Information Gathering

Information Gathering

Passive Information Gathering

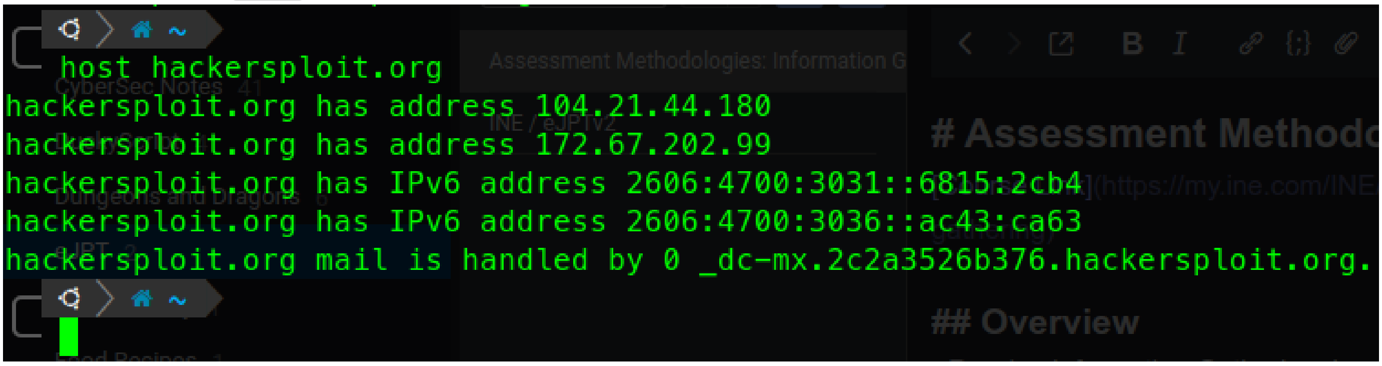
Passive Information Gathering is looking at tools/techniques to obtain information of a target through publicly available information through the internet.

Website Recon & Footprinting

With Website Recon and footprinting, we are looking for:

- IP Addresses
- Directories hidden from search engines
- Names
- Email Addresses
- Phone Numbers
- Physical Address
- Web technologies being used

Using command `host` to find IP address of a website/domain



```
host hackersploit.org
hackersploit.org has address 104.21.44.180
hackersploit.org has address 172.67.202.99
hackersploit.org has IPv6 address 2606:4700:3031::6815:2cb4
hackersploit.org has IPv6 address 2606:4700:3036::ac43:ca63
hackersploit.org mail is handled by 0 _dc-mx.2c2a3526b376.hackersploit.org.
```

2 IPs usually means they a behind a proxy

- robot.txt file (https://hackersploit.org/robots.txt) - Tells search engine what directories of the website it is allowed and not allowed to crawl and grab information on.
- sitemap.xml (https://hackersploit.org/sitemap_index.xml) - Used to provide search engine a way to index a website.

Helpful addons for FF/Chrome

- Builtwith - Shows details and information such as Widgets, and plugins are installed, subdomains, and more.

- Wappalyzer - Another way to identify technologies used on website.
- Whatweb - Use command `whatweb` that is built into Kali, to help obtain information as well.
- Download the website - Use HTTRack - This can be installed on your machine and used to

Whois Enumeration

WHOIS is a query and response protocol used to query databases that store the registered users or assignee's of a resource, such as domain names, IP address blocks, etc.

- Command line utility for `whois`.

```
whois hackersploit.org
Domain Name: hackersploit.org
Registry Domain ID: 77f8fe62a425487cbefef4bf7e27d2ec-LROR
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2022-12-22T11:20:08Z
Creation Date: 2018-04-05T11:27:07Z
Registry Expiry Date: 2024-04-05T11:27:07Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy service provided by Withheld for Privacy
ehf
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED FOR PRIVACY
[...]
```

- Whois Website utility - Can also be used on IP addresses or domains

Website footprinting with Netcraft

Netcraft is used to gather information about a target domain, such as email, registrar, technologies, etc.

DNS Recon

DNS - Domain Name Service

- DNSRecon - Built into Kali - DNSRecon is a Python script that provides the ability to perform: Check all NS Records for Zone Transfers. Enumerate General DNS Records for a given Domain

(MX, SOA, NS, A, AAAA, SPF and TXT). Perform common SRV Record Enumeration. Top Level Domain (TLD) Expansion.

```
dnsrecon -d hackersploit.org
[*] std: Performing General Enumeration against: hackersploit.org...
[-] All nameservers failed to answer the DNSSEC query for hackersploit.org
[*]      SOA dee.ns.cloudflare.com 172.64.32.93
[*]      SOA dee.ns.cloudflare.com 173.245.58.93
[*]      SOA dee.ns.cloudflare.com 108.162.192.93
[*]      SOA dee.ns.cloudflare.com 2803:f800:50::6ca2:c05d
[*]      SOA dee.ns.cloudflare.com 2a06:98c1:50::ac40:205d
[*]      SOA dee.ns.cloudflare.com 2606:4700:50::adf5:3a5d
[*]      NS jim.ns.cloudflare.com 173.245.59.125
[*]      NS jim.ns.cloudflare.com 108.162.193.125
[*]      NS jim.ns.cloudflare.com 172.64.33.125
[...]
```

- DNSDumpster - "A FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process."

WAF with wafw00f

WAF is a Web Application Firewall.

- wafw00f - The Web Application Firewall Fingerprinting Tool.
  - Tells the Web Application Firewall being used to protect the site.

Subdomain Enumeration With Sublist3r

- Sublist3r - is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask.
  - This can be used but can be limited due to rate limiting.

Google Dorking

Google dorking is a way of using google searches for more potentially hidden info.

- Limit results to a domain: `site:[domain]`
  - `site:ine.com`
- Limit results to URL: `inurl:[word]`
  - `inurl:admin`
- Limit results to subdomains: `site:*.[domain]`

    - `site:*.ine.com`
- Limit results to site title: `intitle:[word]`
    - `intitle:admin`
- Limit results to file type: `filetype:[file type]`
    - `filetype:pdf`
- Limit results to indexs: `intitle:index of`
    - Let users view results for an index for a website.
- Find older, cached versions of website: `cache:[domain]`
    - `cache:ine.com`
- Waybackmachine(archive.org) That has snapshots of older version of websites.
- ExploitDB Google Hacking Database - A database of google dorks that have found useful info such as "juicy" information, users, password, etc.

Email Harvesting with theHarvester

TheHarvester - Similar to Sublist3r uses OSINT tools, but finds emails that belong to a domain that may be publically available or have been leaked.

- `theHarvester -d [domain] -b [databases`
    - `theHarvester -d pm.me -b google,linkedin,dnsdumpster,duckduckgo`

Leaked Password Databases

- HaveIBeenPwned - Check if your email or phone is in a data breach

Active Information Gathering

Active Information Gathering is actively interacting with the targets systems to gather information.

DNS Zone Transfers

DNS(Domain Name System) Servers, or name servers, are used to resolve domain names to IP addresses. DNS is setup by a number of companies, like Google(8.8.8.8) and Cloudflare(1.1.1.1).

In certain cases. DNS server admins may want to copy or transfer zone files from one DNS server to another. This process is known as a Zone Transfer. If this is mis-configured and left unsecured, this functionality can be abused by attackers to copy the zone file from the primary DNS server to another. This can provide penetration testers with a wide view of an organizations network layout. It can also in some cases, internal network addresses may be found on an organizations DNS server.

DNS Records

- A - Resolves a hostname or domain to an IPv4 Address

- AAAA - Resolves a hostname or domain to an IPv6 Address
- NS - Refers to the domains nameserver
- MX - Refers a domain to a mail server
- CNAME - Used for domain aliases
- TXT - Text record
- HINFO - Host information
- SOA - Domain Authority
- SRV - Service Records
- PRT - Resolves and IP address to a hostname

