Denial of Service

Mirio Eggmann &
Dario Menzel

Inhalt

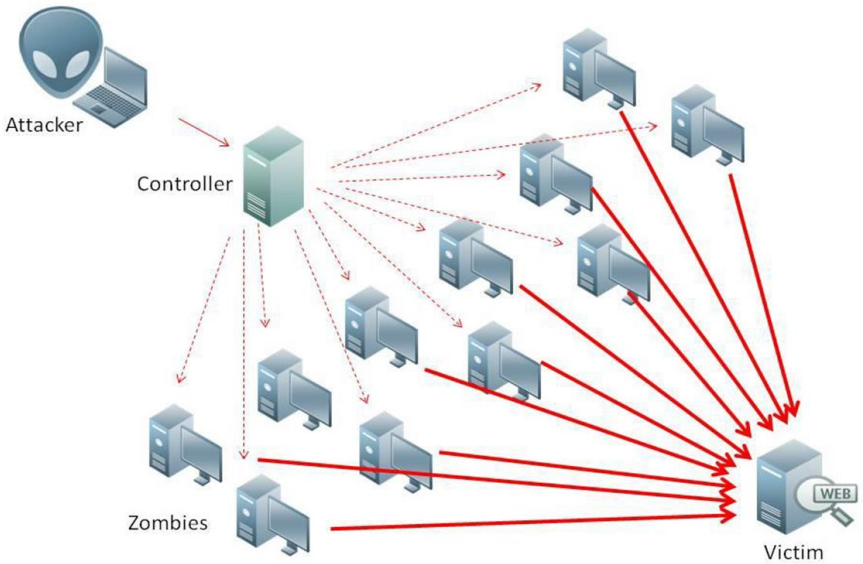
- Einleitung
- Motivation
- Angriffstypen
- Live Demo
- Auswirkungen & Massnahmen
- Fragen

Was ist DoS?

- Denial of Service -> Dienstverweigerung
- Überlastung von Rechnern
- Mutwillig oder unabsichtlich
- Einfach zurückzuverfolgen

DDoS?

- Distributed Denial of Service
- Botnetz
- Schwer zurückzuverfolgen



Motivation

- Politischer Aktivismus
- Schädigung des Konkurrenten
- Erpressung
- Aufmerksamkeit

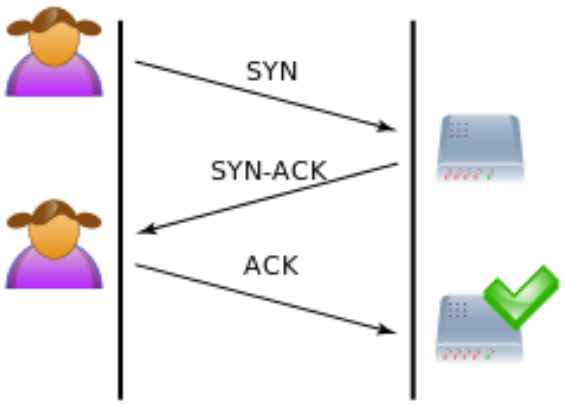
Angriffstypen

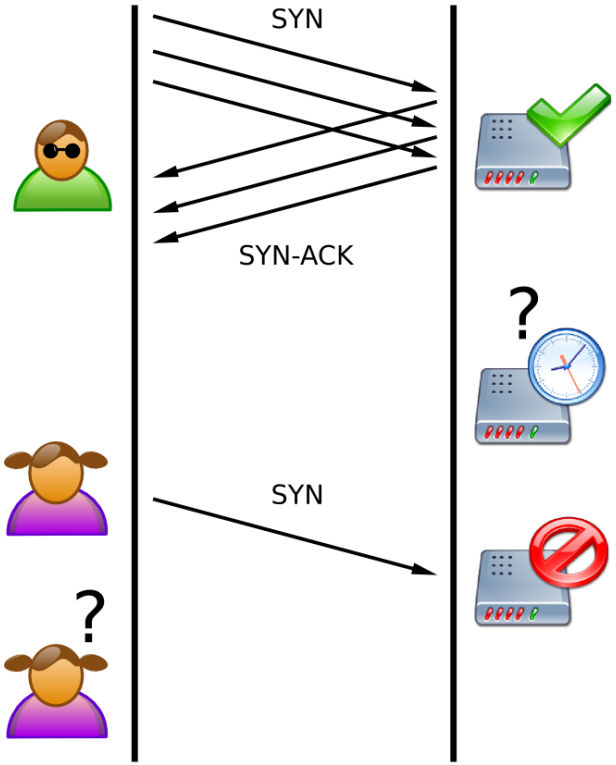
- Applikations-Attacken
- Protokoll-Attacken
- Bandbreiten-Attacken

Nr.	Layer	Beispiele
7	Anwendungsschicht	HTTP-Flooding
6	Präsentationsschicht	
5	Sitzungsschicht	
4	Transportschicht	SYN-Flooding
3	Vermittlungsschicht	ICMP-Flooding

SYN-Flood Attack

- Manipulieren des TCP Protokolls





Live Demo

Auswirkungen & Massnahmen

- Ausfall der Webseite
- Gewinnverlust
- Reputationsverlust

- Firewall
- Genügend Ressourcen
- SYN-Cookies
- Filter-Services
- Capatchas