Aspekte der Netzwerksicherheit: Transmission Control Protocol (TCP)

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de

Version: 1.3.7

Quellen: Folien von Prof. Dr. Henning Pagnia bzgl. Netzwerksicherheit

---

Folien: [HTML] https://delors.github.io/sec-tcp/folien.de.rst.html
[PDF] https://delors.github.io/sec-tcp/folien.de.rst.html.pdf

Fehler melden: https://github.com/Delors/delors.github.io/issues

1. Transmission Control Protocol (TCP)

TCP Grundlagen

- Protokoll der Schicht 4 (Transport Layer) basiert auf IP
- verbindungsorientierte Kommunikation zweier Rechner im Internet zuverlässig und geordnet:
  - Verwerfen von Duplikaten und fehlerhaft übertragener Pakete
  - automatisches Wiederversenden fehlender Pakete
  - Nachrichtenpuffer: Daten werden in korrekter Reihenfolge an Applikation zugestellt
- Verbindungsaufbau immer zwischen zwei Sockets (Socket-Adresse: IP Adresse und 16 Bit-Port-Nummer)

Aufbau einer TCP Verbindung

Dreifacher Handshake:

Terminologie:

SYN: *synchronize (session establishment)*

ACK: *acknowledge*

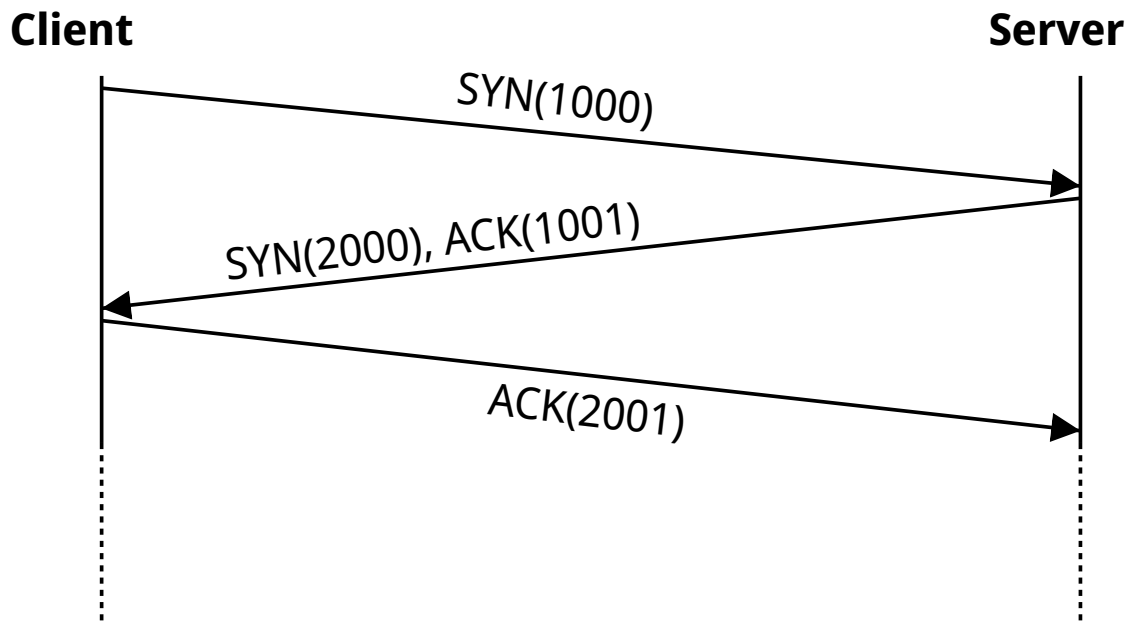
RST: *reset*

Verbindungsaufbau - Ablauf:

1. Client sendet SYN Paket mit initialer Sequenznummer (hier) 1000 an den Server.
2. Server sendet ein SYN-ACK Paket mit seiner initialen Sequenznummer (hier) 2000 und ein ACK mit der Sequenznummer 1001 (initiale Sequenznummer des Clients +1) an den Client
3. Client sendet ein ACK Paket mit Sequenznummer 2001 (initiale Sequenznummer des Servers +1) an den Server; danach ist die Verbindung aufgebaut.

