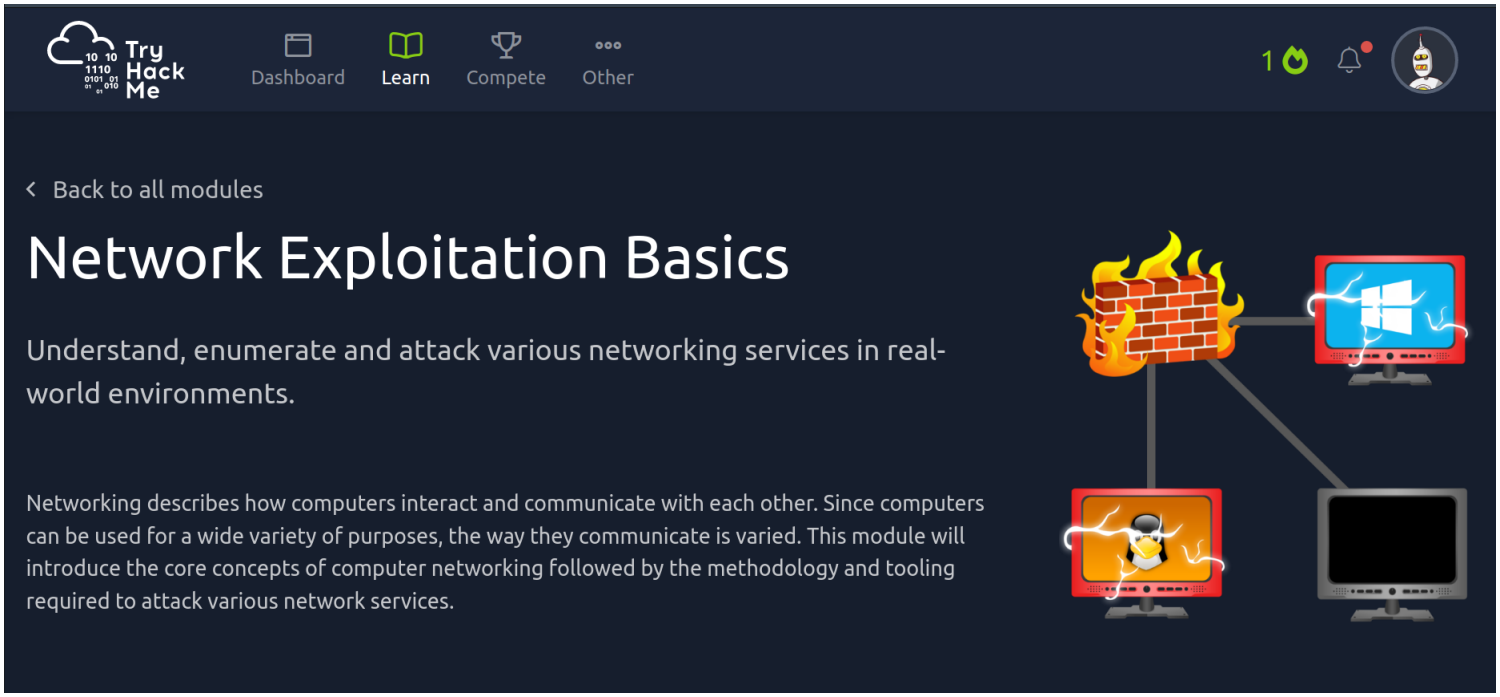
Network Exploitation Basics



Introductory Networking

The aim of this room is to provide a beginner's introduction to the basic principles of networking. Networking is a *massive* topic, so this really will just be a brief overview; however, it will hopefully give you some foundational knowledge of the topic, which you can build upon for yourself.

The topics that we're going to cover in this room are:

- The OSI Model
- The TCP/IP Model
- How these models look in practice
- An introduction to basic networking tools

OSI Model Overview

The OSI (**O**pen **S**ystems **I**nterconnection) Model is a standardised model which we use to demonstrate the theory behind computer networking. In practice, it's actually the more compact TCP/IP model that real-world networking is based off; however the OSI model, in many ways, is easier to get an initial understanding from.
The OSI model consists of seven layers:

OSI:
Application
Presentation
Session
Transport
Network
Data Link
Physical

Layer 7 - Application Layer :

→ provides networking options to program running over a computer
→ works exclusively on applications , provide interface for them to use , in order to transmit data
→ then it passes to layer 6 , that is presentation layer.

