DNS Zone Transfer

Alex Hendren

Nova Scotia Community College

ISEC2025

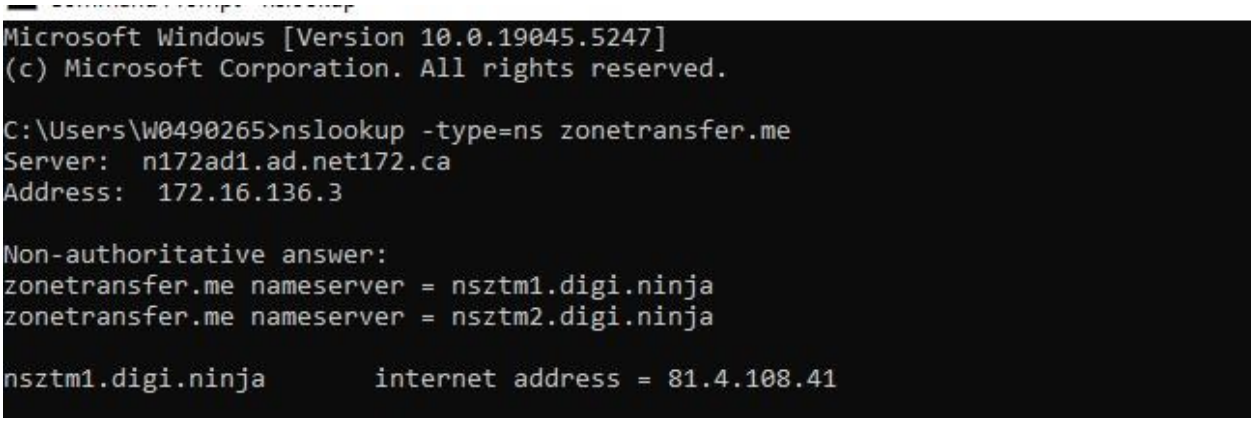
Assignment 1

January 14, 2025

Table of Contents

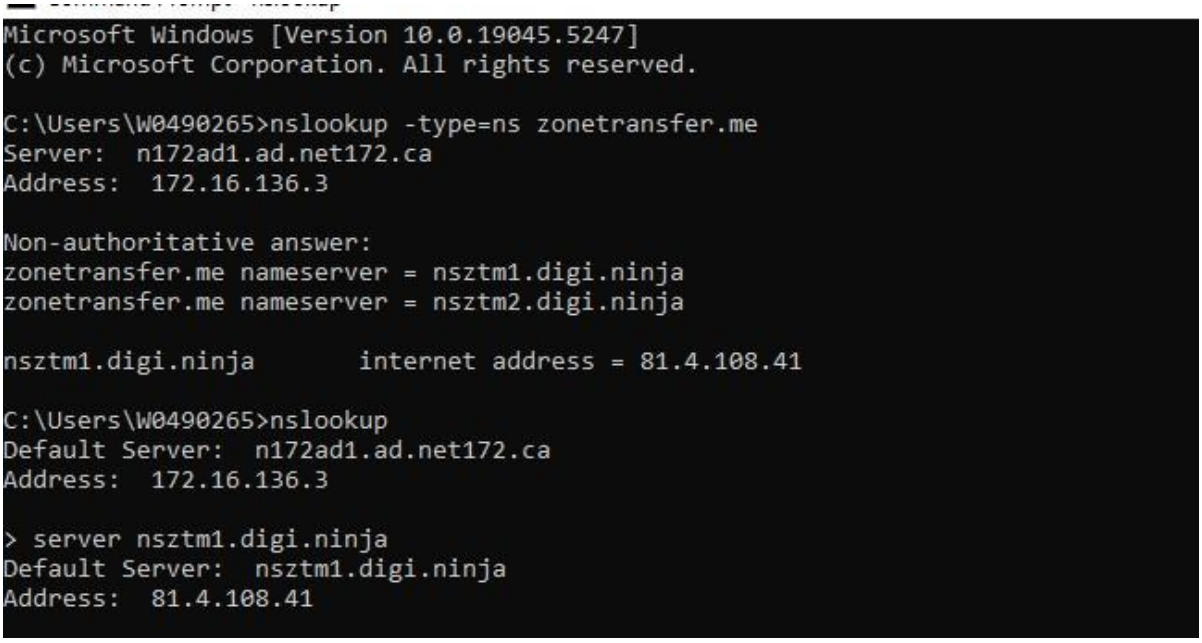
Step 1: Use the command to determine the name server(s) being used by zonetransfer.me

