Shubhangi Dutt
CS-524A

CS- 524 Introduction to Cloud Computing

Assignment-4

Answer 1

There are now 1589 Top-Level Domains (TLDs) on the internet, including 68 revoked, 8 defunct, and 11 test domains. I found this information on April 2,2022 03:07 AM.

Answer 2

a) The following information was available on whois.domaintools.com :-
For Stevens.edu :-
Administrative Contact:

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

For DITUniversity.edu.in (undergraduate) :-
Registry Admin ID:
Admin Name: Agarwal, Amit
Admin Organization: Unison Education Foundation
Admin Street: 3rd Floor, Administrative Block,
Admin City: Dehradun
Admin State/Province: Uttarakhand
Admin Postal Code: 248001
Admin Country: IN
Admin Phone: +91.1357155111
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:

b)

Whois Record for Google.xxx

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) 12083895740
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,778 days old Created on 2011-12-01 Expires on 2022-12-01 Updated on 2021-11-04
Name Servers	NS1.GOOGLEDOMAINS.COM (has 8,000,689 domains) NS2.GOOGLEDOMAINS.COM (has 8,000,689 domains) NS3.GOOGLEDOMAINS.COM (has 8,000,689 domains) NS4.GOOGLEDOMAINS.COM (has 8,000,689 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) x (f) x
Hosting History	1 change on 2 unique name servers over 6 years

Website

Website Title	None given.

Whois Record (last updated on 2022-04-05)

```
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
        REDACTED FOR PRIVACY
        REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
```

When you check for Google.xxx on whois.domaintools.com, you'll see the following

information. All administrative information has been redacted for privacy reasons, however we can see that the website is registered under the name MarkMonitor, Inc with an IANA ID:292. The organization is Google LLC, and registration information is also public.

The .xxx domain was created by ICANN in order to maintain accountability for accessing adult material on the internet. .xxx is an sTLD or a sponsored top-level-domain and it was useful majorly for the following purposes :-

i) It was easier to prevent kids from accessing such sites or employees to access such sites during work by simply blocking the TLD and not having to go to extra lengths to maintain restrictions.

ii)On the other hand it would provide easy access to those who required it.

Answer 3

ICANN (Internet Corporation for Assigned Names and Numbers) is a non-profit organization that manages DNS components all over the world in order to offer users with simple access to legitimate DNSs. The ICANN structure consists of a voting board of 16 directors, 5 liaisons, three supporting organizations, and four advisory committees.
Some roles of ICANN are as follows:-

- Space allocation of IP addresses.
- Management of ARPA TLD and coordination of the protocol identifier's assignment.
- Implementation and introduction of any new TLD
- Country Code TLD management or ccTLD
- Generic TLD management of gTLD
- Root Server System Management

IANA(Internet Assigned Numbers Authority) is in charge of the internet's worldwide unique identifier systems. Since there is no one to govern how the nodes interact, given the fact that the internet is not centrally owned, the IANA controls the system of addresses to guarantee seamless internet operations. IANA is a department of ICANN.
Some of the key responsibilities of IANA are:-

- The IANA provides IP addresses and ASNs which serve as unique identifiers for computers on a network and networks respectively. In other words it is responsible for Number Allocation Systems.
- The IANA is responsible for DNS management. It maintains the data for the DNS Root and is responsible for ccTLDs and gTLDs. The IANA handles .int and .arpa domains.

- Lastly, the IANA is responsible for protocol assignments. The IANA directly allocates numbering assignments to end users or protocol developers.

The difference between the two; IANA and ICANN is now evident. The IANA is an institution that allocates addresses, runs TLDs and maintains root zones while the ICANN is a non-profit corporation that runs IANA and other such departments, i.e. ICANN has a broader scope of running the internet and thus coordinates a world wide space framework. Secondly IANA is headed by ICANN.

ICANN has been in controversy regarding Whois most of which is directed at registrars and ICANN failing to appropriately crack down on domain owners with faulty WHOIS data, fearful of nefarious actors providing bogus data to evade discovery. Whois has tons of data regarding each and every domain that has been registered on it. ICANN fears this data can be faulty and thus only certain people should be provided liberty to alter data. Secondly the data is accessible to everyone i.e. anyone can query website registration records which can therefore be misused by phishers, scammers etc. Therefore a proposal was to provide this data to only 'authenticated requesters'.

Answer 4

a)
The spamhaus project is an effort to monitor and reduce spam behavior on the internet. Spamhaus generates anti-spam lists and distributes them to ISPs, which then utilize these lists to minimize incoming spam by implementing filters. DNS-based blacklists and whitelists are the names given to these listings. This is kept in the form of a database, which contains information such as IP addresses, domain names, and internet resources that may be used to identify spam or malware.