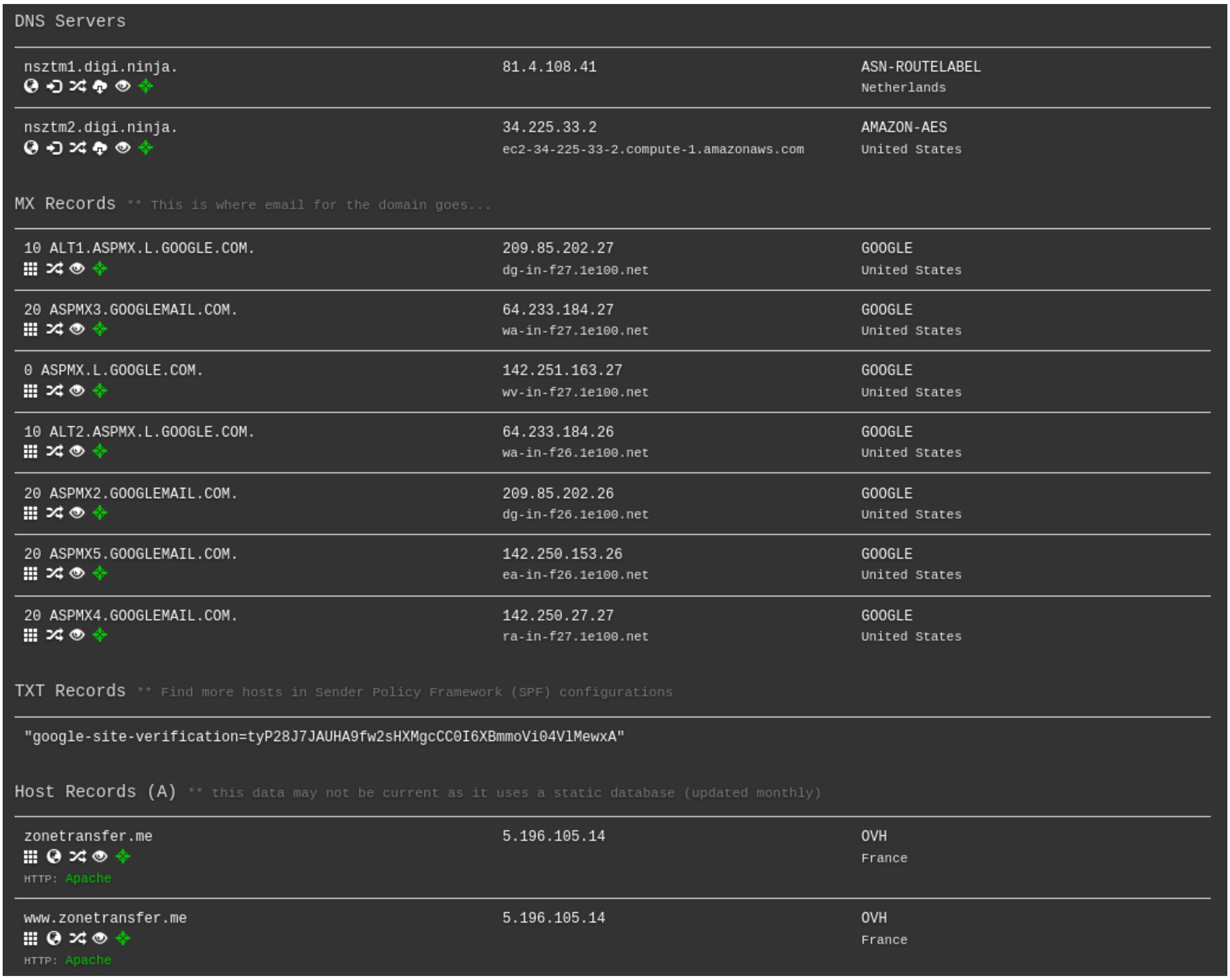
DNS Interrogation

DNS interrogation is the process of enumerating DNS Records for a specific domain.T he objective of the this is to the probe a DNS Server to provide us with DNS record for the specified domain. This can provide us with important information such as the IP address, subdomains, mail server addresses, etc.

Demo

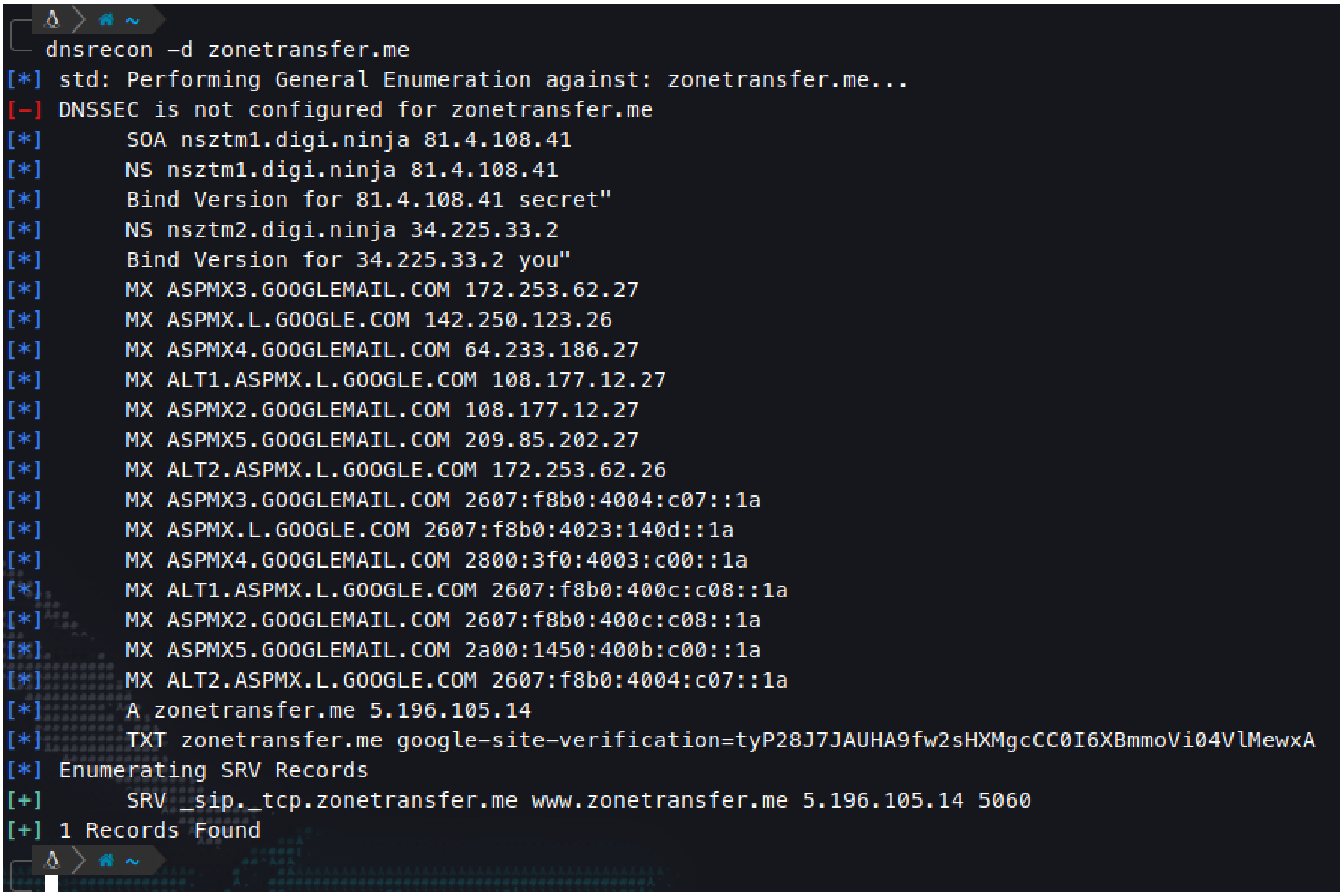
Zonetransfer.me

DNSDumpster



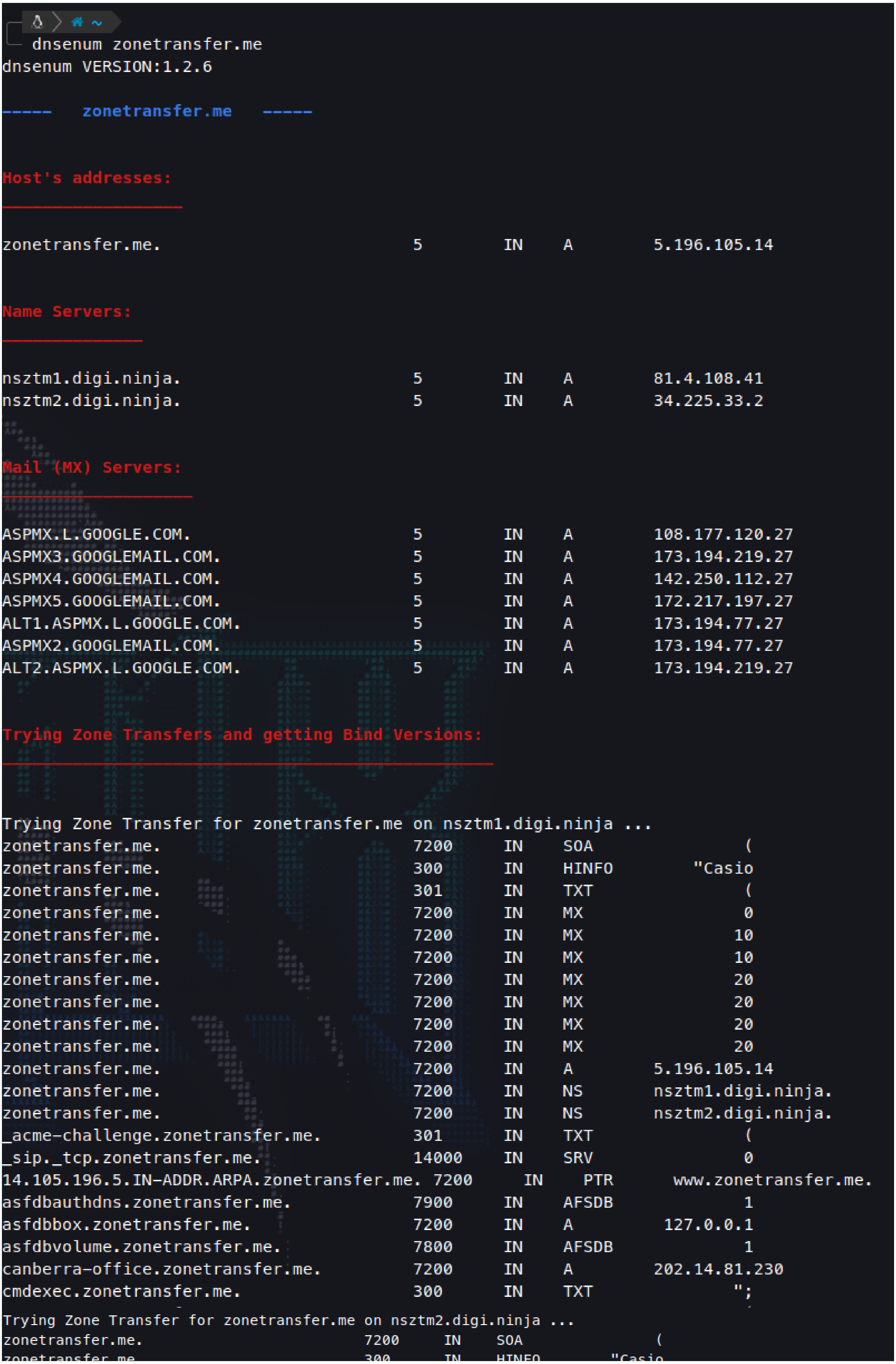
```
DNS Servers

nsztm1.digi.ninja.                        81.4.108.41                              ASN-ROUTELABEL
                                                                                   Netherlands

nsztm2.digi.ninja.                        34.225.33.2                              AMAZON-AES
                                          ec2-34-225-33-2.compute-1.amazonaws.com  United States

MX Records ** This is where email for the domain goes...

10 ALT1.ASPMX.L.GOOGLE.COM.               209.85.202.27                            GOOGLE
                                          dg-in-f27.1e100.net                      United States

20 ASPMX3.GOOGLEMAIL.COM.                 64.233.184.27                            GOOGLE
                                          wa-in-f27.1e100.net                      United States

0 ASPMX.L.GOOGLE.COM.                     142.251.163.27                           GOOGLE
                                          wv-in-f27.1e100.net                      United States

10 ALT2.ASPMX.L.GOOGLE.COM.               64.233.184.26                            GOOGLE
                                          wa-in-f26.1e100.net                      United States

20 ASPMX2.GOOGLEMAIL.COM.                 209.85.202.26                            GOOGLE
                                          dg-in-f26.1e100.net                      United States

20 ASPMX5.GOOGLEMAIL.COM.                 142.250.153.26                           GOOGLE
                                          ea-in-f26.1e100.net                      United States

20 ASPMX4.GOOGLEMAIL.COM.                 142.250.27.27                            GOOGLE
                                          ra-in-f27.1e100.net                      United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

zonetransfer.me                           5.196.105.14                             OVH
                                                                                   France
HTTP: Apache

www.zonetransfer.me                       5.196.105.14                             OVH
                                                                                   France
HTTP: Apache
```

