# DDOS Attacken

# Tutorial

# Grundlagen Distributed Denial of Service Attacken (DDoS)

## 1.1 Übersicht

Im Gegensatz zu einer einfachen Denial-of-Service-Attacke werden Distributed Denial-of-Service-Attacken nicht nur über einen Angriffsrechner gefahren, sondern gleichzeitig im Verbund mit mehreren Rechnern. Dies hat zur Folge, dass es für die Betroffenen sehr aufwendig ist, festzustellen von wo die Angriffe kommen.
Für eine DDoS-Attacke plaziert ein Angreifer einen sogenannten Agenten auf verschiedenen Rechnern im Internet, vornehmlich auf Rechner, die per Standleitung und Breitbandanschluss angebunden sind. Diese Plazierung kann auch schon Monate vor dem eigentlichen Angriffen erfolgen. Wird nun ein Angriff auf ein bestimmtes Opfer gestartet, erfolgen die Angriffe über die Rechner, auf denen die Agenten installiert sind, gleichzeitig und erzeugen in der Gesamtheit ein enormes Angriffsvolumen um das Ziel für alle anderen Anwendungen unerreichbar zu machen.

## 1.2 Die Hintergründe von DDoS

Schon seit den Anfängen des Internets existieren sogenannte „ Denial of Service „ Attacken, deren Ziel es ist, die Verfügbarkeit bestimmter Server und deren Dienste drastisch einzuschränken oder sogar zu verunmöglichen. Mit der Kommerzialisierung- und der damit zunehmenden Wichtigkeit des Internets begann auch die Anzahl der Attacken stark zuzunehmen. Dieses Verhalten ist leicht feststellbar, indem man auf dem Heimcomputer für einige Zeit einen Network Scanner (wie z.B BlackICE Defender) laufen lässt und das Logfile etwas genauer anschaut.

### 1.2.1 Der Anfang im IRC (Internet Relay Chat)

Ähnliche Attacken existieren schon seit einigen Jahren und findet in den IRC Chat-Räumen (IRC = Internet Relay Chat) ihren Anfang. Hacker versuchen in die PC's einzubrechen und diese dann für die Attacken gegen Chat-Räume zu benutzen. Das IRC Protokoll ist deswegen so interessant, weil die erste Person, die den Chat-Raum betritt automatisch den Moderator-Status der Diskussion erhält. Ein Moderator kann andere User hinauskicken oder ihnen den Moderator-Staus verleihen. Wie auch immer, wenn nun der letzte Moderator den Chat-Raum verlässt, werden seine Privilegien an einen normalen User weitergegeben. So versuchen die Hacker alle rivalisierten Moderatoren von anderen Hacker Gangs aus dem Chat hinauszukicken, damit sie den Chat kontrollieren können. Hacker Gangs liefern sich richtige Kriege im Internet um diese Chat-Räume und ihre rivalisierten Gangs zu überwachen. In diesen Chat Underground Kriegen benutzen Hacker automatische Programme „Daemons„ genannt (Eng. Kurzform für Roboter) und versuchen diese auf möglichst vielen Computern im Internet zu verteilen. Ein Typ von diesen „Daemons“ versucht nun automatisch in den Chat-Räumen eingeloggt zu bleiben, den Moderator-Status zu erhalten und diesen Status an andere „Daemons“ weiterzugeben. Ein anderer Typ von „Daemons“ versucht mittels DoS-Attacken existierende Moderatoren von anderen Gangs zu stören, mit dem Ziel, sie aus dem Chat zu schiessen. IRC-Daemons sind seit einigen Jahren erhältlich, aber wirklich gute DoS-Daemons gibt es erst seit einigen Monaten. In der Vergangenheit konnte mit einer einzigen DoS-Attacke (z.B Ping-of-Death) ein Rechner zum Abstürzen gebracht werden, heutzutage sind die meisten Rechner besser geschützt und die Schwachstellen behoben.

