Produceret af:
Asger Hermind Sørensen (cph-as466)
William Sehested Huusfeldt (cph-wh106)
Emil Jogvan Bruun (cph-eb122)

Social Engineering, Denial-of-service attacks

Social Engineering, Denial-of-service attacks

- Explain different ways to use Social Engineering (vectors)
- Discuss ways to detect social engineering attempts (principles)
- Explain the most common DoS strategies
- Discuss common means to minimize threads of DoS

Explain different ways to use Social Engineering (Vectors)

Vishing (Voice Phishing)

- I et telefonopkald hvor man angiver sig for at være en anden person, som f.eks. er relateret til den man vil ind på. For at prøve at få information eller adgang.

Phishing

- Svigagtig forsøg på at anskaffe sensitiv information over elektronisk kommunikation. Det kan for eksempel være en bruger der udgiver sig for at være udbyder af en streaming tjeneste og prøver at lokke kreditkort oplysninger fra brugeren.

Smishing (SMS phishing)

- Beskeder man modtager over sms, hvoraf der bliver påstået at man f.eks. har modtaget en pakke, eller vundet en konkurrence.

Impersonation

- Opgive sig for at være en anden, for det meste en autoritet (skat, nets, e-boks mm.)

Discuss ways to detect social engineering attempts

Mail:

- Stavefejl og uformel formidling
- Holde over linket og se om det stemmer overens med påstanden
- kontrollere afsenderens réele mail adresse.

Telefon:

- Lige så snart du hører en indisk accént.
- Hacker/scammer kan ikke basal information om dig.
- Du har vundet i noget du ikke har deltaget i.

- Udlever ikke følsom information til andre end vedkommende det drejer sig om, f.eks. lad dog for fanden være med at oprette en konto i en mands navn når det er en fucking kvinde der snakker.

SMS:

- Alle SMS'er som du ikke har bedt om.

- Pakke tracking sendes altid over mail også, dobbeltcheck at begge er samme forsender, og at du i øvrigt har bestilt en pakke, hvis nej er den falsk.

Explain the most common DoS strategies

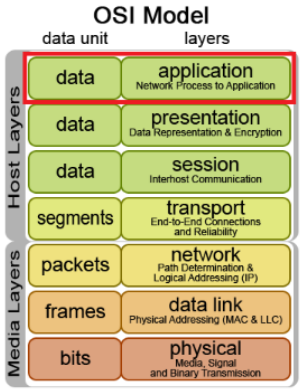
Formålet ved et DoS angreb er at gøre en maskine/netværk utilgængelig for dets brugere. Dette gøres ved at overloade en maskine/resource ved at oversvømme den med requests.

Distributed DoS (DDoS) - Volumetric:

- Her vil man lave requests fra flere forskellige kilder (IP adresser), hvilket gør det næsten umuligt at finde gerningsmanden.
- Ofte vil disse requests komme fra maskiner, som er inficeret med malware.
- Involverer ofte flere end 3-5 nodes.
- Bliver anset som et large-scale angreb og bliver i stigende grad benyttet.

Application layer attacks:

Application Layer Attacks indebærer angreb der går efter sikkerhedsbrud i web services som Apache, NGINX osv. samt flood attack ved brug af GET og POST metoder over HTTP/s.



Discuss common means to minimize threats of DoS

At have nok bandwidth til at kunne håndtere de spikes af trafik der medfølger af et DoS angreb.
Have en god infrastruktur på sine servere som sørger for at opdele trafikken mellem dem.

Der er flere third party softwares samt hardwares lavet til at sikre mod DoS angreb, hvilket kan sættes på din server som beskyttelse. For eksempel har Apache 2.2.15 et module der beskytter sig selv for applikations lags angreb.