Conflood – a non-distributed DoS-Attack

Konstruktion und Analyse des Angriffs im Rahmen der Bachelorarbeit an der Universität Hamburg

Florens Wasserfall
(6wasserf@informatik.uni-hamburg.de)

Kjell Witte
(6witte@informatik.uni-hamburg.de)

Gliederung

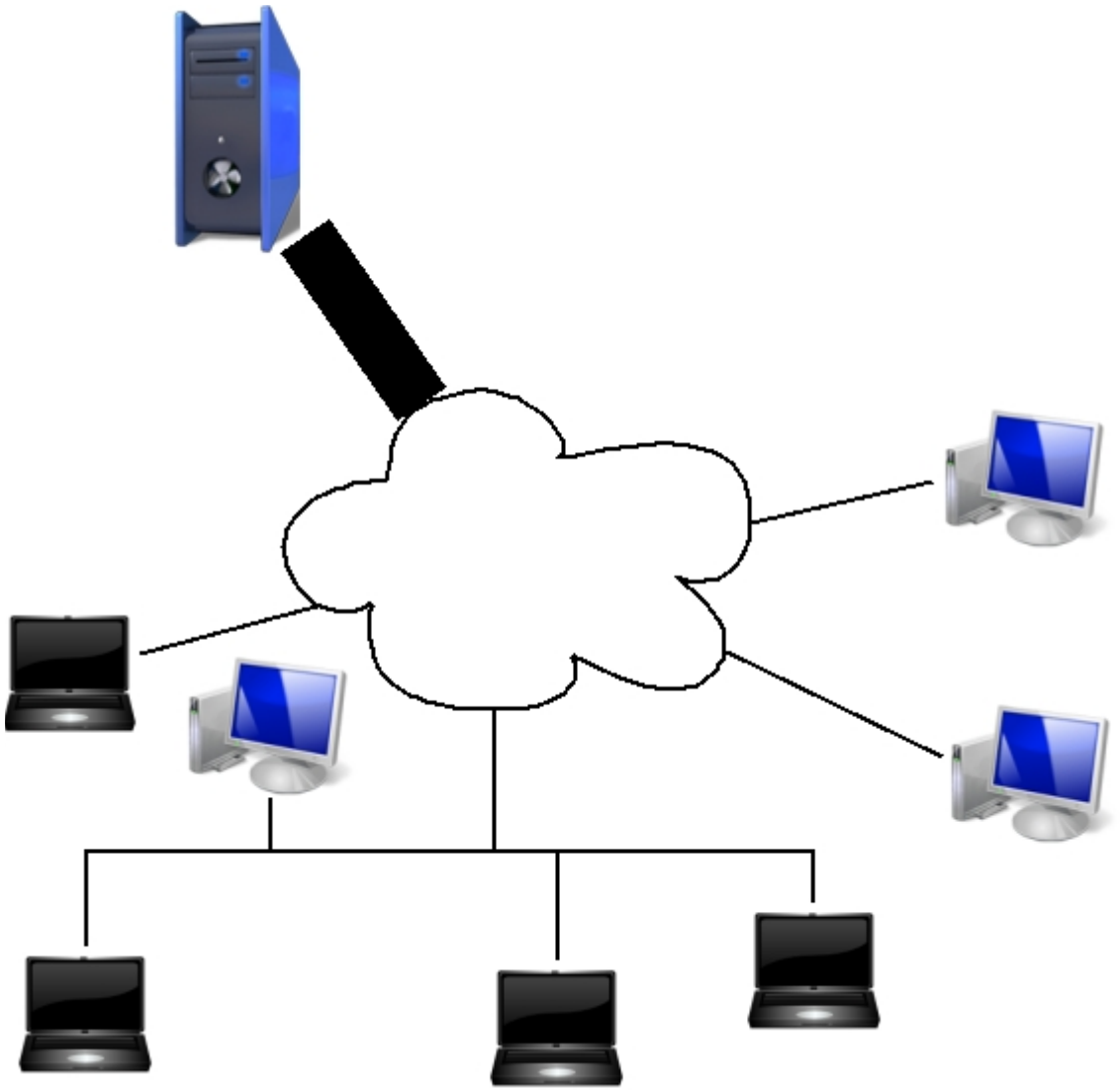
- **Einleitung**
- **Angriff**
  - Prinzip
  - TCP Eigenschaften
- **Lage im Internet**
  - Verwundbare Anwendungen
  - Verwundbarkeitstests
- **Abwehr**
  - Netzwerkebene
  - Anwendungsebene
- **Demo**
- **Verwandte Angriffe**
- **Quellen / Literatur**