### 1.2.2 Das Flooden

Die Hacker mussten also zu einer neuen Methode greifen, das „Flooding“ war geboren. Beim „Flooding“ werden nicht mehr die Rechner angegriffen, sondern die Internet Verbindung der Rechner. In dieser Technik werden eine hohe Anzahl von Pings an einen Rechner gesendet, bis dessen Verbindung keinen anderen Verkehr mehr verarbeiten kann. Das grösste Problem dieser Methode ist, dass der Angreifer eine schnellere Internet Verbindung als das Opfer haben muss. Eine Möglichkeit um dieses Problem beheben zu können, ist das Hacken von Rechnern mit sehr schnellen Internet Verbindungen und diese zum Flooden von anderen Gangs zu benutzen. Nun versuchten die Hacker Gangs die gehackten Rechner zu verbinden und mit einem „Master“ Programm zu steuern. Unbemerkt horchen die „Daemons“ nun auf den gehackten Servern bis sie vom „Master“ den Befehl „go“ mit der Ziel IP-Adresse der kontrahierenden Gangs erhalten und Flooden dann gemeinsam das Ziel. Die Hacker Gangs scannten immer grössere Gebiete des Internets ab und suchten immer mehr Rechner zum Hacken für ihre IRC- oder DoS Daemons. Die sogenannten „Verteilten Denial of Service“ (DDoS) Attacken waren erfunden.

### 1.2.3 DDoS Heute

Nebst dem Cyberwar in den Chat-Räumen werden jetzt auch „grosse“ Internetseiten angegriffen. Ein neuer Trend in Denial-of-Service Angriffen wird seit Mitte 1999 beobachtet und hat Anfang 2000 (Februar) bei Angriffen auf Firmen wie Yahoo, eBay, Buy.com, Amazon, E-Trade, CNN und MSN für internationales Aufsehen gesorgt. Diese Attacken haben der E-Commerce-Branche definitiv das Fürchten gelehrt.

Die Tatsache, dass bei den Angriffen zum Teil Systeme mit enormen Bandbreiten (wie z.B Teilnehmer am Internet-2 mit über 100Mbps) beteiligt sein können und die Kommunikation der an den DDoS-Attacken beteiligten Rechnern (Agenten und Händler) bereits verschlüsselt verläuft (z.B CAST Algorithmus, 64Bit), spitzt die Angelegenheit nochmals zu.

Auf der anderen Seite haben die Systemadministratoren viel dazu gelernt, so ist es viel schwieriger geworden in die grossen Internetserver einzudringen und die entsprechenden DdoS-Agenten und -Händler zu installieren. Ausserdem werden in den Routern Filter eingesetzt, damit IP-Spoofing nicht mehr möglich wird, oder zumindest auf das darunterliegende Netz eingeschränkt wird.

Mit dem Aufkommen der Breitband-Anschlüsse für die grosse Masse mittels Kabel Modem und XDSL Anschlüssen steht der Internetgemeinde ein noch grösseres Problem bevor. Bei den meisten ungeschützen Computern von Privatanwendern ist es ein leichtes einen Agenten für eine DDoS-Attacke zu installieren.

## 1.3 Definition von DoS/DDoS

DoS-Attacken sind Angriffe, welche zum Ziel haben, den betroffenen Host lahm zu legen. Ein Rechner kann auf verschiedene Arten unerreichbar gemacht werden. Man bombardiert ihn mit Paketen, die seine Ressourcen völlig ausschöpfen und ihn sogar zum Absturz bringen können. Die Ressourcen eines Rechners sind die Prozessorleistung, Arbeitsspeicher oder die Bandbreite der Netzwerkanbindung. Bei einem solchen Angriff ist der Host so stark ausgelastet, dass es ihm nicht mehr möglich ist, seinen eigentlichen Aufgaben nachzugehen.
DDoS-Attacken sind DoS-Attacken, die von mehreren Standorten gleichzeitig ausgehen. Von DDoS spricht man ab ungefähr 50 beteiligten Angriffsrechner.

