CSI 3140

Lab 1 :

Exercise 1

1.1

Find the IP address of
www.whitehouse.gov
www.site.uottawa.ca
www.pastis.org

C:\Documents and Settings\gvj>nslookup www.whitehouse.org
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: www.whitehouse.org
*Address: **67.19.217.250***

C:\Documents and Settings\gvj>nslookup www.site.uottawa.ca
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: web0.site.uottawa.ca
*Address: **137.122.89.222***
Aliases: www.site.uottawa.ca

C:\Documents and Settings\gvj>nslookup www.pastis.org
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Server: UnKnown
Address: 192.168.0.1

Name: www.pastis.org
*Address: **64.26.156.34***

Or, another way:

C:\Documents and Settings\gvj>nslookup
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Default Server: UnKnown
Address: 192.168.0.1

> www.whitehouse.org
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: www.whitehouse.org
Address: 67.19.217.250

> www.site.uottawa.ca
Server: UnKnown

Address: 192.168.0.1

Non-authoritative answer:
Name: web0.site.uottawa.ca
Address: 137.122.89.222
Aliases: www.site.uottawa.ca

> www.pastis.org
Server: UnKnown
Address: 192.168.0.1

Name: www.pastis.org
Address: 64.26.156.34

> exit

What domain is mapped to 137.122.14.100 ?

C:\Documents and Settings\gvj>nslookup 137.122.14.100
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Server: UnKnown
Address: 192.168.0.1

*Name: **escher.uottawa.ca***
Address: 137.122.14.100

1.2

Instead of your default DNS server, use 208.67.222.222 and redo 1.1. What happens?

C:\Documents and Settings\gvj>nslookup
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Default Server: UnKnown
Address: 192.168.0.1

> server 208.67.222.222
Default Server: resolver1.opendns.com
Address: 208.67.222.222

> www.whitehouse.org
Server: resolver1.opendns.com
Address: 208.67.222.222

Non-authoritative answer:
Name: www.whitehouse.org
Address: 67.19.217.250

> www.site.uottawa.ca
Server: resolver1.opendns.com
Address: 208.67.222.222

Non-authoritative answer:
Name: web0.site.uottawa.ca
Address: 137.122.89.222
Aliases: www.site.uottawa.ca

> www.pastis.org
Server: resolver1.opendns.com
Address: 208.67.222.222

Non-authoritative answer:
Name: www.pastis.org
Address: 64.26.156.34

> 137.122.14.100

Server: resolver1.opendns.com
Address: 208.67.222.222

Name: escher.uottawa.ca
Address: 137.122.14.100

> exit

C:\Documents and Settings\gvj>

1.3

Ottawa's mayor can be reached at Larry.OBrien@Ottawa.ca.
a- What is the mail server in charge of this address?

In order to find the server handling SMTP traffic, one must look up the MX record

C:\WINDOWS\system32>nslookup
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Default Server: UnKnown
Address: 192.168.0.1

> set type=mx
> Ottawa.ca
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Ottawa.ca MX preference = 15, mail exchanger = merc.rmoc.on.ca
Ottawa.ca MX preference = 10, mail exchanger = mercury1.rmoc.on.ca
Ottawa.ca MX preference = 10, mail exchanger = mercury2.rmoc.on.ca

Ottawa.ca nameserver = ns1.business.allstream.net
Ottawa.ca nameserver = ns2.business.allstream.net
merc.rmoc.on.ca internet address = 192.234.223.127
mercury1.rmoc.on.ca internet address = 192.234.223.129
mercury2.rmoc.on.ca internet address = 192.234.223.128
ns2.business.allstream.net internet address = 207.181.89.3
ns1.business.allstream.net internet address = 207.181.89.2

b- The answer you got was likely labeled as "Non-authoritative answer". Find the authoritative one

To find the authoritative answer, one should set the type to SOA, send point to the corresponding server

C:\WINDOWS\system32>nslookup
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Default Server: UnKnown
Address: 192.168.0.1

> set type=soa
> Ottawa.ca
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Ottawa.ca
*primary name server = **ns1.business.allstream.net***
responsible mail addr = hostmaster.business.allstream.net
serial = 2008121600
refresh = 3600 (1 hour)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 21600 (6 hours)

Ottawa.ca nameserver = ns1.business.allstream.net
Ottawa.ca nameserver = ns2.business.allstream.net
ns2.business.allstream.net internet address = 207.181.89.3
ns1.business.allstream.net internet address = 207.181.89.2
*> **server ns1.business.allstream.net***
Default Server: ns1.business.allstream.net
Address: 207.181.89.2

> set type=mx
> Ottawa.ca
Server: ns1.business.allstream.net
Address: 207.181.89.2

Ottawa.ca MX preference = 10, mail exchanger = mercury2.rmoc.on.ca
Ottawa.ca MX preference = 15, mail exchanger = merc.rmoc.on.ca
Ottawa.ca MX preference = 10, mail exchanger = mercury1.rmoc.on.ca
Ottawa.ca nameserver = ns1.business.allstream.net
Ottawa.ca nameserver = ns2.business.allstream.net
mercury1.rmoc.on.ca internet address = 192.234.223.129
mercury2.rmoc.on.ca internet address = 192.234.223.128
merc.rmoc.on.ca internet address = 192.234.223.127
ns1.business.allstream.net internet address = 207.181.89.2
ns2.business.allstream.net internet address = 207.181.89.3

