1)     Two common authentication bases are something you have such as a smart card and something you are such as a fingerprint or other form of biometric methods. There is also another one which is something you have such as a staff card.

2)     The common resources that can be targeted in DoS attacks are network bandwidth for network and memory storage and the processor capacity for the computer.

3)     In multilevel access control every subject or object is given the clearances and classification of sensitivity and access is determined by a set of rules such as the Bell-La Padula (BLP) rules.

4)     Canary values are used to protect against buffer overflow by overwriting more memory than the buffer, or space provided to write. They will modify a program’s stack frame to detect the buffer overflow but it doesn’t not prevent the attack.

5)     Lamport’s one-time password scheme relies on using hash functions that are collision resistant and one-way. Collision resistant means that there is little to none possibility that a hash function can produce the same hash digest from two different input. And one-way means that the hash function takes any input and produces a hash digest, and it is not possible to obtain the hash digest input.

6)     Two classes of intruder that an intrusion detection system may attempt to find are clandestine which tries to avoid the intrusion detection or auditing system and masquerader, which is to pretend to be a legitimate user.

7)     A master password is typically used to protect against your other passwords. It is like a key to a safe. If you have the correct key, you can open the safe. So this means that if you have the right master password, you can access your other passwords.

8) is capable of distinguishing between humans and computers.

9)     Data aging in the context of intrusion detection systems relates to ensuring that we do not rely heavily on old statistic. Collecting data over a period, and taking all of this into account, we should weight the data as a function of time.

10)  Phishing emails are typically sent in bulk because there is a higher chance of someone getting fooled by it. And thus getting phished.

11)  The Biba model is for the purpose of preventing data modification by someone who isn’t authorized, it also prevents unauthorized data modification by someone who is authorized and maintain internal and external data consistency, while BLP is for the purpose of data confidentiality and controlled access to classified information for example a person cannot convey information to another person who is of a lower level therefore is a model that protect against unauthorized disclosure of information.

12)  Inference is the derivation of conclusions from given information or premises by any acceptable form of reasoning

13)  “Online” and “offline” attacks differ in that online attack requires the connection to be active which might pose some restriction while trying to break the password while offline attack have unlimited chances to break the password.

14)  The term “shellcode” refers to a set of machine instructions an example will be codes that starts a command shell (CMD) which will exploit a vulnerability of a software in the context of hacking.

15)  XSS stands for cross site scripting. Which is a form of injection attacks that an attacker can use to send a malicious script to unsuspecting people which then exploits the vulnerability of the software or web page.

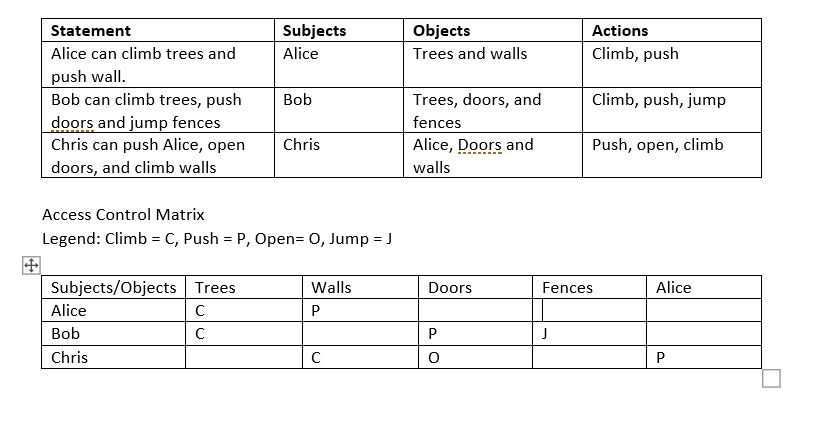
16)  The purpose of sanitization in the context of auditing is to remove any information when there is a user which is not allowed to access or see the information.

