Module 03

Information Gathering

Footprinting and Reconnaissance

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Footprinting a Target

Footprinting is the process of accumulating data regarding a specific target, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease in which they can be exploited.

Using a combination of tools and techniques, coupled with a healthy dose of patience and mind-melding, attackers can take an unknown entity and reduce it to a specific range of domain names, network blocks, subnets, routers, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture.

Lab Scenario

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users' adherence to security policies.

Tests are typically performed using manual or automated technologies to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. Once vulnerabilities have been successfully exploited on a particular system, testers may attempt to use the compromised system to launch subsequent exploits at other internal resources, specifically by trying to incrementally achieve higher levels of security clearance and deeper access to electronic assets and information via privilege escalation.

Information about any security vulnerabilities successfully exploited through penetration testing is typically aggregated and presented to IT and network systems managers to help those professionals make strategic conclusions and prioritize related remediation efforts. The fundamental purpose of penetration testing is to measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.

Lab Objectives

The objective of the lab is to extract information concerning the target organization that includes, but is not limited to:

- IP address range and assigned IP Block of the target
- Retrieve organization information
- Does the organization allow wireless devices to connect to their networks?

- Type of remote access used, either PSTN, RDP, SSH, VPNSSL or VPN IPSec
- Is there a Help Desk service who gives support to the IT end users of the organization?
- Identify an organization's users who can disclose their personal information that can be used for social engineering attacks.

Lab Environment

This lab requires:

- **Windows 7** as host Virtual Machine
- **Kali Linux VM** as attack machine
- A Firefox web browser with Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 45 Minutes

Introduction to Information Gathering

Information gathering is essentially using the Internet to find all the information you can about the target (company and/or person) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists, etc.) methods. While conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources.
Anything you can get ahold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper ads, internal paperwork, etc. Information gathering does not require that the assessor establish contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information (e.g. tax agencies, libraries, etc.)

The information gathering section of the penetration test is important for the penetration tester. Assessments are generally limited in time and resources. Therefore, it is critical to identify points that will be most likely vulnerable, and to focus on them. Even the best tools are useless if not used appropriately and in the right place and time. That is the reason why experienced testers invest an important amount of time in information gathering.

The first phase in a security assessment is focused on collecting as much information as possible about a target application. Information Gathering is the most critical step of an application security test. The security test should aim to test as much of the code base as possible. Thus, mapping all possible paths through the code to facilitate thorough testing is paramount.
This task can be carried out in many different ways.
By using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used.

Lab Tasks

Recommended labs to assist you in footprinting:

- **Lab 1: Footprinting a Target Using Ping Utility**
- **Lab 2: Footprinting a Target Using nslookup Utility**
- **Lab 3: Google Hacking (Google Queries)**
- **Lab 4: Identifying Vulnerabilities and Information Disclosures in Search Engines using Search Diggity**
- **Lab 5: People Search Using the Spokeo Online Tool**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab 1 Footprinting a Target Using Ping Utility

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Ping Utility Overview

ping is a diagnostic tool used for verifying connectivity between two hosts on a network. It sends Internet Control Message Protocol (ICMP) echo request packets to a remote IP address and watches for ICMP responses.

ping used to be a good indicator of a machine's general ability to receive and send IP packets.

If you could ping a host, you also could make an FTP or HTTP connection. Many firewalls explicitly disallow ICMP packets on the grounds that people don't need to know what your internal network looks like and any protocol can be used to launch an attack, even ICMP.

Lab Scenario

Ping Your Network is an essential tool for managing your IP address inventory, tracking changes and determining whether IP addresses and hostnames are in use and reachable.

The lab teaches you how to:

- Use ping
- Emulate the traceroute command with ping
- Find round-trip time (RTT)
- Identify what IP addresses are available and assess the health of specific nodes.
- Identify ICMP protocol type
- Distinguish the difference between successful and unsuccessful ping attempts.

Lab Resources

To run this lab, you will need the following:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible **DNS server**
- This lab will work in the Mile2 CyberRange on **Windows Server 2008** and **Windows 7**.