## 1.4 Denial of Service Attacken

### 1.4.1 Mail-Bombing

Einer der ältesten Denial of Service-Attacks ist das inzwischen »klassische« Mail-Bombing. Hierzu wird ein Empfänger mit einer Vielzahl von gleichlautenden eMails regelrecht bombadiert, so dass das nächste Herunterladen der vorhandenen eMails zur Qual werden dürfte. Die Ausführung erzeugt aber noch ein anderes Opfer:
Eine Mailbombe besteht im Prinzip aus einer einzigen eMail, die an einen SMTP-Mailserver zur Ausführung geschickt wird. Diese eMail hat jedoch die Besonderheit, dass sie die eMail-Adresse des Opfers gleich mehrmals als BCC-Empfänger enthält. Der ausführende Mailserver hat bei entsprechend hoher Angabe von BCC-Empfängern ebenfalls entsprechend genug zu tun, diese eMails zu generieren und zu versenden. Moderne Mailserver unterbinden diese Art von Mail-Bombing. Da immer das gleiche eMail vesendet wird, kann man es gut als Angriff identifizieren. Schwer zu erkennen sind Angriffe, welche die eMail-Inhalte zufällig erzeugen und die Absenderadressen abwechslungsweise aus einer Liste entnehmen. Der Nachteil für den Angreifer ist, dass  er jedes eMail einzeln versenden muss.
Eine sehr unangenehme Variante des Mail-Bombings ist die Anmeldung eines Opfers bei Unmengen von Mailinglisten. Das Opfer muss sich nämlich nach so einer Attacke mühsam aus allen angemeldeten Listen manuell wieder austragen.

### 1.4.2 Broadcast Storms

Broadcast Storms gehören ebenfalls schon zur älteren Generation von Denial of Service-Attacks. Sie richten besonders viel Schaden in lokalen Netzwerken an, in denen jeder Rechner als Gateway fungiert und die Netzwerktopologie nur mangelhaft gewartet wird.
An jeden Rechner wird bei einer Broadcast Storm-Attacke eine Flut an IP-Paketen geschickt, die allesamt an nichtexistierende Ziele adressiert sind. Wird dieser Datenstrom für mehrere Rechner innerhalb dieses Netzwerkes aufrechterhalten, ist das gesamte Netzwerk recht schnell stark überlastet, da die Rechner die falsch adressierten Pakete über die Gateways immer wieder in andere Subnetze verschieben.
Um die Problematik von Broadcast Storms zu vermeiden, ist eine ausgeklügelte und sorgfältige Planung des Netzwerks notwendig, um das »Hängenbleiben« von umherirrenden IP-Paketen von vorneherein zu verhindern bzw. in kürzester Zeit zu eliminieren. Heutzutage erleben Broadcast Storms leider wieder eine Renaissance, da immer mehr lokale Netzwerke an das Internet angebunden werden und dabei immer weniger auf die Sicherheit geachtet wird.

### 1.4.3 Smurf

Smurf-Attacken gehören zur Gruppe der Broadcast Storms, arbeiten aber auf eine etwas andere Weise. Bei einem Smurf Angriff sendet der Angreifer sehr viele ICMP-Pakete (z.B. Ping-Anfragen) an die Broadcast-Adresse eines Netzwerks, so dass dieses Paket von jedem Rechner innerhalb des Netzwerks empfangen wird. Der Angreifer tarnt sich jedoch nicht mit seiner eigenen oder einer nicht-existenten Adresse, sondern mit der Adresse des eigentlichen Opfers. Die ICMP-Anfragen werden nun um die Anzahl der Rechner im Netzwerk vervielfacht; das Netzwerk dient quasi als Sprungbrett. Ist das Netz korrekt konfiguriert, werden die ICMP-Antworten am Router des Netzwerks abgeblockt und gelangen nicht bis zum Rechner des Opfers. Erlaubt das Netz jedoch solche ICMP-Broadcasts gegen aussen, werden die multiplizierten ICMP-Antworten an das Opfer weitergeleitet. Dadurch können Angreifer mit geringer Leitungskapazität (Modem, BA-ISDN) Opfer mit breitbandigen Anschlüssen mit ICMP-Paketen überfluten. Die ICMP-Antworten belegen die gesamte Leitungskapazität und die reguläre Datenkommunikation wird unterbunden. Sehr häufig brechen auch die Server unter diesem Ansturm zusammen und müssen vorübergehend vom Netz getrennt werden.