DNSRecon:

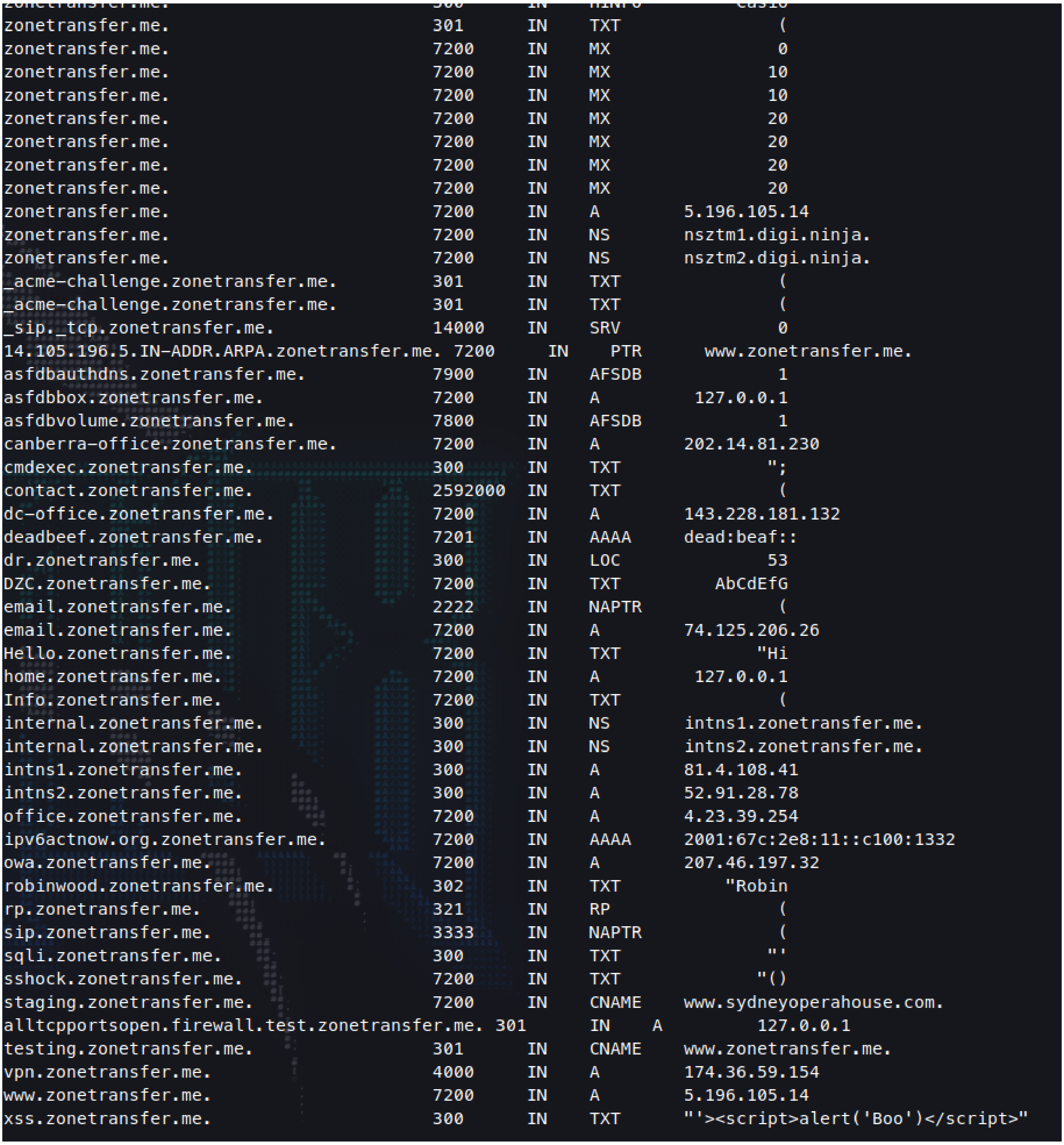


```
dnsrecon -d zonetransfer.me
[*] std: Performing General Enumeration against: zonetransfer.me...
[-] DNSSEC is not configured for zonetransfer.me
[*]      SOA nsztm1.digi.ninja 81.4.108.41
[*]      NS nsztm1.digi.ninja 81.4.108.41
[*]      Bind Version for 81.4.108.41 secret"
[*]      NS nsztm2.digi.ninja 34.225.33.2
[*]      Bind Version for 34.225.33.2 you"
[*]      MX ASPMX3.GOOGLEMAIL.COM 172.253.62.27
[*]      MX ASPMX.L.GOOGLE.COM 142.250.123.26
[*]      MX ASPMX4.GOOGLEMAIL.COM 64.233.186.27
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 108.177.12.27
[*]      MX ASPMX2.GOOGLEMAIL.COM 108.177.12.27
[*]      MX ASPMX5.GOOGLEMAIL.COM 209.85.202.27
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 172.253.62.26
[*]      MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4004:c07::1a
[*]      MX ASPMX.L.GOOGLE.COM 2607:f8b0:4023:140d::1a
[*]      MX ASPMX4.GOOGLEMAIL.COM 2800:3f0:4003:c00::1a
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400c:c08::1a
[*]      MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400c:c08::1a
[*]      MX ASPMX5.GOOGLEMAIL.COM 2a00:1450:400b:c00::1a
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4004:c07::1a
[*]      A zonetransfer.me 5.196.105.14
[*]      TXT zonetransfer.me google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*] Enumerating SRV Records
[+]      SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 5.196.105.14 5060
[+] 1 Records Found
```

DNSEnum:



```
dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

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


Host's addresses:
__________________

zonetransfer.me.                         5        IN    A        5.196.105.14


Name Servers:
______________

nsztm1.digi.ninja.                       5        IN    A        81.4.108.41
nsztm2.digi.ninja.                       5        IN    A        34.225.33.2


Mail (MX) Servers:
___________________

ASPMX.L.GOOGLE.COM.                      5        IN    A        108.177.120.27
ASPMX3.GOOGLEMAIL.COM.                   5        IN    A        173.194.219.27
ASPMX4.GOOGLEMAIL.COM.                   5        IN    A        142.250.112.27
ASPMX5.GOOGLEMAIL.COM.                   5        IN    A        172.217.197.27
ALT1.ASPMX.L.GOOGLE.COM.                 5        IN    A        173.194.77.27
ASPMX2.GOOGLEMAIL.COM.                   5        IN    A        173.194.77.27
ALT2.ASPMX.L.GOOGLE.COM.                 5        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               ";
Trying Zone Transfer for zonetransfer.me on nsztm2.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA                (
zonetransfer.me.                         300      IN    HINFO         "Casio
```