Lab Duration

Time: 10 Minutes

Ping Syntax

Windows

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] nom_cible
```

Linux/Unix/BSD

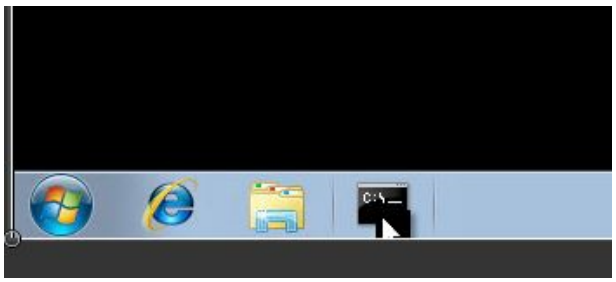
```
ping [-LRUbdfnqrvVaAB] [-c count] [-m mark] [-i interval] [-l preload]
[-p pattern] [-s packetsize] [-t ttl] [-w deadline] [-F flowlabel]
[-I interface] [-M hint] [-N nioption] [-Q tos] [-S sndbuf]
[-T timestamp option] [-W timeout] [hop ...] destination
```

Lab Tasks

Task 1
Locate IP address

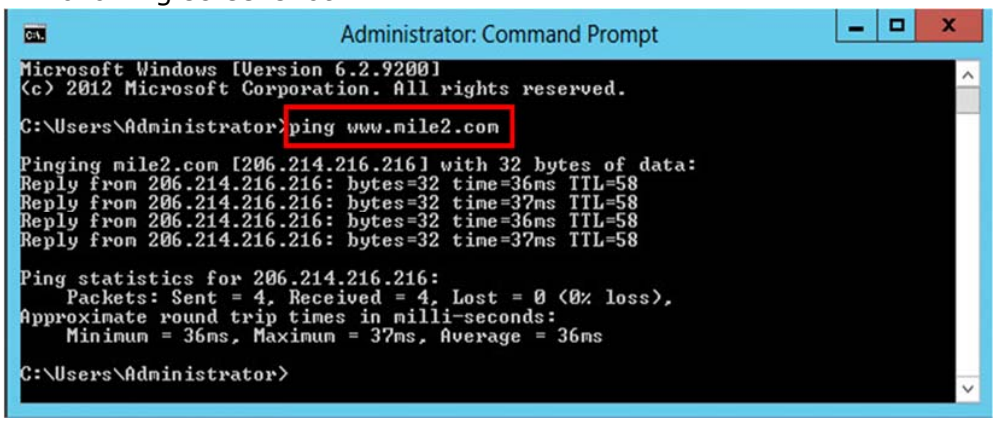
From your Windows 7 or Windows Server 2008 VM

1. Find the IP address for http://www.mile2.com
2. Click **Command Prompt** icon from the taskbar to open the command prompt window



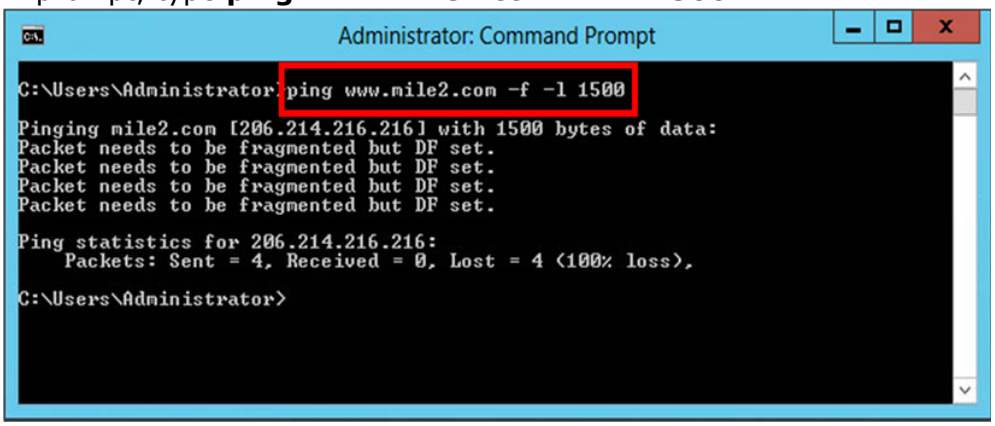
3. Type **ping www.mile2.com** in the command prompt, and press Enter to find out its IP address

4. The displayed response should be similar to the one shown in the following screenshot



The ping command to extract the IP address for www.mile2.com

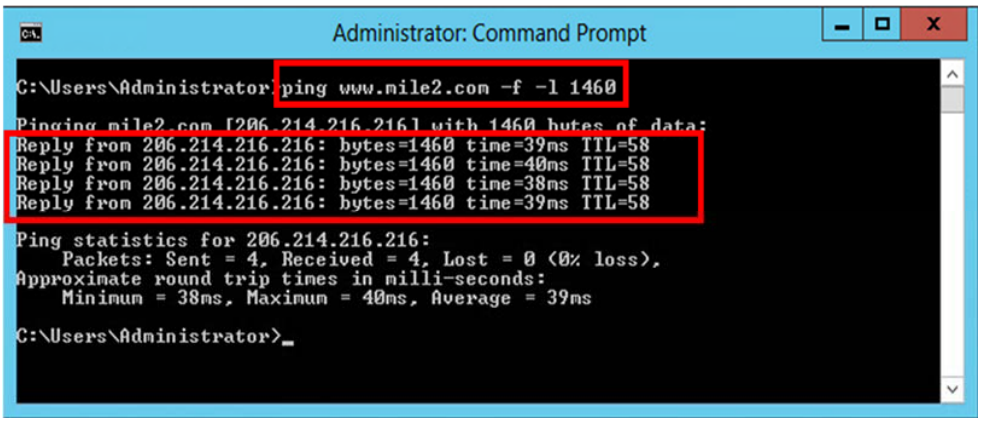
5. You receive the IP address of www.mile2.com that is **206.214.216.216**
6. You also get information in **Ping Statistics**, such as packets sent, packets received, packets lost, and **Approximate round-trip time**
7. Now, find out the maximum frame size in the network. In the command prompt, type **ping www.mile2.com -f -l 1500**



The ping command for www.mile2.com with –f –l 1500 options

8. The display **packet needs to be fragmented but DF set** means that the frame is too large to be on the network and needs to be fragmented. Since we used -f switch with the ping command, the packet was sent, and the ping command returned this error.
9. Type **ping www.mile2.com - f - l 1460**

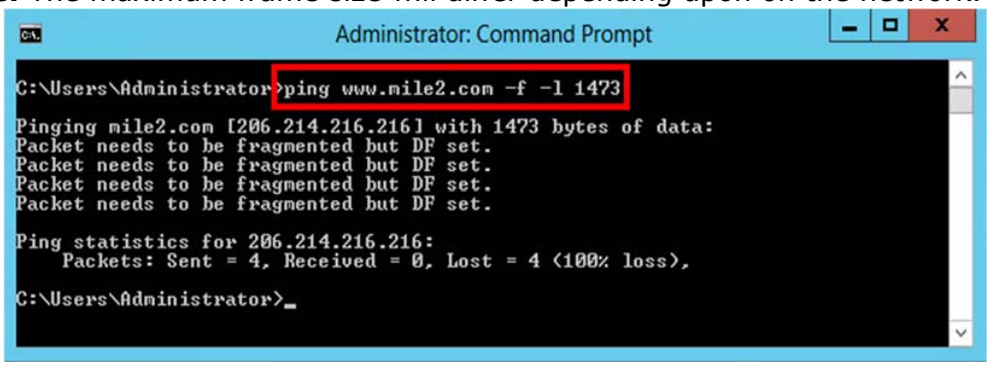
Task 2
Finding Maximum Frame Size



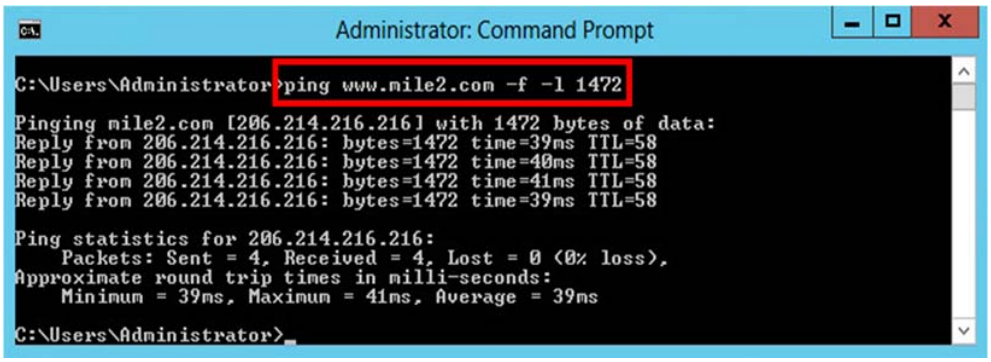
The ping command for www.mile2.com with –f –l 1460 options

10. You can see that the maximum packet size is **less than 1500 bytes and more than 1300 bytes**
11. Now, try different values until you find the maximum frame size. For instance, **ping www.mile2.com -f -l 1473** replies with **Packet needs to be fragmented but DF set** and **ping www.mile2.com -f -l 1472** replies with a **successful ping**. It indicates that 1472 bytes is the maximum frame size on this machine network

Note: The maximum frame size will differ depending upon on the network.



The ping command for www.mile2.com with –f –l 1473 options



The ping command for www.mile2.com with –f –l 1472 options

The router discards packets when TTL reaches 0 value.

12. Now, find out what happens when **TTL (Time to Live) expires**. Every packet in the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the loss of packets.
13. In the command prompt, type ping **www.mile2.com -i 3**. The displayed **response** should be similar to the one shown in the following figure, but with a different IP address.

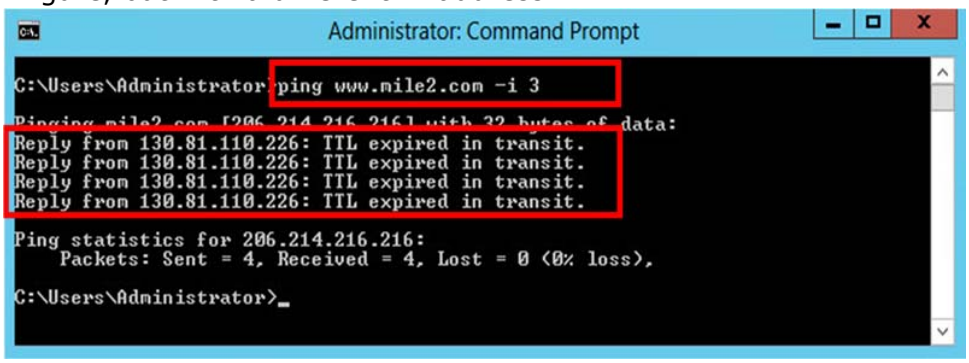


Figure: 1.9- The ping command for www.mile2.com with –i 3 options

14. **Reply from 130.81.110.226: TTL expired in transit** means that the router (130.81.110.226, students will have some other IP address) discarded the frame, because its TTL has expired (reached 0)
15. **Emulate traceroute** command, using **ping - manually**, found the route from your PC to **www.mile2.com**
16. The results you receive are different from those in this lab. Your results may also be different from those of the person sitting next to you.
17. In the command prompt, type **ping www.mile2.com –i 1 -n 1** (Use –n 1 in order to produce only one answer, instead of receiving four answers on Windows or pinging forever on Linux.) The displayed response should be similar to the one shown in the following figure.

