CS 524 Homework #4

Due: April 9, 2019

This homework contains both technical and business-related DNS problems, for the total of **100** points.

Reading assignment: Chapter 5 (and references).

1. **(5 points)** Find out the exact number of all top domain names. Make sure you put a date and time of your finding. (Hint: use the information given at the lecture to locate the list of names at IANA.)
   Answer:
   - The exact number of all top domain names is 1532.
     # Version 2019040200, Last Updated Tue Apr 2 07:07:01 2019 UTC

2. **(5 points)** Experiment with www.internic.net and http://whois.domaintools.com) **and**

   a. Find the information about the *stevens.edu* domain as well as the domain of some other school (for instance, the school you had studied at before you came to *Stevens*). Who are the administrative contacts for the domains listed there?
      Answer:
      - The information for stevens.edu is as follows:
        1. **Domain Name**: STEVENS.EDU
        2. **Registrant**:
           Stevens Institute of Technology
           Castle Point on Hudson
           Information Technology
           Hoboken, NJ 07030
           United States of America
        3. **Administrative Contact**:
           Domain Name Administration
           Stevens Institute of Technology
           Information Technology
           Castle Point on the Hudson
           Hoboken, NJ 07030
           United States of America
           +1.2012165457
           webmaster@stevens.edu
        4. **Technical Contact**:
           Domain Name Administration
           Stevens Institute of Technology
           Information Technology
           Castle Point on the Hudson

Hoboken, NJ 07030
United States of America
+1.2012165457
webmaster@stevens.edu

5. **Name Servers**:
   NRAC.STEVENS-TECH.EDU
   SITULT.STEVENS-TECH.EDU
   DRDNS2.STEVENS.EDU
6. **Domain record activated**: 25-Jun-1998
7. **Domain record last updated**: 26-Sep-2018
8. **Domain expires**: 31-Jul-2019

- The second domain I am finding information is for njit.edu:
  1. **Domain Name**: NJIT.EDU
  2. **Registrant**:
     New Jersey Institute of Technology
     323 Dr. Martin Luther King Boulevard
     323 Martin Luther King Boulevard
     Newark, NJ 07102
     United States of America
  3. **Administrative Contact**:
     Peter Teklinski
     New Jersey Institute of Technology
     CST - 2604 GITC
     323 Martin Luther King Boulevard
     Newark, NJ 07102
     United States of America
     +1.9735962908
     pt@njit.edu
  4. **Technical Contact**:
     Frank Aversa
     New Jersey Institute of Technology
     CST/Networks - 2605 GITC
     323 Dr. Martin Luther King Boulevard
     Newark, NJ 07102
     United States of America
     +1.9735965682
     frank.g.aversa@njit.edu
  5. **Name Servers**:
     DNS2.NJIT.EDU
     DNS1.NJIT.EDU
     NS3.NJIT.EDU
     NS5.NJIT.EDU
  6. **Domain record activated**: 06-Jun-1987
  7. **Domain record last updated**: 26-Sep-2018

8. **Domain expires**: 31-Jul-2019

b. Now, what happens when you try to find the administrative contact for the *.xxx* domain? Explain what you have found.

Answer:

I tried to find administrative contact for the .xxx domain but rather I got the following information:

- The .**xxx domain** extension was created for the global adult entertainment industry. It is intended to provide trusted **domain** names for adult-themed sites and to encourage safe, responsible behavior online. Some country code **domains** require you to provide additional pieces of information for registration.
- Some of the organizations have saved their domain names like for Stanford University.
- Thus, I have gathered registration details rather than having administrative contact:

```
1.  Domain Name: STANFORD.XXX
2.  Registry Domain ID: D186521-AGRS
3.  Registrar WHOIS Server:
4.  Registrar URL: icmregistry.com
5.  Updated Date: 2012-01-30T21:16:13Z
6.  Creation Date: 2011-12-01T05:40:32Z
7.  Registry Expiry Date: 2021-12-01T05:40:32Z
8.  Registrar Registration Expiration Date:
9.  Registrar: ICM Registry LLC
10. Registrar IANA ID: 800080
11. Domain Status: ok https://icann.org/epp#ok
12. Registrant Organization: ICM Registry LLC
13. Registrant State/Province: FL
14. Registrant Country: US
15. Name Server: NSB1.ICMREGISTRY.NET
```

3. **(5 points)** Look up www.cs.*stevens.edu* at http://network-tools.com/nslook/ (or any other DNS lookup tool you decide to use), copy the response, and explain all the entries in the response.

