Homework 4

1. As of June 2019, there are 1589 top-level domains in the root domain, with a few that have been retired and are no longer functional. The list of top-level domains (TLDs) on the Internet covers top-level domains, which are domains in the DNS root zone of the Internet's Domain Name System. The Internet Assigned Numbers Authority (IANA) maintains the authoritative list of all top-level domains at the Root Zone Database. IANA is also in charge of approving new proposed top-level domains.

   (Reference: https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains)

2. A. https://www.stevens.edu/
   Administrative Contact: Domain Name Administration, Information Technology team, Stevens Institute of Technology

   https://kiit.ac.in/
   Administrative Contact: Koel Campus IT department, KIIT University

   b. Administrative contact information for the.xxx domain on the websites mentioned. xxx is a new Sponsored Top-Level Domain (sTLD) created particularly for the online adult entertainment business around the world. It will coexist with other ICANN-accredited TLDs like.com,.net,.org, and others, and will give major benefits and advantages to both providers and consumers.

      Google.xxx

      Domain Name: GOOGLE.XXX
      Registry Domain ID: D29317-AGRS
      Registrar WHOIS Server:
      Registrar URL: http://www.markmonitor.com
      Updated Date: 2018-10-30T09:36:37Z
      Creation Date: 2011-12-01T21:25:32Z
      Registry Expiry Date: 2019-12-01T21:25:32Z
      Registrar Registration Expiration Date:
      Registrar: MarkMonitor Inc.
      Registrar IANA ID: 292
      Registrant Organization: Google Inc.
      Registrant State/Province: CA
      Registrant Country: US
      Name Server: NS3.GOOGLEDOMAINS.COM
      Name Server: NS1.GOOGLEDOMAINS.COM
      Name Server: NS2.GOOGLEDOMAINS.COM

Name Server: NS4.GOOGLEDOMAINS.COM
DNSSEC: unsigned

(Reference: www.internic.net, http://whois.domaintools.com)

3. **Structure and Responsibilities of IANA**

The Internet Assigned Numbers Authority (IANA) is a division of the Internet Business for Assigned Names and Numbers (ICANN), a nonprofit private American corporation. IANA assigns and maintains unique codes and numbering systems for use in the Internet's technical specifications ("protocols"). Their many activities can be divided into three broad categories:

• Domain Names: DNS Root management,.int and.arpa domain management, and IDN practices resources.

• Number Resources: Coordination of the worldwide pool of IP and AS numbers for distribution to Regional Internet Registries.

• Protocol Numbering Systems: The numbering systems for Internet protocols are administered in collaboration with standards organizations.

Structure and Responsibilities of ICANN

ICANN is made up of several separate groups, each of which represents a different internet interest and all of which contribute to ICANN's final judgments. Three supporting organizations are in charge of IP addresses, domain names, and country code top-level domain management. There are four advisory panels that provide suggestions and opinions. Finally, there is a Technical Liaison Group, which collaborates with organizations that develop basic internet protocols. ICANN's responsibilities include:

•It involves the consideration and implementation of new top-level domains (TLDs) as well as the deployment of IDNS.

•It is responsible for coordinating the global Internet's system of unique identifiers, as well as ensuring the Internet's unique identifier systems' stability and security.

• It formalizes ties with operators of root name servers.

• It ensures proper contingency planning and maintains unambiguous root zone change processes.

• It will continue to strengthen the effectiveness of bottom-up policy creation processes by maintaining and improving the multi-stakeholder model and worldwide participation of all stakeholders.

• It implements suitable measures to encourage global Internet stakeholders to participate in ICANN, including as offering instructional services, fostering information sharing, and promoting best practices within industry segments.

• It will perform an assessment of the corporate administrative structure and make appropriate modifications to assure stability, including allocating adequate resources to contract enforcement while considering organizational and corporate governance best practices.

