Dharmi Gujarati

CWID - 20018001

Assignment - 4

Answer: 1

- There are **1591** top domains on the date 10th April 2023 at 8:36pm on the root zone database of IANA.

  Source: Root Zone Database (iana.org)

Answer: 2

A. Information about the stevens.edu domain from the website Stevens.edu WHOIS, DNS, & Domain Info - DomainTools.

- ### Domain Profile

Registrant Org	Stevens Institute of Technology	
Registrar Status		
Dates	9,055 days old Created on 1998-06-25 Expires on 2025-07-31 Updated on 2022-06-03	_
Tech Contact	Domain Name Administration	
IP Address	104.18.130.28 is hosted on a dedicated server	_
IP Location	🇺🇸 - Ohio - Columbus - Cloudflare Inc.	
ASN	🇺🇸 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)	
IP History	14 changes on 14 unique IP addresses over 18 years	_

Hosting History	6 changes on 5 unique name servers over 21 years

- Domain Name: STEVENS.EDU
  Registrant:
  Stevens Institute of Technology
  Castle Point on Hudson
  Information Technology
  Hoboken, NJ 07030
  USA

  Administrative Contact:
  Domain Name Administration
  Stevens Institute of Technology
  Information Technology
  Castle Point on the Hudson
  Hoboken, NJ 07030
  USA
  +1.2012165457

  webmaster@stevens.edu

  Technical Contact:
  Domain Name Administration
  Stevens Institute of Technology
  Information Technology
  Castle Point on the Hudson
  Hoboken, NJ 07030
  USA
  +1.2012165457

  webmaster@stevens.edu

  Name Servers:
  BETTY.NS.CLOUDFLARE.COM
  HASSLO.NS.CLOUDFLARE.COM
  Domain record activated: 25-Jun-1998
  Domain record last updated: 03-Jun-2022
  Domain expires: 31-Jul-2025

Source: Whois Lookup, Domain Availability &amp; IP Search - DomainTools

- **Administrative Contacts for Stevens:**

  Domain Name Administration
  Stevens Institute of Technology
  Information Technology
  Castle Point on the Hudson
  Hoboken, NJ 07030
  USA
  +1.2012165457

- The domain of some other school (Veer Narmad South Gujarat University)

  - **Domain Profile**

Registrant	REDACTED FOR PRIVACY
Registrant Org	Veer Narmad South Gujarat University
Registrant Country	IN
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: —
Registrar Status	ok
Dates	4,726 days old Created on 2010-05-03 Expires on 2029-05-03 Updated on 2021-08-15
Name Servers	ARELY.NS.CLOUDFLARE.COM (has 26,095,337 domains) BRUCE.NS.CLOUDFLARE.COM (has 26,095,337 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR

	PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY(p) (f)
IP Address	104.26.0.67 - 127 other sites hosted on this server
IP Location	🇺🇸 - California - San Jose - Cloudflare Inc.
ASN	🇺🇸 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
IP History	2 changes on 2 unique IP addresses over 0 years
Hosting History	1 change on 2 unique name servers over 1 year

Source: https://whois.domaintools.com/vnsgu.edu.in

- **Administrative Contacts for VNSGU:**

  Domain Name Administration
  Veer Narmad South Gujarat University
  Post Box No 49, Udhna Magdalla Road
  Surat, Gujarat 395007
  INDIA
  +91 (0261) 2227141

B. The administrative contact for the **.xxx domain**:

- **Domain Profile**

Registrant	Moniker Privacy Services
Registrant Org	Moniker Privacy Services
Registrant Country	US
Registrar	Moniker Online Services LLC IANA ID: 228

