ASSIGNMENT-02
COMPUTER NETWORKS
VINAYAKA GADAG

1. Load balancing refers to distributing incoming network traffic across multiple compute resources. How can DNS be used to load balance services? Give a concrete explanation for google.com

   Answer: Domain Name System is used to identify and resolve the IP addresses for hostnames and used to load balance the domains. “A domain can be a website, mail server, or another service that is accessible via the internet.” – (1)
   DNS load balancing is mainly used to distribute the load across the replicated servers. A replicated web servers are a set of IP addresses and associated with one canonical hostname. A canonical hostname is a name assigned to multiple aliases and a canonical hostname will return the resolved IP address when the aliases are accessed. All this process happens in a round-robin fashion. The addresses are picked and assigned based on the DNS rotation algorithm and it always returns the set of IP addresses, and the top of the IP address is picked from the set.
   Example: When we access the alias google.com, DNS query resolves it to a canonical hostname and internally canonical hostname will resolve it to one of the IP addresses from the set of IP addresses based on the user’s location using Google’s load-balance algorithm.

2. DNS has been around since 1985 and the core protocol is still being used today. What is the inherent weakness of DNS (as of RFC1035; excluding DNSSEC)? Give an example of how an attacker might utilize it.

   Answer: DNS’s inherent weakness is it’s recursive and hierarchical approach to resolve the hostname. There are different classes of attacks to DNS. “First type of attack is DDoS bandwidth-flooding attack” – (1). In this attack, attacker bombards the server with loads of packets and several legitimate packets never gets answered in this process. This will lead to an DNS server outage. “Another type of attack is ‘man-in-the-middle’ attack. In this attacker intercepts the DNS queries and sends the false replies to the server. This will lead the local DNS server to accept the bogus response into its cache and redirecting the web user to access the attacker’s website.” – (1)

3. Perform a manual iterative DNS query for mail-relay.iu.edu with dig starting from the root servers. List all commands and their outputs and explain why you issued every command. Do not use tracing features (dig +trace) for your final write-down.

   Answer: When we browse any website, DNS will recursively try to resolve the hostname.

- Here we are trying to go by iterative approach. In this process we will start by contacting the root server to get the domain server information.

```
[vinayakgadag@Vinayakas-MacBook-Pro] ~
❯ dig @d.root-servers.net edu q-A

; <<>> DiG 9.10.6 <<>> @d.root-servers.net edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7451
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1450
;; QUESTION SECTION:
;edu.                           IN      A

;; AUTHORITY SECTION:
edu.            172800  IN      NS      a.edu-servers.net.
edu.            172800  IN      NS      b.edu-servers.net.
edu.            172800  IN      NS      c.edu-servers.net.
edu.            172800  IN      NS      d.edu-servers.net.
edu.            172800  IN      NS      e.edu-servers.net.
edu.            172800  IN      NS      f.edu-servers.net.
edu.            172800  IN      NS      g.edu-servers.net.
edu.            172800  IN      NS      h.edu-servers.net.
edu.            172800  IN      NS      i.edu-servers.net.
edu.            172800  IN      NS      j.edu-servers.net.
edu.            172800  IN      NS      k.edu-servers.net.
edu.            172800  IN      NS      l.edu-servers.net.
edu.            172800  IN      NS      m.edu-servers.net.
```

- Select one of the available ‘edu’ domain server to find the available DNS server for the ‘indiana.edu’ domain.

```
[vinayakgadag@Vinayakas-MacBook-Pro] ~
❯ dig @b.edu-servers.net www.indiana.edu q-A

; <<>> DiG 9.10.6 <<>> @b.edu-servers.net www.indiana.edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46004
```

;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.indiana.edu. IN A

;; AUTHORITY SECTION:
indiana.edu. 172800 IN NS dns1.iu.edu.
indiana.edu. 172800 IN NS dns2.iu.edu.
indiana.edu. 172800 IN NS dns3.iu.edu.