Task 3
Emulate Tracert
Note: IP address varies

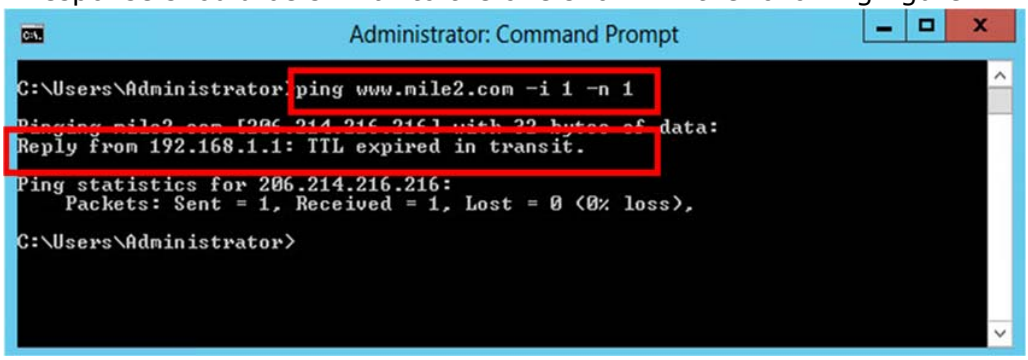


Figure: 1.10- The ping command for www.mile2.com with –i 1 –n 1 options

In the ping command, the –i option means time to live TTL.

This option sets the Time to Live (TTL) value, the maximum of which is 255.

18. We have received the answer from the same IP address in **step one**. This one identifies a firewall or a router. Some firewalls **do not decrement TTL** and are therefore **invisible**.

In the ping command, -t means to ping the specified host until stopped.

Using this option will ping the *target* until you force it to stop using Ctrl-C.

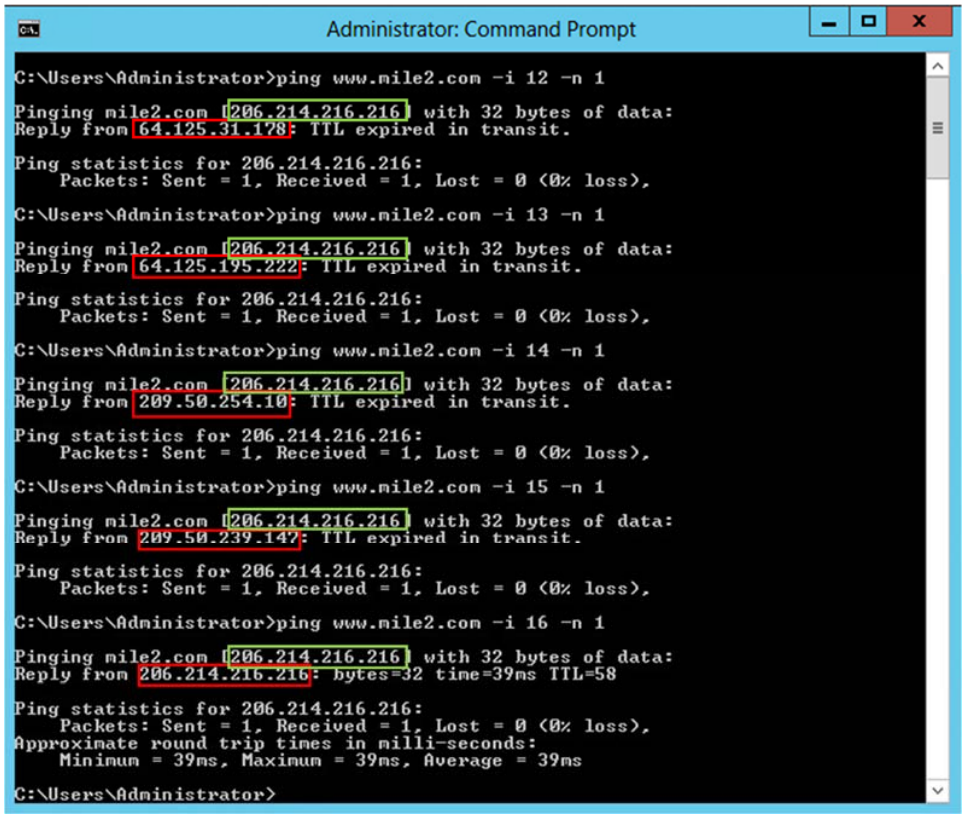


Figure: 1.11- The ping command for www.mile2.com with –i 16 –n 1 options

19. Now, make a note of all the IP addresses from which you receive the reply during the ping to emulate tracert.

Lab Analysis

Document all the IP addresses, reply request IP addresses, and their TTLs.

Tool/Utility	Information Collected/Objectives Achieved
Ping Utility	IP Address: _____ _____ Packet Statistics • Packets Sent:_____ • Packets Received:_____ • Packets Lost:_____ • Approximate RTT:_____ _____ Maximum Frame Size:_____ TTL Response:_____

Quiz

1. **Which of the following tools is designed to test connectivity between two systems by sending an ICMP echo request and waiting for an ICMP?**
   a. ipconfig
   b. netstat
   c. ping
   d. nslookup

2. **Which of the following tools provides a list of network hops between two systems?**
   a. nslookup
   b. ipconfig
   c. ping
   d. traceroute (or tracert)

3. **Which of the following Linux/UNIX command-line tools combines the features of both ping and traceroute?**
   a. ifconfig
   b. netstat
   c. mtr
   d. nbtstat

4. **Which of the following switches would you use with the netstat command to view a system's routing table?**
   a. -s
   b. -a
   c. -e
   d. -r

5. **Which of the following switches would you use with the netstat command to view a system's protocol statistics?**
   a. -s
   b. -a
   c. -e
   d. -r

6. **Which of the following tools would you use to display the TCP/IP configuration for the installed NICs on a Windows system?**
   a. ifconfig
   b. ipconfig
   c. netstat
   d. traceroute

7. Which of the following tools would you use to display the TCP/IP configuration for the installed NICs on a Linux/UNIX system?

a. ipconfig
b. netstat
c. tracerout
d. ifconfig

8. Entering the nslookup command and a server name returns which of the following?

a. Host name of the DNS server that performed the resolution
b. IP address of the DNS server that performed the resolution
c. IP address of the server name entered
d. All of the above

9. Which of the following Linux/UNIX commands can be used to determine a remote system's host name from its IP address?

a. host
b. ping
c. ipconfig
d. netstat

10. Which of the following tools would you use to review and modify a host's address resolution protocol table?

a. netstat
b. nbtstat
c. arp
d. mtr

Answers

1. ping
2. traceroute (or tracert)
3. mtr
4. -r
5. -s
6. ipconfig
7. ifconfig
8. All of the above
9. host
10. arp

Lab 2

Footprinting a Target Using nslookup Tool

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

nslookup Utility Overview

nslookup means name server lookup.
nslookup is useful for checking to see if certain subdomains exist on your domain name, such as ftp.<your domain name> or www.<your domain name>.
It can also be used to check multiple MX (email) records to ensure email is getting routed correctly.