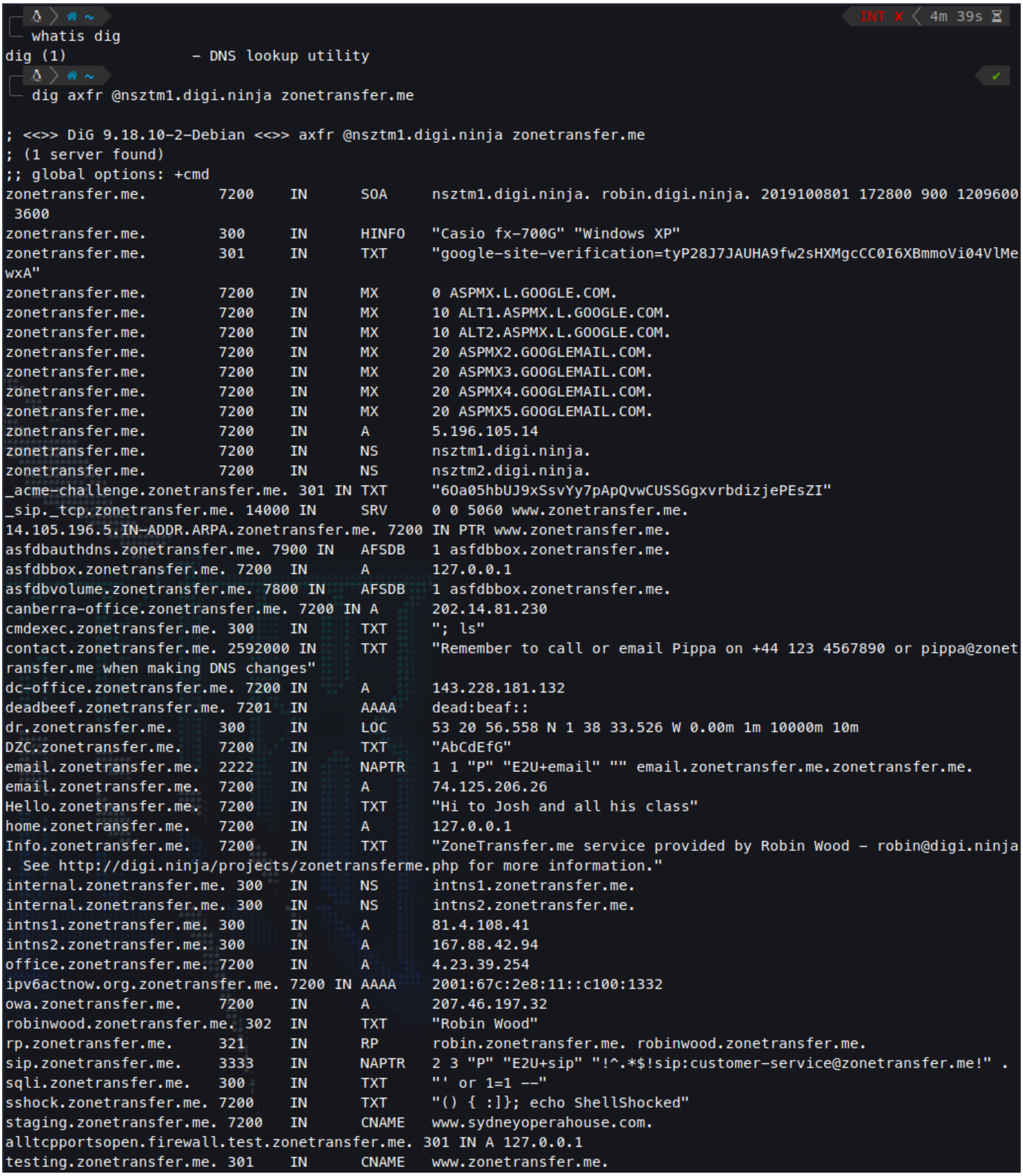


```
zonetransfer.me.                        300      IN    HINFO        "Casio
zonetransfer.me.                        301      IN    TXT              (
zonetransfer.me.                        7200     IN    MX               0
zonetransfer.me.                        7200     IN    MX              10
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>"
```

This is for active recon. This can enumerate publically available records, as well as it can perform Zone Transfer automatically, DNS BruteForce to identify record and subdomains.

DIG

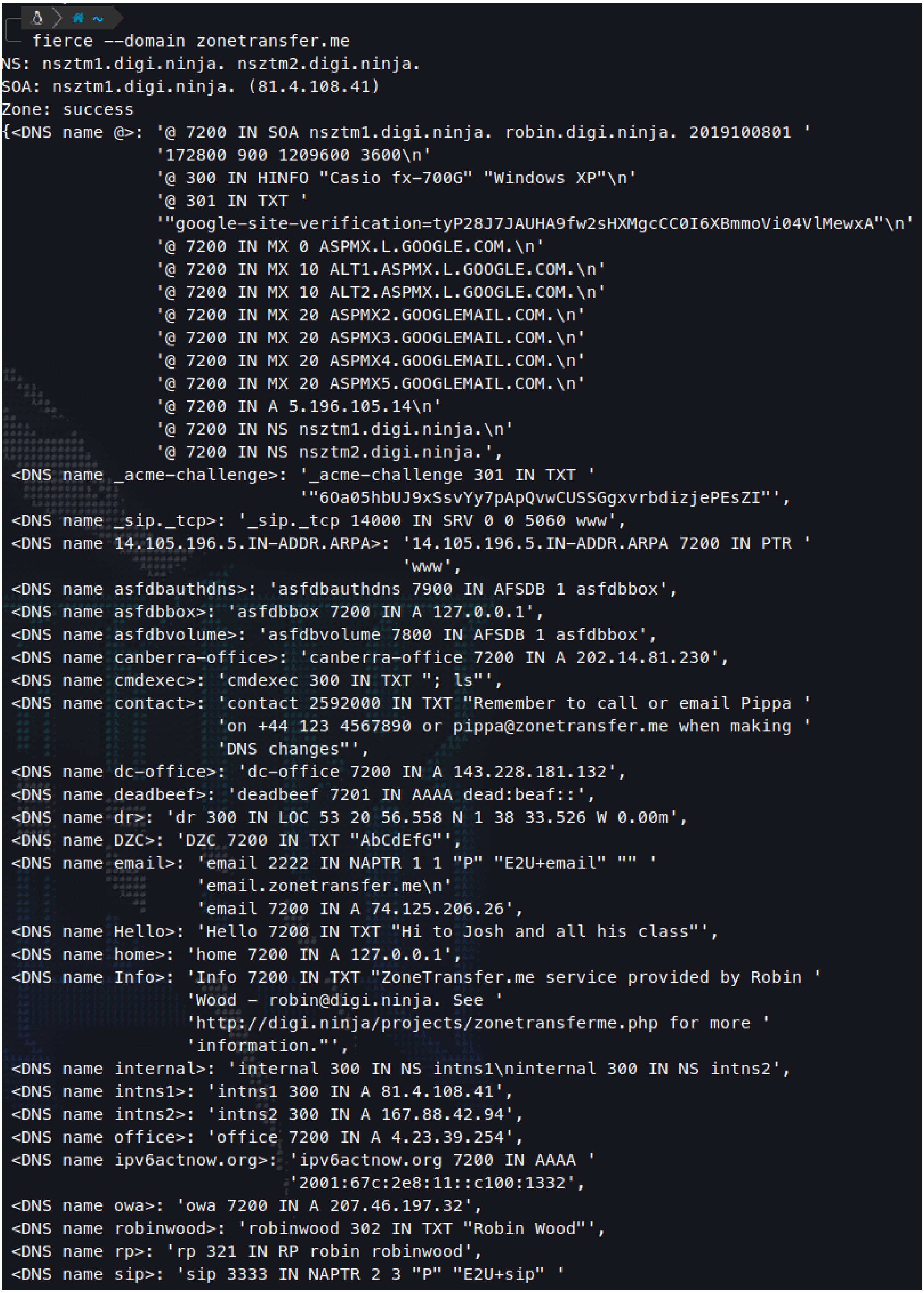
DIG is a DNS Lookup Utility



```
                                                                                INT ✘ 4m 39s
 whatis dig
dig (1)                 - DNS lookup utility
                                                                                           ✓
 dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.18.10-2-Debian <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2019100801 172800 900 1209600
 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMe
wxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
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     "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
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.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonet
ransfer.me when making DNS changes"
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 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
Hello.zonetransfer.me.  7200    IN      TXT     "Hi to Josh and all his class"
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja
. See http://digi.ninja/projects/zonetransferme.php for more information."
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 Wood"
rp.zonetransfer.me.     321     IN      RP      robin.zonetransfer.me. robinwood.zonetransfer.me.
sip.zonetransfer.me.    3333    IN      NAPTR   2 3 "P" "E2U+sip" "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.   300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN      TXT     "() { :]}; echo ShellShocked"
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.
```

