AALBORG UNIVERSITET

Cyberangreb: Hvad er DDoS-angreb, hvem rammer de, og er de lovlige at lave?

Erhvervs-ph.d.
Martin Fejrskov
Institut for Elektroniske Systemer, Aalborg Universitet

Opgave 1 (repetition af terminologi):

a) Hvilken rolle har botmasteren, angriberen og offeret i et DDoS-angreb?
b) Hvad er en bot og et botnet?
c) Beskriv et eksempel på en angriber, der kunne have en politisk motivation for at lave et DDoS-angreb, samt et eksempel på det tilhørende offer.

Opgave 2 (det juridiske aspekt):

a) Find den nugældende version af den danske straffelovs §193 og §263 på Internettet.
b) Beskriv kort, hvorfor de to paragraffer er relevante i forhold til DDoS-angreb.

Opgave 3 (det kommercielle aspekt):

a) Find hjemmesider, der sælger DDoS-angreb på Internettet (du kan søge efter "stresser" og "booter").
b) Sammenlign forskellene og ligheden mellem de forskellige tjenester. Fokuser gerne på de ikke-tekniske, såsom support, abonnementsform, betalingsmetoder, anonymitet osv.
c) Prøv at lave et kvalificeret gæt på, hvor stor en årlig omsætning en given DDoS-tjeneste har. Du kan bruge en af de tjenester, du selv har fundet, eller finde (gamle) kundetal og prisplaner for "webstresser.org", der blev lukket af politiet i 2018.

Opgave 4 (det tekniske aspekt, botnet-størrelse):

a) Brug Internettet til at finde estimerede størrelser på kendte (evt. historiske) botnets som f.eks. Mirai eller Zeus.
b) Forestil dig, at du er en botmaster, der gerne vil kunne lave et volumen-angreb på 10 Gbit/s. Lav en graf, der viser sammenhængen mellem antallet af bots, du skal bruge i dit botnet og hvor mange trafikpakker, hver bot i gennemsnit skal udsende pr. sekund. En trafikpakke indeholder 1500 bytes (1 byte = 8 bit).

Opgave 5 (det tekniske aspekt, firewall-størrelse):

a) Forestil dig, at du ejer en hjemmeside, som du gerne vil beskytte bedst muligt mod et applikations-angreb. Hjemmesiden kører kun på én server, og det tager serveren 4 ms at håndtere en normal forespørgsel. Serveren kan håndtere 6000 normale forespørgsler på ét sekund. Hvor mange forespørgsler håndterer serveren på samme tid?
b) Du frygter at din hjemmeside bliver angrebet med et applikationslags-angreb, der sender 12000 forespørgsler pr. sekund, der hver tager 60 ms at processere. Hvor mange servere skal du bruge for at kunne håndtere angrebstrafikken?