# Security Questions

1. Is security important, and why?

* It is obviously important because if we take an organization which contains customer info and their social and certain documents which cannot be accessed by others, It is the organization’s responsibility to see the information is securely stored which cannot be accessed by others. It can be done by implementing firewalls over the network to see if the hosts accessing the documents are authorized to use the services.

1. Which password is more secure against a brute force attack? Why?
   1. Dog
   2. Doh

* Brute force attack is a type of hacking passwords where a hacker uses a software or a certain script to generate some random possible passwords.

I would personally do not recommend any of the given passwords. A good secured password is a combination of Upper case, Lower Case, Numerical, and alphanumeric, which doesn’t follow a certain pattern which can be guessed.

Among the two options I prefer to use ‘Doh’ because it is little more secured compared to Dog which can be guessed easily.

1. How would you make either previous password more secure? Why?

* A good secured password is a combination of Upper case, Lower Case, Numerical, and alphanumeric, which doesn’t follow a certain pattern which can be guessed. I would add a certain combination to my existing password to make it more secure. It is suggestable to change our passwords once in every two weeks.

1. What is the difference between symmetric and asymmetric encryption?

* Symmetric has a same key for both encryption and decryption, whereas asymmetric has different keys for both encryption and decryption.

1. Someone calls you saying they forgot their password to a locked workstation and they need to get a file to the president of the college right away and they will inform the president that you wouldn’t help them thus resulting in the college being audited by the federal government. All you have to do is set their password in Active Directory and tell them the new password, what do you do?

* I would ask for their credentials first, cross check them with the details on the file. Ask them the security questions and match their answers with the answers on the file, then I will send an authorization code to the phone number on the file and ask them to verify the code received, this way I know the person calling is not a hacker, then I would set their password in Active Directory. I feel sending temporary authorization code to email is not the best way because the probability of an email getting hacked is more compared to phone number.

1. What’s the difference between encryption and encoding?

* Encryption is encapsulating the original information, this way the original information is not exposed to unauthorized users.
* Encoding is setting a password or passcode to the encrypted information. Password will be given to the one receiving it, once the destined user receives it he decode it with the password given.

1. Why should you use HTTPS when logging into a system?

* The main purpose of HTTPS is to make sure confidentiality, integrity and identity of the information we try to reach. HTTPS server keeps our information remains confidential from hacking eyes by decrypting the traffic. Integrity protects the data from being modified without our knowledge. Identity will be kept anonymous.

1. Why would you use DNSSec?

* The purpose of DNSSEC is to increase the security of the Internet as a whole by addressing DNS security weaknesses. Essentially, DNSSEC adds authentication to DNS to make the system more secure.

1. When accessing a website you’re presented with a SSL/TLS certificate issue, what would you do?

* If the website that I’m trying to use is accessible over http then i proceed with my troubleshooting. If i still see an issue, I would like to install SSL Diagnostics tool like SSLDiag for further troubleshooting.

1. A device on the network is continuously trying to login to an account, the system used has no lockout. What do you do?

* We can target account ID of the device for further action.

1. What issue(s) exist when using symmetric encryption when two parties can only communicate online?

* They need to have a safe way to get the key to the each other.

1. If given the option of RSA or Elliptic Curve Encryption, which would you use and why?

* My option is to prefer Elliptic curve encryption in some cases because, we can use smaller keys even for high level of security and fast key generation, which is because of its fancy algorithm.

1. What is the difference between authentication and authorization?

* **Authentication** is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating.
* **Authorization** is the process of verifying that you have access to something. Gaining access to a resource because the permissions configured on it allow you access is authorization

1. If a web application has a vulnerability, does that mean it’s exploitable?

* Yes, to exploit a vulnerability, an attacker might had at least one applicable technique that can connect to a system weakness.

1. In security it’s important to uphold three pillars: Confidentiality, Integrity, and Availability. If an attacker gets a copy of an encrypted file you made and guessed your password thus getting access to an excel file of social-security numbers, names, and addresses, which pillars have been compromised.

* To my knowledge it’s **Confidentiality**.

1. A single-threaded web application is reading data from a ring buffer; however, a vulnerability exists in which a user can pass in data at a slower rate than the application is reading, thus resulting in **null** being read and the application crashing. What type of vulnerability is this?

* I hope it is format string vulnerability.

1. An attacker has exploited a system inside your network of 4k+ devices. There’s a stateful firewall that sits in-between the attacker and the compromised device on the border of the network. The firewall has a signature for a sequence of traffic going to any one given device on the network, a sequence the attacker must use to communicate with the compromised device. How might the attacker do this?
2. An employee in the organization has gone rogue, they need to get a file (not a picture) on their workstation outside the organization to sell. There’s currently software called Data Loss Prevention on the machine that scans all outgoing traffic for a barrage of signatures looking for the data they’re trying to take. How could they get the data off the machine?

* There might be chance of using external devices like USB or hard drive.

1. How would you diagram a setup with the following systems:
   1. Web server
   2. Authentication server
   3. File server
   4. Database server

* I will prefer to setup this system as following,

File Server 🡪 Web Server 🡪 Authentication Server 🡪 Database Server

1. Diagram how a buffer overflow works Diagram how a buffer overflow works.

Parent routine ssssssssssststackstack

Stack growth

buffer

Buffer overflow

High address

Low address

Local variable

Return Address

* Sketch of the stack when buffer overflow occurs. Generally, data in stack stores in FIFO (First in, first out) order.