Closed policy
For each member I say what you can do, if I havent said it, its forbidden

Open police
For each member I say what is forbidden, if I havent said any you can do it

If a member creates a file, is he the owner then?

Question 1
Assume that Bob is a member of a group called "soup". Bob creates a file called "duck.txt", and sets its group to "soup". He then sets the permissions of the file so that owner (user) has access rights "rw-", group has access rights "---", and others have access rights "---".
After having done this, Bob can read the file. Is this true or false?

rw- --- --- A file that only the owner can read and write. No-one else can read or write. No-one has execution rights (e.g. a text file).

Bob created the file so he is the owner therefor he goes under the owner-rule and he can read the file.

TRUE

Question 2
Bob creates a file called "duck.txt", and sets the permissions of the file so that owner (user) has access rights "rw-", group has access rights "r--", and others have access rights "r--". After that, Bob changes the permissions of the directory where the file resides so that owner (user) has access rights "r--", group has access rights "r--", and others have access rights "r--".
After having done this, Bob can read the file. Is this true or false?

File permissions
rw- r-- r--

Directory permissions
r-- r-- r--

r for a directory means that you can list what is in it. To be able to go inside it you need x(execute), and therefor, if you cant go inside the directory you cant show the file

FALSE

Question 3
In a UNIX/Linux file system, it is possible to create a hard link to a directory. True or false?

With "ln" command we can create hard-links to a file. The hard-link points directly to the file, to delete the file we both need to delete the file and the hard-link to it. A hard-link will update permissions if updated

But to create a hard-link to a directory is not possible because this can create endless loops. If the directory point to itself there is no stop

FALSE

Question 4
In a UNIX/Linux file system, it is possible to create a symbolic link to a symbolic link. True or false?

A symlink can point to a directory, point to non-existent objects, point to files and directories outside the same file system. A created symlink wont update permissions if changed in directories

Instead of the need to type

```
cd documents/work/budgets/Engineering/2014/April
```

We create a softlink aprbude to link to the path

```
ln -s documents/work/budgets/Engineering/2014/April aprbudge
```

then instead we can type

```
cd aprbudge
```

to delete(just symlink)

```
rm aprbudge
```

Becuase the symlink can point to non-existing objects we can point it to another softlink.

TRUE

Question 5
The use of nonces is important in authentication protocols. Consider a scenario where Alice wants to authenticate herself to Bob. Mark the statement(s) that are valid.

Select one or more:

-Nonces help to protect against playback(replay) attacks
The nonce is already used and cant be reused, next nonce is what I get from reciever.
-Nonces help to protect from attacks where an imposter claims to be Alice and reuses previous information to prove it.
-Bob generates a nonce and challandes Alice to encrypt it. If Alice can encrypt the nonce, Bob knows that she has the key, and she has been authenticated

Question 6
Among the requirements for a characteristics (such as fingerprint and voice) used for biometrics is that the characteristics has four qualities: Universality, distinctiveness, permanence, and collectability.

Assume that the officials at an airport propose to use DNA for identification, but the proposal is rejected because DNA is considered not to have the required four qualities for biometrics. Which of the four qualities are problematic for DNA biometrics?

Select one:
-Collectability

(Universality-everybody has it, Distinctiveness - dah, thats why its used in crime cases, Permanence - stored dna solve crimes, collectability - we dont have everyones thats why unsolved cases)

Question 7
Which of the following would be suitable to use as nonce?
A nonce should be unique, we dont want attacker to know what it is.

-Random numbers
-Time stamps
- Sequence numbers

You cant determine that I am I with only my DNA, I have not gave it away(what I am aware of)

Question 8
You are worried that you are spending too much time on social media. On the Internet you find a nice little app that plays an annoying sound when you have spent too many hours on social media sites, and you install the app on your computer. After a while you discover that the app also keeps tracks of all web sites you visit, and periodically uploads your web browsing history to a server.

How would you characterize the app that you installed?

Select one or more:

-Trojan horse(it does something but masqeurades it to something else)
-Spyware(a trojan-horse is a spyware)

Question 9
The password system in modern Linux/UNIX operating system makes use of several different concepts to make it more secure. Combine the following descriptions with the proper concepts.

-Contains user records but no password: /etc/passwd

-Contains Passwords hashes: /etc/shadow

-Contains information about hashing algorithm: /etc/shadow

-A password is hashed many times in order to harden the hashing operation: Password stretching

-Randomization of the password hashing operation: Salting

Question 10
The following are examples of authentication. What is the basis of the authentication for each of these examples?

What you know: password, secret key
What you have: secure tokens
What you are: biometrics

-Showing your boarding pass when entering: what you have

-Using the door phone(voice) to ask your friend to unlock the entranche: what you are

-signing a contract by putting your name in handwriting on paper: who you are

-unlocking a door by entering a passcode: what you know

Question 11
You are given the job to improve the security of a password-based login system for user authentication. It is particularly important to make the system less vulnerable to online attacks against specific accounts, where the intruder uses a high-speed computer over a fast network to generate login attempts with random strings as password guesses.

Which of the following could make the system less vulnerable to such attacks?

Select one or more:

-prevent the use of dictionary words in password(but we can build a scentence?)

-blocking an account after too many unsuccessful login attempts

Question 12
Buffer overflow is one of the most common software vulnerabilities. Which statements are correct?

!Developer fails to include code
!Attacker exploits an unchecked buffer to perform a buffer overflow attack, ex heap smashing, stack smashing
!causes application to behave improperly and unexpectedly, the process can operate on malicious data or execute malicius code passed by attacker.

!Is a C problem

Prevent
compile-time
!choise of programming language, safe programming, generate code for checking/ preventing memory abuse
runtime
!stack/heap non-executable, address space randomization(move stack around to prevent address guessing harder), Guard pages(illegal addresses between regions of memory)

Select one or more:

-Bufer overflows are possible because of mistakes or oversights by the programmer

-With a properly designed buffer overflow attack, the attacker may take control over the program being attacked

Question 13
In the UNIX password database, a salt value is associated to each password. Consider the case when Alice is logging in on a UNIX-based server. Which of the following is true?

One salt per password

Select one or more:

-The salt is generated by the server

-the hash is computed from the salt and Alice's password

-The salt makes offline dictionary atacks more difficult