|  |  |  |
| --- | --- | --- |
| **Threat** | **Achievement** | **Adversary action** |
| Spoofing | Gaining access | Adversary gained access to the system |
|  |  |  |
| Tampering | Unauthorized actions (modifications, deletion...) | By doing unauthorized/unintended/unapproved alterations/modifications |
|  |  |  |
| Repudiation | 1.Missed identity  2.Failed traceability  3.Unclaimable | By performing an illegal/malicious operation in a system & denies their involvement with the attack |
|  |  |  |
| Information Disclosure | 1.Information/Data leakage  2.Missed/failed confidentiality  3.Revealed info (sensitive data) | -By using a malicious application/script, adversary access user/application information  -when a website unintentionally reveals sensitive information to its users |
|  |  |  |
| Denial of Service (DOS) | 1.Non-availability  2.Service unavailability  3.Feature unavailability  4.Crashing the system/service | By flooding the target with traffic |
|  |  |  |
| Elevation of Privilege | 1.Undefined roles/responsibilities  2.Uncategorized users  3.Missing user management  4.Unassigned roles/responsibilities  5.Gaining access | Adversary gains more permissions or obtain access to additional, more sensitive systems  -Finding weak points  - By exploiting misconfigurations, bugs, weak passwords, & other vulnerabilities that allow them to access protected asset |
|  |  |  |