

الفصل الأول

جمع معلومات عن الهدف

المؤلف

د.م/ أحمد هاشم الفقي

مستشارى أمن المعلومات و التحول الرقمي

Ahmed.Hashem.ElFiky@outlook.com

محتويات هذا الفصل:

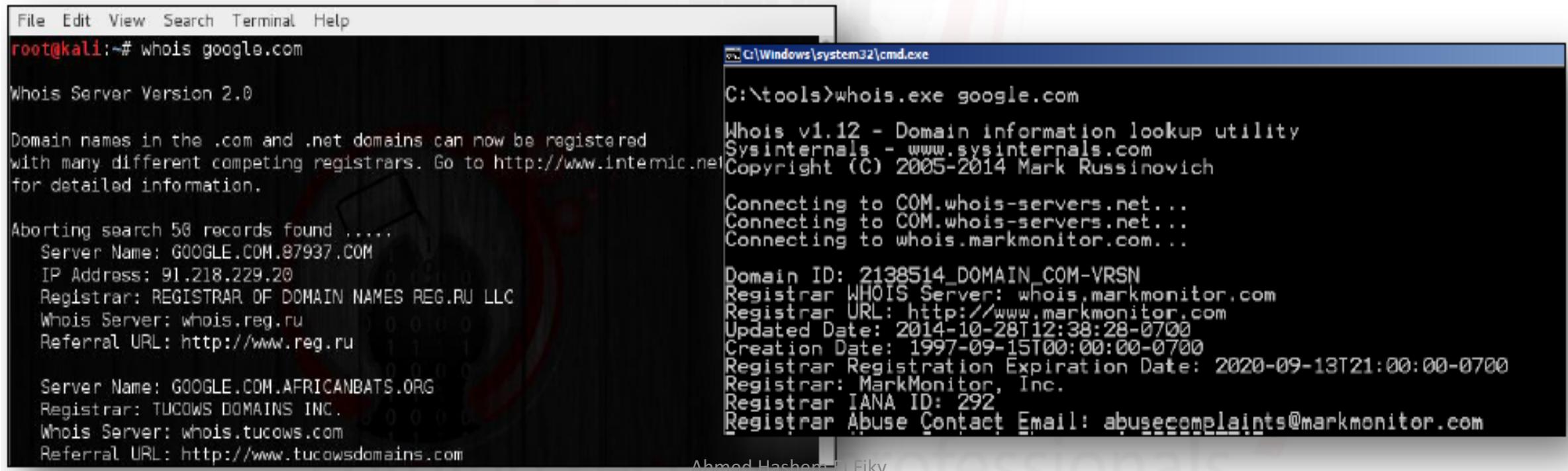
- فهم ال dnsrecon Tool
- فهم ال subbrute Tool
- فهم ال theHarvester Tool
- فهم مصطلح DNS Zone Transfer
- فهم ال fierce Tool
- فهم ال DirBuster Tool
- فهم موقع Shodan HQ
- بناء Functional Graph للهدف
- فهم ال WHOIS Tool
- فهم ال DNS nslookup Tool
- فهم موقع Netcraft
- فهم ال Netcat Tool
- فهم ال WhatWeb Tool
- فهم ال Wappalyzer Tool
- فهم ال Google Search Operators

ما هى أنواع المعلومات التي نسعى لمعرفتها عن الهدف

- نسعى لمعرفة بعض المعلومات عن الهدف و منها (Web server, CMS, Database, ... Infrastructure مثلا)
- معلومات عن ال Application Logic اى كيفية عمل الهدف
- معلومات عن ال IPs, Domains and SubDomains
- معلومات عن ال Virtual hosts

فهم ال WHOIS Tool

- اداة ال WHOIS تبحث عن تفاصيل ownership للهدف من قواعد بيانات مختلفة.
- توجد هذه الاداة فى شكل Web-Based او فى شكل Command-Based



The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal with a black background and white text. It displays the command 'root@kali:~# whois google.com' followed by the output of the Whois Server Version 2.0. The right window is a Windows cmd.exe terminal with a blue title bar and white text. It displays the command 'C:\Windows\system32\cmd.exe C:\tools>whois.exe google.com' followed by the output of the Whois v1.12 utility. Both outputs provide domain registration information for 'google.com'.

```
File Edit View Search Terminal Help
root@kali:~# whois google.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.

Aborting search 50 records found .....
Server Name: GOOGLE.COM.87937.COM
IP Address: 91.218.229.20
Registrar: REGISTRAR OF DOMAIN NAMES REG.RU LLC
Whois Server: whois.reg.ru
Referral URL: http://www.reg.ru

Server Name: GOOGLE.COM.AFRICANBATS.ORG
Registrar: TUCOWS DOMAINS INC.
Whois Server: whois.tucows.com
Referral URL: http://www.tucowsdomains.com

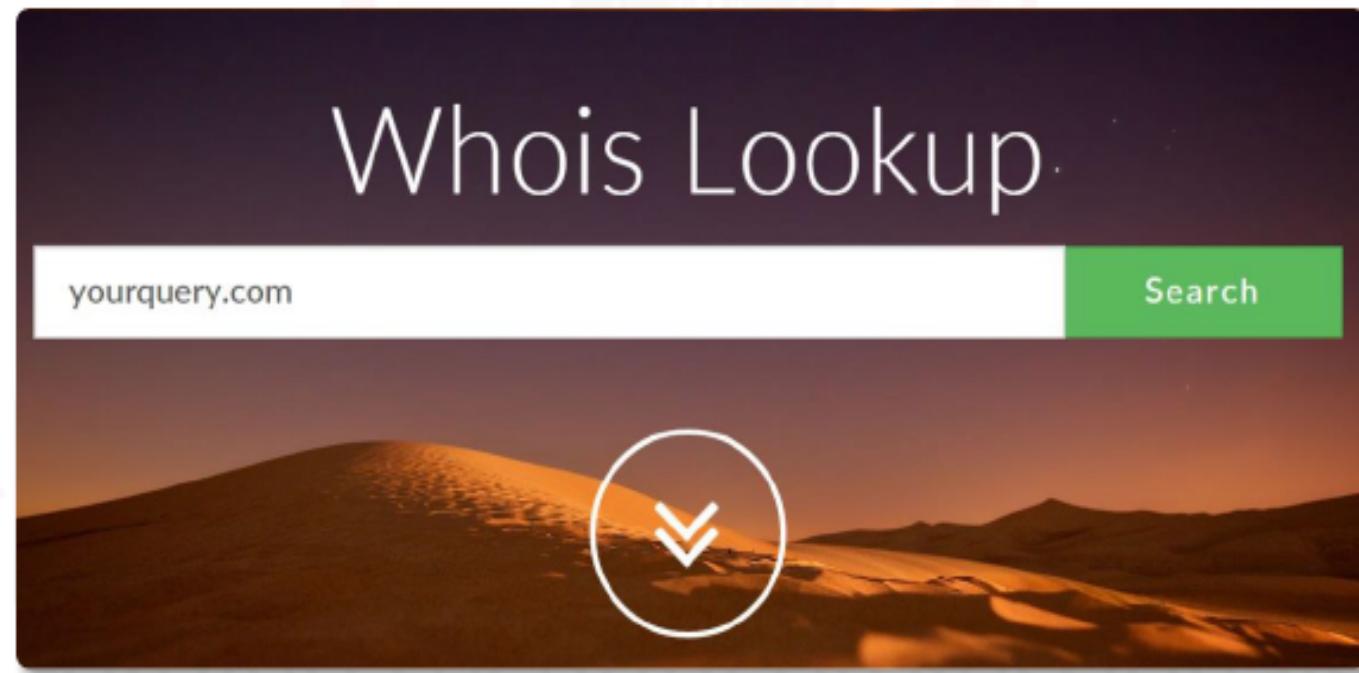
C:\Windows\system32\cmd.exe
C:\tools>whois.exe google.com
Whois v1.12 - Domain information lookup utility
Sysinternals - www.sysinternals.com
Copyright (C) 2005-2014 Mark Russinovich

Connecting to COM.whois-servers.net...
Connecting to COM.whois-servers.net...
Connecting to whois.markmonitor.com...

Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2014-10-28T12:38:28-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
```

