تشهد في المجالس في المنتديات العامة حيث سيتم نشر ملفات الأعداد الخاصة بهم. لجعل الأمور أسوأ، وكثير من الناس يقوموا باستخدام عنوان البريد الإلكتروني الخاصة بالشركة التي يعملون بها. هذه المعلومات هو منجم ذهب بالنسبة للمهاجمين. حتى لو كان مشرف الشبكة هذا يتميز بالذكاء والحرص بما فيه الكفاية عن طريق عدم نشر ملفات الأعداد الخاصة بهم، حيث إنه من الصعب الحصول على دعم من المجتمع دون تسرّب بعض المعلومات دون قصد. لذلك سوف تقرأ بعناية المشاركات الخاصة به [posts] التي كثيرة ما تكتفى بإصدار محدد من البرمجيات، ونماذج الأجهزة ومعلومات الأعداد الحالي، وما شابه ذلك حول الأنظمة الداخلية. يجب تقدير كل هذه المعلومات بعيداً لاستخدامها في المستقبل.

المجالس العامة هي وسيلة ممتازة لتبادل المعلومات والحصول على المساعدة التقنية. ومع ذلك، عند استخدام هذه الموارد، يجب أن تتوخي الحذر وذلك عن طريق استخدام عنوان البريد الإلكتروني المجهولة مثل **Gmail** أو **هوتamil**، بدلاً من عنوان الشركة. النمو الهائل في وسائل الإعلام الاجتماعية مثل الفيس بوك، ماي سبيس، وتويتر يوفر لنا آفاقاً جديدة لبيانات الألغام حول أهدافنا. عند تنفيذ الاستطلاع، فإنها فكرة جيدة لاستخدام هذه الواقع لصالحتنا. النظر في المثال التالي: تقوم بإجراء اختبار الاختراق ضد شركة صغيرة. وقد أدى هذا الاستطلاع ليكتشف لك أن مسؤول الشبكة للشركة لديه حساب تويتر وفيسبوك.

مع الاستفادة من الهندسة الاجتماعية فيمكنك إقامة علاقات صداقه معهم وتقديم تتبّعهم على حد سواء في الفيسبوك وتويتر. بعد بضعة أسابيع من المشاركات المماثلة، يحدث أنه يكتب مثلاً على الفيسبوك "الجدار الذاري توفي دون سابق إنذار اليوم. وواحدة جديدة يتم إعدادها خلال الليل. يبدو أنني سوف أجلس الليل كله لإعادة الأمور إلى وضعها الطبيعي". ومن ثم "انتهيت للتو من عملية الميزانية السنوية. يبدو أنني على دعم خادم **server 2000** لمدة عام آخر". من هذا نرى كمية المعلومات التي يمكن أن تجمعها ببساطة عن طريق رصد ما تم نشره من قبل الموظفين على الانترنت.

## ما هو اليوزنت "USENET"

الجدير بالذكر أن المجالس والشبكات الاجتماعية الموجودة الان والمنتشرة بشكل كبير وواسع ما هي إلا تطوير وتحديث لتلك التقنية العصرية. كانت هذه الفكرة من بنات أفكار السباب توم تراسكوت وجيم إليس خريجي جامعة ديوك وظهرت للعالم سنة 1980 لكن ما هو اليوزنت وما فائدته؟ تستطيع أن تقوم بإضافة مقالات وتعليقات في مجتمع أو شبكة اليوزنت وهو ما يسمى بشكل عام الأخبار فكل مقال في شبكة اليوزنت هو عبارة عن خبر ويتم تصنيفه على شكل تصنيفات أو أقسام تسمى مجموعات الأخبار **newsgroups**. تعد اليوزنت من أقدم شبكات الحاسوب والاتصالات وما زالت موجودة حتى الان وقد ظهرت قبل ظهور الشبكة العالمية والانتشار بها بحوالى عشرة سنوات تقريباً. ولكن ما هي **newsgroups** أو مجموعات الأخبار؟ هي بكل بساطة مجموعات نقاش مثل المجالس التي تستخدم للنقاش بين الأعضاء من مختلف الأماكن الموجودة الان على الشبكة العالمية. تقسم مجموعات الأخبار تلك إلى تistani مجموعات رئيسية تسمى **Big Eight**. وليس معنى هذا عدم وجود مجموعات أخرى، بل يوجد مجموعات أخرى بلغات مختلفة غير الإنجليزية وأيضاً يوجد مجموعة أخرى تسمى **alt**. وسوف نعرض تلك المجموعات التمانية وتعريف لكل واحدة على حدة.

**Comp**: تهتم تلك المجموعة بالمواضيع الخاصة بالكمبيوتر من برامج وغيرها.  
**Humanities**: تهتم بالأدب والفلسفة والتصميمات أي أنها مجموعة متخصصة في الفن.

**Misc**: هذه المجموعة ليس لها شيء محدد فهي تهتم بمواضيع متنوعة عن التعليم والأطفال وغيرها.

**News**: كما نفهم من اسمها فهي تهتم بالأخبار ولكن ليست أخبار عادية فهي تهتم بأخبار النقاشات والآحداث الجديدة عن المجموعات.

**Rec**: خاصة بالتسليه والترفيه من أفلام ومسلسلات.

**Sci**: تضم النقاشات الخاصة بالعلوم والابحاث العلمية.

**Soc**: الاجتماعيات والثقافات المختلفة الموجودة في المجتمع.

**Talk**: تضم نقاشات حول السياسة والدين والمنشئ.

## قرصنة جوجل: قاعدة بيانات قرصنة جوجل (GHDB) (GOOGLE HACKING DATABASE)

المصدر: <http://www.hackersforcharity.org>

هذا المئات (إن لم يكن الآلاف) من عمليات البحث متيره للاهتمام التي يمكن تقديرها. يتم سرد العديد منهم في قسم "قرصنة جوجل" في قاعدة بيانات **GHDB Exploit** تعمل على تنظيم عمليات البحث في فئات مثل **password** و **Username**، وحتى على حسب معدلات البحث كل شهر. يرجى أخذ الوقت الكافي لزيارة هذا الموقع، وإذا كان هذا الموضوع متير بالنسبة لك (فأنه يعني!), النظر في كتاب **Google Hacking for Penetration Testers** الطبعة الثانية.

قاعدة بيانات قرصنة جوجل (**GHDB**) هي قاعدة بيانات تحتوي على عدد كبير من الاستفسارات (تعديلات الاستعلام) التي تحدد البيانات الحساسة. **GHDB** هو تطبيق مجمع بين **HTML** و **جافا سكريبت** التي تستخدم تقنيات متقدمة من الجافا سكريبت والتي أنشئت من قبل **Johnny Long** (قرصان للأعمال الخيرية)، ويوجد في [ <http://www.hackersforcharity.org/ghdb/> ].

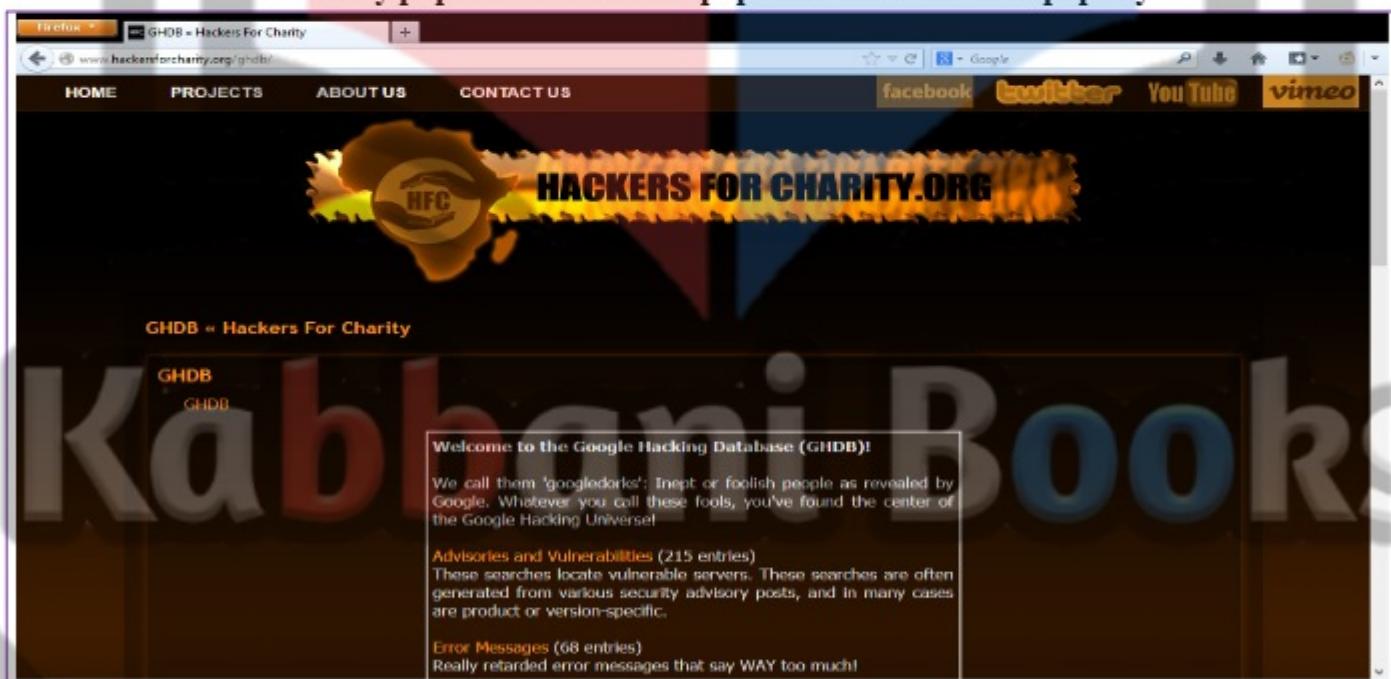
**Offensive Security** يحتوى هو الآخر على **GHDB** في

<http://www.offensive-security.com/community-projects/google-hacking-database/>

لقد تم الدمج بين **GHDB** مع قاعدة بيانات **Exploit database**. **Exploit** **database** على نقاط الضعف في الخوادم/السيرفرات عن طريق **جوجل**

كل بضعة أيام، توجد نقاط ضعف لتطبيق ويب جديد. كثيرا ما يمكن استخدام جوجل لتحديد الخوادم/السيرفرات الضعيفة. على سبيل المثال، في فبراير 2006، تم العثور على ثغرة في **phpBB** ( منتدى مفتوح المصدر للبرمجيات). فقمت القرصنة باستخدام جوجل للتعرف على وجه السرعة على جميع الموقع الموجودة على شبكة الإنترنت التي تستخدم **phpBB** لاستهدافها. قراءة المزيد عن الضعف / استغلال هنا: <http://www.exploit-db.com/exploits/1469/>

"Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"



## الأدوات الأخرى المستخدمة في قرصنة جوجل

بجانب استخدام أداة قواعد بيانات قرصنة جوجل (**GHDB**) التي تم ذكرها في السابق، فإن هناك بعض الأدوات الأخرى التي يمكن أن تساعدك مع قرصنة جوجل. هناك عدد من أكثر أدوات قرصنة جوجل المذكورة على النحو التالي. باستخدام هذه الأدوات، يمكن المهاجمين جمع التحذيرات ونقطات الضعف لخادم ما، معلومات رسالة الخطأ التي قد تكشف عن مسارات الهجوم للملفات الحساسة، الأدلة، بوابات الدخول [**gateway**][\[1\]](#)، وأكثر من ذلك.

ملحوظة: محرك البحث جوجل لا يسمح بتطبيق عملية البحث باستخدام التطبيقات المختلفة لذلك عند استخدام هذه التطبيقات يرجى تجديتها أما بنج فلا يمنع ذلك.



## Metagoofil ▪

[المصدر:](http://www.edge-security.com) **Metagoofil**

هو أداة لجمع المعلومات مصممة لاستخراج البيانات الوصفية (**metadata**) من الوثائق العامة التابعة للشركة الهدف. (**Pdf, doc, xls, ppt, docx, ppx, xlsx**)

**Metagoofil** ينفذ عملية البحث في جوجل لتحديد وتحميل المستندات إلى القرص المحلي ثم استخراج البيانات الوصفية عن طريق ملفات المكتبات المختلفة (**libraries**) مثل **PdfMiner?**, **Hachoir**, **libraries** وغيرها. مع النتائج، فإنه يولد تقريراً يتضمن أسماء المستخدمين، إصدارات البرامج، والخواص أو أسماء الآلة التي قد تساعد في اختبار الاختراق في مرحلة جمع المعلومات.

## Goolink Scanner ▪

[المصدر:](http://www.ghacks.net)

**Goolink Scanner** يزيل ذاكرة التخزين المؤقت (**cache**) من عمليات البحث الخاصة بك، ويجمع وعرض روابط الموقع التي تحتوى على نقاط ضعف فقط. وبالتالي، فإنه يسمح لك لإيجاد المواقع المعرضة للخطر مفتوحة على متصفحها **google** و **googlebots**.

## SiteDigger ▪

[المصدر:](http://www.mcafee.com)

**SiteDigger** يبحث في الذاكرة الموقتة لجوجل (**Google's cache**) ليجد نقاط الضعف ، والأخطاء ، وقضايا الإعداد والمعلومات الشخصية، و شدرات الأمان المتيرة للاهتمام على موقع الانترنت.

## Google Hacks ▪

[المصدر:](http://code.google.com)

**Google Hacks** هو تجميع لعمليات بحث جوجل التي تعرض أدوات جديدة من خدمات البحث وخريطة جوجل. فإنه يسمح لك برؤية الجدول الزمني لنتائج البحث الخاصة بك، عرض الخريطة، البحث عن الموسيقى، البحث عن الكتب، تنفيذ العديد من أنواع أخرى محددة من عمليات البحث.

## BILE Suite ▪

[المصدر:](http://www.sensegost.com)

**BILE Suite** من أجل **BILE Suite Bi-directional Link Extractor**. يتضمن **BILE Suite** كل مخطوطة من سكريبتات برمجية المستخدمة في عمليات التعداد. كل مخطوطة من سكريبتات برمجية لديه وظيفة خاصة بها. **BILE.pl** هو الأداة الأولى أو مجموعة سكريبتات برمجية. **BiLE** يمبل على جوجل و **HTTrack** يستخدم لجمع الملفات من وإلى الموقع المستهدف ، تم تطبيق الخوارزميات البسيطة لاستدلال على الموقع الذي تملك أقوى العلاقات مع الموقع المستهدف.

## Google Hack Honeypot ▪

[المصدر:](http://ghh.sourceforge.net)

**Google Hack Honeypot (GHH)** هو رد فعل لنوع جديد من **malicious web traffic: search engine hackers**. هي مصممة لتوفير عمليات الاستطلاع ضد المهاجمين الذين يستخدمون محركات البحث كأداة قرصنة ضد الموارد الخاصة بك. **GHH** تعمل على تطبيق نظرية المصيدة (**honeypot theory**) لتوفير أمان إضافي إلى شبكة الانترنت الخاصة بك.

## GMapCatcher ▪

[المصدر:](http://code.google.com)

**GMapCatcher** هو **offline maps viewer**. فإنه يعرض خرائط للعديد من مزودي الخدمة مثل: **CloudMade**, **maps.py**, **Skyvector**, **Nokia Maps**, **Bing Maps**, **Yahoo Maps**, **OpenStreetMap** الرسمية المستخدمة لتصفح خريطة جوجل. مع الزر **offline toggle** بإزالة الإتارة من عليه (عدم تفعيله)، فإنه يمكن تحميل خريطة جوجل تلقائياً. بمجرد تحميل الملف، فإنه يصبح موجود على القرص الثابت. وبالتالي، لا تحتاج لتحميل البرنامج مرة أخرى.

## SearchDiggity ▪

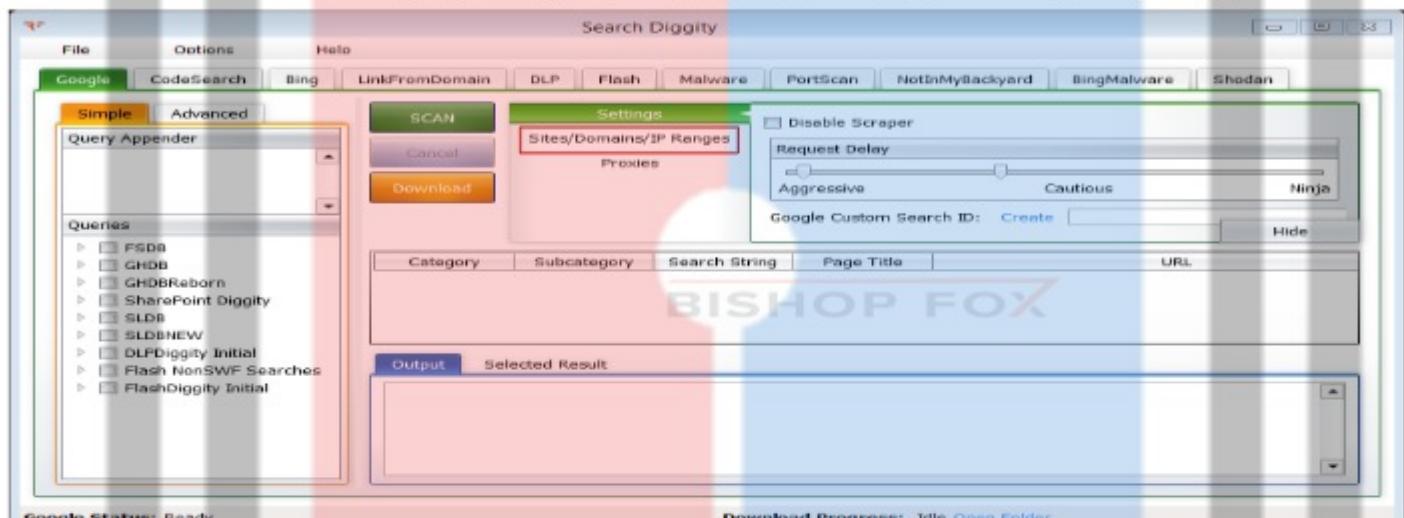
[المصدر:](http://www.stachliu.com)

**SearchDiggity** هو أداة الهجوم الرئيسي للمشروع **Google hacking Diggity**. هو عبارة عن **Stach** وتطبيق **Liu's Diggity** رسميه لمايكروسوفت التي هي بمثابة الواجهة الأمامية لأحدث الإصدارات من أدوات **Diggity** مثل **GoogleDiggity**, **MaIwareDiggity**, **DLPDiggity**, **CodeSearchDiggity**, **LinkFromDomainDiggity**, **Bing-BingDiggity**, **NotInMyBackYard Diggity**, **BingBinaryMalwareSearch**, **SHODANDiggity**, **PortScanDiggity**

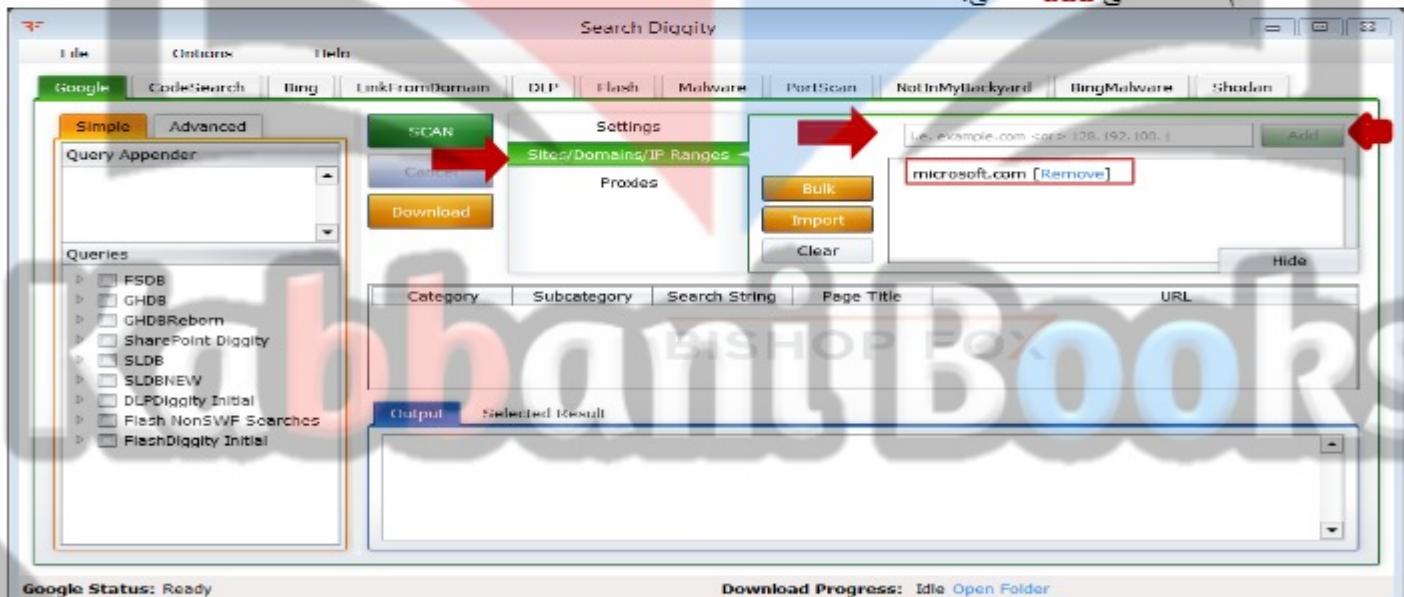
**ملحوظه:** يعتبر هذا الموقع من المواقع التي تعطى أدوات وخبرات في عمليات القرصنة من الطرق السهلة لإيجاد ثغرات المواقع الإلكترونية والتطبيقات هو استخدام جوجل والذي يعتبر من الأدوات السهلة بالنسبة للمهاجم. باستخدام أكواد جوجل في البحث فإنه يمكن المهاجم من إيجاد الثغرات في ملف الكود الخاص بتطبيق معين والذي يدعمه نقطة الدخول الذي يحتاجها لتنفيذ عملية الاختراق واحتراق الوضع الأمني لهذا التطبيق. بما إنك هاكر أخلاقي فإنه يجب عليك استخدام نفس التطبيق لإيجاد الثغرات تم صنع باقش لمعالجة مثل هذه الثغرات.

1- يتم تنبيه البرنامج عن طريق **wizard** الخاص به

2- تم يتم تشغيله فظهور الشاشة التالية ونلاحظ أنها في الوضع الافتراضي وهو **google**



3- نختار التعبير **Sites/Domains/IP Ranges** فظهور مربع حواري تدخل فيه اسم الدومن ولتكن مثلا **microsoft.com** تم نضغط على **add** كالتالي:



4- تم بعد ذلك نذهب إلى القائمة الموجودة في الجانب الأيسر واختيار نوع الطلب الذي تريد البحث عن ولتكن مثلا **SWF Finding Generic** تم نختار **SCAN** فظهور ناتج البحث وهو عباره عن جميع عناوين **URL** في الدومن **microsoft.com** والتي تحتوي على ملفات **SWF**.

#### Google HACK DB

المصدر: <http://www.secpoint.com>

يمكن للمهاجم أيضا استخدام الأداة **SecPoint Google HACK DB** لتحديد المعلومات الحساسة عن موقع الهدف. هذه الأداة تساعد المهاجم على استخراج الملفات التي تحتوي على كلمات السر، ملفات قواعد البيانات، ملفات تصدير واضحة، ملفات قاعدة بيانات العملاء، وما إلى ذلك.



Gooscan

<http://www.darknet.org.uk>

**Gooscan** هو أداة تعمل على إنشاء استفسارات بطريقه أليه ضد تطبيق بحث جوجل. وقد صممت هذه الاستعلامات للعثور على التغرات المحتملة على صفحات الويب

• محوّلات البحث الأخرى

من الواضح أن هناك محركات بحث أخرى وبصرف النظر عن جوجل، يمكنك الاطلاع على قائمة لطيفة من محركات البحث الأخرى، وقدرات يحتملها من خلال هذا الرابط.

<http://www.searchengineshowdown.com/features/>

يوجد محرك بحث الذي استولت وظيفة على انتباهي وهي قدرات البحث عن عناوين لا IP وهذا المحرك هو [gigablast.com](http://gigablast.com). يمكن أن تبحث عن محتوى على شبكة الإنترنت من خلال عنوان IP. هذا يساعد في تحديد **load balancer**، دومين إضافي، وهلم جرا.اكتشف مؤخرًا أن محرك البحث MSN يدعم هو الآخر قدرات البحث عن عناوين لا IP عن طريق استخدام الصيغة [ip:search word].

## 6- عمليات الاستطلاع باستخدام (WHOIS FOOTPRINTING) WHOIS

جمع المعلومات المتعلقة بالشبكة مثل معلومات **WHOIS** عن موقع المنظمة المستهدفة يعتبر مهم جدا عند قرصنة النظام. لذلك، والآن سوف نناقش عمليات الاستطلاع باستخدام **WHOIS**.

(WHOIS LOOKUP) WHOIS پخت

**WHOIS** هو بروتوكول استعلام و استجابة. يستخدم للاستعلام عن بيانات المستخدمين المسجلين أو موارد الإنترنت المسجلة ، مثل اسم الدومين ، عنوان IP ، أو نظام الحكم الذاتي.

**WHOIS** هو عبارة عن قواعد بيانات أنشئت بواسطة مهندسي الشبكة المحلية وتحتوي على معلومات شخصية عن أصحاب الدومين. تتم المحافظة على قواعد بيانات **WHOIS** من قبل سجلات الإنترنت الإقليمية. أنها تحفظ سجل يسمى **جدول البحث (LOOKUP table)** الذي يحتوى على كافة المعلومات المرتبطة بالشبكة، الدومين والعميل (**host**). يمكن لأى شخص الاتصال والاستعلام من قبل هذا الخادم (**server**) للحصول على معلومات عن التبيكات، على وجه الخصوص، الدومين، والمضيفين(**hosts**). يتم الاتصال على قاعدة بيانات السجل المركزي لا **whois** بواسطة **InterNIC**. وعادة ما يتم نشر هذه البيانات من قبل خادم الإحصائيات **whois** عبر منفذ **TCP 43** والتي يمكن الوصول إليها باستخدام برنامج **whois**.

يمكن للمهاجم إرسال استعلام إلى خادم WHOIS للحصول على المعلومات حول اسم الدومين المستهدف، وتفاصيل الاتصال عن صاحبها وتاريخ انتهاء الصلاحية، وتاريخ الإنتقاء، وما إلى ذلك. خادم WHOIS سيستجيب إلى الاستعلام عن المعلومات ذات الصلة. كل هذه المعلومات يمكن استخدامها لمواصلة عملية جمع المعلومات أو لبدء هجوم الهندسة الاجتماعية.

يمكنه أيضا تنفيذ عمليات البحث العكسي. بدلا من إدخال اسم النطاق/الدومين، يمكنك إدخال عنوان IP. وسوف تشمل عادة نتيجة Whois نطاق التبكّة بأكملها الذي ينتمي إلى المنظمة.

المعلومات التي يوفرها لك WHOIS كالاتي:

- اسم الدومين بالتفصيل.
  - بيانات الاتصال لصاحب الدومين.
  - أسماء سيرفرات الدومين.
  - نطاق الشبكة .NETRANGE
  - المكان الذي أنشاء فيه الدومين.
  - آخر السجالت التي تم تجديتها فيه.

(Regional Internet Registries(RIRs)) WHOIS المنشآت التي تعمل على إنشاء

ARIN

AFRINIC

APNIG

LACNIC

## تحليل نتائج WHOIS LOOKUP

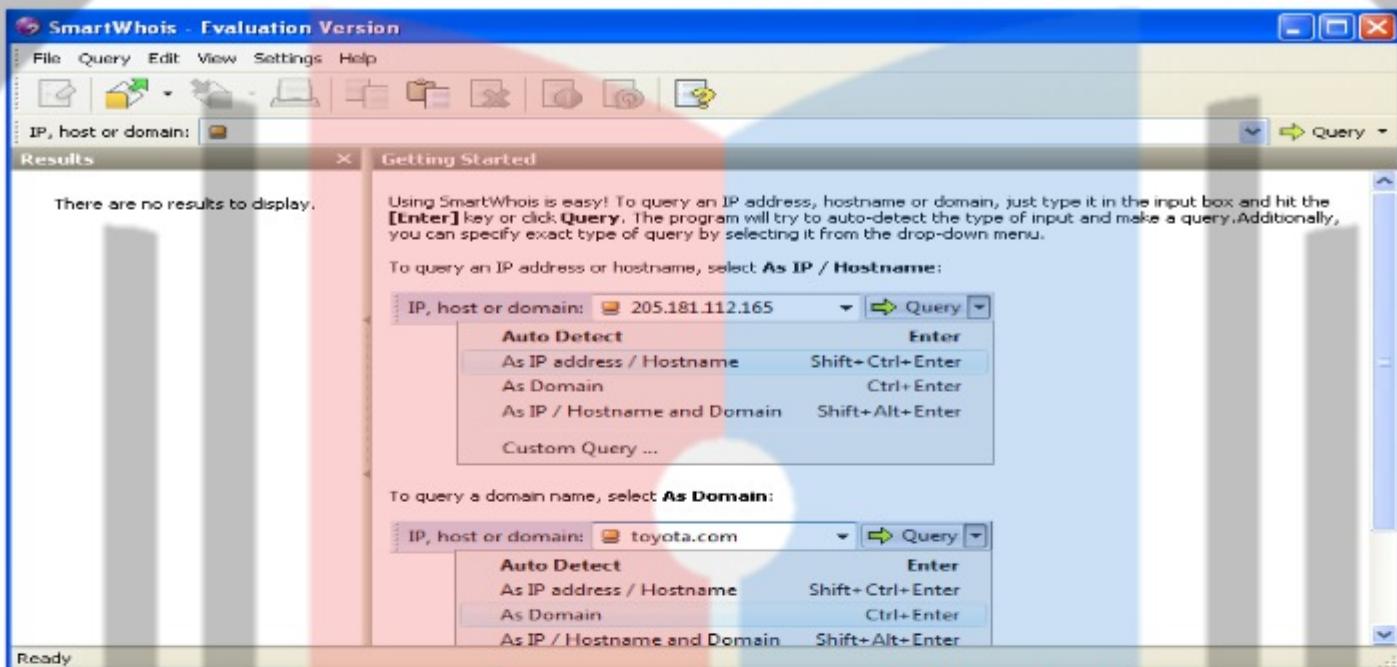
يمكن القيام به باستخدام خدمات **Whois** على شبكة الانترنت مثل **WHOIS Lookup** أو <http://whois.domaintools.com> أو <http://www.ripe.net> أو <http://www.networksolutions.com/whois/index.jsp> أو <http://centralops.net/co>. هنا يمكنك أن ترى ناتج تحاليل نتيجة **WHOIS Lookup** والتي تم الحصول عليها من خلال اثنين من خدمات **WHOIS** المذكورة سابقاً. كل من هذه الخدمات تسمح لك بأداء **WHOIS Lookup** عن طريق إدخال اسم الدومين الهدف أو عنوان IP. خدمة **WHOIS** توفر لك معلومات **domaintools.com** مثل معلومات التسجيل، البريد الإلكتروني، معلومات الاتصال الخالصة بالإداريين (**ADMIN**)، تاريخ الإنقاء وانتهاء الصلاحية، قائمة بسيرفرات الدومين، وما إلى ذلك. ملفات الدومين المتوفرة في <http://centralops.net/co> يعطي لك معلومات مثل عنوان البحث و **domain WHOIS record** و <http://centralops.net/co> وسجلات معلومات DNS.

The image shows two side-by-side screenshots of WHOIS lookup services. On the left is the [domaintools.com](http://whois.domaintools.com) interface, showing detailed registration information for the domain `microsoft.com`, including contact details for Microsoft Corporation and their administrative and technical contacts. It also displays server details like IP addresses and port numbers. On the right is the [centralops.net/co](http://centralops.net/co) interface, which has a more user-friendly search form where you can enter a domain name or IP address. It provides a summary of the WHOIS record for the domain `juggyboy.com`, including the registrant information from `WHOIS.NETWORKSOLUTIONS.COM`.

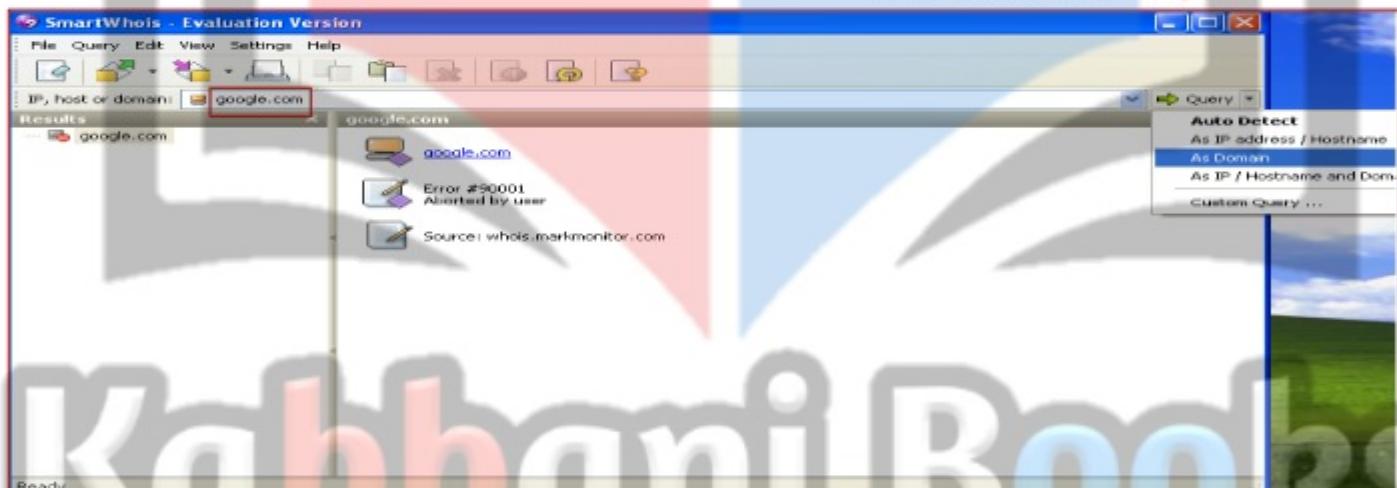
## أدوات (SMARTWHOIS) :WHOIS LOOKUP

**المصدر:** <http://www.tamos.com> هو عبارة عن أداة لجمع المعلومات عن الشبكة والتي تسمح لك بالبحث عن جميع المعلومات المتوفرة حول عناوين IP ، اسم المضيف **hostname**، أو الدومين، بما في ذلك البلد، الولاية أو المقاطعة، المدينة، اسم مزود الشبكة، المسؤول، معلومات الاتصال بالدعم التقني. أنه يساعدك أيضاً في العثور على مالك الدومين، معلومات الاتصال الخاصة بالمالك، عناوين IP الخاصة بالمالك، تاريخ تسجيل الدومين، وما إلى ذلك.