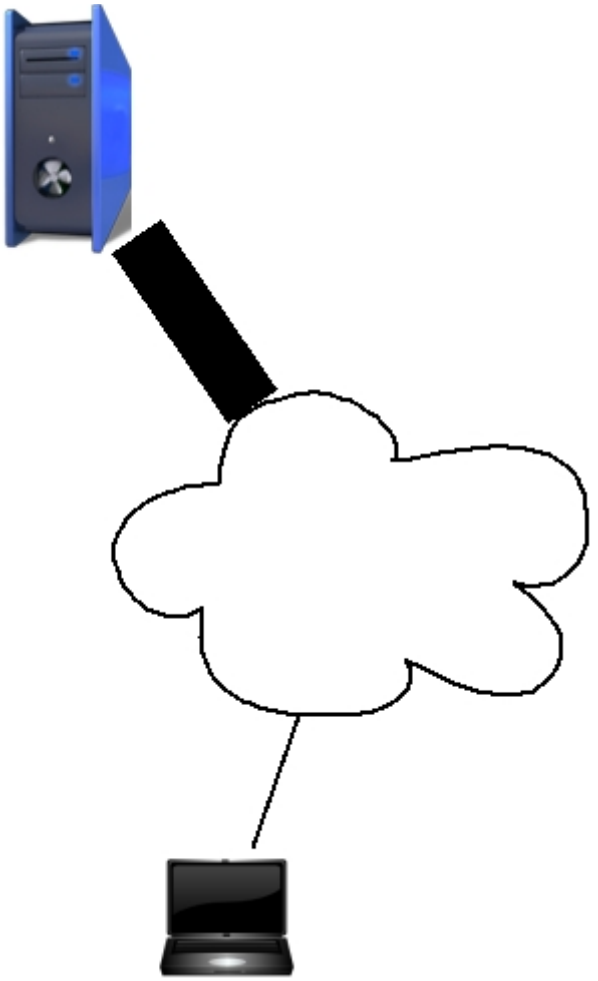
Gliederung

- **Einleitung**
- **Angriff**
  - Prinzip
  - TCP Eigenschaften
- **Lage im Internet**
  - Verwundbare Anwendungen
  - Verwundbarkeitstests
- **Abwehr**
  - Netzwerkebene
  - Anwendungsebene
- **Demo**
- **Verwandte Angriffe**
- **Quellen / Literatur**

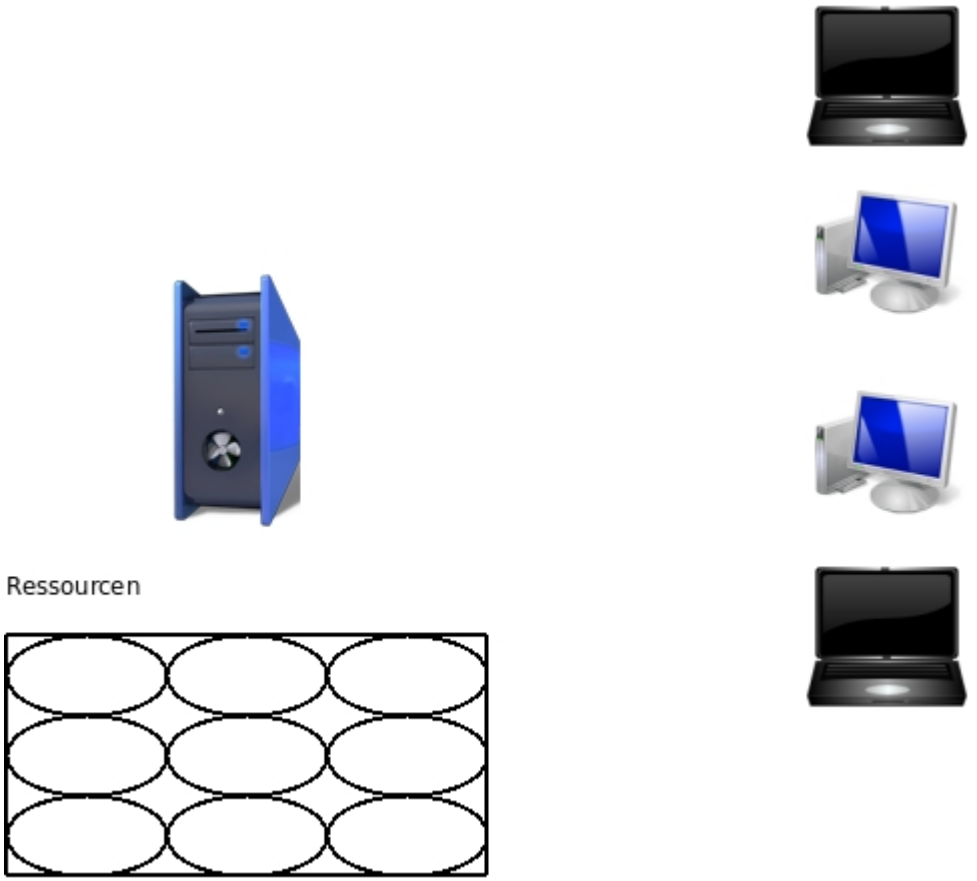
Einleitung

- Inspiriert durch den Vortrag *TCP Denial of Service Vulnerabilities* von Fabian Yamaguchi auf dem 25C3
- Verteilte DoS-Angriffe sind weit verbreitet, hoch aktuell und werden intensiv erforscht
- Nicht-verteilte DoS-Angriffe werden in der Forschung vernachlässigt und scheinen der Vergangenheit anzugehören
- Ziel: Erforschung der Möglichkeit, DoS-Angriffe von einem einzelnen DSL-Anschluss aus durchzuführen

