Colby Heilner
Professor Torres
2/15
IT 140
Lab 3

You have been contracted to conduct an Active/Passive information gathering engagement against the below targets. You are ONLY authorized to utilize the below tools. Do not exceed the limits of this Scope.

ELsfoo

Exploit-DB

Megacorpone

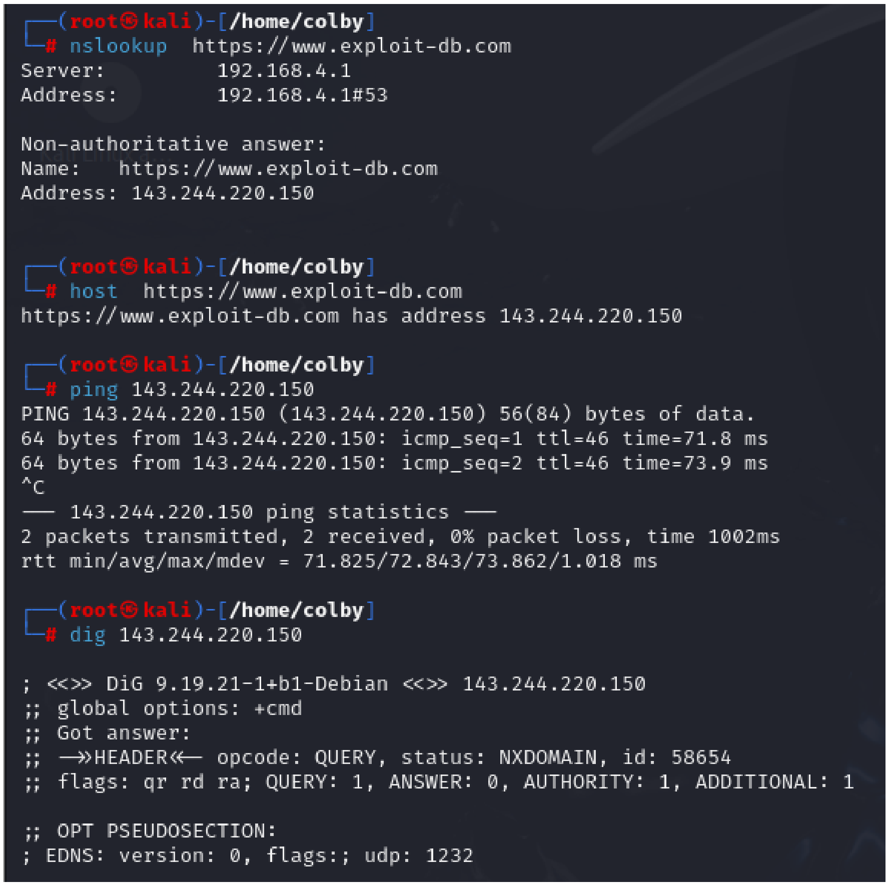
Part A:

Use the below tools (at least 15 of them) and techniques to gather information from the above sites:

- Ping
- traceroute/tracert
- nslookup
- host
- dig
- dnsenum
- dnsmap
- dnsrecon
- zonetransfer-- perform a zone transfer with 3 tools against zonetransfer.me
- wget-- Downlaod megacorpone.com or elsfoo.com site
- curl-- Download megacorpone.com or elsfoo.com site
- Shodan