Layer 6 - Presentation Layer :

→ it recieves data from application layer
→ the data recieved is in the format that application understands , but not standardized to be understood by application layer on receiving computer
→ it makes the data standardized in format
→ it does encryption , compression and other transformation
→ then it is passed to layer 5 , that is Session layer

Layer 5 - Session Layer :

→ it takes formatted data from Presentation Layer
→ it sets up a connection with other computer , across the network
→ if connection is not made or there is an error , process goes no further and stops here
→ is session is made sucessfully , then this layer maintains it
→ it works hand in hand with session layer of recieving computer across the network i.e by syncronising communications
→ session is always unique in every communication , so that we can make multiple requests to different endpoints without data getting mixed up
→ once this session is successful the data is passed on to the next layer that is Layer 4 - Transport layer

Layer 4 - Transport Layer :

→ so it performs various important functions
→ first it selects the protocol over which the data will be transmitted
→ two most common protocols are :
⇒ TCP : Transmission Control Protocol - connection oriented , reliable , if packets are lost, they are re-sent ex - websites loading
⇒ UDP : User Datagram Protocol - connection-less protocol , less reliable , if packets are lost , they are lost. ex- video streaming
→ then it divides the data in byte-sized packets and then they are moved to next layer . in TCP it is called segment, in UDP it is called datagrams

Layer 3 - Network Layer :

→ it is responsible for location destination of our request
→ it finds the best route to reach a network using IPv4 or IPv6 addresses
→ it is based on logical addressing

Layer 2 - Data Link Layer :

→ it is based on physical addressing of transmission
→ it takes packet from network layer and adds an MAC address to it for the reciever
→ each device has a unique hardcoded MAC address
→ it is also duty of this layer to present data in a format suitable for transmission
→ when this layer recieves data it also checks data for currouppted data

Layer 1 - Physical Layer :

→ it basically refer to the hardware used for transmission , ex- ethernet cable
→ it converts binary data to signals while sending and vice versa while receiving

Encapsulation

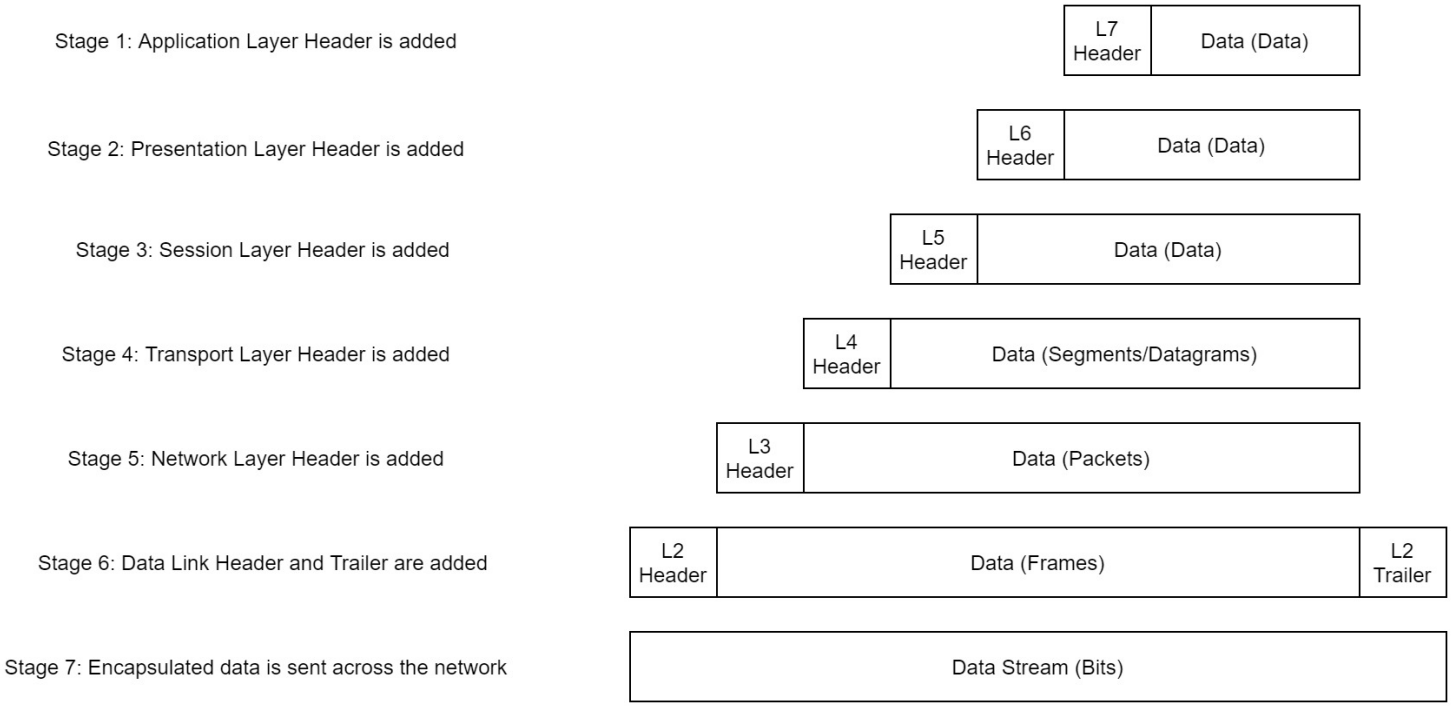
so , as the data is being passed out from one layer to another , layer specific details are added to the start of the transmission