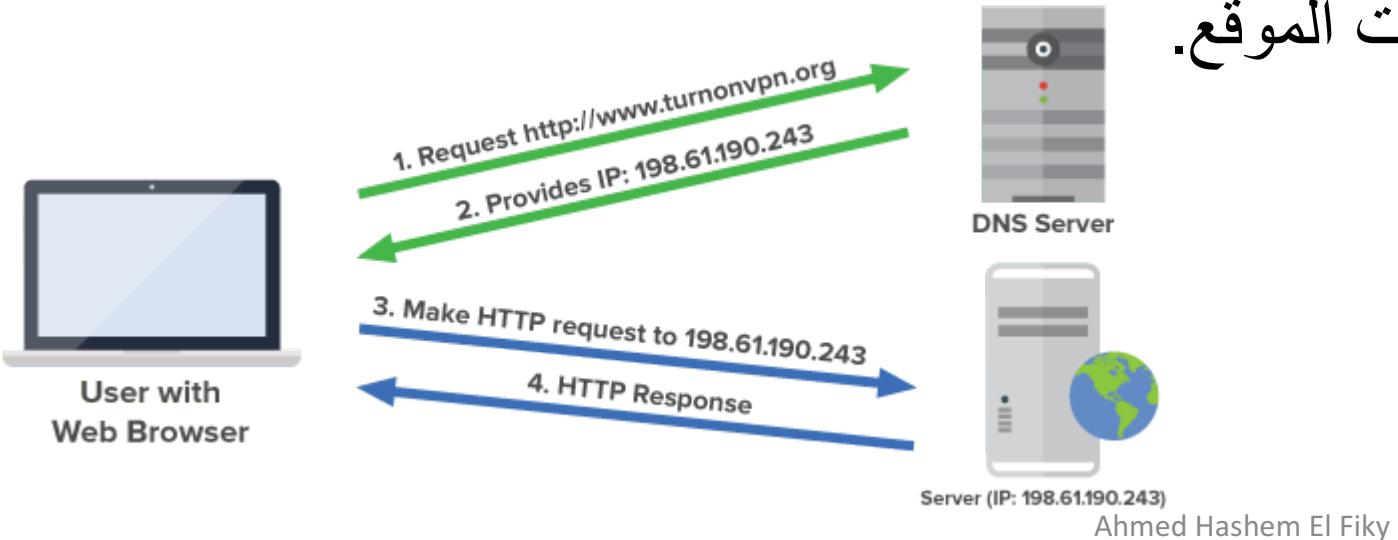
فهم ال WHOIS Tool (نكلة...)

web-based tools such as: whois.domaintools.com



فهم ال DNS

- DNS هو اختصار لمصطلح Domain Name System أو Domain Name Service، و يستخدم لربط اسم الدومن الخاص بك لسرفر معين (أي لشركة الاستضافة الخاصة بك).
- وظيفة DNS هنا هي تحويل اسم النطاق أو الدومن الذي يكتبه الزائر في متصفحات الإنترنـت، إلى IP Address يستطيع الكمبيوتر التعامل والاستجابة له.
- كلما قام أحدهم بكتابة اسم النطاق في المتصفح، يقوم DNS في جزء من الثانية بمطابقة اسم الدومن مع IP Address الخاص بالموقع، ومن ثم يقوم بجلب البيانات أو تحميل الموقع من السرفر المخزن عليه بيانات الموقع.



فهم ال DNS (تكميله...)

- يتكون ال DNS من عدة Records منها:

A record •

- يقوم بتوجيه اسم النطاق إلى عنوان IP الخاص بالخادم المستضيف لموقعك.

NS record •

- يشير إلى اسم الخادم المستضيف لموقعك .

CNAME record •

- يستخدم لإنشاء أسماء مستعارة لاسم النطاق الخاص بك. مثلاً لديك اسم نطاق domain.com يحمل الموقع الإلكتروني، يمكن عمل اسم نطاق فرعي منه مثل web.domain.com باستخدام CNAME

PTR record •

- ترجمة ال IP address إلى اسم ال Domain

فهم الـ DNS (تكميله...)

MX record •

• وهو المسؤول عن توجيه البريد الإلكتروني حيث يتم تعين MX record للاشارة إلى خادم البريد

Common Resource Record Types

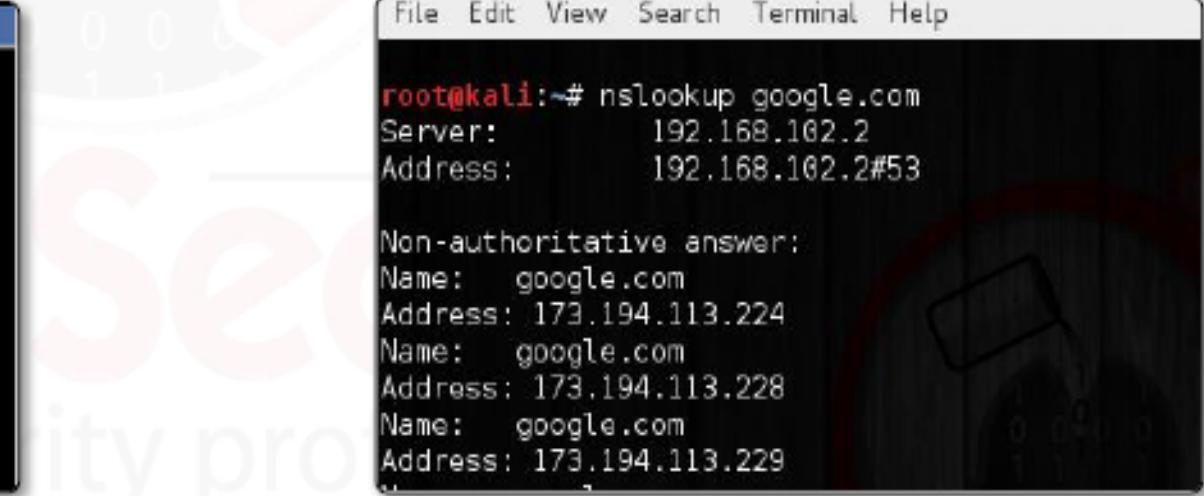
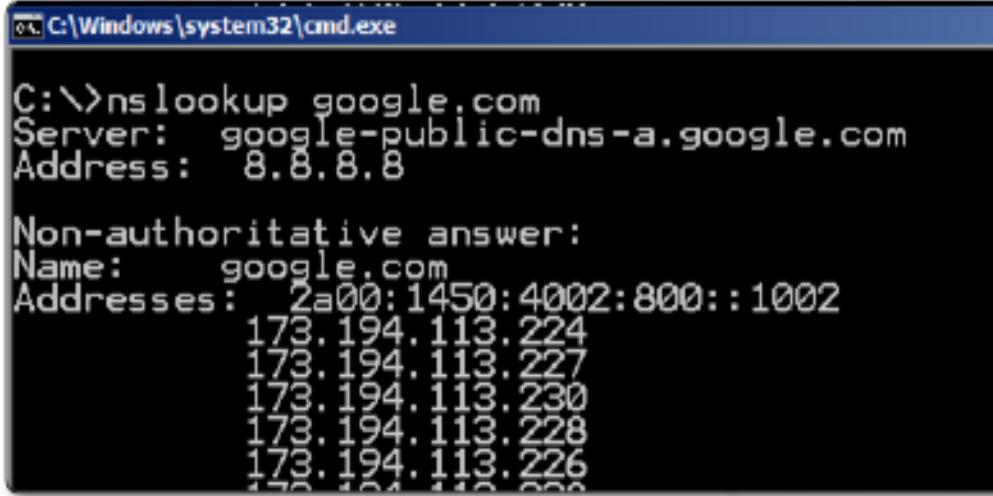
RR Type	Name	Functions
A	Address record	Maps domain name to IP address www.apnic.net. IN A 203.176.189.99
AAAA	IPv6 address record	Maps domain name to an IPv6 address www.apnic.net. IN AAAA 2001:db8::1
NS	Name server record	Used for delegating zone to a nameserver apnic.net. IN NS ns1.apnic.net.
PTR	Pointer record	Maps an IP address to a domain name 99.189.176.203.in-addr.arpa. IN PTR www.apnic.net.
CNAME	Canonical name	Maps an alias to a hostname web IN CNAME www.apnic.net.
MX	Mail Exchanger	Defines where to deliver mail for user @ domain apnic.net. IN MX 10 mail01.apnic.net. IN MX 20 mail02.apnic.net.