   Then use the returned CNAME entry to find the exact IP address. (Now, just for fun, do the *reverse DNS lookup* using the services of the http://dnsquery.org and find the geographic location of the host!)

Does Stevens specify IPV6 addresses to any of its hosts? Does Google?

Answer:

These are the following results which I found:

A	IN	www.cs.stevens-tech.edu.	3600	The IPv4 address for the domain.
	IN	155.246.89.84	604800	
AAAA	IN	www.cs.stevens-tech.edu.	3600 (8ms)	The IPv6 address.
CNAME (canonical name)	IN	www.cs.stevens-tech.edu.	3600 (8ms)	An alias of one domain name to another. This lets a server use more than one domain name.
MX (mail exchange record):	IN	www.cs.stevens-tech.edu.	3600 (9ms)	A list of message transfer agents for the domain. A message transfer agent handles email for the domain.
NS	IN	www.cs.stevens-tech.edu.	3600 (8ms)	An authoritative name server for the domain. There can be more than one NS record per domain. All other servers use a copy of information from the authoritative servers.
TXT	IN	www.cs.stevens-tech.edu.	3600 (9ms)	A record containing information for use outside the DNS. The content takes the form “name=value”. Authentication schemes such as SPF and DKIM use TXT records.

- The IP address is : 155.246.89.84

- The location of the host is :
  - Country :United States (US)
  - Region :New Jersey
  - City :Hoboken
  - Latitude :40.745800018311
  - Longitude :74.032096862793

- Stevens or Google doesn't specify IPV6 addresses to any of its hosts

4. **(5 points)** Find your PC's IP address (preferably at home, if you have an Internet connection there.) Can you find your domain with the reverse look up? If you can, what is the domain name? If you cannot, explain why.

Answer:

- The IP address for my computer is 192.168.112.1
- No, I cannot find domain with the reverse lookup because my computer is not connected to any domain. If my computer would have been connected to any domain, I could have preferably able to find the domain name.

5. (**10 points)** *Research the responsibilities and structure of IANA (www.iana.com) and ICANN (www.icann.com). What are the differences in responsibilities between these two organizations? Search the web for the information and then describe the controversy in ICANN concerning Whois?*

Answer:

- **The structure and responsibilities of IANA are as follows:**

- IANA is broadly responsible for the allocation of globally unique names and numbers that are used in Internet protocols that are published as Request for Comments documents. These documents describe methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.[4] IANA maintains a close liaison with the Internet Engineering Task Force (IETF) and RFC Editorial team in fulfilling this function.
- In the case of the two major Internet namespaces, namely IP addresses and domain names, extra administrative policy and delegation to subordinate administrations is required because of the multi-layered distributed use of these resources.
- IANA is responsible for assignment of Internet numbers which are numerical identifier assigned to an Internet resource or used in the networking protocols of the Internet Protocol Suite. Examples include IP addresses and autonomous system (AS) numbers.

- **The structure and responsibilities of ICANN are as follows:**

- ICANN has been formally organized as a nonprofit corporation "for charitable and public purposes" under the California Nonprofit Public Benefit Corporation Law. It is managed by a 16-member board of directors composed of eight members selected by a nominating committee on which all the constituencies of ICANN are represented; six representatives of its

Supporting Organizations, sub-groups that deal with specific sections of the policies under ICANN's purview; an at-large seat filled by an at-large organization; and the President / CEO, appointed by the board.

- There are currently three supporting organizations: the Generic Names Supporting Organization (GNSO) deals with policy making on generic top-level domains (gTLDs); the Country Code Names Supporting Organization (ccNSO) deals with policy making on country-code top-level domains (ccTLDs); the Address Supporting Organization (ASO) deals with policy making on IP addresses.

➢ **The controversy in ICANN concerning Whois:**

- Intended to be a source of information about domain owners, WHOIS has become a lightning rod for controversy over the years, much of which is aimed at registrars and ICANN for failing to properly crack down on domain owners with inaccurate WHOIS data. Wary of bad actors supplying false data to avoid detection, ICANN however is hoping to improve the process of resolving issues tied to registration data.
- On May 17th, in anticipation of the now approved European General Data Protection Regulation (GDPR), the Internet Corporation for Assigned Names and Numbers (ICANN), an American organization tasked with accrediting registrars and enforcing WHOIS policies, approved a new and revised Temporary Specification for gTLD registration data to ensure its domain information policies meet the EU's new data privacy rules.
- WHOIS refers to the data directly related to a domain name, which includes a name, address, e-mail, phone number and other personal information. Limiting access to previously public data was met with disapproval by law enforcement agencies using WHOIS data to investigate cybercrimes. The International Trademark Association (INTA) protested the Temporary Specification by stating that restriction to WHOIS data will likely increase incidents involving online fraud and abuse. As a result, INTA is now asking stakeholders and IP practitioners worldwide to submit stories detailing the negative effects of restricting access to WHOIS data.