nsLookup is also a useful tool if a domain name is not pointing to our name servers, as you can gain DNS information without the need to contact the owner of the name servers.
The nslookup tool is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line.
In its most basic operation, the nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

Lab Scenario

In the **ping** lab, we gathered information such as IP address, Ping Statistics, Maximum Transmit Unit size and TTL Response using the **ping** utility. Using the IP address found, a Penetration Testing Engineer can perform further findings like port scanning, services, OS detection, and can find the location in which the IP is located and the domain name associated with it.

The next step of reconnaissance is to find the DNS records. You need to find if DNS servers are split into internal and external. Using the nslookup tool, a Penetration Testing Engineer can obtain the IP address of the domain name allowing him or her to find the specific IP address of the person he or she is hoping to target.

There is no way to restrict other users to query with public DNS servers by using the **nslookup** command because this program will simulate the process of how other programs do the DNS name resolution. Being a Penetration Testing Engineer you should be able to prevent such attacks by going into the zone's properties and not allowing zone transfers. You also need to split DNS servers into internal and external. This will prevent an attacker from using the nslookup command to get a list of your zone's records; nslookup can provide you with a wealth of DNS server diagnostic information.

This lab will teach you how to:

- Use nslookup command
- Find the IP address of a machine
- Change the server you want the response from
- Obtain an authoritative answer from the DNS server
- Find name servers for a domain
- Find CNAME (Canonical Name) for a domain
- Find mail servers for a domain
- Identify various DNS resource records

Lab Resources

To run this lab, you will need the following:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible **DNS server**
- This lab will work in the Mile2 CyberRange on **Windows Server 2008** and **Windows Server 7**.

Lab Duration

Time: 5 Minutes

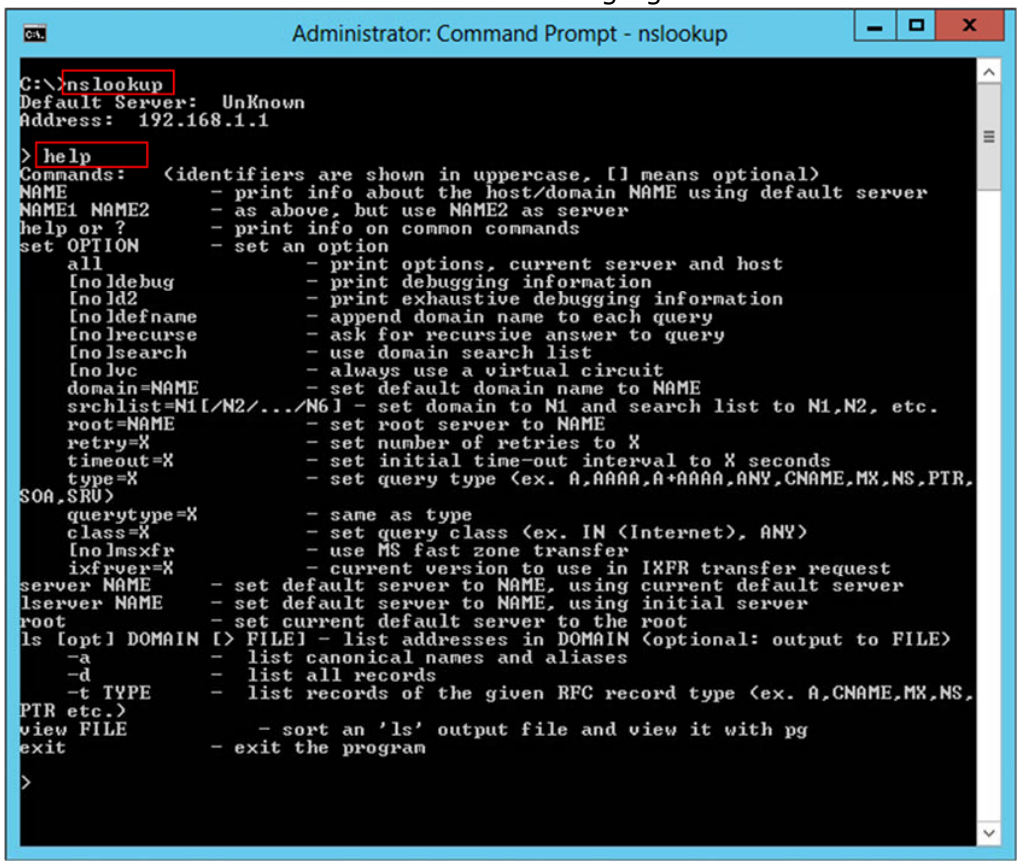
Task 1

Extract Information

1. Click the **Command Prompt** icon on the taskbar to open the command prompt window.

The nslookup command syntax is:
nslookup [-option] [name | -] [server].

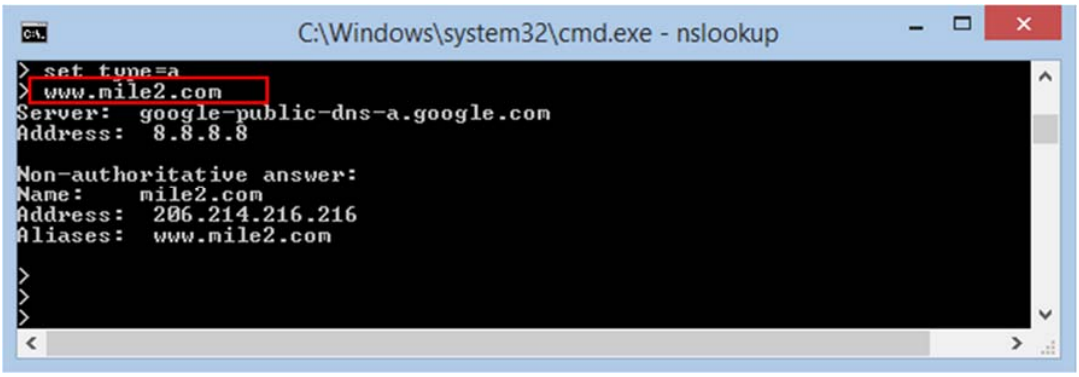
2. In the command prompt, type **nslookup**, and press **Enter**
3. Now, type **help** and press **Enter**. The displayed response should be similar to the one shown in the following figure:



The nslookup command with help option

Typing "help" or "?" at the command prompt generates a list of available commands.

4. In the **nslookup interactive mode**, type "**set type=a**" and press **Enter**
5. Now, type **www.mile2.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure:

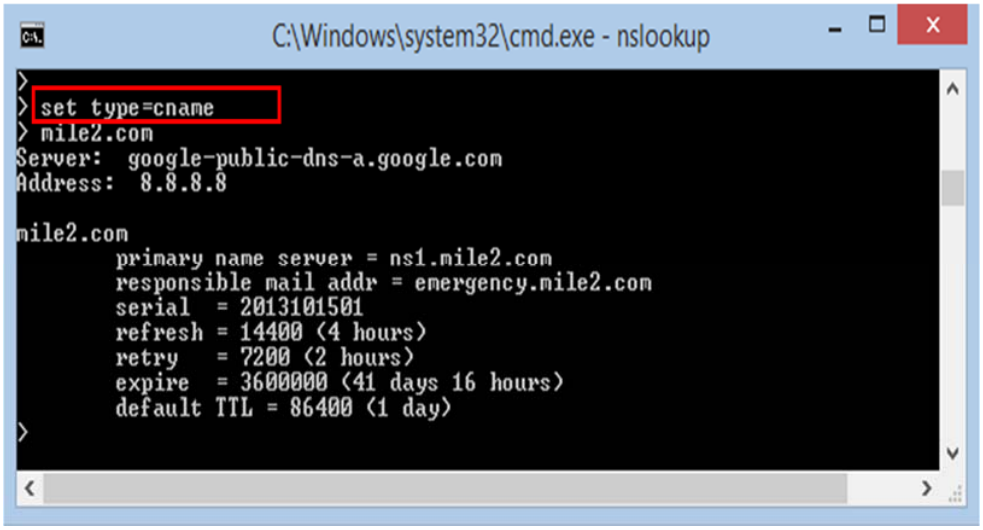


In nslookup command, set type=a option

Task 2

Use Elicit Authoritative

6. You get Authoritative or Non-authoritative answer. The answer varies, but in this lab, it is Non-authoritative answer
7. In nslookup interactive mode, type set type=cname and press Enter
8. Now, type mile2.com and press Enter
   Note: The DNS server address (8 .8 .8 .8) will be different than the one in the screenshot.f
9. The displayed response should be similar to the one shown as follows:
   >set type=cname
   > mile2.com
   Server: *google-public-dns-a.google.com*
   Address: *8. 8.8. 8*



In nslookup command, set type=cname option

Task 3

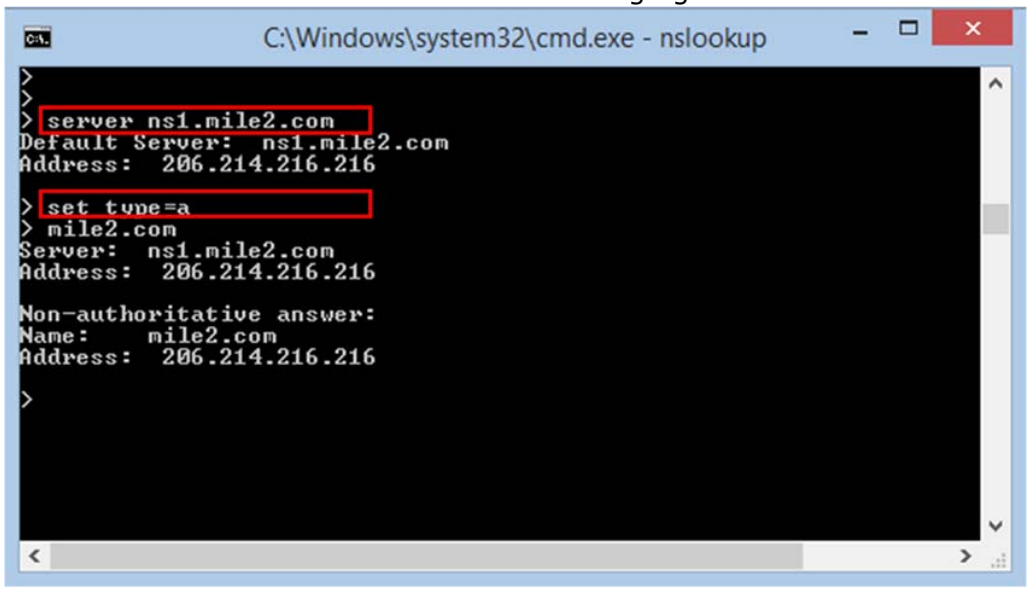
Find CNAME