- Next, select one of the DNS servers to get the resolved server for the host www.mail-relay.iu.edu

[vinayakgadag@Vinayakas-MacBook-Pro] ~
❯ dig @dns1.iu.edu www.mail-relay.iu.edu q-A

; <<>> DiG 9.10.6 <<>> @dns1.iu.edu www.mail-relay.iu.edu q-A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38818
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.mail-relay.iu.edu. IN A

;; AUTHORITY SECTION:
iu.edu. 300 IN SOA dns1.iu.edu. dns-admin.indiana.edu. 2002076869 7200 3600 3600000 300

;; Query time: 28 msec
;; SERVER: 2001:18e8:3:220::10#53(2001:18e8:3:220::10)
;; WHEN: Fri Sep 17 11:47:38 EDT 2021
;; MSG SIZE rcvd: 109

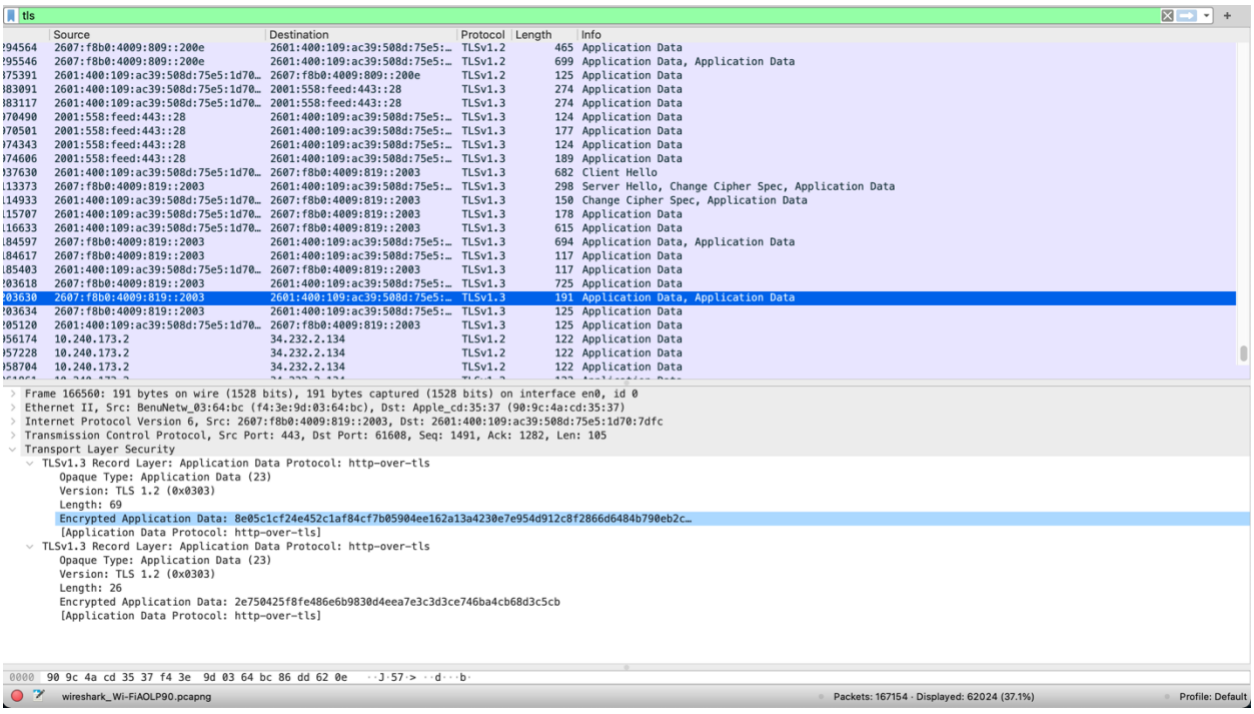
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 31397
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