mail.example.com



فهم ال nslookup Tool

- هي اداة تستخدم لترجمة IP address الى host name و العكس



```
C:\>nslookup google.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: google.com
Addresses: 2a00:1450:4002:800::1002
          173.194.113.224
          173.194.113.227
          173.194.113.230
          173.194.113.228
          173.194.113.226

root@kali:~# nslookup google.com
Server: 192.168.102.2
Address: 192.168.102.2#53

Non-authoritative answer:
Name: google.com
Address: 173.194.113.224
Name: google.com
Address: 173.194.113.228
Name: google.com
Address: 173.194.113.229
```

فهم ال nslookup Tool (تكميلة...)

```
File Edit View Search Terminal Help
root@kali:~# nslookup -type=PTR 173.194.113.224
Server:      192.168.102.2
Address:     192.168.102.2#53

Non-authoritative answer:
224.113.194.173.in-addr.arpa    name = mil01s18-in-f0.le100.net.

Authoritative answers can be found from:

root@kali:~#
```

172.194.113.224 is the IP address we have found in the previous step

فهم ال nslookup Tool (تكاملة...)

```
nslookup -querytype=ANY google.com
```

```
File Edit View Search Terminal Help
root@kali:~# nslookup -querytype=ANY google.com
;; Truncated, retrying in TCP mode.
Server: 192.168.102.2
Address: 192.168.102.2#53

Non-authoritative answer:
Name: google.com
Address: 173.194.113.229
google.com has AAAA address 2a00:1450:4002:800::1004
google.com mail exchanger = 20 alt1.aspmx.l.google.com.
google.com rdata_257 = \# 19 00056973737565737960616E7465632E636F6D
google.com mail exchanger = 50 alt4.aspmx.l.google.com.
google.com mail exchanger = 40 alt3.aspmx.l.google.com.
google.com nameserver = ns1.google.com.
google.com origin = ns1.google.com
google.com mail addr = dns-admin.google.com
google.com serial = 2015032501
google.com refresh = 7200
google.com retry = 1800
google.com expire = 1209600
google.com minimum = 300
google.com nameserver = ns2.google.com.
google.com text = "v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.71/31"
```

فهم ال nslookup Tool (تكاملة...)

IP Location	Singapore Singapore Cloudflare Inc.
ASN	AS13335 CLOUDFLAREN - CloudFlare, Inc. (registered J
Whois Server	whois.arin.net
IP Address	104.20.2.47
NetRange:	104.16.0.0 - 104.31.255.255
CIDR:	104.16.0.0/12
NetName:	CLOUDFLAREN
NetHandle:	NET-104-16-0-0-1
Parent:	NET104 (NET-104-0-0-0-0)
NetType:	Direct Assignment
OriginAS:	AS13335
Organization:	CloudFlare, Inc. (CLOUD14)
RegDate:	2014-03-28
Updated:	2014-03-28
Comment:	https://www.cloudflare.com
Ref:	http://whois.arin.net/rest/net/NET-104-16-0-0-1
OrgName:	CloudFlare, Inc.
OrgId:	CLOUD14
Address:	665 Third Street #207
City:	San Francisco

```
root@kali:~# nslookup statcounter.com
Server:          192.168.102.2
Address:         192.168.102.2#53

Non-authoritative answer:
Name:  statcounter.com
Address: 104.20.2.47
Name:  statcounter.com
Address: 104.20.3.47
```

فهم ال Netcraft Tool

- هي اداة غنية بالمعلومات تستخدم كبديل للادوات WHOIS and nslookup وغيرها من المعلومات الهامة

Netcraft

Network

Site	http://statcounter.com	Netblock Owner	CloudFlare, Inc.
Domain	statcounter.com	Nameserver	may.ns.cloudflare.com
IP address	104.20.3.47	DNS admin	dns@cloudflare.com
IPv6 address	Not Present	PowerDNS	
Domain registrar	unknown		
Organisation	unknown		
Top Level Domain	Commercial		
Hosting country	US		

```
root@kali:~# nslookup statcounter.com
Server:      192.168.102.2
Address:     192.168.102.2#53

Non-authoritative answer:
Name:   statcounter.com
Address: 104.20.2.47
Name:   statcounter.com
Address: 104.20.3.47
```

This is the IP address that we found using nslookup.

فهم الـ Netcraft Tool (تكميله ...)

Netcraft

Network

Site: <http://statcounter.com>

Netblock Owner: CloudFlare, Inc.

Domain: statcounter.com

IP address: 104.20.3.47

IPv6 address: 2607:f8b0:400e::47

ASN: AS13335 CLOUDFLAREN - CloudFlare, Inc. (registered)

Whois Server: whois.arin.net

IP Location: Singapore Singapore Cloudflare Inc.

NetRange: 104.16.0.0 - 104.31.255.255

CIDR: 104.16.0.0/12

NetName: CLOUDFLAREN

NetHandle: NET-104-16-0-0-1

Parent: NET104 (NET-104-0-0-0-0)

NetType: Direct Assignment

OriginAS: AS13335

Organization: CloudFlare, Inc. (CLOUD14)

RegDate: 2014-03-28

Updated: 2014-03-28

Comment: <https://www.cloudflare.com>

Ref: <http://whois.arin.net/rest/net/NET-104-16-0-0-1>

OrgName: CloudFlare, Inc.

OrgId: CLOUD14

Do you remember?
This Netblock belongs
to "CloudFlare", we
have already found it
using whois !

فهم الـ Netcraft Tool (تكميله (...)

Background													
Site title	Microsoft – Official Home Page	Date first seen	August 1995										
Site rank	1082	Primary language	English										
Description	At Microsoft our mission and values are to help people and businesses throughout the world realise their full potential.												
Keywords	Not Present												
Network													
Hosting History													
Netblock owner	IP address	OS	Web server	Last seen	Refresh								
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	29-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	25-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	24-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	22-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	21-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.185.46	unknown	Microsoft-IIS/8.5	15-Mar-2015									
Microsoft Corp One Microsoft Way Redmond WA US 98052	134.170.188.221	unknown	Microsoft-IIS/8.5	14-Mar-2015									

فهم ال Netcat Tool

NetCat هي أداة Unix بسيطة جدًا يمكنها قراءة وكتابة اتصالات شبكة TCP أو UDP تم تصميمها كأداة خفية موثوقة يمكن تشغيلها مباشرة وبسهولة. هنا سوف نستخدمها في الكشف عن نوع الخادم.

```
</>root@kali:~# nc 192.168.102.136 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 30 Mar 2015 14:40:06 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 05 Feb 2015 21:12:05 GMT
ETag: "1847cb-b1-50e5dc184b340"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

Remember that once we establish the connection with netcat, we have to send HEAD / HTTP/1.0 and hit enter two times

From the server field we can see that we are running Apache version 2.2.22 on Linux OS

فهم الـ Netcat Tool (تكميلة...)