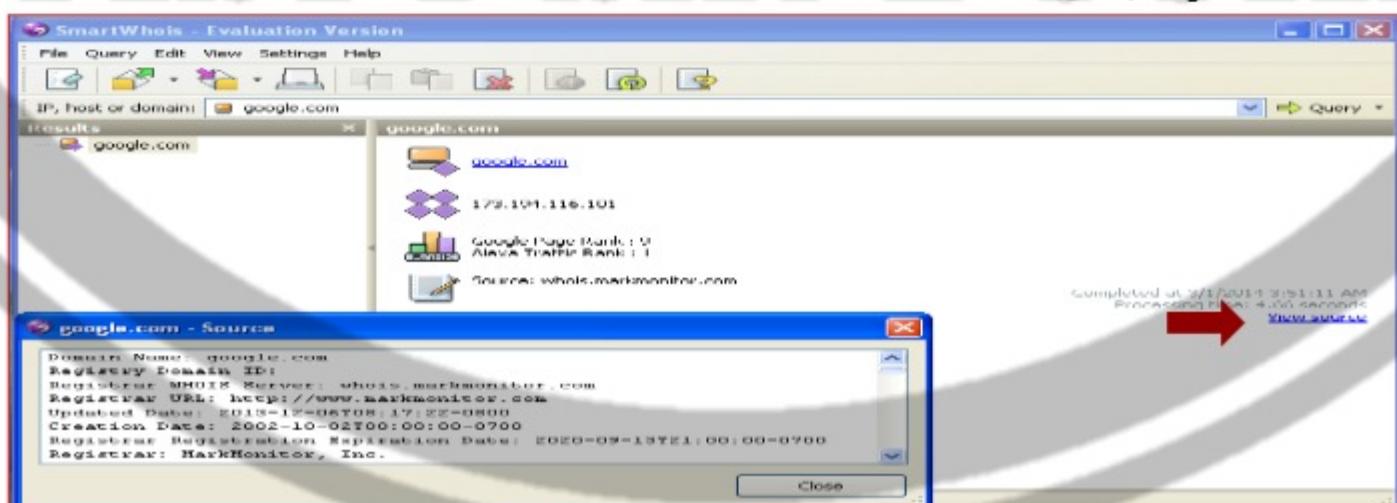
1- نقوم بتنبيه الأداة **SmartWhois** بتتابع **wizard** الخاص بعملية التبییت تم تفعیله فتظهر الشاشة التالیة:



2- في الخلقة **IP, host or domain** يكتب اسم الدومن ولیکن متلا **google.com** تم نصطف على الزر المقابل له المسمى **as domain** ونختار **query** كالاتی:



3- فيعرض لك كل المعلومات عن الدومن بالختصار وتلاحظ في الآخر وجود السطر **view resource** بالصطف عليه يظهر المعلومات بالکامل.



4- يمكنك أيضا استخدامه في الاستعلام عن **hosts** الخاصة بالدومن عن طريق **query as IP/hostname** وأيضا الاستعلام عن **IP** عن طريق **query as IP** وهكذا.

## WHOIS LOOKUP TOOLS

مثل الـ **Smartwhois**، هناك العديد من الأدوات المتاحة في السوق لاسترداد معلومات من خدمة **Whois**. سوف نذكر عدد قليل على النحو التالي:

### Countrywhois •

المصدر <http://www.tamos.com>

**Countrywhois** هو أداة لتحديد الموقع الجغرافي لعنوان **IP**. يمكن استخدامها لتحليل ملفات السجل (**log file**) للخادم، التحقق من رؤوس عناوين البريد الإلكتروني ، تحديد عمليات الاختيال على بطاقات الائتمان عبر الإنترنت، أو في حالة أخرى مثلا اذا كنت في حاجة لتحديد بلد المنشأ بواسطة عنوان **IP**.  
ملحوظة: تم استبعاد هذا التطبيق من القركة المالكة له منذ يناير 2013. لكنه ما زال يعمل ويمكن ايجاده عن طريق البحث في شبكة الويب.

### LanWhoIs •

المصدر <http://lantricks.com>

يوفّر **LanWhoIs** المعلومات حول الدومن والعناوين على شبكة الإنترنت. هذا البرنامج يساعدك على تحديد من، أين، ومتى تم تسجيل الدومن أو الموقع الذي يهمك، والمعلومات عن القائمين عليه الآن. هذه الأداة تسمح لك بحفظ نتيجة البحث في شكل ملف أرتييفي لمشاهدته في وقت لاحق. يمكنك طباعة وحفظ نتيجة البحث على هيئة **HTML**.

### Batch IP Converter •

المصدر <http://www.networkmost.com>

**Batch Ping · Domain-to-IP Converter** هو أداة للشبكات للعمل مع عناوين **IP** . فهو يجمع بين **IP-to-Country Converter** ، **Connection Monitor** ، **Website Scanner** ، **Whois** ، **Tracert** فإنه يسمح لك بالبحث عن عناوين **IP** لواحد أو قائمة من أسماء الدومن والعكس صحيح.

### CallerIP •

المصدر <http://www.calleripro.com>

**CallerIP** هو في الأساس أداة لرصد **IP** والمنفذ (**Ports**) التي يعرض الاتصال الواردة والصادرة التي أدخلت على جهاز الكمبيوتر الخاص بك. كما أنه يسمح لك بالبحث عن أصل كل عناوين **IP** على خريطة العالم. توفر ميزة **Whois reporting features** إحصائيات رئيسية مثل الذين يتم تسجيل **IP** إلى عناوين البريد الإلكتروني جنبا إلى جنب مع الاتصال وأرقام الهواتف.

### WhoIs Lookup Multiple Addresses •

المصدر <http://www.sobelsoft.com>

هذا البرنامج يقدم حلولا للمستخدمين الذين يرغبون في البحث عن تفاصيل الملكية لواحد أو أكثر من عناوين **IP** . يمكن للمستخدمين ببساطة إدخال عناوين **IP** أو تحميلها من ملف. هناك ثلاثة خيارات لموقع البحث: [whois-search.com](http://whois-search.com)، [whois.domaintools.com](http://whois.domaintools.com) ، و [whois.arin.net](http://whois.arin.net) . يمكن للمستخدم تحديد فترة التأخير **delay period** بين عمليات البحث، لتجنب الإغلاق من هذه المواقع. تعرض القائمة الناتجة عناوين **IP** وتفاصيل كل منها. كما يسمح لك لحفظ النتائج إلى ملف نصي.

### WhoIs Analyzer Pro •

المصدر <http://www.whoisanalyzer.com>

هذه الأداة تسمح لك بالوصول إلى معلومات حول نطاقات الدومن المسجلة في جميع أنحاء العالم، يمكنك عرض اسم مالك الدومن، اسم الدومن، وتفاصيل الاتصال الخاصة بمالك الدومن. كما أنه يساعد في العثور على مكان وجود دومنين معين. يمكن أيضا أن يقدم استعلامات متعددة مع هذه الأداة في وقت واحد. هذه الأداة توفر لك القدرة على طباعة أو حفظ نتيجة الاستعلام على هيئة **html**.

### Hotwhois •

المصدر <http://www.tialsoft.com>

**Hotwhois** هو أداة تتبع **IP** التي يمكن أن تكشف عن معلومات قيمة ، مثل البلد ، الدولة، المدينة والعنوان أرقام هاتف الاتصال، و عناوين البريد الإلكتروني وعنوان **IP** . عملية الاستعلام تعطي تقرير عن مجموعة متنوعة من سجلات الإنترنت الإقليمية، وذلك للحصول على

معلومات عن عناوين IP. باستخدام هذه الأداة يمكنك أن تتفاوض على المسجل، يستخدم دومين من النوع أي أنه لا يملك خادم لنفسه.

#### ActiveWhois ▪

المصدر: <http://www.johnru.com>

ActiveWhois هو برنامج قائم على شبكة المعلومات التي تسمح لك بالحصول على معلومات حول أصحاب عنوان IP أو شبكة الدومين. يمكنك أيضا تحديد البلد، والعنوان سواء الشخصية والبريدية للملك، عنوان IP الخاص بالمستخدمين والدومين.

#### WhoisThisDomain ▪

المصدر: <http://www.nirsoft.net>

WhoisThisDomain هو تطبيق للبحث عن تسجيلات الدومين والتي تساعدك للحصول على المعلومات حول الدومين المسجلة، حيث انه يمكن مرتبط بخادم whois بطريقه ما ويحصل منه على سجلات التسجيل للدومين. هو يدعم كل من country code domain و generic domain.

#### WHOIS Lookup Online Tools ▪

بالإضافة إلى الأدوات السابقة يوجد بعض الأدوات التي تكون متوفرة على الشبكة والتي تؤدي إلى استعلام whois كالتالي:

Smartwhois available at <http://smartwhois.com>

Better Whois available at <http://www.betterwhois.com>

Whois Source available at <http://www.whois.sc>

Web Wiz available at <http://www.webwiz.co.uk/domain-tools/whois-lookup.htm>

Network-Tools.com available at <http://network-tools.com>

Whois available at <http://tools.whois.net>

DNSstuff available at <http://www.dnsstuff.com>

Network Solutions Whois available at <http://www.networksolutions.com>

WebToolHub available at <http://www.webtoolhub.com/tn561381-whois-lookup.aspx>

Ultra Tools available at <https://www.ultratools.com/whois/home>

#### WHOIS في نظام التشغيل لينكس (كالي/باك تراك)

وسيلة بسيطة جدا لكنها فعالة لجمع معلومات إضافية حول هدفنا وهو whois. في خدمة Whois يتيح لنا الوصول إلى معلومات محددة حول هدفنا بما في ذلك عناوين IP أو أسماء المضيفين المسجل في خادم الأسماء (DNS) ومعلومات الاتصال التي عادة ما تحتوي على عنوان ورقم هاتف. بناء whois في نظام التشغيل لينكس أي موجودة افتراضياً. لذلك أبسط طريقة لاستخدام هذه الخدمة عن طريق فتح الترمinal وأدخل الأمر التالي:

\$whois@target\_domain

```
root@jana:~# whois
Usage: whois [OPTION]... OBJECT...

-l                           one level less specific lookup [RPSL only]
-L                           find all Less specific matches
-m                           find first level more specific matches
-M                           find all More specific matches
-c                           find the smallest match containing a mnt-irt attribute
-x                           exact match [RPSL only]
-d                           return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]...             do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]...            only look for objects of TYPE
-K                           only primary keys are returned [RPSL only]
-r                           turn off recursive lookups for contact information
-R                           force to show local copy of the domain object even
```

```
root@jana:~# whois syngress.com
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: SYNGRESS.COM
Registrar: SAFENAMES LTD
Whois Server: whois.safenames.net
Referral URL: http://www.safenames.net
Name Server: NS.ELSEVIER.CO.UK
Name Server: NS0-S.DNS.PIPEX.NET
Name Server: NS1-S.DNS.PIPEX.NET
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 15-dec-2010
Creation Date: 10-sep-1997
Expiration Date: 09-sep-2015

>>> Last update of whois database: Sat, 08 Mar 2014 19:12:21 UTC <<<
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
```

من المهم تسجيل كافة المعلومات وإيلاء اهتمام خاص لخوادم DNS. إذا تم سرد خوادم DNS بالاسم فقط، سوف نستخدم الأمر **host** لترجمة تلك الأسماء إلى عناوين IP.

يمكن أيضاً تنفيذ عمليات بحث العكسى. بدلاً من إدخال اسم النطاق، أي يمكنك إدخال عنوان IP. سوف تشمل عادة نتيجة **whois** نطاق القبة بأكملها الذي ينتمي إلى المنظمة.

```
root@jana:~# whois 173.194.39.18
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=173.194.39.18?showDetails=true&showARIN=false&ext=netref2
#
NetRange:      173.194.0.0 - 173.194.255.255
CIDR:          173.194.0.0/16
OriginAS:      AS15169
NetName:       GOOGLE
NetHandle:     NET-173-194-0-0-1
Parent:        NET-173-0-0-0-0
NetType:       Direct Allocation
RegDate:       2009-08-17
Updated:       2012-02-24
Ref:           http://whois.arin.net/rest/net/NET-173-194-0-0-1
```

## (عملية الاستطلاع عن معلومات DNS FOOTPRINTING-7)

**ملحوظه:** تعتبر هذه المرحلة من اهم مراحل الاستطلاع إذا كانت من الممكن ان تغنى عن باقي المراحل.

تنقل الان الى مرحلة أخرى من مراحل عملية الاستطلاع وهي **DNS Footprinting** وفيه هذا الجزء سوف يتم شرح طريق استخراج معلومات DNS والأدوات المستخدمة في ذلك.

خوادم DNS هي هدف ممتاز للقرصنة ومختربي الاختراق. عادة ما تحتوي على المعلومات التي تعتبر ذات قيمة عالية للمهاجمين. DNS هو مكون أساسي في كل من التبكات المحلية لدينا والإنتernet. من بين أمور أخرى، DNS هي المسؤولة عن عملية ترجمة أسماء النطاقات إلى عناوين IP. كبسن، فمن الأسهل بكثير بالنسبة لنا أن نتذكرة "google.com" بدلاً من "74.125.95.105". مع ذلك، فإن آلات يفضلون العكس. يقدم DNS كأنه رجل في المنتصف لتنفيذ عملية الترجمة.



كمختبر اختراق، من المهم التركيز على خادم DNS التي تنتهي إلى هدفنا والسبب بسيط. من أجل DNS يعمل بشكل صحيح، فإنه يجب أن يكون على بيئة من كل عناوين IP واسم الدومين المقابل له من كل كمبيوتر على شبكةها. من حيث الاستطلاع، والحصول على حق الوصول الكامل إلى خادم DNS للشركة هو مثل العثور على وعاء من الذهب في نهاية قوس قزح. أو ربما، أكثر دقة، هو مثل العثور على مخططات تسمى blueprint تحتوي على بنية المنظمة الهدف. لكن في هذه الحالة، هذه المخططات تحتوي على قائمة كاملة من عناوين IP الداخلية وأسماء المضيف التي تنتهي إلى هدفنا.

نذكر واحد من العناصر الرئيسية لجمع المعلومات هو جمع عناوين IP التي تنتهي إلى الهدف. بجانب أنه وعاء من الذهب، هناك سبب آخر لماذا يركزون على DNS هو أنه ممتع جداً في كثير من الحالات هذه الملقطات تمثل إلى العمل بمبدأ "إذا لم يتم كسره، لا تمس ذلك" [if it isn't broke, don't touch it] يعني أنه لا يلمع اعداده إذا لم يتم اختراقه.

إن مسؤولي الشبكة [admin] عديمي الخبرة في كثير من الأحيان يتعاملون مع خادم DNS بالفلك والريبة. في كثير من الأحيان، يختاروا تجاهل هذا المربع تماماً لأنهم لا يفهمونه تماماً. ونتيجة لذلك، فإن ترميم وتحديث أو تغيير إعداد خادم DNS غالباً ما يكون في أولوية منخفضة. هذا إضافة إلى أن معظم خادم DNS تبدو مستقرة جداً. هؤلاء المدراء يفعلون أكبر خطأ في حياتهم المهنية في وقت مبكر حيث أنهم يفتقرون خادم DNS الخاصة بهم، بأقل المشاكل صعوبة والتي تسبب لهم فوضى.

يجب أن نتذكرة بأن خادم DNS تحتوي على سلسلة من السجلات [record] التي تحتوي على عنوان IP واسم المضيف لجميع الأجهزة التي على علاقة بالدومين. يتم نشر العديد من خادم DNS المتعددة (multi DNS) في الشبكة من أجل load balance أو المعاونة. نتيجة لذلك، فإن خادم DNS بحاجة إلى وسيلة للتواصل بالمعلومات. عملية المشاركة هذه تتم من خلال استخدام نقل المنطقة [zone transferee]. أثناء نقل المنطقة (zone transfer)، حيث يشار إليها عادة باسم AXFR، والتي يشار إليها عادة باسم DNS واحد بارسال خادم DNS الأخرى إلى كل المضيفين. هذه العملية تسمح لخادم DNS المتعددة بالبقاء على وفاق. حتى إذا كان غير ناجحين في أداء نقل منطقة (zone transfer)، فلا يزال لدينا بعض الوقت للتحقيق من خادم DNS التي تقع ضمن نطاق عملنا.

## EXTRACTING DNS INFORMATION

يسمح لك بالحصول على معلومات حول بيانات DNS Zone. بيانات DNS Zone هذه تتضمن أسماء الدومين لـ DNS وأسماء أجهزة الكمبيوتر وعناوين IP والكثير حول شبكة اتصال معينة. حيث يقوم المهاجم بأداء DNS Footprinting على شبكة الاتصال الهدف بغية الحصول على المعلومات حول DNS. يتم استخدام المعلومات التي تم جمعها حول DNS للشبكة الهدف لتحديد المضيفين الرئيسيين (KEY host) في الشبكة وذلك لتنفيذ هجمات الهندسة الاجتماعية في جمع المزيد من المعلومات.

يمكن أن يؤدي عن طريق استخدام أدوات مجموعة من الأدوات مثل www.DNSstuff.com والتي بواسطتها يمكن استخراج معلومات DNS مثل عناوين IP، خادم البريد الملحق ، Whois Lookup ، DNS Lookup ، DNS Routing ، وهكذا. إذا كنت تريد جمع معلومات حول الشركة مستهدفة، فمن الممكن استخراج نطاق عناوين IP المستخدمة (IP range)، المستخدمة في IP Routing إذا كانت الشبكة الهدف تسمح للمستخدمين الغير مصرح لهم، أو الغير معروفين بنقل بيانات DNS zone ، فإنه من السهل عليك الحصول على معلومات حول DNS بمساعدة مجموعة من الأدوات.

بمجرد إرسال استعلام باستخدام أدوات استجواب DNS (DNS Interrogation zone) إلى خادم DNS، فإن خادم DNS سوف يستجيب لك مع record stricter الذي يحتوي على معلومات حول DNS record (DNS record) توفر المعلومات الهامة حول الموقع والنوع للخادم ومن هذه السجلات record) كالاتي:

- [A] يشير إلى عنوان IP الخاص بالمضيف (host's IP address).
- [MX] يشير إلى خادم البريد الإلكتروني المرتبط بالدومين (domain's mail server).
- [NS] يشير إلى اسم الخادم المضيف المرتبط بالدومين (host's name server).
- [CNAME] يشير إلى الأسماء المستعارة للخادم المضيف والمترتبة بالدومين (aliases to a host).
- [SOA] يشير إلى الدومين الرئيسي (authority of domain).
- [SRV] يشير إلى الخدمات المسجلة (service record).
- [PTR] يشير إلى عناوين IP الخاص بالدومين وتستخدم في الاستعلام العكسي لـ (IP address to a host name).
- [RP] تشير إلى الأشخاص المسؤولين (responsible person).
- [HINFO] تشير إلى معلومات عن الأجهزة المضيفة المرتبطة بالدومين الرئيسي مثل معلومات عن نظام التشغيل و CPU المستخدم وهذا (HOST information record).

الأدوات المستخدمة في إرسال طلب استعلام عن سجلات DNS RECORD كالاتي:

<http://www.dnsstuff.com>

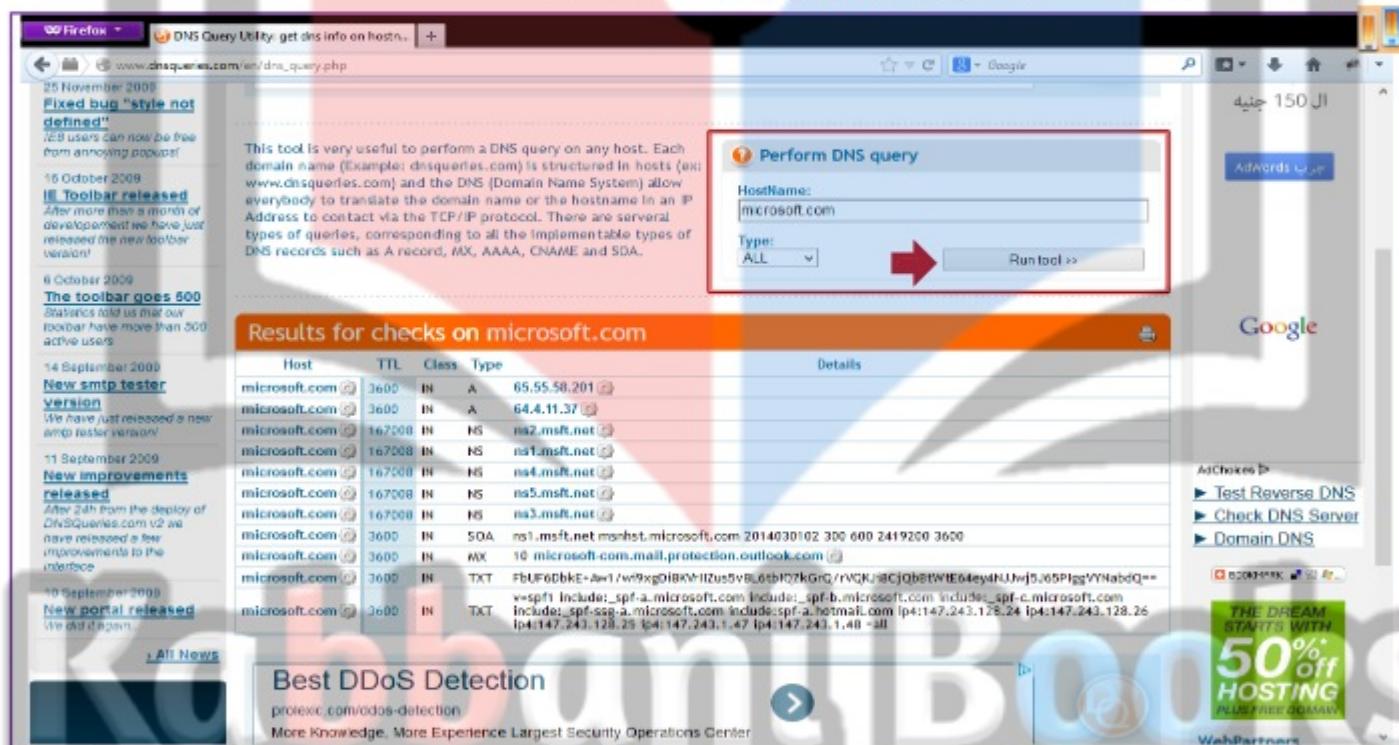
<http://network-tools.com>

## Ping – nslookup - dig

استخراج معلومات DNS (Extracting DNS information) باستخدام [dnsqueries.com](http://www.dnsqueries.com)

يمكنك أداء عملية الاستعلام عن DNS عن طريق استخدام موقع الويب <http://www.dnsqueries.com> والتي تعتبر أداة تسمح لك بتنفيذ أي استعلام عن DNS على أي المضيف. كل اسم دومن على سبيل مثال (dnsqueries.com) عباره عن تركيب من المضيفين (hosts) على سبيل المثال (www.dnsqueries.com) و(DNS Domain name system) يسمح لأي شخص بترجمة اسم الدومن أو اسم المضيف إلى عنوان IP ليتم الاتصال باستخدام البروتوكول TCP/IP.

هناك عدة أنواع من الاستعلامات، والتي تعبّر عن نوع سجلات DNS مثل، **MX** ، **AAAA** ، **CNAME** و **SOA**.  
الآن دعونا نرى كيف أداة عملية الاستطلاع عن DNS باستخدام تلك الأداة. وذلك عن طريق الذهاب إلى متصفح الويب وكتابة <http://www.dnsqueries.com> سوف يتم عرض صفحة الويب الخاصة بهذا الموقع. نقوم بإدخال اسم الدومين الذي تريده الاستعلام في الحقل **Perform DNS query** (هنا أنتا تدخل موقع [Microsoft.com](http://Microsoft.com)) وانقر فوق الزر أداة التسجيل **run tool**؛ سيتم عرض معلومات DNS لموقع [Microsoft.com](http://Microsoft.com) كما هو موضح في الشكل التالي.



#### • عملية الاستطلاع باستخدام الأداة Ping

**Ping**: هو اختصار لـ **packet Internet Groper**. هو أداة معروفة لأغلب مهندسي وخبراء تقنية المعلومات. يعتبر أمر من الأوامر المستخدمة في سطر الأوامر (مثال **LINUX, MSDOS, UNIX**)، وذلك لغرض الفحص والتحقق من الاتصال بمستوى **IP** مع كمبيوتر آخر أو موجه **Router** أو طابعة أو أي جهاز آخر يستخدم بروتوكول **TCP/IP**. يرسل الأمر **ping** مجموعة من حزم البيانات إلى جهاز آخر مستتر في نفس الشبكة ويطلب منه الرد بإشارات معينة على هذه الحزم تم عرض النتائج بأكملها على الشاشة.

لذلك فإن الامر ping يستخدم في الآتي:

1. التعرف على حالة الشبكة وحالة المستضيف (موقع ما أو صفحة).
  2. تتبع وعزل الأعطال في القطع والبرامج.
  3. لاختبار وإدارة الشبكة.

٤. يمكن استخدام الأمر **ping** لعمل فحص ذاتي للحاسوب (**loopback**).

لكن يوجد استخدام اخر لهذه الأداة من قبل القرصنة والتي من شأنها أن تسمح لك بجمع المعلومات المهمة مثل عنوان IP، الحد الأقصى لحجم حزم (frame size) وبعضاً المعلومات الأخرى. يستخدم أيضاً من قبل penetration tester من أجل التأكد من الوصول لجهاز الكمبيوتر الخاص بـ victim.

## كيف يعمل الامر ping؟

يعلم الامر **ping** من خلال إرسال حزمة من البيانات باستخدام البروتوكول **ICMP** (Internet Control Message Packet) إلى الحاسب الآخر (**echo request packet**) ومن تم الانتظار للحصول على رد لتلك الحزمة من البيانات (**ICMP response**). ومن خلال عملية الانتظار للحصول على رد فإن الامر **ping** يعلم علىقياس الوقت المستخدم من ارسال الحزمة حتى الحصول على الرد وهذا يعرف بـ **round-trip time** ويقوم أيضاً بتسجيل أي حزمة تم فقدانها.

في نظام التشغيل ويندوز:

مثال على الامر **ping** نقوم بكتابة الامر التالي في **command prompt (cmd)** في الويندوز.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.certifiedhacker.com

Pinging www.certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=680ms TTL=112
Reply from 202.75.54.101: bytes=32 time=396ms TTL=112
Reply from 202.75.54.101: bytes=32 time=394ms TTL=112
Reply from 202.75.54.101: bytes=32 time=450ms TTL=112

Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 394ms, Maximum = 680ms, Average = 480ms

C:\WINDOWS\system32>
```

>ping@www.certifiedhacker.com

## ستلاحظ المعلومات التالية نتيجة استخدام الامر ping:

انه تم ارسال 4 حزم من المعلومات **packets** ولم يفقد منها شيء. حيث الخاتمة **sent=4** و **received=4** و **lost=0** والتي تعني انه لم يفقد اي حزم. كما سترى أيضاً معلومة الزمن الذي أخذته كل حزمة في الذهاب والعودة بالميللي تانية. كما يوضح أيضاً الحجم الأساسي للحزمة الواحدة وهي 32 بايت.

نلاحظ ايضاً اننا على بعض المعلومات الأخرى مثل عنوان **IP** المقابل لـ [www.certifiedhacker.com](http://www.certifiedhacker.com) وهو 202.75.53.101.

ويمكن ايضاً الحصول على معلومات عن الحزمة **packet** التي تم ارسالها مثل عدد الحزم التي تم ارسالها وأيضاً التي تم استقبالها، عدد الحزم التي فقدت في الطريق وأيضاً **approximate round trip times**.

الشكل العام لأمر ping

Ping [-t] [-a] [-n] [-l] [-f] [-i] [-v] [-r] [-s] [-w] [-j] targetname

## هذا بعض المعايير المستخدمة مع الامر ping:

هذا يوضح بعض المعايير الاختيارية والتي توفر مع الأمر **ping**:

- (-t) والتي تخبر الامر **ping** بان يستمر بالإرسال للعنوان المطلوب حتى يتوقف عن الإجابة وإذا أردنا مقاطعة الإحصائيات وعرضها نضغط على **CTRL+Break** ولمقاطعة **ping** وإنائه نستخدم **CTRL+C**.
- (-a) لعرض الرقم التعريفي للعنوان المحدد.
- يمكن أيضاً استخدامه لمعرفة أكبر حجم للحزم (**max frame size**) من الممكن ارساله بواسطة الامر **ping** كالتالي:

C:\WINDOWS\system32>ping www.certifiedhacker.com -f -1 1500

```
Pinging www.certifiedhacker.com [202.75.54.101] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
```

```
Ping statistics for 202.75.54.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

C:\WINDOWS\system32>

نلاحظ انه اعطي هذه الرسالة **[Packet needs to be fragmented but DF set.]** والتي تعني انه يريد منك تجزئة حجم الرسالة وتصغيرها حيث استخدمنا (-f) والتي يمكن تحديد حجم الرسالة عن طريقه حيث الحجم الافتراضي هو 32 بايت واستخدمنا أيضاً معه الصيغة (-f) حتى لا يقوم بتجزئة الرسالة وارسلها مرة واحدة. تقوم الان بتصغر الحجم تدريجياً ولتكن متلا 1300 كالتالي:

```
C:\WINDOWS\system32>ping www.certifiedhacker.com -f -l 1300
```

```
Pinging www.certifiedhacker.com [202.75.54.101] with 1300 bytes of data:  
Reply from 202.75.54.101: bytes=1300 time=509ms TTL=112  
Reply from 202.75.54.101: bytes=1300 time=510ms TTL=112  
Reply from 202.75.54.101: bytes=1300 time=509ms TTL=112  
Reply from 202.75.54.101: bytes=1300 time=507ms TTL=112  
  
Ping statistics for 202.75.54.101:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 507ms, Maximum = 510ms, Average = 508ms
```

```
C:\WINDOWS\system32>
```

نجد انه قام بارسال الرسالة نستنتج من ذلك ان اقصى حجم للرسالة يمكن ارساله بواسطة **Ping** يندرج بين 1500 و 1300 نحاول تجربة الأرقام من 1300 و 1500 فلنجرب مثلا 1473 كالتالي:

```
C:\WINDOWS\system32>ping www.certifiedhacker.com -f -l 1473
```

```
Pinging www.certifiedhacker.com [202.75.54.101] with 1473 bytes of data:  
Packet needs to be fragmented but DF set.  
Packet needs to be fragmented but DF set.  
Packet needs to be fragmented but DF set.  
Packet needs to be fragmented but DF set.
```

```
Ping statistics for 202.75.54.101:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\WINDOWS\system32>
```

نجد انه لم ينجح في الارسال فلنجرب 1472 كالتالي:

```
C:\>ping www.certifiedhacker.com -f -l 1472
```

```
Pinging www.certifiedhacker.com [202.75.54.101] with 1472 bytes of data:  
Reply from 202.75.54.101: bytes=1472 time=359ms TTL=114  
Reply from 202.75.54.101: bytes=1472 time=320ms TTL=114  
Reply from 202.75.54.101: bytes=1472 time=282ms TTL=114  
Reply from 202.75.54.101: bytes=1472 time=317ms TTL=114
```

```
Ping statistics for 202.75.54.101:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 282ms, Maximum = 359ms, Average = 319ms
```

```
C:\>
```

نجد هنا انه نجح في الارسال إذا أكبير حجم ممكنا للرسالة التي يرسلها الامر **ping** لهذا الموقع هو 1472.

نجد ان الصيغة المتحكمه في حجم الرسالة/الحزمة (frame size) هنا (-l).

جميع الحزم (**FRAME**) تملك صلاحية **TTL** (Time to live) والتي عند وصولها الى الرقم صفر فان الموجه **router** يقوم باستبعاده حيث يستخدم هذه التقنية في منع فقد الحزم (**loss of packet**).

يمكن أيضا استخدام الصيغة (-i) والتي تحدد المدة الزمنية لكل حزمة ومقاسه بالميللي ثانية او بمعنى اوضح تستخدم في وضع قيمة **TTL** لكل حزم. يمكن أيضا استخدام الصيغة (-n) والتي تتحكم في عدد الحزم المرسلة حيث العدد الافتراضي هو 4.

في نظام التشغيل جنو/لينكس

الصيغة العامة للأمر **ping** في لينكس كالتالي:

```
ping [-c count] [-i interval] [-l preload] [-p pattern] [-s packetsize] [-t ttl] [-I interface] [-T timestamp option] [-W timeout] destination
```

```
root@jana:~# ping www.google.com  
PING www.google.com (173.194.113.144) 56(84) bytes of data.  
64 bytes from ham02sll-in-f16.1e100.net (173.194.113.144): icmp_req=1 ttl=45 time=868 ms  
64 bytes from ham02sll-in-f16.1e100.net (173.194.113.144): icmp_req=2 ttl=45 time=1184 ms  
64 bytes from ham02sll-in-f16.1e100.net (173.194.113.144): icmp_req=3 ttl=45 time=1290 ms  
64 bytes from ham02sll-in-f16.1e100.net (173.194.113.144): icmp_req=4 ttl=45 time=1503 ms  
^C64 bytes from ham02sll-in-f16.1e100.net (173.194.113.144): icmp_req=5 ttl=45 time=1101 ms  
  
--- www.google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 6672ms  
rtt min/avg/max/mdev = 868.603/1189.831/1503.831/209.613 ms, pipe 2
```



حيث نلاحظ اننا قمنا بكتابة الامر **ping** متبعاً باسم الا **host**. فنجد انه تم ارسال الحزم ولكن نجد انه لا يتوقف حتى تقوم بالضغط على **Ctrl+C** ونجد انه يعطي رسالة للتوضيح **ttl** والوقت المستغرق في ارسال الحزمة نجد انه هو الاخر يأتى معه العديد من الخيارات كالتالي:

Table 5-1. Command Line Switches for the ping Command

Switch	Effect
<b>-c count</b>	Send only <i>count</i> echo requests before exiting.
<b>-i interval</b>	Pause <i>interval</i> seconds between echo requests.
<b>-w timeout</b>	Exit after <i>timeout</i> seconds have passed, even if all echo replies have not been received.
<b>-b</b>	Allow the specified address to be a network or broadcast address, effectively pinging every host on the specified network. (Only available to the root user.)
<b>-f</b>	Ping flooding. Send echo requests as quickly as possible. For every request sent, print a *. For every reply received, print a backspace. A resulting progression of periods across the screen implies packets are being dropped by the network. (Only available to the root user).