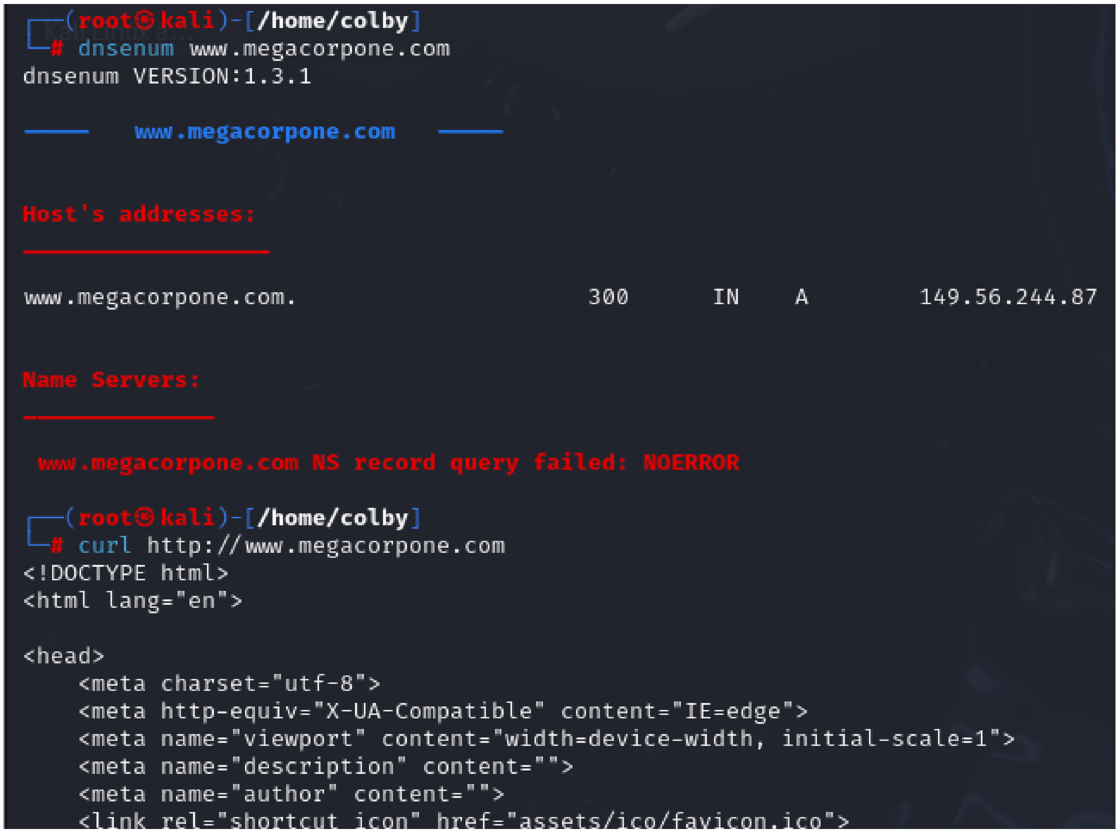
- Fierce
- DMitry
- Netcraft
- Maltego
- FOCA
- Google Hacking Database
- Metagoofil
- Exiftool
- Sublist3r
- recon-ng

host, ping, dig, nslookup

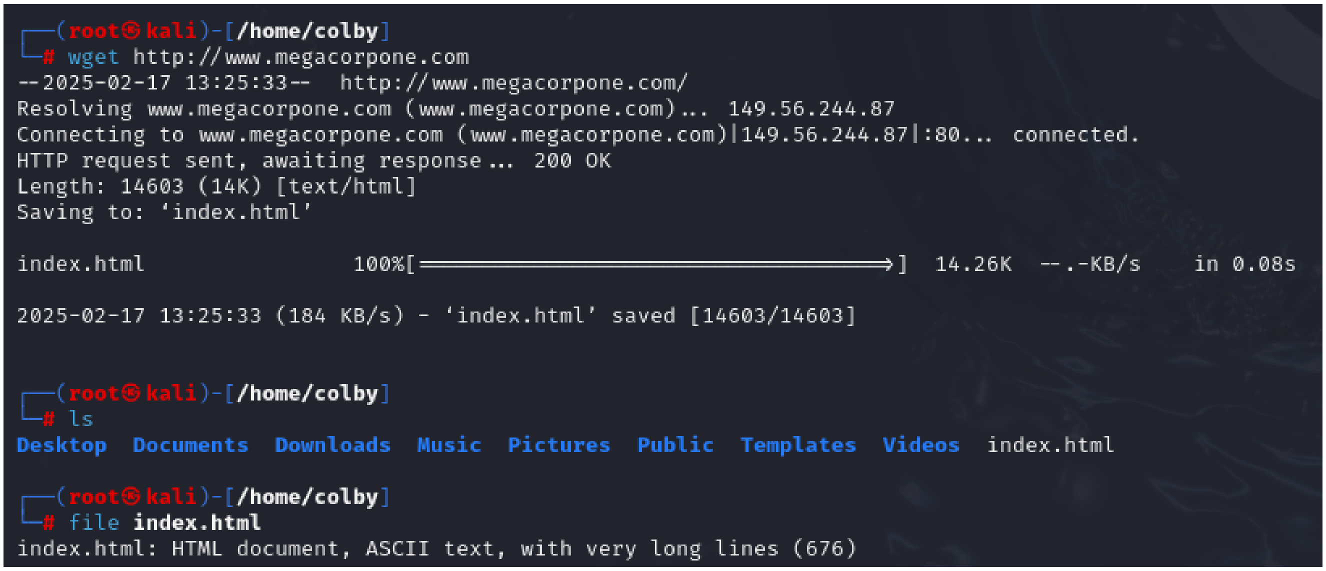


```
┌──(root㉿kali)-[/home/colby]
└─# nslookup  https://www.exploit-db.com
Server:         192.168.4.1
Address:        192.168.4.1#53

Non-authoritative answer:
Name:   https://www.exploit-db.com
Address: 143.244.220.150


┌──(root㉿kali)-[/home/colby]
└─# host  https://www.exploit-db.com
https://www.exploit-db.com has address 143.244.220.150

┌──(root㉿kali)-[/home/colby]
└─# ping 143.244.220.150
PING 143.244.220.150 (143.244.220.150) 56(84) bytes of data.
64 bytes from 143.244.220.150: icmp_seq=1 ttl=46 time=71.8 ms
64 bytes from 143.244.220.150: icmp_seq=2 ttl=46 time=73.9 ms
^C
--- 143.244.220.150 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 71.825/72.843/73.862/1.018 ms

┌──(root㉿kali)-[/home/colby]
└─# dig 143.244.220.150

; <<>> DiG 9.19.21-1+b1-Debian <<>> 143.244.220.150
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 58654
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
```

