

**2. Start Of Authority (SOA): ns1-39.azure-dns.com**

**Server 1: ns1-39.azure-dns.com (IPv4: 150.171.10.39, IPv6: 2603:1061:0:10::27)**

**Server 2: ns2-39.azure-dns.net (IPv4: 150.171.16.39, IPv6: 2620:1ec:8ec:10::27)**

**Output:**

**$ dnsrecon -d microsoft.com**

[\*] std: Performing General Enumeration against: microsoft.com...

[-] DNSSEC is not configured for microsoft.com

[\*] SOA ns1-39.azure-dns.com 150.171.10.39

[\*] SOA ns1-39.azure-dns.com 2603:1061:0:10::27

[\*] NS ns2-39.azure-dns.net 150.171.16.39

[\*] NS ns2-39.azure-dns.net 2620:1ec:8ec:10::27

[\*] NS ns4-39.azure-dns.info 13.107.206.39

[\*] NS ns4-39.azure-dns.info 2620:1ec:bda:10::27

[\*] NS ns3-39.azure-dns.org 13.107.222.39

[\*] NS ns3-39.azure-dns.org 2a01:111:4000:10::27

[\*] NS ns1-39.azure-dns.com 150.171.10.39

[\*] NS ns1-39.azure-dns.com 2603:1061:0:10::27

[\*] MX microsoft-com.mail.protection.outlook.com 104.47.54.36

[\*] MX microsoft-com.mail.protection.outlook.com 52.101.11.0

[\*] MX microsoft-com.mail.protection.outlook.com 52.101.40.26

[\*] MX microsoft-com.mail.protection.outlook.com 52.101.8.49

[\*] MX microsoft-com.mail.protection.outlook.com 104.47.53.36

[\*] A microsoft.com 20.70.246.20

[\*] A microsoft.com 20.236.44.162

[\*] A microsoft.com 20.112.250.133

[\*] A microsoft.com 20.231.239.246

[\*] A microsoft.com 20.76.201.171

[\*] AAAA microsoft.com 2603:1010:3:3::5b

[\*] AAAA microsoft.com 2603:1030:b:3::152

[\*] AAAA microsoft.com 2603:1030:20e:3::23c

[\*] AAAA microsoft.com 2603:1030:c02:8::14

[\*] AAAA microsoft.com 2603:1020:201:10::10f

[\*] TXT microsoft.com d365mktkey=j2qHWq9BHdaa3ZXZH8x64daJZxEWsFa0dxDeilxDoYYx

[\*] TXT microsoft.com v=spf1 include:\_spf-a.microsoft.com include:\_spf-b.microsoft.com include:\_spf-c.microsoft.com include:\_spf-ssg-a.msft.net include:spf-a.hotmail.com include:\_spf1-meo.microsoft.com -all

[\*] TXT microsoft.com atlassian-domain-verification=xvoaqRfxSg3PnlVnR4xCSOlKyw1Aln0MMxRiKXnwWroFG7vI76TUC8xYb03MwMXv

[\*] TXT microsoft.com d365mktkey=3uc1cf82cpv750lzk70v9bvf2

[\*] TXT microsoft.com facebook-domain-verification=fwzwhbbzwmg5fzgotc2go51olc3566

[\*] TXT microsoft.com google-site-verification=pjPOauSPcrfXOZS9jnPPa5axowcHGCDAl1\_86dCqFpk

[\*] TXT microsoft.com fg2t0gov9424p2tdcuo94goe9j

[\*] TXT microsoft.com t7sebee51jrj7vm932k531hipa

[\*] TXT microsoft.com google-site-verification=M--CVfn\_YwsV-2FGbCp\_HFaEj23BmT0cTF4l8hXgpvM

[\*] TXT microsoft.com google-site-verification=GfDnTUdATPsK1230J0mXbfsYw-3A9BVMVaKSd4DcKgI

[\*] TXT microsoft.com d365mktkey=SxDf1EZxLvMwx6eEZUxzjFFgHoapF8DvtWEUjwq7ZTwx

[\*] TXT microsoft.com hubspot-developer-verification=OTQ5NGIwYWEtODNmZi00YWE1LTkyNmQtNDhjMDMxY2JjNDAx