fierce

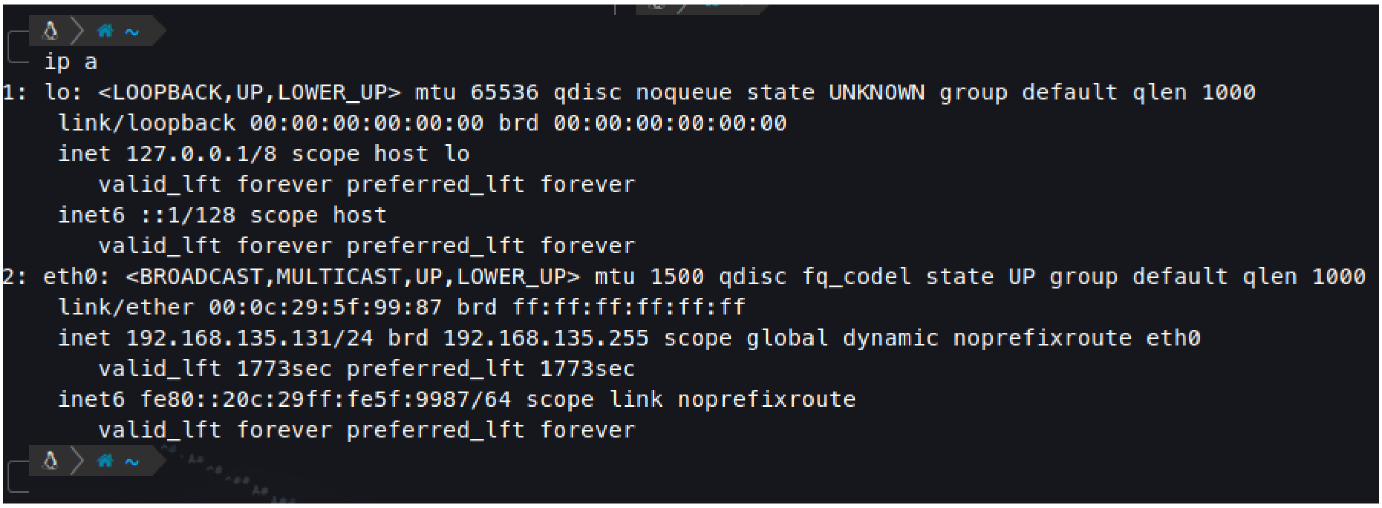
A DNS reconnaissance tool for locating non-contiguous IP space. Can be used to BruteForce DNS records and/or subdomains.



```
fierce --domain zonetransfer.me
NS: nsztm1.digi.ninja. nsztm2.digi.ninja.
SOA: nsztm1.digi.ninja. (81.4.108.41)
Zone: success
{<DNS name @>: '@ 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2019100801 '
               '172800 900 1209600 3600\n'
               '@ 300 IN HINFO "Casio fx-700G" "Windows XP"\n'
               '@ 301 IN TXT '
               '"google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"\n'
               '@ 7200 IN MX 0 ASPMX.L.GOOGLE.COM.\n'
               '@ 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.\n'
               '@ 7200 IN MX 10 ALT2.ASPMX.L.GOOGLE.COM.\n'
               '@ 7200 IN MX 20 ASPMX2.GOOGLEMAIL.COM.\n'
               '@ 7200 IN MX 20 ASPMX3.GOOGLEMAIL.COM.\n'
               '@ 7200 IN MX 20 ASPMX4.GOOGLEMAIL.COM.\n'
               '@ 7200 IN MX 20 ASPMX5.GOOGLEMAIL.COM.\n'
               '@ 7200 IN A 5.196.105.14\n'
               '@ 7200 IN NS nsztm1.digi.ninja.\n'
               '@ 7200 IN NS nsztm2.digi.ninja.',
 <DNS name _acme-challenge>: '_acme-challenge 301 IN TXT '
                             '"6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"',
 <DNS name _sip._tcp>: '_sip._tcp 14000 IN SRV 0 0 5060 www',
 <DNS name 14.105.196.5.IN-ADDR.ARPA>: '14.105.196.5.IN-ADDR.ARPA 7200 IN PTR '
                                       'www',
 <DNS name asfdbauthdns>: 'asfdbauthdns 7900 IN AFSDB 1 asfdbbox',
 <DNS name asfdbbox>: 'asfdbbox 7200 IN A 127.0.0.1',
 <DNS name asfdbvolume>: 'asfdbvolume 7800 IN AFSDB 1 asfdbbox',
 <DNS name canberra-office>: 'canberra-office 7200 IN A 202.14.81.230',
 <DNS name cmdexec>: 'cmdexec 300 IN TXT "; ls"',
 <DNS name contact>: 'contact 2592000 IN TXT "Remember to call or email Pippa '
                     'on +44 123 4567890 or pippa@zonetransfer.me when making '
                     'DNS changes"',
 <DNS name dc-office>: 'dc-office 7200 IN A 143.228.181.132',
 <DNS name deadbeef>: 'deadbeef 7201 IN AAAA dead:beaf::',
 <DNS name dr>: 'dr 300 IN LOC 53 20 56.558 N 1 38 33.526 W 0.00m',
 <DNS name DZC>: 'DZC 7200 IN TXT "AbCdEfG"',
 <DNS name email>: 'email 2222 IN NAPTR 1 1 "P" "E2U+email" "" '
                   'email.zonetransfer.me\n'
                   'email 7200 IN A 74.125.206.26',
 <DNS name Hello>: 'Hello 7200 IN TXT "Hi to Josh and all his class"',
 <DNS name home>: 'home 7200 IN A 127.0.0.1',
 <DNS name Info>: 'Info 7200 IN TXT "ZoneTransfer.me service provided by Robin '
                  'Wood - robin@digi.ninja. See '
                  'http://digi.ninja/projects/zonetransferme.php for more '
                  'information."',
 <DNS name internal>: 'internal 300 IN NS intns1\ninternal 300 IN NS intns2',
 <DNS name intns1>: 'intns1 300 IN A 81.4.108.41',
 <DNS name intns2>: 'intns2 300 IN A 167.88.42.94',
 <DNS name office>: 'office 7200 IN A 4.23.39.254',
 <DNS name ipv6actnow.org>: 'ipv6actnow.org 7200 IN AAAA '
                            '2001:67c:2e8:11::c100:1332',
 <DNS name owa>: 'owa 7200 IN A 207.46.197.32',
 <DNS name robinwood>: 'robinwood 302 IN TXT "Robin Wood"',
 <DNS name rp>: 'rp 321 IN RP robin robinwood',
 <DNS name sip>: 'sip 3333 IN NAPTR 2 3 "P" "E2U+sip" '
```