Dnsenum, curl, wget

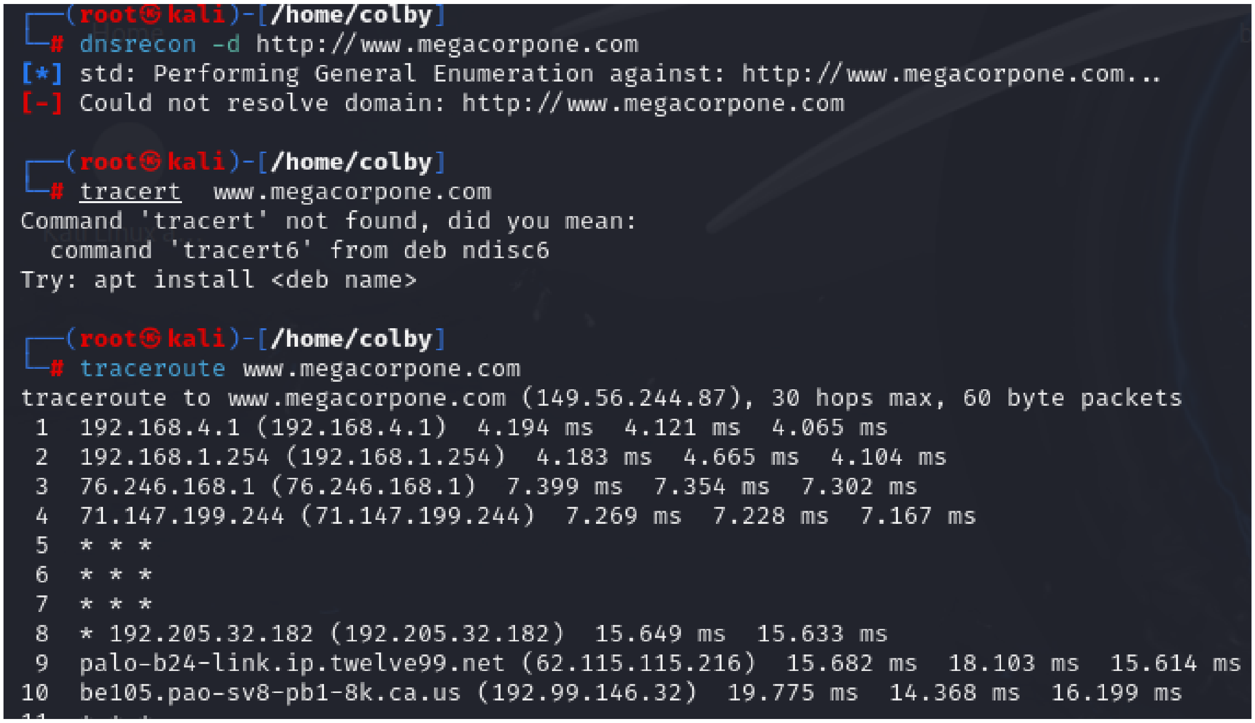


```
┌──(root㉿kali)-[/home/colby]
└─# dnsenum www.megacorpone.com
dnsenum VERSION:1.3.1

─────   www.megacorpone.com   ─────


Host's addresses:
__________________

www.megacorpone.com.                    300      IN    A        149.56.244.87


Name Servers:
______________

 www.megacorpone.com NS record query failed: NOERROR

┌──(root㉿kali)-[/home/colby]
└─# curl http://www.megacorpone.com
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">
    <link rel="shortcut icon" href="assets/ico/favicon.ico">
```



```
┌──(root㉿kali)-[/home/colby]
└─# wget http://www.megacorpone.com
--2025-02-17 13:25:33--  http://www.megacorpone.com/
Resolving www.megacorpone.com (www.megacorpone.com)... 149.56.244.87
Connecting to www.megacorpone.com (www.megacorpone.com)|149.56.244.87|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14603 (14K) [text/html]
Saving to: ‘index.html’

index.html              100%[====================================>]  14.26K  --.-KB/s    in 0.08s

2025-02-17 13:25:33 (184 KB/s) - ‘index.html’ saved [14603/14603]


┌──(root㉿kali)-[/home/colby]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  index.html

┌──(root㉿kali)-[/home/colby]
└─# file index.html
index.html: HTML document, ASCII text, with very long lines (676)
```