Das Betriebssystem sollte die initialen Sequenznummern zufällig wählen, so dass ein Angreifer diese nicht leicht vorhersagen kann. Beide Seiten haben eigene Sequenznummern, die unabhängig voneinander sind.

Bei einer laufenden Verbindung werden die Sequenznummern inkrementiert und es ist nicht (mehr) erkennbar wer die Verbindung aufgebaut hat.



Ports bei TCP

- Port-Nummern werden für die Kommunikation zwischen zwei Diensten/Prozessen verwendet
- Ports sind 16 Bit Zahlen (0-65535)
- (Unix) Ports < 1024 sind privilegiert (nur root kann diese öffnen)
- einige Port-Nummern sind Standarddiensten zugeordnet

Port-Nummern einiger Standarddienste [1]

Ungeschützte Dienste (Kommunikation findet ohne Verschlüsselung statt.)

Protokoll	Dienst	Portnummer
ftp	Dateitransfer	21
smtp	Simple Mail Transfer Protocol	25
dns	Domain Name System	53
http	Hypertext Transfer Protocol	80
login	Login auf entfernte Rechner	513

Geschützte Dienste (Die Kommunikation ist verschlüsselt.)

Protokoll	Dienst	Portnummer
ssh	Secure Shell	22
https	HTTP über Secure Socket Layer	443
smtps	SMTP über Secure Socket Layer	465
imaps	IMAP über Secure Socket Layer	993
pop3s	POP3 über Secure Socket Layer	995

[1] Port numbers assigned by IANA

Angriffe auf TCP - Motivation

- Netzwerkprogrammierung mit TCP ist relativ komfortabel.
- Viele Dienste sind mit TCP implementiert.

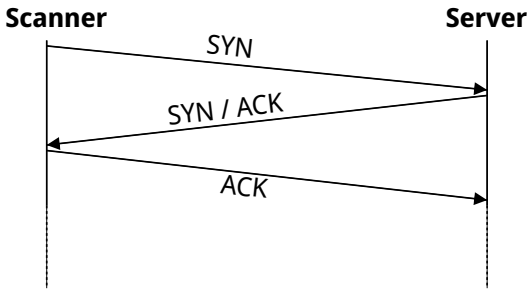
  Insbesondere in der Anfangszeit hatten viele TCP Dienste sowohl technische als auch konzeptionelle Schwachstellen. Einige dieser Schwachstellen sind bis heute nicht behoben.
- Das Auffinden von angreifbaren Diensten kann mit Hilfe von Port Scans systematisch erfolgen.

  Server haben heutzutage im Allgemeinen alle nicht verwendeten Dienste geschlossen.

Port Scans: TCP Connect Scan

Vorgehen

Aufbau vollständiger Verbindungen
zu allen bzw. zu ausgewählten Ports.



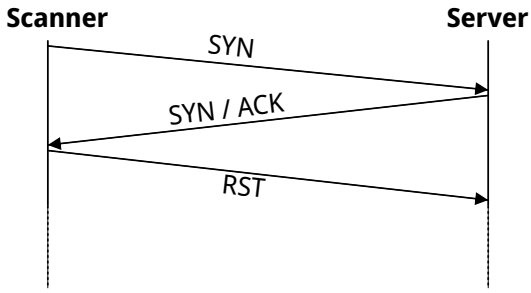
Bewertung

- simpelster Port Scan
- große Entdeckungsgefahr (Scan selbst ist kein Angriff)
- mögliche Verbesserung: zwischen dem Scannen mehrerer Ports Pausen einstreuen (Wie lange?)

Port Scans: TCP SYN Scan

Vorgehen

1. Senden eines TCP-Segments mit gesetztem SYN-Flag an einen Port
2. falls der *Port offen* ist, kommt SYN/ACK zurück danach RST senden
3. falls der *Port nicht offen* ist, kommt RST (oder nichts) zurück



Bewertung

- kein vollständiger Verbindungsaufbau
- meist nicht protokolliert
- geringe(re) Entdeckungsgefahr

Port Scans: Stealth Scans

Vorgehen: Versenden eines für den Verbindungsaufbau ungültigen TCP-Segments an einen Port:

- NULL-Scan (keine Flags)
- ACK-Scan (ACK-Flag)
- FIN-Scan (FIN-Flag)
- XMAS-Scan (alle Flags)

Laut RFC kommt RST zurück, falls der Port offen ist. (Reaktion ist de-facto aber abhängig vom Betriebssystem und oft kommt keine Antwort zurück.)