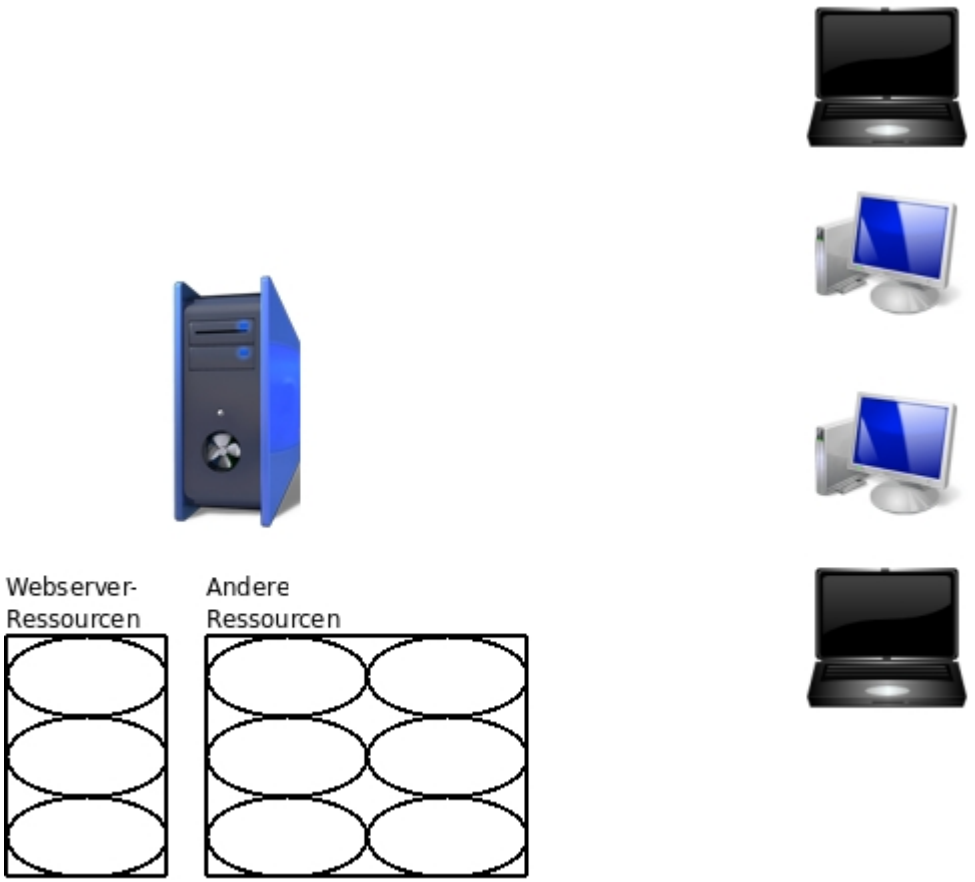




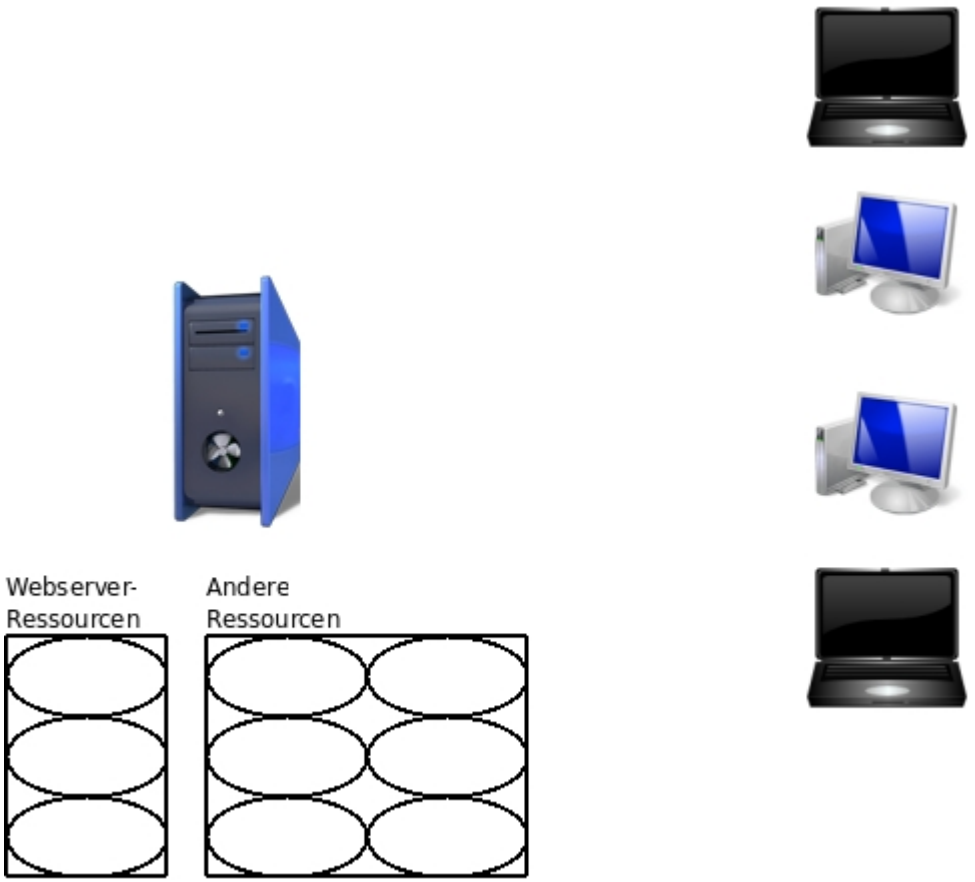
Angriff



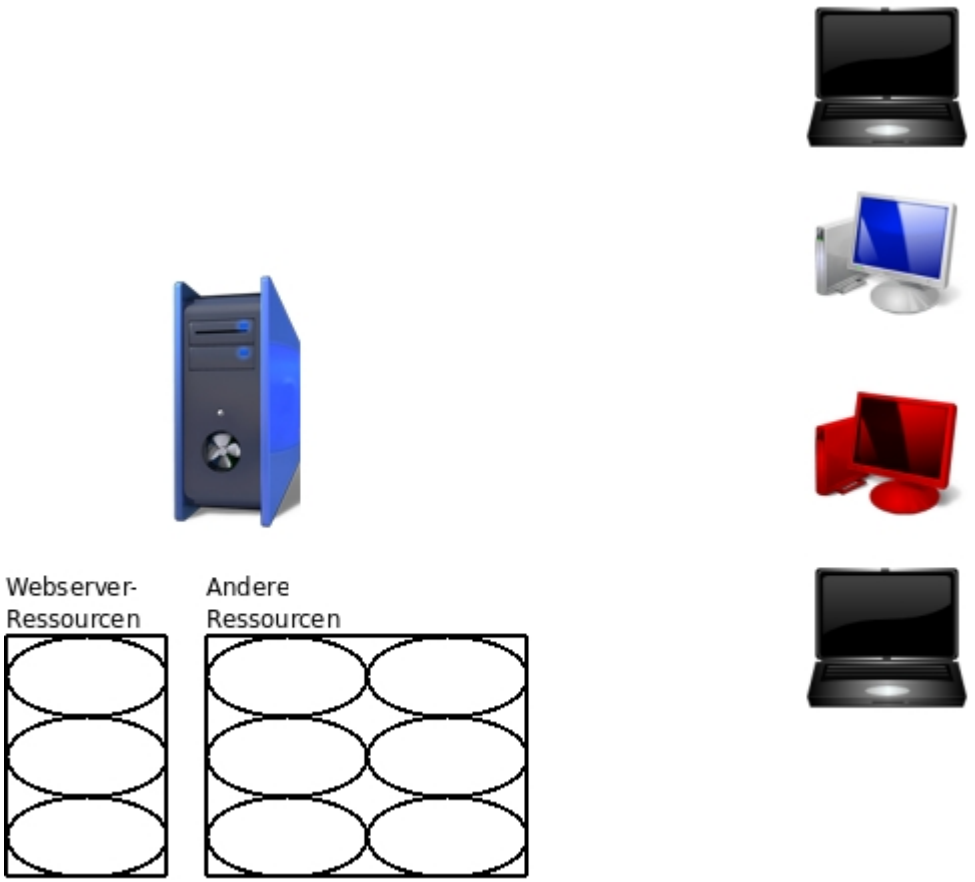
Angriff