10. In nslookup interactive mode, type **server ns1.mile2.com** and press Enter. Type Exit to get back to the command prompt.

In nslookup command, root=NAME option means to set the current default server to the root NAME.

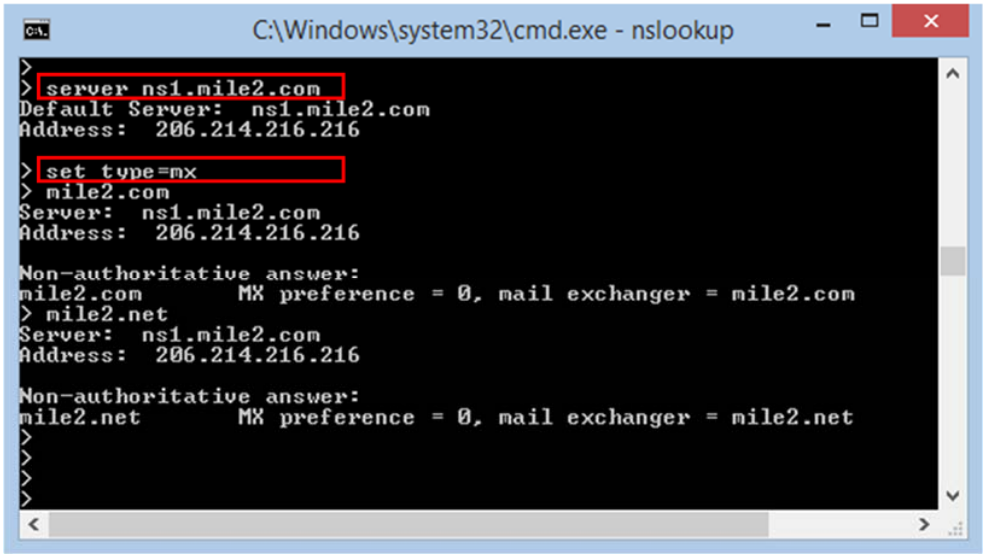
The configuration options of NSLOOKUP determine the operation and results of your name server queries. These options can be specified in command-mode queries, interactive-mode queries, or in the user_id.NSLOOKUP.ENV data set. When you include NSLOOKUP options with the initial NSLOOKUP command the (-) operand must immediately precede the option. If you specify NSLOOKUP options while in interactive mode, the SET subcommand must precede the option. Specifying NSLOOKUP options in the user_id.NSLOOKUP.ENV data set is optional. Use the SET subcommand before the option if you want to reset the option value. The (-) operand is not valid preceding options in the user_id.NSLOOKUP.ENV data set.

11. Now, type set type=a and press Enter.
12. Type www.mile2.com and press Enter. The displayed response should be similar to the one shown in the following figure.



In nslookup command, set type=a option

13. If you receive a request timed out message, as shown in the previous figure, then your firewall is preventing you from sending DNS queries outside your LAN.
14. In nslookup interactive mode, type set type=mx and press Enter.
15. Now, type mile2.com and press Enter. The displayed response should be similar to the one shown in the following figure.



In nslookup command, set type=mx option

Lab Analysis

Document all **NSlookup** findings: IP addresses, DNS server names, and other DNS information.

Tool/Utility	Information Collected/Objectives Achieved
Nslookup	**DNS Server Name:** 8.8.8.8 **Non-Authoritative Answer:** 206.214.216.216 **CNAME (Canonical Name of an alias)** • **Alias:** ns1.mile2.com • **Canonical name:** google-public-dns-a.google.com **MX (Mail Exchanger):** mile2.com

Lab 3 Google Hacking Tools - Google Queries

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Google Hacking Overview

Google.com is undoubtedly the most popular search engine in the world. It offers multiple search features like the ability to search images and news groups. However, its true power lies in its powerful commands that can be used and misused.

This technique focuses on using specific targeted expressions to query the Google databases to harvest information about people and organizations.

Google Hacking makes extensive use of advanced operators and linked options to create targeted queries that can be run in the Google search engine. Many times, the searches will be targeted at assembly information about specific technologies such as web management services while other searches will target user credentials.

Lab Scenario

1. This section is to gather information about Mile2 or other sites of interest and use various Google Queries. To do this the Google Hacking Database on www.exploit-db.com should be explored as well as trying out the many google queries.

Lab Resources

To run this lab, you will need the following:

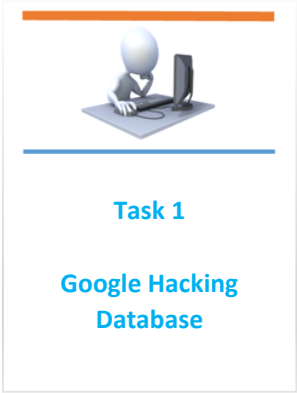
- Kali Linux VM or any Windows VM.

Lab Duration

Time: 5 Minutes

Lab Tasks

1. We are now going to learn how to use some of the advanced Google queries.



Task 1

Google Hacking Database

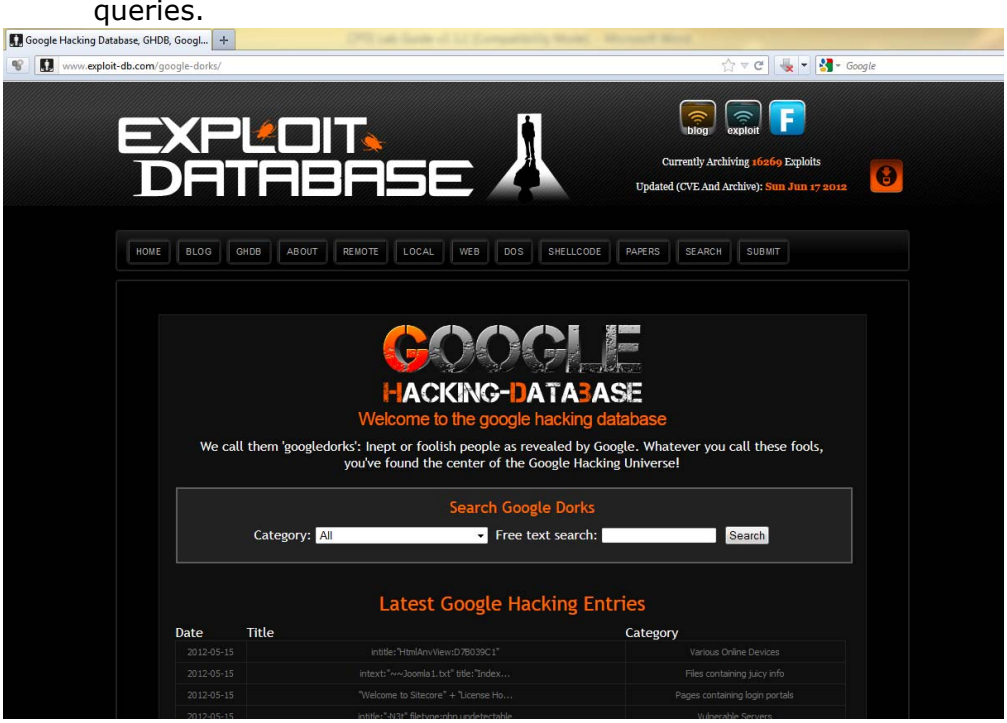


Figure 3.1 - http://www.exploit-db.com/google-dorks/

Task 2

Advanced Operators at a Glance

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Figure 3.2 – Google search Advanced Operators

Task 3

Google Queries

2. Practice utilizing the following Google Queries.
   a. The "allinurl" command is used to search for a particular string present in the URL.
