STUDENT NAME: CHONG HUI WEN

UOW ID: 7311436

PART A:

1. Password-based authentication and multi-factor authentication.

2. Network Bandwidth Consumption (for network) where the volume of traffic is reached and further traffic cannot be transmitted, or Memory Starvation Attacks whereby memory storage and processor capacity (for computer) is fully utilized.

3. Security labels, where the subjects are given labels that corresponds to the clearances, which every user has a clearance and objects are given labels that corresponds to classifications or sensitivity, which every action/operation has a sensitivity rating.

4. Buffer overflow by placing a known values between a buffer and control data, just before the return address and to check that it hasn't changed so the attacker isn't able to overwrite it.

5. Only used for one session or one transaction. It typically consists of two parts; the set-up and the process.

6. Masqueraders, who are illegitimate users that are imitating legitimate users and Misfeasors, who are legitimate users misusing the privileges that they have.

7. Social engineering and communication eavesdropping, as having a master password removes the need to remember dozens of passwords and prevent users from choosing very simple weak or duplicate password.

8. Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), as it makes use of the human ability to correct distortions in images and typically performs image recognition far better than existing automated systems.

9. Whereby valuable data does not get stolen by attackers as aging data most likely refers to old data that might seem valuable to attackers as but might not be that essential to the organization as it might be old statistics.

10. The attacker cannot expect to fool most people but only hope to fool just some.

11. Biba model is for the purpose of integrity control while BLP is for the purpose of access control. Integrity control refers to that the Biba model protects against unauthorized modification of information whereas access control refers to BLP

model protecting against unauthorized disclosure of information.

12. Derivation of sensitive information from non-sensitive, typically aggregate data.

13. Differ in that online attacks require the connection to be active which may impose certain restrictions while attempting to break the password, whereas offline attacks have unlimited attempts to break the password.

14. Shellcode refers to inserting your own code into the buffer, in the context of buffer overloading.

15. Cross-site scripting, which is a type of injection attacks used by attackers where they can send a malicious script to unsuspecting user and exploits vulnerabilities of dynamic web pages. In particular, by involving the use of such vulnerabilities to gather data from a user that should not be gathered.

16. Prevent cross-contamination, in which removing information that a user should not be able to see to provide confidentiality.

PART B:

1. An authenticated user is a non-anonymous user whose identity has been confirmed and such user can then access the system. Whereas an authorized user is a user that has the required permissions to access a particular file, or is in a group/role that has the required access permissions.

2. The three types of attacks against password systems are dictionary attack, a brute-force attack and hybrid attack. A dictionary attack makes use of a "dictionary" of all common known words and try to find out the password, whereas Brute-force attack refers to the trial of trying all the possible combinations of the password until it is correct. Hybrid attack refers to the combination of brute-force and dictionary attack where we make use of dictionary as the basis but take variants on each of the words tested. Countermeasures against dictionary attack can include making use of words that are not commonly found in the dictionary or random words that does not make sense. Alternatively, we can make use of salt and frequently change the password.

3. Two outcomes an attack may aim for with a Buffer overflow attack include exploitation by them to cause an attack against availability, such as denial of service and by running some arbitrary code to steal valuable information (attack on data confidentiality) and modify data (data integrity attack).

   Buffer Overflow are usually the result of poor coding, particularly for C and C++ programmers as they are vulnerable to the temptation of using unsafe yet easy-to use string-handling functions such as strcpy(). It occurs because of the way that memory and memory management works due to when more information is placed in a buffer than it it meant to hold.

BUFFER (8 BYTES)								OVERFLOW	
U	S	E	R	N	A	M	E	1	2

4. Salting refers to the salt used in UNIX based password system, where the password and salt is hashed to hide the relationship between a user and the password used. Salt refers to a value that is randomly generated. UNIX based password systems do not store password directly in UNIX but in an encrypted file using a password known by the system. It is used in hashing where instead of having only the password being hashed, the password is combined with the salt and then hashed. The salt that is stored is somewhere too, and such method is used so that the attacker would have many combinations to try with the salts to and can used to slow down some attackers to prevent them from finding the correct password hash.

5. An encrypted virus is usually encrypted with a cipher to avoid detection. The virus code is encrypted, except for the decryption routine and key. It does so by encrypting documents and files that are valuable and renders them unreadable by

the applications that created them and is smart enough to leave the system files alone so that it goes undetected.