6. (**50 points)** The *Spamhaus* attack

   a. (5 points) Read https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/ . Describe (in no more than a couple of paragraphs) the *Spamhaus* attack and explain the dangers of open recursive resolvers.

   Answer:

   - A significant component of the DDOS traffic targeted at Spamhaus is coming from a technique that has been known for years a variety of reflection attack commonly known as a "DNS amplification attack." By relying on the fact that an answer to a DNS query can be much larger than the query itself, attackers are able to both amplify the magnitude of the traffic directed against a DDOS victim and conceal the source of the attacking machines. The dangers of open recursive resolvers: A recursive resolver would

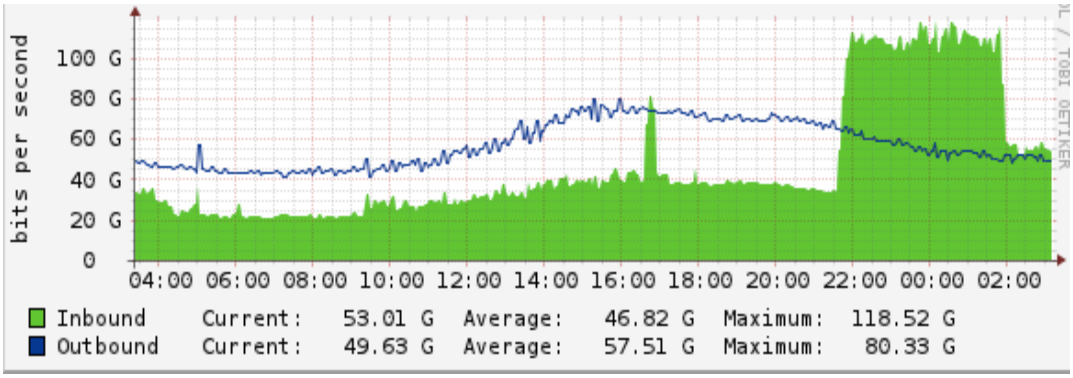
be a DNS server that queries an authoritative name server to resolve a domain/ address.

- The open resolver, believing the spoofed source address, sends a response which can be hundreds of bytes in size to the machine it believes originated the request. The end result is that the victim's network connection is hit with several hundred bytes of information that were not requested.
- They will be discarded when they reach the target machine, but not before exhausting a portion of the victim's network bandwidth. And the traffic reaching the victim comes from the open resolver, not from the machine or machines used to initiate the attack.
- Given a large list of open resolvers to reflect against, an attacker using a DNS amplification attack can hide the origin of their attack and magnify the amount of traffic they can direct at the victim by a factor of 40 or more.
- DNS operators who operate open resolvers without taking precautions to prevent their abuse generally believe they are harming nobody, but as the Spamhaus DDOS proves, open resolvers can be effortlessly coopted by attackers and used in criminal attacks on third parties.

b. (45 points) Find out (you will need to search the Web and sort a lot of information out!) how cloud services were used to mitigate this attack.