Bewertung
▫ Zugriff wird meist nicht protokolliert
▫ Scan bleibt unbemerkt

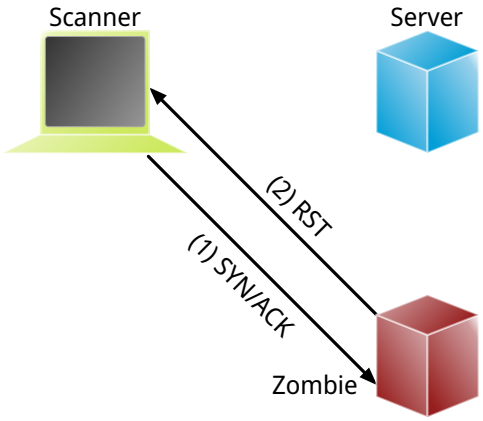
XMAS-Scan:

Bei diesem Scan sind alle Flags gesetzt; ein XMAS-Scan wird auch als Christmas-Tree-Scan bezeichnet, da das Paket erleuchtet ist wie ein Weihnachtsbaum.

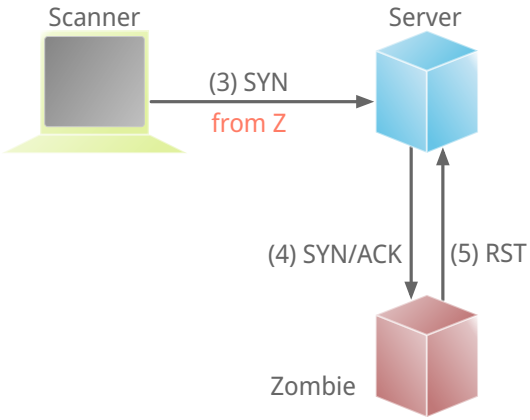
Port Scans: Idle Scan [2]

Bei allen bisher betrachteten Scans kann der Scanner prinzipiell identifiziert werden. Unter Verwendung eines sog. Zombies geht es auch anders:

Sondiere IP ID des Zombies:



Starte Scan:



Zombie: ein Rechner (Computer, Drucker oder anderes IoT Gerät) im Internet *möglichst ohne eigenen Netzverkehr* und mit *altem* Betriebssystem, bei dem die IP ID in vorhersehbarer Weise inkrementiert wird. (Bei modernen Betriebssystemen ist die IP ID zufällig, **konstant** oder sogar `null`.)

Grundlegende Idee:

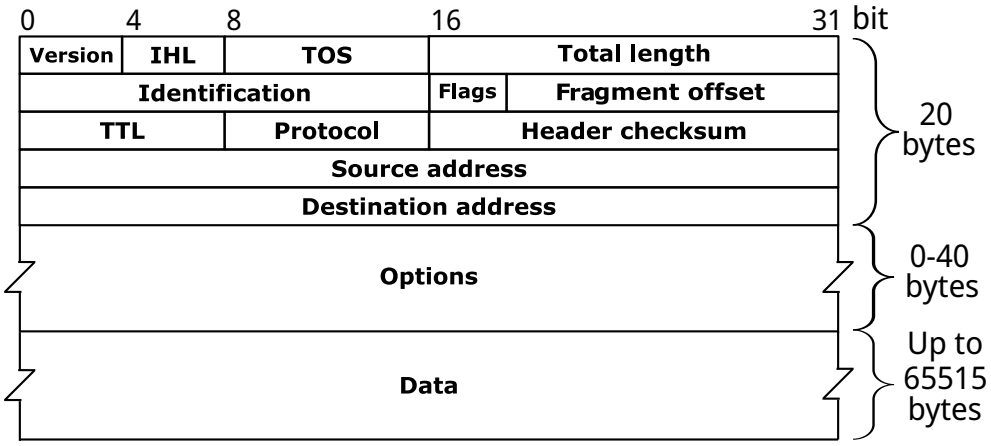
Der Zombie sendet ein RST Paket zurück, da er kein SYN gesendet hat und kein SYN/ACK erwarte. Dadurch erfährt der Angreifer die aktuelle IP ID des Zombies. Über diesen Seitenkanal - d. h. die Veränderung der IP ID des Zombies - kann der Angreifer nun den Zustand des Ports auf dem Zielrechner ermitteln.