المشكلة مع الأمر **ping** هو أنه يسمح لك باستخدام **ICMP** للتحقق من مضيف واحد [host] في وقت واحد. الأمر **fping** يسمح لك بتتبع العديد من المضيفين [multiple host] باستخدام أمر واحد. سوف تتيح لك أيضاً قراءة ملف به أسماء المضيفين المتعددة أو عنوان IP وإرسالها باستخدام حزمة **ICMP swap fping** لتشغيل **ICMP echo requests** على الشبكة، عن طريق اتباع التالي:

```
fping -asg network/host bits
fping -asg 10.0.1.0/24
```

ملحوظة: التعريف **g** يستخدم إذا كنت تستخدم عنوان IP.

```
root@jana:~# fping -as www.google.com
www.google.com

 1 targets
 1 alive
 0 unreachable
 0 unknown addresses

 0 timeouts (waiting for response)
 1 ICMP Echos sent
 1 ICMP Echo Replies received
 0 other ICMP received

135 ms (min round trip time)
135 ms (avg round trip time)
135 ms (max round trip time)
 0.136 sec (elapsed real time)
```

## • الأداة nslookup

**NSLOOKUP** هو الأداة التي يمكن استخدامها للاستعلام من مقدمات DNS وربما الحصول على سجلات حول مختلف المضيفين التي هي على علم بها. بناءً على العديد من إصدارات لينكس بما في ذلك كالي و حتى يتوفر لنظام التشغيل **Windows**. **NSLOOKUP** يعمل بطريقة مختلفة جداً بين مختلف أنظمة التشغيل، ولكن يجب مراجعة دائماً خصوصيات لنظام التشغيل الخاصة بك. يمكن استخدام الأداة **nslookup** من قبل القراءة للحصول على عنوان IP لدومنين معين والذى يتيح له في إيجاد عنوان IP الخاص بالشخص الذي يأمل في مهاجمته. على الرغم من أنه من الصعب تقييد المستخدمين الآخرين للاستعلام مع خادم DNS باستخدام الأمر **nslookup** لأن هذا البرنامج يختار محاكاة عملية قيام البرامج الأخرى من ترجمة الأسماء من خلال طلبات لخادم DNS، ووظيفة مختبر الاختراق [penetration tester] هو أن يكون قادر على منع مثل هذه الهجمات من خلال الذهاب إلى 'zone properties'. في **zone transfer tab** تحديد خيار لعدم السماح **zone transfer**. هذا لمنع المهاجمين من استخدام الأمر **nslookup** للحصول على قائمة لسجلات المنطقة (zone's record) الخاص بك. **NSLOOKUP** يمكن أن يوفر لك تزورة من المعلومات التفصيلية لخادم DNS.

**NSLOOKUP** هو الأداة التي يمكن تشغيلها في الوضع التفاعلي [interactive mode]. هذا يعني ببساطة أننا سوف نستدعي البرنامج أولاً ثم نطعنه بمقاييس معينة حتى يجعله يعمل بشكل صحيح. نبدأ باستخدام **NSLOOKUP** من خلال فتح الترمinal (terminal) في اللينكس او **command prompt** في الويندوز والدخول الى الامر عن طريق كتابة **nslookup**.

## Command prompt in windows

```
C:\>WINDOWS\system32>nslookup
Default Server: Unknown
Address: 192.168.16.1

> help
Commands:  <identifiers are shown in uppercase, [] means optional>
NAME      - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ?   - print info on common commands
set OPTION - set an option
    all     - print options, current server and host
    no Idebug - print debugging information
    no Id2   - print exhaustive debugging information
    no Idefname - append domain name to each query
    no Irecuse - ask for recursive answer to query
    no Isearch - use domain search list
    no Ivc   - always use a virtual circuit
    domain=NAME - set default domain name to NAME
    searchlist=N1[N2/...]/N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME - set root server to NAME
    retry=X   - set number of retries to X
    timeout=X - set initial time-out interval to X seconds
    type=X    - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,
    SOA,SRV)
    querytype=X - same as type
    class=X   - set query class (ex. IN <Internet>, ANY)
    no Imxfr  - use MS fast zone transfer
    ixfrver=X - current version to use in IXFR transfer request
server NAME - set default server to NAME, using current default server
lserver NAME - set default server to NAME, using initial server
root        - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a      - list canonical names and aliases
    -d      - list all records
    -t TYPE - list records of the given RFC record type (ex. A,CNAME,MX,NS,
    PTR etc)
view FILE   - sort an 'ls' output file and view it with pg
exit        - exit the program
>
```

## Terminal in Linux

```
root@jana:~# nslookup
>
```

بإصدار الأمر "nslookup"، تكون قد بدأنا **nslookup** من نظام التشغيل. بعد كتابة "Enter" تم كتابة "nslookup" تتم كتابة "Enter". ولكن قبل هذا فإنه سوف يعرض بيانات الملقن الذي يستخدمه في عمليات الفحص اليومية عبر الانترنط وأقصد هنا الملقن الخاص بمنقدمي خدمة الانترنت (ISP). يمكنك أيضاً معرفة هذا عن طريق كتابة الكلمة **server** أو **lserver**. عند هذه النقطة، يمكنك إدخال المعلومات الإضافية التي تحتاجها **NSLOOKUP** لكي يعمل. نبدأ بتغيير الأمر **NSLOOKUP** عن طريق إدخال الكلمة "server" لمقن DNS وعنوان IP لمقن "server" التي تريد الاستعلام عنه. مثال كالتالي:

```
>server@8.8.8.8
```

**ملحوظة:** للإستعلام عن اسم ملقن آخر مباشرة، نستخدم الأمر **server** أو الأمر **lserver** للتبديل إلى الملقن الاسم هذا. يستخدم الأمر **server** الملقن المحلي للحصول على عنوان الملقن للتبديل إليه بينما يستخدم الأمر **lserver** الملقن الافتراضي الحالي للحصول على العنوان.

```
> server
Server: Unknown
Address: 192.168.16.1

*** Unknown can't find server: Non-existent domain
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> server
Server: google-public-dns-a.google.com
Address: 8.8.8.8

*** google-public-dns-a.google.com can't find server: Non-existent domain
>
```

سوف يقبل الأمر ببساطة ويقوم لكم سطر آخر مع العلامة ">". نحن نريد تحديد نوع السجل الذي نبحث عنه. أثناء عملية الاستطلاع، هناك أنواع عديدة من السجلات التي ربما كنت مهتماً بها. للحصول على قائمة كاملة من الأنواع المختلفة لسجل **DNS** ووصفهم، يمكنك استخدام المهارات المكتسبة حديثاً من خلال بحث جوجل الخاص بك. إذا كنت تبحث عن معلومات عامة، يجب تعين **any** إلى **any** باستخدام الكلمة الأساسية "**any**" كالتالي:

```
>set type=any
```

نتأكد من عدم وجود تباعد/مسافة أو ستحصل على رسالة خطأ. نكتب اسم الدومن الذي ت يريد ان تبحث عنه. إذا كنت تبحث عن معلومات محددة من ملقن **DNS** مثل عنوان **IP** لمقн البريد الذي يتعامل مع البريد الإلكتروني للمنظمة الهدف، نستخدم التسجيل **[set type=mx]**.

تم نخت استجواب DNS الأولى لدينا مع **NSLOOKUP** عن طريق إدخال الدومن الهدف بعد العلامة [>].

```
> set type=any
> syngress.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
syngress.com      nameserver = ns0-s.dns.pipex.net
syngress.com      nameserver = ns1-s.dns.pipex.net
syngress.com      nameserver = ns.elsevier.co.uk
syngress.com
    primary name server = ns.elsevier.co.uk
    responsible mail addr = hostmaster.elsvier.co.uk
    serial = 2014031103
    refresh = 3600 <1 hour>
    retry = 900 <15 mins>
    expire = 2419200 <28 days>
    default TTL = 900 <15 mins>
syngress.com      internet address = 50.87.186.171
syngress.com      MX preference = 10, mail exchanger = syngress.com.inbound10.mxlogic.net
syngress.com      MX preference = 10, mail exchanger = syngress.com.inbound10.mxlogicmx.net

ns1-s.dns.pipex.net      internet address = 158.43.193.83
ns.elsevier.co.uk      internet address = 193.131.222.35
ns0-s.dns.pipex.net      internet address = 158.43.129.83
>
```

نفترض أنك تريد أن تعرف ما هو خادم البريد المستخدمة للتعامل مع البريد الإلكتروني **syngress.com**. في المثال السابق، توصلنا إلى أن واحدة من خوادم أسماء **Syngress** كان "ns.elsevier.co.uk". هنا مرة أخرى، يمكننا استخدام نوع السجل كالتالي:

```
> syngress.com
Server: [8.8.8.8]
Address: 8.8.8.8

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
syngress.com      MX preference = 10, mail exchanger = syngress.com.inbound10.mxlogicmx.net
syngress.com      MX preference = 10, mail exchanger = syngress.com.inbound10.mxlogic.net
>
```

ملحوظة: إذا أعطى لك **timeout** فاستخدمه مرة أخرى حتى يستجيب DNS إلى طلبك.

نفس ما سبق في جنو لينكس كالتالي:

```
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> server
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> syngress.com
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
syngress.com
    origin = ns.elsevier.co.uk
    mail addr = hostmaster.elsvier.co.uk
    serial = 2014031103
    refresh = 3600
    retry = 900
    expire = 2419200
    minimum = 900
syngress.com      nameserver = ns1-s.dns.pipex.net.
syngress.com      nameserver = ns.elsevier.co.uk.
syngress.com      nameserver = ns0-s.dns.pipex.net.

Authoritative answers can be found from:
ns.elsevier.co.uk      internet address = 193.131.222.35
> ■
```



نلاحظ هذه الرسالة تم اعطى اسم خادم الأسماء الخاص به. هذا يخبرك انه لكي تحصل على اجابة اكيدة يمكنك سؤال هذا الخادم. لاحظنا سابقا عند الاستعلام عن الدومنين **Syngress** نجد انه يحتوي على ثلاث خوادم/ملقمات **DNS** يتعامل معها ونجد ان الملقم الرئيسي لهم والذي طلب منك سؤاله حتى تحصل على اجابة اكيدة هو **[ns.elsevier.co.uk]**. نذهب الى هذا الخادم/الملقم باستخدام التعبير **[server]** تم اسم ملقم/خادم الاسماء DNS. هذا يعني كما قلنا سابقا اننا سوف نستخدم هذا الخادم/الملقم في السؤال عن الدومنين الذي نريد. نفترض هنا أيضا اننا نريد تحديد السجل **[mx]** لمعرفة ملقمات/خوادم البريد الإلكتروني كالاتي:

```
> server 193.131.222.35
Default server: 193.131.222.35
Address: 193.131.222.35#53
> set type=mx
> syngress.com
Server:          193.131.222.35
Address:         193.131.222.35#53

syngress.com      mail exchanger = 10 syngress.com.inbound10.mxlogicmx.net .
syngress.com      mail exchanger = 10 syngress.com.inbound10.mxlogic.net .
>
```

تخيص ذلك: ان عملية **nslookup** تتم في الوضع **non-interactive mode** او في الوضع **interactive mode**. لتشغيل **nslookup** في الوضع **interactive mode** ويتم ذلك عن طريق كتابة الامر **nslookup** بدون أي صيغ اضافية او استخدام الصيغة **(-)** تم بليه اسم المضيف **ip** او عنوان **hostname** في **command prompt**. الذي يؤدي الى الدخول الى الامر وظهور العلامة(**>**). اما لتشغيله في الوضع **non-interactive mode** فيتم ذلك عن طريق كتابة الامر **nslookup** تم يتبعه أي من الصيغ التالية سواء اسم المضيف **hostname** او عنوان **ip** (IP address).  
عند استخدام الأداة **nslookup** فإنه سوف تستقبل **non-authoritative answer** او **authoritative answer** وذلك لأن **nslookup** افتراضيا يسأل خادم الأسماء **nameserver** من أجل ترجمة الاستعلام الخاص به. و خادم الأسماء الخاص بك (**nameserver**) يكون غير موثق **not authority** لاسم الذي تسأل عنه. يمكنك أيضا الحصول على اجابة موثقه (**authoritative answer**) عن طريق ارسال الطلب الى خوادم أسماء موثقه (**authoritative nameserver**) عن أسماء الدومنين التي تزيد الاستعلام عنه.

### ما الاستخدام الآخر الهام لهذه الأداة؟

يمكن استخدام الأداة **Nslookup** لنقل منطقة كاملة [zone transfer] باستخدام الأمر **ls**. يكون هذا الأمر مفيداً لمعرفة كافة المضيفين داخل الدومن البعيد (يعنى اصح معرفة كل السجلات record) الداخلية والخارجية). يكون بناء الجملة للأمر **ls** كالتالي:  
**>ls [- a | d | t type] domain [> filename]**

يؤدي استخدام الأمر **ls** بدون وسائل إلى إرجاع قائمة بكل بيانات العنوان وأسماء الملقمات. يؤدي التعبير **[-a]** إلى إرجاع الاسم المستعار والأسماء المترافق عليها **[canonical names and aliases]**, بينما يؤدي التعبير **[-d]** إلى إرجاع كافة البيانات والتغيير **[-t]** إلى التصفيحة حسب النوع.

يمكن حظر عمليات نقل المنطقة (zone transfer) في ملقم **DNS** بحيث تقوم العناوين أو التبيكات الموثقة فقط بإجراء هذه الوظيفة. يظهر الخطأ التالي في حالة تعين أمان المنطقة (منع عملية نقل المنطقة):

**\*\*\*Can't list domain example.com.: Query refused**

### • الأداة **dig**

**Dig** أداة أخرى عظيمة لاستخراج المعلومات من **DNS**. تعمل مع نظام التشغيل لينكس فقط للعمل مع الامر **dig**. فنحن ببساطة نفتح الترمinal وندخل الأمر التالي:

**dig @target\_ip**

بطبيعة الحال، سوف يتم استبدال "target\_ip" مع عنوان IP الفعلي الذي تستهدفه. من بين أمور أخرى، **dig** يجعل من السهل جدا محاولة نقل المنطقة لذلك فهو تطوير لـ **nslookup** وأسهل منه في عملية نقل المنطقة (zone transfer). تجدر الإشارة إلى أن نقل المنطقة يستخدم لسحب سجلات متعددة من خادم **DNS**. في بعض الحالات، يمكن أن يؤدي نقل منطقة في إرسال ملقم **DNS** المستهدفة



كافة السجلات التي يحتوي عليها. هذا هو قيمة خاصة إذا كان الهدف الخاص بك لا يميز بين عناوين IP الداخلية والخارجية عند إجراء نقل المنطقة (**zone transfer**).

يمكننا محاولة نقل المنطقة مع `dig` باستخدام التبديل **[t@AXFR]**. إذا أردنا محاولة نقل المنطقة من الدومين ذات العنوان IP 192.168.1.23 إلى دومين وهي "example.com" نكتب الأمر التالي:

```
dig@192.168.1.23@example.com-t@AXFR
```

إذا سمح بعملية نقل المنطقة ولم تمنع، فإنك سوف تملك قائمة بأسماء المضيفين وعناوين IP من ملقم DNS المستهدف.

- بعض الأدوات الأخرى المستخدمة في عملية الاستطلاع عن DNS عن دومين معين كالتالي:

DIG available at <http://www.kloth.net>

myDNSTools available at <http://www.mydnstools.info>

Professional Toolset available at <http://www.dnsstuff.com>

DNS Records available at <http://network-tools.com>

DNSData View available at <http://www.nirsoft.net>

DNSWatch available at <http://www.dnswatch.info>

DomainTools Pro available at <http://www.domaintools.com>

DNS Lookup Tool available at <http://www.webwiz.co.uk>

DNS Query Utility available at <http://www.webmaster-toolkit.com>

### الأدوات المستخدمة في عملية الاستطلاع عن DNS في نظام التشغيل كali/باك تراك فقط

في هذا الجزء، سوف نؤدي بعض الحيل باستخدام خدمة التعداد "enumeration service". خدمة التعداد هي العملية التي تسمح لنا بجمع المعلومات من الشبكة. سوف تقوم بدراسة تقنيات تعداد DNS [DNS enumeration]. تعداد DNS هي عملية تحديد كافة الخوادم لا DNS وإدخالات للمنظمة الهدف. تعداد DNS سوف يسمح لنا بجمع المعلومات الهامة عن المنظمة مثل أسماء المستخدمين وأسماء أجهزة الكمبيوتر، عناوين IP، وهكذا. كيف تفعل هذا؟

#### الأداة **DNSSwalk**

هذه الأداة هي **DNS database debugger**. ينفذ عمليات نقل المنطقة (**zone transfer**) من الدومين المحدد، ويتحقق من قاعدة البيانات بطرق عديدة لفحص التوافق الداخلي، وكذلك التصحيف وفقاً للتصریح الممنوح من قبل الملقم DNS. هذه الأداة مبرمجة بلغة بيرل. اسم الدومين المحدد في سطر الأوامر يجب أن تنتهي !!.

#### طريقة استخدامها:

تستخدم مع اسم الدومين هكذا `[dnswalk@3.2.1.in-addr.arpa.]` أو اسم الدومين العكسي، مثل `[dnswalk@podunk.edu.]` الأداة `:dnsenum`

هذه الأداة أقوى من `dnswalk` ومبرمجها هي الأخرى بلغة بيرل. تعمل هذه الأداة عن طريق كتابة الأمر التالي في الترمinal

```
Sdnsenum@--enum@www.google.com
```

```
root@jana:~# dnsenum --enum www.google.com
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.

----- www.google.com -----

Host's addresses:

www.google.com          87      IN      A       173.194.113.144
www.google.com          87      IN      A       173.194.113.145
www.google.com          87      IN      A       173.194.113.147
www.google.com          87      IN      A       173.194.113.148
www.google.com          87      IN      A       173.194.113.146

Name Servers:

www.google.com NS record query failed: NOERROR
root@jana:~#
```

## ما نوع المعلومات التي يمكن جمعها بواسطة dnsenum؟

- 1- الحصول على عنوان المضيف (hosts address) (السجل A) / الحصول على خوادم الأسماء DNS / الحصول على سجل mx .
- 2- تنفيذ استعلامات AXFR على خوادم الأسماء (DNS) والحصول على إصدارات BIND .
- 3- الحصول على أسماء النطاقات الفرعية الإضافية (subdomain) والأسماء الإضافية (extra name) عن طريق استخدام استعلام جوجل المتقدم (google scraping).
- 4- استخدام تقنية Brute force في تخمين أسماء النطاقات الإضافية (subdomain name) وذلك بواسطة ملف txt يحتوي على (subdomain name) 95 sub domain name ليرجعها في محاولته لمعرفة أسماء النطاقات الفرعية الحقيقة (subdomain name) .
- 5- بحسب نطاقات الشبكة من الفئة C وتنفيذ استعلامات whois عليها.
- 6- تنفيذ عمليات البحث العكسي (reverse lookup).
- 7- كتابة الناتج إلى ملف txt .

هذا بعض الخيارات الإضافية التي يمكن تشغيلها باستخدام Dnsenum وأنها تشمل ما يلى:

```
--threads [number]
-r
-d
-o
-w
--enum = [--threads 5 -s 20 -w]
```

يسمح لك بتعيين عدد العمليات التي سوف يتم تشغيلها في وقت واحد  
 يسمح لك بتمكين عمليات البحث العكسي [recursive lookup]  
 يسمح لك بتعيين تأخير الوقت بالثواني بين طلبات whois  
 يسمح لك لتحديد مكان إخراج الناتج  
 يسمح لك بتمكين استعلامات whois على نطاق الشبكة من النوع سى

يمكنك الاطلاع على باقي التعبيرات باستخدام .man  
**dnsmap** • الأداة

هي أيضاً تأثير مماثله للأدوات السابقتين (dnswalk , dnsenum) من ناحية إيجاد أسماء النطاقات الفرعية (subdomain name) من أجل عملية التخمين (brute forcing) من أجل عملية التخمين (wordlist). هذه الأداة يمكنها تخزين نتائجها في ملف، ويمكن استخدامها بدون صلاحيات المستخدم الجذري (root privilege). لاستخدام هذا الامر نكتب في терминал dnsmap كالتالي:

```
root@jana:~# dnsmap
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

usage: dnsmap <target-domain> [options]
options:
-w <wordlist-file>
-r <regular-results-file>
-c <csv-results-file>
-d <delay-millisecs>
-i <ips-to-ignore> (useful if you're obtaining false positives)

e.g.:
dnsmap target-domain.foo
dnsmap target-domain.foo -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap target-fomain.foo -r /tmp/ -d 3000
dnsmap target-fomain.foo -r ./domainbf_results.txt
```

```
root@jana:~#
```

عند كتابة هذا الامر بدون أي تعبيرات أخرى فإنه يعطيك قائمه بجميع التعبيرات التي من الممكنة ان تستخدم معه.

- [**-w**] يكتب بعدها مسار الملف wordlist الذي سوف يستخدم في brute forcing .
  - [**-r**] هذه تعنى regular-results-file تستخدم في تنظيم ناتج الامر في ملف الناتج .
  - [**-c**] هي اختصار ل CSV وهي نوع الملف الذي سوف تخزن فيه النتائج بطريقة منتظمة .
  - [**-d**] هي اختصار لكلمة delay وتعنى التأخير وذلك بالمilli ثانية .
  - [**-i**] هو اختصار لل IP وتعنى هنا IP الذي تريد تجاوزه في عملية الفحص (IP's To Ignore) .
- ثم بعد ذلك امثله لطريقة استخدام هـ الامر. هذه الأداة تأخذ بعض من الوقت لكي تعطي نتيجة نهائية.

## • الأداة dnsrecon

هي أيضاً إداه تشبه الأدوات السابقة الذكر وتقوم تقريباً بنفس المهام وتسخدم **brute force** لمعرفة النطاقات الفرعية (**subdomain**). تعمل هذه الأداة في شكل استعلام (**query**) وذلك على **NS** و**SOA** و**MX** وسجلات **DNS**. هذه الأداة تم تطويرها من قبل كارلوس بيريز باستخدام لغة البايثون.

في الوقت التي تم الكتابة فيه عن هذه الأداة، فإنها تدعم الآتي:

- 1- معرفة أسماء النطاقات الإضافية (**subdomain**) وأسماء المضيفين (**hostname**) باستخدام تقنية **brute force**.
- 2- تدعيم البحث عن السجلات الأساسية في ملقم **(A,NS,SOA,MX) DNS**.
- 3- التوسيع في عمليات البحث إلى **TLD** وذلك للドومين الهدف.
- 4- يدعم نقل المنطقة (**zone transfer**) لجميع سجلات **NS**.
- 5- يدعم البحث العكسي (**Reverse Lookup**).
- 6- يدعم سجلات **SRV**.

يبداً عمل هذه الأداة عن طريق كتابة الامر **dnsrecon.py** مع مجموعة من التعبيرات لتحديد طريقة عملها في الترمinal.

نجد ان هذه الأداة تأتي بمجموعه من التعبيرات/الخيارات التي تتيح لك الكثير من المميزات كالتالي:

- 1- استخدام هذه الأداة للحصول على السجلات التقليدية من ملقم **DNS** للدومن الهدف وذلك عن طريق استخدام التعبير **[ -d ]** والذي يوضع بعده اسم الدومن المستهدف. نستخدم معه أيضاً الخيار **[ -t ]** وذلك لتحديد نوع عملية الاستطلاع الذي تريده والذي يأتي معه العديد من الخيارات كالتالي:

**[ std ]** تعنى عمليات الاستطلاع التقليدية من ملقم **DNS** والتي تشمل السجلات الآتية

**SOA, NS, A, AAAA, MX and SRV if AXFR on the NS Servers fail.**

**[ rvl ]** تعنى عملية البحث العكسي.

**[ brt ]** تعنى استخدام تقنية **brute force**.

**[ srv ]** للبحث عن سجلات **SRV**.

**[ axfr ]** تستخدم لاختبار ملقم **DNS** هل تم اعداده بطريقة خاطئة وكان يدعم نقل المنطقة أم لا.

**[ goo ]** استخدام محرك البحث جوجل.

**[ tld ]** تعنى **TOP LEVEL DOMAIN**

```
root@jana:~# dnsrecon.py -t std -d google.com
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for google.com
[*] SOA ns1.google.com 216.239.32.10
[*] NS ns1.google.com 216.239.32.10
[*] NS ns4.google.com 216.239.38.10
[*] NS ns3.google.com 216.239.36.10
[*] NS ns2.google.com 216.239.34.10
[*] MX alt4.aspmx.l.google.com 74.125.25.27
[*] MX alt2.aspmx.l.google.com 173.194.69.27
[*] MX aspmx.l.google.com 173.194.66.27
[*] MX alt3.aspmx.l.google.com 173.194.71.26
[*] MX alt1.aspmx.l.google.com 173.194.70.27
[*] MX alt4.aspmx.l.google.com 2607:f8b0:400e:c03::1a
[*] MX alt2.aspmx.l.google.com 2a00:1450:4008:c01::1b
[*] MX aspmx.l.google.com 2a00:1450:400c:c05::1a
[*] MX alt3.aspmx.l.google.com 2a00:1450:4010:c04::1a
[*] MX alt1.aspmx.l.google.com 2a00:1450:4001:c02::1b
[*] A google.com 173.194.45.72
[*] A google.com 173.194.45.68
[*] A google.com 173.194.45.73
```

امثله أخرى:

**dnsrecon.py -t std -d google.com (Standard (-t std))**

**dnsrecon.py -t tld -d google.com (Top Level Domain (-t tld))**

**dnsrecon.py -t axfr -d club.net (Zone transfer (-t axfr))**

**dnsrecon.py -t rvl -i 66.249.92.100,66.249.92.150 (Reverse Record Enumeration (-t rvs))**

## • الأداة fierce

قبل الكلام عن هذه الأداة سوف نتكلم أولاً ما هو نقل المنطقة **zone transfers**؟

إذا كان المصطلح **نقل المنطقة** [**zone transfer**] غير مألوف لك او لا تعرفه، أو لا تعرف الآليات الكامنة وراء تحديات **DNS**، فأوصي بقده أن تقرأ حول هذا الموضوع قبل القراءة في الاستمرار. ويكيبيديا لديها بعض الرؤية في هذا المصطلح من خلال هذا الرابط:

[http://en.wikipedia.org/wiki/DNS\\_zone\\_transfer](http://en.wikipedia.org/wiki/DNS_zone_transfer)  
<http://support.microsoft.com/kb/164017/ar>

(English)  
(Arabic)

المصطلح **zone transfer** (نقل منطقة او تحويل المنطقة) هو مصطلح يستخدم للإشارة إلى العملية التي يتم نسخ محتويات ملف منطقة من ملقم DNS أساسي إلى ملقم DNS ثانوي.

نقل المنطقة ستحدث خلال أي من الحالات التالية:

- عند بدء تشغيل خدمة DNS على خادم/ملقم DNS الثانوي.
- عند انتهاء مدة صلاحية وقت التحديث.
- عندما يتم حفظ التغييرات إلى ملف المنطقة الأساسية وهناك قائمة إعلام.

أساساً، يمكن المقارنة بين نقل المنطقة (zone transfer) وبين استنساخ قاعدة بيانات (database replication) بين خوادم DNS ذات الصلة. عادة ما يتم إجراء تغييرات على ملفات المنطقة على ملقم DNS الأساسي ومن ثم يتم تكرارها من قبل نقل المنطقة (zone transfer) إلى الملقم/الخادم ثانوي.

لأجل، هناك الكثير من المسؤولين الذين يدعون خوادم DNS الخاصة بهم بطريقه خاطئة، ونتيجة لذلك، فإن أي شخص يسأل عن الحصول على نسخة من ملقم/خادم DNS يتلقى الطلب. وهذا يعني تسليم القراءة التخطيط لشبكة الشركة سواء هيكل الشبكة الخارجية او الداخلية على طبق من فضة.

الآن سوف نحاول القيام بعملية نقل المنطقة (zone transfer) للدومن [www.offensive-security.com](http://www.offensive-security.com). وذلك باستخدام الأمر `host` او الأمر `dig` في لينكس لمحاولة نقل المنطقة. يمكنك أيضاً معرف أسم ملقم/خادم DNS إما باستخدام `nslookup` أو باستخدام الأمر `host`.

```
root@jana:~# host -t ns offensive-security.com
offensive-security.com name server ns3.no-ip.com.
offensive-security.com name server ns1.no-ip.com.
offensive-security.com name server ns5.no-ip.com.
offensive-security.com name server ns4.no-ip.com.
offensive-security.com name server ns2.no-ip.com.
root@jana:~#
```

هنا قمنا بمعرفة اسم خادم الأسماء DNS للدومن [offensive-security.com](http://www.offensive-security.com) وذلك باستخدام الأمر `host` تم التعبير [t] الذي يوضح بعده نوع **record** التي تطلبها وهذا استخدمنا `ns` أي **record** الخاص بخادم الأسماء DNS.

```
root@jana:~# host -l offensive-security.com ns4.no-ip.com
; Transfer failed.
Using domain server:
Name: ns4.no-ip.com
Address: 204.16.254.44#53
Aliases:
```

```
Host offensive-security.com not found: 5(REFUSED)
; Transfer failed.
root@jana:~#
```

بعد الحصول على اسم خادم الأسماء DNS الخاص بالدومن [offensive-security.com](http://www.offensive-security.com) قمنا بعمل نقل منطقة (zone transfer) مع التعبير [I] ولكن نلاحظ ان العملية فشلت. وذلك لأن خادم الأسماء الخاص به تم اعداده جيداً.

للمساعدة في كتابة أسرار بيانت بلغة البایتون حيث تساعدك مباشرة في نقل المنطقة (zone transfer) يمكنك زيارة الرابط التالي:

<http://www.dnspython.org/examples.html>

كما ذاقينا سابقاً، فإن معظم المسؤولين اليوم لديهم ما يكفي من الخبرة لمنع الناس من استكمال نقل المنطقة [zone transfer] غير مصرح بها بشكل عشوائي. ومع ذلك، لم نقدر كل شيء. إذا فشل نقل المنطقة [zone transfer] ، هناك العبرات من الأدوات الجيدة لاستجواب [DNS interrogation] DNS **Fierce** هي وسيلة سهلة الاستخدام وعبارة عن سكريبت بيرل قوى التي يمكن أن توفر لك العبرات من الأهداف الإضافية. في كالي، يمكنك أن تجد **Fierce** في المجلد </usr/bin>. مرة أخرى، يمكنك ببساطة فتح الترمinal وكتابة الأمر "Fierce" (جنيا إلى جنب مع رموز التبديل(التعديلات) المطلوبة) ولكن تعلم في باك تراك لا بد من استدعائهما أولاً عن طريق الآتي:

Application → backtrack → Information gathering → network analysis → DNS analysis → fierce

يمكن استخدام هذه الطريقة في كالي أيضاً كالاتي:

Applications → Kali Linux → Information Gathering → DNS Analysis → fierce

هذا يطبع رسالة تساعدك على استخدام **fierce** وكيفية تشغيله.

يمكن تنفيتها إذا كنت لا تستخدم نظام تشغيل يدعم هذه الأداة عن طريق [apt-get install fierce].

سيبدأ هذا الاسكريبت من خلال محاولة إكمال نقل المنطقه [zone transfer] من الدومنين المحدد. في حال فشل هذه العملية، فإنه سوف يتحول إلى **brute-force host names** وذلك عن طريق إرسال مجموعة من الاستعلامات إلى ملف **DNS** الهدف. هذا يمكن أن يكون وسيلة فعالة للغاية لكتف أهداف إضافية.

لإجراء فحص لدومن مع الأداة "fierce" الذي يستخدم تقنيات مختلفة للعثور على كافة عناوين **IP** وأسماء المضيفين التي يستخدمها الهدف. يمكننا ذلك باستخدام الأمر التالي:

**root@kali:~# perl fierce.pl**

بما انه سكريبت من النوع بيرل فنقوم بتشغيله على النحو هذا ولكن هذا يؤدي الى ظهور الرسالة التالية:

**Can't open perl script "fierce.pl": No such file or directory**

هذا ليس جيدا ولكن ماذا حدث. هذه الرسالة تعنى خطأ (**bugs**) وهذا يعني انه لا يوجد الاسكريبت **fierce**.

```
root@jana:~# locate fierce.pl
root@jana:~# locate fierce
/usr/bin/fierce
/usr/share/applications/kali-fierce.desktop
/usr/share/doc/fierce
/usr/share/doc/fierce/changelog.Debian.gz
/usr/share/doc/fierce/copyright
/usr/share/kali-menu/applications/kali-fierce.desktop
/var/lib/dpkg/info/fierce.list
/var/lib/dpkg/info/fierce.md5sums
root@jana:~#
```

لذلك عند استخدام هذه الأداة نستخدمها كالتالي:

**Sfierce@dns@domain\_name\_on\_theinternet.com**

بعض المسائل التي من الممكن ان تقابلك عند استخدام **fierce** في بعض نسخ كالي هو ظهور الرسالة التالية عند استخدام الامر **fierce**.

