Input Validation:
A program looks for special characters or SQL keywords that might point to an attempt at SQL injection before executing a user's search query.

Integrity:
A client receives a file from a server; prior to opening the file, the client determines its hash value. The data is regarded as intact and has not been altered during transmission if the hash that was received and sent by the server matches.

Intrusion Detection System:
An intrusion detection system is installed on the company's network, and it actively searches for odd trends in network traffic. It takes automatic action to protect the network when it notices an abrupt spike in requests, akin to a DDoS attack.

IP Spoofing:
By spoofing an IP address, an attacker tries to hide the source of a malicious payload. To make it seem as though requests are coming from a reliable and authentic server, a hacker modifies packets' source IP address.

John The Ripper:
Security experts uses John The Ripper to test the strength of passwords on a server.

Kerberos:
Kerberos uses sophisticated encryption for authentication to guarantee secure communication within a corporate network. In order to prevent unwanted access, Microsoft uses it as their default authorization software.

KeyLogger:
Unknowingly installing a keylogger on their computer causes it to log each keystroke that is made to obtain sensitive information such as login credentials and credit card numbers.

Logic Bombs:
A logic bomb is introduced into the payroll system of the company by an employee. If specific requirements are satisfied, like losing one's job, the malicious code activates and causes disruptions in the system.

Lightweight Directory Access Protocol (LDAP):
LDAP serves as a central directory for authentication in a Windows-based network. By securely storing and managing usernames and passwords, it enables users to access a variety of resources.

Malware:

A user unintentionally downloads malware disguised as a software update. This malicious software infects the system, jeopardizing data integrity and potentially causing harm to the user's computer.

MAC Address:
Changing the MAC address of their device in order to impersonate another device on the local network.

Multi-factor Authentication:
To gain access to a secure banking portal, users must enter both a password and a one-time password (OTP) sent to their mobile device.

MD5:
MD5 for tasks like password hashing to avoid storing plain text thus making it impossible to obtain original text.

Metasploit:
A security professional employs Metasploit to simulate cyber attacks and identify vulnerabilities in a company's system.

Meterpreter:
During a penetration test, the security team uses Meterpreter, an advanced Metasploit payload, to gain access to a target system's memory.