Acquiring access

In access attacks an adversary exploits security weaknesses to obtain access to a system or the network. Phishing, pharming and password breaking (bruto force, dictionary, etc) are typically used to obtain system access. When access is obtained, the adversary can modify or delete data and add, modify, or remove network resources. Typical access attacks are:

- Unauthorised system access by exploiting the vulnerabilities of operating systems or executing a script or a hacking program to obtain access to a system.
- Unauthorised privilege escalation to obtain a high level of access, like administrative privileges, to gain control of the network system.
- Unauthorised data manipulation involves interpreting, altering, and deleting confidential data.

Mitigation

Development

- Use digital signatures to ensure that data has not been modified while it is being transmitted or simply stored
- Implement an authentication mechanism to control which users are allowed to access which data
- Regularly back up important data
- Establish and maintain control over all inputs
- Establish and maintain control over all outputs
- Don't roll your own security algorithms, and if you do have it be audited by a team of experts
- Use libraries and frameworks that make it easier to avoid introducing weaknesses
- Allow locked-down clients

---

threats, network, access, fruit