※ Hinweis

Sollte ein Intrusion Detection System vorhanden sein, so wird dieses den Zombie als Angreifer identifizieren.

Hintergrund - IP ID

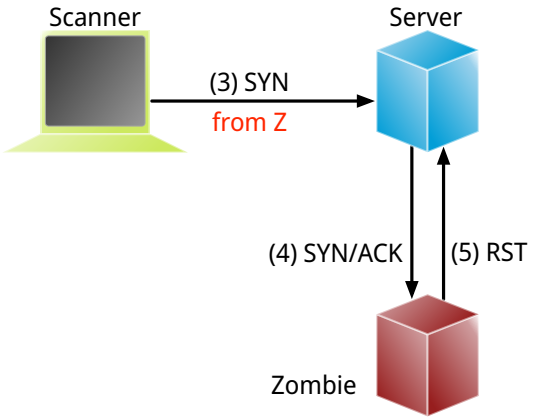
Das Feld *IP Identifikation (IP ID)* dient der Identifizierung einer Gruppe von Fragmenten eines einzelnen IP-Datagramms.


0
4
8
16
31
bit
Version
IHL
TOS
Total length
Identification
Flags
Fragment offset
TTL
Protocol
Header checksum
Source address
Destination address
20 bytes
Options
0-40 bytes
Data
Up to 65515 bytes

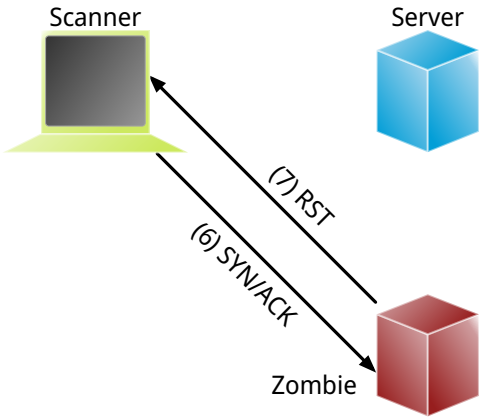
[2] NMap Book

Port Scans: Idle Scan

Starte Scan:



Sondiere IP ID des Zombies:



Port Scans: Idle Scan - Zusammenfassung

- Angreifer sendet SYN/ACK Paket an Zombie
- der Zombie antwortet mit RST und enthüllt seine IP ID ( *IP Fragment Identification Number*).
- Angreifer sendet SYN („mit IP vom Zombie“) an Port des Servers:

  [**Port offen**] Der Zielrechner antwortet mit SYN/ACK an den Zombie, wenn der Port offen ist. Der Zombie antwortet darauf mit RST an den Server, da er kein SYN gesendet hat und kein SYN/ACK erwartet und *erhöht seine IP ID*.

  [**Port geschlossen**] Der Zielrechner antwortet mit RST an den Zombie, wenn der Port geschlossen ist. Dies wird vom Zombie ignoriert.
- Der Angreifer sendet wieder ein SYN/ACK an den Zombie, um die IP ID zu erfahren.

Mit einem IDLE Scan kann nicht unterschieden werden, ob der Port geschlossen oder gefiltert ist.

Port Scans mit nmap

- alle Arten von Port-Scans möglich
- auch OS fingerprinting
- u. U. sogar Ermittlung der Versionsnummern von Diensten

```
$ nmap 192.168.178.121 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-14 13:16 PST
Nmap scan report for Michaels-MacBook-Pro (192.168.178.121)
Host is up (0.0056s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
445/tcp  open  microsoft-ds
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
```

OS-Fingerprinting

Beim OS-Fingerprinting werden Datenpakete analysiert, die aus einem Netzwerk stammen, um Informationen für spätere Angriffe zu gewinnen. Durch die Erkennung des Betriebssystems, mit dem ein Netzwerk arbeitet, haben Hacker es leichter, Schwachstellen zu finden und auszunutzen. OS-Fingerprinting kann auch Konfigurationsattribute von entfernten Geräten sammeln. Diese Art von Aufklärungsangriff ist in der Regel (einer) der erste(n) Schritt(e).

