A. Identity and Authentication

Briefly describe the difference between identity and authentication.

Identification is a way to describe the principal, such as first name + last name, username, or an email.
Authentication is proving the principal is who they say they are.

Example: When I log into a system, I identify myself with my username, "cunnin42". Then I prove to the system I am who I say I am, by providing my password: "corigesaregood".

Give an example where we might want authentication but not use identity.

This answer depends on how identity is defined. If identity is defined as linking a principal to a specific user, then such a system is possible. See example 1 below. However, if "identification" is broad-based (such as anonymous credentialing), then authentication may simply be used to divide into the role of "authorized" and "not-authorized". With this view, then any authentication does use identity (It would make no sense to authenticate otherwise. Why would you authenticate if you didn't make some distinction between authenticating and not authenticating?)

Your answer depends more on your explanation behind your answer.

Ex 1: A distributed computing network where authorized users are given a token to access system resources, but they do not log in with a user name, only the token that authorizes them.

Give an example where we might use identity without authentication.

An online forum where anyone is allowed to post, but posters do not have unique accounts and everything is 'anonymous'. Posters are never required to prove they are who they are that user.

B. Biometrics

Give an example of using biometrics for identification

Many various answers, some example answers could include (but are not limited to): FBI Fingerprint database, photos, a person's voice, etc.

Give an example of using biometrics for authentication but not identification

Many various answers, an example answer could be: A theme park ride that allows only people above a certain height to participate.

C. Password Mechanism

A company employs the following password verification mechanism, designed for user convenience. The user is logged in as soon as they enter the correct password (no need to click submit or hit enter.) If they mistype the password, the password is rejected as soon as an incorrect character is entered.

Explain the problem with this approach, and devise an attack that allows you to easily guess a user's password.

For each character of the password, try each character one at a time until the system allows you to progress to the next character. This allows you to break a password one character at a time, significantly defeating the security of a complex password.

Give a measure of the expected strength of a password, and how strong the password really is given your attack. Assume that there are S possible characters, and the password is length L.

Expected strength of a password is S^L, but in our attack the strength is reduced to $S * L$.

D. Malware

What are the differences between scareware and ransomware?

Scareware: Does not affect any permanent damage to the system, but attempts to trick the victim into thinking they have a problem that only the attacker can solve, usually for an exchange of money.

Ransomware: The attacker affects some change to the victim's system, and will only undo the change in exchange for money. The main difference from Scareware is that the system is actually compromised in some way, and it is not just a trick.

Malware can be used to form a Botnet. Explain the steps involved in doing so.

To form a botnet, two critical steps must be taken: the distribution of the malware that takes control of victim's computer, and a control structure to control the botnet. A description of both should be given.

Malware is often used for the financial gain of the malicious actor. It is reasonably obvious how this happens with scareware and ransomware. Explain briefly how a botnet might be used for financial gain of whoever releases the malware, and how this might impact detection.

Answers for this question can vary quite a bit.
Example of how a botnet can be used for financial gain is: threatening companies with DOS attacks unless they pay, or mining cryptocurrencies using victim's computing power.
How these two examples impact detection: threating companies requires contact, and can expose the attacker to law enforcement, while mining cryptocurrencies makes the hidden malware more obvious to the user and more likely to be detected on the victim's computer.