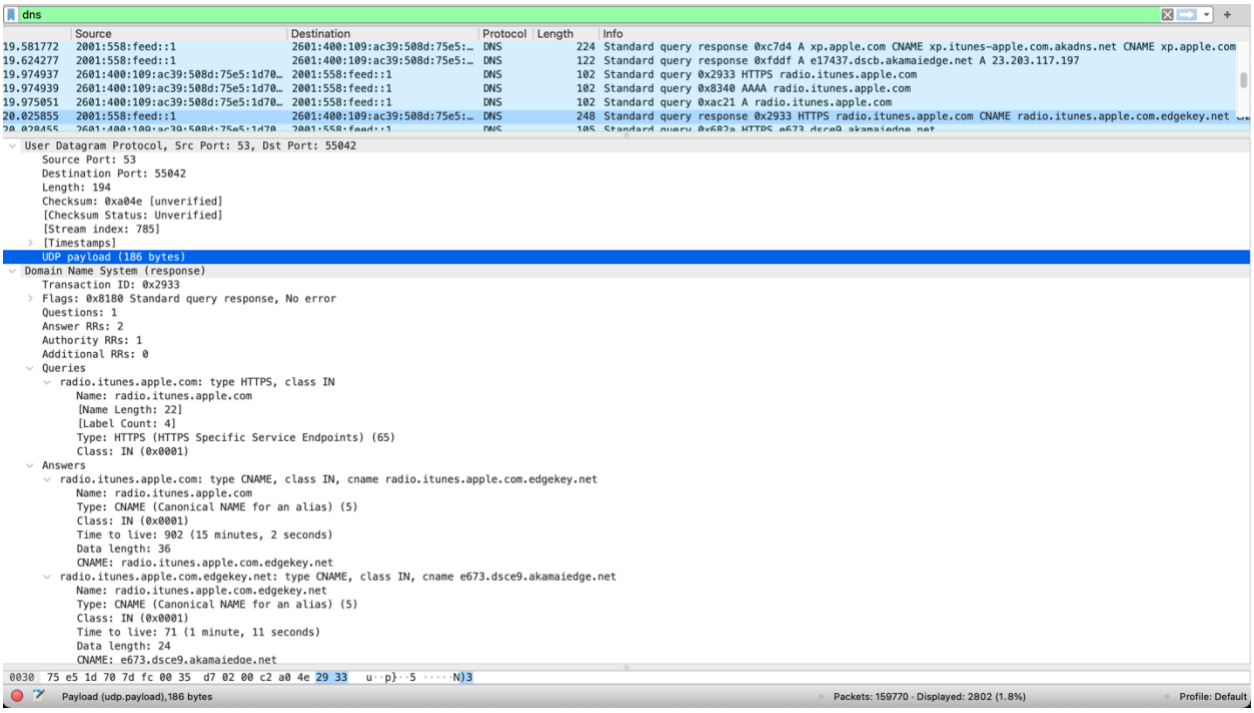
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;q-A. IN A

;; Query time: 29 msec
;; SERVER: 2001:18e8:3:220::10#53(2001:18e8:3:220::10)
;; WHEN: Fri Sep 17 11:47:38 EDT 2021
;; MSG SIZE rcvd: 32

4. You are sitting in a coffee shop and are connected to a public WLAN. You fire up wireshark and start sniffing the traffic of other customers. You notice that all their traffic is over https so you cannot simply read it. You also notice something striking about the DNS traffic, what is it and what are the implications?

Answer: When we sniff the traffic using wireshark. The TLS will give the encrypted information but on the same side we could see the information about User Datagram protocol and DNS response when we filter it to DNS packets. The DNS packets include the queries and answers. The answers include the recursive details, CNAME for an alias, SOA, TTL information like minimum TTL.





5. Suppose that IU has an internal DNS cache. You are an ordinary user (no network admin). Can you determine (and if yes, how) if a given external website was recently accessed?

Answer: As an ordinary user we can discover the website if it is recently accessed by looking at the DNS cache locally using DNS local server or try running the dig command and check the response time. If it returns the query response in no-time or less time than the external website is visited before and stored the cache in internal DNS server. In below screenshot we can observe that the first response took 8 msec and second took 0 msec.

```
vgadag@silo:~$ dig www.amazon.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39903
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.amazon.com.                        IN      A

;; ANSWER SECTION:
www.amazon.com.         1699    IN      CNAME   tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com. 20 IN CNAME   www.amazon.com.edgekey.net.
www.amazon.com.edgekey.net. 224 IN      CNAME   e15316.a.akamaiedge.net.
e15316.a.akamaiedge.net. 20     IN      A       184.51.221.199

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 17 12:43:12 EDT 2021
;; MSG SIZE  rcvd: 169

vgadag@silo:~$ dig www.amazon.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62567
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.amazon.com.                        IN      A

;; ANSWER SECTION:
www.amazon.com.         1698    IN      CNAME   tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com. 18 IN CNAME   www.amazon.com.edgekey.net.
www.amazon.com.edgekey.net. 222 IN      CNAME   e15316.a.akamaiedge.net.
e15316.a.akamaiedge.net. 18     IN      A       184.51.221.199

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 17 12:43:14 EDT 2021
;; MSG SIZE  rcvd: 169
```

REFERENCES

1 Computer Networking: A Top-Down Approach, 7th ed

2 https://www.lifewire.com/what-is-a-dns-cache-817514