**Okay, trying the good old fashioned way... brute force**

**Can't open hosts.txt or the default wordlist**

**Exiting...**

حل هذه المشكلة نذهب الى موقع الويب التالي:

<http://ha.ckers.org/fierce/hosts.txt>

حيث نجد ان هذه عبارة عن قائمة من الأسماء تحتوي على **2280** مضيف المستتركة. **Fierce** يستخدم هذه القائمة للبحث عن أسماء مضيف معين ضمن الدومنين. بعد ذلك نقوم بالبحث عن نطاق عناوين **IP** تم تفعيل عمليات البحث الحكسي لعناوين **IP**. نقوم بنسخ هذا الملف **hosts.txt** في المجلد الحالي (~، المجلد الرئيسي للجذر) وتشغيل **fierce** مرة أخرى.

يمكن استخدام التعبير [-wordlist] لتحديد مكان الملف **hosts.txt** الذي تكلمنا عنه من قبل إذا لم يستطيع تحديد مكانه.

أيضاً يمكن استخدام التعبير [-file] لإخراج ناتج البحث في ملف تم بتبعه اسم الملف الذي تريد حفظ ناتج البحث فيه.

```

root@jana:~# fierce -dns google.com
DNS Servers for google.com:
ns4.google.com
ns2.google.com
ns1.google.com
ns3.google.com

Trying zone transfer first...
    Testing ns4.google.com
        Request timed out or transfer not allowed.
    Testing ns2.google.com
        Request timed out or transfer not allowed.
    Testing ns1.google.com
        Request timed out or transfer not allowed.
    Testing ns3.google.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
 Nope. Good.
Now performing 2281 test(s)...
173.194.45.84 academico.google.com
173.194.45.80 academico.google.com
173.194.45.81 academico.google.com
173.194.45.83 academico.google.com

```

بعض الأمثلة الأخرى:

#### fierce@-dns@company.com (Standard Fierce scan)

أسلوب البحث الافتراضي لاستخدام الامر **fierce**

#### fierce@-dns@company.com@-wide (Standard Fierce scan and search all class c ranges found for PTR names that match the domain)

هذا يضمن أسلوب البحث الافتراضي للأداء **fierce** مع بحث لجميع النطاقات من الفئة C وذلك من أجل أسماء PTR التي تعادل الدومن

#### fierce@-dns@company.com@-only@zt (Fierce scan that only checks for zone transfer)

هذا يضمن فقط الفحص من أجل نقل المنطقة (**zone transfer**)

#### fierce@-dns@company.com@-ztstop (Fierce scan that does not perform brute forcing if a zone transfer is found)

الفحص باستخدام الأداء **fierce** لن يتم استخدام تقنية **brute forcing** إذا كان عملية نقل المنطقة (**zone transfer**) متاحة

#### fierce@-dns@company.com@-wildcstop (Fierce scan that does not perform bruteforcing if a wildcard is found)

الفحص باستخدام الأداء **fierce** لن يتم استخدام تقنية **brute forcing** إذا وجدت (**wildcard**)

#### • الأداة dnsdict6

هذه الأداة يطلق عليها أيضاً **THC-IPV6-ATTACK-TOOLKIT** أو **thc-ip6**. هي أيضاً أداة تشابه الأدوات السابقة الذكر في جمع المعلومات من ملقن **DNS**. بمجرد كتابتها في الترمinal بدون أي تغييرات فإنه يعطي جميع المساعدات الممكنة مع هذه الأداة.

#### فيما يلى طبيعة المعلومات التي يمكن جمعها بواسطة dnsdict6

- النطاقات الفرعية (**subdomain**).

- عنوانين **IPv6** سواء **IPv4** او

- سجلات **SRV**.

- سجلات خوادم الأسماء **[NS]** وسجلات خوادم البريد الإلكتروني **[MX]**.

#### To open dnsdict6 go to > Kali Linux > Information Gathering > DNS Analysis > dnsdict6

بمجرد فتح **dnsdict6** ، سوف تجد مختلف الخيارات التي تظهر على الشاشة. أفضل اختيار هو اتباع هذه الخيارات، لذلك لا تقم بتشغيل الامر مباشرة، ولكن حاول فهم ما يمكن القيام به بواسطة هذه الخيارات لذلك دعونا نرى فائدة هذه الخيارات مع الأمثلة التوضيحية:

#### - [dnsdict6@-4@url] – **[IPv4]**

- [-t@no.] تحديد عدد العمليات التي يمكن القيام بها. العدد الافتراضي هو 8 والحد أقصى هو 32

- [-d] لعرض معلومات **IPv6** او **IPv4** من سجلات **NS** و **MX** في ملقن الأسماء **DNS**

- [-S] أداء سجلات الخدمة **SRV**.

- [-smlx] هذه الخيارات هو لاختيار حجم القاموس يحمل في ترتيبه عوامل عده: **s** صغيرة، **m** متوسطة، **I** كبير، **x** اكبر.



```
Syntax: dnsdict6 [-d46] [-s|-m|-l|-x] [-t THREADS] [-D] domain [dictionary-file]
Enumerates a domain for DNS entries, it uses a dictionary file if supplied
or a built-in list otherwise. This tool is based on dnsmap by gnucitizen.org.

Options:
-4      also dump IPv4 addresses
-t NO   specify the number of threads to use (default: 8, max: 32).
-D     dump the selected built-in wordlist, no scanning.
-d     display IPv6 information on NS and MX DNS domain information.
-S     perform SRV service name guessing
-[smlx] choose the dictionary size by -s(mall=50), -m(edium=796) (DEFAULT)
       -l(arge=1416), or -x(treme=3211)
```

#### - المثال الأول

استخدامها في عمليات الاستطلاع بالإعدادات الافتراضية كالتالي:

```
root@jana:~# dnsdict6 facebook.com
Starting DNS enumeration work on facebook.com. ...
Starting enumerating facebook.com. - creating 8 threads for 798 words...
Estimated time to completion: 1 to 2 minutes
www.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
blog.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
dns.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
www2.facebook.com. => 2a03:2880:f008:307:face:b00c:0::1
dev.facebook.com. => 2401:db00:10:df02:face:b00c:0::1
new.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
secure.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
login.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
my.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
ca.facebook.com. => 2a03:2880:f008:301:face:b00c:0::1
beta.facebook.com. => 2a03:2880:10:8f11:face:b00c:0::1
```

هذا هو إخراج الأمر الذي يمكن القيام به، فإنه يدل على إدخالات DNS مختلفة على الشاشة مع عناوين IPv6 . يظهر لك هذه الأداة قائمة كبيرة من الإدخالات إذا كان الهدف هو كبير مثل الفيسبيوك، وجوجل.

#### - المثال الثاني

هذا سوف نقوم بعرض سجلات NS,MX DNS وذلك باستخدام التعبير [d] ونقوم بإضافة 4 إليه اذا كنت تريد العناوين المقابلة له من النوع IPv4 كالتالي:

```
root@jana:~# dnsdict6 -d4 facebook.com
Starting DNS enumeration work on facebook.com. ...
Gathering NS and MX information...
NS of facebook.com. is a.ns.facebook.com. => 69.171.239.12
NS of facebook.com. is b.ns.facebook.com. => 69.171.255.12
No IPv6 address for NS entries found in DNS for domain facebook.com.
MX of facebook.com. is msgin.t.facebook.com. => 173.252.79.16
No IPv6 address for MX entries found in DNS for domain facebook.com.

Starting enumerating facebook.com. - creating 8 threads for 798 words...
Estimated time to completion: 1 to 2 minutes
ns1.facebook.com. => 69.171.239.12
www.facebook.com. => 31.13.86.49
```

#### - الأداة dnsrevenum6

اداة بسيطة وسريعة وتحتاج اسرع اداه لعملية بحث عكسى باستخدام عناوين IPv6 من ملقم DNS

```
dnsrevenum6@dns-server@ipv6address
dnsrevenum6@dns.test.com@2001:db8:42a8::/48
```



## اللداة dnstracer

**Dnstracer** تستخدم هذه الأداة في تتبع سلسلة من خوادم DNS إلى المصدر. حيث يحدد من أين يحصل ملقم الأسماء (DNS) على معلوماته تم بتتبع هذه السلسلة من خوادم DNS إلى الخادم الذي تعطيه البيانات.

#dnstracer©www.mavetju.org (Search for the A record of www.mavetju.org on your local nameserver)

يستخدم في البحث عن السجل A للموقع [www.mavetju.org](http://www.mavetju.org) من خلال خالق الأسماء DNS الخاص بك.

#dnstracer©-s©.©-q©mx mavetju.org (Search for the MX record of mavetju.org on the root-nameserver)

يستخدم في البحث عن السجل عن الاسماء المدخلة **MX** للدومن **mavetju.org** في خادم الأسماء الجذري (**root-nameserver**). التحيل [s] يوضع بعده اسم خادم الأسماء **DNS** الذي ت يريد البحث فيه عن السجلات. الخيار [q] يوضع بعده نوع السجل الذي ت يريد أن تبحث عنه.

يستخدم في البحث عن السجل PTR للمضيف وذلك خاص بالعناوين من النوع IPv4.

يستخدم في البحث عن السجل PTR للمضيف وذلك خاص بالعناوين من النوع IPv6.

Serversniff

المصدر: <http://www.serversniff.net>

هو موقع ويب يحتوى على العديد من الأدوات التي يمكن استخدامها في جمع المعلومات وتم تقسيم هذه الأدوات في مجموعات كالتالي:

IP tools لحم كل المعلمات المتعلقة بالعنوان IP

**DNS** الخادم **Name Server**

DNS - Name Server



## **NETWORK FOOTPRINTING-8**

الخطوة التالية بعد استرداد معلومات DNS هي جمع المعلومات المتعلقة بشبكة الاتصال. لذا، فإننا الآن سوف ننافس عملية الاستطلاع عن الشبكة (network Footprinting)، والتي تغير الوسيلة لجمع المعلومات المتعلقة بالشبكة (network-related information). يصف هذا المقطع كيفية تحديد نطاق الشبكة (network range)، وتحديد نظام التشغيل، والمسار لكي تصل لهذه الشبكة (Traceroute)، وأدوات تتبّع المسار.

#### **(LOCATE NETWORK Range) تحديد نطاق الشبكة**

لتتنفيذ عملية الاستطلاع عن الشبكة **Network Footprinting** فإليك سوف تحتاج إلى جمع المعلومات الأساسية والهامة حول المنظمة الهدف مثل ماذان تفعل المنظمة، الذين يعملون لها وما نوع الأعمال التي يؤدونها. الإجابات على هذه الأسئلة تعطيك فكرة حول الهيكل الداخلي للشبكة الهدف.

بعد جمع المعلومات المذكورة أعلاه، فإن المهاجم يمكنه قيامه بتحصيل على نطاق الشبكة (**Network Range**) للنظام الهدف. يمكن للمهاجم أيضا الحصول على معلومات أكثر تفصيلاً عن قاعدة بيانات السجل الإقليمي بشأن تخصيص IP وطبيعة التخصيص (**Regional registry database regarding IP allocation and the nature of the allocation**). يمكن للمهاجم أيضا تحديد الشبكة الفرعية [**subnet mask**] للدومنين. يمكن للمهاجم أيضا تتبع الطريق بين النظام الخاص به والنظام الهدف أي بمعنى آخر معرفة جميع أجهزة التوجيه **router** التي يمر بها حتى يصل إلى الشبكة الهدف. هناك أداتين أكثر سعية لعملية التتبع (**traceroute tools**) وهي **VisualRoute** و **NeoTrace**. الحصول على عناوين IP الخاصة من الممكن أن تكون مفيدة بالنسبة للمهاجمين.

قامت **The Internet Assigned Numbers Authority [IANA]** بحفظ الكتل الثلاثة التالية من عنوان IP للشبكة الانترنت الخالصة: **192.168.0.0-172.31.255.255 (172.16/12 prefix)**, **10.0.0.0-10.255.255(10/8 prefix)**, **192.168.255.255 (192.168/16 prefix)**

نطاق الشبكة يمكنه ان يعطيك فكرة عن كيفية شكل الشبكة، الآلات الموجود في الشبكات على الحالية، وأنه يساعد أيضا على تحديد هيكل الشبكة (**network topology**) ، جهاز التحكم في الوصول، ونظام التشغيل المستخدم في الشبكة الهدف. للحصول على نطاق الشبكة الخاص بالشبكة الهدف، نقوم بإدخال عنوان IP الخاص بالخادم (الذي تم جمعه بواسطة **WHOIS**) في التطبيق (<https://www.arin.net/knowledge/rirs.html>) أو يمكنك الذهاب إلى الموقع (<https://www.arin.net/knowledge/rirs.html>) وإدخال الا IP للخادم الهدف في مربع النص **SEARCH Whois**. سوف تحصل على نطاق الشبكة الخاص بالشبكة الهدف. إذا لم يتم اعداد خادم الا DNS بشكل صحيح، فإن المهاجم لديه فرصة جيدة للحصول على قائمة بالأجهزة الداخلية على الخادم. أيضا، في بعض الأحيان يمكن للمهاجم تتبع الطريق إلى آل (trace a route)، ومن خلال هذا التتبع فإنه يمكنه الحصول على عناوين IP الداخلية، والتي قد تكون مفيدة.

**Network Whois Record**

```

Queried whois.arin.net with "n 207.46.232.182"...
NetRange:      207.46.0.0 - 207.46.255.255
CIDR:          207.46.0.0/16
OriginAS:
NetName:       MICROSOFT-GLOBAL-NET
NetHandle:     NET-207-46-0-0-1
Parent:        NET-207-0-0-0-0
NetType:       Direct Assignment
NameServer:    NS2.MSFT.NET
NameServer:    NS4.MSFT.NET
NameServer:    NS1.MSFT.NET
NameServer:    NS5.MSFT.NET
NameServer:    NS3.MSFT.NET
RegDate:       1997-03-31
Updated:       2004-12-09
Ref:           http://whois.arin.net/rest/net/NET-207-46-0-0-1
OrgName:       Microsoft Corp
OrgId:         MSFT
Address:       One Microsoft Way
City:          Redmond
StateProv:     WA
PostalCode:   98052
Country:       US
RegDate:       1998-07-10
Updated:       2009-11-10
Ref:           http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName:  Abuse
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@hotmail.com
OrgAbuseRef:   http://whois.arin.net/rest/poc/ABUSE231-ARIN

```

ملحوظة: سوف تحتاج إلى استخدام أكثر من إداه لجمع المعلومات عن الشبكة حيث استخدام إداه واحدة لن يكون لديه المقدرة في جمع المعلومات التي تريدها.

في كالي/إيك تراك لينكس  
▪ الأداة :**Dmitry**

هي إداه لديها القدرة على جمع أكبر قدر ممكن من المعلومات عن المضيف. من هذه المعلومات نطاقات النطاقات الفرعية (**subdomain**), عناوين البريد الإلكتروني، المعلومات المحدثة، **whois lookups**, **tcp port scan**، وأكثر من ذلك.



توجد في كالي في المسار التالي:

Application → Kali Linux → Information gathering → Live Host Identification → dmitry

```
root@jana:~# dmitry
Deepmagic Information Gathering Tool
There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
-o      Save output to %host.txt or to file specified by -o file
-i      Perform a whois lookup on the IP address of a host
-w      Perform a whois lookup on the domain name of a host
-n      Retrieve Netcraft.com information on a host
-s      Perform a search for possible subdomains
-e      Perform a search for possible email addresses
-p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@jana:~#
```

انظر الى كم التقنيات التي من الممكن ان تؤدي بواسطة هذه الاداء دعنا نستخدم الامر التالي:

**Sdmity@wnspb@targethost.com@o@/root/Desktop/dmitry-result**

هذا استخدم التعبير [w] وذلك لعمل **whois lookup** والتعبير [n] لجمع معلومات من **NetCraft** و [s] للبحث عن **subdomain**. واستخدم التعبير [o] لوضع ناتج البحث في ملف خارجي وهذا كما هو موضع في الملف التعريفي.

```
root@jana:~# dmitry -wnspb google.com -o /teba.txt
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to '/teba.txt.txt'

HostIP:173.194.112.71
HostName:google.com

Gathered Inic-whois information for google.com
-----
Domain Name: GOOGLE.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.GOOGLE.COM
```

#### ▪ الأداة netmask

تستخدم لمعرفة نطاق الشبكة لدومن معين كالاتى:

```
root@jana:~# netmask google.com
173.194.113.65/32
root@jana:~#
```

#### ▪ الأداة scapy

هذه الأداة لها العديد من الوظائف ولها أهمية خاصة والتي سوف تطرق اليها لاحقا ولكن ما يهمنا الان هو جمع المعلومات لنطاق الشبكة باستخدام هذه الأداة يبدا عمل هذه الأداة بكتابة الامر **scapy** في الترمinal فتعمل على انشاء **Interactive shell** اخر كالاتى:

```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> 
```

لمعرفة نطاق الشبكة لدومن معين نقوم بإدخال السطر التالي في **Interactive shell** للأداة **scapy** كالاتى:

```
ans,unans=sr(IP(dst="www.targethost.com/30", ttl=(1,6))/TCP())
```



```
root@jana:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> ans,unans=sr(IP(dst="www.google.com/30", ttl=(1,6))/TCP())
Begin emission:
*****Finished to send 24 packets.
```

نقوم بكتابة المسطر التالي للحصول على ناتج السطرين السابقين في جدول كالتالي:

```
ans.make_table( lambda (s,r): (s.dst, s.ttl, r.src) )
>>> ans.make_table( lambda (s,r): (s.dst, s.ttl, r.src) )
173.194.39.20 173.194.39.21 173.194.39.22 173.194.39.23
1 192.168.16.1 192.168.16.1 192.168.16.1 192.168.16.1
2 41.221.137.3 41.221.137.3 41.221.137.3 41.221.137.3
>>>
```

للحصول على **TCP traceroute** مع الأداة **scapy** نكتب السطرين التالي:

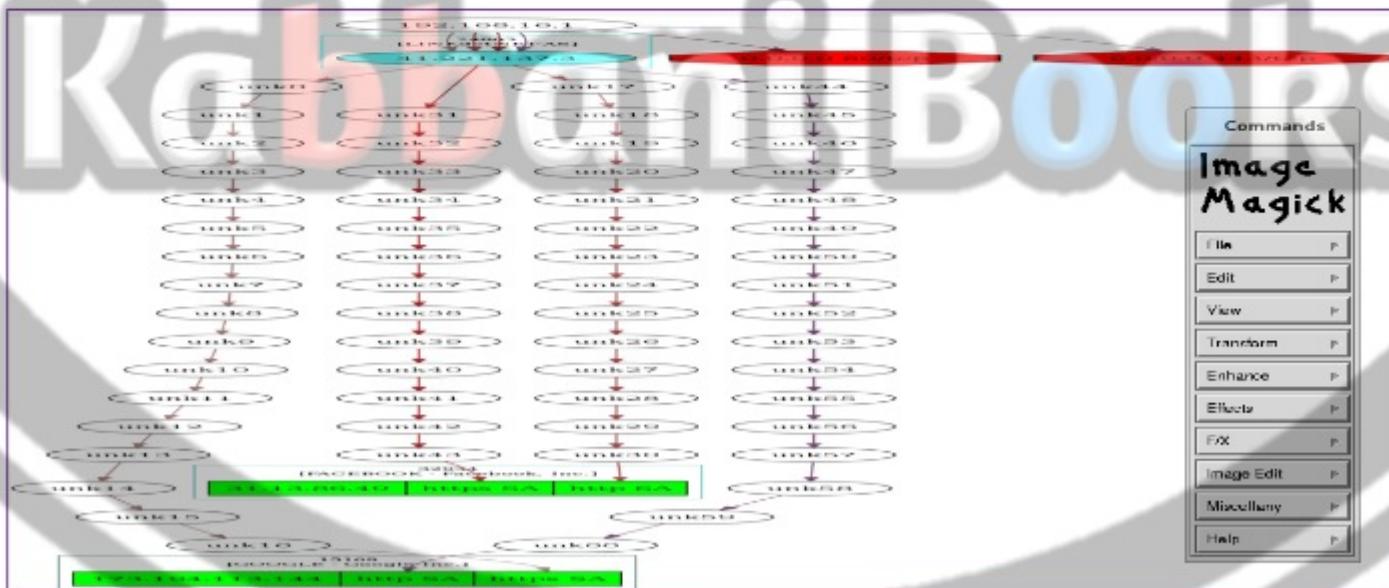
```
res,unans=traceroute(["www.google.com","www.Kali-
linux.org","www.targethost.com"],dport=[80,443],maxttl=20,retry=-2)
```

```
>>> res,unans=traceroute(["www.google.com","www.Kali-linux.org","www.facebook.com"],dport=[80,443],maxttl=20,retry=-2)
Begin emission:
*****Finished to send 120 packets.
*****Begin emission:
Finished to send 99 packets.
Begin emission:
Finished to send 99 packets.

Received 23 packets, got 21 answers, Remaining 99 packets
0.0.0.0:tcp443 0.0.0.0:tcp80 173.194.113.144:tcp443 173.194.113.144:tcp80 31.13.86.49:tcp443 31.13.86.49:
tcp80
1 192.168.16.1 11 192.168.16.1 11 192.168.16.1 11 192.168.16.1 11 192.168.16.1 11 192.168.16.1
11
2 - - - - 41.221.137.3 11 41.221.137.3 11 41.221.137.3 11 41.221.137.3
16 - - - - - - - - - - 31.13.86.49 SA -
17 - - - - - - - - - - 31.13.86.49 SA 31.13.86.49
18 - - - - - - - - - - 31.13.86.49 SA 31.13.86.49
19 - - - - - - - - - - 31.13.86.49 SA 31.13.86.49
20 - - - - - - - - - - 31.13.86.49 SA 31.13.86.49
21 - - - - - - - - - - 31.13.86.49 SA 31.13.86.49
>>>
```

لرؤية النتائج هذا في شكل رسومي نكتب السطرين التالي:

```
res.graph()
```



ويمكن حفظ النتائج في ملف خارجي باستخدام الصيغة الآتية:

```
res.graph(target="> /tmp/graph.svg")
```

للخروج نستخدم الصيغة `.exit()`



## (DETERMING THE OPERATING SYSTEM) تحديد نظام التشغيل

### NetCraft - 1

[المصدر:](http://news.netcraft.com)

حتى الآن قمنا بجمع المعلومات حول عنوانين IP، نطاقات الشبكة، أسماء الخوادم، وما إلى ذلك من الشبكة المستهدفة. الآن حان الوقت لمعرفة نظام التشغيل الذي يعمل في الشبكة الهدف. وتسمى هذه التقنية من الحصول على معلومات حول نظام التشغيل OS الخاص بالشبكة الهدف بـ **OS Footprinting**. وسوف تساعدك الأداة نيتكرافت على معرفة نظام التشغيل OS قيد العمل على الشبكة الهدف.

نيتكرافت هي شركة لمراقبة الانترنت مقرها في برانفورد أون أفون، إنكلترا. أبرز الخدمات التي يتم رصدها هذه الايام هو تقديم كتف عن نظام تشغيل الخادم. نيتكرافت يمكن استخدامها للعثور على غير مباشر عن المعلومات حول خادم الويب على شبكة الانترنت، بما في ذلك نظام التشغيل الأساسي، نسخة خادم الويب، الرسوم البيانية، وما إلى ذلك.

دعونا نرى كيف يساعدنا نيتكرافت في معرفة نظام التشغيل على الشبكة المستهدفة. نقوم بفتح العنوان التالي <http://news.netcraft.com> في متصفح الويب الخاص بك أي كان نوعه وكتابة اسم الدومن الخاص بالشبكة التي تستهدفها في الحقل (هذا سوف نستخدم اسم الدومن **microsoft.com** على سبيل المثال). فإنه يعرض جميع المواقع المرتبطة بهذا الدومن جنبا إلى جنب مع نظام التشغيل الذي يعمل على كل موقع كالتالي:

What's that site running?

[Subscribe to our RSS feed](#) [Get News updates by email](#)

**Microsoft neck and neck with Amazon in Windows hosting**

Microsoft has edged ahead of Amazon to become the largest hosting company as measured by the number of web-facing Windows computers. The pair have been neck and neck for almost nine months: Microsoft now has 23,400 web-facing Windows computers against Amazon's 22,600, barring companies with less connectivity separate to their business – including China.

فاظهر النتيجة كالتالي:

Netcraft Services

- Netcraft News
- Phishing & Security
- Anti-Phishing Toolbar
- Phishing Site Feed
- Hosting Phishing Alerts
- Fraud Detection
- Phishing Site Countermeasures
- Audited by Netcraft
- Open Redirect Detector
- Web Application Security Testing
- Web Application Security Course
- Internet Data Mining
- Wilton Dataset Websites
- Hosting Provider Switching Analysis
- Hosting Provider Server Count
- Hosting Reseller Survey
- SSL Survey
- Internet Exploration
- What's that site running?
- Search DNS
- Sites on the Move
- Performance
- Hosting Prospects
- Performance Alerts

Search Web by Domain

Explore 1,500,544 web sites visited by users of the Netcraft Toolbar

3rd March 2014

Results for microsoft.com

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		august 1995	ms hotmail	Windows server 2012
2. technet.microsoft.com		august 1999	microsoft corporation	Windows server 2012
3. qa.microsoft.com		november 2001	ms hotmail	Windows server 2008
4. support.microsoft.com		october 1997	microsoft corporation	unknown
5. windows.microsoft.com		june 1998	microsoft corporation	unknown
6. msdn.microsoft.com		september 1998	microsoft corporation	Windows server 2012
7. social.technet.microsoft.com		august 2000	microsoft corporation	citrix metacenter
8. office.microsoft.com		november 1998	microsoft corporation	unknown
9. answers.microsoft.com		august 2000	microsoft limited	Windows server 2008
10. social.msdn.microsoft.com		august 2005	microsoft corporation	citrix metacenter
11. download.microsoft.com		august 1999	akamai technologies	Linux
12. search.microsoft.com		january 1997	akamai technologies	Linux
13. e15officessetup.microsoft.com		may 2012	microsoft corporation	Windows server 2008
14. www.microsoft.com		www 1999	microsoft corporation	Windows server 2008

## SHODAN Search Engine -2

[المصدر: http://www.shodanhq.com](http://www.shodanhq.com)

يستخدم SHODAN Search Engine (routers, server, etc) بستخدام مجموعه واسعه من الفلتر.

The screenshot shows the SHODAN homepage with a search bar at the top containing the word "voip". Below the search bar is a world map with red dots indicating found devices. A banner below the map says "EXPOSE ONLINE DEVICES." and lists "WEBCAMS, ROUTERS, POWER PLANTS, IPHONES, WIND TURBINES, REFRIGERATORS, VOIP PHONES." Buttons for "TAKE A TOUR" and "FREE SIGN UP" are visible. Below the map, there's a section titled "IN THE PRESS" with several news snippets from various sources like The Register, threatpost, DerStandard, and ZDNet, each with a small thumbnail and a brief description.

The screenshot shows the SHODAN search results for "microsoft.com". The search bar at the top has "microsoft.com" in it. The results page shows two sections of search results. On the left, there's a snippet for "Did you mean: hostname[microsoft.com]". On the right, there are two main sections of results. The first section is for "87.106.87.87" (161 Internet AG) with a timestamp of "Analysed on 02.03.2014". The second section is for "220 microsoft.com" (Microsoft BEIMTP MAIL Service) with a timestamp of "Analysed on 02.03.2014". Both sections show detailed HTTP headers and responses. A sidebar on the right contains advertisements for Hurricane Labs and HackerTarget.

## TRACEROUTE

العثور على مسار [man-in-the middle] (target host) هو ضروري لاختبار ضد الهجمات من النوع [man-in-the middle] (route). تحتاج إلى العثور على مسار المضيف الهدف في الشبكة. وهذا يمكن أن يتحقق مع مساعدة من أداة تتبع المسار traceroute المقدمة مع معظم أنظمة التشغيل. فإنه يسمح لك بتنبيه المسار أو الطريق التي تمر من خلالها الحزم للمضيف الهدف عبر الشبكة.

تستخدم مفهوم **Traceroute** بروتوكول **TTL** الموجود في رأس الـ **IP** وذلك للعثور على مسار المضيف الهدف في الشبكة. وهذه الأداة يمكنها عرض التفاصيل حول مسار تحرك الحزم **IP** بين نظامين مختلفين. حيث أنه يمكن أن يعرض لك عدد الموجهات **routers** التي تمر بها الحزم خلال رحلته أو تحركه في الشبكة بين النظامين، المدة الزمنية التي تأخذها الحزمة ذهاباً وإياباً بين اثنين من أجهزة التوجيه [routers]، وإذا كان لدى أجهزة التوجيه إدخالات **DNS**، فإنه يعرض أيضاً أسماء الموجهات وشبكة الاتصال الخاصة بهم، فضلاً عن الموقع الجغرافي.

وهو يعمل عن طريق استغلال ميزة في بروتوكول الإنترنت تسمى **TTL** (Time to Live) للإشارة إلى العدد الأقصى من أجهزة التوجيه التي يمكن للحزمة [packet] أن تمر من خلاله. سيكون لكل جهاز توجيه **router** الذي يعالج الحزمة إنفاس مجال العد الخاص بالحقل **TTL** في رأس **ICMP** [TTL] تمر من جهاز إلى آخر أو يعني آخر أن الحزمة سوف تمر بعدد من أجهزة التوجيه لكي تصل إليك من خلال ذلك فإن كل جهاز توجيه [router] تمر من خلاله سوف يقوم بإيقاف رقم من الحقل **TTL** الموجود في بروتوكول **ICMP** تلو الآخر. عندما يصل العد صفر، سيتم تجاهل الحزمة وستحال رسالة خطأ إلى منسق الحزمة. لذلك فإن فكرة عمله يقوم عن طريق إرسال حزمة من النوع **ICMP** ويجعل **TTL** الموجود فيه يساوي واحد ويتم إرساله. أول موجة يقابل الحزمة [First router] يقوم بخصم رقم واحد من **TTL** فيصبح الرقم صفر وعند ذلك يتم تجاهل الحزمة وارسال رسالة إلى الجهاز المضيف أنه تم تجاهل الحزمة. هنا يتم تسجيل عنوان **IP** وأسم **DNS** الخاص بهذا الموجه (**router**)، ثم يقوم بإرسال حزمة أخرى ولكنها هنا تحمل **TTL** يساوي 2 لذلك فإن الحزمة يصنع طريقه من خلال الموجه الأول ويتجه إلى الموجه الثاني والذي يقوم هو الآخر بتجاهل الحزمة وارسال رسالة إلى الجهاز المضيف المنقى للحزمة أنه تجاهل الحزمة. ويستمر في فعل هذا وتسجيل عنوان **IP** وأسماء **DNS** إلى أن يصل إلى الجهاز الهدف أو أن يقرر أن الجهاز الهدف من المستحيل أن يصل إليه [unreachable]. في هذه العملية، فإنه يسجل الوقت الذي استغرقه كل حزمة في السفر ذهاباً وإياباً إلى كل جهاز التوجيه [router]. أخيراً، عندما يصل إلى المقصد، فإنه سوف يتم إرسال **ICMP ping** العادي إلى المرسل. وبالتالي، هذه الأداة تساعد في الكشف عن عنوان **IP** الخاصة بالـ **hops** الموجودة في المسار التي اتخذته الحزمة لكي يصل إلى المضيف الهدف.

