Name: Chng Yia Qing Whitney
UOW No: 6956865

Part A

1) Two common authentication bases are What the subject knows and What the subject has.

2) Two common resources that can be targeted in DoS attacks are network bandwidth (for network) or memory storage and processor capacity (for computer)

3) In multilevel access control every subject or object is given clearances and classification, or sensitivity and access is determined by a set of rules, for example, Bell-La Padula rules.

4) Canary values are used to protect against by buffer overflow attack. Canary values do this by placing known values between a buffer and control data on then stack to monitor buffer overflows.

5) Lamport's one-time password scheme relies on using hash functions that are one-way and collision resistant. One-way means the hash function takes in any input and produces a hash digest, and there is no way one can obtain the input from the hash digest. Collision resistant means there is no possibility (very small) that a hash function can product the same hash digest from two different input.

6) Two classes of intruder that an intrusion detection system may attempt to find are Clandestine, who try to avoid the intrusion detection or auditing system and Masquerader, who pretends to be a legitimate user.

7) A master password is typically used to protect sensitive information such as other passwords and certificates.

8) CAPTCHA is capable of distinguishing between humans and computers.

9) Data aging in the context of intrusion detection systems related to ensuring that the data does not over rely or heavily rely on old statistics by weighing data as a function of time.

10) Phishing emails are typically sent in bulk because the attacker cannot expect to fool most people, the attack just hopes to fool some.

11) The Biba model is for the purpose of Integrity Control while BLP is for the purpose of Access control.

12) Inference is the derivation of sensitive information from non-sensitive, typically aggregate data.

13) "Online" and "Offline" attacks differ in that, online attacks require the connection to be active which may impose certain restrictions while attempting to break the password while offline attack has unlimited changes to break the password.

Name: Chng Yia Qing Whitney
UOW No: 6956865

14) The term “shellcode” refers to a small piece of code that is introduced in the command shell in the context of being used as the payload to exploit the vulnerability of a software.

15) XSS stands for an abbreviation for cross site scripting. It is a type of infection attack where an attacker can use it to send a malicious script to an unsuspecting user.

16) The purpose of sanitization in the context of auditing is to remove any information from log entries for which there is a user who is not allowed to see that information.

Part B

1) An authenticated user is a user who has been successfully identified by the system for example, logging in to email using username and password, this user will then be allowed to access the system. An authorized user is a user that has individual permissions to access a file or in a group or has a role that has the permissions, like reading or writing.

2) The three distinct attacks are dictionary attack, brute-force attack, and hybrid attack. A dictionary attack utilizes a “dictionary” that consists of all known/common words, steps through the words that can be used as sets of passwords to try. Brute-force attack is trying every possible combination of password until it is correct. Hybrid attack is a combination of dictionary and brute-force attack. This is where a “dictionary” is used as a basis but with variants with each of the words tested. A countermeasure against a dictionary attack is to use words that are not commonly found in a dictionary or to use random words.

4) “Salt” is a randomly generated value. It is used in hashing where instead of hashing only the password, the password is combined with the salt and then hashed. This “salt” is then stored somewhere else. This is to hide the relationship between a user and the password used. This way of protecting the password is used so that in the case where the “attacker” manages to get the password file, the “attacker” has numerous combinations to try the password that has many salts, this delays the “attacker” from finding the correct password hash.

5) Encrypted virus is a virus that encrypts its payload with the intention of making detection of the virus harder. The virus gets into the system (can be through infected attachments through emails, suspicious links) and starts encrypting documents and files on the system. The virus makes files unreadable and the only way to decrypt the files is to have access to the encryption key used in the encryption process.

6) Two primary properties used in malware classification are firstly, based on how it spreads or propagates to reach the desired targets, and then on the actions or payloads it performs once a target is reached. The two distinct methods of identifying a virus are signature-based protection and behavioral detection. Signature-based protection has its own existing database of known infection database, when an “attack” or “threat” is identified, this threat will then be attached

with its own signature. Behavioral detection is a method that monitors the actions of installed programs for any potential threats.

7) A honey pot is a decoy that lures attackers away from production systems. It is usually a computer attached to the network that runs a special software to emulate services, application, and protocols. Honeypots can be used to rule the attacker to stay on the system long enough for the administrators to respond to the attack. In this case, the honeypots act as decoys in the intrusion detection and prevention system.

Part C

Question 1

a. Unix protects passwords as it uses a hashing algorithm called crypt. What this does is that the protection is through a one-way transformation of the password by a one-way hash function.

b.