the data added into these packets are called headers ,

• for example header of network layer will contain IP addresses from source to destination etc.

• header of transport layer includes data relation to protocol used , that can be wither TCP or UDP .

so at each layer the data gets a header and at each layer data gets a different name which is hown in the diagram below :



so basically this process of adding layers to the data at each layer till it reaches the last layer is called encapsulation

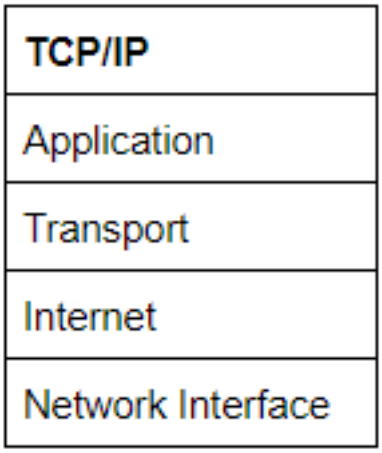
while recieving the data , each header is removed one by one till it reaches the top layer and this process of removing of headers is called de-encapsulation

this basically standardize the process of transfer of data across network

TCP/IP Model

okay so, TCP/IP model is the model that is actually used in modern days networking , as it is the accepted standard of today

TCP/IP layer looks like this :



it consist of 4 layers , but it cover the same range of functions as seven layers of OSI model

• some recent sources split this model into 5 layers breaking the network interface into 2 parts i.e :

◇ Data Link
◇ Physical Layer
* just like OSI model did

but the official guide (RFC1122) describes only 4 layers shown in the diagram above

what basically done in TCP/IP model is that layers are merged in one another like this :

OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link	Network Interface
Physical	

• Data Link and Physical Layer is merged into one Network Interface Layer

• Application Layer , Presentation Layer , Session Layer these three are merged into one Application Layer

we study OSI Layer for learning purposes only *

then there comes TCP protocol in TCP/IP model which we will look :

so TCP is a connection0oriented protocol that means it first forms a connection with the reciever .

the connection is made using a handshake called TCP-3-Way Handshake , lets look at it :