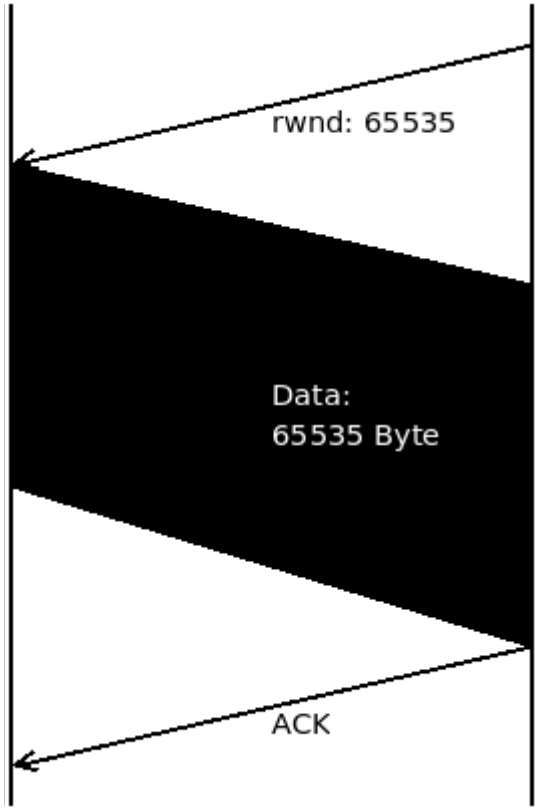
Angriff



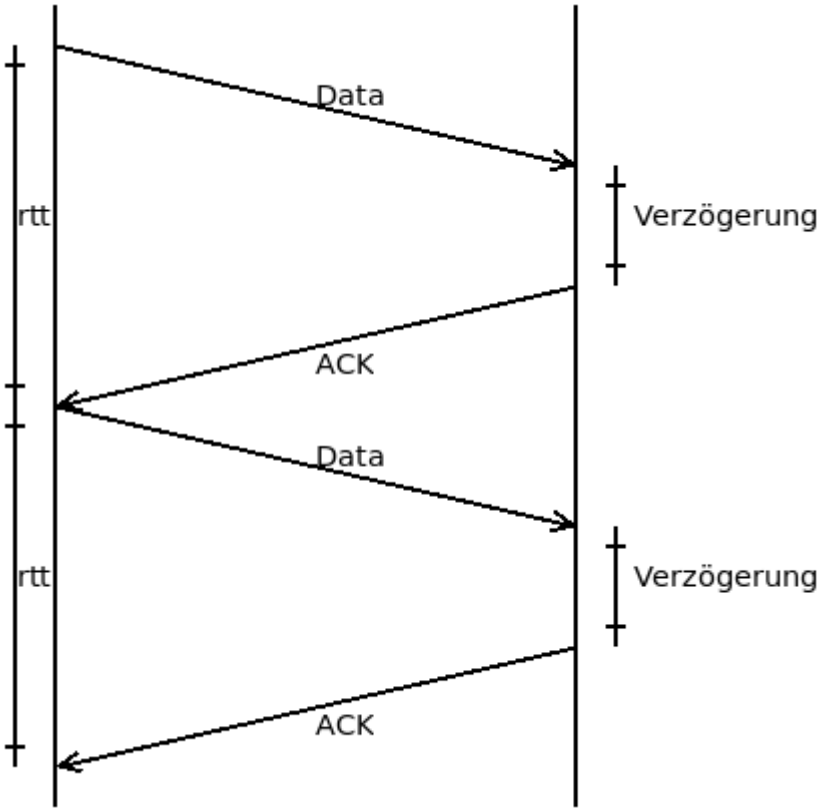
Angriff



TCP-Eigenschaft 1:
Receiver-Window (rwnd)