Exercise 2

2.1 find the basic commands of the SMTP protocol (enough to send a text email)

HELO
MAIL FROM:
RCPT TO:
DATA

2.2 take your @site.uottawa.ca email address (or @uottawa.ca address). Find the IP address of the mail server dealing with that address

In order to find the server handling SMTP traffic, one must look up the MX record

C:\Documents and Settings\gvj>nslookup
**** Can't find server name for address 192.168.0.1: Non-existent domain*
**** Default servers are not available*
Default Server: UnKnown
Address: 192.168.0.1

> set type=MX
> site.uottawa.ca
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
*site.uottawa.ca MX preference = 15, mail exchanger = **mxin.site.uottawa.ca***

site.uottawa.ca nameserver = dns1.ccs.carleton.ca
site.uottawa.ca nameserver = csi0.csi.uottawa.ca
mxin.site.uottawa.ca internet address = 137.122.89.159
dns1.ccs.carleton.ca internet address = 134.117.1.11

2.3 using the *telnet* command, send yourself an email from Bill.Gates@microsoft.com

C:\Documents and Settings\gvj>telnet mxin.site.uottawa.ca 25
220 mxin.site.uottawa.ca ESMTP Sendmail 8.13.1/8.13.1; Sun, 20 Jan 2008 17:18:29 -0500 (EST)
HELO mail.pastis.org
250 mxin.site.uottawa.ca Hello ottawa-hs-64-26-156-34.s-ip.magma.ca [64.26.156.34], pleased to meet you
MAIL FROM: Bill.Gates@microsoft.com
250 2.1.0 Bill.Gates@microsoft.com... Sender ok
RCPT TO: gvj@site.uottawa.ca
250 2.1.5 gvj@site.uottawa.ca... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Hi Guy, how's your day?
cheers
Bill
.
250 2.0.0 m0KMIT3f052639 Message accepted for delivery
quit
221 2.0.0 mxin.site.uottawa.ca closing connection

Connection to host lost.

C:\Documents and Settings\gvj>

2.4 check you email to see that you have received the message

2.5 find in this email where you can see that it is a fake

In the message headers:

Return-Path: <Bill.Gates@microsoft.com>
Received: from courriel.site.uottawa.ca ([unix socket])
by courriel.site.uottawa.ca (Cyrus v2.3.1) with LMTPA;
Sun, 20 Jan 2008 17:19:47 -0500
X-Sieve: CMU Sieve 2.3
Received: from mxin.site.uottawa.ca (mxin.site.uottawa.ca [137.122.89.159])
by courriel.site.uottawa.ca (8.13.4/8.13.4) with ESMTP id m0KMJlfg044073
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT)
for <gvj@site.uottawa.ca>; Sun, 20 Jan 2008 17:19:47 -0500 (EST)
(envelope-from Bill.Gates@microsoft.com)
Received: from mail.pastis.org (ottawa-hs-64-26-156-34.s-ip.magma.ca [64.26.156.34])
by mxin.site.uottawa.ca (8.13.1/8.13.1) with SMTP id m0KMIT3f052639
for gvj@site.uottawa.ca; Sun, 20 Jan 2008 17:19:19 -0500 (EST)
(envelope-from Bill.Gates@microsoft.com)
Date: Sun, 20 Jan 2008 17:18:29 -0500 (EST)
From: Bill.Gates@microsoft.com
Message-Id: <200801202219.m0KMIT3f052639@mxin.site.uottawa.ca>
To: undisclosed-recipients:;
X-Canit-CHI2: 0.48
X-Bayes-Prob: 0.0001 (Score 0, tokens from: @@RPTN, 10_Tag_Only)
X-Spam-Score: 4.20 (****) [Tag at 5.00]
L_T_COMBINED,MISSING_DATE,MISSING_SUBJECT,RDNS_DYNAMIC,SPF(softfail,2)
X-CanItPRO-Stream: 10_Tag_Only (inherits from default)
X-Canit-Stats-ID: 5539596 - 9f0d4825b273
X-Scanned-By: CanIt (www . roaringpenguin . com) on 137.122.89.159

Hi Guy, how's your day?
cheers
Bill

Exercise 3

3.1 using the *telnet* command, get the page http://www.google.com

C:\Documents and Settings\gvj>telnet www.google.com 80
GET / HTTP/1.1
Host: www.google.com

HTTP/1.1 302 Found
Location: http://www.google.ca/
Cache-Control: private
Set-Cookie: PREF=ID=28627661036cd202:TM=1200868077:LM=1200868077:S=G1Q2AufAKwJbc
V3g; expires=Tue, 19-Jan-2010 22:27:57 GMT; path=/; domain=.google.com
Content-Type: text/html
Server: gws
Content-Length: 218
Date: Sun, 20 Jan 2008 22:27:57 GMT

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<T ITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.ca/">here</A>.
</BODY></HTML>

C:\Documents and Settings\gvj>

NOTE that

C:\Documents and Settings\gvj>telnet www.google.ca 80
GET / HTTP/1.1
Host: www.google.ca

Does indeed return the document

3.2 can you fetch the page using only IP address? Why?

Yes you can