Homework 4, David Rasoly

Question 1:

The problem that I chose to cover is DNS Infrastructure Hijacking Campaign, taken from https://www.us-cert.gov/ncas/alerts/AA19-024A.
The National Cybersecurity and Communications Integration Center (NCCIC), has discovered an attempt of Man In The Middle attacks on organization DNS Servers, by using compromised credentials. These attacks can exploit the DNS Servers by redirecting users traffics and encryption certificates involved with the hijacked servers.
Once an attacker has the credentials of a DNS server, it can take control or manipulate records of the servers files and databases, including cached addresses,Mail Exchange, and the name of the server itself. Since encryption certificates also takes place, the attacker can manipulate incoming and exploit user sensitive data.

To prevent these attacks, the following measures should be considered:

- Update credentials of the DNS servers.
- Enhance the credential level to multi factor authentication account.
- Verify that the public DNS records are indeed correct.
- Disable and block fraudulently requested certificates.

Question 2 :

1. SMTP message structure :
    a. Envelope - similar to actual mails and letters, an email also has an envelope which has sender and receiver properties. The sender and receiver are used by the SMTP server to indicate who is the sender and the receiver(s).
    b. Header - the first part of the content, which includes From - who the message is from - could be forged, To - who the message is addressed, Subject - placed by the sender as the subject of the email, Date - date and time which the email was composed, Received - the date which the server received the email.
    c. Body - the second part of the content, this is a sequence of ASCII characters.
2. While SMTP supports ASCII encoding, and doesn't support file sharing and multiple languages that may require richer encoding such as UTF8, the Multipurpose Internet Mail Extension protocol supports additional fields as an extension to the SMTP protocol, using additional headers such as Content-Type - describes the type of media, Content-Transfer-Encoding - specifies the encoding of the message body, Content-Description and Content-Disposition, which supports file names when attachment is involved.
3. POP3 vs IMAP
    a. POP3 stores mail locally, therefore it is always accessible even without an internet connection, unlike IMAP which requires connection.

    b. IMAP is available and accessible from multiple different locations, while POP3 stores emails locally and mark the downloaded emails as new mails at one client.
4. SMTP relay is a service that supports transportation of emails between email hosting services. It could be used maliciously by spammers - a spammer could send an email to a relay service, and by that could cause the service a slower bandwidth and IP blacklisting - as other services would treat this service as a spammer service.

Question 3 :

A proxy server acts as a gateway or a mediator between client(s) and a service. Let's assume that Alice is a ten years old girl that wants to buy a cookie at Bob's store, so instead of going to the store itself, Alice asks her father, Mr Proxy, to fetch some cookies.Alice father also made sure that each time Alice browses the web, it will go through a proxy server to limit her browsing time, prevent her from arriving to unwanted websites and keep general control and monitoring of how Alice can use the web.
Reasons for using proxy :

- Caching - the proxy server can cache data that is frequently used and thus have faster access to cached resources.
- Routing - routing specific requests to designated services and prevent certain requests by IP blocking.
- Logging - monitor the transportation of users in a network that uses the proxy, such as organization that would like the employees usage of the internet.

Question 4 :

A. Since neither the PC that I am using at Harvard doesn't know Yale's address nor the DNS server at Harvard, then it will attempt to resolve address of yale recursively, looking for the root, then edu server, from the end of the address to the beginning , doing the following steps : Reaching www.yale.edu .
    a. My computer at Harvard asks the Harvard DNS server for the www.yale.edu. Harvard DNS doesn't know the address for this website.
    b. Harvard DNS server asks the Root Server for this address, the root doesn't know Yale's address either.
    c. The Root Server tells Harvard DNS Server to ask the edu Server for the address. The edu Server doesn't know this address.
    d. The Harvard DNS asks for yale.edu for this address and finds it successfully.