Part b

1. Authentication is the act of validating the users of who they are supposed to be or claimed to be through passwords, one-time pins, authentication apps and biometrics. In some cases, the system requires more than one successful factor before granting access to the user. Whereas Authorization is the process of giving the user permission to access specification information. In an secure environment, authorization must always follow authentication. So the person have to first prove their identity through the authentication before getting any authorization. So to summarize authentication is to confirm users are who they are and authorization gives the user permission to access information
2. The three distinct type of attacks against password systems are brute-force attack, dictionary attack and hybrid attack. A brute-force attack is trying all of the possible combination of the password until it gets it right. A dictionary attack uses a dictionary of all known words and try to find the password. Hybrid attack is the combination of both the brute-force and dictionary attack where they use the dictionary as the basis but take variants on each of the words tested. To protect against these forms of attacks, we can use words that are not commonly found in the dictionary or use random words. Another method will be to use salt and regularly change the password.
3. The first outcome an attack may aim for with a buffer overflow attack is to first introduce extra codes and sending this new instructions to the application to gain access to the IT system and another outcome is to overwrite and crash the system. The attack works by using a Denial of Service (DoS) attack where by too much data on the memory will make the stack to be overwritten, if too much formation has been overwritten on the stack, the system might not be able to function and will crash, or the attack can just overwrite enough information on the stack to cause the pointer to point to the attacker’s code and hence allowing the attacker to gain access to the system.
4. The salt is a randomly generated value. It is used in hashing where instead of only the password being hashed, the password is then combined with the salt value and then hashed together. The salt will be stored separately somewhere. This is used so that the adversary have many combination to try from with many salts and delay the attackers from finding the correct password hash.
5. Encrypted virus is a conceal virus that avoids detection. It is encrypted with a cipher. Since it is able to get pass detection, it will easily access the system without being caught by the intruder detection system (IDS)
6. The two primary properties used in malware classifications is that it needs a host program, and another is independent. The two distinct methods of identifying a virus is manipulation detection codes and signature scanning
7. Honeypots is used to divert attackers from a critical system and collect information about the attacker’s activities. They try to hold the attackers on the system long enough for the administrators to respond to it.

Part c)

1. The diagram refers to the construction of client puzzles
2. H represent the hash
3. The x[j](k+1, L) is sent to the client
4. The client will respond with the x[j](1,k) to be joined with x[j](k+1, L) to get y[j]
5. The client will be expected to do minimal work so the authentication can be fast
6. Yes, answers from client has to be unique as each connection is unique. The answer have to match with the server secret. Hence it will be unique
7. Unix protects their user password by hashing it with a salt value that is randomly generated the password is combined with the salt value and hashed together then the salt is stored elsewhere.
8. Method B will be better at generating a stronger password. This is because the number of possible combinations in method B is higher than method A. However, it is important that the attacker does not know the pattern of creating the password otherwise the attacker is able to break the password easier due to the pattern.
9. The two type of error rates that occurs in authentication systems are False Rejection Rate (FRR) and False Acceptance Rate (FAR). FRR is the proportion of authentication attempts that results in false rejections and FAR is the proportion of authentication attempts that results in false acceptance



b) Alice : (Trees, Climb), (Walls, Push)

    Bob   : (Trees, Climb), (Doors, Push), (Fences, Jump)

    Chris : (Alice, Push), (Doors, Open), (Walls, Climb)

c) The two list will be Bob and Chris because together they have all the objects mentioned

d) An example will be if Alice is a manager then allow read/write access to information

1. The major components in an IDS are Agent, Director and Notifier. The job of an agent is to collect data from a set of hosts. The job of the director is to further analyses information using the analysis engine. And it runs of different system, so attackers won’t be able to compromise it. And lastly the notifier job is to notify the correct party regarding reports from the director.
2. The three different types of firewalls and their functionalities are:

Proxy Firewalls, they run at the application layer to filter out incoming traffic between our network and the traffic source.

Software firewalls, they are firewalls that are installed on a local device. They isolate individual networks endpoints from one another

Packet-filtering firewalls, they have a collection of rules based on TCP or IP whereby the incoming and outgoing IP packet is weighted and then forwarded or discarded.

1. It is a single firewall with three network interfaces. The first interface is the public interface and it is connected to the internet. The second interface is to connect to a demilitarized zone which public services are attached. And Lastly the third interface is to connect to the intranet for access to and from the internal network
2. A firewall cannot protect against internal attackers and viruses.
3. Direct attacks is getting the information of individual element directly from the database and indirect is through sufficient number of information through individual elements of data which then needs to be inferred to get the information you want.
4. The three methods are query set restriction, Data perturbation and Output perturbation

Query set restriction suppresses sensitive information whereby we do not disclose an output when the query set is either too big or small.

Data perturbation through data-swapping so that the statistic that are constructed are false data used in a modified database which is still consistent with the original.

Output perturbation is similar to data perturbation, but it is achieved by distorting the statistical output, one of the method is using random-sample query method.

select123 \*

from123 students

where123 dept = %d

group123 by123 gender