Die Angreifer selbst sind nur sehr schwer zu identifizieren, da sie sich als das Opfer tarnen (IP-Spoofing). Die einzige sichere Abwehr ist, die Administratoren der als Sprungbrett dienenden Netzwerke über ihr Sicherheitsloch zu informieren und zu überzeugen, ihre Netze korrekt zu konfigurieren, um das Nach-Aussen-Leiten von Broadcastpings (ICMP) zu unterbinden.

### 1.4.4 Fraggle

Fraggle ist der Bruder von Smurf. Er funktioniert genau gleich, ausser dass er UDP-Echo-Pakete anstatt ICMP-Echo-Pakete versendet.

### 1.4.5 TCP Syn Flooding (Land Attacks)

Diese Attacke nutzt den Handshake-Mechanismus beim Aufbau einer TCP-Verbindung aus. Bevor eine Verbindung zwischen zwei Rechnern aufgebaut wird, sendet der Absender ein spezielles TCP-Pakete an den Empfänger, um eine Verbindung anzukündigen (SYN-Pakete, SYN = Synchronize). Der Empfänger sendet dann ein Antwort-Paket (SYN/ACK-Paket, ACK = Acknowledgement = Empfangsbestätigung) zurück an den Absender. Das SYN/ACK-Paket muss vom Initiant mit einem ACK-Paket bestätigt werden damit der Verbindungsaufbau komplett ist. Wenn der Absender eine falsche IP-Adresse benutzt, wird das SYN-ACK-Paket ins Nirgendwo geschickt und das Opfer sendet nach einem bestimmten Intervall die Quittung erneut, da er vom Verlust der Daten ausgeht. Nach einer bestimmten Zeit wird der Verbindungsaufbau abgebrochen. Während dieser Zeit wird Speicherplatz und Rechenleistung benötigt. Führt nun ein Absender eine TCP Syn Flooding-Attacke aus, sendet er nicht, wie vom Empfänger erwartet, ein ACK-Paket aus, sondern bombardiert den Empfänger weiterhin mit SYN-Paketen. Der Empfänger quittiert alle diese SYN-Pakete. Hier tritt nun der Fehler bei entsprechend fehlerhaften TCP-Implementierungen auf, die bei einem weiteren SYN-Paket nicht nur für das gerade empfangene SYN-Paket ein SYN/ACK-Paket verschickt, sondern auch für alle bisher empfangenen. Wenn die gefälschte IP-Adresse des Angreifers dazu nicht existiert , sendet der Router ein ICMP-Unreachable-Paket (Host/Netzwerk unerreichbar) zurück. Auf diese Weise wird auf dem Empfänger-Netzwerk schnell ein hoher Datenverkehr erzeugt und das Opfer ist nicht mehr erreichbar.