	URL: http://www.moniker.com Whois Server: whois.moniker.com abusereport@moniker.com (p) +1.9546071294
Registrar Status	clientTransferProhibited
Dates	10,498 days old Created on 1994-07-14 Expires on 2023-07-13 Updated on 2022-07-14
Name Servers	NS1.SERVERSTACK.COM (has 2,322 domains) NS2.SERVERSTACK.COM (has 2,322 domains) NS3.SERVERSTACK.COM (has 2,322 domains) NS4.SERVERSTACK.COM (has 2,322 domains)
Tech Contact	Moniker Privacy Services 2320 NE 9th St, Second Floor, Fort Lauderdale, FL, 33304, US 27d24766d85175c12f506af5117415ce815fbc53daf3471290c967c6c1130a68@xxx.com.whoisproxy.org (p) +1.3006886311 (f) +1.9545859186

- **Administrative Contacts for .xxx domain:**

  Moniker Privacy Services
  2320 NE 9th St, Second Floor,
  Fort Lauderdale, FL, 33304, US
  27d24766d85175c12f506af5117415ce815fbc53daf3471290c967c6c1130a68@xxx.com.whoisproxy.org
  (p) +1.8006886311 (f) +1.9545859186

- The administrative contact for the google.xxx domain:
  - **Domain Profile**

Registrant	REDACTED FOR PRIVACY (DT)
Registrant Org	Google LLC
Registrant Country	US
Registrar	MarkMonitor, Inc. IANA ID: 292 URL: www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2083895740
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	4,149 days old Created on 2011-12-01 Expires on 2023-12-01 Updated on 2022-11-04
Name Servers	NS1.GOOGLEDOMAINS.COM (has 9,927,513 domains) NS2.GOOGLEDOMAINS.COM (has 9,927,513 domains) NS3.GOOGLEDOMAINS.COM (has 9,927,513 domains) NS4.GOOGLEDOMAINS.COM (has 9,927,513 domains)
Tech Contact	REDACTED FOR PRIVACY (DT) REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) (f)
Hosting History	1 change on 2 unique name servers over

7 years

- **Administrative Contacts for google.xxx:**

  MarkMonitor, Inc.
  IANA ID: 292
  URL: www.markmonitor.com
  Whois Server: whois.markmonitor.com
  abusecomplaints@markmonitor.com
  (p) +1.2083895740

➢ <u>Answer 3:</u>

- **Responsibility of IANA**

The Internet domain name system is a public asset, and the .af ccTLD is under the sovereign control of the Transitional Government. UNDP will administer the .af ccTLD for the benefit of the Afghan community.

An oversight committee will be created to advice on issues related to the policies and management of the .af ccTLD. Members of the Afghanistan Domain Administration Committee would be:

- The Minister of Telecommunications
- UNDP Afghanistan Country Director and Technical Management Focal Point (Mr. Marc Lepage)
- Representations from the user community

- **Structure at IANA**

IANA (Internet Assigned Numbers Authority) is a department of ICANN (Internet Corporation for Assigned Names and Numbers) that is responsible for managing the global DNS (Domain Name System). The structure of IANA is designed to ensure that it operates transparently and collaboratively with the various stakeholders that are involved in the management of the Internet.

IANA also works closely with a number of other organizations that are involved in the management of the Internet, including the Internet Engineering Task Force (IETF), the Regional Internet Registries (RIRs), and various technical working groups and standards bodies.

- **Responsibility at ICANN**

  ICANN provides the community with the necessary support and tools to carry out public responsibility related activities that enhance the multistakeholder model and support ICANN's mission.

  ICANN has established programs to raise awareness and encourage the participation in ICANN's multi-stakeholder model.

  A board of directors, support groups, and advisory committees are all parts of ICANN's organizational structure. The board of directors of ICANN is in charge of managing day-to-day operations and setting policy. On a variety of ICANN's work-related topics, such as policy creation, technical standards, and stakeholder engagement, supporting groups and advisory committees offer counsel and suggestions.

- **Structure at ICANN**

  The ICANN organizational structure was created to guarantee that it functions openly and cooperatively with the numerous parties engaged in the administration of the Internet.