TCP-Eigenschaft 2:
Round-Trip-Time (rtt)



Gliederung

- **Einleitung**
- **Angriff**
  - Prinzip
  - TCP Eigenschaften
- **Lage im Internet**
  - Verwundbare Anwendungen
  - Verwundbarkeitstests
- **Abwehr**
  - Netzwerkebene
  - Anwendungsebene
- **Demo**
- **Verwandte Angriffe**
- **Quellen / Literatur**


IIS7
internet information services


LIGHTTPD
fly light.


NGINX


SQUID

Echte Verwundbarkeitstest aus rechtlichen Gründen nicht möglich

„Light-Test“: viele gleichzeitige Verbindungen von einer IP

Abbruch bei 100 Verbindungen

Abbruch bei 10 fehlgeschlagenen Verbindungsversuchen

Random-IPs

- **Stichprobengröße: 102**
- **Herkunft: von nmap generierte Ips**

Alexa 100

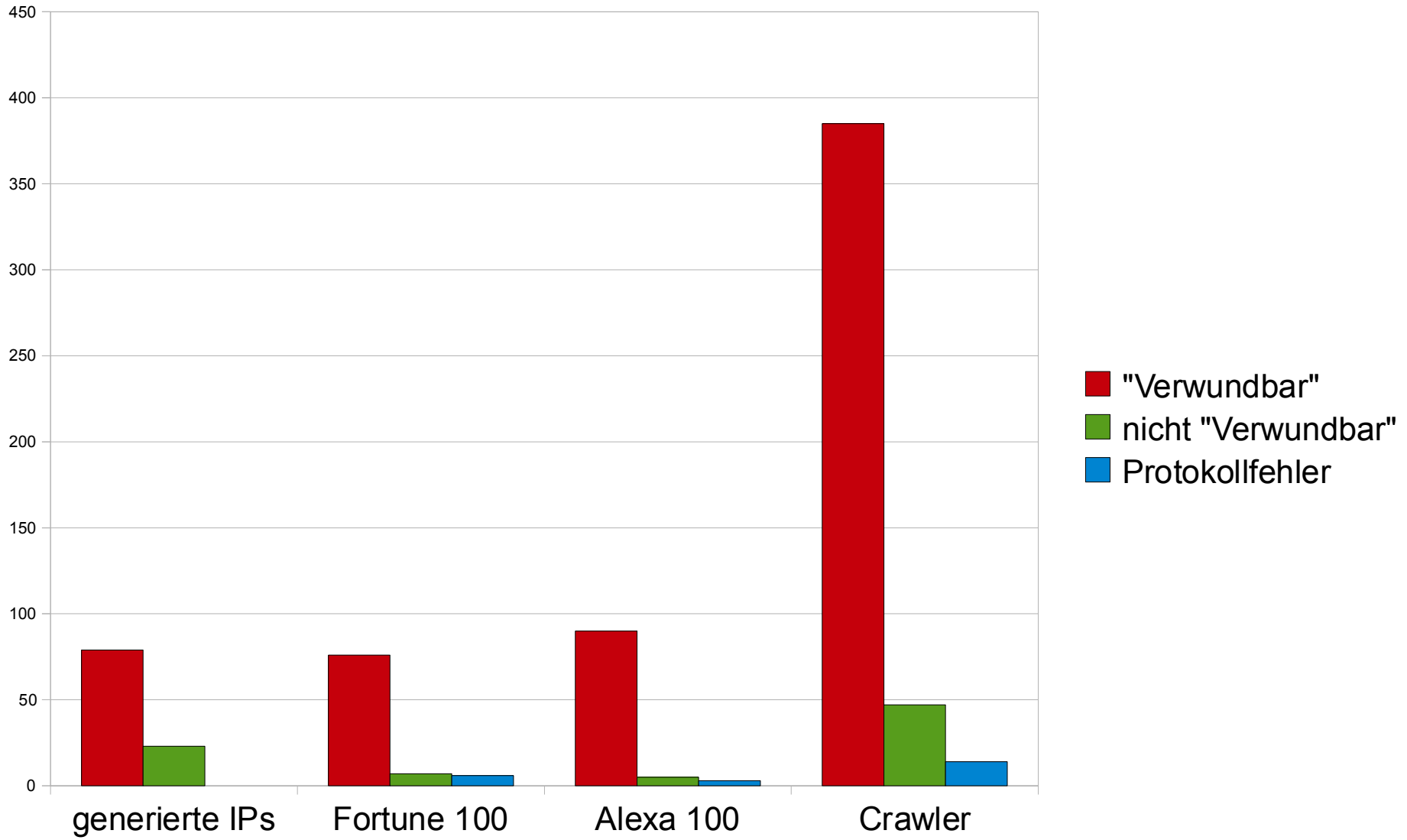
- **Stichprobengröße: 95**
- **Herkunft: alexa.com ranking**