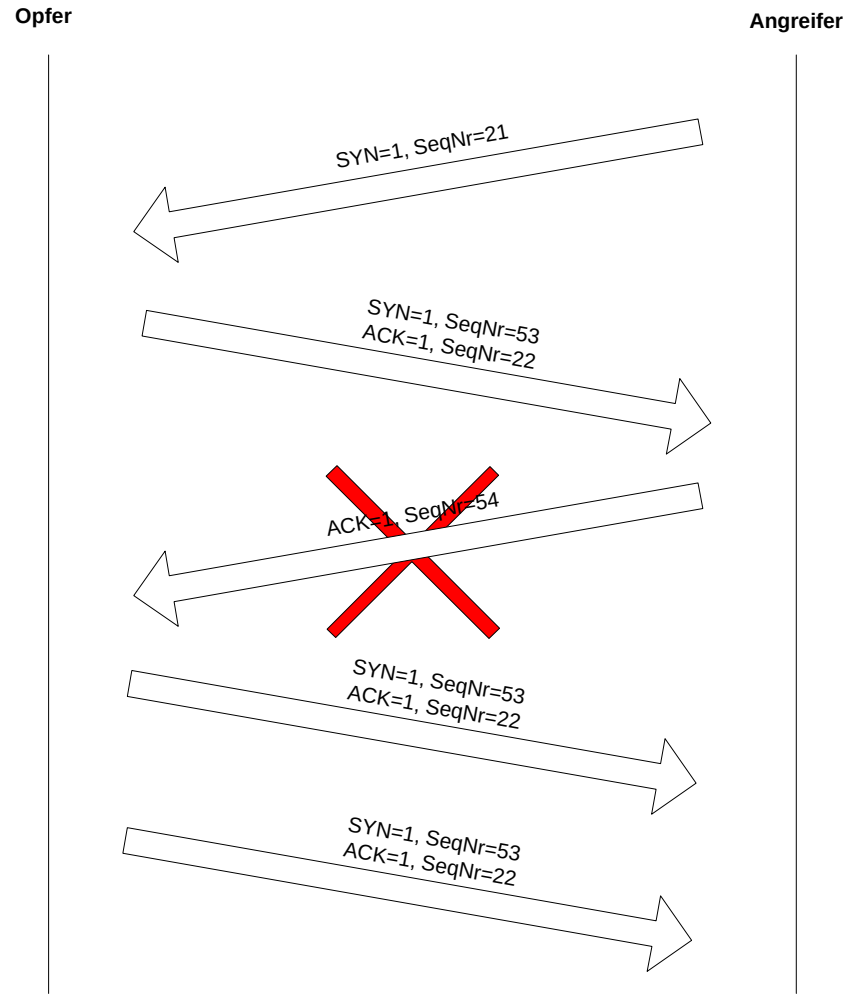


**Abbildung 1: TCP-Verbindungsaufbau**

### 1.4.6 Large Packet-Attacks (Ping of Death)

Ein besonders hinterhältiger Veteran der Denial of Service-Attacks sind die Large Packet-Attacks, auch bekannt unter Ping of Death.
Die Wirkungsweise von Large Packet-Attacks ist zugleich einfach und fatal. Das IP-Protokoll verpackt alle Daten beim Absender in 64 kB grosse Päckchen. Diese werden jedoch protokollintern vor der Übertragung in kleinere Päckchen zerlegt, um sie einfacher übertragen zu können (fragmentieren). Beim Empfängerrechner werden diese einzelnen Päckchen wieder zusammengefügt (reassemblieren), allerdings erst, wenn alle Einzelteile vorliegen. Ist das ankommende Paket am Ende grösser als 64 kB, läuft ein interner Speicherpuffer über und bringt im ungünstigsten Fall den Rechner zum Absturz.

### 1.4.7 Ping Flooding

Das Ping Flooding gehört zu den Denial of Service-Attacks, die keine Sicherheitslöcher ausnutzen. Pings werden benutzt, um die Erreichbarkeit von anderen Hosts im Netz zu prüfen. Ein angepingter Host quittiert hierzu einen Ping mit einer Echo-Antwort, einem Pong.

Beim Ping Flooding wird ein Host jedoch mit unzähligen Ping-Anfragen bombardiert, die der Host alle bearbeitet (falls keine entsprechenden Mechanismen die Abarbeitung von rasch wiederholenden Ping-Anfragen verhindert) und entsprechend das eigene System und die Netzverbindung auslastet.
Ping Flooding ist einer der Denial of Service-Attacken, die beim Opfer teuer werden können. Wird eine Netzverbindung eines Hostes nämlich nach dem erzeugten Datenaufkommen abgerechnet, können hohe Summen entstehen.