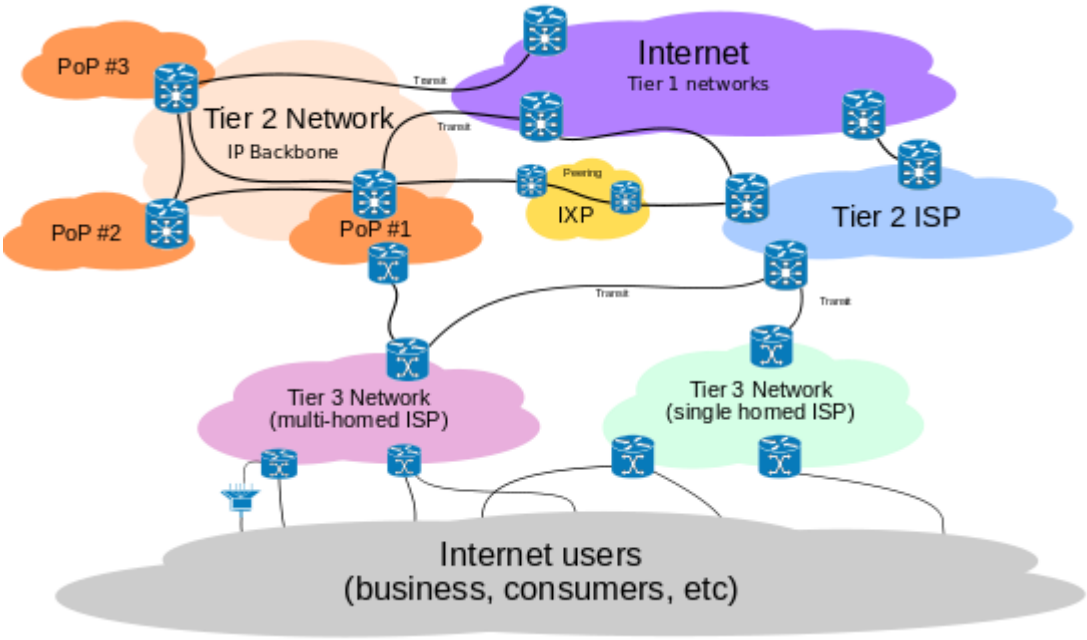
Answer:

- When Spamhaus was under attack it turned to Cloudfare, a content delivery network and distributed DNS service provider. Cloudfare successfully mitigated the attack and hence Spamhaus was still online with its services. The perimeter of the attack included the organization's website as well as the Tier 1 internet exchanges.



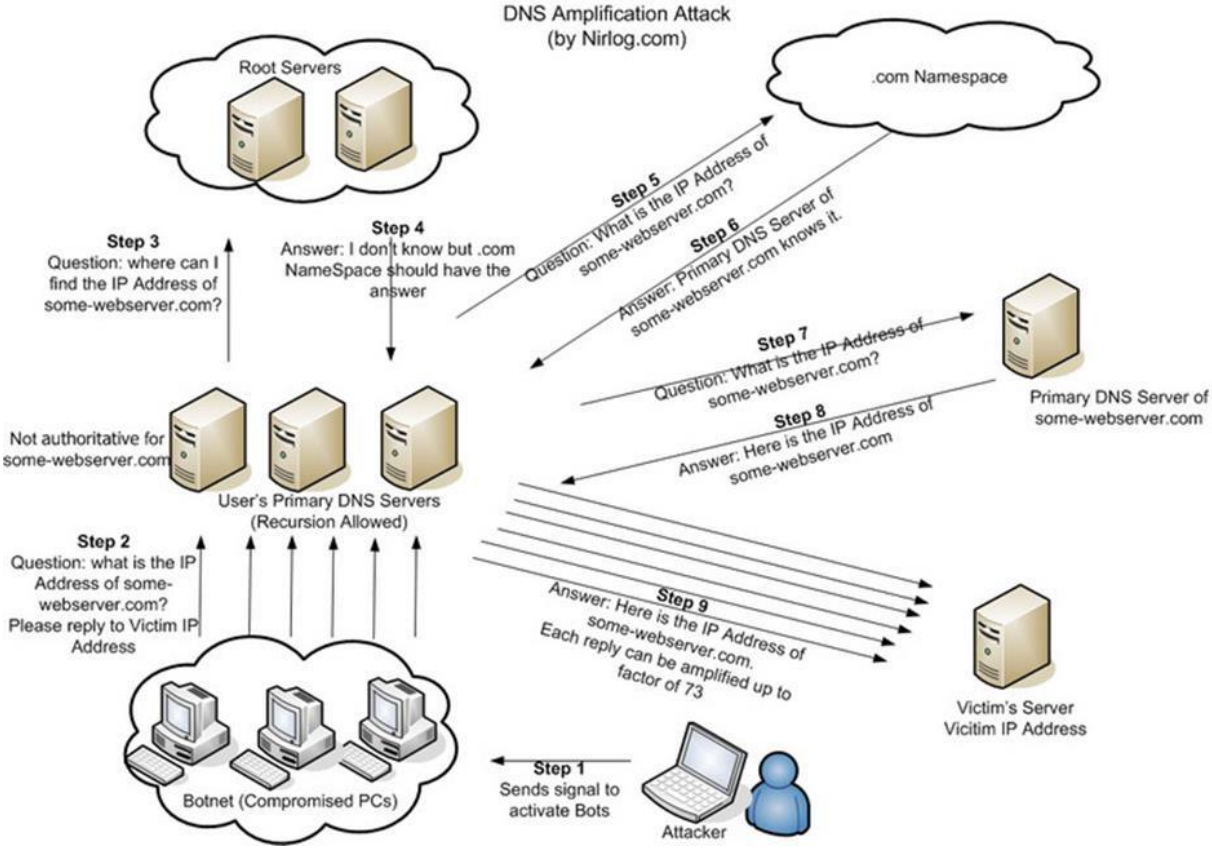
- The attack started with a 10 Gbps of attack force mainly coming from open DNS recursors. The next day, March 19, the attack increased to 90 Gbps and stayed prevalent to around the next two days. From then on March 22, the attack bandwidth reached 120 Gbps causing a very high load on the network. Cloudfare's Anycast technology came to the rescue, which managed the huge load and distributed it over its data centers all over the world. Since the Internet is an interconnection of different networks and they each maintain a connection through different routes, Cloudfare used this model to distribute its network load by connecting to large networks and other carriers through which the traffic is routed. Also, it connects to its Internet exchanges where a large number of networks meet in a central point. With reference from