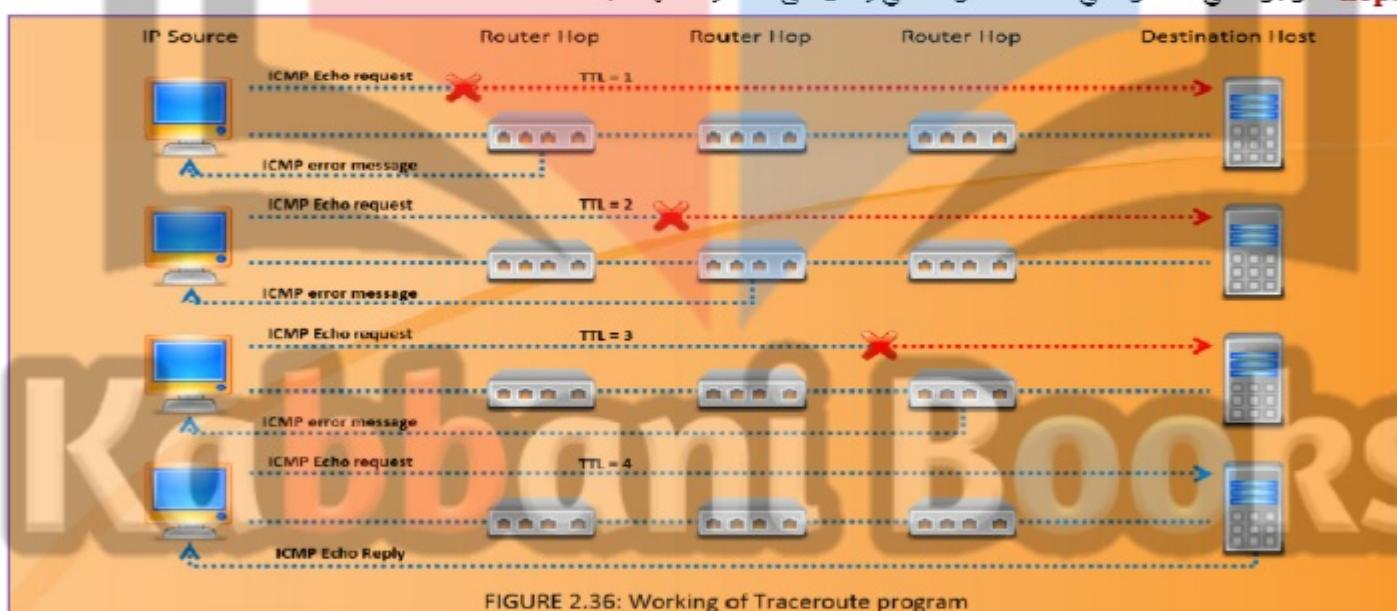


FIGURE 2.36: Working of Traceroute program

### كيفية استخدام الامر **tracert**

الذهاب إلى **command prompt** في نظام التشغيل ويندوز وكتابة الامر **tracert** متبعاً بعنوان **IP** الهدف أو اسم الدومن الهدف كالتالي:

C:\>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:

```

1 1262 ms    186 ms    124 ms  195.229.252.10
2 2796 ms    3061 ms    3436 ms  195.229.252.130
3 155 ms     217 ms    155 ms  195.229.252.114
4 2171 ms    1405 ms    1530 ms  194.170.2.57
5 2685 ms    1280 ms    655 ms  dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
6 202 ms     530 ms    999 ms  dxb-emix-rb.so100.emix.ae [195.229.0.230]
7 609 ms     1124 ms   1748 ms  iarl-so-3-2-0.Thameside.cw.net [166.63.214.65]
```



```
8 1622 ms 2377 ms 2061 ms eqixva-google-gige.google.com [206.223.115.21]
9 2498 ms 968 ms 593 ms 216.239.48.193
10 3546 ms 3686 ms 3030 ms 216.239.48.89
11 1806 ms 1529 ms 812 ms 216.33.98.154
12 1108 ms 1683 ms 2062 ms ns3.google.com [216.239.36.10]

Trace complete.
```

تحليل ناتج الامر traceroute analysis

لقد رأينا كيف يساعدك الأداة **Traceroute** في معرفة عنوانين IP للأجهزة الوسيطة مثل أجهزة التوجيه **router**، حدران الحمائية، وما إلى ذلك والذي يوجد بين المصدر والوجهة. هذا يمكنك من رسم الرسم التخطيطي [topology diagram] لشبكة الاتصال من خلال تحليل نتائج الأداة **Traceroute**. بعد تشغيل **traceroute** مرات عده، فإنك سوف تكون قادرًا على معرفة موقع أي **HOP** معينة في الشبكة المستهدفة. دعونا ننظر في نتائج **Traceroute** التالية التي تم الحصول عليها:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
  - traceroute 1.10.20.10, third to last hop is 1.10.10.1
  - traceroute 1.10.20.10, second to last hop is 1.10.10.50
  - traceroute 1.10.20.15, third to last hop is 1.10.10.1
  - traceroute 1.10.20.15, second to last hop is 1.10.10.50

من خلال تحليل هذه النتائج، فإن المهاجم يمكنه رسم خططه، للتحقق من الهدف على النحو التالي:

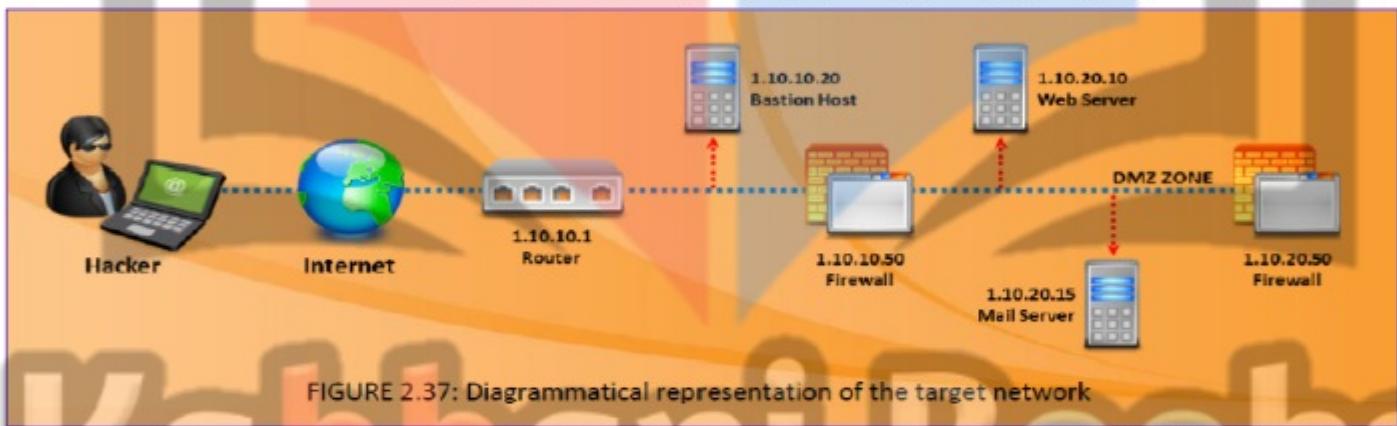


FIGURE 2.37: Diagrammatical representation of the target network

هذا الامر متوفّر ايضاً في نظام التشغيل لينكس باسم traceroute

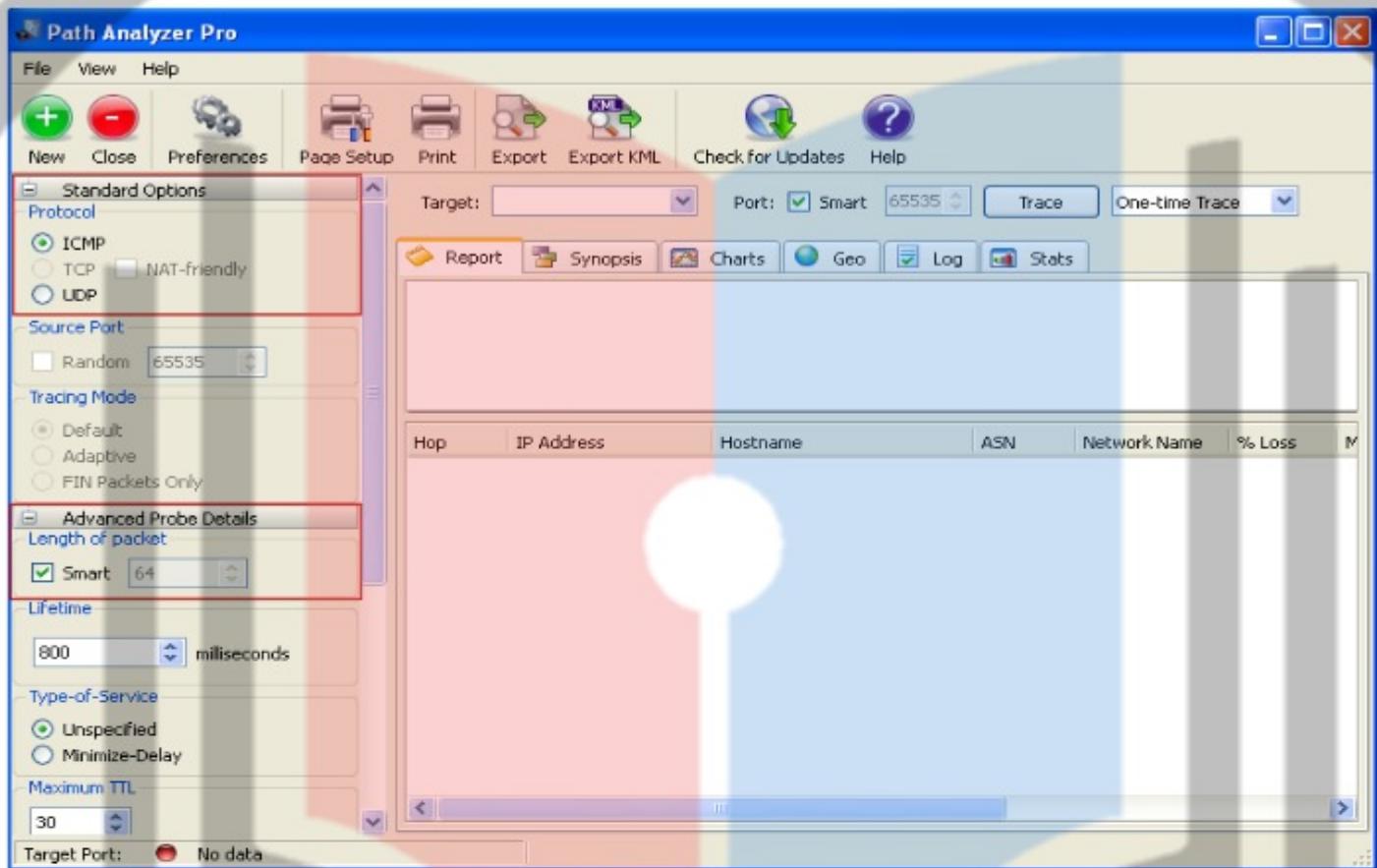
## TRACEROUTE TOOLS

و VisuaRoute 2010 Path Analyzer Pro هما أداتين يشبهوا في عملهم Traceroute وذلك للتبسيط مسار القبكة الهدف.

المصدر: <http://www.pathanalyzer.com>

**Path Analyzer Pro** هي أداة ذات وجه رسومي من النوع traceroute والتي تعمل على عرض المسار الذي تتخذه الحزمة من المصدر إلى الوجه بطريقه رسوميه. هي تزودك أيضاً بمجموعه من المعلومات الأخرى مثل رقم الـ hop التي يمر بها وعنوان IP الخاص به، واسم المضيف، ASN، اسم الشبكة، std. dev، avg. latency، latency %LOSS، وغيرها من المعلومات الخاصة بكل hop يمر به يمكنك أيضاً تحديد موقع الجغرافي للذي يملك عنوان IP الموجود في الشبكة الهدف. يمكنه أيضاً ان يكتف لك الفلاتر وجداران الحماية وبغض الأetiاء الأخرى الموجودة في الشبكة.

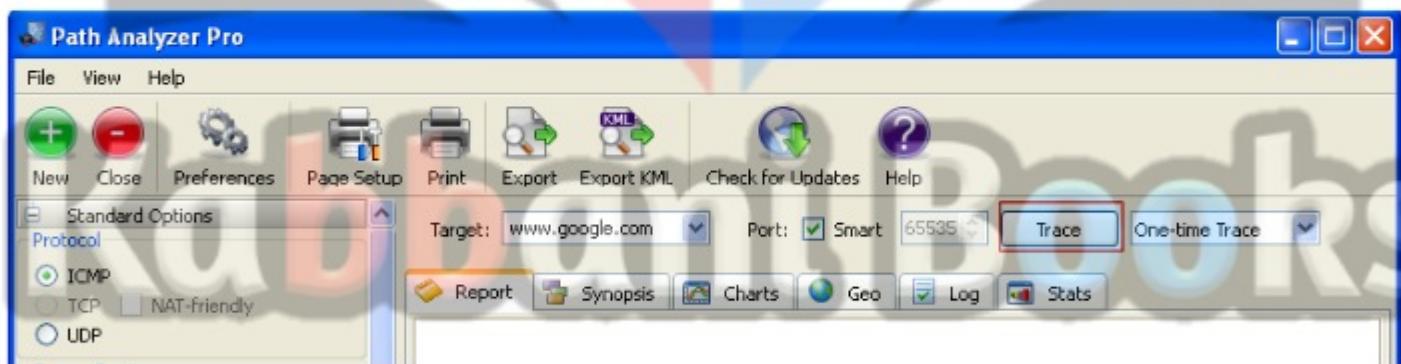
- 1- يقوم بتنبيه عن طريق اتباع الـ **wizard** الخاص بعملية التنبيه
  - 2- يقوم بفتح البرنامج الان عن طريق الخط من بين على الايقونة المعبّرة عنه.
  - 3- فتظهر رسالة تزيد منك التسجيل فنختار الخيار **Evaluate** لاستخدام النسخة



4- في الجزء **Standard Options** نختار **ICMP** وفى الجزء **Advanced Probe Details** نختار **smart** ونترك باقى الخيارات كما هى.

5- للحصول على نتائج أفضل يجب الغاء تفعيل جدار الحماية لديك.

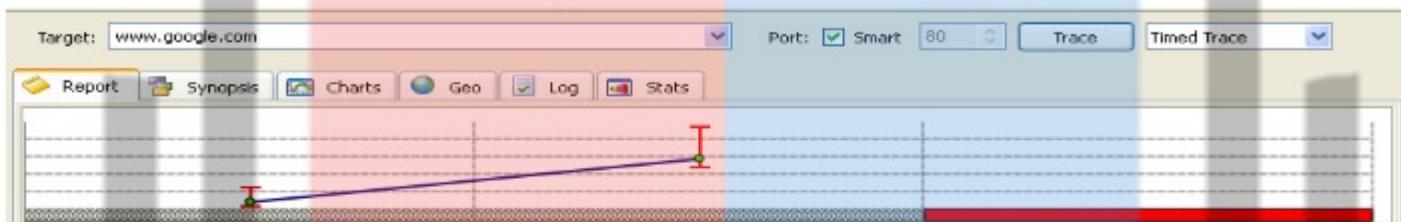
6- تقوم بكتابة اسم الدومن الهدف في الخانة المقابلة لـ **target** ولتكن مثلا [www.google.com](http://www.google.com) ويكون كالتالى:



7- في الخانة المقابلة للزر **Trace** نختار من القائمة المنسدلة **Timed Trace** بدلا من **One-time Trace** تم نصطف على الزر **HH:MM:SS** فتظهر شاشه أخرى تضع فيها الوقت المستغرق في عملية التتبع ولتكن مثلا 3 دقائق حيث يستخدم التشكيل **Trace** تم الضغط على الزر **Accept** بعد الانتهاء من عملية تتبع المسار تظهر النتائج كالتالى:



- 8- يمكن الضغط على **Report** وذلك لظهور لك الرسم البياني الخطى لمسار الحزمة من المصدر الى الهدف.
- 9- يمكن الضغط على **Synopsis** وذلك لظهور لك ملخص علمية للتتبع [traceroute].
- 10- يمكن الضغط على **Charts** وذلك لظهور لك الرسم البياني لعملية التتبع التي قمت بها.
- 11- يمكن الضغط على **Geo** وذلك لظهور لك خريطة تخليله توضح المسار الذى اخذهت الحزمة من المصدر الى الهدف.
- 12- يمكن حفظ هذه العملية فى ملف خارجي عن طريق الضغط على زر **Export**.



ملحوظه هذا التطبيق متوفـر أـيضاً عـلى جـمـيع نـظـمـة التشـفـيل الأـخـرى مـثـل ماـك وجـنـو/لينـكس.

## VisualRoute 2010 - 2

[المصدر:](http://www.visualroute.com) <http://www.visualroute.com>

تطبيق اخر قائم على الوجه الرسومية وهي أداة آخرى للتتبع تعرض لك تحليلاً **hop-by-hop**. وأنها تمكنك أيضاً من تحديد الموقع الجغرافي للموجهات **routers** والخادم **server** وأجهزة **IP** الأخرى. أنها قادرة على توفير معلومات التتبع في ثلاثة أشكال: تحليلاً شامل **[geographical view of the routing]** ، في جدول بيانات **[in a data table]** ، وعرض جغرافي للموجهات **[an overall analysis]** . جدول البيانات يحتوى على معلومات مثل رقم **hop**، عنوان **IP**، اسم **node** والموقع الجغرافي، وهكذا حول كل مرحلة في الطريق. المميزات التي يعرضها كالاتى:

[Hop-by-hop traceroutes, Reverse tracing, Historical analysis, Reverse DNS, Ping plotting, Port probing, Firefox and IE plugin]



FIGURE 2.39: VisualRoute 2010 screenshot

يوجـد بعض الأـدـوات الأـخـرى التـي تـشـبـه فـي عملـها كـل مـن **VisualRoute Path Analyzer Pro** كـالـاتـى:

Network Pinger available at <http://www.networkpinger.com>

GEOSpider available at <http://www.oreware.com>

vTrace available at <http://vtrace.pl>

Trout available at <http://www.mcafee.com>

Roadkil's Trace Route available at <http://www.roadkil.net>

Magic NetTrace available at <http://www.tialsoft.com>

3D Traceroute available at <http://www.d3tr.de>

Analogx HyperTrace available at <http://www.analogx.com>

Network Systems Traceroute available at <http://www.net.princeton.edu>

Ping Plotter available at <http://www.pingplotter.com>



## ٩- عملية الاستطلاع من خلال الهندسة الاجتماعية (FOOTPRINTING THROUGH SOCIAL ENGINEERING)

حتى الآن ناقشنا تقنيات مختلفة لجمع المعلومات إما بمساعدة موارد أو أدوات الإنترنت. الأن سوف نناقش عملية الاستطلاع عن طريق الهندسة الاجتماعية، فن الاستيلاء على المعلومات من الناس عن طريق التلاعب بهم. يعطي هذا القسم مفهوم الهندسة الاجتماعية والتقنيات المستخدمة لجمع المعلومات.

**الهندسة الاجتماعية social engineering:** هي عملية غير فنية (non-technical) تماماً والتي يقوم فيها المهاجم بالاحتيال على الشخص الهدف والحصول منه على المعلومات السرية حول الشبكة/المنظمة الهدف مثل هذه الطريقة يكون الشخص الهدف غير مدرك لحقيقة أن شخصاً ما يقوم بسرقة المعلومات السرية منه. في الواقع إن المهاجم يلعب لعبة ماكرة مع الهدف من أجل الحصول على معلومات سرية. المهاجم يستفيد من طبيعة مساعدة الناس وضيقهم لتقديم معلومات سرية.

لأداء الهندسة الاجتماعية، عليك أولاً كسب ثقة المستخدم المصرح له تم خداعه للكشف عن المعلومات السرية. الهدف الأساسي من الهندسة الاجتماعية هو الحصول على المعلومات السرية المطلوبة تم استخدام هذه المعلومات في عملية القرصنة مثل الوصول غير مصرح به إلى النظام [gaining unauthorized access to the system] ، سرقة الهوية، التجسس الصناعي، التخلف على الشبكة، ارتکاب عمليات الاحتيال، وما إلى ذلك. من المعلومات التي يتم الحصول عليها عن طريق الهندسة الاجتماعية قد تشمل تفاصيل بطاقة الائتمان، أرقام الضمان الاجتماعي، أسماء المستخدمين وكلمات السر والمعلومات الشخصية الأخرى وأنظمة التسخين وإصدارات البرامج، عناوين بروتوكول الإنترنت، أسماء الخوادم، معلومات تحطيم الشبكة، وأكثر من ذلك بكثير. المهندسين الاجتماعيين يقوموا باستخدام هذه المعلومات لاختراق النظام أو ارتکاب عمليات احتيال.

الهندسة الاجتماعية يمكن أن تؤدي بكثير من التقنيات المختلفة مثل

### - التنصت [eavesdropping]

#### Shoulder surfing

- البحث في قمامه المنظمة الهدف (dumpster diving)

- الانتحال على موقع الشبكات الاجتماعية impersonation on social networking sites

كما ذكر سابقاً **dumpster driving, shoulder surfing, eavesdropping** هي تقنيات ثلاثة مستخدمة لجمع المعلومات عن طريق الأشخاص الذين يستخدمون الهندسة الاجتماعية. دعونا نناقش هذه التقنيات الخاصة بالهندسة الاجتماعية لفهم الكيفية التي يمكن أن يؤديها في الحصول على معلومات سرية.

## EAVESDROPPING (التنصت)

التنصت [eavesdropping] هو فعل الاستماع سراً إلى المحادثات بين الناس سواء من خلال الهاتف أو محادثات الفيديو بدون موافقتهم. يشمل أيضاً قراءة الرسائل السرية من وسائل الاتصال مثل الرسائل الفورية أو رسائل الفاكس. وبالتالي، فإنه في الأساس فعل اعتراض الاتصالات دون موافقة طرف الاتصال. مكاسب المهاجم من هذا هو جمع المعلومات السرية من خلال الاستفادة من التنصت على محادثة هاتفية، واعتراض ملفات الصوت والفيديو، أو الاتصال الكتابي.

## SHOULDER SURFING

مع هذه التقنية، فإن المهاجم يقف وراء الضحية ويلاحظ أنشطة الضحية على الكمبيوتر مثل ضربات المفاتيح أثناء إدخال أسماء المستخدمين وكلمات السر وغيرها سراً.

يستخدم هذا الأسلوب عادةً للحصول على كلمات السر، PINs، الرموز الأمنية، أرقام الحسابات، معلومات بطاقة الائتمان، وبيانات مماثلة. فإنه يمكن أن يؤديها في مكان مزدحم لأنه من السهل نسبياً الوقوف وراء الضحية دون معرفته.

## DUMPSTER DIVING

هذه التقنية معروفة أيضاً باسم **trashing**، حيث يقوم المهاجم بالحصول على المعلومات من القمامه الخاصة بالشركة الهدف. قد يحصل المهاجم على معلومات حيوية مثل فواتير الهاتف، معلومات الاتصال، المعلومات المالية والمعلومات المتعلقة بالعمليات، مطبوعات للكود المصدر (printouts of source code)، مطبوعات من المعلومات الحساسة، وغيرها من المعلومات وذلك من صناديق القمامه الخاصة بالشركة الهدف، وصناديق القمامه الخاصة بالطابعة، ملاحظات لاصقة في مكاتب المستخدمين، وما إلى ذلك من المعلومات التي تم الحصول عليها يمكن أن تكون مفيدة للمهاجمين لارتكاب عملية القرصنة.



## 10- عمليات استطلاع من خلال شبكات التواصل الاجتماعي [FOOTPRINTING THROUGH SOCIAL NETWORKING SITE]

على الرغم من ان عملية الاستطلاع من خلال مواقع الشبكات الاجتماعية تبدو مماثلة لعملية الاستطلاع عن طريق الهندسة الاجتماعية، ولكن هناك بعض الاختلافات بين الطرقتين. في عملية الاستطلاع عن طريق الهندسة الاجتماعية، فإن المهاجم يتحاول على الناس للكتف عن المعلومات في حين أنه في عملية الاستطلاع من خلال مواقع الشبكات الاجتماعية، فإن المهاجم يجمع المعلومات المتاحة من خلال مواقع الشبكات الاجتماعية. حيث يمكن للمهاجمين استخدام مواقع الشبكات الاجتماعية كوسيلة لتنفيذ هجمات الهندسة الاجتماعية. ويوضح هذا القسم كيف وماذا يمكن جمعه من المعلومات من مواقع الشبكات الاجتماعية عن طريق الهندسة الاجتماعية.

### عملية الاستطلاع باستخدام الهندسة الاجتماعية من خلال موقع التواصل الاجتماعي

موقع الشبكات الاجتماعية هي خدمات عبر الإنترنت أو نلاين، المنصات، أو الموقع الذي تسمح للناس بالتواصل مع بعضهم البعض، وبناء العلاقات الاجتماعية بين الناس. استخدام موقع الشبكات الاجتماعية في تزايد سريع. أمثلة على موقع الشبكات الاجتماعية تشمل **google+, Pinterest, Twitter, LinkedIn, Myspace, Facebook** ومميزاتها الخاصة. قد يكون القصد موقع واحد للاتصال بالأصدقاء والأسرة وغيرها، وأخر قد يكون القصد لتبادل التشكيلات المهنية وغيرها وموقع الشبكات الاجتماعية مفتوحة للجميع. المهاجمون قد يستفيدون من هذا لانتزاع المعلومات الحساسة من المستخدمين إما عن طريق التصفح من خلال لمحات عامة عن المستخدمين أو عن طريق خلق صورة وهمية وخداع المستخدم لاعتقاد انه مستخدم حقيقي. هذه المواقع تسمح للناس بالبقاء على اتصال مع الآخرين، الحفاظ على الشخصية المهنية، وتبادل المعلومات مع الآخرين. على موقع الشبكات الاجتماعية، يقوم الناس بنشر معلومات مثل تاريخ الميلاد، المستوى التعليمي، خلفيه عن العمل، أسماء الزوجين، وغيرها، الشركات قد تنشر معلومات مثل القراء المحتملين، والمواقع، والأخبار القائمة عن الشركة. بالنسبة للمهاجمين، فإن موقع الشبكات الاجتماعية يعتبر مصدراً كبيراً للتور على معلومات عن الشخص الهدف أو الشركة. هذه المواقع تساعد مهاجم لجمع المعلومات فقط التي تم تحديدها من قبل الشخص أو الشركة. المهاجمين يمكنهم بسهولة الوصول إلى الصفحات العامة لهذه الحسابات. للحصول على مزيد من المعلومات حول الهدف، فإن المهاجمين يقومون بإنشاء حسابات وهمية واستخدام الهندسة الاجتماعية لإغراء الضحية للكتف عن مزيد من المعلومات. على سبيل المثال، يمكن للمهاجم إرسال طلب صدقة إلى الشخص الهدف من حساب وهمي، وإذا قبل الضحية طلبه، فإن المهاجم يمكنه الوصول إلى صفحات محدودة عن الشخص المستهدف على هذا الموقع. وبالتالي، فإن موقع الشبكات الاجتماعية يمكنها أن تكون مصدراً فيما للمعلومات عن المهاجمين.

### المعلومات المتاحة على موقع التواصل الاجتماعي (INFORMATION AVAILABLE IN THE SOCIAL NETWORKING SITE)

حتى الأن، لقد ناقشنا كيف يمكن للمهاجم انتزاع المعلومات من مواقع الشبكات الاجتماعية، والآن سوف نناقش ما هي المعلومات التي يمكن للمهاجم الحصول عليها من موقع الشبكات الاجتماعية. الناس عادة يقوم بإنشاء صفحة شخصيه على موقع التواصل الاجتماعي من أجل توفير المعلومات الأساسية عنهم وللحصول على علاقة مع الآخرين. يحتوي الملف الشخصي عموماً على بعض المعلومات مثل الاسم ومعلومات الاتصال (رقم الهاتف النقال، البريد الإلكتروني)، معلومات الأصدقاء، معلومات عن أفراد الأسرة، اهتماماتهم، والأنشطة، الخ. الناس عادة يرتبطون بأصدقائهم ويقومون بالدردشة معهم. يمكن للمهاجمين جمع المعلومات الحساسة من خلال الأحاديث الخاصة بهم. موقع الشبكات الاجتماعية يسمح أيضاً لناس بمشاركة الصور والفيديو مع أصدقائهم. إذا كان الناس لا يقومون بتعيين إعدادات الخصوصية الخاصة بهم لأنفسهم، فإن المهاجمين يمكنهم الاطلاع على الصور ومقاطع الفيديو المقتربة من قبل الضحية. يمكن للمستخدمين الانضمام إلى مجموعات للعب الألعاب أو لتبادل وجهات النظر والاهتمامات. المهاجمون يمكنهم انتزاع المعلومات حول اهتمامات الضحية من خلال تتبع مجموعة تم يمكنه ان يتحاول على الضحية للكتف عن مزيد من المعلومات. يمكن للمستخدمين إنشاء أحداث لإعلام المستخدمين الآخرين حول المناسبات القادمة. مع هذه الأحداث، يمكن للمهاجمين كشف أدق قطط الضحية. بالنسبة للأفراد، والمنظمات يمكنهم ان يستخدموا موقع التواصل الاجتماعي للتواصل مع الناس، والترويج لمنتجاتهم، وجمع الملاحظات حول منتجاتهم أو خدماتهم، الخ.

أنشطة المنظمة على موقع التواصل الاجتماعي والمعلومات ذات الصلة التي يمكن للمهاجم انتزاعها هي كما يلى:

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Background check to hire employees	Type of business

TABLE 2.1: What organizations Do and What Attacker Gets

## جمع المعلومات عن طريق الفاسبوك [COLLECTION FACEBOOK INFORMATION]



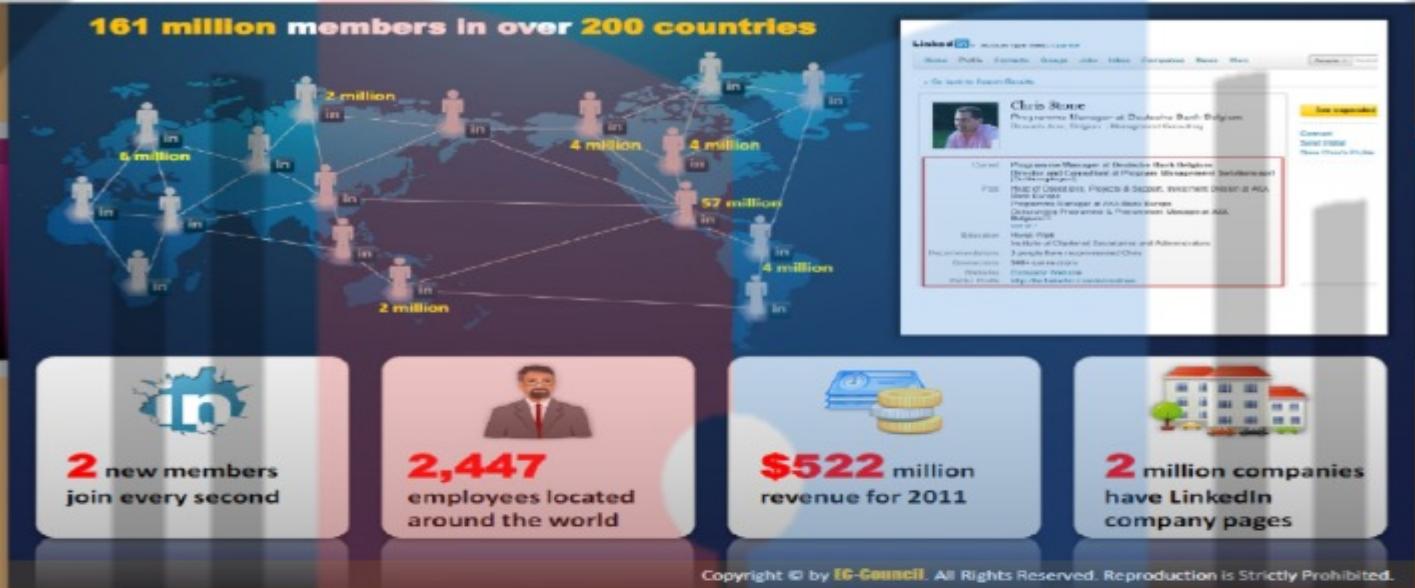
الفاسبوك هو واحد من أكبر مواقع التواصل الاجتماعي في العالم، حيث يملك أكثر من 845,000,000 مستخدم نشط شهرياً في جميع أنحاء العالم. أنه يتبع للناس إنشاء الصفحة الشخصية الخاصة بهم، إضافة الأصدقاء، تبادل الرسائل الفورية، إنشاء أو الانضمام إلى مجموعات أو مجتمعات مختلفة، وأكثر من ذلك بكثير. يمكن للمهاجم الاستيلاء على جميع المعلومات التي قدمتها الضحية في الفاسبوك. لانتزاع المعلومات من الفاسبوك، ينبغي أن يكون للمهاجم حساب نشط. المهاجم يقوم بتسجيل الدخول للحساب الخاص به، يقوم بالبحث عن الشخص المستهدف أو المنظمة. تصف الملف الشخصي للشخص الهدف قد يكشف الكثير من المعلومات المقيدة مثل رقم الهاتف، رقم البريد الإلكتروني، الأصدقاء، التفاصيل التعليمية، التفاصيل المهنية، الاهتمامات، الصور، وأكثر من ذلك بكثير. يمكن للمهاجم استخدام هذه المعلومات لمزيد من التخطيط لعملية القرصنة، مثل الهندسة الاجتماعية، للكشف عن مزيد من المعلومات حول هذا الهدف.

## جمع المعلومات عن طريق التويير [COLLECTION TWITTER INFORMATION]



تويير هو موقع تواصل الاجتماعي آخر ذات سعيه كبرى يستخدمها الناس لإرسال وقراءة الرسائل النصية [text-based messages]. فإنه يسمح لك بتتبع أصدقائك، والخبراء والمتأثرين المفضليين لك، وما إلى ذلك. هذا الموقع أيضاً يمكن أن يكون مصدراً كبيراً للمهاجمين للحصول على معلومات حول الشخص الهدف. هذا مفيد في استخراج المعلومات مثل المعلومات الشخصية، معلومات الأصدقاء، أنشطة الشخص الهدف التي تم نشرها باسم تويير، أما الذي يتبعه الهدف [following]، المستخدمين الذين يتبعون الهدف، الصور التي يتم تحميلها، وما إلى ذلك. المهاجم قد يحصل على معلومات مقيدة من تويير المستخدم الهدف.

## [COLLECTION LINKEDIN INFORMATION] LINKEDIN جمع المعلومات عن طريق لينكدين



على غرار الفاسبوك وتويتر، **LinkedIn** هو موقع آخر للتواصل الاجتماعي للمتخصصين **professionals**. أنه يتيح للناس إنشاء وإدارة صفحته الشخصية وتعريفها. أنه يسمح للمستخدمين لبناء والانخراط مع شبكتهم المهنية. وبالتالي، فإن هذا يمكن أن يكون مصدر معلومات كبير بالنسبة للمهاجم. المهاجم قد يحصل على معلومات مثل تفاصيل التوظيف الحالية وتفاصيل العمل الماضية وتفاصيل التعليم وتفاصيل الاتصال، وأكثر من ذلك بكثير عن الشخص الهدف. المهاجم يمكنه جمع كل هذه المعلومات مع عملية الاستطلاع **[Footprinting]**.

## [COLLECTION YOUTUBE INFORMATION] جمع المعلومات عن طريق يوتيوب



اليوتيوب هو موقع ويب على شبكة الانترنت يتيح لك رفع ومشاهدة ملفات الفيديو ومشاركة من خلال العالم كله. المهاجم يمكنه عن طريق اليوتيوب البحث عن جميع ملفات الفيديو المرتبطة بالهدف ومن خلالها جمع المعلومات عنه.

## ( تتبع المستخدمين على مواقع التواصل الاجتماعي ) TRACKING USERS ON SOCIAL NETWORKING SITES

من أجل حماية أنفسنا من الاختيال عبر الإنترنت والهجمات، فإن الأشخاص الذين يعانون من المعرفة القليلة حول جرائم الإنترنت يستخدمون هويات وهمية على مواقع التواصل الاجتماعي. في مثل هذه الحالات، فإنك لن تحصل على معلومات دقيقة عن المستخدم الهدف. لذلك لتحديد الهوية الحقيقة للمستخدم الهدف، يمكنك استخدام أدوات مثل **Get Someone's IP or IP-GRABBER** لتنبيه الهويات الحقيقة للمستخدمين.

إذا كنت ت يريد أن تتبع هوية مستخدم معين، فإنه يجب عليك القيام بما يلى:

- قم بفتح متصفح الويب لديك تم قم بطبع عنوان URL التالي فيه:

<http://www.myiptest.com/staticpages/index.php/how-about-you>

- نلاحظ الحقول الثلاثة الموجودة في الجزء السفلي من صفحة الويب، **Redirect URL: http:// Link for person** أو **Link for you**

Find / Get someones IP Address

Can I get someones IP Address ?  
The answer is both yes and maybe, and it may not do you any good. Try this tool to find someones IP Address.