quelle: http://www.netplanet.org/sicherheit/

### 1.4.8 Ping-AT-Attacks

Der amerikanische Modemhersteller Hayes hat Ende der Siebzigerjahre eine einheitliche, zeilenorientierte und öffentliche Befehlssprache für Modems entwickelt, welche die sogenannten AT-Befehle enthält. Durch diese Befehle wird es möglich, dass jedes Modem angesprochen werden kann, in welches diese einheitliche Sprache implementiert wurde. Heute ist dies praktisch bei allen Modems der Fall, so dass jene Modems von den Betriebssystemen und der Software einheitlich angesprochen werden kann. Sobald sich ein Modem im Offline-Modus befindet, kann es über AT-Befehle angesprochen werden. Findet ein Wechsel in den Online-Modus statt, kann das Modem nicht mehr mittels der AT-Befehle angesprochen werden, da es sich im Übertragungsmodus befindet. Dies kann verhindert werden, indem man dem Modem die Zeichenkette des dreimaligen Drückens des Escape-Zeichens sendet, welches als "+++" gekennzeichnet wird. Dabei wird in den Kommandomodus gewechselt. Aus Sicherheitsgründen muss zwischen diesem Umschaltkommando in den Kommando-modus und den ersten AT-Befehl mindestens eine Pause von einer Sekunde vorhanden sein. Einige Modemhersteller verzichten aus patentrechtlichen Gründen auf eine solche Pause, so dass bei jenen Modellen der Umschaltbefehl in den Kommandomodus und ein kompletter AT-Befehl direkt hintereinander eingegeben werden können. Diese Voraussetzung eignet sich für einen gemeinen Angriff. Man schickt an einen Empfänger über das Internet ein spezielles Ping-Paket, welches zum Beispiel die Sequenz "+++ATH0" enthält, was das Umschalten in den Kommandomodus und Beenden der Verbindung bedeutet. Laut Ping-Protokoll antwortet der Rechner des Empfängers auf die Ping-Anfrage mit der Spiegelung des Paketes. Kennt das Modem nun die oben genannte Pause zwischen dem Umschalten und dem darauffolgenden AT-Paket nicht, wird es den Paketinhalt des Antwort-Pings als abzuarbeitende Sequenz interpretieren und die Verbindung trennen.

quelle: http://www.computec.ch/mruef/texte/dos.html

## 1.5 Wie funktionieren DDoS Angriffe

### 1.5.1 Grundprinzip eines Angriffs

Bevor ein Angreifer einen Distributed Denial of Service Angriff starten kann, muss ein mehrstufiges Netzwerk aus sogenannten Master- und Daemonsystemen aufgebaut werden. (Siehe Abbildung 2).