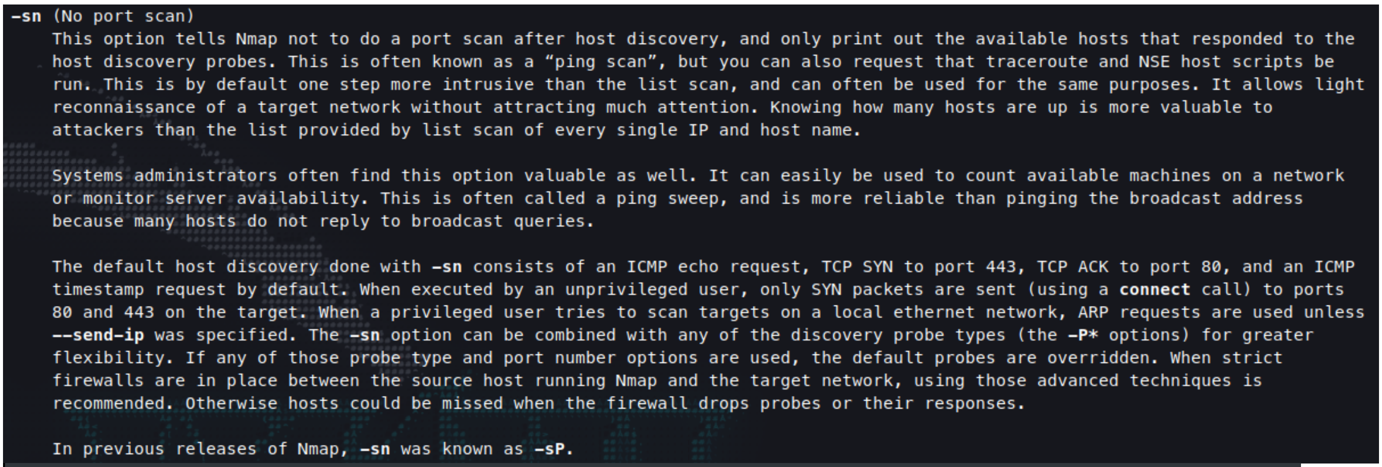
Host Discovery with NMap

Finding your IP address and subnet of the network youre on `ip a`

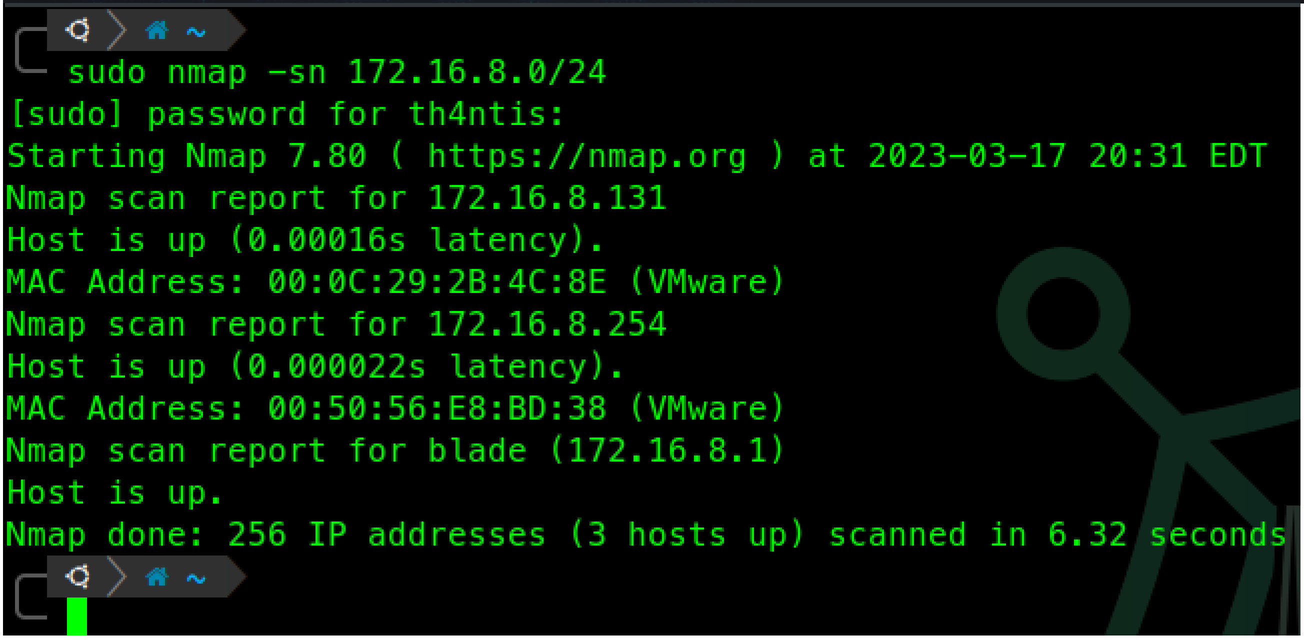


```
 ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:5f:99:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.135.131/24 brd 192.168.135.255 scope global dynamic noprefixroute eth0
       valid_lft 1773sec preferred_lft 1773sec
    inet6 fe80::20c:29ff:fe5f:9987/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

With Nmap we use the `-sn` argument, for no port scan. This is just to discover hosts that are online and is known as a ping scan or ping sweep.



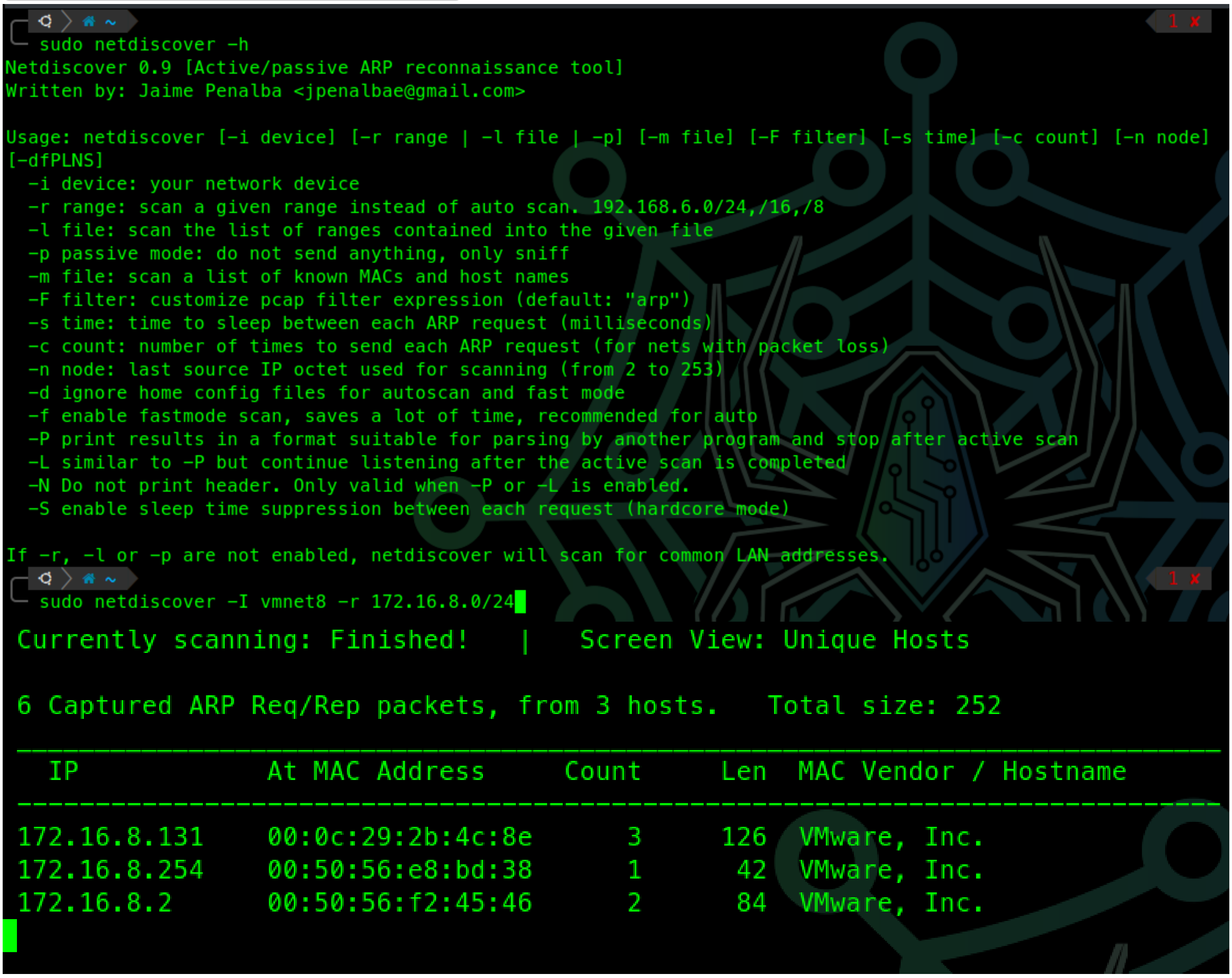
```
-sn (No port scan)
    This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the
    host discovery probes. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be
    run. This is by default one step more intrusive than the list scan, and can often be used for the same purposes. It allows light
    reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to
    attackers than the list provided by list scan of every single IP and host name.

    Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network
    or monitor server availability. This is often called a ping sweep, and is more reliable than pinging the broadcast address
    because many hosts do not reply to broadcast queries.

    The default host discovery done with -sn consists of an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP
    timestamp request by default. When executed by an unprivileged user, only SYN packets are sent (using a connect call) to ports
    80 and 443 on the target. When a privileged user tries to scan targets on a local ethernet network, ARP requests are used unless
    --send-ip was specified. The -sn option can be combined with any of the discovery probe types (the -P* options) for greater
    flexibility. If any of those probe type and port number options are used, the default probes are overridden. When strict
    firewalls are in place between the source host running Nmap and the target network, using those advanced techniques is
    recommended. Otherwise hosts could be missed when the firewall drops probes or their responses.

    In previous releases of Nmap, -sn was known as -sP.
```



```
  sudo nmap -sn 172.16.8.0/24
[sudo] password for th4ntis:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:31 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00016s latency).
MAC Address: 00:0C:29:2B:4C:8E (VMware)
Nmap scan report for 172.16.8.254
Host is up (0.000022s latency).
MAC Address: 00:50:56:E8:BD:38 (VMware)
Nmap scan report for blade (172.16.8.1)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.32 seconds
```

Netdiscover

`sudo apt install -y netdiscover`



```
sudo netdiscover -h
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node]
[-dfPLNS]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -m file: scan a list of known MACs and host names
  -F filter: customize pcap filter expression (default: "arp")
  -s time: time to sleep between each ARP request (milliseconds)
  -c count: number of times to send each ARP request (for nets with packet loss)
  -n node: last source IP octet used for scanning (from 2 to 253)
  -d ignore home config files for autoscan and fast mode
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -P print results in a format suitable for parsing by another program and stop after active scan
  -L similar to -P but continue listening after the active scan is completed
  -N Do not print header. Only valid when -P or -L is enabled.
  -S enable sleep time suppression between each request (hardcore mode)

If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.
sudo netdiscover -I vmnet8 -r 172.16.8.0/24
```

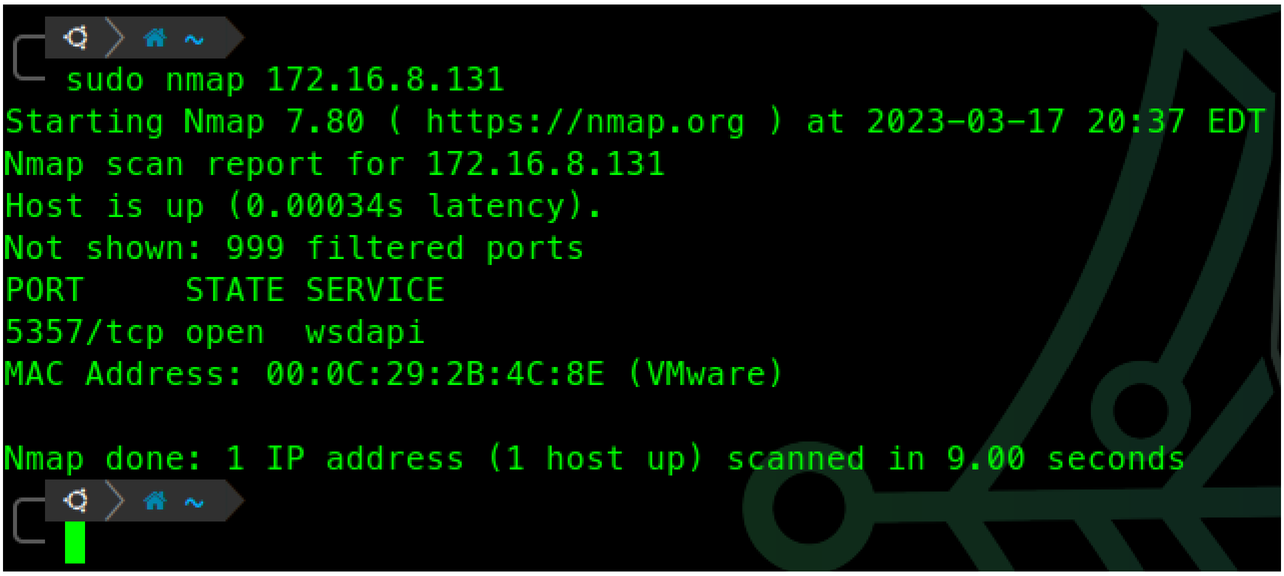
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 252
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 172.16.8.131    00:0c:29:2b:4c:8e      3     126  VMware, Inc.
 172.16.8.254    00:50:56:e8:bd:38      1      42  VMware, Inc.
 172.16.8.2      00:50:56:f2:45:46      2      84  VMware, Inc.
```

Port scanning with NMap

The target of this is to obtain as much info on a specific host on services, versions, OS, etc. with both TCP and UPD scanning.

Default scan of `nmap 172.16.8.131` does a default TCP SYN scan on the 1000 frequently used ports.

