1.Give three examples of excellent passwords and explain why each would be a good choice to protect a system from unauthorized users.

Tthad\_123@abc

Tri\_chau\_123@abc

Sfsgsg123@#$%

They are exellent passwords because they contain upper, lower cases, symbols, numbers long length

2.Password management software/apps promise to keep passwords safe, while allowing fast and easy access for authorized users when they need to retrieve them. For at least one of these software packages or apps:

a.Describe in detail how secure you believe it is.

I believe it because they create strong password can against hacker. They are different with each other so easy to maintain.

b.List the vulnerabilities that you believe it faces in day-to-day use.

For example : spam email can be spreaded virus to computer

c.Compare your software’s most significant benefits to at least two other competitors.

Microsoft word, google chrome

3.In the past, some systems operators have had difficulty revoking system access in a timely manner for temporary contract employees who are no longer active on the contracted project. Sometimes, these contractors are engaged to work on the project only a few days a month, during which they require full access.

a.What are the challenges posed by this group of employees?

The challenges if working like that is when you have any problems and want to have someone to fix it right the way, but no one there

b.As systems administrator, how would you manage access for them?

As an admin I will be flexible the day that employees works . which means there are always one employee there

4.Explain the concept of password salting using terminology that would be appro-priate for a high school student, and without resorting to computer jargon.

Salting is a password storage technique whereby a random string of symbols and char-acters are added to a user password before it is encrypted (technically, it is hashed) and saved

5.If you were the manager of a small computing center, list at least three tech-niques that you would use to convince a busy, reluctant, systems operator to perform regular backups. Explain the best and worst possible techniques to assure your success.

Backup: important file, customers information, database, document

Update data regular, save in many places, backup file

6.Visitors to a work site might be able to learn how to access systems using passwords that are displayed in plain sight in the area surrounding their work space.

a.How would you convince your users to safeguard their passwords?

I can tell them that a lot of people around them can steal their password and do something to them. So you must protect your password. If you don’t do that you may lose your personal information

b.What specific advice would you give them?

You should pay attention with anyone, notify if someone around you. Set password long and more complex.

7.Assume that you are tasked with writing a new password security policy.

a.Explain the critical elements of the new policy if it is to be successful.

Length more than 8 characters, lower , upper , symbols, no name, day of birth

b.Explain how you would verify its effectiveness.

It will not be in the dictionary. Hard to determine the password

8.Keeping the critical patches current is an important aspect of both system security and system administration. Should executive management be made aware of this or any aspect of system security? Explain why or why not.

Yes, they system security and system administration are very important because based on the system it can limit cyber attack.

9.Given multi-network access, it’s common for users to have multiple user identifications and passwords.

a.How would you manage these multi-password situations?

You can save in note book or use application

b.Describe both the advantages and disadvantages of your solution.

Advantage :

Notebook: save many password , hard to remember,

Use application: same thing

Disadvantage:

Notebook: lose notebook

Application: hacker

10.Describe the advantages and disadvantages of password generator software. Would you recommend the use of such software for your own system? Explain why or why not.

Advantages:

Strong enough,

Disadvantages:

We canot remember that password

Yes : if you don’t know how to generate the strong password,

No: don’t use for every application.

11.The U.S. legislation known as HIPAA (Health Insurance Portability and Accountability Act of 1996) protects the privacy of patient medical data, which is valued on a day-to-day basis. Yet, in an emergency, patients might want their caregivers to have fast and easy access to their medical history, medications, and so on. Acknowledging the need for patient privacy, as well as the need for accessibility, describe several advantages and disadvantages of maintaining strict patient data confidentiality. Describe your suggestions on how to balance these conflicts.

The conflict is need to have strong and access fast. My suggestion is the password not to be very strong so we can access faster.