# Denial of service

Deniel of service (DoS) je napad na resurse kao što su server, aplikacija i servis sa ciljem da se spreči ili uspori opsluživanje njihovih pravih korisnik. Može nastati kada se žrtva optereti od strane jednog ili više računara. Međutim, može nastati i „nenamerno“ kao posledica ekspletacije resursa ili usled neefikasnosti koda.

Najčešći DoS napad je distribuirani DoS napad (DDoS) koji nastaje kada veliki broj računara istovremeno pristupa istom ciljnom resursu. Može nastati i kao posledica relativno istovremenog aktiviranja malarwe programa koji su inficirali veliki broj računara i pristupaju istom resursu preko mreže.

DoS se može javiti kao posledica:

* *Unos od strane korisnika bez prikladne validacije* – npr. u numerici aplikacija računa vrednost nekog složenog izraza i algoritam za njegovo izračunavanje treba da se izvršava n puta. Ukoliko se ne ograniči da to n bude npr. 100, prilikom unosa 1000000 tada se troši znatno više resursa i usporava rad sistema i opsluživanje drugih korisnika.
* *Neadekvatno oslobađanje resursa* – npr. prilikom izuzetka se ne zatvara konekcija sa bazom tj. ako se ne rukuje pravilno sa connection pool mehanizmom pa se nagomila prevelik broj otvorenih konekcija.
* *Buffer overflow –* kada korisnik unese veću količnu podataka od one što je dozvoljena. Da bi se to sprečilo, teba proveravati veličinu unetih podataka i na klijentskoj i na serverskoj strani.
* *Skladištenje prevelike količine podataka u sesiju –* nastaje kada se velika količina podataka npr. rezultat nekog upita nad bazom podataka smesti u sesiju. Može nastati i ako se na sesiju kače podaci a korisnik nije ulogvan što olakšava napad.
* *Opterećenje sistema na transmisionom nivou (TCP/UDP)*

SYN DDoS (SYN flood DoS) napad preopterećuje TCP transmisioni nivo tako što napadač neprestano šalje SYN zahteve ciljanom sistemu pokušavajući da konzumira što više resursa žrtve i time ne uspe da reaguje na legitimni saobraćaj.

Kada DoS napad koristi UDP, napadač šalje veliku količinu UDP paketa svim mogućim portovima na žrtvi. Tada žrtva traži odgovarajući port i ako ga ne nađe šalje nazad ICMP poriku. Usled velike količine UDP paketa, biće prisiljena da nazad šalje veliki broj ICMP paketa.

* *Opterećenje sistema na aplikativnom nivou (HTTP)*

Kada napadač koristi GET metodu HTTP, tada se šalje veliki broj legitimnih GET zahteva

Postoji nekoliko načina da se DoS napadi spreče:

* Korišćenjem hardvera koji će registrovati neuobičanje radnje i suspendovati sumnjiv pristup sistemu
* Stalnom analizom koda i testiranjem performansi resursa odnosno njihove izdržljivosti
* Ograničiti veličinu dokumenta koji se mogu poslati na server
* Obezbediti veći protok
* Rezultate pretraga ne kačiti na sesiju
* Ograničiti broj rezultata pretrage koji se isporučuju korisniku u jednoj interakciji.
* Isključiti UDP i ograničiti na koje porteove server radi
* Validirati unete podatke