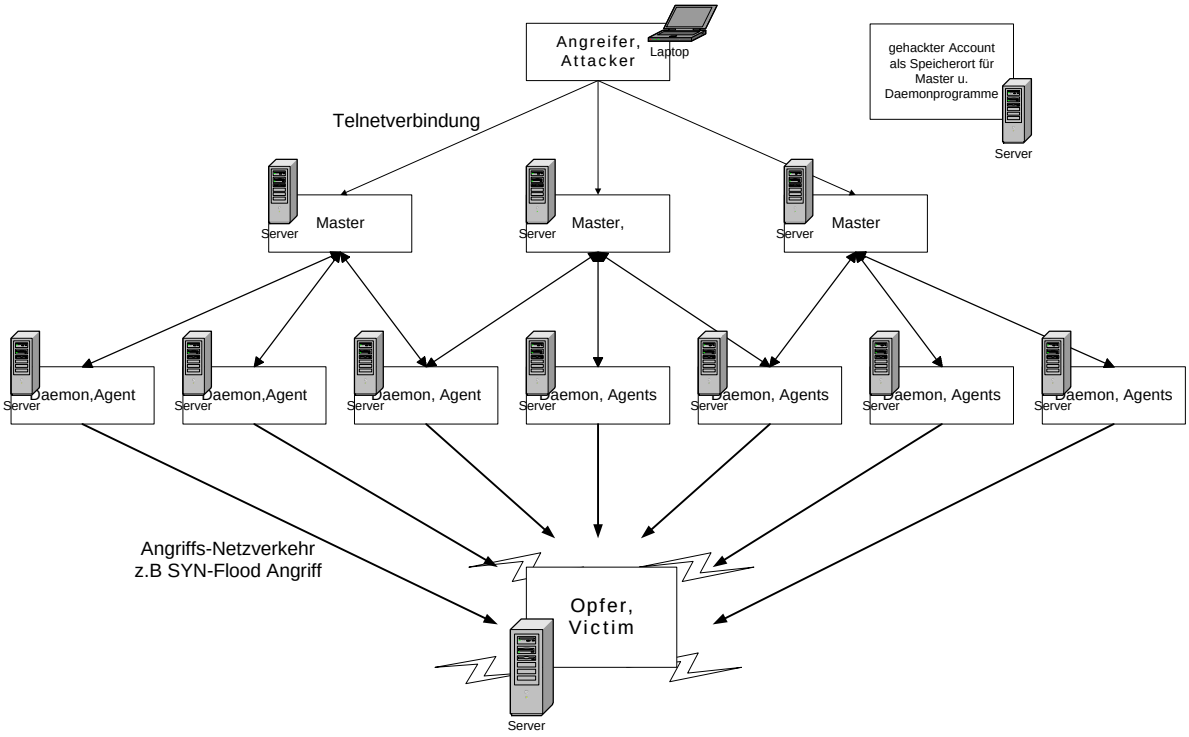


**Abbildung 2 : DDoS Angriffsszenario**

Zum Verständnis:

| | |
|---|---|
| Client | Eine Applikation die zum Initialisieren einer Attacke (beim Senden von Befehlen zu anderen Komponenten) gebraucht werden kann<br>(Vom Attacker gesteuert) |
| Server | Ein Server ist ein Prozess, der Dienste leistet und zur Verfügung stellt |
| Daemon | Linux / Unix Daemonen sind Prozesse die nicht an einen Benutzer oder Kontrollterminal gebunden sind. Sie erledigen im stillen Verwaltungsaufgaben und stellen Dienstleistungen zur Verfügung. (z.B. Koordinieren der DDoS Pakete, Netzdienste: inetd, sendmail) |
| Master | Ein Host, auf dem ein Client laeuft (Vom Angreifer gesteuert) |
| Agent | Ein Host, auf dem ein Daemon laeuft |
| Handler | Zweiter Client (nur bei Stacheldraht), der Client bei Stacheldraht übernimmt die Verschlüsselung. |

Hinweis: Bei den verschiedenen DDoS-Tools werden die einzelnen beteiligten Rechner nicht immer gleich bezeichnet.

Der Angreifer kommuniziert über eine Verbindung (z.B Telnet) mit den verteilten Mastern. An diese sendet er das Angriffskommando. Dieses Kommando besteht aus den Daten des Opfers (IP-Adresse, Portnummer, Angriffsart). Dies ist der einzige Verkehr der vom Angreifer aus geht. Danach übernehmen die Master die weitere Steuerung und Koordination des Angriffs. Jeder Master steuert eine bestimmte Anzahl an sogennanten Daemons. Damit beim Entdecken eines Masters durch einen Netzwerk-Sniffers nicht gerade alle Daemons unbrauchbar werden, teilen die Angreifer die Master in gut durchdachten Teilgebiete auf. Die Daemons befinden sich wieder auf anderen Systemen und können sich weit verstreut im Netz befinden. Erst die Daemonsysteme führen auf Anweisung des Masters den eigentlichen Angriff aus. Dies kann z.B eine SYN-Flood Attacke sein, bei der der Angreifer ein Paket zum Aufbau einer TCP-Verbindung (SYS-Pakete) an das Opfersystem sendet. Dieses reserviert einen Port und sendet ein sog. SYN-ACK Paket zurück. Da der Angreifer jedoch seine IP-Adresse gespooft hat, bekommt der Absender keine Bestätigung zurück . Das Opfersystem wiederholt und verwirft die reservierte Verbindung nach einem eingestellten Zeitraum entgültig. Unter Windows-NT dauert diese Zeit genau 189 Sekunden.

Wird dieser Verbindungsaufbau nicht nur einmal, sondern parallel sehr häufig ausgeführt, führt dies dazu, dass der Rechner anderweitig nicht mehr angesprochen werden kann.