  The structure of ICANN consists of many essential elements:

  1. Board of Directors: The Board of Directors of ICANN is in charge of establishing the organization's policies and long-term course. There are up to 20 voting members on the Board, including the CEO and delegates from several stakeholder organizations.
  2. Supporting Groups and Advisory Committees: These organizations include the Governmental Advisory Committee, the Address Supporting Organization, the Country Code Names Supporting Organization, the Generic Names Supporting Organization, and the Security and Stability Advisory Committee. (GAC).
  3. Staff of ICANN: The staff of ICANN is in charge of managing the organization's daily operations and providing assistance to the Board, Supporting Organizations, and Advisory Committees in their work.
  4. Public Participation: ICANN's organizational design also incorporates procedures for including the general public in its deliberations. This

includes chances for public input on suggested policies and activities, as well as involvement in public meetings.

Overall, ICANN's organizational structure is built to make sure that it collaborates with the numerous parties engaged in the administration of the vital infrastructure of the Internet in an open, responsible, and cooperative manner.

Source: Internet Assigned Numbers Authority (iana.org)

Internet Corporation for Assigned Names and Numbers (ICANN)

- **Differences in responsibilities between IANA and ICANN:**

The worldwide DNS (Domain Name System), as well as the distribution of IP addresses and other Internet protocol parameters, are all managed by IANA, a division of ICANN. The administration of the Internet's unique identifier systems, such as domain names, IP addresses, and protocol parameters, is coordinated and managed overall by ICANN.

IANA is managing the assignment of IP addresses and AS numbers, coordinating certain protocol assignments, and managing the DNS Root Zone. ICANN is coordinating the policies and procedures for the allocation of domain names and IP addresses, ensuring the stability and security of the Internet's unique identifier systems.

- **Controversy in ICANN concerning Whois:**

Most of the search engine results, particularly those at the top of the search result hierarchy, link to webpage of registrars attempting to sell domain names and related services. It is not at all intuitive how to access WHOIS in order to find the domain name registrant information. In order to become proficient with WHOIS, it's important to start in the right place. ICANN organization's WHOIS look-up tool makes it easier to conduct WHOIS searches.

Sometimes results may not show any contact information for the actual operator of a domain name and instead display information from a privacy and proxy service. Some registries and registrars offer privacy or proxy services that show only the contact information of the service, to shield users who don't want their personal information to appear in the database. Their anonymity is not guaranteed since registrars may abide by any legal requirements to share the identity of the customer. Likewise, registries or registrars in countries where privacy laws prohibit the collection and publishing of personal data are not required to break those laws to satisfy WHOIS. Instead, they are eligible to follow ICANN's procedure for handling conflicts with local law, and to apply for a WHOIS Data Retention Specification Waiver. Privacy issues are still being explored by on-going policy development efforts.

In response to these concerns, ICANN has sought to create a new Whois system that is a compromise between the need for accountability and openness and the need for registrant privacy. Finding the optimal balance between these conflicting interests has been a difficult problem, as stakeholders from different segments of the Internet community had opposing perspectives.

Source: Basics of WHOIS | ICANN WHOIS

➢ Answer 4:

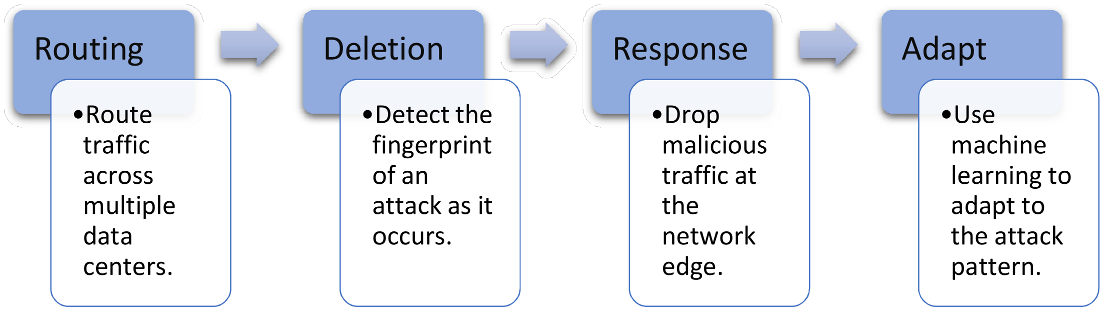
A. The Spamhaus attack, which occurred in 2013, was a large-scale Distributed Denial-of-Service (DDoS) attack against Spamhaus, an international organization that monitors spam emails and related activities. The attack, one of the largest on record at the time, was carried out by a criminal group in retaliation for Spamhaus blacklisting their spam activity.

