



Denial of Service

2. Ein Angreifer kann Ihr Authentisierungs-System unbrauchbar oder unverfügbar machen.
3. Ein Angreifer kann einen Client unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Client, authentisiert, temporär**).
4. Ein Angreifer kann einen Server unverfügbar oder unbrauchbar machen, aber das Problem verschwindet, sobald der Angriff aufhört (**Server, authentisiert, temporär**).
5. Ein Angreifer kann einen Client unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Client, anonym, temporär**).
6. Ein Angreifer kann einen Server unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat. Das Problem verschwindet nach dem Angriff (**Server, anonym, temporär**).
7. Ein Angreifer kann einen Client unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, authentisiert, persistent**).

Denial of Service



Denial of Service cont.

- 8. Ein Angreifer kann einen Server unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, authentisiert, persistent**).
- 9. Ein Angreifer kann einen Client unverfügbar machen, ohne dass je eine Authentisierung stattgefunden hat, und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, anonym, persistent**).
- 10. Ein Angreifer kann, ohne zu authentisieren, einen Server unverfügbar machen. Das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, anonym, persistent**).
- J. Ein Angreifer kann das Logging-Subsystem außer Betrieb setzen.
- Q. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine (volumenbasierte) DoS Attacke um den Faktor 10 zu verstärken.
- K. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine DoS Attacke mehr als 100fach zu verstärken.
- A. Sie haben eine neue DoS Attacke erfunden.

Denial of Service