so lets understand what does a handshake look like and how it flows ,

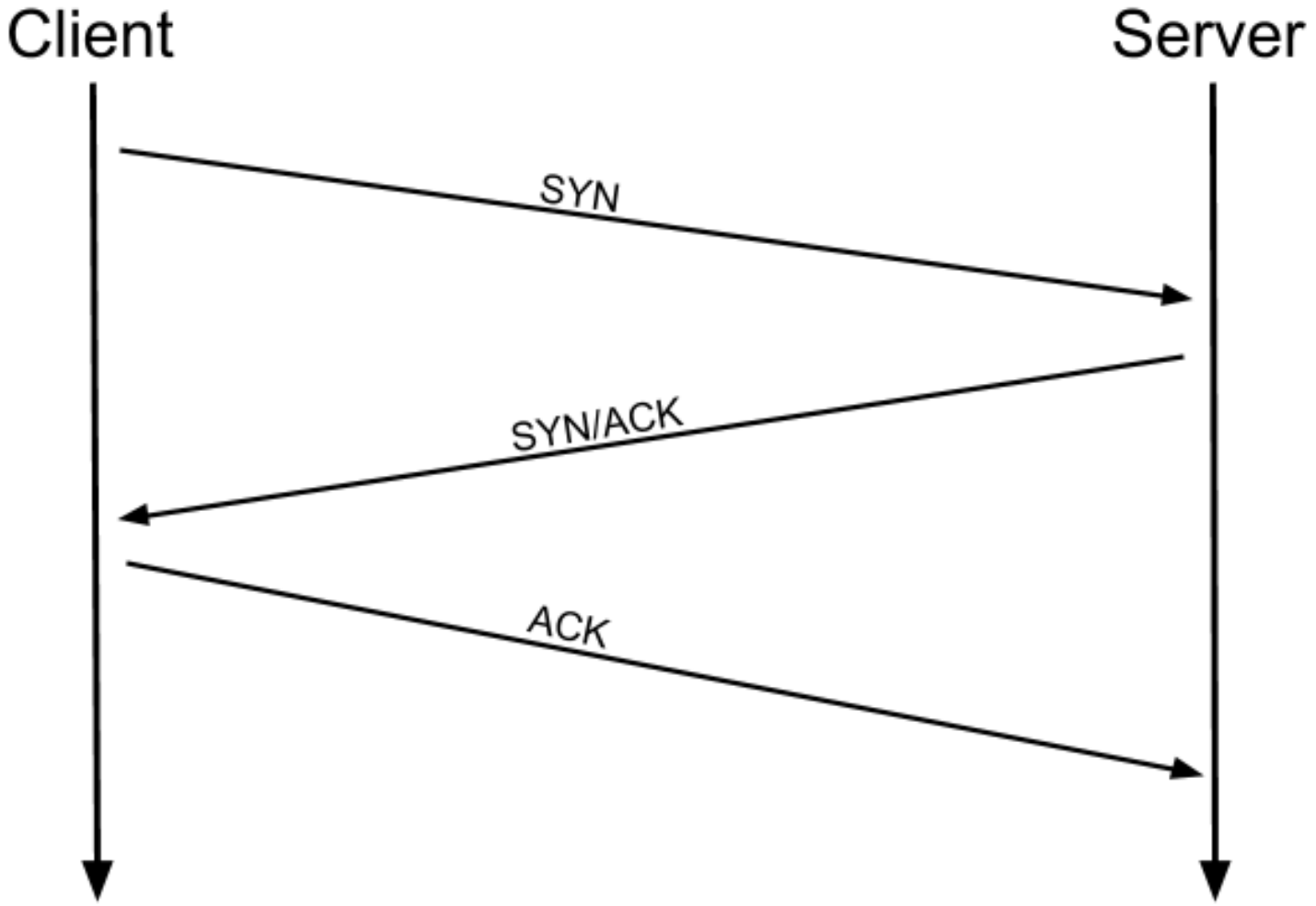
so in this handshake network send packets , each packet has a unique bit set in it , bits are like flags or simply indicators

• so the first packet send is a SYN packet that SYN stands for synchronise , which basically indicate we want to initialize a connection to remote endpoint

• then the server or remote endpoint replies with a SYN-ACK packet that means synchronise-acknowledge , that means syn has been acknowledged

• then at last we send a ACK packet , for confirming that the connection has been set up successfully and now data can be exchanged seamlessly

to visualize the concept look at this :



Ping

so what is Ping ?

ping is a tool that we used to test wether a connection to a remote endpoint is possible or not .

it can be a website over the internet or a remote device like PC .