Differences in responsibilities between IANA and ICANN

- According to the Memorandum of Understanding (MoU), the institution that runs TLDS is IANA, but the institution that runs IANA is ICANN
- IANA oversees Top-Level Domains and IP address ranges, ports, and other relevant features, whereas ICANN is a non-profit organization that coordinates the Internet's global space structure.

Controversy in ICANN concerning Whois

Regulators on the internet are pursuing a contentious plan to limit public access to WHOIS Web site registration details. Proponents of the plan claim that it will improve the accuracy of WHOIS data and protect the privacy of domain name registrants. Critics argue that such a change would be impossible to implement and would make combating phishers, spammers, and scammers more difficult.

The current WHOIS system, which is inconsistently managed by hundreds of domain registrars and allows anyone to query Web site registration records, has been proposed by a working group within The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that oversees the Internet's domain name system. The group suggests building a more centralized WHOIS lookup system that is closed by default to replace the current system. The WHOIS data would be accessible only to "authenticated requestors who are held accountable for acceptable use," according to an interim report (PDF) by the ICANN working group.

(Reference: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority, https://www.iana.org, https://www.icann.org/resources/pages/what-2012-02-25-en, http://www.securityweek.com/icanns-rolling-controversyverification-whois-registration-data)

4. Spam Haus was the target of a distributed denial of service (DDoS) attack exploiting a long-known vulnerability in the Domain Name System (DNS) which permits origination of massive quantities of messages at devices owned by others using IP address spoofing.

   A. Spamhaus uses a technique that has been around for a long time: a type of reflection attack known as a "DNS amplification attack." As an industry leader in DNS software, ISC sees the Spamhaus DDOS as an excellent occasion to educate DNS operators why it's critical to avoid running a "open" recursive resolver, a policy suggestion we've made since 2005. The attacker forges a "spoofed" source address for a DNS query that is only a few bytes long and sent to an open resolver. The open resolver, believing the faked source address, sends a response to the computer it believes issued the request, which can be hundreds of bytes in size. As a result, the victim's network connection is bombarded with hundreds of bytes of data that were not requested. When they reach the target system, they will be rejected, but not before using up some of the victim's network capacity. And the open resolver is the source of the traffic that reaches the victim, not the machine or machines who launched the attack. An attacker utilizing a DNS amplification assault can mask the origin of their attack and magnify the quantity

of traffic they can aim at the victim by a factor of 40 or more if they have a large list of open resolvers to reflect against. DNS operators that operate open resolvers without taking safeguards to avoid abuse feel they are causing no harm, but as the Spamhaus DDOS demonstrates, open resolvers can be easily coopted by attackers and utilized in criminal assaults against third parties.

B. The Spamhaus website has been under attack since March 18. The onslaught was so enormous that the Spamhaus crew had no idea how big it was. It was enormous enough to completely overwhelm their connection to the rest of the Internet and take their website down. These massive attacks, known as Layer 3 attacks, are impossible to defend against with any on-premise solution. Spamhaus' blocklists are delivered using DNS, and a vast list of volunteer organizations replicate their DNS infrastructure to ensure it is secure. The website, on the other hand, was unavailable.

   Large-scale Layer 3 attacks are almost often the result of a combination of factors. Each of these sources sends traffic to a single Internet address, thereby causing a tidal wave that overwhelms the target's resources. In this way, the attack is spread out (the first D in DDoS — Distributed Denial of Service). Attack traffic can come from a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords (e.g., the Anonymous LOIC model), a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords.

   Because an attacker performing a Layer 3 attack isn't concerned with receiving a response to the requests they make, the packets that make up the attack don't have to be precise or formatted correctly. Attackers will spoof all of the information in attack packets, including the originating IP, to make it appear as if the attack is coming from an endless number of places. Because data packets can be completely randomized, measures like IP filtering become nearly useless even upstream.