[\*] TXT microsoft.com d365mktkey=QDa792dLCZhvaAOOCe2Hz6WTzmTssOp1snABhxWibhMx

[\*] TXT microsoft.com d365mktkey=6358r1b7e13hox60tl1uagv14

[\*] TXT microsoft.com google-site-verification=uFg3wr5PWsK8lV029RoXXBBUW0\_E6qf1WEWVHhetkOY

[\*] TXT microsoft.com docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840

[\*] TXT \_dmarc.microsoft.com v=DMARC1; p=reject; pct=100; rua=mailto:itex-rua@microsoft.com; ruf=mailto:itex-ruf@microsoft.com; fo=1

[\*] Enumerating SRV Records

[+] SRV \_xmpp-server.\_tcp.microsoft.com sipdog3.microsoft.com 131.107.1.47 5269

[+] SRV \_sip.\_tls.microsoft.com sipdir.online.lync.com 52.112.66.139 443

[+] SRV \_sip.\_tls.microsoft.com sipdir.online.lync.com 2603:1037:0:a::b 443

[+] SRV \_sip.\_tls.microsoft.com sipdir.online.lync.com 2603:1037:0:1::b 443

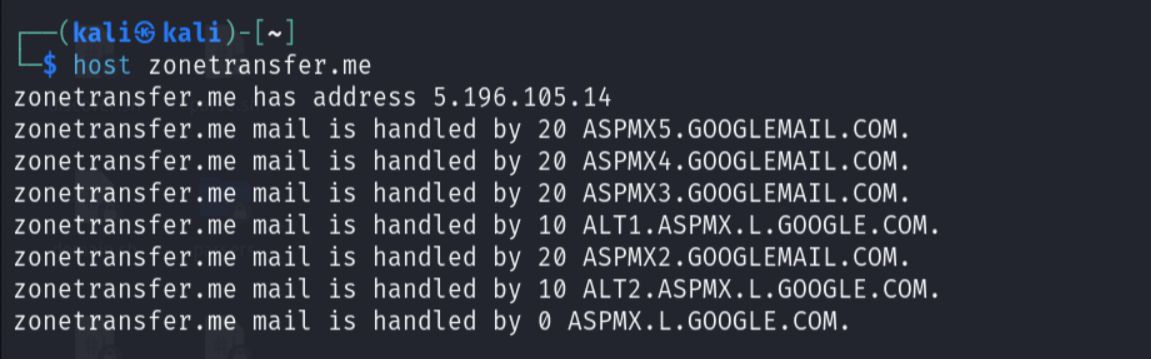
[+] SRV \_sip.\_tls.microsoft.com sipdir.online.lync.com 2603:1037:0:b::b 443

[+] SRV \_sip.\_tls.microsoft.com sipdir.online.lync.com 2603:1037::b 443

[+] SRV \_sipfederationtls.\_tcp.microsoft.com sipfed.online.lync.com 52.112.127.17 5061

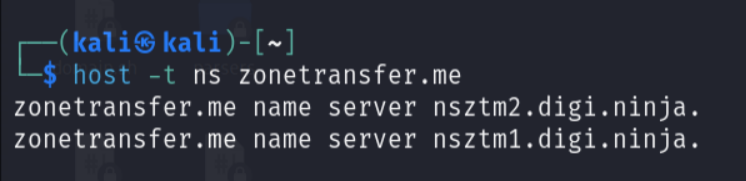
3. **Record Types:**

1. **Address Records: (zonetransfer.me)**
2. **Mail Exchange/Records: (ALT1.ASPMX.L.GOOGLE.COM., ASPMX2.GOOGLEMAIL.COM., ALT2.ASPMX.L.GOOGLE.COM., ASPMX.L.GOOGLE.COM., ASPMX5.GOOGLEMAIL.COM., ASPMX4.GOOGLEMAIL.COM., & ASPMX3.GOOGLEMAIL.COM.)**



**4. Two name servers:**

1. **nsztm1.digi.ninja**
2. **nsztm2.digi.ninja**



**5. What looks exposed & problematic:**

1. **alltcpportsopen.firewall.test.zonetransfer.me**

* **A hacker could see this port and attempt to open all the TCP ports to gain access to the system.**

1. **ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332**

* **This appears to be some sort of vulnerability in IPv6 that could be exploited by a threat actor.**

**Output:**

**$ host -l zonetransfer.me nsztm1.digi.ninja**

Using domain server:

Name: nsztm1.digi.ninja

Address: 81.4.108.41#53

Aliases:

zonetransfer.me has address 5.196.105.14

zonetransfer.me name server nsztm1.digi.ninja.

zonetransfer.me name server nsztm2.digi.ninja.