Choosing a six-digit number:

Entropy: $\log_2 N^l$

= $\log_2 10^6$

= 6 $\log_2$ 10 = 6 x $\frac{log10^{10}}{log10^2}$ = 19.93 bits

Complexity = $2^{19.93}$ = 998,913.34

Choosing a letter (upper or lower), followed by two digits, followed by a lower-case letter, followed by one digit, then by symbol *.

A letter (upper or lower)	52
Two digits	10^2
A lower-case letter	26
One digit	10
A symbol *	1

Entropy: 1 x $\frac{log10(52\ x\ 100\ x\ 26\ x\ 10\ x\ 1)}{log10^2}$

= 1 x $\frac{log10(1{,}352{,}000)}{log10^2}$

= 20.37 bits

Complexity = $2^{20.37}$ = 1,355,130.16

From the computation above, the second method is more complex. The entropy is higher at the same time which means the pattern is harder to identify. Hence, the second method is better for generating a password.

c. The two types of error that occur in authentication systems are False Acceptance Rate (FAR) and False Rejection Rate (FRR). False Acceptance Rate 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.

Question 2.

Subject	Alice	Bob	Chris		
Object	Tree	Wall	Door	Fence	Alice
Actions	Climb	Push	Jump	Open	

a. Control Access Matrix:

Subject/Object	**Tree**	**Wall**	**Door**	**Fence**	**Alice**
Alice	Climb	Push			
Bob	Climb		Push	Jump	
Chris		Climb	Open		Push

b.

Access Control List:

Tree: (Alice, climb), (Bob, climb)

Wall: (Alice, push), (Chris, climb)

Door: (Bob, push), (Chris, open)

Fence: (Bob, jump)

Alice: (Chris, push)

Capabilities:

Alice: (Tree, Climb), (Wall, Push)

Bob: (Tree, Climb), (Door, Push), (Fence, Jump)

Chris: (Wall, Climb), (Door, Open), (Alice, Push)

c. Access control matrix is used to restrict a subject from accessing object(s) that the subject is not authorized to act on. Capabilities is from the perspective of the subject, and access control list is from the perspective of objects. To efficiently determine all actions available to an object, the access control matrix list is more efficient because it shows the access from the object perspective, basically showing which subject and action that is associated with the object.

d. An example of an Attribute-Based Access Control would be allowing users who are of type employees and have a department HR to access the HR system and only during business hours within the same time zone as the company.

Question 3.

a. The diagram refers to the construction of client puzzles.

b. h is the hashing function.

c. x[j](k+1,L) is sent to the client.

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 should be unique because the process is stateless. The information is contained within the solution itself that exists in the server.

Question 4.

a. The major components in an IDS are agents, director, and notifier. The agents gather data from sources, log files, networks, or other processes. They will then pre-process the information before handing it over to the director. The director gathers information from agents and further analyses the information using an analysis engine and the notifier notifies the appropriate party regarding the reports received from the director.

b. The three types of firewalls are packet-filtering firewall, stateful inspection firewall and application-level gateway. Pack-filtering firewall has a collection of rules, each incoming and outgoing IP packet is weighed up with respect to the rules and then either forwarded or discarded. Stateful inspection firewall monitors communications packets over a period of time and examines both incoming and outgoing packets. It monitors all sessions and verifies all packets. Application-level gateway filters incoming node traffic to certain specifications, which means that only transmitted network application data is filtered.

c. A screened-subnet firewall system is a model that uses three important components for security: public interface which is connected to the global Internet, a middle zone that acts as a buffer and an additional subnet that is connected to an intranet or other local architecture.

d. The two types of threat a firewall cannot protect against are internal attackers or service that by-pass the firewall, example dial-up connection.

Question 5

a. Family

b. A statistical database is a primarily defined based on the data or information that it provides, which is based on the nature of the query results. We use it to protect data that are inherently sensitive, from a sensitive source, declared as sensitive, a sensitive component of a tuple, or sensitive in relation to earlier disclosed information.

Name: Chng Yia Qing Whitney
UOW No: 6956865

c. Two the methods that can be used to provide protection against statistical inference are trying to design a database in a way that inferences are reduced and attempting to reject specific/sequence of queries which may lead to inference attack.

d. Syncookies prevent SYN flooding attacks 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 is a phishing browser that is embedded within an actual browser as an image. If a user clicks on the picture, the attacker will gain be able to attack the user.

Homograph attack is a method of deception where a threat leverage on the similarities of scripts aka script spoofing. It registers a domain that looks similar to a real website. The users who access these websites will get their data stolen.