6. Two primary properties used in malware classification are based on how it spreads or propagates to reach the desired targets and next, the payloads it performs once a target is reached. Two distinct methods of identifying a virus includes monitoring, as the normal behaviour of a system is typically different from the activity profile of an infected system. For instance, virus monitors monitor known methods of virus activity, such as attempts to write to system files, write to a boot sector, modify interrupt vectors and detect abnormal behaviour of the system. Signature Scanning can also be used, and signature extraction is a non-trivial process. The infection is disassembled and the key portions are identified, before the key portions are combined to form a signature and the signature is checked against a large library of programs to reduce the chance of false positives occurring when signature accidentally matches some library code.

7. Honeypot is typically a decoy that is used to lure attackers away from the production system, and usually a computer attached to the network that runs special software that replicates services, applications and protocols and can be used to divert attackers from a critical system and buys some time for the administrators to collect information about the attacker's activities and to respond to the attack. In the case of intrusion detection system, it acts as a decoy.

PART C:

1.

a) Unix protects user passwords by using salting and hashing. As in UNIX based password systems, the passwords are not directly stored. UNIX based password systems do not store password directly in UNIX but in an encrypted file containing hashes of the password is stored using a password known by the system. The password is inputted when the system is booted and makes use of salting. The salt refers to a value that is randomly generated, and the hash of the combination of the salt and the password is stored. Salt that is stored is somewhere too. It makes use of an hashing algorithm called crypt to protect its password, via a one-way transformation of the password by the one-way hash function. Each encrypted password is a a 13-character stored string constructed by crypting the password concatenated with the salt, with the salt value being random and from a large enough space to ensure that has the advantage of giving different encrypted passwords to users with the actual same password.

b) The chances of choosing Method A provides a stronger password. Although the second methods seem more complex, but because the pattern of creating a password is known to an attacker, this reduces the entropy of the password, and hence the complexity.

c) The two types of error that occur in authentication systems are False Acceptance Rate (FAR) and False Rejection Rate (FRR). False Acceptance Rate (FAR) is the proportion of authentication attempts resulting in false acceptances, and False Rejection Rate (FRR) is the proportion of authentication attempts resulting in false rejections.

d) An example of a Lamport's One-time password as follows:

1. Setup
    a. In the setup process, a user is selecting a password that is secret to him/her
    b. In the setup process, a user is selecting a password that is secret to him/her
2. Process:
    a. A user, let's say Alice, request for connection to a server.
    b. The server issues a challenge n;
    c. The user responds with one-time password which is generated as $h\ n{-}1\ password$
    d. The server checks if $h\ h\ n{-}1\ password = h\ n\ password$
    e. If it matches, then server accepts the communication request. If it does not, the server rejects the communication request.
    f. Once the user has been authenticated, the server needs to update its information.
    g. The system will then replace $xn = h\ n\ password$ with the one-time password sent by the user's, that is, $xn{-}1 = h\ n{-}1\ password$.

h. The value n is replaced by $n - 1$.
i. When n reaches 0, the system will have run out of passwords in the hash chain and will have to run a new setup process, with a new base password

2.

a)

Object Subject	**Trees**	**Wall**	**Fences**	**Door**	**Alice**
Alice	Climb	Push			
Bob	Climb	Push	Jump		
Chris		Climb		Open	Push

b) Access Control List: (ACL)

Trees: (Alice, Climb), (Bob,Climb)
Wall: (Alice, Push), (Bob, Push), (Chris, Climb)
Fences: (Bob, Jump)
Door: (Chris, Open)
Alice: (Chris, Push)

Capability List: (CL)
Alice: (Climb, Trees), (Push, Wall)
Bob: (Climb, Trees), (Push, Wall), (Jump, Fences)
Chris: (Climb, Wall), (Open, Door), (Push, Alice)

c) Access control matrix/list is used to restrict subject from accessing objects that the subject is not authorized to act on. Capabilities is from the perspective of subject, and access control list is from the perspective of objects. If we want to efficiently determine all the available to a subject, the capabilities list is more efficient because capabilities list shows/lists all the objects the subject can access, and the operations/authorization allowed to access those objects.

d) There are two types of Attribute-based Access control, namely subject attributes, or Object Attributes. For instance, allowing only users who are type=employees and have department=HR to access HR/Payroll system, and during only business hours within the same time zone as the company. This prevents from unauthorized users and actions from accessing information that they should not be allowed to see.