```
</>root@kali:~# nc 134.170.185.46 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Cache-Control: private
Content-Length: 23
Content-Type: text/html
Location: http://www.microsoft.com
Server: Microsoft-IIS/8.5
Set-Cookie:
ASPSESSIONIDACRQQCDQ=LKKMCDHAFINIAMHBICPIMLJE; path=/
...
```

The following output shows us that the remote Web Server is using IIS version 8.5

فهم الـ Netcat Tool (تكميلة...)

```
</>root@kali:~# nc 134.170.188.221 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
..stripped output...
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET ←
X-UA-Compatible: IE=EmulateIE7
Date: Tue, 31 Mar 2015 07:48:01 GMT
Connection: close
```

In this case, the header tells us the Web App is using ASP.NET. Other possible values are PHP, JSP, JBoss and so on.

فهم أداة ال WhatWeb

- هي أداة تستخدم أيضاً لمعرفة نوع ال Server او الخادم .

```
root@kali:~/tools/WhatWeb# ./whatweb www.elearnsecurity.com
http://www.elearnsecurity.com [302] HTTPServer[Microsoft-IIS/7.5], IP[199.193.116.231],
Microsoft-IIS[7.5], RedirectLocation[https://www.elearnsecurity.com/], Title[Document
Moved], UncommonHeaders[x-xss-protection,x-frame-options,strict-transport-security], X-
Frame-Options[sameorigin], X-Powered-By[MOS 6502], X-XSS-Protection[1; mode=block]
https://www.elearnsecurity.com/ [200] HTML5, HTTPServer[Microsoft-IIS/7.5], IP[199.193.
116.231], JQuery, Microsoft-IIS[7.5], PoweredBy[eLearnSecurity,], Script[text/javascript],
Title[eLearnSecurity - IT Security training courses for individuals and corporation
s], UncommonHeaders[x-xss-protection,x-frame-options,strict-transport-security], X-Fram
e-Options[sameorigin], X-Powered-By[MOS 6502], X-UA-Compatible[IE=edge], X-XSS-Protection[1;
mode=block]
root@kali:~/tools/WhatWeb#
```

```
root@kali:~/tools/WhatWeb# ./whatweb -v www.elearnsecurity.com
http://www.elearnsecurity.com/ [302]
http://www.elearnsecurity.com [302] HTTPServer[Microsoft-IIS/7.5], IP[199.193.116.231], Mi
ectLocation[https://www.elearnsecurity.com/], Title[Document Moved], UncommonHeaders[x-xss
ions,strict-transport-security], X-Frame-Options[sameorigin], X-Powered-By[MOS 6502], X-XS
ock]
URL   : http://www.elearnsecurity.com
Status : 302
HTTPServer -----
    Description: HTTP server header string. This plugin also attempts to
                  identify the operating system from the server header.
    String     : Microsoft-IIS/7.5 (from server string)

IP -----
    Description: IP address of the target, if available.
    String     : 199.193.116.231

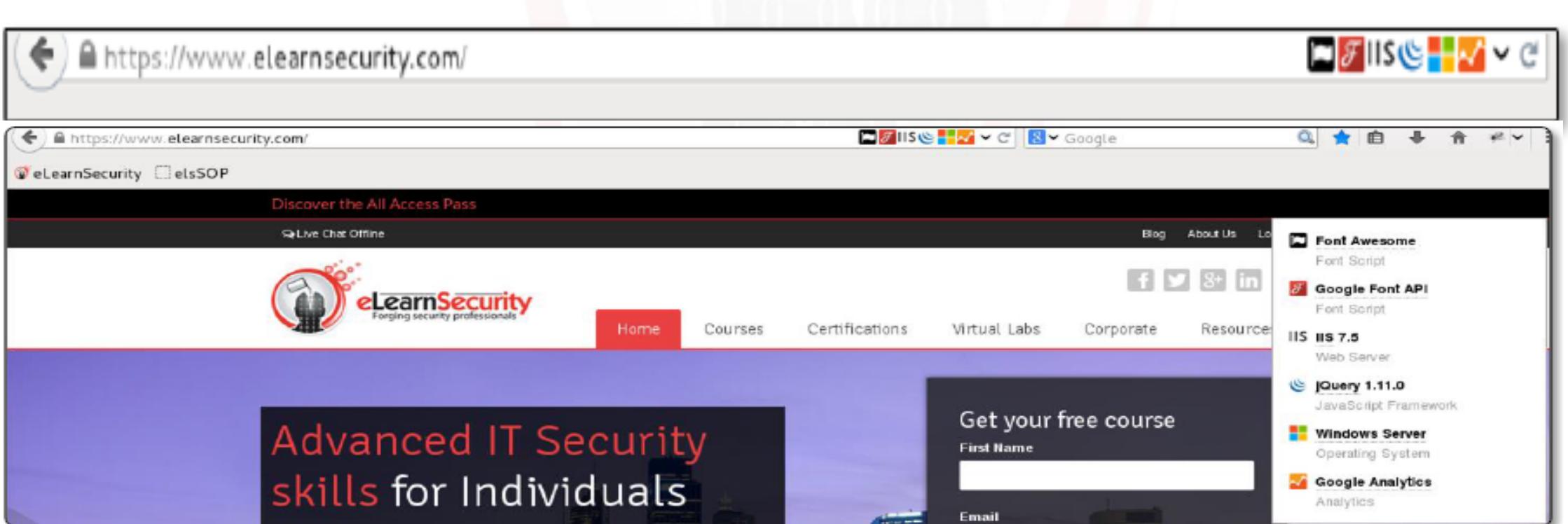
Microsoft-IIS -----
    Description: Microsoft Internet Information Services (IIS) for Windows
                  Server is a flexible, secure and easy-to-manage Web server
                  for hosting anything on the Web. From media streaming to
                  web application hosting, IIS's scalable and open
                  architecture is ready to handle the most demanding tasks. -
                  homepage: http://www.iis.net/
    Version    : 7.5

RedirectLocation -----
    Description: HTTP Server string location, used with http-status 301 and
                  302
    String     : https://www.elearnsecurity.com/ (from location)