   Go to google.com and type this in the search box:

   allinurl: Mile2 Faq

   The command searched for Mile2 with pages containing FAQ sections.

   b. You can also search particular top level domains like .net /.org /.np /.jp /.in /.gr etc.
   Go to google.com and type this in the search box:

   allinurl:config.txt site:jp
   allinurl:admin.txt site:edu

3. We are now going to practice searching for Index browsing enabled directories. This is a very simple but powerful way of gaining information. First of all, we need to understand that "index browsing" enabled directories are those directories on the Internet that can be browsed just like ordinary directories. We will be using Google to find these types of "interesting" directories.
   a. Go to google.com and type this in the search box:

   "Index of /admin"
   "Index of /secret"
   "Index of /cgi-bin" site:.edu
   (Try With& without the period for edu)

   Note: You can begin to think outside the box and be creative and think of other interesting ways to exploit index browsing.

4. Now, we are going to practice searching for particular file types. You can specify the extension of the filename you want to search for using the "filetype" command.
   a. Go to google.com and type this in the search box:

   filetype:pdf site:com contactlist
   filetype:doc site:mil classified

5. This document is only meant to give some basic ideas about exploiting google.com.
   a. This site is also very helpful.

   http://www.searchlore.org

6. Here are examples of advanced Google searches.
    a. Web Servers Default Installation for servers with default installation:
        i. IIS Query

“The web server designed for Windows NT server”

        ii. Apache Queries

“It Worked!"
“Test Page for Apache Installation on Web Site”

        iii. Password Files Disclosure Queries

inurl:password.txt
allinurl:passwd.txt site: website name
"index of /" + passwd.txt
“index of /" +users.pwd +authors.pwd +administrators.pwd

        iv. Bulletin Board System Password File Disclosure Query

allinurl:/wwwboard/passwd.txt

        v. HTTP Credentials Disclosure Query

http://admin:*@www

        vi. Sensitive Files Access Query

Query: allinurl:/.bash_history

        vii. Sensitive Directories Access Queries

"index of /members" + "Parent Directory"
"index of /private" + "Parent Directory"
"index of /admin" + "Parent Directory"

        viii. Microsoft Outlook Web Access Anonymous Logon Query

inurl:exchange/root.asp?acs=anon

        ix. Confidential Information’s Leak Queries

"Do not distribute"
"Internal use only"
"Internal use only" filetype:pdf

        x. Proxy and Terminal (RDP) servers Queries

inurl:8080
inurl:tsweb site:edu

Lab 4 Automated Vulnerabilities Search using Search Diggity

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Search Diggity Overview

SearchDiggity 3.1 is the primary attack tool of the Google Hacking Diggity Project. It is Bishop Fox's MS Windows GUI application that serves as a front-end to the most recent versions of the Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Lab Scenario

Before attacking any website, it's critical to do good reconnaissance. A few minutes of recon can save you hours on a hack. Simply trying various attacks without first finding out which attacks the site is vulnerable to is pure foolishness.

Google Hacks is a compilation of carefully crafted Google searches that expose novel functionality from Google's search and map services. For example, you can use it to view a timeline of your search results, view a map, search for music, search for books, and perform many other specific kinds of searches. You can also use this program to use google as a proxy.