3.

a) The Context of this diagram refers to the construction of client puzzles.
b.
b) h refers to the hash function
c) X[j](k+1,L) is sent to the client. This is generated by taking a sub-puzzle and taking k bit as the solution of the puzzle

d) The client should respond with x[j](1,k) to be joined with x[j](k+1,L) to get y[j].

e) The client is expected to do minimal work so that the authentication can be fast.

f) The answer from the client is unique because the client needs to submit the correct solution to gain a connection, to prove that only a live user, not a zombie machine for example, will actively work on answering the problem appropriately.

4.

a) The three major components of IDS include Physical Intrusion Detection Systems, Network-Based Systems and Host-Based Systems. Host-based systems aid in identifying unauthorized behavior ion a specific device basis and it monitors data and can alert the user if any suspicious activity is happening. Network based systems makes use of network intrusion systems, through hub packets, network taps, or span ports to gather all the data for the network. Once the data is processed, the system flags any activity that looks suspicious and lastly, Physical Intrusion Detection Systems includes access control systems that are used to secure any entryway, such as making use of biometrics that scans for fingerprints or card readers to verify identity before allowing access. Motion sensors that detect motion can be used to send out alerts if motion is detected in an area that shouldn't be accessed at a specific time or day.

b) The common types of firewalls include Packet-filtering firewalls, Stateful inspection firewalls or stateful packet filtering and MAC layer firewalls. A packet filtering firewall has a collection of rules, in which each incoming and outgoing IP packet is weighed up with respect to the rules, and then either forwarded or discarded. The rules are typically based on IP or TCP header fields, If a rule is matched, we determine whether to forward or discard the packet and If there is no match to any rule, then a default action is taken.

Stateful Inspection firewalls is useful for filtering traffic built on stateless protocol such as UDP. It allows UPD packet in (carrying a response) only as a response to a previous outgoing UPD packet (carrying a request) and the firewall must remember outgoing UPD packet.

MAC layer firewalls operate at the data link layer and typically specify the specific traffic allowed from/to a network interface card, or something similar.

c) The Screened-subnet firewall system is the most expensive, and the most common setting whereby two packet-filtering routers are used and creation of an isolated sub-network, the DMZ is used.

d) A firewall cannot protect against internal attackers or services that bypass the firewall such as dial-up connection.

5.

a) We made use of methods such as Identity based policies, whereby only students are allowed to access information from the website and lecturer teaching the module are allowed to modify the contents of the web page. Role based access control (RBAC) were also used in lectures, where students (role) are only allowed to access information given to them

and others were hidden. Multi-level policies such as the Bell-LaPadula Model prevent sensitive data to be restricted and specifying allowable paths of information flow in a secure system. Lastly, the Biba Model ensures that a subject can modify an object if the integrity level of the subject dominates the integrity level of the object. This is the no write up policy.

b) Statistical databases refer to an aggregate-query interface, where information is provided by means of statistical (aggregate) queries on an attribute (column) of a relational table. It is primarily defined based on the data or information that it provides.

c) Data perturbation can be used in statistical database to change the values in the database such that the statistical information is accurate, but the inferential data is inaccurate to provide protection against inference attack. Output perturbation can also be used as well, whereby the results are fairly accurate but inference to leak little information about the individual data. One such common method is the Random-sample query method,

d) Syncookie provides protection against connection-based denial of service by not dropping connection when the SYN queue fills up until the server receives a “correct” ACK from the client. At this time, the server can reconstruct the SYN queue entry and then connection proceeds as usual.

e) Picture-in-picture attacks refers to having two windows, the outer real window, and the inner fake window where attackers get unsuspecting users to visit a website and makes use of images to generate fake browser look-alike inside the main window.

Homograph attacks refer to the method of deception in which that a malicious party deceives unsuspecting users about what the remote system they are communicating with and exploit the fact that many characters look alike. For example, a regular user might not be able to spot the difference between I (i in caps) and l (L in small letters).