Ping works on ICMP protocol .

example :

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ping www.google.com
PING www.google.com (172.217.27.164) 56(84) bytes of data.
64 bytes from del11s03-in-f4.1e100.net (172.217.27.164): icmp_seq=1 ttl=118 time=5.20 ms
64 bytes from kix05s07-in-f4.1e100.net (172.217.27.164): icmp_seq=2 ttl=118 time=11.9 ms
64 bytes from kix05s07-in-f164.1e100.net (172.217.27.164): icmp_seq=3 ttl=118 time=6.49 ms
64 bytes from kix05s07-in-f164.1e100.net (172.217.27.164): icmp_seq=4 ttl=118 time=8.50 ms
64 bytes from kix05s07-in-f4.1e100.net (172.217.27.164): icmp_seq=5 ttl=118 time=4.52 ms
64 bytes from kix05s07-in-f164.1e100.net (172.217.27.164): icmp_seq=6 ttl=118 time=13.8 ms
64 bytes from kix05s07-in-f164.1e100.net (172.217.27.164): icmp_seq=7 ttl=118 time=6.03 ms
^C
── www.google.com ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6363ms
rtt min/avg/max/mdev = 4.523/8.068/13.816/3.284 ms
```

we get ICMP echo replies back with a time , that means that google is accessible ,

we can also see the IP address of google , ping can be used to get IP address of a server

Ping is mostly enabled by default on all devices ,

Traceroute

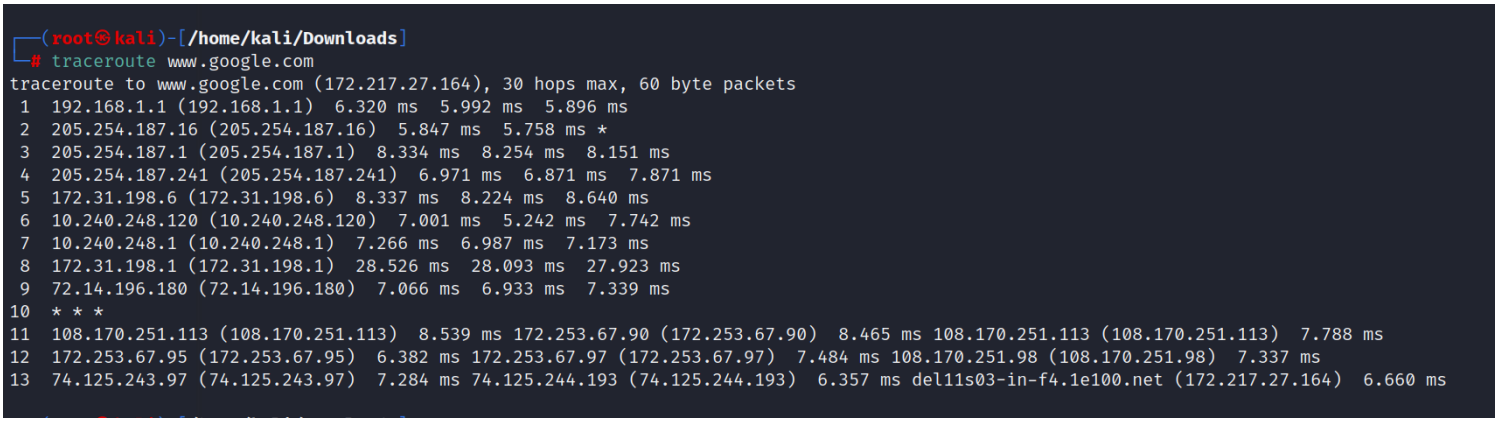
traceroute utility can be used to map our path to a target server ,

in simplet terms when we connect to a endpoint , we have to go through other routers and machines ,

we can use traceroute command to see those routers and machines , in between our connection .

in windoes the tool is called : “tracert”

example :



Whois

so what happens is when we visit a website we enter its domain name ,

for example www.google.com - in which the domain is google

which then with the help of DNS servers gets converted into an valid IP address and we are able to visit the website .

so these domain names are purchased by companies , website owners and these domain registrar information is stored in a databse .

we can use "Whois" tool to look for that database and gain valuable information

example :

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2022-01-26T16:45:06Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2031-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-06-06T13:43:13Z <<<
```

Dig

so lets first understand about DNS and what does it do and how does it work .

so when we enter a domain name , it gets converted to a IP adderess using DNS (Domain Name System)

lets understand DNS ,

at a basic level DNS allows us to ask a special server to give us the IP of the website we are trying to reach .

lets break this down further :

→ First the computer checks in its cache if the IP to a website is available or not .

if not ,

→ then it sends a request to a recursive DNS server , that is known to our router on our network in that cache it look for IP

if not found ,

⇒ then the recursive DNS server passes the request to root name server which relays our request to Top-Level Domain Servers

then each TLD server is divided by extensions like :