Title -----
    Description: The HTML page title
```

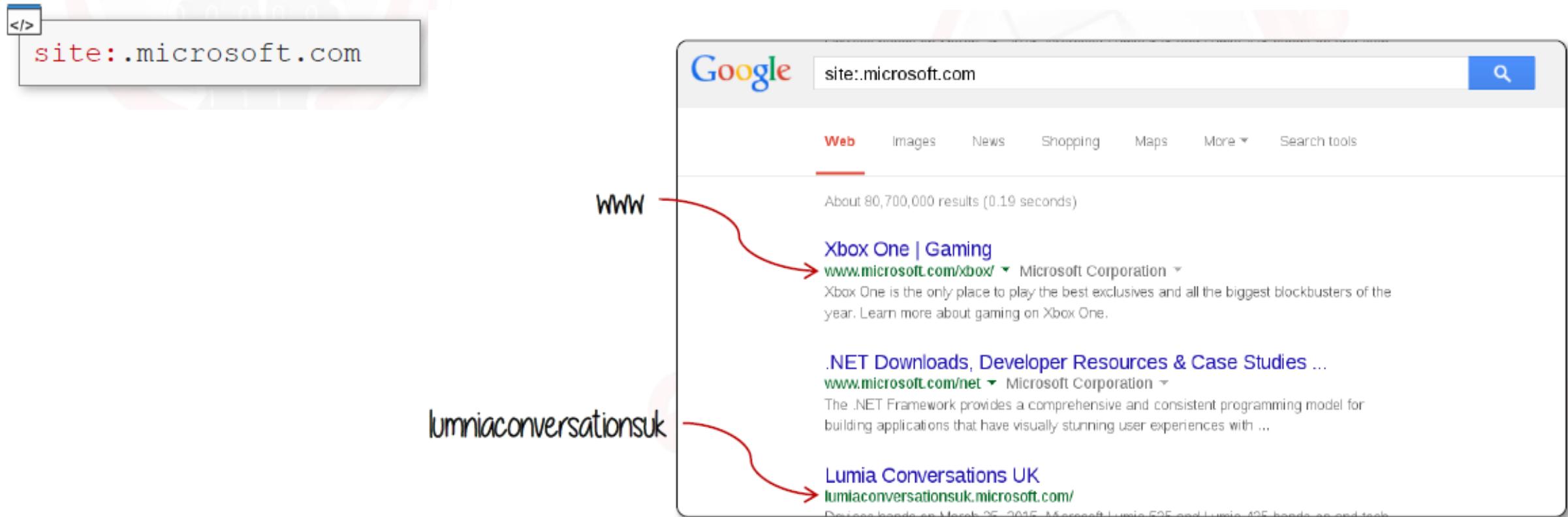
فهم أداة ال Wappalyzer

- هي إضافة في متصفح ال Firefox تستخدم لمعرفة نوع الخادم و لغات البرمجة المستخدمة و معلومات أخرى



فهم أداة الـ Google Search Operators

- هي Tools تستخدم في موقع جوجل للبحث بشكل اسرع و ادق.



فهم أداة الـ Google Search Operators (نكمله ...)

The screenshot shows two Google search results pages side-by-side. Both pages have identical headers: a top bar with 'site:.microsoft.com -inurl:www.' or 'site:.microsoft.com -site:www.microsoft.com' in a box, followed by a search bar containing the query, and a main search area with a red 'Web' tab selected and other options like Images, News, Shopping, Maps, More, and Search tools.

Left Panel (Query: site:.microsoft.com -site:www.microsoft.com):

- Web** Images News Shopping Maps More Search tools
- About 80,700,000 results (0.26 seconds)
- Cookies help us deliver our services. By using our services, you agree to our use of cookies. [Learn more](#) [Got it](#)
- PCs with the Microsoft Signature Experience - Microsoft Store**
<https://signature.microsoft.com/> ▾
Microsoft Store PCs with Signature help ensure you get the best experience with Windows 8.1. It is the cleanest PC experience with no junkware installed!H.
- Microsoft Office - Tools to Get Work Done | Sign in**
<https://office.microsoft.com/> ▾
From desktop to web for Macs and PCs, Office delivers the tools to get work done. View product information or sign in to Office 365.
- Microsoft Azure: Cloud Computing Platform & Services**
<https://azure.microsoft.com/> ▾

Right Panel (Query: site:.microsoft.com -inurl:www.):

- Web** Images News Shopping Maps More Search tools
- About 76,700,000 results (0.18 seconds)
- Microsoft Ignite - Register**
<ignite.microsoft.com/register> ▾
Full Conference Pass, All access, All breakout sessions, All social events, \$2,220. The Full Conference Pass provides access to all sessions, content, and the ...
- Guide Covering Steps to Download Candy Crush Saga ...**
<curah.microsoft.com/374817> ▾
2 days ago - Hi companions the amusement I'm offering to you down here today is the particular case that is the most addictive and clients who are playing ...
- MSDN Code Gallery - Microsoft**
<https://code.msdn.microsoft.com/> ▾
Items 1 - 10 of 8429 - Download and share sample applications, code snippets, and other resources with the developer community.

فهم أدلة الـ Google Search Operators (نكمله ...)

```
</>  
site:microsoft.com -site:subdomain1.microsoft.com  
-site:subdomain2.microsoft.com -inurl:subdomain3.microsoft.com
```

```
intitle:"Apache HTTP Server" intitle:"documentation"
```

```
intitle:"Apache HTTP Server" intitle:"documentation" site:target.com
```

فهم أداة الـ Google Search Operators (نكمله ...)

"Index of" bak

filetype:"bak"

or

filetype:"inc"

"Directory listing for" bak

فهم ال dnsrecon Tool

- هذه الاداة تستخدم للبحث عن ال SubDomains للهدف

```
dnsrecon -d microsoft.com -g
```

```
root@kali:~# dnsrecon -d microsoft.com -g
[*] Performing General Enumeration of Domain: microsoft.com
[-] DNSSEC is not configured for microsoft.com
[*]      SOA ns1.msft.net 208.84.0.53
[*]      SOA ns1.msft.net 2620:0:30::53
[*]      NS ns3.msft.net 193.221.113.53
[*]      NS ns3.msft.net 2620:0:34::53
[*]      NS ns4.msft.net 208.76.45.53
[*]      NS ns4.msft.net 2620:0:37::53
[*]      NS ns1.msft.net 208.84.0.53
[*]      NS ns1.msft.net 2620:0:30::53
[*]      NS ns2.msft.net 208.84.2.53
[*]      NS ns2.msft.net 2620:0:32::53
[*]      MX microsoft-com.mail.protection.outlook.com
[*]      CNAME www.microsoft.com toggle.www.ms.akadns.net
[*]      CNAME toggle.www.ms.akadns.net www.microsoft.com-c.edgekey.net
[*]      CNAME www.microsoft.com-c.edgekey.net www.microsoft.com-c.edgekey.net.globalredi
[*]      CNAME www.microsoft.com-c.edgekey.net.globalredir.akadns.net e10088.dspb.akamaie
[*]      A e10088.dspb.akamaiedge.net 72.247.197.45
[*]      CNAME ieonline.microsoft.com any.edge.bing.com
[*]      A any.edge.bing.com 204.79.197.200
[*]      CNAME windows.microsoft.com origin.windows.microsoft.com.akadns.net
[*]      A origin.windows.microsoft.com.akadns.net 134.170.119.140
[*]      CNAME support.microsoft.com wildcard.support.microsoft.com.edgekey.net
[*]      CNAME wildcard.support.microsoft.com.edgekey.net e10315.g.akamaiedge.net
[*]      A e10315.g.akamaiedge.net 2.17.104.63
```

فهم الـ subbrute Tool

- هذه الاداة تستخدم للبحث عن الـ SubDomains للهدف

```
root@kali:~/tools/subbrute# python subbrute.py microsoft.com
microsoft.com
www.microsoft.com
home.microsoft.com
cs.microsoft.com
my.microsoft.com
members.microsoft.com
blogs.microsoft.com
search.microsoft.com
i.microsoft.com
feeds.microsoft.com
forums.microsoft.com
math.microsoft.com
news.microsoft.com
games.microsoft.com
dev.microsoft.com
mail.microsoft.com
info.microsoft.com
music.microsoft.com
support.microsoft.com
help.microsoft.com
s.microsoft.com
e.microsoft.com
office.microsoft.com
profile.microsoft.com
member.microsoft.com
```

```
git clone https://github.com/TheRook/subbrute.git
```

```
python subbrute.py -h
```

```
python subbrute.py -h -s [path_to_file.txt]
```

فهم ال theHarvester Tool

- هذه الاداة تستخدم للبحث عن ال SubDomains للهدف

```
theharvester [options]
```

-d	Domain to search
-l	Limit the results to work with
-b	Data source (bing, google, linkedin, pgp, all,...)
-f	Output to HTML or XML file (optional - good for long lists)