   Spamhaus, a non-profit anti-spam organization, contacted CloudFlare on March 19, 2013, in the afternoon. They were experiencing a big DDoS attack on their website and requested if we could assist them in reducing the impact.
   CloudFlare quickly mitigated the assault, restoring access to the site. (See below for more information on how we achieved it.) We started recording data regarding the attack once we were on our network. At first, the assault was a little one (around 10Gbps). Around 16:30 UTC, there was a small increase that lasted around 10 minutes and was most likely a test. The attackers then unleashed a massive wave about 21:30 UTC.

   The attacker in the Spamhaus case was issuing requests to open DNS resolvers for the ripe.net DNS zone file. In their DNS requests, the attacker used the CloudFlare IPs assigned to Spamhaus as the source. The open resolvers reacted with a DNS zone file, generating 75Gbps of attack traffic in total. The requests were likely 36 bytes long

(e.g., dig ANY ripe.net @X.X.X.X +edns=0 +bufsize=4096, where X.X.X.X is replaced with the IP address of an open DNS resolver), while the response was 3,000 bytes long, resulting in a 100x amplification factor.
They discovered approximately 30,000 different DNS resolvers that were used in the assault. This amounts to an average of 2.5Mbps per open DNS resolver, which is tiny enough to go unnoticed by most DNS resolvers. Because the attacker employed DNS amplification, he just needed control of a botnet or a cluster of servers to generate 750Mbps, which is doable with a tiny botnet or a few AWS instances. It bears repeating: open DNS resolvers are the Internet's scourge, and until service providers make real attempts to block them, these attacks will become more common and large.

While big Layer 3 attacks are difficult to mitigate with an on-premise DDoS solution, CloudFlare's network was built expressly to thwart these types of attacks from the start. Anycast was heavily used by CloudFlare. This means that each of our 23 data centers around the world broadcasts the same IP address. Requests are routed to the nearest facility by the network itself. This helps us ensure that a visitor is routed to the nearest data center on our network in typical circumstances.

When an attack occurs, Anycast helps to efficiently dilute it by dispersing it throughout our facilities. Because each data center assigns each CloudFlare customer the same IP address, traffic cannot be concentrated in a single area. Instead of being a one-to-many attack, it becomes a one-to-many attack.

At each of our data centers, the attack becomes reasonably trivial to stop once it has been diluted. With Layer 3 attacks, none of the attack traffic reaches the customer's servers since CloudFlare acts as a virtual shield in front of our clients' sites. As soon as they signed up for our service, traffic to Spamhaus's network plummeted to levels below those before the attack began. While DNS reflection accounted for the majority of the traffic involved in the attack, the attacker also used a few other attack tactics. One of them was an ACK reflection attack. A handshake occurs when a TCP connection is formed. The TCP session is started by the initiating server sending a SYN (synchronize) request to the receiving server. The receiving server responds with an acknowledgement code (ACK) (for acknowledge). Data can be exchanged after that handshake.

The attacker sends a series of SYN packets to servers with a faked source IP address pointing to the intended victim in an ACK reflection. The servers then send an ACK to the victim's IP address. This, like the DNS reflection attack, hides the assault's origins by making it appear to come from legitimate servers. Unlike the DNS reflection attack, however, there is no amplification factor: the bandwidth used by the ACKs is symmetrical to the bandwidth used by the attacker to create SYNs. Unmatched ACKs are dropped by CloudFlare, which mitigates these types of attacks.

When CloudFlare detects one of these major attacks, network operators will contact us to complain about how we are targeting their infrastructure with abusive DNS queries or SYN floods. Their infrastructure is, in effect, being utilized to reflect an attack on us. They clean up their network by working with and educating network operators, which helps to solve the fundamental cause of these huge attacks.

