|  |  |  |
| --- | --- | --- |
| **Ataque** | **Descripción** | **Control (medida de mitigación)** |
| Dos | Es un ataque que satura un sistema o red con varias peticiones con el fin de que los usuarios les sean imposible acceder al sistema o red. | IPS y firewalls.  Tecnologías Antispoofing (DHCP snooping, guardián de la ip de origen, inspección del ARP y ACLs).  Vigilancia del tráfico. |
| Dictionary | Es un ataque que pretende encontrar la contraseña intentado usar un diccionario de palabras el cual puede contener las contraseñas más comunes o las contraseñas que podría usar la víctima. | Usar contraseñas seguras es decir que tengan al menos 8 caracteres y que estas tengan mayúsculas, minúsculas, caracteres especiales y números.  Deshabilitar o bloquear las cuentas después de que se haya producido un número específico de inicios de sesión fallidos. |
| Exploitation | Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio. | Mantener el software actualizado con el propósito de “parchar” las vulnerabilidades de algún programa. |
| Spoofing | Es una técnica la cual consiste en hacer pasar una computadora por otra con el fin de examinar y obtener la información de la otra computadora para algún fin. | Tecnologías Antispoofing (DHCP snooping, guardián de la ip de origen, inspección del ARP y ACLs). |