```
theharvester -d microsoft.com -b google -l 200  
-f /root/Desktop/msresults.html
```

Console

```
[+] Emails found:  
-----  
oss@microsoft.com  
secure@microsoft.com  
joakim.karlen@microsoft.com  
Edvard.bergstrom@microsoft.com  
dinei@microsoft.com  
cormac@microsoft.com  
@microsoft.com  
hiballan@microsoft.com  
thomkar@microsoft.com  
antr@microsoft.com  
simonpj@microsoft.com
```

```
[+] Hosts found in search engines:  
-----  
[-] Resolving hostnames IPs...  
72.247.197.45:www.microsoft.com  
134.170.119.140:windows.microsoft.com  
168.62.198.20:commerce.microsoft.com
```

E-mails names found:

- oss@microsoft.com
- secure@microsoft.com
- joakim.karlen@microsoft.com
- Edvard.bergstrom@microsoft.com
- dinei@microsoft.com
- cormac@microsoft.com
- @microsoft.com
- hiballan@microsoft.com
- thomkar@microsoft.com
- antr@microsoft.com
- simonpj@microsoft.com

HTML

Hosts found:

- 72.247.197.45:www.microsoft.com
- 134.170.119.140:windows.microsoft.com
- 168.62.198.20:commerce.microsoft.com
- 2.17.104.63:support.microsoft.com
- 191.235.177.147:azure.microsoft.com

security professionals

```
theharvester -d elearnsecurity.com -b linkedin -l 200
```

فهم مصطلح DNS Zone Transfer

- يقصد بهذا المصطلح تمرير نسخة من قاعدة البيانات الخاصة ب DNS Server 1 إلى DNS Server 2.

```
nslookup -type=NS mydomain.com
```

```
</>
nslookup
server [NAME SERVER FOR mydomain.com]
ls -d mydomain.com
```

```

C:\>nslookup -type=NS elsfoo.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
elsfoo.com      nameserver = ns.elsfoo.com
elsfoo.com      nameserver = ns6.dnsmadeeasy.com
elsfoo.com      nameserver = ns5.dnsmadeeasy.com
elsfoo.com      nameserver = ns7.dnsmadeeasy.com

C:\>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> server ns.elsfoo.com
Default Server: ns.elsfoo.com
Address: 74.50.103.103

> ls -d elsfoo.com
[ns.elsfoo.com]
elsfoo.com.          SOA    ns.elsfoo.com bernyreed.elsfoo.com. (41 900 600 86
elsfoo.com.          NS     ns6.dnsmadeeasy.com
elsfoo.com.          NS     ns7.dnsmadeeasy.com
elsfoo.com.          NS     ns.elsfoo.com
elsfoo.com.          NS     ns5.dnsmadeeasy.com
elsfoo.com.          MX     5      alt1.aspmx.l.google.com
elsfoo.com.          MX     5      alt2.aspmx.l.google.com
elsfoo.com.          MX     10     aspmx2.googlemail.com
elsfoo.com.          MX     10     aspmx3.googlemail.com
elsfoo.com.          MX     1      aspmx.l.google.com
elsfoo.com.          TXT   "google-site-verification=omyr9Nazb1WYCs_
axvvtCjTI2EA4_S-Q"
elsfoo.com.          TXT   "v=spf1 include:_spf.google.com ~all"
ns6.dnsmadeeasy.com. A     208.80.124.13
ns7.dnsmadeeasy.com. A     208.80.126.13
ns5.dnsmadeeasy.com. A     208.94.148.13
ns5.dnsmadeeasy.com. AAAA 2600:1800:5::1
admin               A     74.50.103.103
intranet            A     74.50.103.103
ns                 A     74.50.103.103
private             A     74.50.103.103
www                A     74.50.103.103
elsfoo.com.          SOA    ns.elsfoo.com bernyreed.elsfoo.com. (41 900 600 86
>

```



```
dig @nameserver axfr mydomain.com
```

- nameserver is a nameserver for mydomain.com
- axfr is the mnemonic opcode for the DNS zone transfer.

```
root@kali:~# dig @ns.elsfoo.com AXFR elsfoo.com
```

```
; <>> DiG 9.8.4-rpz2+rl005.12-P1 <>> @ns.elsfoo.com AXFR elsfoo.com
; (1 server found)
;; global options: +cmd
elsfoo.com.          3600   IN      SOA     ns.elsfoo.com. bemyreed.elsfoo.com. 41 900 600 86400
elsfoo.com.          3600   IN      NS      ns6.dnsmadeeasy.com.
elsfoo.com.          3600   IN      NS      ns7.dnsmadeeasy.com.
elsfoo.com.          3600   IN      NS      ns.elsfoo.com.
elsfoo.com.          3600   IN      NS      ns5.dnsmadeeasy.com.
elsfoo.com.          3600   IN      MX      5 alt1.aspmx.l.google.com.
elsfoo.com.          3600   IN      MX      5 alt2.aspmx.l.google.com.
elsfoo.com.          3600   IN      MX      10 aspmx2.googlemail.com.
elsfoo.com.          3600   IN      MX      10 aspmx3.googlemail.com.
elsfoo.com.          3600   IN      MX      1 aspmx.l.google.com.
elsfoo.com.          3600   IN      TXT    "google-site-verification=omyr9NazbIWYCs_DW29VGj_zMJ."
elsfoo.com.          3600   IN      TXT    "v=spf1 include:_spf.google.com -all"
ns6.dnsmadeeasy.com. 3600   IN      A       208.80.124.13
ns7.dnsmadeeasy.com. 3600   IN      A       208.80.126.13
ns5.dnsmadeeasy.com. 3600   IN      A       208.94.148.13
ns5.dnsmadeeasy.com. 3600   IN      AAAA   2600:1800:5::1
admin.elsfoo.com.    3600   IN      A       74.50.103.103
intranet.elsfoo.com. 3600   IN      A       74.50.103.103
ns.elsfoo.com.        3600   IN      A       74.50.103.103
private.elsfoo.com.   3600   IN      A       74.50.103.103
www.elsfoo.com.       3600   IN      A       74.50.103.103
elsfoo.com.          3600   IN      SOA     ns.elsfoo.com. bemyreed.elsfoo.com. 41 900 600 86400
;; Query time: 144 msec
;; SERVER: 74.50.103.103#53(74.50.103.103)
;; WHEN: Tue Mar 31 12:01:01 2015
;; XFR size: 22 records (messages 1, bytes 800)
```

فہم ال Virtual Hosts

Virtual Hosts = Shared Hosting Environment

- حيث الخادم الذي له IP واحد يحمل أكثر من موقع / host

Here for example there are multiple virtual hosts associated to the IP address 192.168.3.2.



فهم أداة الـ Fierce

- تستخدم هذه الاداة لمعرفة ال IP address اللى على نفس ال Hosts

```
root@kali:~/tools/hostmap# fierce -dns elearnsecurity.com
DNS Servers for elearnsecurity.com:
ns1.elearnsecurity.com
ns.elearnsecurity.com
ns5.dnsmadeeasy.com
ns6.dnsmadeeasy.com
ns7.dnsmadeeasy.com