(Reference: https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/)

5. A. Amazon Route 53 allows us to register new domain names or transfer existing ones, and it supports a wide range of generic top-level domains (such as.com or.org) and geographic top-level domains (such as .be or .us). It also allows us to manage the IP listed for domain names in the Internet's DNS phonebook, as well as create, update, and manage public DNS entries. Route 53 converts specific domain names, such as www.example.com, into IP addresses, such as 192.0.2.1. It also sends automated requests to the application over the Internet to ensure that it is reachable, accessible, and functional, also a health check to monitor the overall health and execution of the application, web servers, and other resources.

   B. AWS allegedly called the service Route 53 after TCP or UDP port 53, which is used to process all DNS requests.

   C. Amazon Route 53 is built to work with other AWS services and functionalities. It is also possible to map domain names to Amazon EC2 instances, Amazon S3 buckets, Amazon CloudFront distributions, and other AWS services using Amazon Route 53. Fine tuning can update the DNS data by combining the AWS Identity and Access Management (IAM) service with Amazon Route 53. Using Amazon Route 53's Alias record feature, one may link the zone apex (example.com vs. www.example.com) to Elastic Load Balancing instance, Amazon CloudFront distribution, AWS Elastic Beanstalk environment, or Amazon S3 website bucket.

   D. A domain is a DNS concept that applies to all domains. Domain names are immediately recognizable names for Internet sites that are numerically addressed. Amazon.com is an example of a domain. An Amazon Route 53 notion is a hosted zone. A hosted zone is similar to a standard DNS zone file in that it represents a group of records that may be managed together and are associated with a single parent domain name. The hosted zone's domain name must be a suffix on all resource record sets within the hosted zone. The amazon.com hosted zone, for example, may contain records named www.amazon.com and www.aws.amazon.com, but not www.amazon.ca. To create, check, change, and delete hosted zones, utilize the Route 53 Management Console or API. We can also register new domain names and move existing domain names into Route 53's management using the Management Console or API.

E. A variable called the time to live (TTL) associated with each record determines how long a DNS resolver stores a response. There is no default TTL for any record type in Amazon Route 53. For caching DNS resolvers to cache our DNS records for the duration of time provided by the TTL, we must always give a TTL for each record.

F. There is no set charge.
Zones that are hosted For the first 25 hosted zones, $0.50 per month per hosted zone Additional hosted zones are $0.10 per month per hosted zone.

The costs indicated above for monthly hosted zones are not prorated for partial months. A hosted zone is charged on the first day of each month after it is set up. A hosted zone that is erased within 12 hours of its establishment is not charged to allow for testing; nonetheless, any queries on that zone are charged at the rates listed below.

Flow of Traffic $50.00 per month per policy record The application of an Amazon Route 53 Traffic Flow policy to a specific DNS name (such as www.example.com) in order to use the traffic policy to manage traffic for that DNS name is represented by a policy record. The aforementioned monthly price is prorated for partial months. For traffic policies that are not coupled with a DNS name via a policy record, there is no charge.

Typical Inquiries The first 1 billion inquiries per month will cost $0.400 per million queries. Over 1 billion inquiries per month – $0.200 per million queries

Queries for latency-based routing The first 1 billion inquiries per month will cost $0.600 per million queries. Over 1 billion inquiries per month – $0.300 per million queries

Geo DNS Lookups The first 1 billion inquiries per month will cost $0.700 per million queries. $0.350 per million inquiries – a monthly volume of over 1 billion queries

The above query fees are prorated; for example, a hosted zone with 100,000 normal queries will be paid $0.040, while a hosted zone with 100,000 Latency Based Routing questions will be charged $0.060.

Alias records mapped to Elastic Load Balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, and Amazon S3 website buckets are all free to query. All query types, including ordinary queries, latency-based routing queries, and geo queries, can have alias records created. The Amazon Route 53 usage report lists these searches as "Intra-AWS-DNS-Queries," "Intra-AWS-LBR-Queries," or "Intra-AWS-Geo-Queries."

(Reference: https://aws.amazon.com/route53/,
https://aws.amazon.com/route53/faqs/,
https://en.wikipedia.org/wiki/Amazon_Route_53)