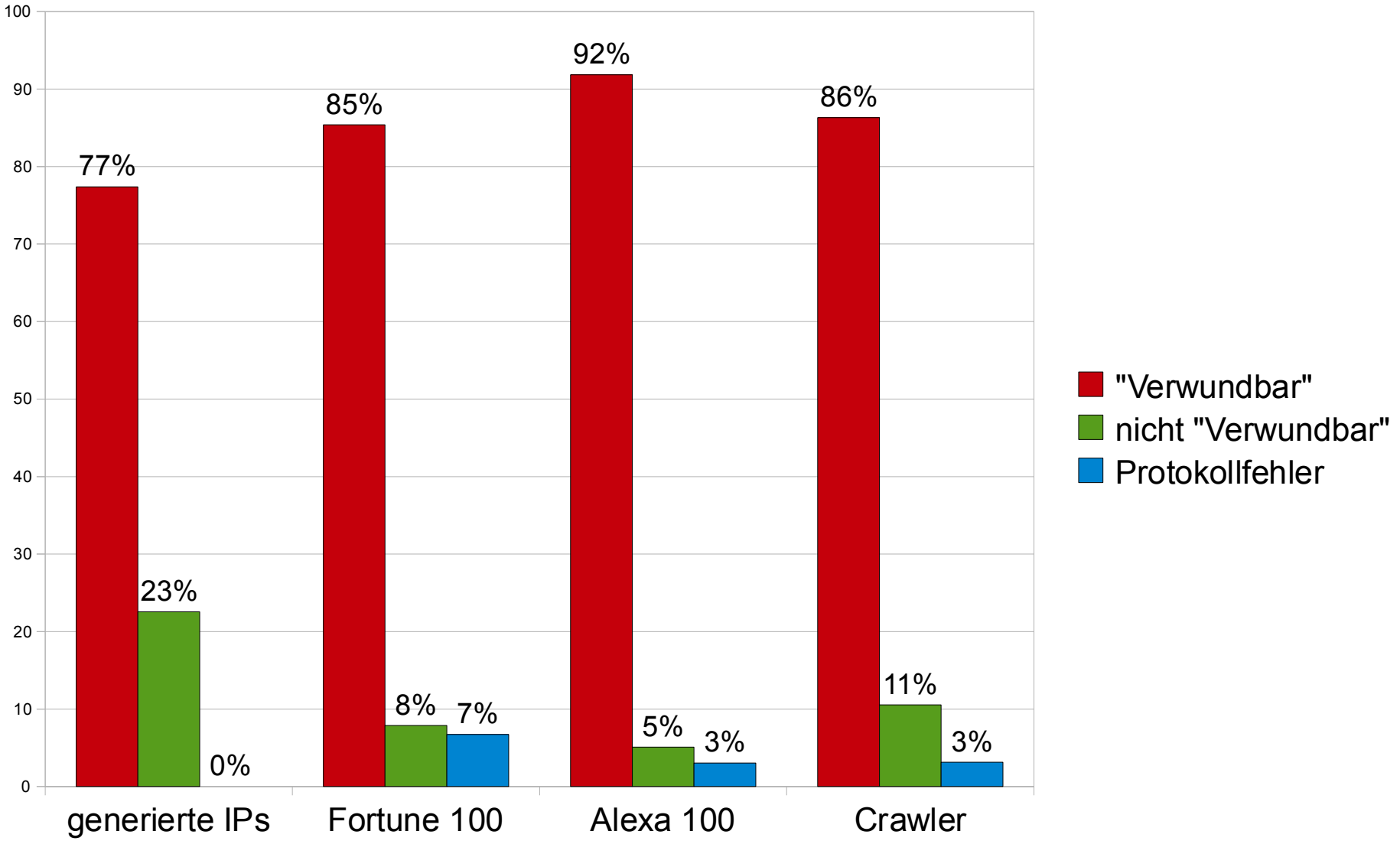
Fortunes 100

- **Stichprobengröße: 85**
- **Herkunft: Fortune Magazine Liste**

Webcrawler

- **Stichprobengröße: 432**
- **Herkunft: per Webcrawler ermittelt**


450
400
350
300
250
200
150
100
50
0
generierte IPs
Fortune 100
Alexa 100
Crawler
"Verwundbar"
nicht "Verwundbar"
Protokollfehler