14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.

asfdbbox.zonetransfer.me has address 127.0.0.1

canberra-office.zonetransfer.me has address 202.14.81.230

dc-office.zonetransfer.me has address 143.228.181.132

deadbeef.zonetransfer.me has IPv6 address dead:beaf::

email.zonetransfer.me has address 74.125.206.26

home.zonetransfer.me has address 127.0.0.1

internal.zonetransfer.me name server intns1.zonetransfer.me.

internal.zonetransfer.me name server intns2.zonetransfer.me.

intns1.zonetransfer.me has address 81.4.108.41

intns2.zonetransfer.me has address 167.88.42.94

office.zonetransfer.me has address 4.23.39.254

ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332

owa.zonetransfer.me has address 207.46.197.32

alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1

vpn.zonetransfer.me has address 174.36.59.154

www.zonetransfer.me has address 5.196.105.14

6. **Number of Records: 23 Records**

**(**nsztm1.digi.ninja has 11 and nsztm2.digi.ninja has 12.**)**

**Output:**

**$ dnsenum zonetransfer.me**

dnsenum VERSION:1.2.6

----- zonetransfer.me -----

Host's addresses:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zonetransfer.me. 5822 IN A 5.196.105.14

Name Servers:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

nsztm2.digi.ninja. 10612 IN A 34.225.33.2

nsztm1.digi.ninja. 10166 IN A 81.4.108.41

Mail (MX) Servers:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ALT1.ASPMX.L.GOOGLE.COM. 105 IN A 172.253.126.27

ASPMX2.GOOGLEMAIL.COM. 105 IN A 172.253.126.27

ALT2.ASPMX.L.GOOGLE.COM. 105 IN A 173.194.219.26

ASPMX.L.GOOGLE.COM. 105 IN A 74.125.202.27

ASPMX5.GOOGLEMAIL.COM. 105 IN A 172.217.197.27

ASPMX4.GOOGLEMAIL.COM. 105 IN A 142.250.112.27

ASPMX3.GOOGLEMAIL.COM. 105 IN A 173.194.219.27

Trying Zone Transfers and getting Bind Versions:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...

zonetransfer.me. 7200 IN SOA (

zonetransfer.me. 300 IN HINFO "Casio

zonetransfer.me. 301 IN TXT (

zonetransfer.me. 7200 IN MX 0

zonetransfer.me. 7200 IN MX 10

zonetransfer.me. 7200 IN MX 10

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN A 5.196.105.14

zonetransfer.me. 7200 IN NS nsztm1.digi.ninja.

zonetransfer.me. 7200 IN NS nsztm2.digi.ninja.

\_acme-challenge.zonetransfer.me. 301 IN TXT (

\_sip.\_tcp.zonetransfer.me. 14000 IN SRV 0

14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.

asfdbauthdns.zonetransfer.me. 7900 IN AFSDB 1

asfdbbox.zonetransfer.me. 7200 IN A 127.0.0.1

asfdbvolume.zonetransfer.me. 7800 IN AFSDB 1

canberra-office.zonetransfer.me. 7200 IN A 202.14.81.230

cmdexec.zonetransfer.me. 300 IN TXT ";

contact.zonetransfer.me. 2592000 IN TXT (

dc-office.zonetransfer.me. 7200 IN A 143.228.181.132

deadbeef.zonetransfer.me. 7201 IN AAAA dead:beaf::

dr.zonetransfer.me. 300 IN LOC 53

DZC.zonetransfer.me. 7200 IN TXT AbCdEfG

email.zonetransfer.me. 2222 IN NAPTR (

email.zonetransfer.me. 7200 IN A 74.125.206.26

Hello.zonetransfer.me. 7200 IN TXT "Hi

home.zonetransfer.me. 7200 IN A 127.0.0.1

Info.zonetransfer.me. 7200 IN TXT (

internal.zonetransfer.me. 300 IN NS intns1.zonetransfer.me.

internal.zonetransfer.me. 300 IN NS intns2.zonetransfer.me.