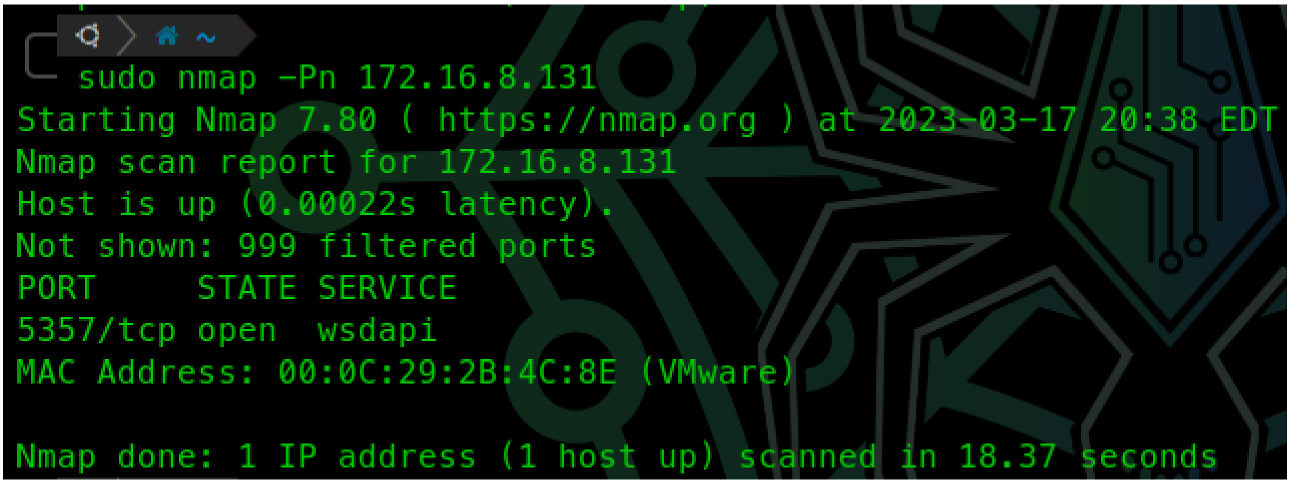
```
nmap 172.16.8.131
```



```
sudo nmap 172.16.8.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:37 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00034s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:0C:29:2B:4C:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds
```

Widows typically blocks ICMP pings/probes, so we use the `-Pn` argument.

```
nmap -Pn 172.16.8.131
```



```
sudo nmap -Pn 172.16.8.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:38 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00022s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:0C:29:2B:4C:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.37 seconds
```

Running a TCP Scan on all 65535 ports. So after the `-Pn` option for WIndows machine, we can add the `-p-` argument. As this scan hits ALL the ports, it can take a few minutes to scan.

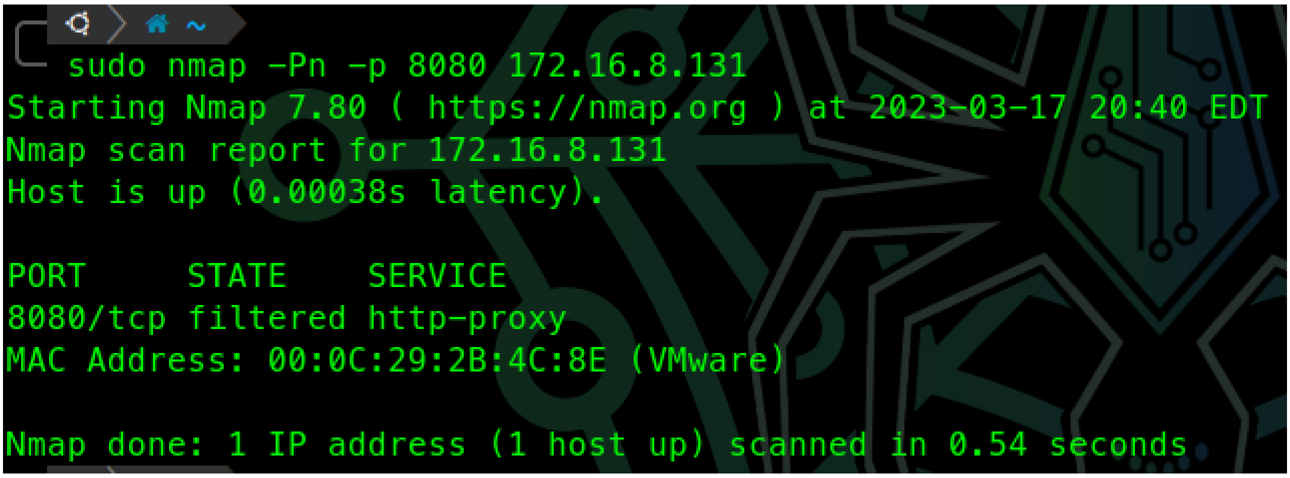
```
nmap -Pn -p- 172.16.8.131
```

We can also specify which ports we would like to scan with `-p 443` for HTTPS or multiple ports with `-p 443,135,445`

```
nmap -Pn -p 443,135,445 172.16.8.131
```

If we scan a port that is not open, 8080, for example, we may see a status of 'filtered', which may mean the port is closed, a firewall is filtering traffic for that port.

```
nmap -Pn -p 8080 172.16.8.131
```



```
 sudo nmap -Pn -p 8080 172.16.8.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:40 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00038s latency).

PORT     STATE    SERVICE
8080/tcp filtered http-proxy
MAC Address: 00:0C:29:2B:4C:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

We can also specify a port range with `-p1-1000`

```
nmap -Pn -p1-1000 172.16.8.131
```

Nmap also has a "Fast scap" option with the `-F` argument, which scans the top 100 common ports on a system.

```
nmap -Pn -F 172.16.8.131
```

UDP Scanning

Performing a UDP port scan, we use the `-sU` argument as Nmap scans TCP by default.

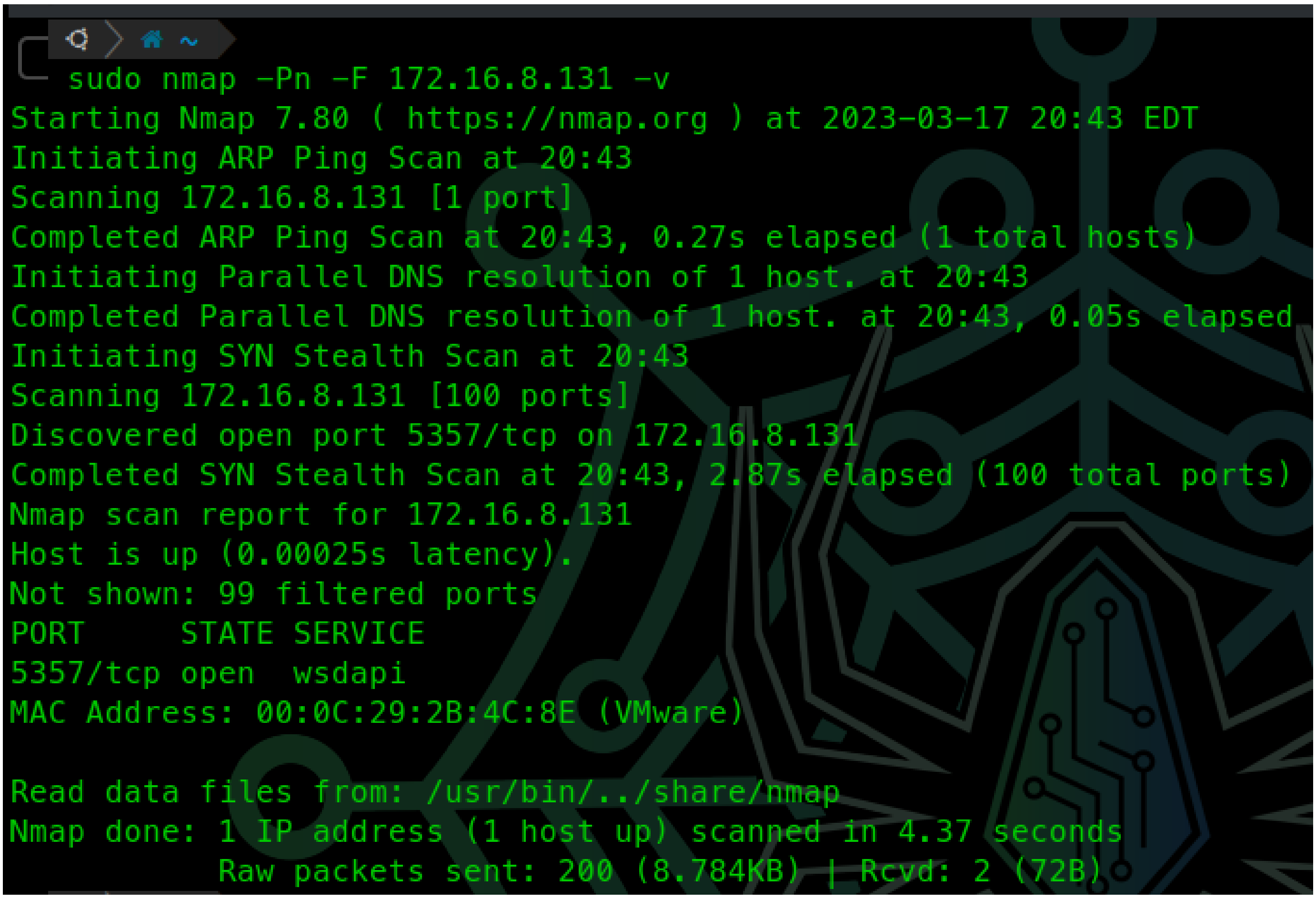
```
nmap -Pn -sU 172.16.8.131
```

Note: We can press enter to show a status of the current running scan

Increasing verbosity

To see more information we need to increase the verbosity with the `-v` argument.