Tracert, dnsrecon

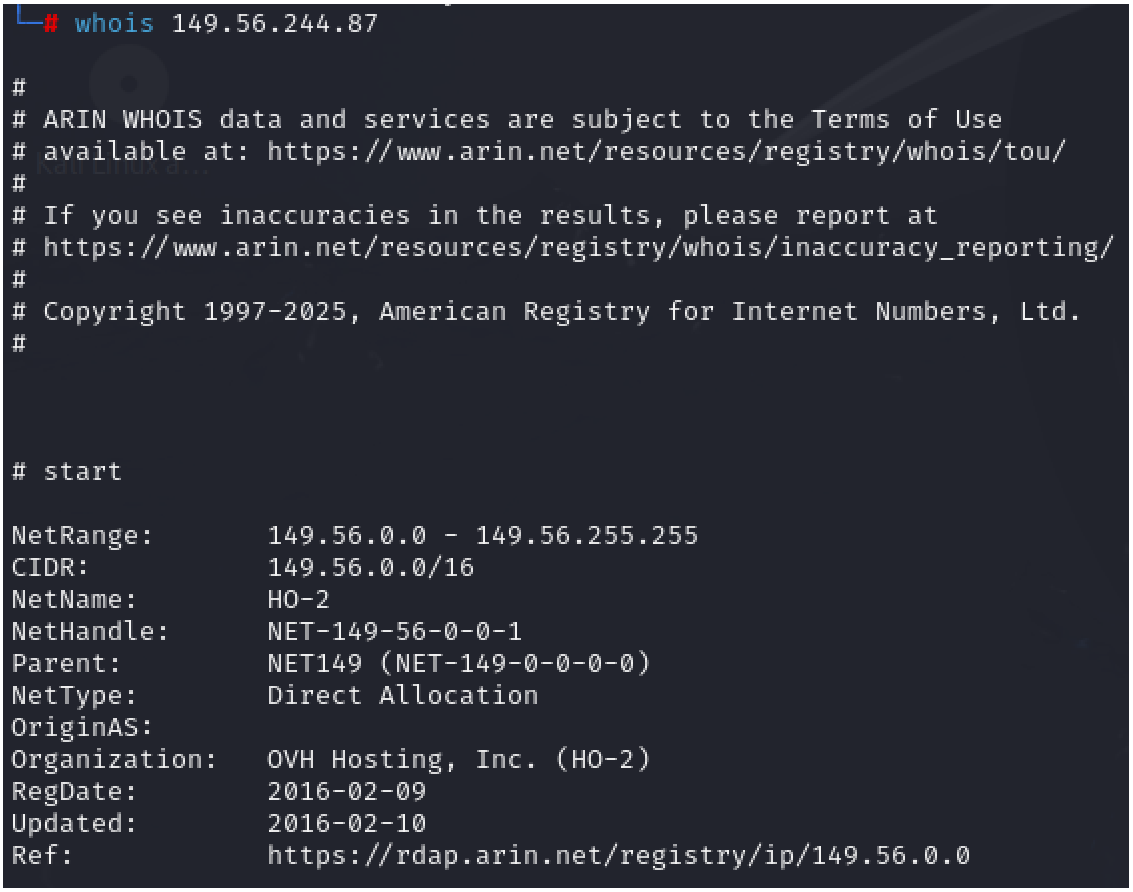


```
┌──(root㉿kali)-[/home/colby]
└─# dnsrecon -d http://www.megacorpone.com
[*] std: Performing General Enumeration against: http://www.megacorpone.com...
[-] Could not resolve domain: http://www.megacorpone.com

┌──(root㉿kali)-[/home/colby]
└─# tracert  www.megacorpone.com
Command 'tracert' not found, did you mean:
  command 'tracert6' from deb ndisc6
Try: apt install <deb name>

┌──(root㉿kali)-[/home/colby]
└─# traceroute www.megacorpone.com
traceroute to www.megacorpone.com (149.56.244.87), 30 hops max, 60 byte packets
 1  192.168.4.1 (192.168.4.1)  4.194 ms  4.121 ms  4.065 ms
 2  192.168.1.254 (192.168.1.254)  4.183 ms  4.665 ms  4.104 ms
 3  76.246.168.1 (76.246.168.1)  7.399 ms  7.354 ms  7.302 ms
 4  71.147.199.244 (71.147.199.244)  7.269 ms  7.228 ms  7.167 ms
 5  * * *
 6  * * *
 7  * * *
 8  * 192.205.32.182 (192.205.32.182)  15.649 ms  15.633 ms
 9  palo-b24-link.ip.twelve99.net (62.115.115.216)  15.682 ms  18.103 ms  15.614 ms
10  be105.pao-sv8-pb1-8k.ca.us (192.99.146.32)  19.775 ms  14.368 ms  16.199 ms
```