Link for person: <http://www.myiptest.com/img.php?id=u3bdquryey&rdr-www.g>

Redirect URL: <http://www.gmail.com>

Link for you:  
[http://www.myiptest.com/staticpages/index.php/how-about-you?id=u3bdquryey&show\\_ip=1](http://www.myiptest.com/staticpages/index.php/how-about-you?id=u3bdquryey&show_ip=1)

**Topics**  
What's this (FAQ)

**Friend Sites**  
Hosting  
Neighbors

**Blacklist IP check**

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

FIGURE 2.44: Tracing identity of user's

## 2.4 أدوات عملية الاستطلاع FOOTPRINTING TOOLS

يمكن القيام بها عن طريق مساعدة من الأدوات. العديد من المنظمات تقدم الأدوات التي تجعل جمع المعلومات مهمة سهلة. هذه الأدوات ضمن الحد الأقصى من المعلومات التي يمكن جمعها. في هذا الجزء سوف يتم شرح استخدام هذه الأدوات في جمع المعلومات من مصادر مختلفة.

### FOOTPRINTING TOOL: MALTEGO

المصدر: <http://paterva.com>

في نظام التشغيل ويندوز

Maltego هو تطبيق مفتوحة المصدر يتميز بالذكاء وتطبيق الطلب السريع [intelligence and forensics application]. يمكن استخدامه لمراقبة جميع المعلومات لجميع الأعمال المتعلقة بالأمن [Security related work]. Maltego هو عبارة عن منصة وضعت لتقديم صورة واضحة للتهديدات الممكنة على البيئة التي تملکها وتغيرها منظمة ما. يمكن أن تستخدم لتحديد العلاقات والروابط في العالم الحقيقي بين الناس، القبائل الاجتماعية، الشركات والمؤسسات والواقع الإلكتروني، والبنية التحتية للإنترنت (الدوامين وأسماء عناوين IP)، والجارات [phrases]، والانتماءات [affiliations]، والوثائق، والملفات.

Internet Domain

Personal Information

FIGURE 2.45: Maltego showing Internet Domain and personal information

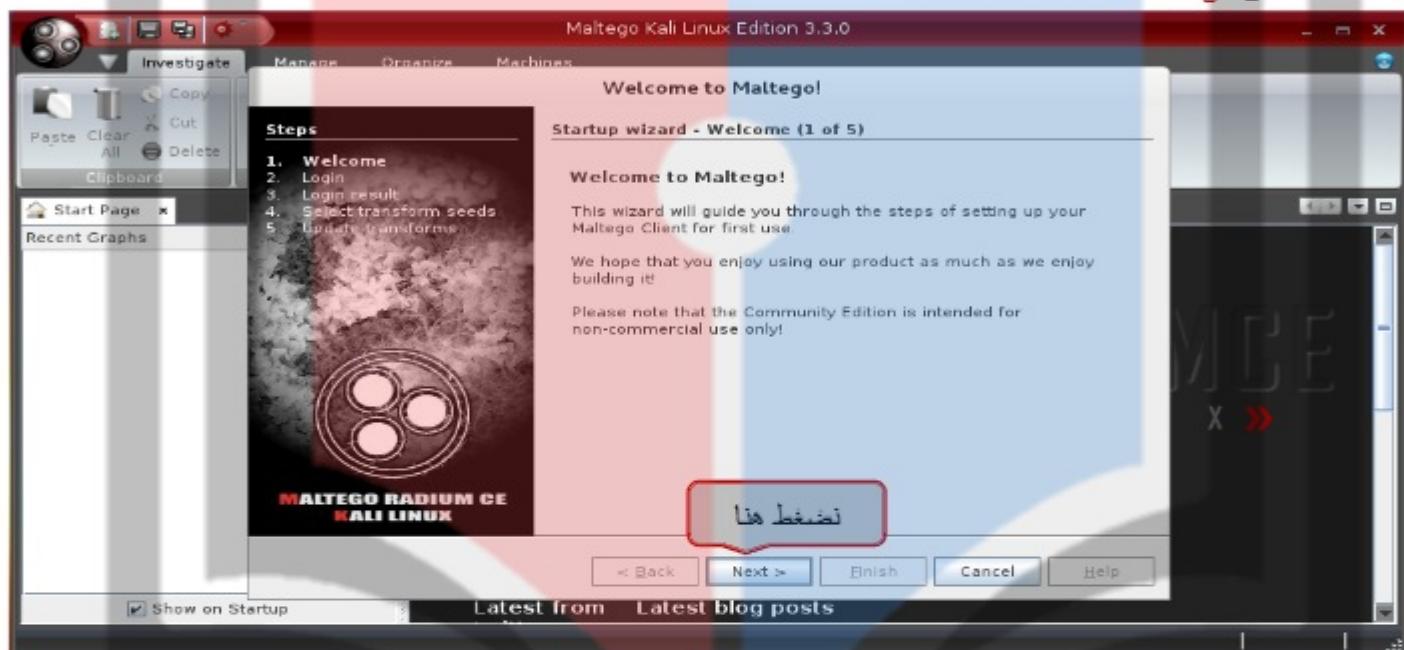
في نظام التشغيل كالي/باك تراك

**Maltego** هي أداة استطلاع متعددة الأغراض التي يمكن جمع المعلومات المقتوية العامة على شبكة الإنترنت. لديه إمكانيات استطلاع **DNS**، ولكنه يذهب أعمق من ذلك بكثير في عمليات جمع المعلومات. فإنه يأخذ المعلومات ويعرض النتائج في الرسم البياني للتحليل.

لبدء المعلومات، انقل إلى قائمة **Application** في كالي، وانقر على القائمة **Maltego**. تم حدد

### Information Gathering → DNS Analysis → Maltego

الخطوة الأولى لاستخدام **Maltego** هو التسجيل فيه. لا يمكنك استخدام التطبيق من دون التسجيل.  
بعد الضغط على **Maltego** تظهر الشاشة التالية:



كما قلنا سابقاً لابد من التسجيل في البرنامج أولاً وإجراء عملية التسجيل نذهب الى الرابط التالي ونعمل على تسجيل لبياناتنا فيه:

<https://www.paterva.com/web6/community/maltego/>

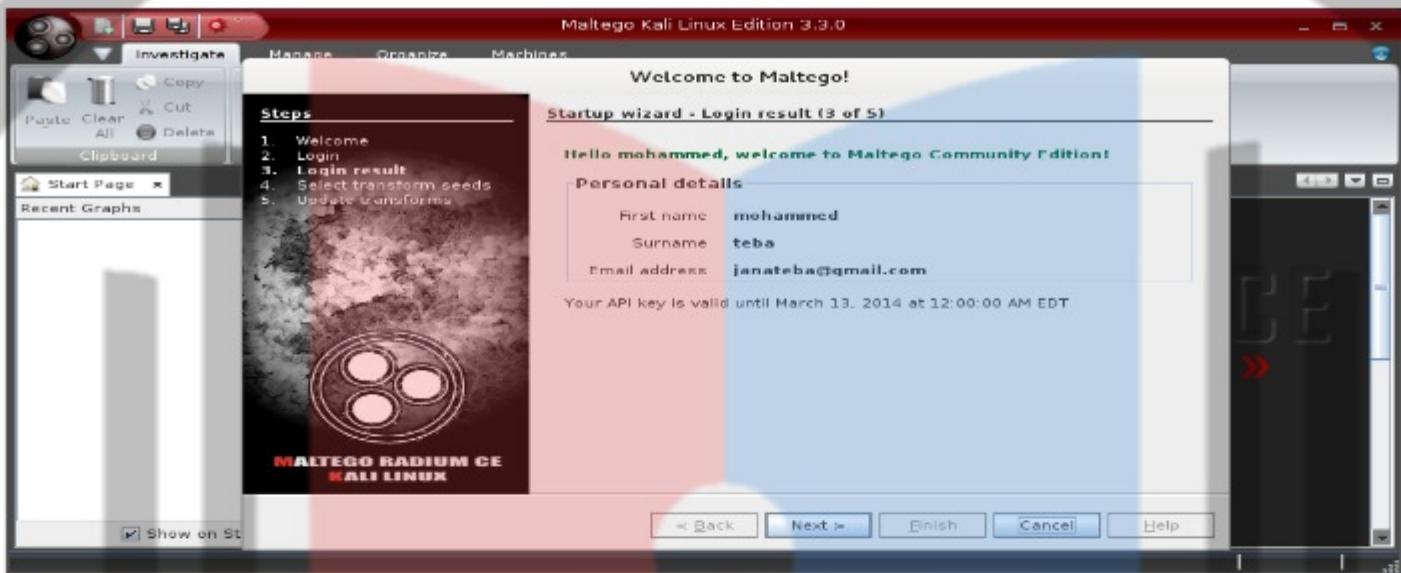


ندخل البيانات التي استخدمناها في عملية

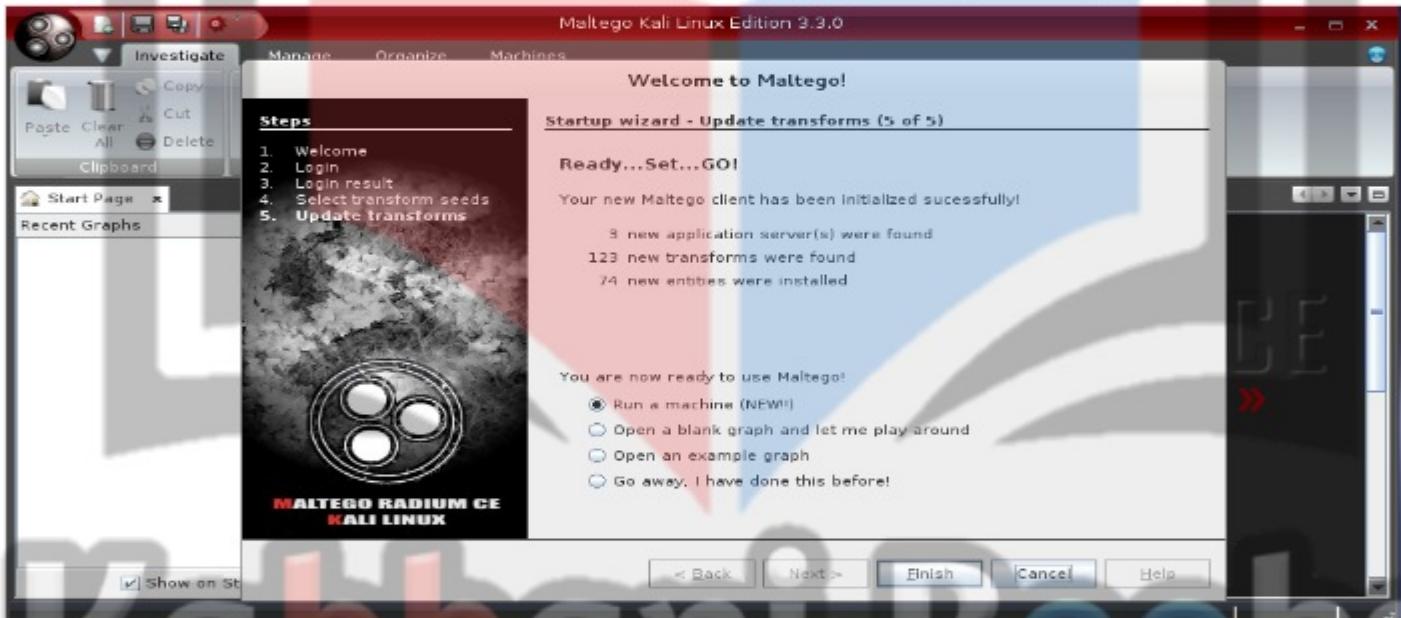
التسجيل تم تضغط

Next





ثم نضغط **next** حتى تصل إلى الشاشة التالية تم نضغط **Finish** كالتالي:



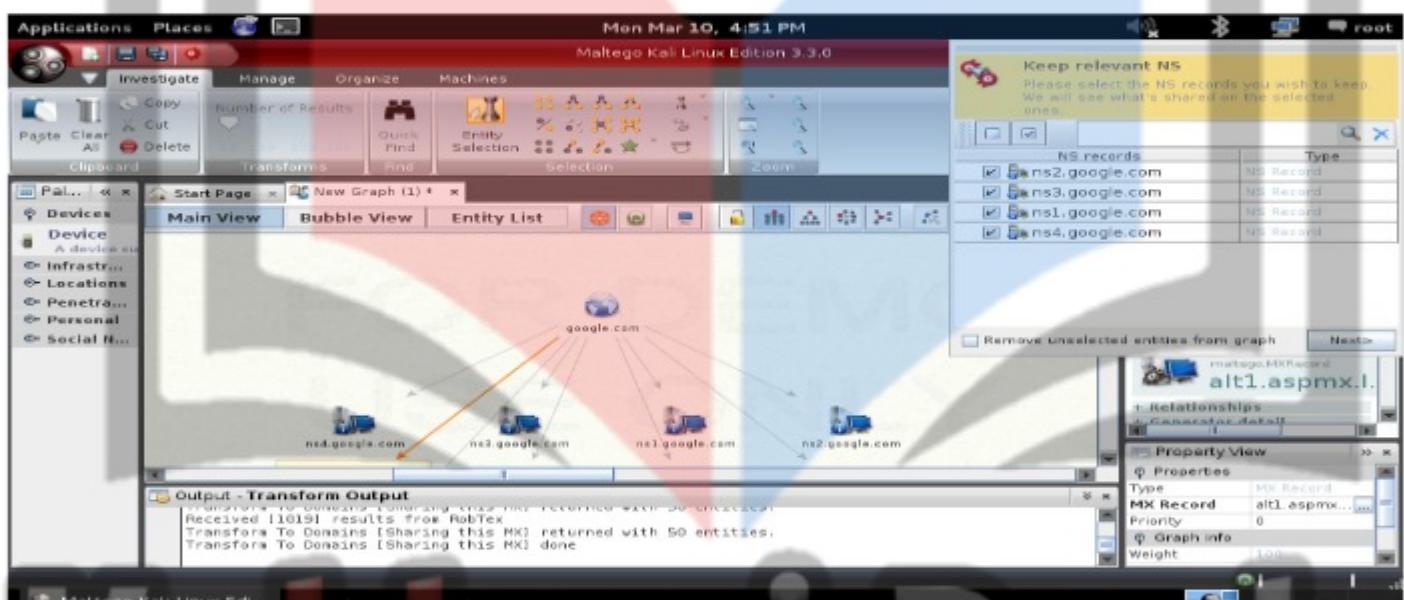
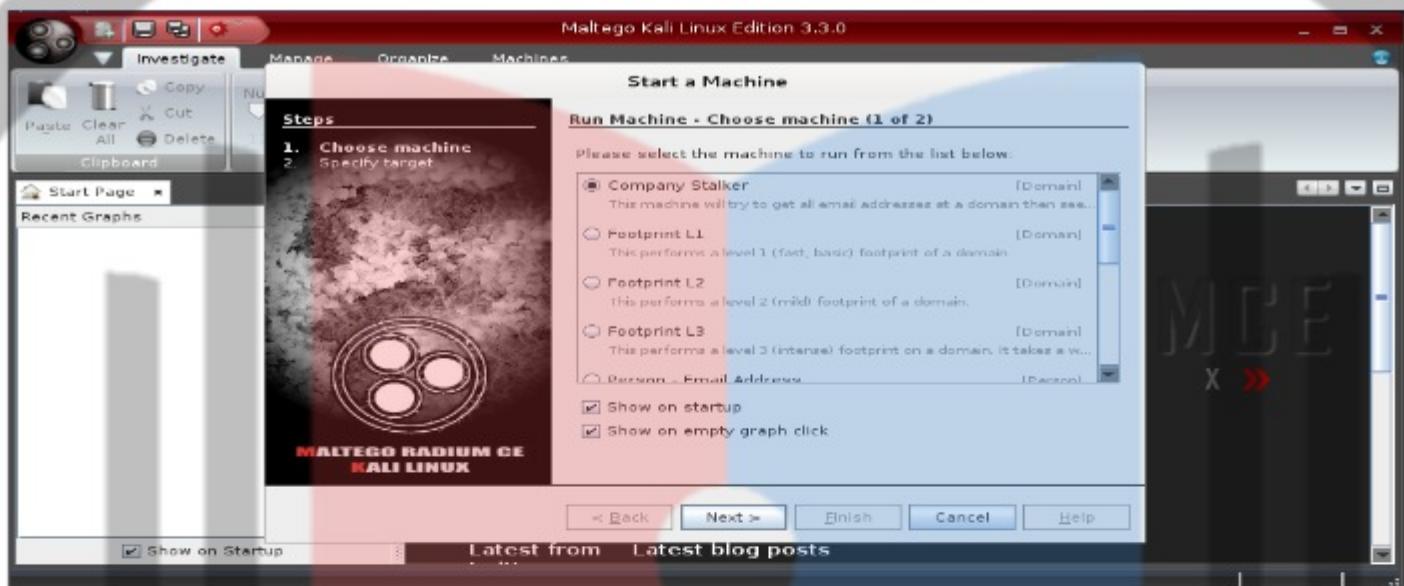
لديه طرق عدة لجمع المعلومات. أفضل طريقة لاستخدام **Maltego** هو الاستفادة من معالج بدء التشغيل (**run a machine**) لتحديد نوع المعلومات التي ترغب في جمعها. المستخدمين ذوي الخبرة قد يريدون أن يبدأ مع رسم بياني فارغة (**open a blank graph**) أو تخطي هذا الـ **wizard**. قوة **Maltego** هي أنه يتيح لك مراقبة بصرية للعلاقة بين الدومين، والمنظمة، والناس. يمكنك التركيز حول منظمة معينة، أو نظرة على منظمه والشركات ذات الصلة من استعلامات **DNS**.

اعتماداً على خيارات الفحص المختارة فإن **Maltego** يمكنه أداء المهام التالية:

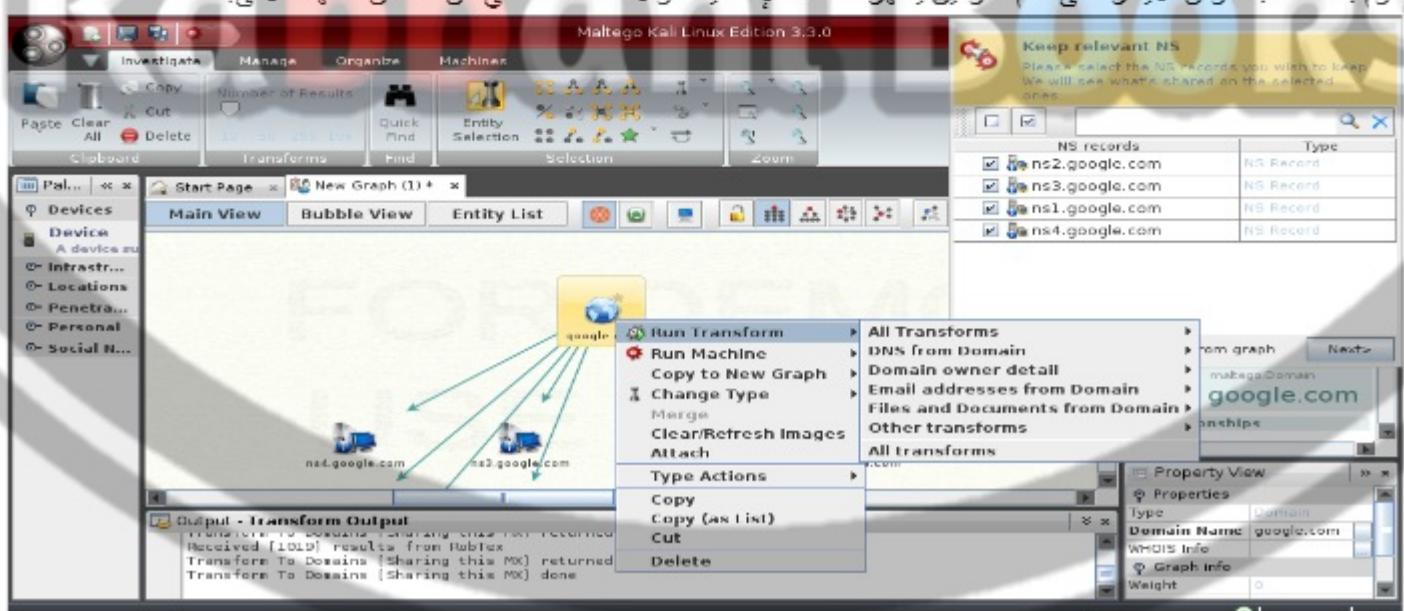
- 1 [Associate an e-mail address to a person] ضم عناوين البريد الإلكتروني للأشخاص.
- 2 [Associate websites to a person] ضم مواقع الويب للأشخاص.
- 3 [Verify an e-mail address] التحقق من البريد الإلكتروني.
- 4 [Gather details from Twitter, including geo location of pictures] جمع المعلومات من تويتر، بما في ذلك تحديد الموقع الجغرافي للصور.
- 5 جمع أرقام التليفونات والتكنولوجيا من المعلومات عن طريق استخدام محركات البحث.

ملحوظة: هذا التطبيق من أهم التطبيقات في جمع المعلومات.

معظم الميزات لا تحتاج إلى تفسير، وتتمثل كيفية استخدامها بتحت وصف الميزة. ويستخدم عادة **Maltego** في جمع المعلومات واستخدامها في بعض الأحيان كخطوة أولى خلال هجوم الهندسة الاجتماعية.



نقوم بالضغط بالماوس الأيسر على اسم الدومنين يظهر مختلف الإمكانيات والاستعلامات التي من الممكن إداتها كالتالي:



## FOOTPRINTING TOOL: DOMAIN NAME ANALYZER PRO

المصدر: <http://www.domainpunch.com>  
**Domain Name Analyzer Professional** هو برنامج على نظام التشغيل ويندوز لإيجاد وإدارة والحفظ على أسماء الدومن المتعددة. أنها تدعم عرض البيانات الإضافية (expiry and creation dates, name server information)، علامات الدومن، عمليات بحث **whois** التأكدي (TV.NET.COM for thin model whois TLDs).



## FOOTPRINTING TOOL: WEB DATA EXTRACTOR

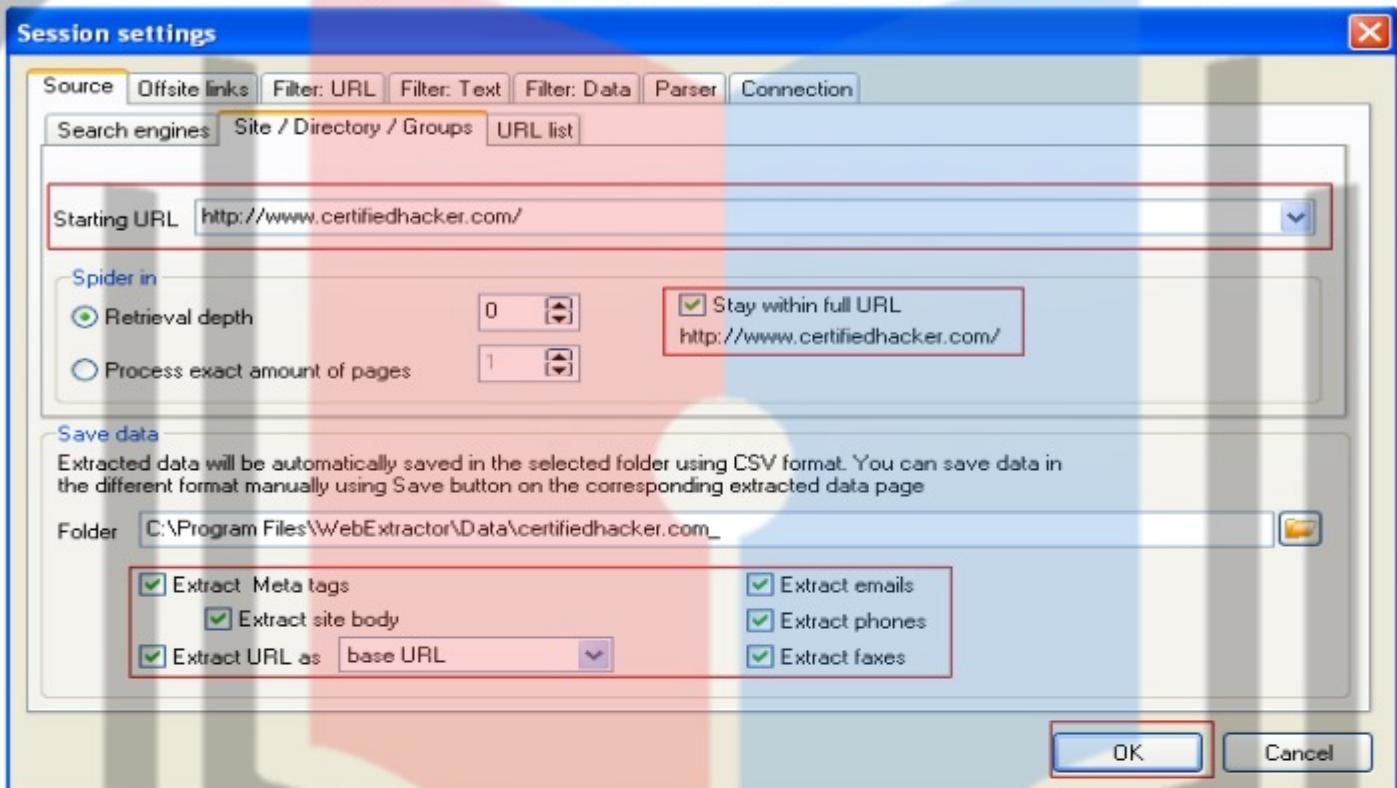
المصدر: <http://www.webextractor.com>  
**Web Data Extractor** هو أداة لاستخراج البيانات. فإنه يعمل على استخراج بيانات الاتصال للشركة الهدف (البريد الإلكتروني، والهاتف، والفاكس) من شبكة الإنترنت. يعمل على استخراج عنوانين **URL** والعالمة الوصفية **meta tag** (العنوان، **desc**)، الكلمة الرئيسية (العنوان، **title**) لتعزيز الموقع، يبحث عن منقى الدومنين، وما إلى ذلك.  
 المهاجمون يبحتو باستمرار عن أسهل الطرق لجمع المعلومات. هناك العديد من الأدوات المتاحة للمهاجمين التي بواسطتها يمكنهم استخراج قاعدة بيانات الشركة. بمجرد الوصول إلى قاعدة البيانات، فإنه يمكن أن يجمع عنوانين الموظفين، البريد الإلكتروني، أرقام الهاتف، عنوانين الواقع الداخلي في الشركة، وهكذا. مع هذه المعلومات التي تم جمعها فإنه يمكن إرسال رسائل البريد الغير مرغوبة [spam email] للموظفين لملء صندوق البريد الخاص بهم، اقتحام الموقع الإلكتروني للشركة، تعديل عنوانين الواقع الداخلي. كما أنها قد تتيح بعض الفيروسات الخبيثة لجعل قاعدة البيانات غير صالحة للعمل. باعتبارك مختبر اختراق، فإنه يجب عليك أن تكون قادرًا على التفكير من وجهة نظر القرصان ومحاولة غلق كل السبل الممكنة لجمع المعلومات عن المنظمات. يجب أن تكون قادرًا على جمع كل المعلومات السرية لتنظيم وتنفيذ ميزات الأمان لمنع تسرب بيانات الشركة.

1- تقوم بتنبيه التطبيق باتباع الـ **wizard** الخاص بعملية التثبيت.

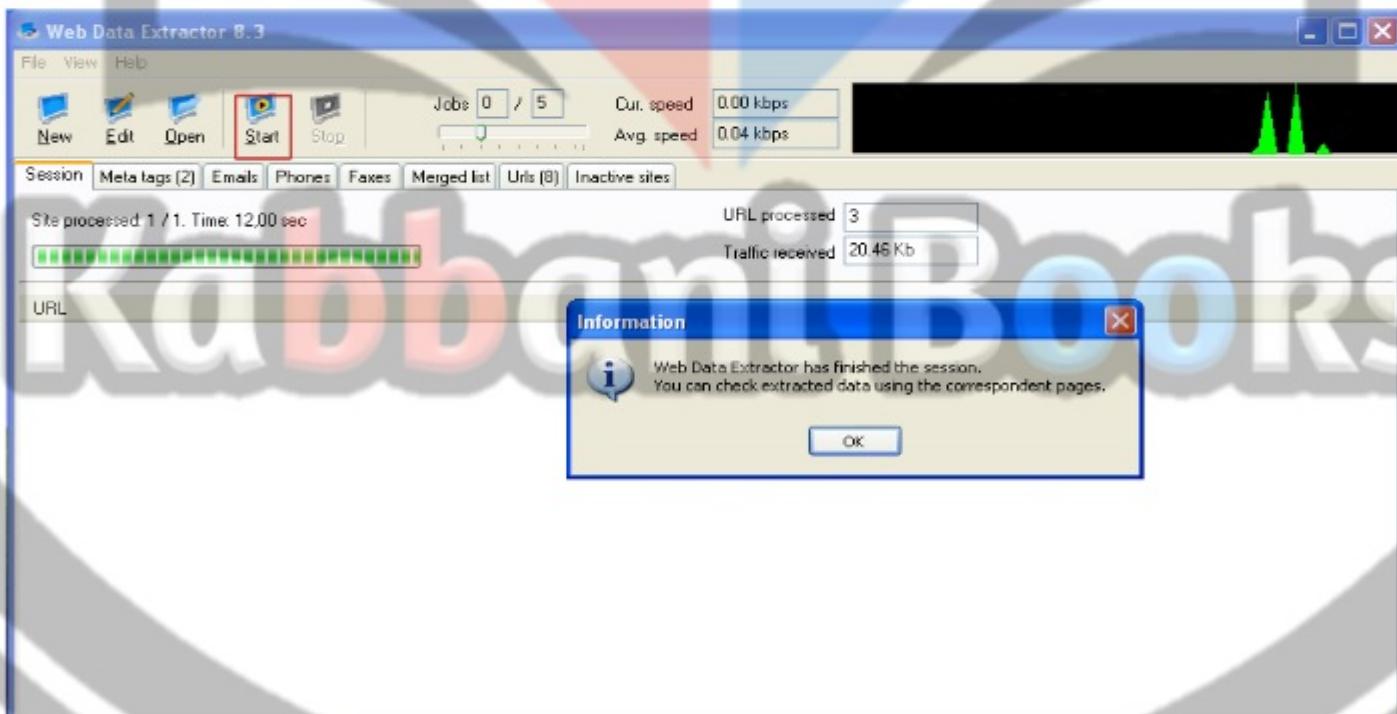
2- بعد الانتهاء من عملية التثبيت تقوم بتشغيل البرنامج من خلال الأيقونة المعروفة عنه فتظهر الشاشة التالية:



3- نضغط على الزر **New** لبدا session جديد فتظهر القائمة التالية والتي تقوم فيها بإدخال عنوان **URL** عن المنظمة الهدف ولتكن مثلاً هنا **CHECK BOXES** تم عمل <http://www.certifiedhacker.com> على جميع الخيارات المتاحة كالتالي:



4- تم نضغط على **OK** فترجع الى الشاشة الرئيسية ونضغط على **start** لابداً جمع المعلومات وعند الانتهاء يخبرك برسالة انه قد أنهى عملية جمع المعلومات كالتالي:



5- يمكن عرض نوعية المعلومات بالتنقل بين الأزرار الآتية:



6- يمكن ايضاً حفظ المعلومات التي قمت بجمعها عن طريق الضغط على **Save Session** في **File** تم ونحد المكان الذي نحفظ فيه.



## ADDITIONAL FOOTPRINTING TOOLS

بالإضافة إلى الأدوات المستخدمة في عملية الاستطلاع التي تم ذكرها لاحقاً هناك عدة أدوات أخرى كالتالي:

Prefix WhoIs available at <http://pwhois.org>

NetScanTools Pro available at <http://www.netscantools.com>

Tctrace available at <http://www.phenoelit-us.org>

Autonomous System Scanner (ASS) available at <http://www.phenoelit-us.org>

DNS DIGGER available at <http://www.dnsdigger.com>

Netmask available at <http://www.phenoelit-us.org>

Binging available at <http://www.blueinfy.com>

Spiderzilla available at <http://spiderzilla.mozdev.org>

Sam Spade available at <http://www.majorgeeks.com>

Robtex available at <http://www.robtex.com>

Dig Web Interface available at <http://www.digwebinterface.com>

Domain Research Tool available at <http://www.domainresearchtool.com>

Activewhois available at <http://www.johnru.com>

yoName available at <http://yoname.com>

Ping-Probe available at <http://www.ping-probe.com>

SpiderFoot available at <http://www.binarypool.com>

CallerIP available at <http://www.callerippro.com>

Zaba Search available at <http://www.zabasearch.com>

GeoTrace available at <http://www.nabber.org>

DomainHostingView available at <http://www.nirsoft.net>

## FOOTPRINTING COUNTERMEASURES 2.5

حتى الآن ناقشنا أهمية **Footprinting**، ومختلف الطرق التي يمكن أن يؤديها **Footprinting**، والأدوات التي يمكن استخدامها للـ

**Footprinting**. الأن سوف نناقش المضادات ليتم تطبيقها من أجل تجنب الكشف عن المعلومات الحساسة.

**Footprinting Countermeasures** هي تدابير أو إجراءات متعددة لمواجهة أو تعويض الإفصاح عن المعلومات. وفيما يلي بعض التدابير المضادة لعملية الـ **Footprinting** على النحو التالي:

1- إعداد أجهزة التوجيه [router] للحد من الرد على طلبات الـ **Footprinting**.

2- قفل المنافذ مع تكوين جدار الحماية المناسب.

3- تقييم والحد من كمية المعلومات المتاحة قبل نشرها على موقع/شبكة الإنترنـت وتحطيل الخدمات الغير ضرورية.

4- منع محركات البحث من التخزين المؤقت [caching] لا **webpage** واستخدام خدمات تسجيل المجهول.

5- إعداد خوادم الويب لتجنب تسرب المعلومات وتحطيل البروتوكولات غير المرغوب فيها.