Es gibt zwei Arten von OS-Fingerprinting: (1) Aktiv und (2) passiv.

1. Bei einem aktiven OS-Fingerprinting-Versuch senden die Angreifer ein Paket an das Zielsystem und warten auf eine Antwort, um den Inhalt des TCP-Pakets zu analysieren.
2. Bei einem passiven Versuch agieren die Angreifer eher als "Schnüffler", der keine absichtlichen Änderungen oder Aktionen im Netzwerk vornimmt. Passives OS-Fingerprinting ist ein unauffälligerer, aber wesentlich langsamerer Prozess.

Port Knocking

- Ein Knock-Daemon versteckt offene Ports auf dem Server.
- Zugriffe auf alle Ports werden im Log-File protokolliert.
- Knock-Daemon beobachtet das Log-File.
- Erst nach Erkennen einer vordefinierten (Einmal-)Klopfsequenz öffnet der Knock-Daemon den gewünschten Port für diesen Client.
- Client kann nun die Verbindung aufbauen.
- Weiterentwicklung: TCP Stealth

  In diesem Fall werden offene Ports dadurch versteckt, dass sie nur auf spezielle SYN-Pakete mit bestimmten Sequenznummern reagieren. Die Sequenznummern sind ggf. kryptografisch abgesichert und basieren auf vorher ausgetauschten Schlüsseln.

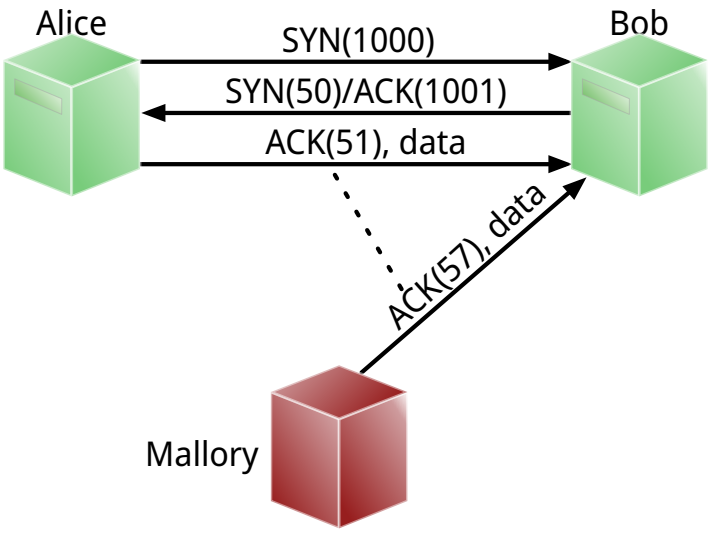
Weiterführend

Alternativen zu einer Knock-Sequenz ist zum Beispiel, dass der Port nur dann als offen gilt, wenn die IP ID eine bestimmte Sequenznummer aufweist.

M.Krzywinski: Port Knocking: Network Authentication Across Closed Ports in SysAdmin Magazine 12: 12-17. (2003)

Connection Hijacking

Angreifer übernimmt eine bestehende - zum Beispiel eine bereits durch (Einmal-)Passwort authentisierte - Verbindung.



TCP/IP-Hijacking ist eine Form eines Person-in-the-Middle-Angriffs. Der Angreifer bestimmt erst die IP-Adressen der beiden Sitzungsteilnehmer.

Danach gibt es mehrere Möglichkeiten:

- Der Angreifer schickt ("in einer Pause") ein Paket mit der passenden Sequenznummer an den Server.

  (Dies kann dann in einem ACK-Storm enden, was ggf. unterbunden werden muss (zum Beispiel durch das Senden eines RSTs), oder ignoriert werden kann.)
- Der Angreifer macht einen Client mit einem DoS-Angriff unerreichbar, um sich dann mit dem Anderen zu verbinden, indem er die Netzwerk-ID des ausgeschalteten Clients nutzt.

Denial-of-Service (DoS) Angriffe

Ziel des Angreifers: Lahmlegen eines Dienstes oder des ganzen Systems ...

- durch Ausnutzen von Schwachstellen ( *vulnerabilities*) wie z. B. Buffer Overflows
- durch Generierung von Überlast (Ausschöpfen von RAM, CPU, Netzwerkbandbreite, ...)