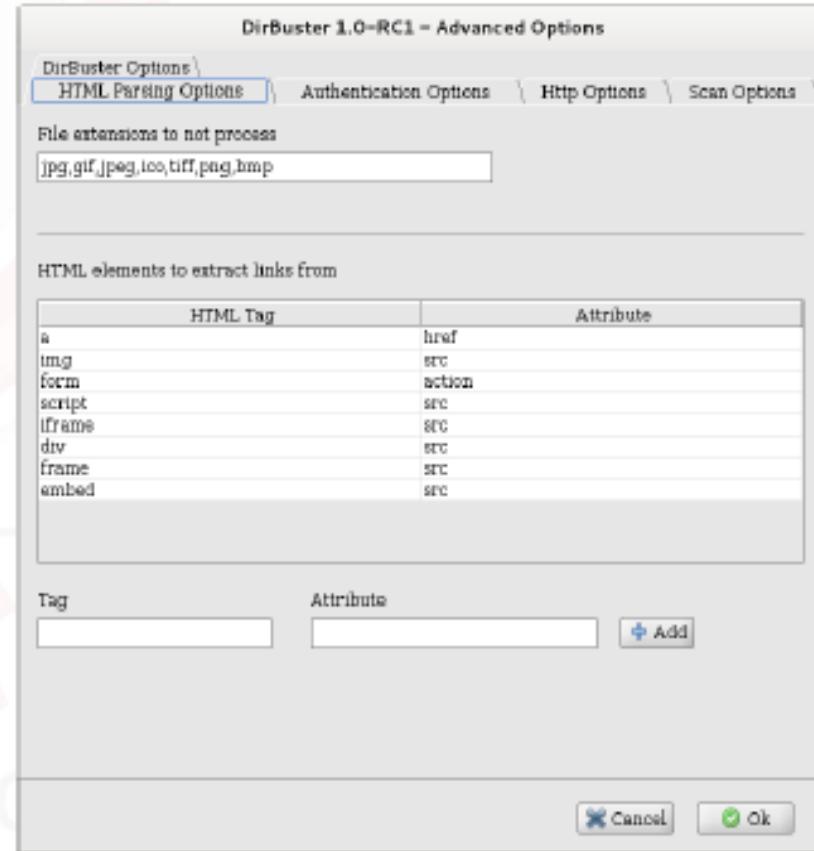
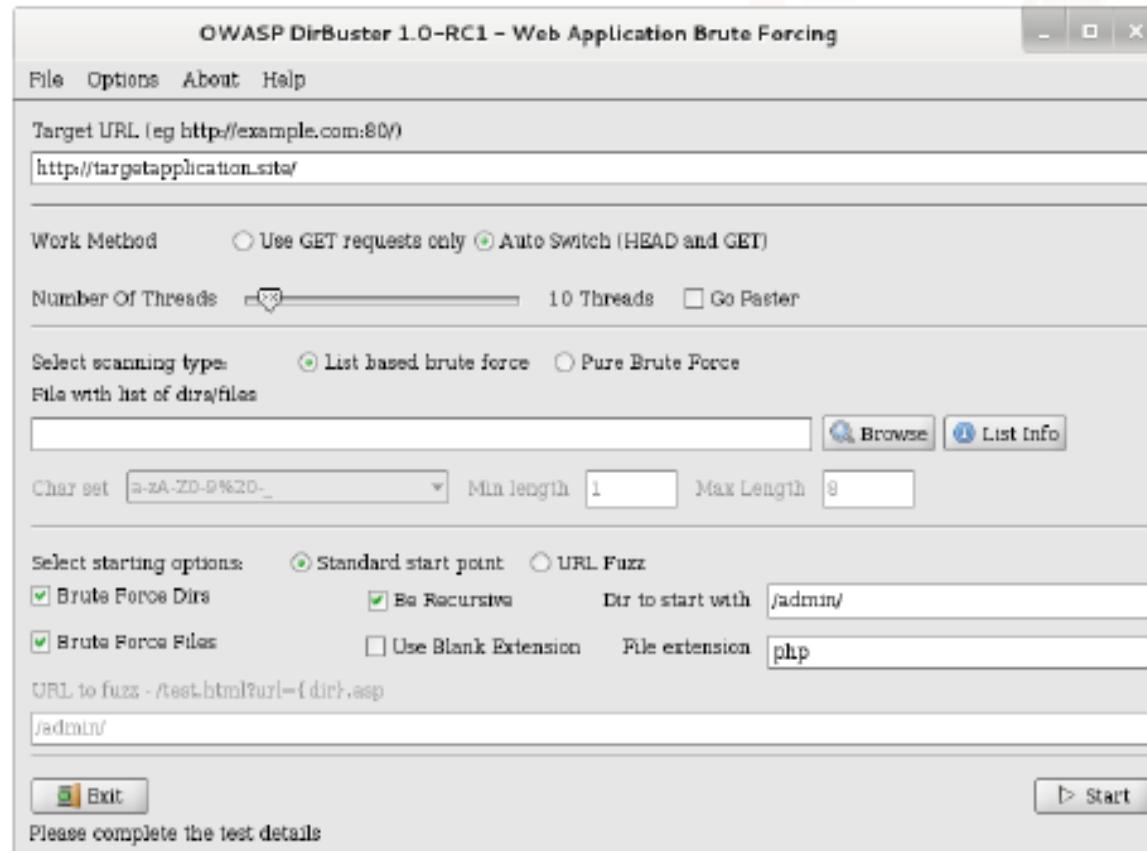
Trying zone transfer first...
Testing ns1.elearnsecurity.com
    Request timed out or transfer not allowed.
Testing ns.elearnsecurity.com
    Request timed out or transfer not allowed.
Testing ns5.dnsmadeeasy.com
    Request timed out or transfer not allowed.
Testing ns6.dnsmadeeasy.com
    Request timed out or transfer not allowed.
Testing ns7.dnsmadeeasy.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 2280 test(s)...
162.220.56.82 blog.elearnsecurity.com
162.220.56.82 community.elearnsecurity.com
199.193.116.231 lib.elearnsecurity.com
199.193.116.231 members.elearnsecurity.com
199.193.116.231 mgmt.elearnsecurity.com
199.193.116.232 ns.elearnsecurity.com
199.193.116.233 ns1.elearnsecurity.com
199.193.116.231 webmail.elearnsecurity.com
199.193.116.231 www.elearnsecurity.com
```

فهم ال DirBuster Tool

- هي أداة تستخدم لاكتشاف الملفات المخبية في الموقع.



فهم موقع Shodan HQ

- هو موقع يستخدم لجمع المعلومات عن الهدف من نوع الخادم و ال Ports المفتوحة عليه و غيرها من المعلومات الهامة.

Shodan searches includes the following protocols

- HTTP(S)
- SSH
- SNMP
- MySQL / MondoDB
- RDP
- FTP
- Telnet
- and few more

1. Find Apache servers in San Francisco:

apache city:"San Francisco"

The screenshot shows the Shodan search interface with the query "apache city:'San Francisco'" entered in the search bar. The results page displays a total of 49,771 findings. A prominent result is listed with the IP address 104.236.142.160, which is identified as belonging to Digital Ocean and located in the United States, San Francisco. The result includes a detailed view of the server's configuration, including its operating system (Ubuntu) and the Apache web server version (2.4.18). The response header indicates an HTTP/1.1 301 Moved Permanently status.

Shodan Developers Book View All...

SHODAN apache city:"San Francisco" Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
49,771

TOP COUNTRIES

104.236.142.160
Digital Ocean
Added on 2018-02-25 03:44:45 GMT
United States, San Francisco
Details

HTTP/1.1 301 Moved Permanently
Date: Sun, 25 Feb 2018 03:48:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Cache-Control: no-cache
Location: <https://www.economycontractorsupply.com/>
Content-Length: 8
Content-Type: text/html; charset=utf-8

2. Find Nginx servers in Australia:

nginx country:"AU"

SHODAN Developers Book View All... [nginx country:"AU"](#) Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS **124,512**

TOP COUNTRIES  Australia 124,512

Apache2 Debian Default Page: It works

106.167.136
88.39.0.1a8.ip4.static.si-reverse.com
SoftLayer Technologies
Added on 2018-02-25 03:49:22 GMT
 Australia, Sydney
[Details](#)

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Sun, 25 Feb 2018 03:45:16 GMT
Content-Type: text/html
Content-Length: 18781
Last-Modified: Thu, 29 Jun 2017 07:56:43 GMT
Connection: keep-alive
ETag: "5954b2bb-29cd"
Accept-Ranges: bytes

3. Find GWS (Google Web Server) servers:

"Server: gws" hostname:"google"