Cloudfare's architecture, we have Internet Exchanges in major cities. Cloudfare connects to these exchanges such as the London Internet Exchange, Amsterdam Internet Exchange, Frankfurt Internet Exchanges and few others. The globally used website networks like Facebook, Google also connect through these exchanges. When the attackers were unable to fight out this load distribution technique employed by Cloudfare they started hitting these exchanges for breaking the networks.



- According to reports by Cloudfare, there was tremendous amount of traffic in Europe, which was facing the peak of attacks. Amidst all this, we had on the same hand controversial talks of Cloudfare boasting its service for DDoS protection for this big attack that they were successfully able to mitigate. One such blog post was on Gizmodo which posted the whole hot controversy as "That Internet War Apocalypse is a Lie" and just a false hype. It claimed that Cloudfare was largely exaggerating the attack to affect the whole internet backbone. For Gizmodo, this appeared as a ploy through which Cloudfare tried to market its services since the internet records did not show any evidences of the services being slow over the period. In addition, the internet backbone is capable of supporting traffics worth Tbps bandwidths and it is hard to imagine that only a Gbps attack could bring it down.
- On investigating into the issue, the flaw was found due to a vulnerability in the configuration of the DNS servers available across the internet. In server terminology, there is an expression known as "resolvers." What this does is basically it replies with information about a particular address, domain or a site name and sends it back to the receiver. The loophole present on these DNS servers available on the internet was that they were configured with the open resolver functionality. If anyone asks for any information from these DNS servers, it will run a query and return the results to that particular entity. The hackers misused this functionality of the DNS servers, and to further add to the mishap they mixed it up with spoofed address for these DNS queries. An attacker spoofed an IP address for a particular website/domain that they wanted to

hit and sent a query to multiple DNS servers with the open resolver functionality. On receiving this query, we had these open resolvers sending in loads of information to the spoofed IP address that had been attacked, and thereby flooding its network. When we have multiple servers echoing the same information to a particular destination we can all imagine the amount of clogging it may cause. After this incident, The Open Resolver Project committee began investigating the issue and tracking the servers known open to these vulnerabilities. It is estimated that over 27 million servers were tracked with the open resolver functionality all across the internet. The only patch was to fix this vulnerability through secure configuration.



- It is suspected that the hosting provider Cyberpunker had sponsored this attack after the Spamhaus committee blacklisted it. Sven Olaf Kamphuis, a self-proclaimed internet freedom fighter, was suspected by the New York Times as he recently talked about bringing down the services of Spamhaus. Sven denied from this fact although still he is a strong suspect since he is also known as the prince of spam. There are still investigations going on to get to the actual suspect with some proof of evidence. Regardless of this fact, an attack of 300 Gbps or rather a larger future attack could definitely rocket out the whole internet network. To muster our defenses we have to focus on the fact of how important security is and the need to patching and securing publicly exposed infrastructures. We also have Best Current Practices 38 [BCP 38], a set of guidelines that would limit the effectiveness of some DDoS attacks. These are very old guidelines, but are yet to be implemented effectively. In order to have a safe internetwork we need cooperation and support from all the ISPs, enterprises and small-

scale networks, which indeed requires a lot of effort. During the past several months, there have been such incidences of DDoS attacks against US financial institutions like Bank of America, Citibank and JPMorgan Chase.