Beispiel

Ping-of-Death

(Historisch: aus dem Jahr 1997)

Ein `ping` (vgl. Internet Control Message Protocol (ICMP)) verwendet üblicherweise kleine Nachrichten, aber die verwendete Länge ist einstellbar.

Falls die Länge zu groß ist ⇒ Buffer Overflow ⇒ Systemabsturz!

Variante: mittels Fragmentierung ließen sich generell übergroße IP-Pakete (>65,536 Byte) erstellen.

Denial-of-Service: SYN-flooding Angriff

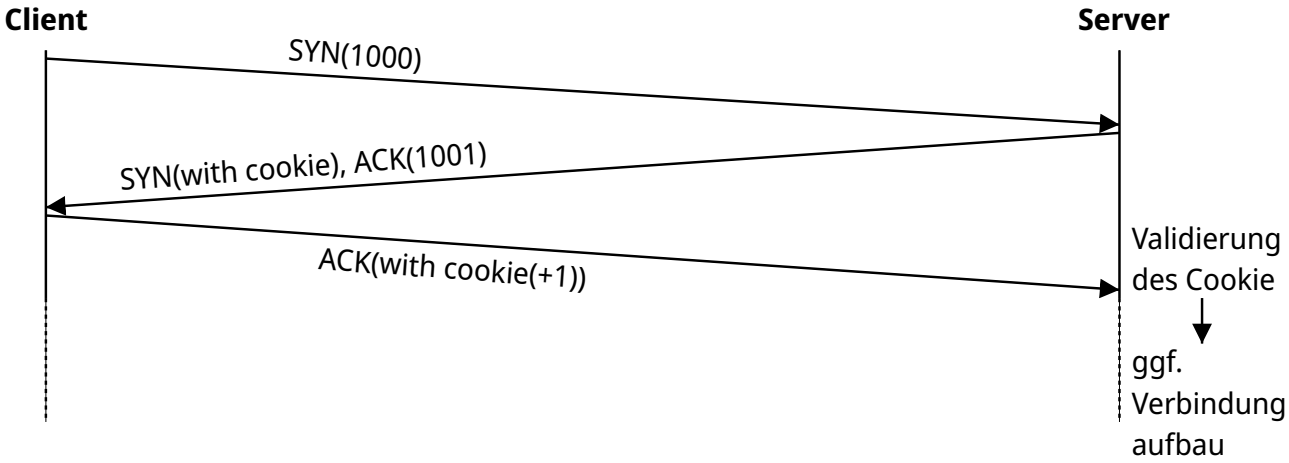
- Angriff auf Design
- Angreifer sendet eine Verbindungsaufbauanforderung (gesetztes SYN-Flag) an Zielmaschine
- Server generiert eine halboffene TCP-Verbindung
- Angreifer wiederholt in schneller Folge dieses erste Paket zum Verbindungsaufbau

  ⇒ vollständiges Füllen der internen Systemtabelle

  ⇒ Anfragen normaler Benutzer werden zurückgewiesen
- Angreifer verwendet i. Allg. IP-Spoofing weswegen Firewalls wirkungslos sind.
- Abwehr: SYN-Cookies

SYN-Cookies - D J. Bernstein

SYN-Cookies sind speziell konstruiert initiale Sequenznummern.

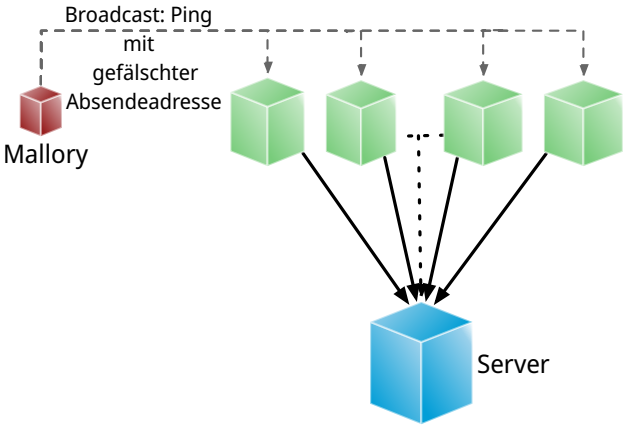


Der Cookie ermöglicht es, dass keine Informationen im Speicher gehalten werden müssen. Der Cookie encodiert die Informationen, die der Server benötigt, um die Verbindung aufzubauen: Client IP, time window, etc.