- The attackers used a technique known as DNS amplification, in which they leveraged open recursive resolvers to flood Spamhaus with large amount of traffic, overloading the server, and disrupting the network. Open recursive resolvers are DNS servers configured to respond to DNS queries from any client, authorized or not. The open resolver responds with a much larger response than the original request, amplifying attack traffic and overwhelming the target server. Open recursive resolvers are especially dangerous because they can be used as part of a criminal conspiracy to launch DDoS attacks, as was the case with the Spamhaus attack.
- It is a large-scale DDoS attack carried out against the Spamhaus organization using a DNS amplification technique that leverages open recursive resolvers. The danger of open recursive resolvers is that they can be exploited by attackers to launch DDoS attacks, jeopardizing the security and availability of DNS and Internet infrastructure.

- Therefore, it is important for organizations to secure their DNS infrastructure by configuring their servers to respond only to authorize clients and implementing other security measures.

  Source: Is Your Open DNS Resolver Part of a Criminal Conspiracy? - ISC

B. DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack. By utilizing specially designed network equipment or a cloud-based protection service, a targeted victim is able to mitigate the incoming threat.


Routing
•Route traffic across multiple data centers.
Deletion
•Detect the fingerprint of an attack as it occurs.
Response
•Drop malicious traffic at the network edge.
Adapt
•Use machine learning to adapt to the attack pattern.

[DDoS Mitigation Stages]

- There are 4 stages of mitigating a DDoS attack using a cloud-based provider:

1. **Routing** - By intelligently routing traffic, an effective DDoS mitigation solution will break the remaining traffic into manageable chunks preventing denial-of-service.

2. **Detection** - in order to stop a distributed attack, a website needs to be able to distinguish an attack from a high volume of normal traffic. If a product release or other announcement has a website swamped with legitimate new visitors, the last thing the site wants to do is throttle them or otherwise stop them from viewing the content of the website. IP reputation, common attack patterns, and previous data assist in proper detection.

3. **Response** - in this step, the DDoS protection network responds to an incoming identified threat by intelligently dropping malicious bot traffic, and absorbing the rest of the traffic. Using WAF page rules for application layer (L7) attacks, or another filtration process to handle lower level (L3/L4)

attacks such as memcached or NTP amplification, a network is able to mitigate the attempt at disruption.

4. **Adaptation** - A good network analyzes traffic for patterns such as repeating offending IP blocks, particular attacks coming from certain countries, or particular protocols being used improperly. By adapting to attack patterns, a protection service can harden itself against future attacks.

Source: What is DDoS mitigation? | Cloudflare

➢ Answer 5:

A. Route 53 routes the end users to your site reliably with globally-dispersed Domain Name System (DNS) servers and automatic scaling. It set up your DNS routing in minutes with domain name registration and straightforward visual traffic flow tools. It customizes DNS routing policies to reduce latency, improve application availability, and maintain compliance. Route 53 can be integrated with other AWS services to enhance its capabilities and provide a comprehensive solution to customers. We can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking.

Source: Amazon Route 53 | DNS Service | AWS

What is Amazon Route 53? - Amazon Route 53

B. The name Route 53 comes from the port 53 is used by DNS servers, where DNS server requests are addressed. It's a reference to the Route 66 highway, which is a well-known American highway that connects Chicago to Santa Monica, California.