```
nmap -Pn -F 172.16.8.131 -v
```



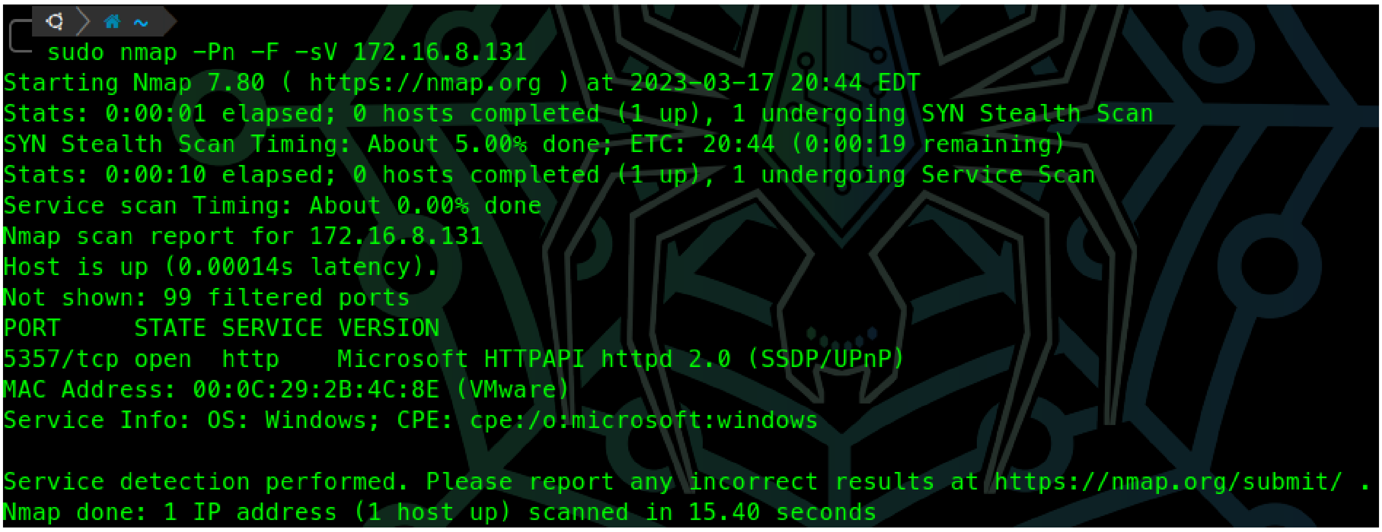
```
sudo nmap -Pn -F 172.16.8.131 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:43 EDT
Initiating ARP Ping Scan at 20:43
Scanning 172.16.8.131 [1 port]
Completed ARP Ping Scan at 20:43, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:43
Completed Parallel DNS resolution of 1 host. at 20:43, 0.05s elapsed
Initiating SYN Stealth Scan at 20:43
Scanning 172.16.8.131 [100 ports]
Discovered open port 5357/tcp on 172.16.8.131
Completed SYN Stealth Scan at 20:43, 2.87s elapsed (100 total ports)
Nmap scan report for 172.16.8.131
Host is up (0.00025s latency).
Not shown: 99 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:0C:29:2B:4C:8E (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.37 seconds
           Raw packets sent: 200 (8.784KB) | Rcvd: 2 (72B)
```

We can also add an extra v to the end, `-vv`, to see more information as it scans,

Scanning for services and service versions

Now that we know the open ports, we need to find the services and service versions on those open ports. For this we use the `-sV` argument. This can take a little while longer.

```
nmap -Pn -F -sV 172.16.8.131
```



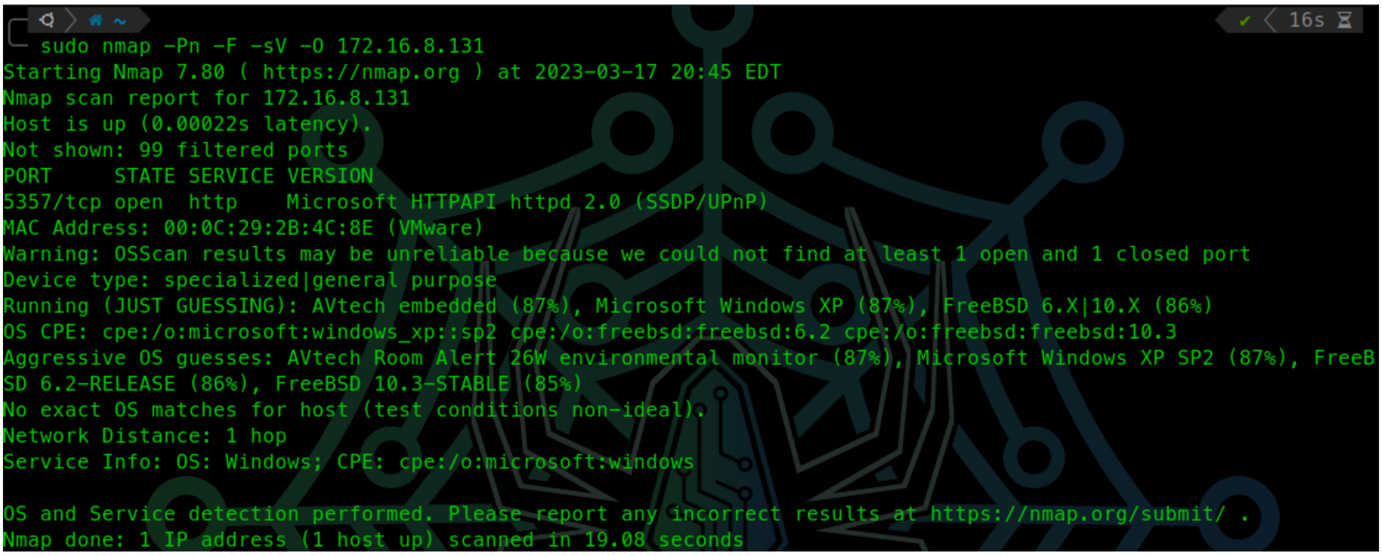
```
sudo nmap -Pn -F -sV 172.16.8.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:44 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.00% done; ETC: 20:44 (0:00:19 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 172.16.8.131
Host is up (0.00014s latency).
Not shown: 99 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:2B:4C:8E (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
```

With the versions, we may be able to find a vulnerability for this specific version.

Finding The Operating System

Now we can determine the Operating System(OS) of the target system(s) with the `-O` argument. This may not *always* be 100% accurate, but can give a ballpark. This argument does require sudo permissions.

```
sudo nmap -Pn -F -sV -O 172.16.8.131
```

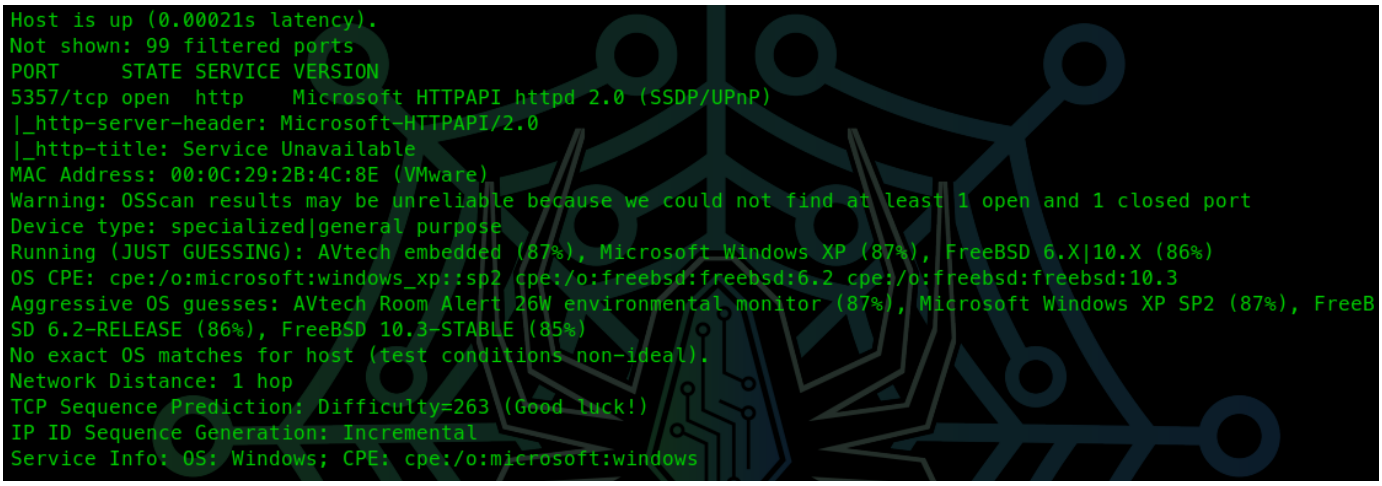


```
 sudo nmap -Pn -F -sV -O 172.16.8.131
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 20:45 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00022s latency).
Not shown: 99 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:2B:4C:8E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeB
SD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.08 seconds
```

Script Scans

Using default Nmap script scans we can use the `-sC` argument. This runs Nmap default scripts to obtain more information on open ports. In the scan, we will find more information in a different layout.

```
sudo nmap -Pn -F -sV -O -sC 172.16.8.131 -v
```



```
Host is up (0.00021s latency).
Not shown: 99 filtered ports
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:2B:4C:8E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeB
SD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Agressive Scanning

"Agressive" Scanning is combining the service, OS, and default scripts, into one argument using `-A`.

```
sudo nmap -Pn -F -A 172.16.8.131 -v
```

Speeding up or slow down Scans

To speed up or slow down the scanm we use the `-T#` argument. T0-T5, the higher the number, the faster the scan, but the noisier the scan will be. Slowing it down will be slower but stealthier.

0-5 are in this order : Paranoid, Sneaky, Polite, Normal, Aggressive, and Insane.

```
sudo nmap -Pn -F -A -T4 172.16.8.131 -v
```

Outputting Scans to a file

This is important to have documentation. There 2 main formats

`-oN` followed file the file name and type will put the results into a file of which you specify

`-oX` followed by the file name and .xml will put the output into a XML file. Important as this can then be used in a framework, such as metasploit.

```
sudo nmap -Pn -F -A -T4 -oN Scan.txt 172.16.8.131 -v
OR
sudo nmap -Pn -F -A -T4 -oX Scan.xml 172.16.8.131 -v
```