Distributed Denial-of-Service (DDoS) Angriff

Opfer wird von sehr vielen Angreifern mit Nachrichten überflutet.

Ein Beispiel: Smurf-Angriff:

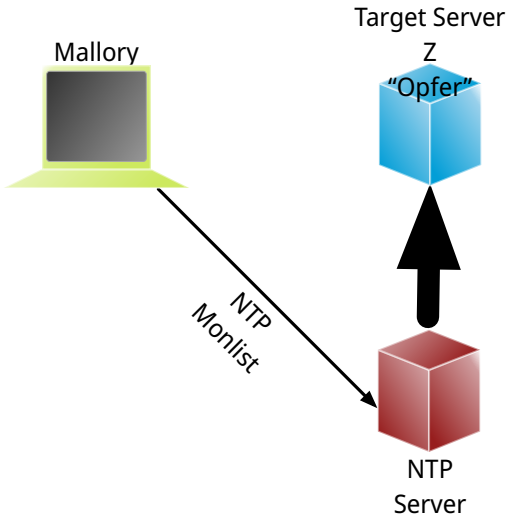


Distributed Denial-of-Service (DDoS) Angriff

- Bot-Netze (Botnetze) werden verwendet, um DDoS-Angriffe durchzuführen.
- Bot-Netze können viele 10.000 Rechner umfassen.
- IoT Geräte sind besonders beliebt (z. B. IP-Kameras, Smart-TVs, Smart-Home Geräte, ...), da diese oft nicht ausreichend geschützt sind und trotzdem permanent mit dem Internet verbunden sind.
- Beliebte Ziele:
  - Onlinespieleserver
  - Banking-Portale
  - politische Webseiten
- Firewalls und Intrusion Detection Systeme sind meist wirkungslos, da die Angriffe von vielen verschiedenen IP-Adressen kommen.

Distributed-Reflected-Denial-of-Service Angriff

Idee eines (DRDoS) Angriffs



- Es wird eine Anfrage an einen Server gesendet, die eine große Antwort auslöst.

  Z. B. hat(te) der NTP Monlist Befehl eine Antwort, die ca. 200 Fach größer ist als die Anfrage!

- Mittels IP-Spoofing wird die IP-Adresse des Opfers als Absenderadresse verwendet.
- Es werden insbesondere Dienste basierend auf UDP verwendet, da hier keine Verbindung aufgebaut werden muss.
- Nehmen einen signifikanten Teil aller DDoS-Angriffe ein.
- Die Tatsache, dass die Sender legitime Server sind, erschwert die Abwehr.
- *Egress Filtering* kann helfen, die Verwendung von IP-Spoofing zu verhindern.

Bereits im Jahr 2018 wurde ein Angriff mit einer Bandbreite von 1,7 TBit/s beobachtet.

Egress Filtering: Der Router verwirft alle Pakete, die eine Absenderadresse verwenden, die nicht aus dem eigenen Netzwerk stammt.

Distributed-Denial-of-Service-Angriffe (DDoS)

[...] Google's DDoS Response Team has observed the trend that distributed denial-of-service (DDoS) attacks are **increasing exponentially in size**. Last year, we blocked the largest DDoS attack recorded at the time. This August [2023], we stopped an even larger DDoS attack — 7½ times larger — that also used new techniques to try to disrupt websites and Internet services.

This new series of DDoS attacks reached **a peak of 398 million requests per second (rps)**, and relied on a novel HTTP/2 “Rapid Reset” technique based on stream multiplexing that has affected multiple Internet infrastructure companies. By contrast, last year's largest-recorded DDoS attack peaked at 46 million rps.

—Okt. 2023 - DDoS Attack with 398 Million RPS

Cloudflare hat Mitte Mai den "größten jemals registrierten" Denial-of-Service-Angriff (DDoS) mit [...] 7,3 Terabit pro Sekunde (TBit/s) blockiert. [...] Diese Attacke war demnach rund 12 Prozent größer als der vorherige Rekord und lieferte ein massives Datenvolumen von 37,4 Terabyte in nur 45 Sekunden. [...]