6- استخدام **IDS** التي يمكن إعداده لرفض الحركات المقبوـلة والتقط أثـامـات **Footprinting**.

7- أداء تقيـيـة الـ **Footprinting** وإزالة أي معلومات حساسة يتم العثور عليها.

8- فرض السياسات الأمنية لتنظيم المعلومات التي من الممكن أن تكشف لأطراف ثالـة بـواسـطة الموظـفين.

9- فصل مجموعة **DNS** الداخلية عن مجموعة **DNS** الخارجية.

10- تحطيل قوائم الدليل واستخدام **split-DNS**.

11- تنبيـيـة الموظـفين حول مختلفـ الحـيلـ المستـخدمـةـ منـ قـبـلـ الـهـندـسـةـ الـاجـتمـاعـيـةـ وـالمـخـاطـرـ.

12- تقيـيـدـ المـدخـلاتـ غـيرـ مـتـوقـعةـ مـثـلـ |<>|.

13- تجنب **domain-level cross-linking** للأصول الحرجة.

14- تشفـيـرـ كلمـاتـ المرـورـ وـحـماـيـةـ المـعـلـومـاتـ الحـاسـاسـةـ.

15- عدم تـمـكـنـ البرـوتـوكـولاتـ التـيـ لـيـسـ مـطلـوبـةـ.

16- استـخدـمـ دائمـاـ **IPsec / TCP / IP**.

17- إعداد **IIS** ضد **banner gabbing**.

## FOOTPRINTING PENETRATION TESTING 2.6

حتى الآن نلخص كل التقنيات والأدوات الازمة لاختبار أمن النظام أو الشبكة الازمة. الآن حان الوقت لوضع كل تلك التقنيات في وضع العمل. اختبار أمن النظام أو الشبكة باستخدام تقنيات مماثلة لتلك التي يستخدمها المهاجمين مع أنواع كافية يعرف باسم اختبار الاختراق. وينبغي إجراء اختبار الاختراق للتحقق ما إذا كان المهاجم قادرًا على الكشف عن معلومات حساسة رداً على محاولات **Footprinting**. اختبار الاختراق [Penetration testing] هو وسيلة تقييم للنظام أو أمن الشبكة. في هذا الأسلوب من التقييم، يعمل مؤدي هذا النوع من الاختبار [pen tester] باعتباره شخص خارجي يريد اختراق النظام حيث يحاكي هجوماً للفرصنة من أجل الحصول على التغرات الأمنية.

### FOOTPRINTING PEN TESTING

**Footprinting Pen Testing** يستخدم لتحديد طبيعة معلومات المؤسسة المتاحة للجمهور على شبكة الإنترنت مثل هندسة الشبكات وأنظمة التشغيل والتطبيقات والمستخدمين. في هذه الطريقة، يحاول **Pen Tester** جمع المعلومات الحساسة المتاحة للجمهور عن الهدف من خلال التظاهر بأنه مهاجم. قد يكون الهدف مجموعة محددة أو شبكة **Pen tester** يمكنه تنفيذ أي هجوم مثل ما يمكنه أن يؤديه المهاجم. يجب عليه أن يحاول استخدام كل الطرق الممكنة لجمع أكبر قدر ممكن من المعلومات لضمان الحد الأقصى من نطاق الاختبار **Footprinting Pen Testing**. إذا وجد لا **Pen tester** أية من المعلومات الحساسة موجودة على أي مورد من المعلومات المتاحة للجمهور، فإنه يجب إدخال هذه المعلومات وكتابه تقرير عن ذلك.

أهم مزايا إجراء اختبار الاختراق **Pen testing** ما يلي:

- يوفر لك فرصة لمنع استرجاع سجل **DNS** من الخوادم المتاحة للعموم.
- يساعدك على تحذف تسرب المعلومات.
- يمنع محاولات الهندسة الاجتماعية.

اختبار الاختراق [Penetration test] هو وسيلة إجرائية لاختبار الأمان والمتمثل في الخطوات التالية المختلفة. ينبغي اتباع الخطوات التالية واحدة تلو الأخرى من أجل ضمان أقصى قدر من نطاق الاختبار. هنا هي الخطوات المتبعة في **Footprinting Pen testing**:

#### 1- الخطوة الأولى: Get proper authorization (الحصول على الترخيص اللازم)

يجب أن يتم تنفيذ **Pen test** مع إذن. لذا، فإن الخطوة الأولى من **Footprinting pen testing** هو الحصول على الترخيص اللازم من الأشخاص المسؤولين، مثل مسؤولي النظام [**admin**].

#### 2- الخطوة الثانية: Define the scope of the assessment (تحديد نطاق التقييم)

تحديد نطاق التقييم الأمني هو شرط مسبق لاختبار الاختراق. تحديد نطاق التقييم يحدد مجموعة من الأنظمة في الشبكة وذلك لفحصها والموارد التي يمكن استخدامها في الاختبار، وما إلى ذلك. يحدد أيضًا حدود لا **Pen tester**. بمجرد تحديد النطاق، يجب أن تخلط لجمع المعلومات الحساسة باستخدام تقنيات **Footprinting** المختلفة.

#### 3- الخطوة الثالثة: Perform Footprinting through search engines (إجراء Footprinting عن طريق محركات البحث)

Footprinting عن محركات البحث مثل **جوجل**، **ياهو**، **Bing**، **Ask**، **Dogpile**، وما إلى ذلك. لجمع المعلومات حول المنظمة المستهدفة مثل تفاصيل الموظفين، صفحات تسجيل الدخول، وبوابات الإنترنت (**gateway**)، الخ. والتي يمكنها أن تساعدك في أداء الهندسة الاجتماعية وغيرها من أنواع متقدمة من الهجمات.

#### 4- الخطوة الرابعة: Perform website Footprinting (أداء عملية الاستطلاع عن الموقع الإلكتروني)

أداء عملية الاستطلاع عن الموقع الإلكتروني باستخدام أدوات مثل **BlackWidow**، **HTTrack Web Site Copier**، **Webriffer**، وما إلى ذلك لبناء خريطة تفصيلية لبنية الموقع والهندسة المعمارية.

#### 5- الخطوة الخامسة: Perform email Footprinting (عملية الاستطلاع باستخدام البريد الإلكتروني)

أداء عملية الاستطلاع باستخدام البريد الإلكتروني عن طريق استخدام أدوات مثل **PoliteMail**، **eMailTrackerPro**، **Email Lookup - Free Email Tracker**، وما إلى ذلك. لجمع معلومات حول الموقع الفعلي للفرد لأداء الهندسة الاجتماعية والتي يدورها قد تساعد في رسم خرائط الشبكة للمنظمة الهدف.

#### 6- الخطوة السادسة: Gather competitive intelligence (جمع معلومات عن المنافسين)



جمع المعلومات الاستخباراتية عن الشركات/المنظمات التنافسية باستخدام أدوات مثل **Business Wire**, **SEC Info**, **Hoovers**, وما إلى ذلك. هذه الأدوات تساعدك على استخراج المعلومات حول المنافس مثل إنشائها وموقع الشركة، وتحليل تقدمها في السوق، السلطات العليا، وتحليل المنتج وتفاصيل التسويق، وأكثر من ذلك.

#### 7- الخطوة السابعة: Perform Google hacking (تنفيذ قرصنة جوجل)

أداء قرصنة جوجل باستخدام أدوات مثل **SiteDigger**, **MetaGoofil**, **GHDB**, وما إلى ذلك. يحدد التغرات الأمنية في الرمز الكودي وأعداد الموقع. عادة ما يتم قرصنة جوجل بمساعدة مُتّخلي جوجل المتقدمة التي تحدد سلسلة محددة من النص مثل إصدارات تطبيقات الويب التي بها نقاط الضعف.

#### 8- الخطوة الثامنة: Perform WHOIS Footprinting (عملية الاستطلاع باستخدام قواعد whois)

أداء تقنية **WHOIS Footprinting** لاستخراج معلومات حول домين معين. يمكنك الحصول على معلومات مثل اسم الدومين وعنوان IP، اسم مالك الدومين، الاسم المسجل، وتفاصيل الاتصال بهم بما في ذلك أرقام الهاتف، البريد الإلكتروني، وما إلى ذلك. أدوات مثل **Activewhois**, **Whois Pro**, **Countrywhois**, **Smartwhois** تساعدك على استخراج هذه المعلومات. يمكنك استخدام هذه المعلومات لأداء الهندسة الاجتماعية للحصول على مزيد من المعلومات.

#### 9- الخطوة التاسعة: Perform DNS Footprinting (أداء عملية الاستطلاع عن قواعد DNS)

أداء **DNS record** باستخدام أدوات مثل **DNS Footprinting**, **NSLOOKUP**, **DIG**, وما إلى ذلك. لتحديد المضيفين الرئيسيين في الشبكة وأداء هجمات الهندسة الاجتماعية. حل اسم الدومين لمعرفة عنوان IP الخاص به، وسجلات DNS، وما إلى ذلك.

#### 10- الخطوة العاشرة: Perform network Footprinting (أداء عملية الاستطلاع عن الشبكة)

أداء **Network Pinger**, **VisualRoute 2010**, **Path Analyzer Pro** باستخدام أدوات مثل **Network Footprinting**. يسمح لك للكشف عن نطاق الشبكة ومعلومات عن الشبكات الأخرى من الشبكة المستهدفة. باستخدام كل هذه المعلومات، يمكنك رسم "الرسم تخطيطي" للشبكة عن الشبكة الهدف.

#### 11- الخطوة الحادية عشر: Perform social engineering (تنفيذ الهندسة الاجتماعية)

تنفيذ تقنيات الهندسة الاجتماعية مثل **dumpster diving**, **shoulder surfing**, **eavesdropping** التي قد تساعد على جمع المعلومات الأكثر أهمية عن المنظمة الهدف. من خلال استخدام الهندسة الاجتماعية فإنه يمكنك جمع تفاصيل عن الموظفين في المنظمة الهدف، وأرقام الهواتف، والعناوين، وعنوان البريد الإلكتروني، وما إلى ذلك. يمكنك استخدام هذه المعلومات لكتف المزيد من المعلومات.

#### 12- الخطوة الثانية عشر: Perform Footprinting through social networking sites (من خلال الشبكات الاجتماعية)

أداء **Footprinting** من خلال موقع التواصل الاجتماعي على موظفي المنظمة الهدف التي تم الحصول على أسمائهم من خلال عملية الهندسة الاجتماعية. يمكنك جمع معلوماتهم من ملفاتهم الشخصية على موقع الشبكات الاجتماعية مثل **الفاسبوك**, **LinkedIn**, **تويتر**, **جوجل+**, **Pinterest** وما إلى ذلك، والتي تساعد في أداء الهندسة الاجتماعية. يمكنك أيضاً استخدام الناس كمحركات بحث للحصول على معلومات حول الشخص الهدف.

#### 13- الخطوة الثالثة عشر: Document all the findings (توثيق جميع النتائج)

بعد تنفيذ كل تقنيات الـ **Footprinting**، وجمع وتوثيق جميع المعلومات التي تم الحصول عليها في كل مرحلة من مراحل الاختبار. يمكنك استخدام هذه الوثيقة لدراسة وفهم وتحليل الواقع الأمني للمنظمة المستهدفة. هذا يتيح لك أيضًا العثور على التغرات الأمنية. عندما تجد التغرات الأمنية، يجب أن تشير إلى التدابير المضادة لهذه التغرات.

### FOOTPRINTING PEN TESTING REPORT TEMPLATES ( قالب/شكل تقارير عملية اختبار الاختراق )

عادة ما يتم إجراء اختبار الاختراق لتعزيز الأمان في محیط المؤسسة. بمتابعة إنك **Pen Tester** فإنه يجب عليك جمع المعلومات الحساسة مثل تفاصيل الخادم، نظام التشغيل، وما إلى ذلك حول الهدف من خلال إجراء **Footprinting**. عملية تحليل النظام وشبكة الدفاعات عن طريق كسر أمنها مع أدوات كافية (أي أخلاقياً) دون التسبب في أي ضرر. العثور على التغرات ونقطة الضعف في الشبكة أو أمن النظام. الآن تدرج جميع نقاط الضعف جنباً إلى جنب مع التدابير المضادة المعنية في التقرير، مثل تقرير **Pentester**. تقرير **Pentester** هو تقرير حصلت بعد إجراء اختبارات اختراق الشبكة أو تدقيق أمنى. فهو يحتوي على كل التفاصيل مثل نوع الاختبارات التي قمت بها، وأساليب القرصنة المستخدمة، ونتائج عملية القرصنة. بالإضافة إلى ذلك، يتضمن التقرير أيضاً المخاطر الأمنية ونقطة الضعف للمؤسسة. إذا تم تحديد أي الضعف خلال أي اختبار، فإنه يجب ذكر تفاصيل سبب الضعف جنباً إلى جنب مع التدابير المضادة. وبينما دائمًا أن يبقى التقرير سري. إذا وقعت هذه المعلومات في أيدي المهاجمين فإنها قد تستخدم لشن هجمات.

ينبغي أن يتضمن تقرير الاختبار التفاصيل التالية:

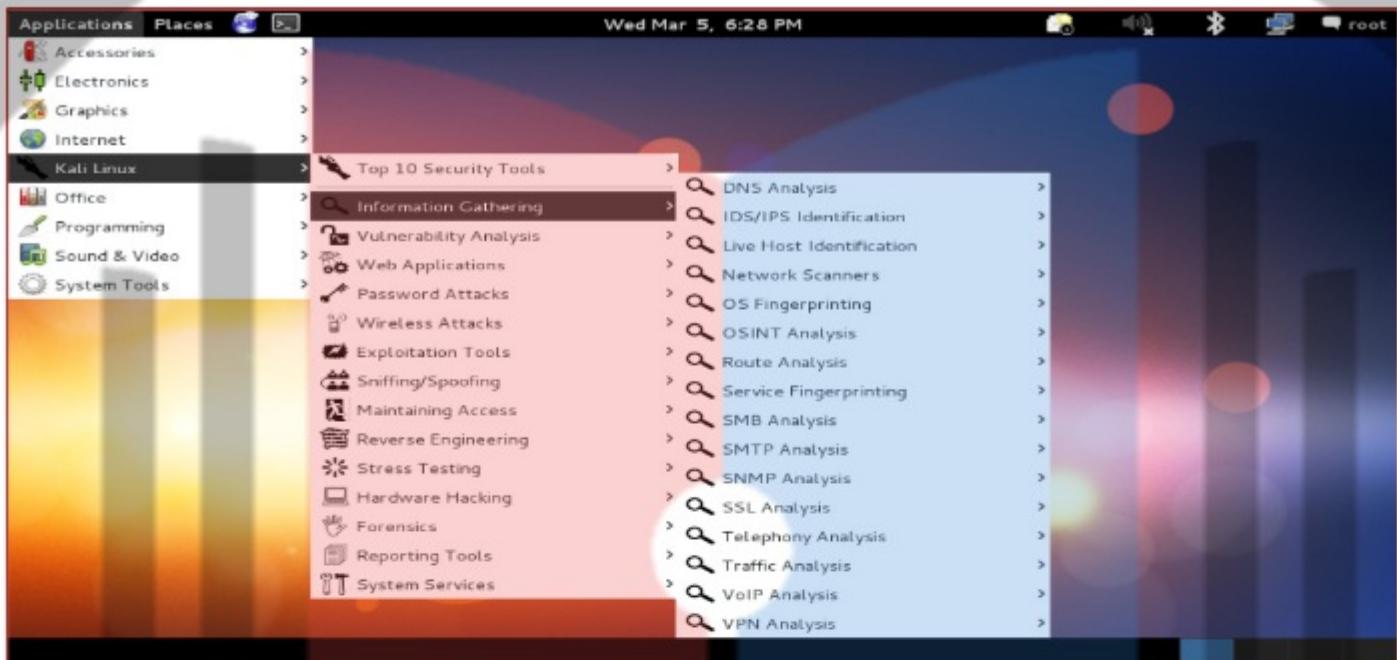
<b>Pen Testing Report</b>	
<b>Information obtained through search engines</b>	<b>Information obtained through people search</b>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Employee details:</li> <li><input checked="" type="checkbox"/> Login pages:</li> <li><input checked="" type="checkbox"/> Intranet portals:</li> <li><input checked="" type="checkbox"/> Technology platforms:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Date of birth:</li> <li><input checked="" type="checkbox"/> Contact details:</li> <li><input checked="" type="checkbox"/> Email ID:</li> <li><input checked="" type="checkbox"/> Photos:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>
<b>Information obtained through website footprinting.</b>	<b>Information obtained through Google</b>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Operating environment:</li> <li><input checked="" type="checkbox"/> Filesystem structure:</li> <li><input checked="" type="checkbox"/> Scripting platforms used:</li> <li><input checked="" type="checkbox"/> Contact details:</li> <li><input checked="" type="checkbox"/> CMS details:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Advisories and server vulnerabilities:</li> <li><input checked="" type="checkbox"/> Error messages that contain sensitive information:</li> <li><input checked="" type="checkbox"/> Files containing passwords:</li> <li><input checked="" type="checkbox"/> Pages containing network or vulnerability data:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>
<b>Information obtained through email footprinting.</b>	<b>Information obtained through competitive intelligence</b>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> IP address:</li> <li><input checked="" type="checkbox"/> GPS location:</li> <li><input checked="" type="checkbox"/> Authentication system used by mail server:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Financial details:</li> <li><input checked="" type="checkbox"/> Project plans:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>

<b>Pen Testing Report</b>	
<b>Information obtained through WHOIS footprinting</b>	<b>Information obtained through social engineering</b>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Domain name details:</li> <li><input checked="" type="checkbox"/> Contact details of domain owner:</li> <li><input checked="" type="checkbox"/> Domain name servers:</li> <li><input checked="" type="checkbox"/> Netrange:</li> <li><input checked="" type="checkbox"/> When a domain has been created:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Personal information:</li> <li><input checked="" type="checkbox"/> Financial information:</li> <li><input checked="" type="checkbox"/> Operating environment:</li> <li><input checked="" type="checkbox"/> User names and passwords:</li> <li><input checked="" type="checkbox"/> Network layout information:</li> <li><input checked="" type="checkbox"/> IP addresses and names of servers:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>
<b>Information obtained through DNS footprinting</b>	<b>Information obtained through social networking sites</b>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Location of DNS servers:</li> <li><input checked="" type="checkbox"/> Type of servers:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Personal profiles:</li> <li><input checked="" type="checkbox"/> Work related information:</li> <li><input checked="" type="checkbox"/> News and potential partners of the target company:</li> <li><input checked="" type="checkbox"/> Educational and employment backgrounds:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>
<b>Information obtained through network footprinting</b>	
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Range of IP addresses:</li> <li><input checked="" type="checkbox"/> Subnet mask used by the target organization:</li> <li><input checked="" type="checkbox"/> OS's in use:</li> <li><input checked="" type="checkbox"/> Firewall locations:</li> <li><input checked="" type="checkbox"/> Others:</li> </ul>	

## OTHER TECHNIQUE OF INFORMATION GATHERING WITH KALI LINUX 2.7

ملحوظة: في هذا الجزء سوف نتكلم عن بعض الأدوات الأخرى المستخدمة في جمع المعلومات عن طريق استخدام نظام التشغيل جنو/لينكس "التوزيعة كالي لينكس وباك تراك 5".

تحتوي توزيعة كالي لينكس وباك تراك 5 على قائمه غنيه بالأدوات تحت عنوان **Information Gathering** مخصصه لعملية **Footprinting**. يمكن أن تمايز كتابا منفصلا لتعطية كافة الأدوات والأساليب المتاحة لجمع المعلومات. سيركز هذا الجزء على باقي مواضيع الاستطلاع الموجودة على الإنترنت، وتلك التي توفرها كالي لينكس.



## COMPANY WEBSITE

هناك الكثير من المعلومات القيمة التي يمكن الحصول عليها عن موقع الويب المستهدف. أكثر مواقع الشركات تضع قائمه بفرقهم التقني والشخصيات العامة، وأعضاء من التوظيف والموارد البشرية. يمكن أن تصبح هذه الأهداف عرضه لجهود البحث الأخرى وهجمات الهندسة الاجتماعية.

يمكن الحصول على معلومات أكثر قيمة من خلال النظر في الشركات الأخرى المدرجة كشركاء، الوظائف الخالية الحالية، المعلومات التجارية، والسياسات الأمنية. عملية الاستطلاع عن التريلك ذو المركز الاعلى يمكن أن يكون هاما مثل الهدف الرئيسي، وذلك لأن الشركاء قد يوفروا مصدرا جديدا للحصول على معلومات استخبارية.

الملف **robots.txt** متاح للعامة ويوجد في الموقع الذي تعطي تعليمات **robots** على شبكة الإنترنت بمنع محركات البحث من الوصول إلى الملفات المهمة (محركات البحث تعرف أيضا باسم محركات العنكبوت للبحث "search engine spiders"), وهذا يطلق عليه

**The Robots Exclusion Protocol**



التعبير "Disallow /" يخبر المتصفح بعدم إمكانية زيارة المجلدات الرئيسية، ومع ذلك، يمكن تجاهلها بإعطاء الباحثين الأذكاء هدف لجعله يكون متاحاً لل العامة. لعرض الملف **Robots.txt**، يجب العثور عليه في المسار الجذري للموقع الهدف. على سبيل المثال، نضيف التعبير "robots.txt" للموقع مثل الآتي:

"<http://www.facebook.com/robots.txt>"

```
# Notice: Crawling Facebook is prohibited unless you have express written permission. See: http://www.facebook.com/apps/site_scraping_toe_terms.php

User-agent: *
Disallow: /ajish/
Disallow: /ajish.php
Disallow: /auto_login.php
Disallow: /checkboxpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photo_size.php
Disallow: /shareer/

User-agent: Googlebot
Disallow: /ajish/
Disallow: /ajish.php
Disallow: /auto_login.php
Disallow: /checkboxpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photo_size.php
Disallow: /shareer/

User-agent: search
Disallow: /ajish/
Disallow: /ajish.php
Disallow: /auto_login.php
Disallow: /checkboxpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php

User-agent: linkedin
Disallow: /ajish/
Disallow: /ajish.php
Disallow: /auto_login.php
Disallow: /checkboxpoint/
Disallow: /contact_importer/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /l.php
Disallow: /p.php
Disallow: /photo.php
```

## THE HARVESTER: DISCOVERING AND LEVERAGING E-MAIL ADDRESSES

**Harvester** أداة ممتازة لاستخدامها في عمليات الاستطلاع. **Harvester** بسيط في عمله ولكن سكريبت قوي وفعال من النوع يأيّتون كتبه كريستن مورتوريلا [Christian Martorella]. هذه الأداة تسمح لنا بسرعة وبذلة سرد كلا عنوان البريد الإلكتروني وال نطاقات/الدوامين الفرعية التي ترتبط مباشرةً بهدفنا من المهم دائماً استخدام أحدث نسخة من **Harvester** وذلك لأن العديد من محركات البحث تعمل على تحديث وتغيير أنظمتها بانتظام. حتى التغييرات الطفيفة لسلوك محرك البحث يمكن أن يجعل الأدوات الآلية غير فعالة. في بعض الحالات، تقوم محركات البحث بتحديد النتائج قبل عوته المعلومات لك. أيضاً العديد من محركات البحث تستخدم تقنيات [throttling techniques] من شأنها أن تحاول أن تمنعك من تشغيل عمليات البحث الآلية.

**Harvester** يمكن استخدامها للبحث في جوجل (google) ، بنسج(Bing) ، وخوادم PGP لرسائل البريد الإلكتروني ، والمضيفين (hosts) ، والنطاقات الفرعية(subdomain). يمكن أيضاً البحث في LinkedIn عن أسماء المستخدمين. معظم الناس تعتبر تحميل عنوان البريد الإلكتروني الخاص بهم غير حميدة. لقد ناقشنا بالفعل مخاطر الإرسال إلى المنتديات العامة باستخدام عنوان البريد الإلكتروني الخاص بك المتوفّر من قبل القرفة الخاصة بك، ولكن هناك مخاطر إضافية يجب أن تكون على علم بها. دعونا نفترض مثلاً من خلال عملية الاستطلاع الخاص بك للكشف عن عنوان البريد الإلكتروني للموظفين الذين يعملون في المنظمة التي تستهدفها. قبل البحث ومعالجة المعلومات قبل الرمز "@"، يجب أن تكون قادرین على إنشاء سلسلة من أسماء المستخدمين المحتملين للتسلیکة. ليس بالملوک لدى المنظمات استخدام أسماء المستخدم وعنوان البريد الإلكتروني نفسهم (قبل الرمز "@"). مع حفنة من أسماء المستخدمين المحتملين، يمكننا محاولة جعل brute force يجد طريقه إلى أية خدمات، مثل **Virtual Private Networks**، **Secure Shell**، أو **VPN**. يجد طريقه إلى أي خدمة، مثل **FTP**، والتي سوف نكتشفها أثناء الخطوة 2 (Scanning).

**theharvester** هو أداة مبنية داخل كالي. أسرع طريقة للوصول إلى **Harvester** هو فتح نافذة الترمinal وكتابة الأوامر إذا كنت في حاجة إلى المسار الكامل للبرنامج وكانت تستخدم كالي، **Harvester** (وتقريراً كل الأدوات الأخرى) يمكن العثور عليها في المجلد /usr/bin/. مع ذلك، نذكر أن الميزة الرئيسية لكالي أنه لم يعد تحتاج لتشغيل أي أداة الوصول إلى المجلد الرئيسي الذي يحتوي على الأدوات مثل الباك تراك حيث إنك ببساطة تقوم بفتح الترمinal وكتابة الأمر. ملحوظة: إذا كنت تعمل على نظام تشغيل لينكس ولكن توزيع أخرى غير كالي أو باك تراك فيمكنك تحميل هذه الأداة من الموقع التالي: <http://www.edge-security.com>

مثل لتشخيصها في باك تراك بعد الذهب إلى المسر الخاص بها كالتالي:

<http://www.syngress.com> © 2010 Syngress Media, Inc.

مُثُلُ لِتَشْخِيْلِهَا فِي كَالِي

Theharvester©-d©syngress.com©-l©10©-b©google

```
root@jana:~# theharvester -d syngress.com -l 10 -b google
```

A decorative banner at the top of the slide features a repeating pattern of stylized, blocky letters resembling 'E' or 'H' in white on a dark background.

[ - ] Searching in Google:  
Searching 0 results...

[+] Emails found:

solutions@syngress.com  
chris@syngress.com  
sales@syngress.com

[+] Hosts found in search engines:

198.81.200.140:booksite.syngress.com  
79.170.91.51:www.syngress.com

هذا الامر سوف يقوم بالبحث عن البريد الإلكتروني وال نطاقات الفرعية [subdomain] والمضيفين [Hosts].

قبل مناقشة نتائج هذه الأداة، دعونا نبحث الأمر أقرب قليلاً. يستخدم "theharvester.py" لاستدعاء الأدلة. يستخدم التعبير [-d] لتحديد الدومن الهدف. يستخدم [-l] للحد من عدد النتائج التي يتم إرجاعها لنا. في هذه الحالة، فإن هذه الأداة ترجع لنا 10 نتائج فقط. يتم استخدام [-b] لتحديد مستودع البحث الذي نريد أن نستخدمه. يمكننا الاختيار من بين مجموعة واسعة بما في ذلك [google](#), [LinkedIn](#), [PGP](#), [Bing](#)، وأكثر من ذلك في هذا المثال، اخترنا البحث باستخدام جوجل. إذا لم تكون متذكراً من مصدر البيانات لاستخدامها في البحث الخاص بك، يمكنك أيضاً استخدام [-b all] ليشمل جميع مستودعات البحث في وقت واحد للبحث والتي يمكن استخدامها.

الآن انت تفهم تماماً كفاية استخدام الأمر لتشغيل الأداة، دعونا نلقى نظرة على النتائج. كما ترون، فإن **harvester** فعال في تحديد العديد من عذويين البريد الإلكتروني التي يمكن أن تكون ذات قيمة بالنسبة لنا. هو أيضاً ناجح في العثور على اثنين من النطاقات الفرعية.

METAGOOFIL

اداة أخرى ممتازة لجمع المعلومات وهي **MetaGoofil**. **MetaGoofil** هي اداة استخراج البيانات الوصفية (**metadata**) وتم كتابتها من قبل نفس الاشخاص الذين انشئوا **harvester**. غالباً ما تعرف البيانات الوصفية بأنها "بيانات عن البيانات". عند إنشاء مستند مثل **Microsoft Word** أو عرض تقديمي لـ **PowerPoint**, يتم إنشاء بيانات إضافية وتخزينها داخل الملف. غالباً ما تتضمن هذه البيانات قطعة مختلفة من المعلومات التي تصف الوثيقة بما في ذلك اسم الملف، حجم الملف، صاحب الملف أو اسم المستخدم الخاص بالشخص الذي قام بإنشاء الملف، والموقع أو المسار حيث تم حفظ الملف. تحت هذه العملية تلقائياً دون أي تدخل أو تفاعل من قبل المستخدم. قدرة المهاجم على قراءة هذه المعلومات قد يقدم بعض الأفكار الفريدة عن المنظمة المستهدفة بما في ذلك أسماء المستخدمين، أسماء الكمبيوتر أو الخادم، مسارات الشبكة، الملفات المشاركة، وغيرها من الأشياء الجيدة. **MetaGoofil** هي الأداة التي تنظر إلى الانترنت بحثاً عن الوثائق التي تتنمي إلى الهدف الخاص بك. بعد العثور على هذه الوثائق، **MetaGoofil** يقوم بالتحميل لهم ومحاولاً

استخراج البيانات الوصفية المفيدة. **MetaGoofil** بنى في كالي ويمكن استخدامه من خلال فتح نافذة الترمinal و تشغيل الأمر **metagoofil** (جنبًا إلى جنب مع رموز التبديل المناسبة) أو من خلال التنقل إلى مسار تنفيذ **MetaGoofil** الذي يقع في **/usr/bin**.

فكرة جيدة لإنشاء مجلد "ملفات". الغرض من هذا المجلد هو حفظ كافة الملفات المستهدفة التي سيتم تحميلها، وهذا يحافظ على المجلد الأصلي نظيف.

يمكنك تشكيل **MetaGoofil** عن طريق إصدار الأمر التالي:

```
root@jana:~# ./metagoofil.py -d syngress.com -t pdf,doc,xls,pptx -n 20 -o files -f results.html  
root@jana:~# metagoofil -d syngress.com -t pdf,doc,xls,pptx -n 20 -o files -f results.html
```

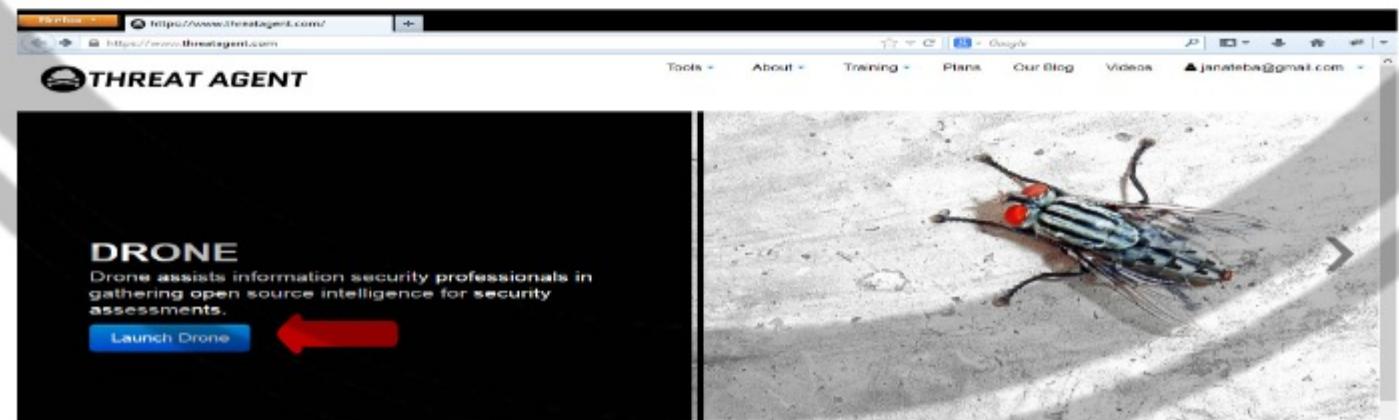
دعونا نبحث في تفاصيل هذا الأمر. يستخدم **MetaGoofil** لاستدعاء البرنامج النصي **metagoofil**. يتم استخدام [d] لتحديد الدومنين الهدف المراد تفتيشه. يتم استخدام [t] للتبدل لتحديد أي نوع أو أنواع الملفات التي تزيد من **MetaGoofil** محاولة إيجاده وتحميله. في وقت كتابة هذا التقرير، كان **MetaGoofil** قادر على استخراج البيانات الوصفية من الصيغ التالية: **pdf**, **xls**, **odp**, **ppt**, **doc**, **xlsx**, **docx**, **odx**, **pptx**. يمكنك إدخال أنواع ملفات متعددة عن طريق فصل كل نوع باستخدام الفاصلة (ولكن بدون مسافات). يتم استخدام [n] لتحديد عدد الملفات من كل نوع التي ترغب في تحميله لفحصها. يمكنك أيضا تحديد أنواع الملفات الفردية للحد من النتائج التي تم إرجاعها. نستخدم التبديل [o] لتحديد المجلد حيث تزيد تخزين كل الملفات التي يقوم **MetaGoofil** بتحميله. أخيرا نستخدم التبديل [f] لتحديد ملف الإخراج. هذا الأمر ينشأ وثيقة تنسيق سهلة للمراجعة والفهرسة. افترضيا سوف **MetaGoofil** أيضا عرض أية نتائج في، التمثال

#### THREAT AGENT: ATTACK OF THE DRONES

الخيار آخر للاستطلاع، والذي يتضمن العديد من أدوات لجمع المعلومات في مكان واحد، ThreatAgent Drones. وقد تم تطوير هذه الأداة من قبل ماركوس كاري، يمكنك التسجيل للحصول على حساب مجاني، من خلال موقع الويب التالي:

<https://www.threatagent.com>

**ThreatAgent** يأخذك في جمع **OSINT (open source intelligence)** إلى المستوى التالي من خلال استخدام عدد من المواقع المختلفة، والأدوات، والتقييمات لإنقاء ملف كامل للك عن الهدف الخاص بك. القيء الوحيد الذي تحتاجه هو اسم المؤسسة واسم النطاق كما هو مبين في التسلسل.



