OS Security

The different security concerns are

1. Breach of confidentiality
2. Breach of integrity
3. Breach of availability
4. Theft of service
5. Denial of service

Masquerading is when a user pretends to be someone else to exploit the process.

A replay attack is when a valid data transmission is fraudulently repeated.

A trap door is when there exist holes in a code for entry for malicious software.

A logic bomb creates holes in the security layers of the software.

A stack or buffer overflow occurs when more data is sent to a program than needed, and the program on the attacker's side is written for

1. Overflowing a CLI
2. Overwriting a return address on the stack with the address of malicious code
3. Write code for the next space in stack the attacker wishes to execute

One solution to this is disable execution of code in stack.

OS hardening is the process of securing a system by reducing its surface of vulnerability, which is large when the system performs more functions.

This can be done via patches and security updates.