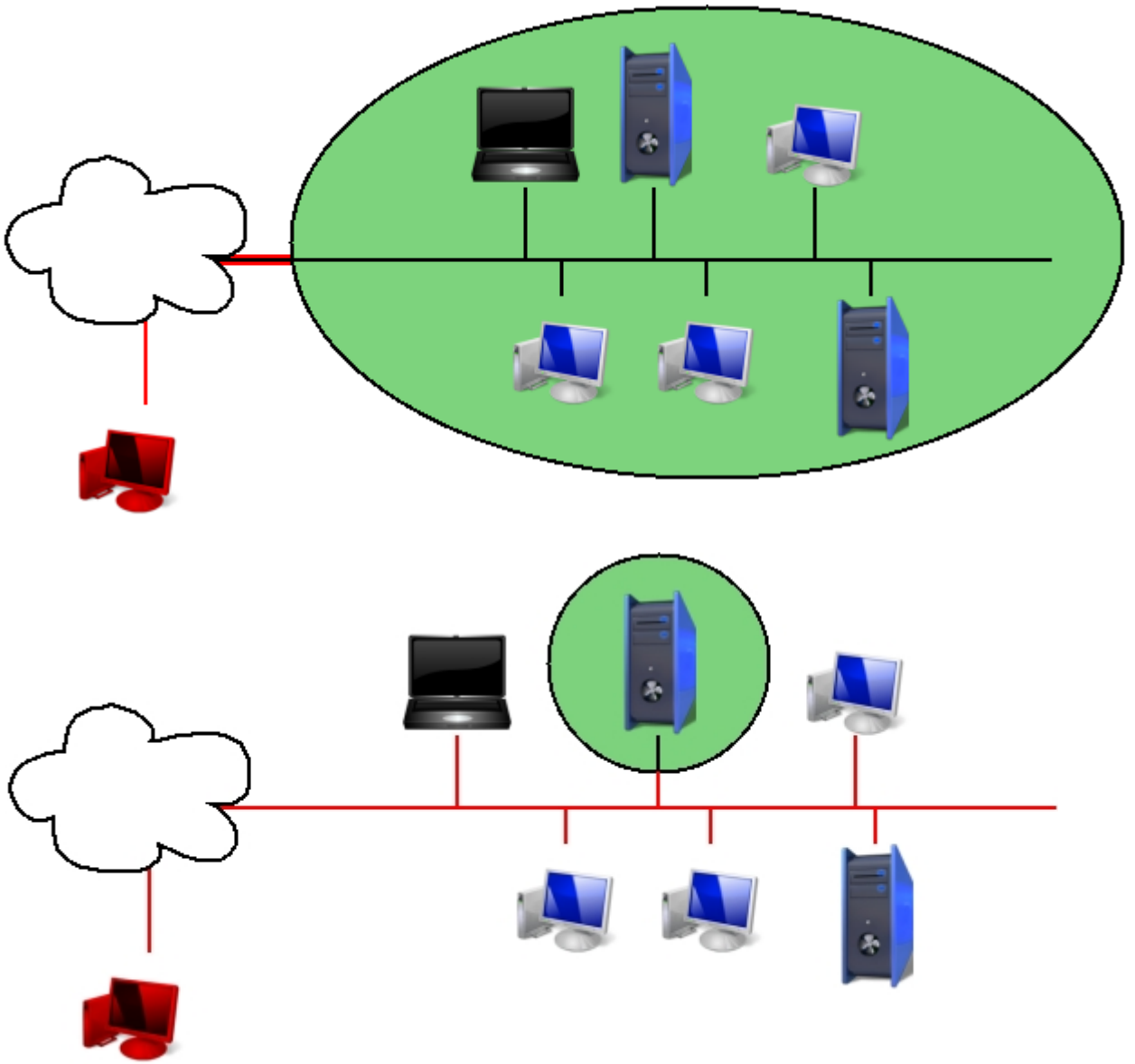

100
90
80
70
60
50
40
30
20
10
0
77%
23%
0%
85%
8%
7%
92%
5%
3%
86%
11%
3%
generierte IPs
Fortune 100
Alexa 100
Crawler
"Verwundbar"
nicht "Verwundbar"
Protokollfehler

Gliederung

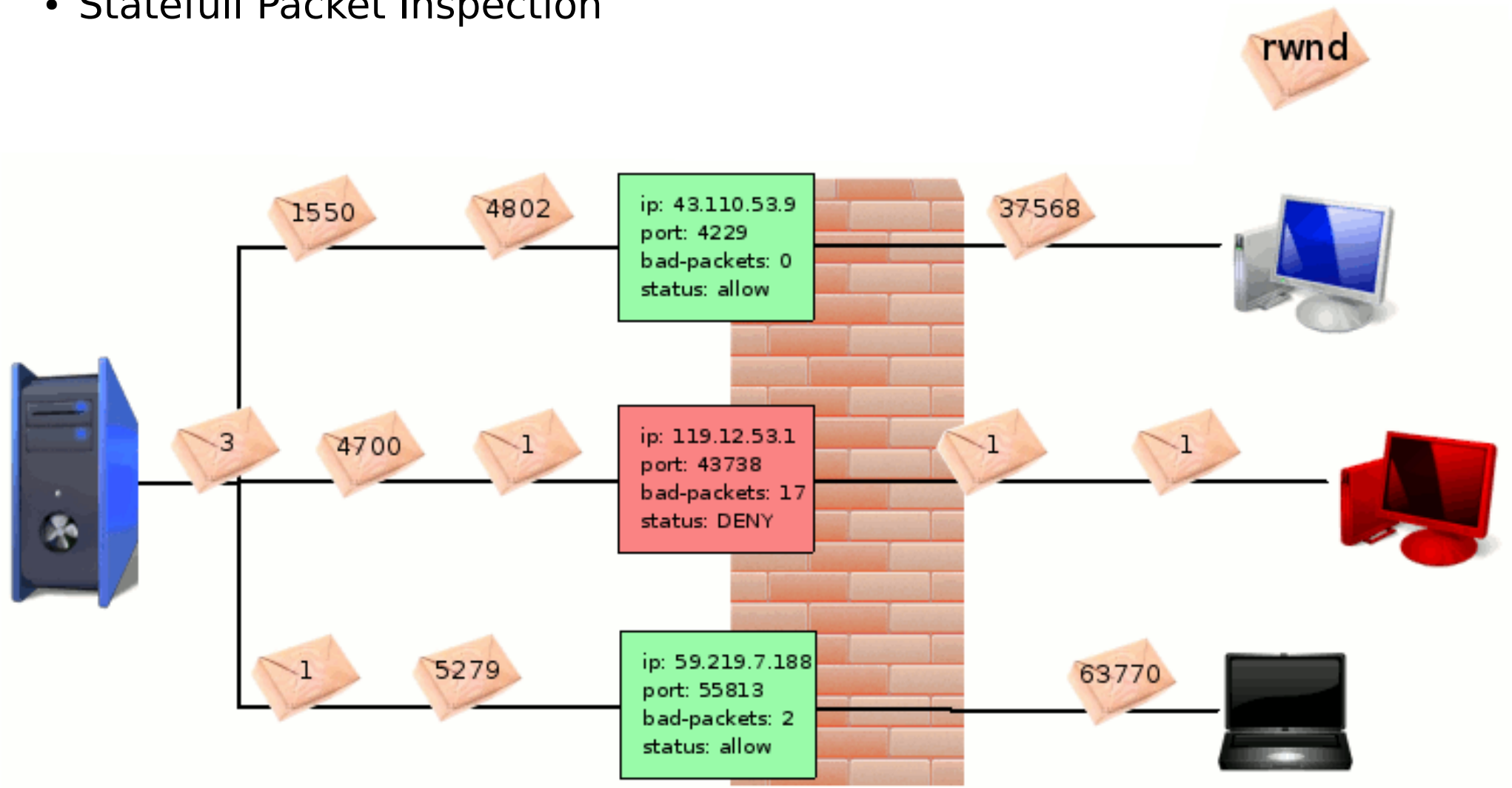
- **Einleitung**
- **Angriff**
  - Prinzip
  - TCP Eigenschaften
- **Lage im Internet**
  - Verwundbare Anwendungen
  - Verwundbarkeitstests
- **Abwehr**
  - Netzwerkebene
  - Anwendungsebene
- **Demo**
- **Verwandte Angriffe**
- **Quellen / Literatur**