.com websites have a different TLD server

.co.uk have different TLD server

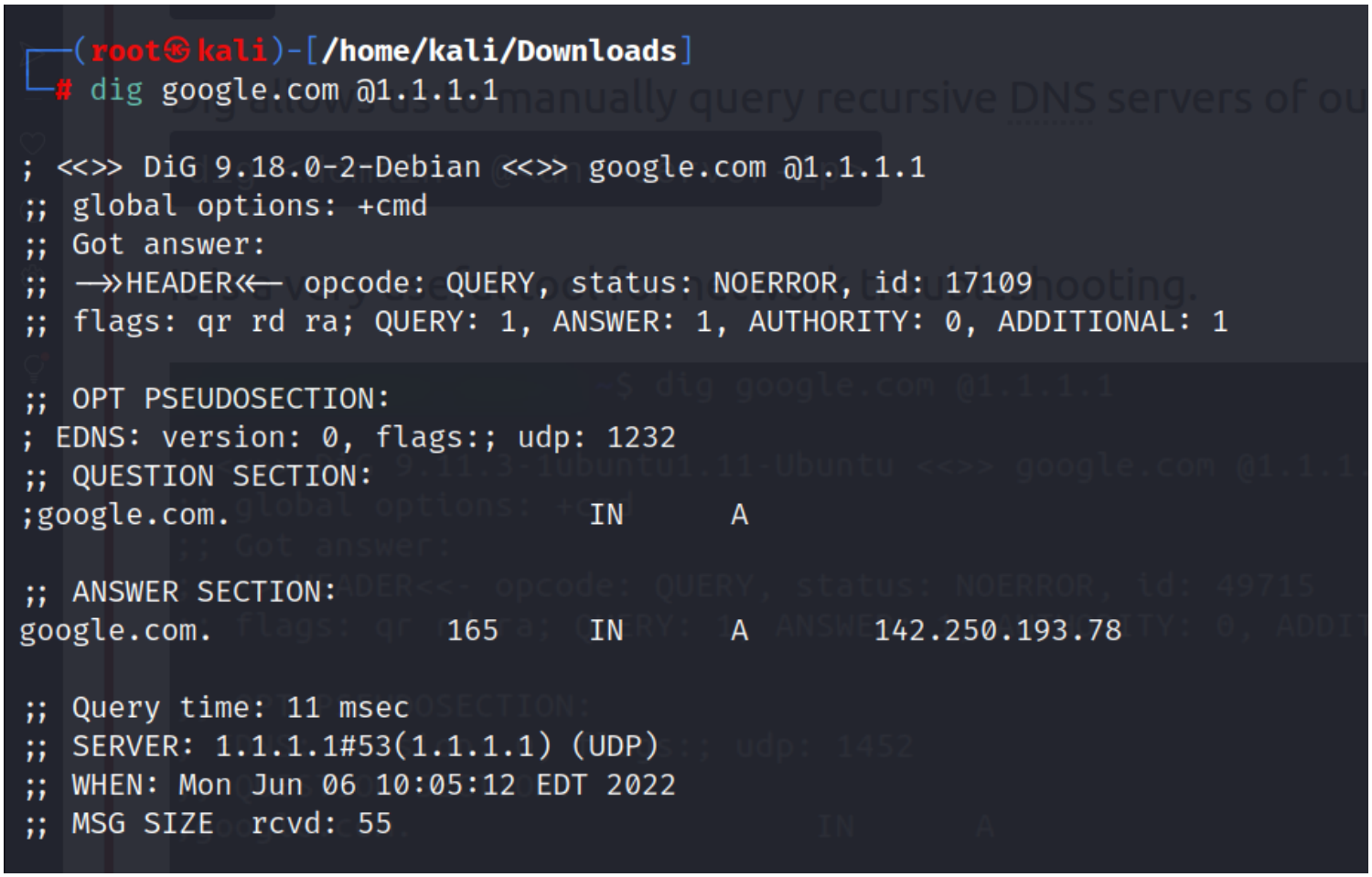
then at last there is a authoritative name server that store DNS records for domains directly

Authoritative name servers have DNS records for every website on the world that has a valid domain

---

we can use dig command to manually query recursive DNS servers .

example :



answer section gives us the IP information