The objective of this lab is to demonstrate how to identity vulnerabilities and information disclosures in search engines using Search Diggity. You will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Lab Resources

To carry out the lab, you need:

- Search Diggity located on Desktop
  This lab will work on the Mile2 CPTE Cyber Range – **Windows 7**

Lab Duration

Time: 10 Minutes

Lab Tasks

Use Windows 7 VM

1. On the Desktop, click the Search Diggity icon.

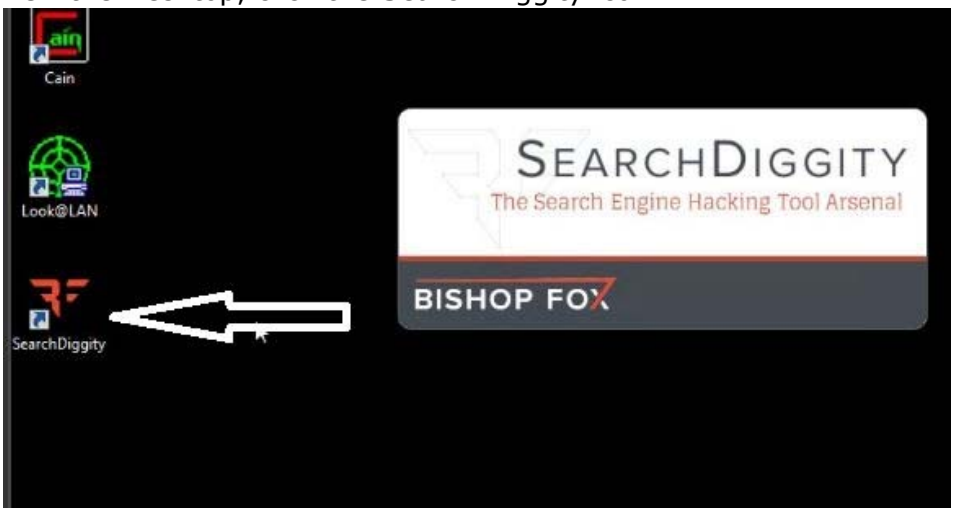
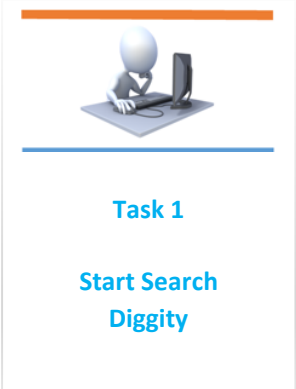


Figure: 4.1 - Windows Server 2012 - Start Menu



Task 1

Start Search Diggity

2. The Search Diggity main window appears with Google Diggity as the Default.

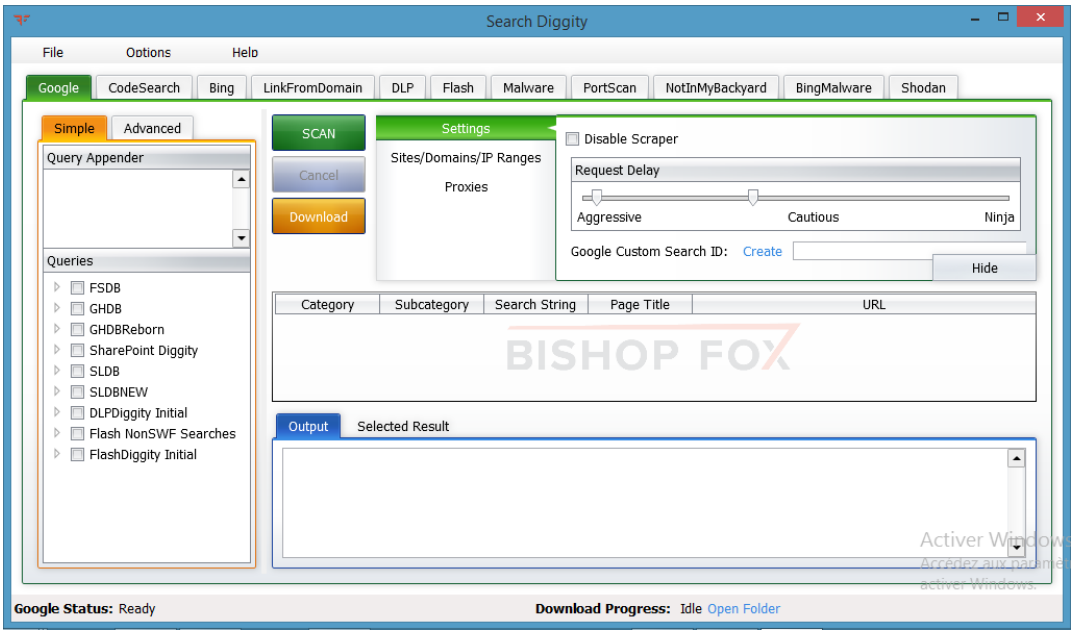


Figure: 4.2 - Search Diggity - Main window

Queries — Select Google Dorks (search queries) to use in scan by checking appropriate boxes.

3. Select Sites/Domains/IP Ranges and type the domain name in the domain field. Click Add.

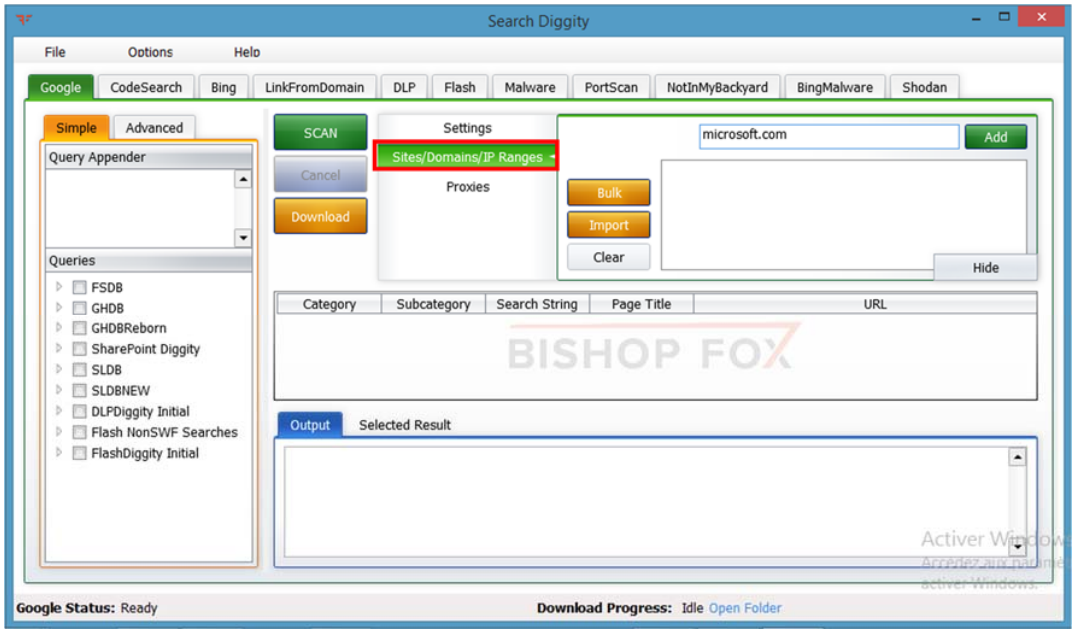


Figure: 4.3 - Search Diggity - Selecting Sites/Domains/IP Ranges

Download_Button - Select (highlight) one or more results in the results pain, then click this button to download the search result files locally to your computer. By default, downloads to C:\Diggity Download

Import Button - Import a text file list of domains/IP ranges to scan. Each query will be run against Google with site: your domain name.com appended to it.

4. The added domain name will be listed in the box below the Domain held

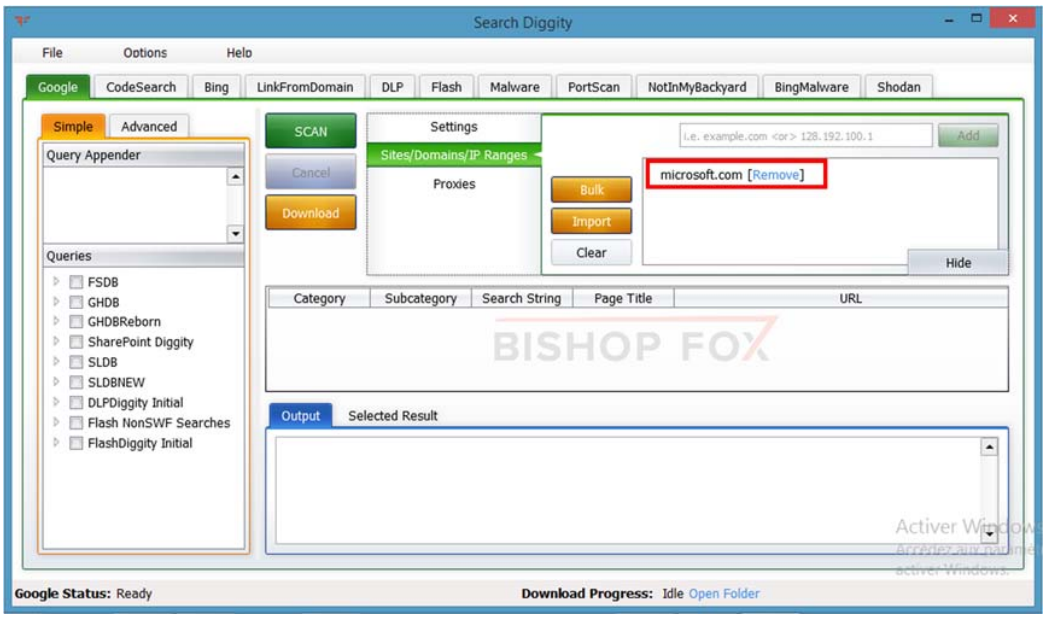


Figure: 4.4 - Search Diggity – Domain Added

5. Now, select a Query from the left pane that you wish to run against the website that you have added in the list and click Scan

Task 2

Run Query against a website

Note: In this lab, we have selected the query SWF Finding Generic. Similarly, you can select other queries to run against the added website.

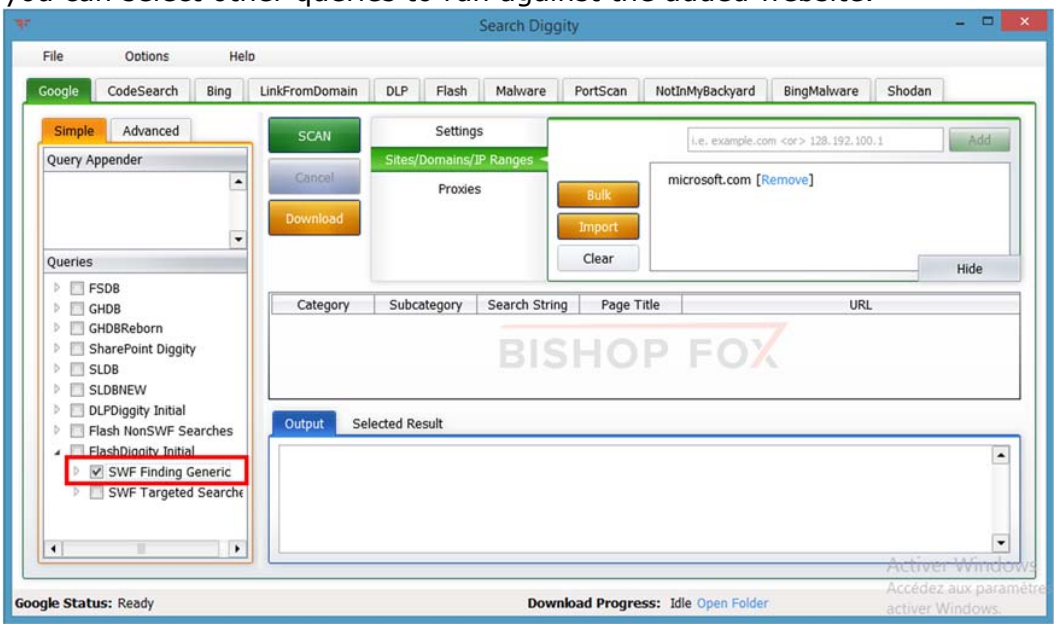


Figure: 4.5 - Search Diggity - Selecting query and Scanning

When scanning is kicked off, the selected query is run against the complete website.

Simple — Simple search text box will allow you to run one simple query at a time, instead of using the Queries checkbox dictionaries.

Note: Search Diggity will almost always trigger google bot detection which will delay further scanning for 15 minutes. If that happens start the scan and move on to the next lab, then come back to check the results.

6. The following screenshot shows the scanning process

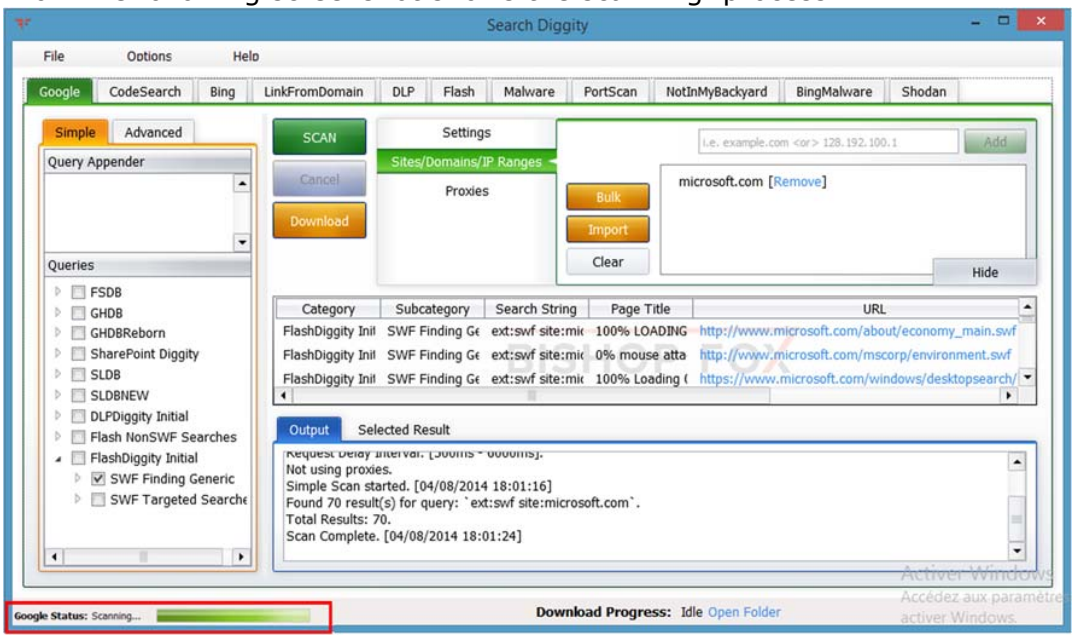


Figure: 4.6 - Search Diggity – Scanning Process

Output - General output describing the progress of the scan and parameters used.

7. All the URLs that contain the SWF extensions will be listed and the output will show the query results

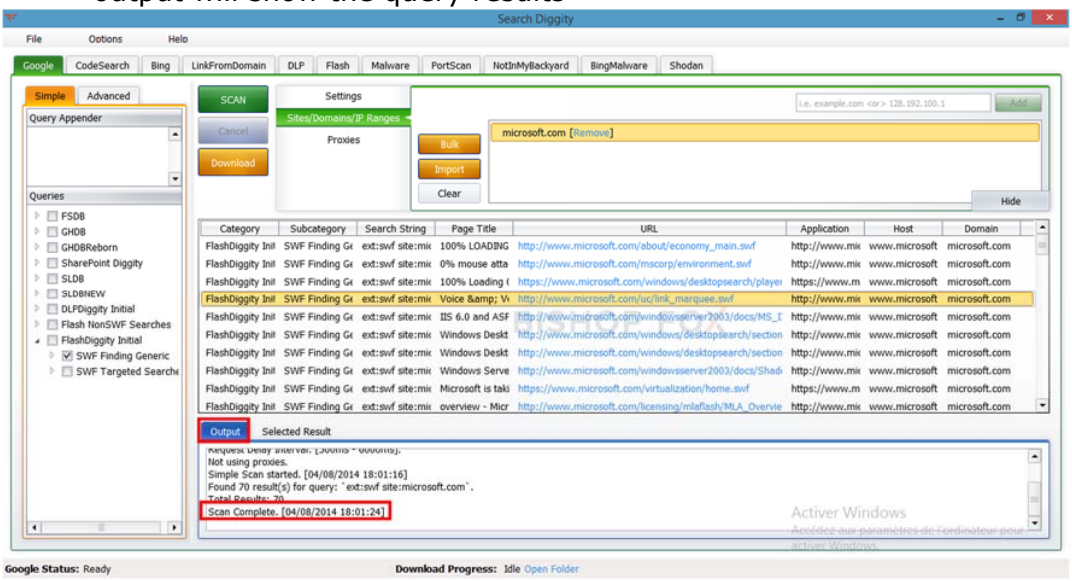


Figure: 4.7 - Search Diggity - Output window

Note: SWF is Shockwave Flash Format

Lab Analysis

Retrieve all results to determine the vulnerabilities and note the information disclosed about the website.

Tool/Utility	Information Collected/Objectives Achieved
Search Diggity	Many error messages found relating to vulnerabilities Results returned by Google Diggity

Lab 5

People Search Using the Spokeo Online Tool

ICON KEY

Important Information

Quiz

CPTE Labs

Course Review

Spokeo Overview

Spokeo is a people search website that aggregates data from many online and offline sources (such as phone directories, social networks, photo albums, marketing surveys, mailing lists, government censuses, real estate listings, and business websites). This aggregated data has, in the past, included demographic data, social profiles, and estimated property and wealth values.