Abwehr

- Abwehrbereiche
  - Netzwerkebene
  - Anwendungsebene



- Anzahl gleichzeitiger Verbindungen pro IP-Adresse
- Statefull Packet Inspection



- Unterstützung durch Server-Anwendung:
  - Begrenzung der Verbindungen per IP
  - extern auswertbare Logdateien schreiben
  - Eintrag in Logdatei sofort nach Verbindungsaufbau

Dateigröße: ~ 5300 Byte (www.google.de)
1 Byte / Paket
alle 10 Sekunden 1 Paket

Übertragungsdauer: 5300 * 10 = 53000 Sekunden = 14,7 Stunden!

Erkennen des Angriffs frühestens nach 14,7 Stunden!

Demo

florens@lap2: ~/uni/ba/dslDoS/dist/Release/GNU-Linux-x86

Datei Bearbeiten Ansicht Terminal Hilfe

```
florens@lap2:~/uni/ba/dslDoS/dist/Release/GNU-Linux-x86$ sudo ./dsldos -a conflood -s 192.168.0.100 -d 192.168.0.1 -p 80 -
u testfile.txt --connections-per-second 20 -D 4
Welcome to dslDoS, we will run in debug-level 4
 dsldos::main:  Starting a conflood attack
 ConFlood::startAttack: Starting the ack packets part of a conflood attack
 ConFlood::startAttack: Starting the create connections part of a conflood attack
Connections established: 19 Connections failed: 0
Connections established: 39 Connections failed: 0
Connections established: 59 Connections failed: 0
Connections established: 79 Connections failed: 0
Connections established: 99 Connections failed: 0
Connections established: 119 Connections failed: 0
Connections established: 139 Connections failed: 0
Connections established: 159 Connections failed: 0
Connections established: 179 Connections failed: 0
Connections established: 199 Connections failed: 0
Connections established: 219 Connections failed: 0
Connections established: 239 Connections failed: 0
Connections established: 259 Connections failed: 0
^CCanceled...
florens@lap2:~/uni/ba/dslDoS/dist/Release/GNU-Linux-x86$
```

- Receiver-Window:
  Zur zusätzlichen Verschleierung kann für jedes Paket ein zufälliger, sehr niedriger Wert genommen werden. Dadurch wird die Erkennung schwieriger.

- Round-Trip-Time:
  Einige Server haben in ihrer Standardkonfiguration schon einen sehr hohen Toleranzwert. Durch - dem Angriff vorangehendes - Probing kann dieser Wert ermittelt und als künstliche Verzögerung verwendet werden.

- Slowloris
  - Zielt auf dieselbe Beschränkung
  - Sendet unvollständige HTTP-Header an den Server
  - Verhindert damit ein Schließen des Sockets

- TCP SYN Flooding
  - Sehr hohe Anzahl Verbindungen
  - Einsatz nur praktikabel als DDos

- PHP Interpreting Host Flooding
  - Viele Anfragen nach dynamisch generierten PHP-Seiten senden
  - Der Host muss die Seiten berechnen → Auslastung

Quellen / Literatur

[Pos81] J. Postel. Transmission control protocol. RFC 793, Internet Engineering Task Force, September 1981.

[APS99] M. Allman, V. Paxson, and W. Stevens. TCP congestion control. RFC 2581, Internet Engineering Task Force, April 1999.

[BSI07] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Erkennung und Abwehr von DDoS-Angriffen im Internet - Einschätzung und Bewertung aktueller Bedrohungen, Bonn, 2007.

[Slo09] http://ha.ckers.org/slowloris