Spamhaus was subjected to a DDOS (distributed denial of service) attack in March 2013, in which the attackers exploited an open resolver to block spamhaus channels with amplified response data. The attackers made use of the fact that a resolver will always generate a response to a query whether it is the correct information requested or an error message. During this attack The attackers requested data from the resolver using the victims IP and the data was then sent to the given IP address.This generally would not have been an issue but the file requested was huge; a massive DNS zone file. The request was tiny, but the response from the resolver was massive and was transmitted to the falsified address. Using other such open resolvers, several similar requests were generated. Because of the repeated huge responses, when the response was received on the spamhaus ip address, it blocked the other traffic. This is known as a DNS Amplification Attack.

DNS operators who maintain open resolvers often do not realize how attackers can use this service for evil. The spamhaus DDOS clearly shows how an open resolver can be used for an amplification attack, It can amplify data by a factor of 100x thus bringing the site down or worse leaving it exposed for other attackers.

b)
On March 18 spamhaus began getting tons of traffic on its channels, it was large to the point where spamhaus got disconnected to the rest of the internet. Their website went down instantly with the sudden bursts of traffic coming their way and they had no on-premise solution to mitigate this attack. The attack was a DNA-Amplification-Attack that can be explained using a simple example; consider a port that supports 10 Gbps but you pass 11 Gbps traffic to it, in this case the port will become a bottleneck for the rest of the traffic and the traffic originally sent. This is what the sudden bursts of traffic did to the spamhaus website.

The attack on spamhaus came from a number of sources with fake IP addresses which created requests and directed traffic to spamhaus thus creating a huge traffic burst on the site's servers. Therefore the term distributed was used in DDOS. Spamhaus was the target of a distributed denial of service (DDOS) operation in which the perpetrators used an open resolver to block spamhaus channels with amplified response data. In a recursive query, a resolver must always provide a response, which might be the correct information or an error message. In this example, the attackers utilized a bogus IP address to request a large DNS zone file for ripe.net; the request was only some bytes long(~30 bytes), but the response was gigantic(about 3000 bytes @75 Gbps), and it was sent to the spamhaus's IP address. Several identical requests were created by using other such open resolvers. Because of the repeated large responses, when a response was received on the spamhaus ip address, it blocked all other traffic.

This is when Cloudflare was asked to help with the problem. Cloudflare used Anycast to assist slow down the assault at first and ultimately terminate it completely. Cloudflare has 23 data centers around the world, and anycast causes each of them to issue a call to the IP address, which subsequently redirects traffic to them, clearing up traffic on the attacked IP address. Because traffic is not concentrated in any one spot, it is diffused and the bottleneck is removed. Because the traffic has been redirected to other places, the website can now be reactivated. Cloudflare dealt with the spamhaus assault in this manner.

Shubhangi Dutt
CS-524A

Answer 5

a)
Amazon Route 53 is a cloud-based DNS service that allows users to transform DNS names in string format to IP addresses in order to link machines on a network. Route 53 links customers to Amazon Web Services infrastructure such as EC2 instances, load balancers, and so on. It allows users to create, update, remove, and administer DNS names as well as geographic and generic TLDS. Users may also use it to monitor the health (accessibility, performance and functioning) of their websites by configuring DNS health checks. It can also be used to link end users to infrastructure outside of AWS.

b)
It was named so because it refers to TCP and UDP port 53 and handles all requests through the same port number.

c)
AWS Route 53 is intended for use with EC2 instances, Elastic Load Balancing load balancers, Amazon S3 buckets, CloudFront distributions, and other AWS infrastructure components. Route 53, for example, may be used to map zone apex in load balancers, ec2 instances, s3 buckets, and so on using a 'Alias record,' and it enables detailed control over DNS data.
d)
A zone file is a collection of DNS name-to-IP address mappings. A hosted zone is similar to a zone file in that it contains a group of entries that all belong to the same parent domain. All records in the same collection will have the parent domain name as a suffix to identify them. This is a phrase that was coined for Route 53 and is exclusive to the AWS Route 53 service. A domain name is a common phrase used while utilizing DNS services. A domain name is a unique string name that identifies an IP address.

e)
Route 53 does not have a default TTL value. It must be set by the user in order to define the time limit to cache DNS records.

f)
There is no minimum fee as route 53 is a pay-as-you-go service. A user will incur charges in the following cases:-

- Creating a hosted zone - There is a monthly charge for managing a hosted zone
- Creating DNS queries- There is a charge for every query run outside the AWS infrastructure. For queries within the AWS infrastructure the user incurs no charge.

- Creating and managing domain names- An annual charge is incurred for each domain name registered via Route 53.

Resources

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains#:~:text=IANA%20also%20oversees%20the%20approval,retired%20and%2011%20test%20domains.
https://www.iana.org/about
https://www.iana.org/about/presentations/davies-atlarge-iana101-080929.pdf
http://archive.icann.org/tr/english.html#:~:text=What%20is%20ICANN's%20Role%3F,can%20find%20all%20valid%20addresses.
https://icannwiki.org/Internet_Assigned_Numbers_Authority#Roles_at_ICANN
https://www.securityweek.com/icanns-rolling-controversy-verification-whois-registration-data
https://en.wikipedia.org/wiki/The_Spamhaus_Project