Part B:

- Using the above details, try to find 1 IP address from your research that belongs directly to your target. Is it possible? (why/why-not).

  Not sure, the one Ip a found a lot belongs to OVH 149.56.244.87. I do not see why it would not be possible. If the company hosts on prem web servers I believe they would then "own" the IP.



```
└─# whois 149.56.244.87

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       149.56.0.0 - 149.56.255.255
CIDR:           149.56.0.0/16
NetName:        HO-2
NetHandle:      NET-149-56-0-0-1
Parent:         NET149 (NET-149-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   OVH Hosting, Inc. (HO-2)
RegDate:        2016-02-09
Updated:        2016-02-10
Ref:            https://rdap.arin.net/registry/ip/149.56.0.0
```

- List 10 other tools that can be used for Active Information Gathering (not scanning tools)

theHarvester

Maltego

FOCA

Netcraft

Recon-ng

Metagoofil

SpiderFoot

Shodan

Censys

Whois Lookup

Part C:

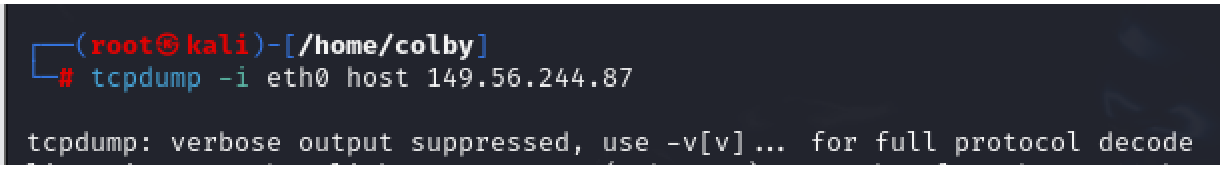
- Which tool created the most noise on the network?

  For me it would have been dnsenum.

- Which tool created the least amount of noise on the network?.

  Most likely whois lookup, because they are still considered passive

- What tcpdump command did you use to narrow down the target of your packet capture for the above scans?



```
┌──(root㉿kali)-[/home/colby]
└─# tcpdump -i eth0 host 149.56.244.87

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
```