For this step, I used the command “nslookup -type=ns zonetransfer.me” to list the name servers for zonetransfer.me



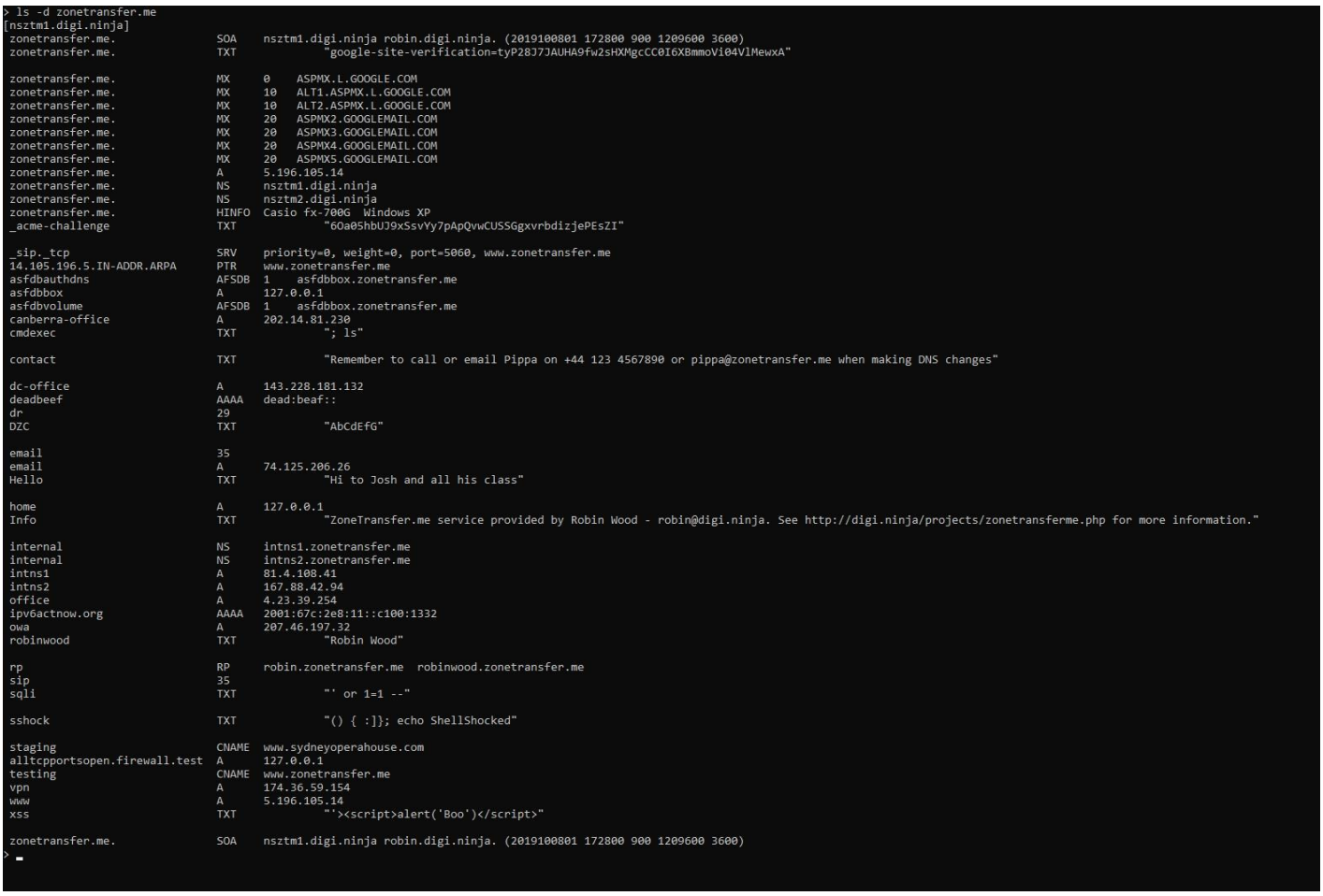
Step 2: Use the command structure to make the name server being used by zonetransfer.me to be your name server.