The screenshot shows the Shodan search interface with the query "Server: gws" and "hostname:google" entered. The results page displays a total of 88,636 findings across various countries. A world map highlights the top countries where these servers are found, with the United States and China being the most prominent. The results are presented in two main sections: one for a 302 Moved response and another for a 301 Moved response.

TOTAL RESULTS
88,636

TOP COUNTRIES

Russian Federation 12,958

302 Moved
179.98.24.153
153.g8-qqgym.google.com
GS Networks Ltda
Added on 2018-02-25 03:50:09 GMT
Brazil, Goiania
[Details](#)

HTTP/1.1 302 Found
Location: https://www.google.com.vn/?gfe_rd=cr&dcr=0&ei=ejGSwueCBo5Bo4Dh_53IAg&gws_rd=ssl
Cache-Control: private
Content-Type: text/html; charset=UTF-8
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Sun, 25 Feb 2018 03:46:03 GMT
Server: gws
[Conf...](#)

301 Moved
180.128.141.214

4. Search with CVE ID

vuln:cve-2014-0160

Shodan Developers Book View All... SHODAN vuln:cve-2014-0160 Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Like 102 Download Results Create Report

TOTAL RESULTS
113,693

TOP COUNTRIES

Country	Count
United States	29,160
China	8,394
Germany	7,383
France	5,350

37.203.96.161
BH Telecom d.d. Sarajevo
Added on 2018-02-25 03:51:23 GMT
 Bosnia and Herzegovina, Tuzla
[Details](#)
Affected by
 Heartbleed

SSL Certificate
Issued By:
- Common Name: support
- Organization: Fortinet
Issued To:
- Common Name: FGT40C3913027H4
- Organization: Fortinet

HTTP/1.1 200 OK
Date: Sun, 25 Feb 2018 03:47:17 GMT
Last-Modified: Mon, 19 Feb 2018 06:57:03 GMT
ETag: "bf6_4f_5a8a753f"
Accept-Ranges: bytes
Content-Length: 79
Content-Type: text/html
X-Frame-Options: SAMEORIGIN

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: RFC2409/Oakley Group
2

Here are some other basic filters which you can easily use with Shodan:

- **city**: find devices in a particular city
- **country**: find devices in a particular country
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

For Webcams –

- **Code:** Server: SQ-WEBCAM
- **Link** – <https://www.shodan.io/search?query=Server%3A+SQ-WEBCAM>

For Cams –

- **Code:** linux upnp avtech
- **Link** – <https://www.shodan.io/search?query=linux+upnp+avtech>

For Netcam –

- **Code:** netcam
- **Link** – <https://www.shodan.io/search?query=netcam>

For Default Passwords –

- **Code:** "default password"
- **Link** – <https://www.shodan.io/search?query=%22default+password%22>

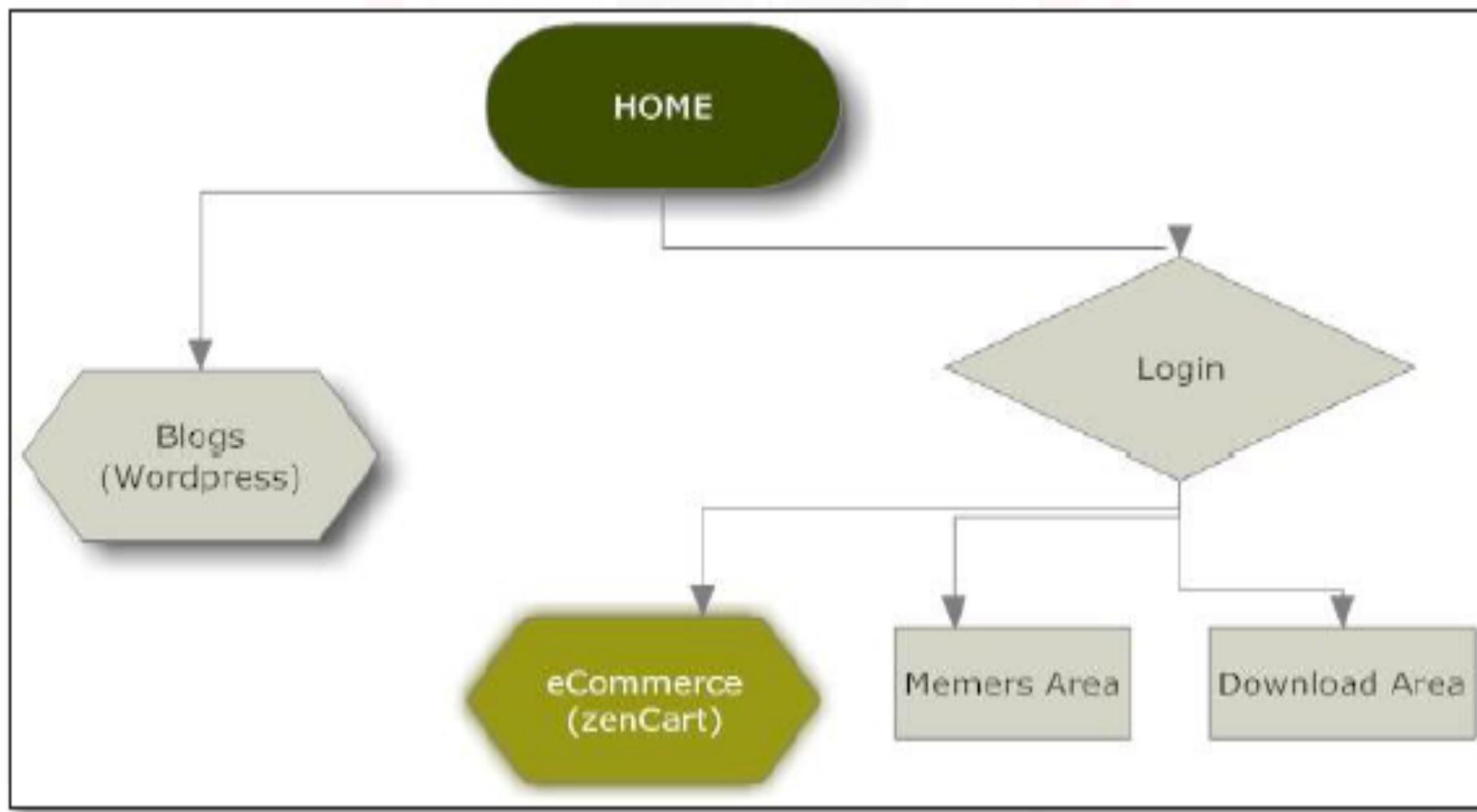
بناء لـ Functional Graph

Our first step in this case will be to consider the overall scope of the application:

- What is it for?
- Does it allow user registration?
- Does it have an administration panel?
- Does it take input from the user?
- What kind of input?
- Does it accept file uploads?
- Does it use JavaScript or Ajax or Flash? And so on.

The following questions should help guide you:

- What is the purpose of the website/web application?
 - Sell online?
 - Corporate online presence?
 - Blogging?
- What seems to be the core of the website?
 - Selling products?
 - Do they sell memberships? digital contents?
- Does it require login to perform certain actions?
- What are the main areas of the website?
 - Blogs?
 - eCommerce area?



Name:

Organization: Foo Inc.

Date:

10-10-2009

Information gathering - phase



تم بحمد الله انتهاء الفصل الاول