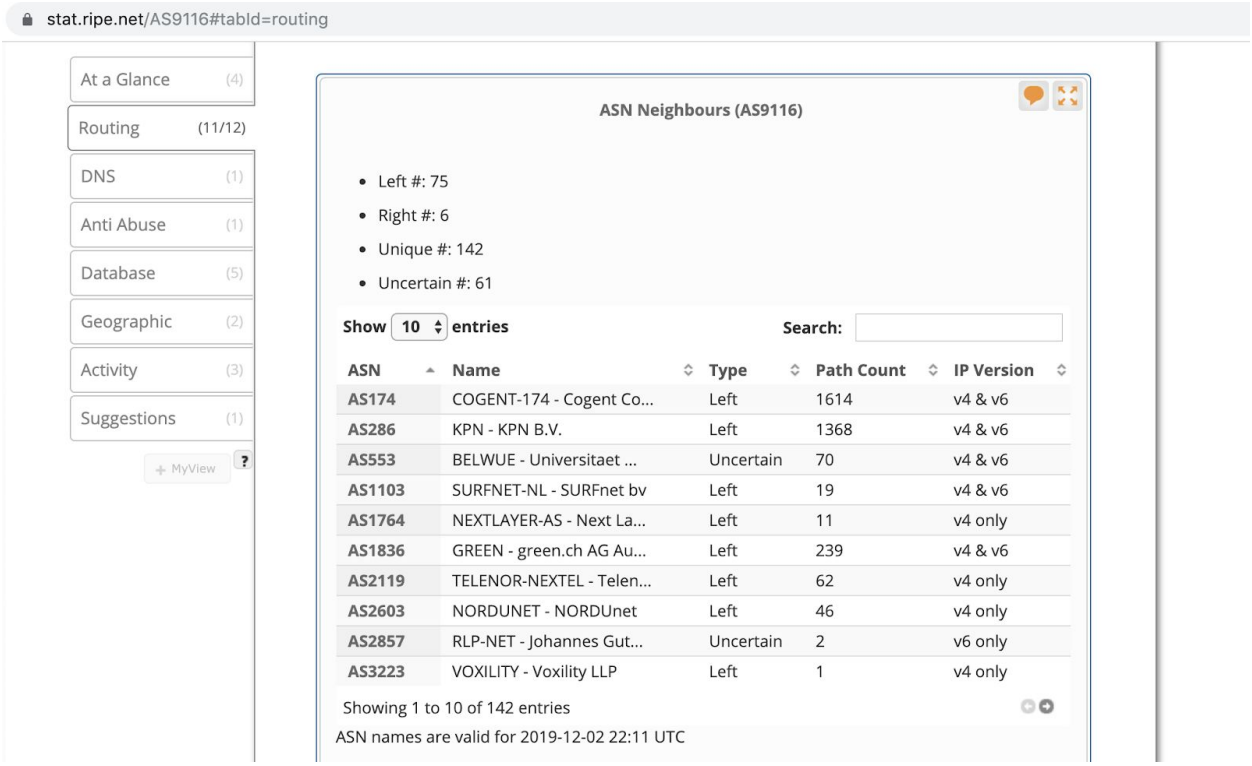
   A good tool to see it would be to use the command dig, which can describe the steps from a machine to a host.

B. At part A of the question, Harvard's DNS asks the Root Server for the address, how does it know what the Root Server is and what is its IP address? The administrator of the DNS server will have to seed the DNS with IP address of root servers. These address will be stored at the database of Harvard's DNS server, and deemed cached. Let's

assume that the steps at Part A of the questions has been executed, and now Harvard DNS server knows Yale address, if the address was cached - then the lookup for Yale's address will be faster, and will be reduced to step "a" instead of steps "a,b,c & d".

Question 5 :

A. Using the website www.whatismyasn.org, My public IP number is 87.68.57.141, surfing from Israel. My Origin AS is : "9116 , GOLDENLINES-ASN 012 Smile Communications Main Autonomous Systems", which is similar to the name of my ISP provider - "012 Smile Telecom, by Partner".
B. AS9116 is connected to other Autonomous System by BGP protocol. Using a website tool called stat.ripe.net (by European IP Networks), a lookup for an Autonomous System can be made along with other interesting statistics, including routing to AS Neighbours. As shown in the diagram below, we could see that that AS9116 is connected to 142 other Autonomous Systems.



Question 6 :

In September 2014, Some of Lenovo's Laptops had a pre-installed spyware called Superfish that allowed SSL interception of the browsing data from the user of the infected computer. SSL encryption allows other software to intercept and monitor browsing data of secured websites. One of the most popular Internet Browsers, Firefox, was infected by this malware, in result - Mozilla released a fix and there are several online guides about the incident along with a hotfix.

Superfish malware functioned as an interceptor by adding trusted root certificate to the Windows OS and Firefox root stores, and by that - gain authorization to inject content to secure location trusted with this certificate. The infected users had their private key of the installed certificate to be available to anyone with an internet connection, simply because Superfish installed the same certificate to all the infected computer, this means that if an infected A computer access a sensitive information, another infected B computer or a hacker that has this private key could use it to access this very sensitive information.

In order to reduce the damages caused by this breach, Lenovo instructed its users to remove superfish with detailed explanation and support. As for Firefox infected browser - it was impossible to remove the infection due to the root certification that Superfish installed, and a hotfix was deployed to fix this malware by Mozilla.

A suggestion to prevent such interception vulnarbilities at the future using browsers would be to allow safe SSL interception would be usage of addons, which are easier to use, configure and modify.