intns1.zonetransfer.me. 300 IN A 81.4.108.41

intns2.zonetransfer.me. 300 IN A 167.88.42.94

office.zonetransfer.me. 7200 IN A 4.23.39.254

ipv6actnow.org.zonetransfer.me. 7200 IN AAAA 2001:67c:2e8:11::c100:1332

owa.zonetransfer.me. 7200 IN A 207.46.197.32

robinwood.zonetransfer.me. 302 IN TXT "Robin

rp.zonetransfer.me. 321 IN RP (

sip.zonetransfer.me. 3333 IN NAPTR (

sqli.zonetransfer.me. 300 IN TXT "'

sshock.zonetransfer.me. 7200 IN TXT "()

staging.zonetransfer.me. 7200 IN CNAME www.sydneyoperahouse.com.

alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1

testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.

vpn.zonetransfer.me. 4000 IN A 174.36.59.154

www.zonetransfer.me. 7200 IN A 5.196.105.14

xss.zonetransfer.me. 300 IN TXT "'><script>alert('Boo')</script>"

Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...

zonetransfer.me. 7200 IN SOA (

zonetransfer.me. 300 IN HINFO "Casio

zonetransfer.me. 301 IN TXT (

zonetransfer.me. 7200 IN MX 0

zonetransfer.me. 7200 IN MX 10

zonetransfer.me. 7200 IN MX 10

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN MX 20

zonetransfer.me. 7200 IN A 5.196.105.14

zonetransfer.me. 7200 IN NS nsztm1.digi.ninja.

zonetransfer.me. 7200 IN NS nsztm2.digi.ninja.

\_acme-challenge.zonetransfer.me. 301 IN TXT (

\_acme-challenge.zonetransfer.me. 301 IN TXT (

\_sip.\_tcp.zonetransfer.me. 14000 IN SRV 0

14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.

asfdbauthdns.zonetransfer.me. 7900 IN AFSDB 1

asfdbbox.zonetransfer.me. 7200 IN A 127.0.0.1

asfdbvolume.zonetransfer.me. 7800 IN AFSDB 1

canberra-office.zonetransfer.me. 7200 IN A 202.14.81.230

cmdexec.zonetransfer.me. 300 IN TXT ";

contact.zonetransfer.me. 2592000 IN TXT (

dc-office.zonetransfer.me. 7200 IN A 143.228.181.132

deadbeef.zonetransfer.me. 7201 IN AAAA dead:beaf::

dr.zonetransfer.me. 300 IN LOC 53

DZC.zonetransfer.me. 7200 IN TXT AbCdEfG

email.zonetransfer.me. 2222 IN NAPTR (

email.zonetransfer.me. 7200 IN A 74.125.206.26

Hello.zonetransfer.me. 7200 IN TXT "Hi

home.zonetransfer.me. 7200 IN A 127.0.0.1

Info.zonetransfer.me. 7200 IN TXT (

internal.zonetransfer.me. 300 IN NS intns1.zonetransfer.me.

internal.zonetransfer.me. 300 IN NS intns2.zonetransfer.me.

intns1.zonetransfer.me. 300 IN A 81.4.108.41

intns2.zonetransfer.me. 300 IN A 52.91.28.78

office.zonetransfer.me. 7200 IN A 4.23.39.254

ipv6actnow.org.zonetransfer.me. 7200 IN AAAA 2001:67c:2e8:11::c100:1332

owa.zonetransfer.me. 7200 IN A 207.46.197.32

robinwood.zonetransfer.me. 302 IN TXT "Robin

rp.zonetransfer.me. 321 IN RP (

sip.zonetransfer.me. 3333 IN NAPTR (

sqli.zonetransfer.me. 300 IN TXT "'

sshock.zonetransfer.me. 7200 IN TXT "()

staging.zonetransfer.me. 7200 IN CNAME www.sydneyoperahouse.com.

alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1

testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.

vpn.zonetransfer.me. 4000 IN A 174.36.59.154

www.zonetransfer.me. 7200 IN A 5.196.105.14

xss.zonetransfer.me. 300 IN TXT "'><script>alert('Boo')</script>"

Brute forcing with /usr/share/dnsenum/dns.txt:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zonetransfer.me class C netranges:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.23.39.0/24

5.196.105.0/24

52.91.28.0/24

74.125.206.0/24

81.4.108.0/24

143.228.181.0/24

167.88.42.0/24

174.36.59.0/24

202.14.81.0/24

207.46.197.0/24

Performing reverse lookup on 2560 ip addresses:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

0 results out of 2560 IP addresses.

zonetransfer.me ip blocks:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

done.