For this step, I used the command “server nsztm1.digi.ninja” to change my name server to zonetransfer.me



Step 4: Execute a zone transfer against the name server with the nslookup command.

For this step, I used the command ls -d zonetransfer.me to request a zone transfer.



```
> ls -d zonetransfer.me
[nsztm1.digi.ninja]
 zonetransfer.me.               SOA    nsztm1.digi.ninja robin.digi.ninja. (2019100801 172800 900 1209600 3600)
 zonetransfer.me.               TXT            "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"

 zonetransfer.me.               MX     0    ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     10   ALT1.ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     10   ALT2.ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     20   ASPMX2.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX3.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX4.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX5.GOOGLEMAIL.COM
 zonetransfer.me.               A      5.196.105.14
 zonetransfer.me.               NS     nsztm1.digi.ninja
 zonetransfer.me.               NS     nsztm2.digi.ninja
 zonetransfer.me.               HINFO  Casio fx-700G  Windows XP
 _acme-challenge                TXT            "6Oa0ShbUJ9xSsvVy7pApQvwCUSSGgxvrbdizjePEsZI"

 _sip._tcp                      SRV    priority=0, weight=0, port=5060, www.zonetransfer.me
 14.105.196.5.IN-ADDR.ARPA      PTR    www.zonetransfer.me
 asfdbauthdns                   AFSDB  1    asfdbbox.zonetransfer.me
 asfdbbox                       A      127.0.0.1
 asfdbvolume                    AFSDB  1    asfdbbox.zonetransfer.me
 canberra-office                A      202.14.81.230
 cmdexec                        TXT            "; ls"

 contact                        TXT            "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes"

 dc-office                      A      143.228.181.132
 deadbeef                       AAAA   dead:beaf::
 dr                             29
 DZC                            TXT            "AbCdEfG"

 email                          35
 email                          A      74.125.206.26
 Hello                          TXT            "Hi to Josh and all his class"

 home                           A      127.0.0.1
 Info                           TXT            "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more information."

 internal                       NS     intns1.zonetransfer.me
 internal                       NS     intns2.zonetransfer.me
 intns1                         A      81.4.108.41
 intns2                         A      167.88.42.94
 office                         A      4.23.39.254
 ipv6actnow.org                 AAAA   2001:67c:2e8:11::c100:1332
 owa                            A      207.46.197.32
 robinwood                      TXT            "Robin Wood"

 rp                             RP     robin.zonetransfer.me  robinwood.zonetransfer.me
 sip                            35
 sqli                           TXT            "' or 1=1 --"

 sshock                         TXT            "() { :]}; echo ShellShocked"

 staging                        CNAME  www.sydneyoperahouse.com
 alltcpportsopen.firewall.test  A      127.0.0.1
 testing                        CNAME  www.zonetransfer.me
 vpn                            A      174.36.59.154
 www                            A      5.196.105.14
 xss                            TXT            "'><script>alert('Boo')</script>"

 zonetransfer.me.               SOA    nsztm1.digi.ninja robin.digi.ninja. (2019100801 172800 900 1209600 3600)
> _
```