# DRONE

Open Source Intelligence

**Deploy Drone**

Company Domain

تم نصيحته هنا فتظهر ثالثة أخرى نضع بها اسم الدومن

New Drone Mission

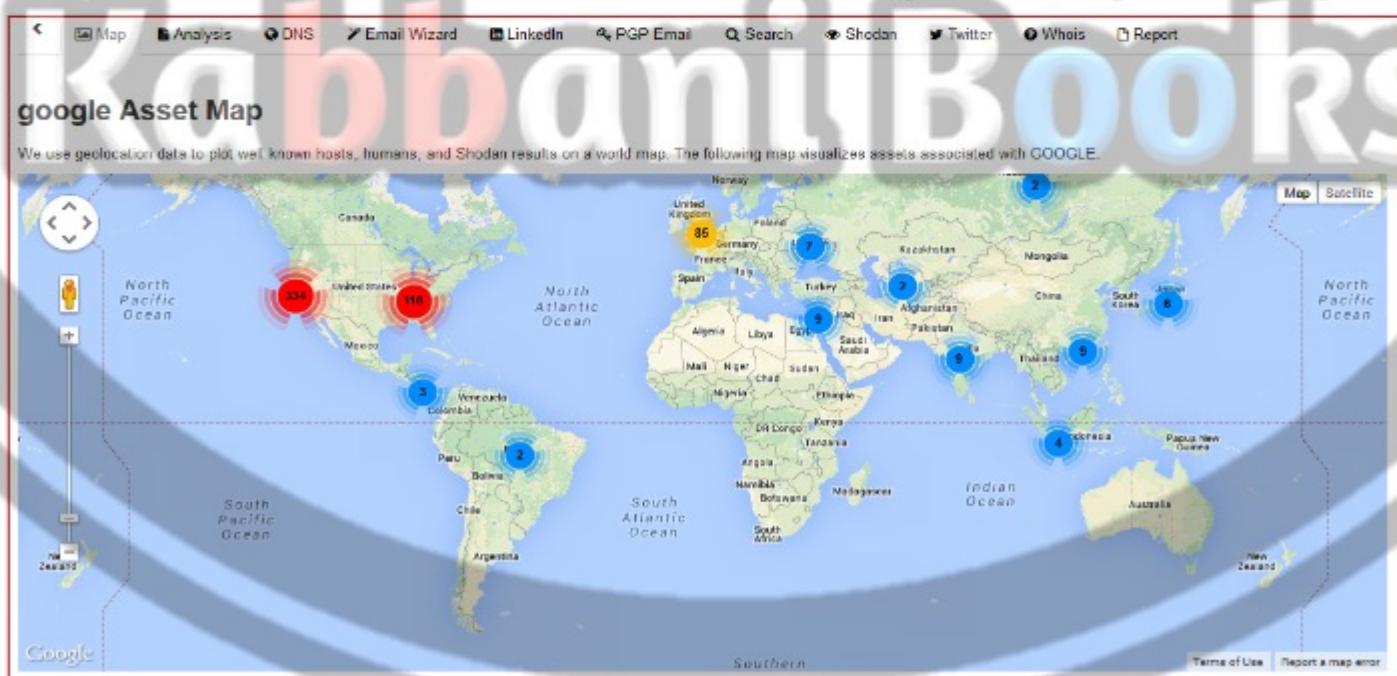
Company Name: dooale

Domain Name: dooale.com

**Deploy Drone**

Company Domain

بمجرد انتهاء Drone من استخراج جميع المعلومات عن مختلف المواقع، فإنه سوف يقدم تقريراً لك بعد ذلك عن نطاقات عذلين IP ، وعنوانين البريد الإلكتروني، وجهات الاتصال داخل المنظمة، والمنفذ (ports) المفتوحة [من خلال Shodan] ، وأكثر من ذلك بكثير. متبرة للاهتمام بما فيه الكفاية. انظر إلى ما توصل إليه موقع الويب هذا من نتائج.



**Map** **Analysis** **DNS** **Email Wizard** **LinkedIn** **PGP Email** **Search** **Shodan** **Twitter** **Whois** **Report**

### google DNS Enumeration

The following hostnames were discovered via DNS Enumeration.

Hostname	IP Address	City	Country
academico.google.com	74.125.228.50	Mountain View	United States
accounts.google.com	173.194.68.84	Mountain View	United States
admin.google.com	74.125.228.34	Mountain View	United States
ads.google.com	74.125.228.41	Mountain View	United States
alerts.google.com	74.125.228.40	Mountain View	United States

[Subscribe for All Results](#) 94 Results

**Map** **Analysis** **DNS** **Email Wizard** **LinkedIn** **PGP Email** **Search** **Shodan** **Twitter** **Whois** **Report**

### google Email Wizard

Email Wizard allows you to perform possible email address permutations based on LinkedIn information.

First Name	Last Name	Email
Nichole	Wade	nichole.wade@google.com
Life	At	life.at@google.com
Eric	Schulman	eric.schulman@google.com
Matthew	Worby	matthew.worby@google.com
Larry	Page	larry.page@google.com

[Subscribe for All Results](#) 529 Results

**Map** **Analysis** **DNS** **Email Wizard** **LinkedIn** **PGP Email** **Search** **Shodan** **Twitter** **Whois** **Report**

### google LinkedIn Accounts

First Name	Last Name	Title	Locality
Ido	Bela	Ido Bela, Senior Software Engineer at Google	Greater New York City Area
Alli	Stewart	Alli Stewart, Technical Recruiter at Google	Austin, Texas
Michael	Galpin	Michael Galpin, Software Engineer at Google	San Francisco Bay Area
Jonathan	Jarvis	Jonathan Jarvis, Designer at Google	Greater New York City Area
Sarah	Magee	Sarah Magee, Admin Assistant at Google	Ireland

[Subscribe for All Results](#) 529 Results

DARKNET · INVISIBLE WEB · HIDDEN WEB · DEEP WEB 2.8

- مقدمة -

لقد تم إدخال مصطلح "deep web" على مدى السنوات القليلة الماضية للدلالة على محتوى الإنترنت الذي لا يصل إليه محركات البحث. أو بمعنى آخر هي جميع المحتويات الموجودة على شبكة الانترنت التي لا يمكن الوصول إليها مباشرة من خلال الارتباطات التشعبية [hyperlinks]. على وجه الخصوص: نماذج HTML، خدمات ويب. وهذه تمثل 500 مره أكثر من المحتوى على الشبكة العامة بالنسبة لـ 2004 وهي تحتوي على مئات الآلاف من قواعد بيانات deep web على حسب احصائيات 2004. لا شك اننا جميعا نستخدم الانترنت. لكن هل تعلم ان ما تتصفحه من على الانترنت العادي ليس كل محتوى الانترنت فهناك العديد من المواقع توجد ولا أحد يعلم عنها شيء. هذه الموقع وكل ما هو على شاكلتها من المواقع تقدم خدمات معينة يعلمها معظم مستخدمي الانترنت حول العالم. لكن ما لا تعلمها ان هناك العديد والعديد من المواقع التي لا يعلم عنها معظم مستخدمي الانترنت وهذه المواقع التي لا يعلم عنها معظم مستخدمي الانترنت تمثل اغلب محتوى الانترنت.



## محتوى DEEP WEB كالاتي:

- صفحات الويب الديناميكية [Dynamic web pages] : الصفحات المولدة ديناميكيًا من قبل **HTTP** (الإنترنت العادي) الموقع المحجوبة [Blocked sites] : الموقع الذي تحظر محركات البحث العنكبوتية مثل جوجل للذهاب واسترجاع محتوياتها عن طريق استخدام **CAPTCHAs** ، **HTTP headers** ، أو إدخالات ملف **robots.txt** على سبيل المثال.
- الموقع غير مرتبطة [Unlinked sites] : الصفحات التي لا ترتبط بأي صفحة أخرى، وتمنع محركات البحث العنكبوتية [Web crawler] من احتمالية الوصول إليها.
- الموقع الخاصة [private site] : الصفحات التي تتطلب التسجيل والتوثيق **log-in/password** للدخول إليها.
- الموقع الغير [Non-HTML/Contextual/Scripted] : المحتوى متفرقة في شكل مختلف، ويتم الوصول إليها عن طريق الجافا سكريبت أو فلاش، أو هي سياق معتمد (نطاق IP محدد).
- شبكات محدودة الوصول [Limited-access networks] : المحتوى على هذه الموقع لا يمكن الوصول إليها من قبل جمهور الانترنت العامة.

هاذين النقطتين تشكلان فنتين مستقلتين للDNS:

**Sites with domain names registered**: موقع ذات أسماء نطاقات مسجلة في خادم الأسماء (**DNS**) الجذري (أي **TLD**). هذه هي الموقع التي تم تسجيلها باستخدام تقنية التسجيل المستقلة من قبل هيئة الإنترنت للأسماء والأرقام (**ICANN**) لتبيين أسماء المضيفين.

**ICANN = Internet Corporation for Assigned Names and Numbers**

أسماء النطاقات الافتراضية تتبع تسلسل هرمي في تسميتها والتي يتم تسميتها من قبل **ICANN**، وهي المسؤولة عن تحديد نطاقات **TLD** القواسبية (على سبيل المثال **.gov**, **.edu**, **.com**, وهكذا). وبالتالي، يتم مزامنة DNSs القواسبية وفقاً لاسم التسلسل الهرمي الذي تم تعييفه من قبل **ICANN** ويمكنه أيضاً حل جميع أسماء النطاقات المسجلة من قبل **ICANN**. مع ذلك يمكن للمرء، الاتصال إلى ملقمات **DNS** الخاصة التي تدير مساحات إضافية غير معترف بها من قبل **ICANN**، مما يسمح بتسجيل أسماء نطاقات ولكنها لا تتبع قواعد **TLD** الغير قياسي. في حين حل أسماء النطاقات هذه يتطلب استخدام خوادم **DNS** محددة، ويمكن استخدامها في تقديم بعض المزايا في شكل، وسيلة سهلة لا يمكن تعقبها، وأحياناً لتسجيل أسماء النطاقات الجديدة.

**Darknet and alternative routing infrastructures**: هي موقع تم استضافتها على البنية التحتية التي تتطلب برامج محددة للوصول إلى محتوياتها. من أمثلة هذه النظم هي خدمات تور [TOR's] الغير مرئية أو الموقع المستضيفة على متربو الإنترنت (I2P). يتم تحديد هذه الموقع بشكل عام وكذلك عن طريق اسم نطاق غير قياسي يتطلب استخدام نفس البرنامج لحلها إلى نقطة النهاية للتوجيه.

الجدير بالذكر أن محركات البحث العنكبوتية لا ترى مثل هذه الموقع، وذلك ليس بسبب وجود قيود التقنية. حيث يمكن لموقع البحث العنكبوتية حل اسم **DNS** البديل من خلال ربطه إلى واحد من خوادم **DNS** المحددة والمتحدة للجمهور وتطبيقات **TOR** و**I2P** ويحمل وكأنه **SOCKS proxy**، مما يجعل من الممكن لمحركات البحث العنكبوتية للوصول إلى المحتويات المذكورة. حيث نلاحظ وجود تسرب ملحوظ وحيد للمعلومات من **Darknet** إلى محرك البحث وهذا يحدت بفضل خدمة **tor2web gateway** مثل **tor2web**، والذي يقدم نطاق/دومين للوصول إلى محتوى موقع الخدمات المخفية مباشرة.

## :TOR2WEB

المصدر: <http://www.tor2web.org/config>

هو عباره عن بروتوكلي يتم ربطه بمحركات البحث العنكبوتية مثل جوجل ليتمكنه من البحث في موقع الويب المخفية (**deep web**) ويمكنك معرفة طريقة فعل ذلك عن طريق الانتقال الى هذه الموقع ورؤيه طريقة الربط. يتم ذلك عن طريق استبدال الامتداد [**.onion**] بالامتداد [**.tor2web.org**] في المتصفح العادي بدون استخدام تطبيق خاص. لكن هذا لن يعني عن استخدام التطبيق الخاص بهذه البيئة من الانترنت.

مثال على ذلك <https://xzzpowtjlobho6kd.tor2web.org> فيصبح هكذا <https://xzzpowtjlobho6kd.onion>

## نظرة عامة على شبكات الإنترنت الموجودة في الخفاء (DEEP WEB)

حتى الآن، يوجد تلات شبكات رئيسية لمنح الاتصال الغير مرئي لكل من العميل والخادم هما **Freenet**, **I2P**, **TOR**.

**ملحوظه:** الاثنين الآخرين لم يصلوا بعد إلى نفس الاعتماد الذي وصلت إليه **TOR** ولكن الميزات التقنية الحالية التي يمكنها أن تؤدي إلى أن يصبحوا بدانل قابلة للتطبيق في المستقبل القريب (على سبيل المثال، تصبح شبكة **TOR** لا يمكن الاعتماد عليها للغاية بالنسبة للمستخدمين).

### شبكة TOR

وضعت شبكة **TOR** في الأصل من قبل مختبر أبحاث للبحرية الأمريكية [U.S. Naval Research Laboratory]. قدم للمرة الأولى في عام 2002. فإنه يسمح للاتصالات المجهولة من خلال استغلال شبكة من **volunteer nodes** (أي أكثر من 3,000 حتى الآن) المسؤولة عن توجيه طلبات متفرقة بحيث يمكن إخفاء حركة مرور البيانات من أدوات مراقبة الشبكة. للاتسقادة من شبكة **TOR**، يحتاج المستخدم لتثبيت البرامج التي تعمل بمتابعة **SOCKS proxy**. برنامج **TOR** يخفى الاتصالات إلى أي خادم/سيرفر على شبكة الإنترنت عن طريق اختيار عدد من العقد (**node**) ذات تتبع العشوائي لتشكيل دائرة. قبل الدخول إلى الشبكة، يتم تشفير كل طلب بشكل متكرر باستخدام المفتاح العمومي لكل عقدة محددة. تم، من خلال الارتداد من تتبع [relay] واحدة إلى أخرى، ورفع كل طبقة من التشفير بقالة التتابع التالي، حتى يتم الوصول إلى عقدة الخروج ومن ثم يمكن للطلب الغير متغير الذهاب إلى وجهتها.

اعتماد هذه الآلية من التشفير متعدد الطبقات يعطي المزايا التالية:

- الخادم/الملمق الذي يتلقى الطلب القادم من شبكة **TOR** سوف ترى بأنها صادرة عن العقدة الأخيرة في دائرة **TOR** (أي عقدة الخروج [**exit node**]) ولكن هناك توجد طريقة واضحة للتتابع طلب العودة إلى أصله.
- كل عقدة [**node**] داخل الدائرة لا تعرف سوى **hop** السابق وبالتالي للطلب ولكنه لا يمكن فك محتوياته ولا معرفة وجهتها النهائية.
- العقدة الوحيدة التي يمكن **TOR** عرض طلب غير متفرقة هي عقدة الخروج ولكن حتى هذا لا يعرف أصل الطلب، يعرف فقط العقدة السابقة في الدائرة **hop**.

في الإصدارات الأخيرة من بروتوكول **TOR**، لقد تم إدخال وظائف جديدة للسماح لكامل الموقع ان يتم استضافتها على عقد **TOR**، مما يجعلها لا يمكن تعقبها. من المعروف أن الخدمات التي يتم تشغيلها ضمن شبكة **TOR** بأنها "خدمات خفية". **Approach** يعمل عن طريق تخزينه لمعلومات اتصال الوصول للخدمة الخفية على تسلق عقدة الانقاء (**rendezvous node**) التي سوف تعمل ك وسيط وكمنفذ للتشفير في [DHT] (Distributed Hash Table).

حيث يختار **DHT** بمتابعة تسلق من أشكال موزع **DNS**. حيث تعمل على حل اسم المضيف **onion** إلى معلومات الاتصال الازمة لتأسيس اتصال إلى الخدمة المخفية. في هذه الحالة، يتم إخفاء عنوانين لا **IP** لكل من العميل والملمق/الخادم من أي طرف ثالث يحاول تحويل أو منع حركة المرور. حتى يتم إخفاء الموقع الحقيقية عن بعضها البعض.

يمكن تحميل التطبيق المسنون عن الدخول إلى شبكة **TOR** وهو متصل توفر من الرابط التالي:

<https://www.torproject.org/>

### شبكة I2P

لقد تم تصميم **I2P** باعتباره [P2P anonymous peer-to-peer] يعمل على توزيع طبقة الاتصال والتي يمكنها تشغيل أي خدمة إنترنت تقليدية. قد تم تطويرها منذ عام 2003 باعتبارها تطوير لشبكة **Freenet network** ، والذي يهدف إلى السماح لعدة خدمات للتشغيل بجانب **HTTP**. بينما **TOR** انشاء في البداية لتمكين عدم الكشف عن الهوية عند الاتصال إلى خدمة الإنترنط (أي **WWW**) تم مدد في وقت لاحق إلى الخدمات العامة الخفية، الهدف من **I2P** هو توفير وسيلة للمستخدمين للوصول إلى الخدمات (على سبيل المثال، **IRC**, **web mail**, **bit torrent**) بطريقة خفية.

مشروع **I2P** اختصاراً لـ **Invisible Internet Project** هو برنامج حر ومجاني يمكن مستخدميه من الاتصال بدون الكشف عن الهوية على شبكة الإنترنط. الشبكة تمكن التطبيقات التي تستخدمنها من الحفاظ على خصوصية المستخدم حيث تشمل تطبيقات التصفح المجهول، والبريد الإلكتروني والمدونات ومشاركة الملفات. يهدف البرنامج إلى دعم حرية التعبير والرأي وتجاوز حجب الموقع على الأنترنط يمكنه التعبير عن رأيك بحرية دون الخوف من أن تعرف مستخدم البرنامج.

هي شبكة تخفى تؤمن طبقة يمكن أن تستخدمها التطبيقات الحساسة بالنسبة للهوية الشخصية للاتصال بشكل آمن حيث تغطى جميع البيانات بعدة مستويات من التشفير إضافةً لكون الشبكة موزعة وديناميكية بنفس الوقت بدون الاعتماد على أطراف موثوقة.

تتوافق العديد من التطبيقات التي تتداخل مع **I2P** وتشمل البريد الإلكتروني، تطبيقات الند للند (**P2P**)، محادثة **IRC** وغيرها.

تم البدء بمشروع **I2P** في العام 2003 لدعم جهود كل من يحاول بناء المجتمع الحر وذلك من خلال تأمين نظام تواصل خفي، غير قابل للمرقابة وأمن **I2P**. هي نتاج جهود تصافرت لإنتاج شبكة قليلة التأخير، موزعة بشكل كامل، مستقلة، خفية، مزنة وأمنة. الهدف هو العمل بنجاح ضمن بيئة معادية بالرغم من كون موارد المنظمة المالية أو السياسية تحت الهجوم. كل ما يتعلق بهذه الشبكة مفتوح المصدر ومتوفر بدون أي تكلفة وهذا ما يضمن لمن يستخدمه أن هذه الشبكة تؤدي ما تدعى به، بالإضافة إلى تمكين الآخرين من المشاركة في تطويرها في مواجهة المحاولات العدوانية لخنق الكلمة الحرية.

التحفي ليس شيئاً حديثاً، يعني أننا لا نحاول أن نصنع شيئاً "خفياً بالكامل"، ولكن نعمل على أن يجعل الهجمات أكثر وأكثر تكلفة لمن يريد أن يتسلل إليها. **I2P** هي مزيج من الشبكات قليلة التأخير وهناك حدود للتخفيف الموفر بواسطة نظام كهذا، ولكن تطبيقات مثل **I2PSnark** ، **I2P mail** و **Syndie** توسيع هذا النظام وتتوفر المزيد من الوظائف الإضافية والحماية.

ما تزال **I2P** عملاً قيد الإنجاز لا يحب أن يعتمد عليه في الوقت الراهن في التخفيف بشكل "مضمون" وذلك بسبب حجم الشبكة الصغير نسبياً وقلة المراجعة الأكاديمية الممتددة. كما لا تعتبر حالياً متاحة ضد الهجمات من قبل أشخاص بموارد غير محدودة وقد لا تكون أبداً كذلك. تبعاً للحدوديات المورونة من كونها مزيج من الشبكات قليلة التأخير.

المبدأ الرئيسي **TOR** هو خلق دوائر (أي مسارات متفرقة من خلال مجموعة عشوائية من العقد للوصول إلى لعقدة الخروج التي هي بمثابة وكيل أو إلى نقطة الالقاء التي تعمل ك وسيط للتواصل مع خدمة الخفية). **I2P**، من ناحية أخرى، يستخدم الانفاق **TUNNEL**. كل عقدة في شبكة **I2P** هو جهاز التوجيه. أنه يخلق ويحافظ على مجموعة من المسارات الظاهرة الواردة والصادرة. على سبيل المثال، إذا عقدة **A** يريد أن يرسل رسالة إلى عقدة **B**، فإنه يقوم بتوجيه رسالته إلى واحدة من الأنفاق في الخارج جنباً إلى جنب مع المعلومات اللازمة للوصول إلى واحدة من الأنفاق الواردة.

يتم تخزين المعلومات حول الأنفاق الواردة، والتي تنتهي إلى حد كبير في **DHT** ، في **TOR** التي هي بمثابة قاعدة بيانات شبكة لا مركزية.

يتم تشفير كل الاتصالات باستخدام طبقات متعددة: التشفير من نقطة إلى نقطة بين المرسل والمنتقى، والتشفير النقل بين أجهزة التوجيه في الشبكة، والتشفير من النهاية إلى النهاية في الأنفاق. نلاحظ أن، **TOR** يستخدم نظام تشفير يسمى "**onion routing**"، والتوجيه المتغير المستخدم في **I2P** يعرف باسم "**garlic routing**" والموقع الخفي الذي يتم استضافتها في شبكة **I2P**، تسمى أيضاً "**eepsites**".

يمكنك تحميل التطبيق المسنون عن الولوج لهذه الشبكة من خلال الرابط التالي:

<http://geti2p.net/en/>

## شبكة FREEINET

تم تطويره منذ عام 2000، ويمكن اعتباره سلف لا **I2P**. ولكنه على عكس **pure DHT** في شكل شبكة تراكب غير منظم. هذا يعني أن كل عقدة مسؤولة عن مجموعة فرعية من الموارد المتاحة في الشبكة، ويقدم لهم التعاون عندما ينافي الطلب. وعلاوة على ذلك، فإن العقد يحفظ قائمة بالعقد المجاورة، والمعروفة عادة بالجيران الموثوقين، وذلك لزيادة الأمان. ويعرف هذا باسم "**small world principle**". العقد والبيانات يتم تعرفيهم بواسطة المفتاح، الممثلة عادة مع قيمة المهاش. عندما تبحث عن مورد ما، فإن طلابك سوف يسافر عبر جميع العقد الجيران حسب الأفضلية.

فرینت هو أكثر ملاءمة عند استخدام محتوى التابت مثل المواقع التابتة ولا يتعامل بشكل جيد مع صفحات الويب المولدة ديناميكياً أو غيرها من أشكال خدمات الإنترنت (على سبيل المثال، **IRC**، والبريد، وغيرها).

## ALTERNATIVE DOMAIN ROOTS

**Alternative Domain Roots** ، المعروف أيضاً باسم "**rogue TLDs**" ، تشير إلى فئة من الشبكات التي تستخدم كيانات **DNS** ولكن التي ليست تحت سيطرة **ICANN**، وتكون على التقى من النطاقات [**.com** / **.net** / **.org**] . التقليدية. النطاقات المسجلة ضمن **rouge TLD** تتطلب استخدام خوادم أسماء (**named server**) مخصصه. من ناحية أخرى، اعتماداً على المؤسسة التي تعمل على ت Tesselar **DNS root** ، فإن تسجيل اسم الدومن قد يكون أقل إثارة للمتاكيل لـ **malicious actors** ، كما في حالة **.bit domain** .

نطاق جديد تتبّع نموذج **P2P** باختصار، هذا يعني أنه عند تسجيل اسم نطاق جديد فبدلاً من التعامل مع السلطات المركزية يتم نشره مستقلًا في شبكة **P2P** المصنوعة من كافة ملفات **.bit DNS** . حتى يصبح كل ملقم/خادم على علم بالنطاقات المسجلة حديثاً.



في حين ان **alternative DNS domains** لا يقدم أشكال معينة من عدم الكشف عن الهوية على عکس **TOR**، ولكنها ت تعرض بعض المزايا الواضحة لجهات **malicious actors** مثل الحماية ضد **domain sinkholing** ومروره في اداره النطاقات/الدومنين، وحتى الان، إمكانية "الهروب" من محرك البحث العنكبوتية. في حين انه من الممكن من الناحية الفنية لمحرك البحث العنكبوتى الوصول الى الآن، على سبيل المثال، وذلك ببساطة باستخدام خوادم DNS الخاصة به)، فإنه لا يحدث عادة، وإذا كان كذلك، فلن تظهر النتائج للمستخدمين.

#### فيما يلي قائمه بـ ALTERNATIVE DOMAIN ROOTS الفعالة:

**Namecoin**: مسؤول عن [bit TLD]. هو قائم في عمله على P2P يعمل بنفس مبدأ bitcoins. للوصول إلى هذا الدومنين من قبل العميل فإنه يحتاج الى تشغيل **dedicated DNS client** أو الرجوع إلى أحد خوادم DNS التي تعتبر بوابة لهذه الشبكة على الإنترنت.

يمكنك استخدام **FreeSpeechMe** على متصفح الفايرفوكس لرؤية الموقع [bit]. وذلك عن طريق الذهاب الى الموقع التالي [http://www.freespeechme.org] وهو أيضا يحتوى على قائمه بمواقع [bit].

**Cesidian root**: عباره عن alternative DNS تدار من قبل المواطنين الإيطاليين تستخدم نطاقات TLD التالية [.cw,.6w,.5w,.ispisp] وليست لدعم رؤية Mr. Tallini's السيسية والذي يتغلب أيضا منصب محافظ (UMMOA) وتعنى United Micronations Multioceanic Arcipelago وهذا يضم 30 مقسم/خادم DNS حول العالم يعمل على كل من IPv4 وIPv6. لمزيد من المعلومات <http://cesidianroot.net>

**Namespace.us**: هذه المنظمة تقدم 482 Alternative TLD مثل [.academy - .big - .manifesto]. وجدت في السوق منذ عام 1986، تأسست لتوضيغ عدد محدود (في ذلك الوقت) من نطاقات Alternative TLD المتاحة، وقدمت أسرع عملية في تسجيل هذه النطاقات، فضلاً عن الخدمات الأخرى ذات الصلة بالمجال. بعد أن فشلت في أواخر 1990 أن يكون لها نطاقات TLD متكاملة في منطقة DNS root، فإنه لا يزال موفراً بديل لأسماء النطاقات حتى الآن، وتقدم خوادم DNS الخامسة التي تعمل على حل كل من نطاقات الطبايا، مثل التي تقدمه ICANN.

**OpenNIC**: هذا المشروع يتكون من شبكة من خوادم DNS التي تديرها Hobbists والمتطلعون التي تهدف إلى تقديم بنية تحتية غير محايدة ومستقلة عن الحكومات والمنظمات ، ومجاناً للجميع. يمكن لأي شخص تقديم جهاز كمبيوتر لاستخدامها كخادم tier-2 DNS مع ترتيب احترام سياسة المنظمة بشأن أنها، والأداء، وإخفاء الهوية. بالإضافة إلى تقديم شبكة من خوادم DNS القائلية، هذا الـ DNS يوفر أيضاً مساحة بديلة للنطاقات العليا 14 [14 TLDs] ويدعم أربع نطاقات بديلة TLD من NewNations، وهي المنظمة التي تقدم domain root لكيانات سياسية معينة مثل Tibetan أو الشعب الكردي.

لمزيد من المعلومات <http://www.opennicproject.org>

**Deep Web**: هو مجموعة من المواقع الغير معروفة والتي لا يتم ارتيافتها في موقع البحث ولن تجدها عند قيامك بالبحث في اي موقع بحث لأنها تستخدم نطاقات مختلفة عن التي يستخدمها الانترنت العادي فمتى نحن نعرف النطاق .com و .net. ولكن الانترنت الخفي لا يستخدم مثل هذه النطاقات بل هو يستخدم نطاقات مثل onion و .i2p و .bit. وغيرها

مثال على ذلك كالاتي:

ofrmtr2fphxkqgz3.onion

استخداماته تستخدم هذه المواقع في black market (السوق السوداء) مثل بيع السلاح المحظيات الجنسية ويوجد عليه العديد من مواقع الهاكرز والدروزن في الهاكرز.

**Darknet**: هي موقع متواجدة ولكنها لا تستخدم البروتوكولات المعروفة مثل http:// وهو يستخدم في مشاركة الملفات وعليه تستطيع ان نقول ان من يستخدم هذه المواقع هم من يقومون بمارسه الاعمال الغير مشروعه على الانترنت وهم يستخدمون هذه المواقع لأنه لا يمكن للحكومات او اي جهة اخرى بتعقبهم.

ما أهميتها؟

أهمية هذا الجزء أنه أكبر بكثير من المحتوى المرئي من الانترنت ويقدر حجمه بأنه 500 ضعف محتوى الويب المرئي (الويب المرئي هو الجزء الذي يمكن الوصول إليه عن طريق محركات البحث)، وينتشر أيضًا بكفاءة المعلومات الموجودة فيه وكثرتها، ولذا فقد الكثير من المعرفة في هذا الجزء.

ما سبب أنه مخفى أو لا يمكن لمحركات البحث أن تراه؟

سمى هذا الجزء من الانترنت deep web أو invisible web لأن محركات البحث لا يمكن أن تراه أو تجده بسهولة أو ببساطة هذا المحتوى غير مصمم ليفهرس أو ليتم رؤيته على محركات البحث، ولنفهم أكثر يجب أن نعرف كيفية عمل محركات البحث:



## محتوياته:

- محتويات قواعد البيانات **Databases** مثل قواعد بيانات المنشورات وأرقام التليفونات وأدلة المكتبات.
  - الملفات الغير نصية كـ **PDF** والصور وملفات الورد.
  - البيانات المحمية بكلمة سر.
  - البيانات دائمة التغيير **Dynamic data** مثل الأخبار ومواعيد رحلات الطيران.
  - التعليقات على المقالات.
  - البيانات الموجودة في الموقع الاجتماعي **Twitter** و **Facebook**.
  - التدوينات.
  - المرجعيات **Bookmarks** في موقع مشاركة المرجعية.
  - أسلحة مخدرات دروس وبرامج هاكرز نادرة أشياء غير أخلاقية
- اقول لك ان الهدف من انشاء تلك المواقع المظلمة السرية هو العمل بعيداً عن اعين الرقابة والشرطة والسلطات. الهدف غير مشروع كعقد صفقات اسلحة غامضة او قصص وروایات ممنوعة لا يمكن نشرها على الشبكة المحلية والعالمية المعروفة. كالاتجار في المخدرات الخطيرة وغيرها.
- ستجد كل ما هو ممنوع وإجرامي في هذا ولا تظنين ان تلك المواقع الممتعة فقط. انها عبارة عن السوق السوداء **Black Market's**. لكل شيء لا يمكنك تخيله سوف تجد بها المواقع الاجتماعية للتواصل وبرامج الهاكر الغامضة ومحاضراتها "طبعاً كل حاجة بفلوس" ليس مجاني في هذا العالم والا فما الفائدة منه
- طبعاً هناك مواقع مجانية مثل: شبكات التواصل الاجتماعي كالفيسبوك، كالدرستة المجانية التي تجدها على هذا الرابط [2hluuzwi7tuceu6.onion](http://2hluuzwi7tuceu6.onion)

من الفوائد العظيمة لهذا هو التخفي وقت الاختراق حيث عند تصفح الانترنت المظلم او الخفي تقدر تتصفح الواقع العادي بس الواقع المخفية تظهر هي الأخرى.

### كيفية البحث في محتويات الانترنت الخفي:

يوجد موقع بحث تحاول فهرسة الويب الخفي مثل الآتي:

<http://infomine.ucr.edu/>

<http://www.completeplanet.com/index.jsp>

<http://vlib.org/>

<https://archive.org/>

<http://clusty.com/>

<http://lookahead.surfwax.com/index-2011.html>

فيما يلى بعض مواقع الويب التي تحتوى على قائمه بجميع مواقع الويب الخفية dark web كالاتى:

<http://deepweblinks.org/>

<https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web>

### كيفية الدخول الى الانترنت المظلم؟

لدخول الى الانترنت المظلم يجب تحميل برنامج خاصه لذلك كمثال فانا استعمل جوجل كروم لتصفح الانترنت وكروم غير قادره على تصفح

نطاقات اخرى غير .com.gov.net.الخ

توجه الى هذا الموقع وقوموا بتحميل المتصفح الخاص بفتح تلك المواقع (متصفح تور)

<https://www.torproject.org/>

حجم المتصفح 22ميغا سهل الاستخدام ويسمى موزيلا فايرفوكس بالضبط

1- بعد فك ضغط البرنامج سوف تجدون ملفا باسم **Start Tor Browser.exe**

2- قم بالضغط عليه وانتظر حتى يتم الاتصال بتقبيلة **Tor** التي ستعامل من خلالها مع نطاقات الواقع التي تنتهي بالامتداد **Onion**

3- انتظر دقيقة تقريباً حتى يتم الاتصال ولسوف يفتح لك المتصفح تلقائياً. عقب البحث عن شبكة تور **Tor** التي تتحدى عنها قم بعمل

رفقيش في المرة الاول وسوف يتم الاتصال بنجاح

من خلال هذا المتصفح الفريد من نوعه يمكنك الاتصال بتقبيلة الانترنت المظلم والخفى والعميق.

الحمد لله تعالى نكون هنا انتهينا من الوحدة الثانية وهي عملية جمع المعلومات

Dr. Mohammed Sobhy Teba

<https://www.facebook.com/tibea2004>

د. محمد صبحي طيبة