Stellen Sie sich vor, Sie könnten mit Ihrem Smartphone 12,5 Millionen hochauflösende Fotos schießen und hätten nie einen vollen Speicherplatz." Und das alles in 45 Sekunden.

[...] Mitgewirkt hätten über 122.145 Quell-IP-Adressen, die sich über 5433 autonome Netzwerksysteme in 161 Ländern erstreckten.

—22.06.2025 Heise.de - Rekord DDoS Angriff

[...] Der letzte rekordverdächtige Überlastungsangriff ist noch gar nicht so lange her, da vermeldet Cloudflare schon den nächsten beobachteten Spitzenwert. Am Montag erreichte ein Distributed-Denial-of-Service-Angriff (DDoS) in der Spitze eine Last von 11,5 Terabit pro Sekunde. Das entspricht umgerechnet mehr als 1,4 Terabyte je Sekunde oder dem Inhalt von 184 randvollen DVDs.

[...] Dabei sendeten die Angreifer 5,1 Milliarden Pakete pro Sekunde (Bpps). Bei letzterer handelte es sich demnach um eine UDP-Flood-Attacke, die ihren Ausgangspunkt hauptsächlich in der Google-Cloud hatte. Die Zeitspanne, die der Höchstlast-Angriff einnahm, war etwa 35 Sekunden lang, schreibt Cloudflare weiter.

—03.09.2025 - Heise.de: Überlastungsattacke erreicht 11,5 TBit pro Sekunde

Distributed Denial-of-Service Angriffe - Beispiele

- **TCP Stack Attacks** SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, other combinations of TCP Flags, slow TCP attacks
- **Application Attacks**:HTTP GET/POST Floods, slow HTTP Attacks, SIP Invite Floods, DNS Attacks, HTTPS Protocol Attacks
- **SSL/TLS Attacks**: Malformed SSL Floods, SSL Renegotiation, SSL Session Floods
- **DNS Cache Poisoning**
- **Reflection Amplification Flood Attacks**: TCP, UDP, ICMP, DNS, mDNS, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service
- **Fragmentation Attacks**: Teardrop, Targa3, Jolt2, Nestea
- **Vulnerability Attacks**
- **Resource Exhaustion Attacks**: Slowloris, Pyloris, LOIC, etc.
- **Flash Crowd Protection**
- **Attacks on Gaming Protocols**

Schutz vor DDoS-Angriffen: On-Site Maßnahmen

- Aufrüsten der Ressourcen (z. B. Bandbreite, CPU, RAM, ...)
- Exemplarische Sofortmaßnahmen bei aktivem Angriff:
  - Whitelisting von IP-Adressen von besonders wichtigen Clients
  - Blacklisting von IP-Adressen aus bestimmten Bereichen
  - Captchas
  - Überprüfung der Browser-Echtheit
- Anti-DDos Appliances

Achtung!

Diese Maßnahmen sind häufig teuer und ggf. begrenzt effektiv; wenn der Angriff die verfügbare Bandbreite übersteigt, sind diese Maßnahmen darüber hinaus wirkungslos.

Schutz vor DDoS-Angriffen: Off-Site Maßnahmen

- Einbinden des ISP
- Einbinden spezialisierter Dienstleister

  (Im Angriffsfall wird mittels BGP-Rerouting der Traffic an den Dienstleister umgeleitet, der dann die DDos Attacke filtert.)
- Content-Delivery-Networks (CDNs) für statische Inhalte (z. B. Cloudflare, Akamai, ...)
- Distributed Clouds

Übung

1.1. Port Scans - IDLE Scan

- Warum kann bei einem IDLE Scan nicht festgestellt werden weshalb ein Port geschlossen oder gefiltert ist?
- Welchen Wert hat die IP ID des Zombies, der einem IDLE Scan durchführt, wenn der Zielport offen bzw. geschlossen ist, wenn der Scanner diesen wieder abfragt?

Übung

1.2. DDoS

1. Welches Problem entsteht wenn zum Schutze vor Angriffen auf die Verfügbarkeit die Ressourcen von IT-Systemen und deren Internet-Anbindung erhöht werden?
2. Recherchieren Sie was ein „Low and Slow Angriff“ ist.
3. Wo kann überall „Egress filtering“ statt finden.