Lab Scenario

A Penetration Testing Engineer must collect all possible information about a Target before beginning the test. There are many tools available, which can be used to gather information on people, employees, and organizations to conduct a penetration test. In this lab, you will learn to use the Spokeo online tool to collect confidential information of key persons in an organization.

The objective of this lab is to demonstrate the footprinting techniques to collect people's information using people search services. Students need to perform a people search using http://www.spokeo.com.

Lab Resources

In the lab, you will need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the Mile2 Cyber Range - on Windows 7

Lab Duration

Time: 5 Minutes

Lab Tasks

Use Windows 7 VM

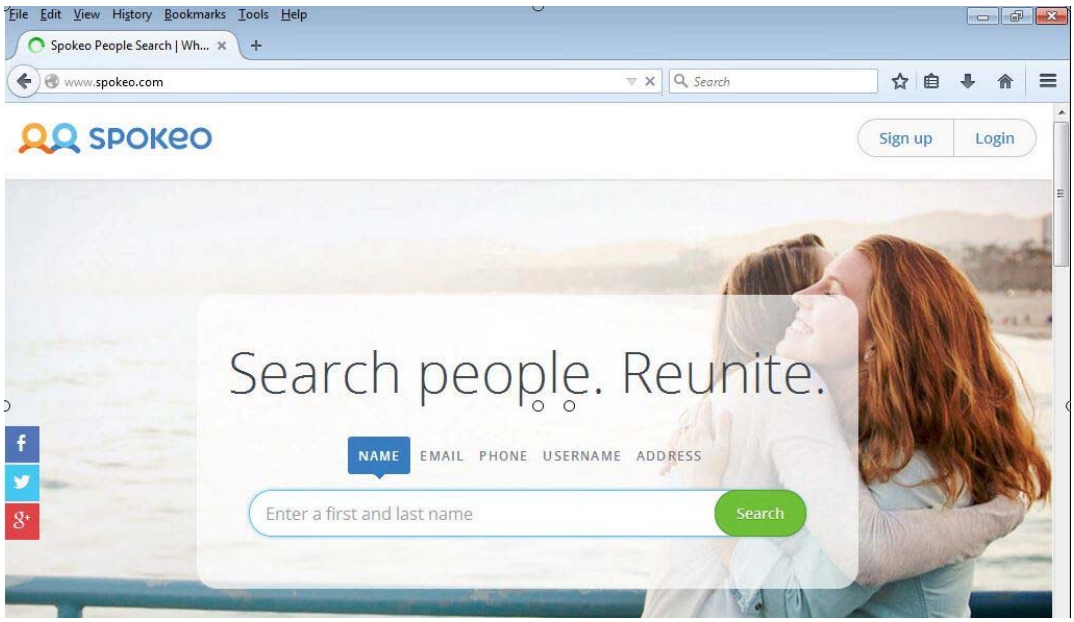
Task 1

People Search with Spokeo

1. Click the Firefox icon on the taskbar to launch the Firefox browser

2. Open a web browser, type http://www.spokeo.com, and press Enter on the keyboard.

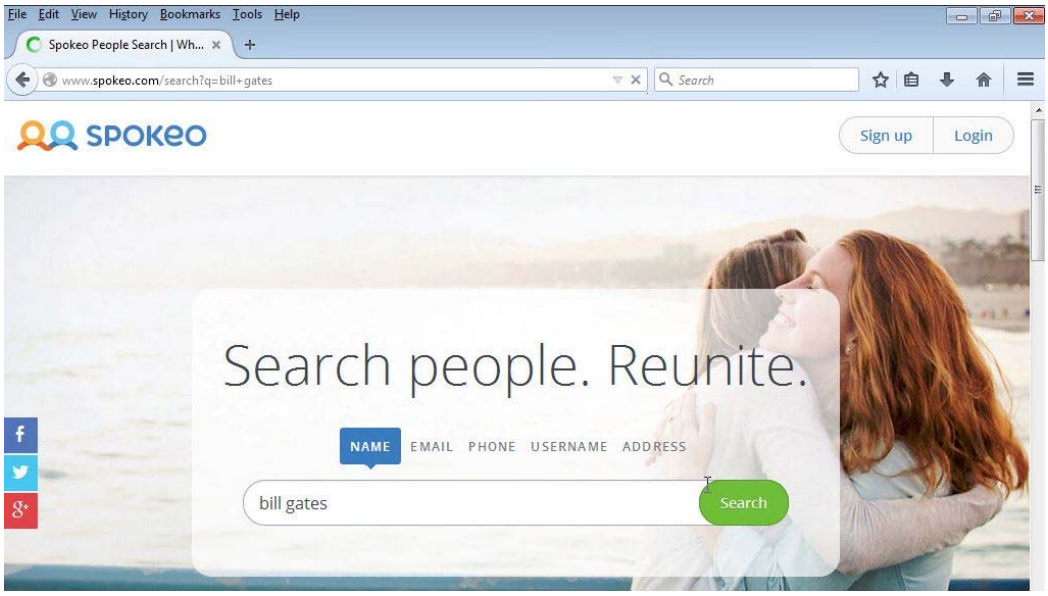
According to the site, Spokeo does not originate data and the information available is only as good as its source.



Spokeo utilizes deep web crawlers to aggregate data.

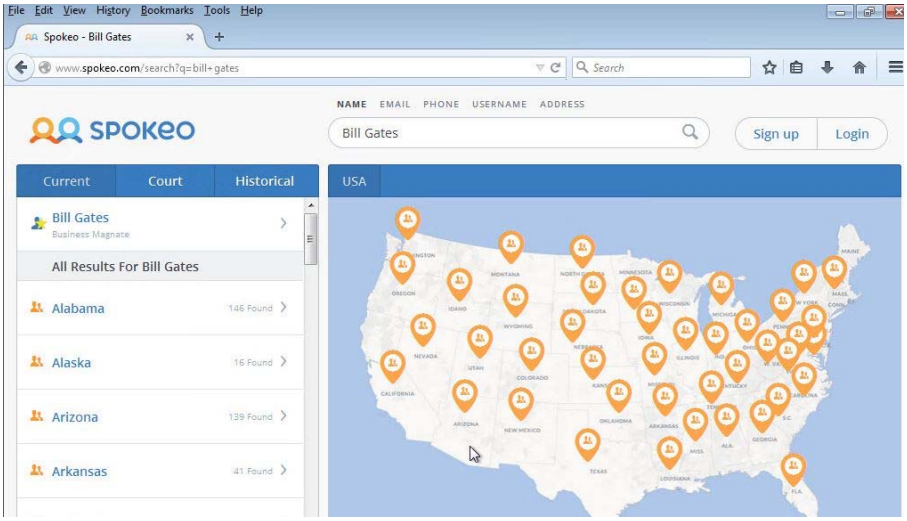
Searches for people can be made from a name, email, phone number, username or address, though the number of searches per month are limited for searches other than those by name.

3. To begin the search, input the name of the person you want to search for in the Name field and click **Search.**

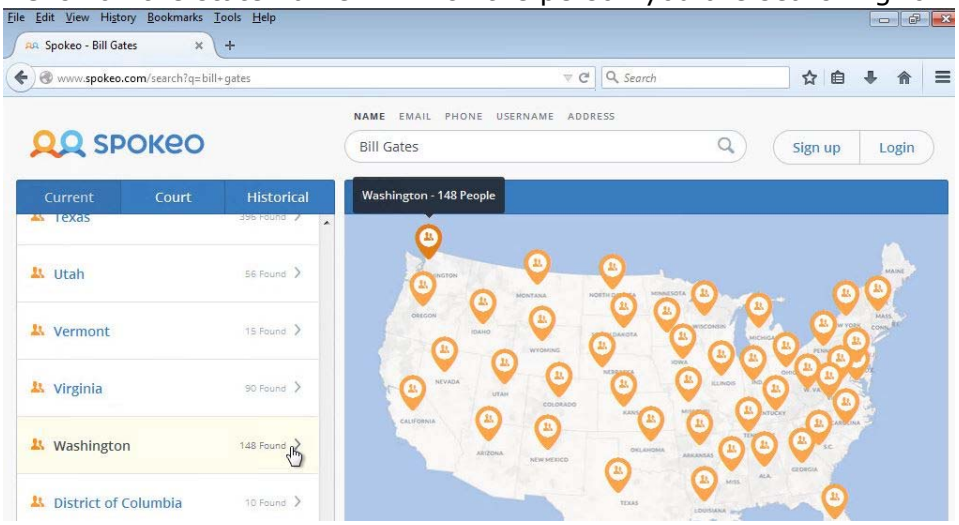


Spokeo's email search scans through 60+ social networks and public sources to find the owner's name, photos, and public profiles. Spokeo's reverse email lookup works with addresses from Yahoo.com, Hotmail.com, Gmail.com, AOL.com and many more.

4. Spokeo redirects you to search results with the name you have entered.



5. Click on the state name in which the person you are searching for lives.



Spokeo aggregates publicly available information from phone books, social networks, marketing surveys, real estate listings, and other public sources. This third-party data is then indexed through methods similar to those used by Google or Bing to create a listing. Because Spokeo only collects this data and does not create it, we cannot fully guarantee its accuracy.

6. Now, click on the appropriate City name for your search

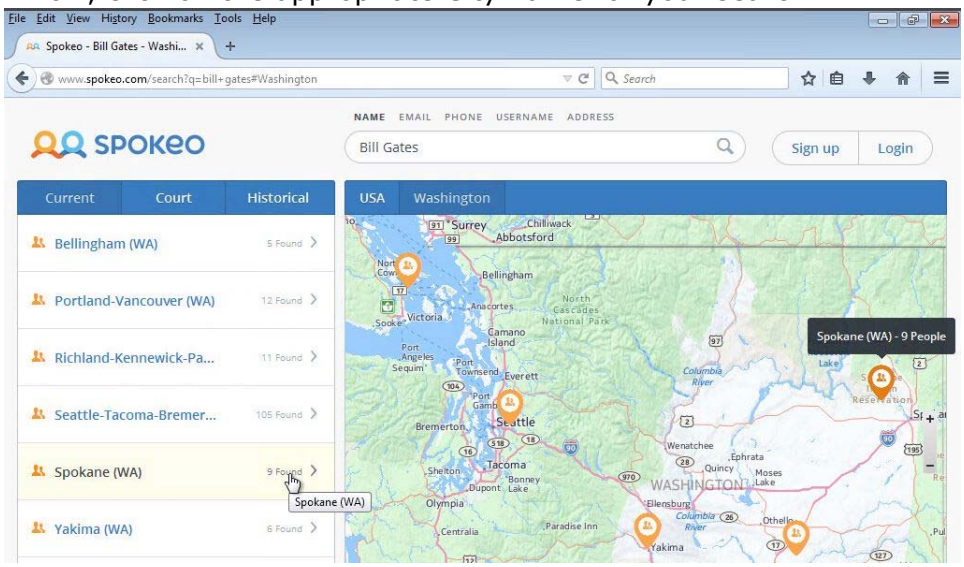


Figure: 5.7- Spokeo Search Result

7. Search results display the Address, Phone Number, Email Address, City and State, etc.

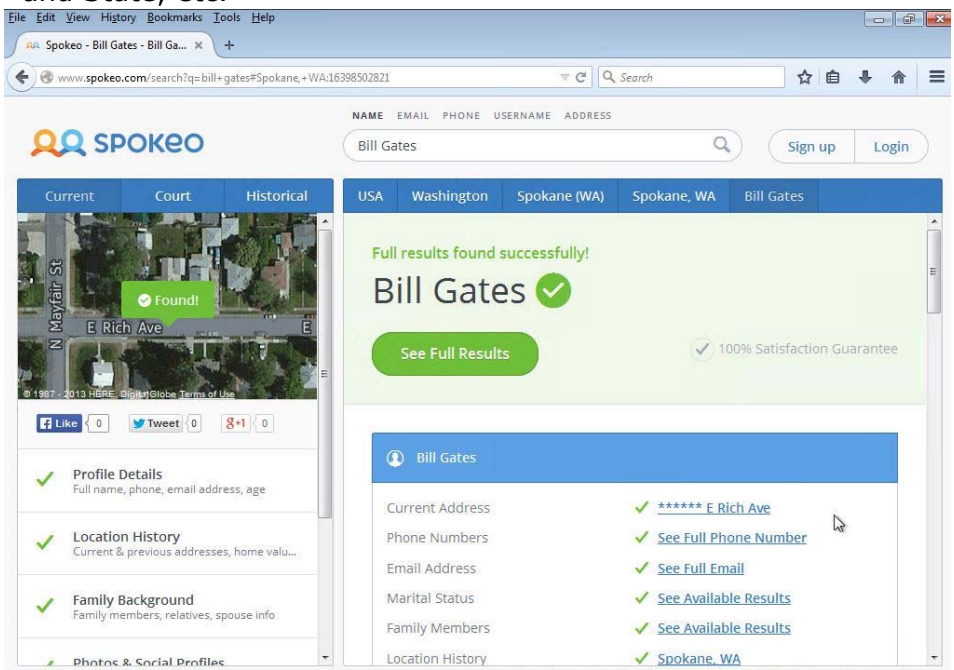


Figure: 5.8- Spokeo Search Result

Lab Analysis

Analyze and document all the results discovered in this lab.

Tool/Utility	Information Collected/Objectives Achieved
Spokeo	**Profile Details:** • Current Address • Phone Number • Email Address • Marital Status • Education • Occupation
	Online Map: Information about where the person has lived and detailed property information
	Family Background: Information about household members for the person you searched
	Photos & Social Profiles: Photos, videos, and social network profiles
	Neighborhood: Information about the neighborhood
	Reverse Lookup: Detailed information for the search done using phone numbers

Questions

1. How do you collect all the contact details of key people using Spokeo?
2. Is it possible to remove your residential listing? If yes, how?
3. How can you perform a reverse search using Spokeo?
4. List the kind of information that a reverse phone search and email search will yield.