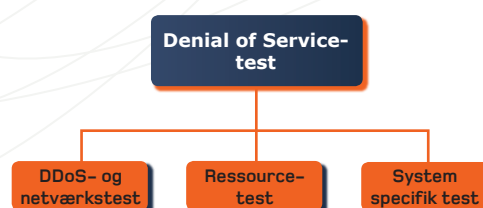


Kan du modstå et DoS-angreb?

Internettet har lige godt en milliard brugere, der uden forudgående autentifikation kan kontakte og dermed tappe ressourcer fra virksomhedens netværk og systemer. Hermed bringes tilgængeligheden i fare og virksomheden må dermed forholde sig til omkostningerne hvis f.eks. et centralt system kan blive gjort utilgængeligt. Disse omkostninger kan inkludere bl.a. tabt produktion, PR og ordrer.



For at imødegå disse trusler og risici bedst muligt er et effektivt forsvar mod Denial of Service-angreb nødvendigt. Ezena tilbyder dybdegående sikkerhedstest af netop dette forsvar. Ved et DoS-angreb er målet at gøre kundens system eller netværk utilgængeligt. Dette mål kan oftest nås ved at lokalisere og anvende begrænsede ressourcer eller ved at udnytte manglende patchning eller en u hensigtsmæssig konfiguration i enten netværket eller det testede system. De konkrete angrebsmetoder er forskellige alt efter om det testede system f.eks. er en firewall, et website eller en VPN-forbindelse. Produktet indeholder således megen manuel gennemgang, hvorfor testen skræddersyes til netop kundens installation.

Ved en Ezena Denial of Service (DoS) test foretages overordnet følgende:

DDoS- & netværkstests

Sårbarhedsanalyse af det testede systems netværksimplementering, herunder dets modtagelighed over for DoS-, amplifikations- og DDoS-angreb.

Ressourcetest

DoS-tests der lægger den størst mulige belastning på begrænsede ressourcer. Dette omfatter alt fra fysiske ressourcer (f.eks CPU-tid, HD-plads, båndbredde etc.) til programmeringsmæssige ressourcer (f.eks. datastrukturer, processer etc.). Belastningstest der tester systemets reaktionstid og tilgængelighed ved op til mange hundrede samtidige brugere.

System specifikke test

Automatiseret og manuel sårbarhedsanalyse mht. kendte DoS-relaterede sårbarheder specifikt for det testede system. Manuel gennemgang af systemets konfiguration og funktionalitet mhp. at udføre mulige DoS-angreb.