Source: Amazon Route 53 - Wikipedia

C. Other Amazon services like Elastic Load Balancing, AWS Certificate Manager, and AWS CloudFront are compatible with AWS Route 53. For instance, if your EC2 instances are served by an Elastic Load Balancer, Route 53 can direct traffic to the load balancer, which can then distribute it to the EC2 instances. Similarly, Route 53 can direct traffic to the encrypted destinations using SSL/TLS certificates obtained using AWS Certificate Manager.

- **Examples:**
  - **Elastic Load Balancer:**
    Route 53 can be used with Elastic Load Balancing to send traffic to the load balancer, which then distributes it to the registered EC2 instances or other AWS services. Advanced capabilities including geographic routing and latency-based routing, which can be used to direct traffic to the nearest or fastest destination depending on the user's location or network conditions, are offered by Route 53.

  - **Amazon Certificate Manager:**
    Traffic can be routed to encrypted endpoints utilizing SSL/TLS certificates obtained through ACM using Route 53 and AWS Certificate Manager. A custom domain name can be mapped to an AWS resource, such as an ELB load balancer or an Amazon CloudFront distribution that is protected by an ACM SSL/TLS certificate using Route 53. Without the need for manual certificate maintenance, this provides secure communication between the end user's web browser and the website or web application.

Source: What is Amazon Route 53? - Amazon Route 53

Elastic Load Balancing Documentation (amazon.com)

D. A hosted zone is a group of DNS records that specify how traffic is forwarded to a particular domain, whereas a domain name is a distinctive name that identifies a website or application on the internet.
In plainer terms, a hosted zone is like a map that tells how to go to a street address, whereas a domain name is like a street address.
A domain represents the entire set of names that are contained under an organizational domain name. For example, all domain names ending with .com are part of the "com" domain.
There are 2 types of hosted zone: Public and Private.
Public hosted zones contain records that specify how you want to route traffic on the internet.

Private hosted zones contain records that specify how you want to route traffic in an Amazon VPC.

Source: Working with hosted zones - Amazon Route 53

E. Time-to-live (TTL) is a numerical value used for data validity and expiration. A TTL stands for the amount of time data should remain valid and available before a computing system discards it.
Route 53 has a default TTL value of 300 seconds (5 minutes). The TTL value determines how long a DNS resolver should cache a DNS response before it expires and needs to be refreshed. However, users can configure their own TTL values to meet their specific needs.

It's also important to keep in mind that TTL values are used to control how long DNS resolvers cache records. Before all DNS resolvers reflect a change in a record's TTL, it may take up to the original TTL value.

Source: Amazon Route 53 FAQs - Amazon Web Services

F. With Amazon Route 53, you don’t have to pay any upfront fees or commit to the number of queries the service answers for your domain. Like with other AWS services, you pay as you go and only for what you use:

1) Managing hosted zones: You pay a monthly charge for each hosted zone managed with Route 53.
2) Serving DNS queries: You incur charges for every DNS query answered by the Amazon Route 53 service, except for queries to Alias A records that are mapped to Elastic Load Balancing instances, CloudFront distributions, AWS Elastic Beanstalk environments, API Gateways, VPC endpoints, or Amazon S3 website buckets, which are provided at no additional charge.
3) Managing domain names: You pay an annual charge for each domain name registered via or transferred into Route 53.

Your monthly bill from AWS will list your total usage and dollar amount for the Amazon Route 53 service separately from other AWS services.

The cost of AWS Route 53 is determined by the particular features used and the volume of use. Hosted zones, queries, and domain registration all have distinct costs. The starting price for a hosted zone is $0.50 per hosted zone per month, whereas the starting price for a million queries is $0.40. Depending on the top-level domain, the cost of domain registration can vary from a few dollars to several hundred dollars annually.

Source: Amazon Route 53 pricing - Amazon Web Services