7. **(10 points)** Study the *Amazon Route 53* service and answer the following questions

   a. What does *Route 53* do?
   Answer: Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking. If you choose to use Route 53 for all three functions, perform the steps in this order:
   1. Register Domain Names
   2. Route internet traffic to the resources for your domain.
   3. Checking the health of resources.

   b. Why is it called Route 53?
   Answer: The name is a reference to TCP or UDP port 53, where DNS server requests are addressed.

   c. What other Amazon services is it designed to work with (please explain how it happens with one or two examples)?
   Answer: Amazon Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS.
   For example: Redirecting Internet Traffic to another Domain and Redirecting HTTP Requests to HTTPS

   d. What is the difference between the domain name and *hosted zone*?
   Answer: A **hosted zone** is an Amazon Route 53 concept. A hosted zone is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent **domain name**. All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix.

   e. Does *Route 53* have a default for the *Time-to-live (TTL)* value*?*
   Answer: Yes, Route 53 has a default for the Time-to-live value.

   f. What is the pricing of the service?
   Answer: The pricing of the service are as follows:

- **Hosted Zones :**
  $0.50 per hosted zone / month for the first 25 hosted zones
  $0.10 per hosted zone / month for additional hosted zones
- **Queries:**
  Standard Queries

$0.400 per million queries – first 1 Billion queries / month
$0.200 per million queries – over 1 Billion queries / month
Latency Based Routing Queries
$0.600 per million queries – first 1 Billion queries / month
$0.300 per million queries – over 1 Billion queries / month
Geo DNS and Geoproximity Queries
$0.700 per million queries – first 1 Billion queries / month
$0.350 per million queries – over 1 Billion queries / month

- **Traffic Flow:** *$50.00 per policy record / month*
- **Health Checks:**

	AWS Endpoints	Non-AWS Endpoints
Basic Health Checks	$0.50* per health check / month	$0.75 per health check / month
Optional health check features: • HTTPS • String Matching • Fast Interval • Latency Measurement	$1.00 / month per optional feature	

8. **(10 points)** Take a look at https://www.twistlock.com/2018/11/13/open-source-cloud-discovery-tool/ and learn what the Cloud Discovery service is. Explain how the tool works. What does it do? (Just research your answer and explain how you understand it.)

   Incidentally, this is the tool Amazon uses. Does *Route 53* provide a similar service? If so, how? What are the differences?

   Answer:
   - Cloud Discovery is an open source tool that helps infrastructure, operations, and security teams identify all the cloud native platform services, such as container registries, managed Kubernetes platforms, and serverless services used across your cloud providers, accounts, and regions.
   - Cloud Discovery is a powerful tool for audit and security practitioners that want a simple way to discover all the 'unknown unknowns' across environments without having to manually login to multiple provider consoles, click through many pages, and manually export the data.

➢ **Working of Cloud Discovery tool:**

- Cloud Discovery connects to cloud providers' native platform APIs to discover services and their metadata and requires only read permissions. Cloud Discovery also has a network discovery option that uses port scanning to sweep IP ranges and discover cloud native infrastructure and apps, such as Docker Registries and Kubernetes API servers, with weak settings or authentication. This capability is useful for discovering 'self-installed' cloud native components not provided as a service by a cloud provider, such as a Docker Registry running on an EC2 instance.
- Cloud Discovery is provided as a simple Docker container image that can be run anywhere and works well for both interactive use and automation. Cloud Discovery supports asset identification on AWS, Azure, and Google Cloud Platform but it's designed to be easily pluggable with support for more cloud platforms coming soon.

➢ **Comparison between Route 53 and Cloud Discovery Service:**

- Amazon Route 53 is a scalable domain name system (DNS) service intended to give business and developers a reliable way to direct end users to applications. ... Amazon Route 53 answers requests, known as "queries", to translate domain names into their corresponding IP addresses while Cloud Discovery makes it easy to discover all the cloud native services deployed across all your accounts and see them all in a consolidated report. Discover ECS clusters, ECR repositories, EKS clusters, and Lambda functions in use across every account and region. See verbose details about each of them in a simple, nicely formatted, HTML report. Designed to make it easy for auditors and security professionals to find rogue and unmanaged deployments, Cloud Discovery simply takes a list of accounts and IAM credentials at runtime and does the rest automatically.