### 1.5.2 Ein DDoS Angriffsszenario in 7 Schritten

Dieses Kapitel zeigt, wie das Netzwerk und der ganze DDoS Angriff aus Master- und Daemonsystemen aufgebaut wird. Dieser Aufbau erfolgt im Vorfeld, also bevor der eigentliche Angriff auf das Opfer erfolgt. Es ist möglich , dass auf vielen Systemen solche Master oder Daemons „schlummern“ und erst nach einigen Wochen aktiviert werden und einen Angriff durchführen.

**Schritt 1:** Account hacken
Ein potentieller Angreifer verschafft sich auf einem ans Internet angeschlossene Rechnersystem einen gestohlenen Account. Meistens handelt es sich dabei um ein System mit vielen Usern und hoher Bandbreite, um seine Anwesenheit zu verdecken.
Dieser Account dient als Speicher für Master- und Daemonprogramme und das Planen der Attacke. Ein Angreifer besitzt meistens mehrere solche Accounts, damit die Systeme redundant sind.

**Schritt 2:** Scanning
Im zweiten Schritt erfolgt das Scannen grosser Netzwerke zur Identifizierung potentieller Ziele. Dazu werden Scanning Tools auf den „gestohlenen“ Accounts benutzt. Mittels Internet Security Scanner werden Schwachstellen auf Servern gefunden um so an Root-rechte auf den Systemen zu gelangen. Der Angreifer prüft ausserdem welche Dienste und Ports auf dem System aktiv sind.
Unter Unix wurden Schwachstellen in den Remote-Procedure-Call (RPC) Diensten wie *cmsd*, *statd* oder *amd* benutzt.

**Schritt 3:** Rechner angreifen
Nachdem dem Angreifer bekannt ist, auf welchen Systemen welche Sicherheitslücken vorliegen, generiert der Angreifer ein Script, welches diese Sicherheitslücken angreift. Dabei werden z.T bekannte Tools genutzt, die diese Sicherheitslöcher automatisch ausnützt und vorher auf den gestohlenen Accounts abgelegt wurden.

**Schritt 4:** DDoS Netzwerkfestlegung
Im vierten Schritt legt der Angreifer seine späteren Daemon- und Mastersysteme fest. Auf den „gehackten“ Systeme werden weitere Speicher genutzt, um dort die „pre-compiled binaries“ der Daemons zu lagern.

**Schritt 5:** Automatische Installation
Im fünften Schritt erzeugt der Angreifer ein Script, welches die Liste der „in Besitz genommenen“ Rechner benutzt und ein weiteres Script erzeugt, das den Installationsprozess automatisiert als Hintergrundprozess durchführt. Diese Automatisierung erlaubt den Aufbau eines weit verbreitenden Denial-of-Service-Netzes ohne Wissen der eigentlichen Besitzer der Systeme. Auch für diese Installation existieren Tools, die der Angreifer nutzen kann

**Schritt 6:** Masterinstallation
Als letztes erfolgt die Installation der Masterprogramme. Dies wird meist „ von Hand „ und mit besonderer Sorgfalt durchgeführt, da die Masterprogramme eine Schlüsselrolle im Netzwerk des Angreifers besitzen. Optional wird ein „Rootkit“ installiert, welches zur Verdeckung der Anwesenheit der Programme, Dateien und Netzwerkverbindungen dient. Die Masterprogramme werden bevorzugt auf Primary-Name-Server-Hosts installiert. Auf solchen Systemen ist meist eine grosse Anzahl an Netzwerkverbindungen zu finden, da diese für einen extrem grossen Netzwerkverkehr ausgelegt sind. Dies verdeckt die Aktivitäten bez. den Netzwerkverkehr der Master sehr gut. Weiterhin werden solche Systeme selbst bei dem Verdacht auf Denial-of-

Service Aktivitäten nicht so schnell aus dem Netz genommen, da ihre Bedeutung für das eigene Netz zu gross ist.

**Schritt 7:** Der Angriff
Nun sind die Vorbereitungen für den DDoS-Angriff abgeschlossen und der Angriff auf das Opfer kann durchgeführt werden.

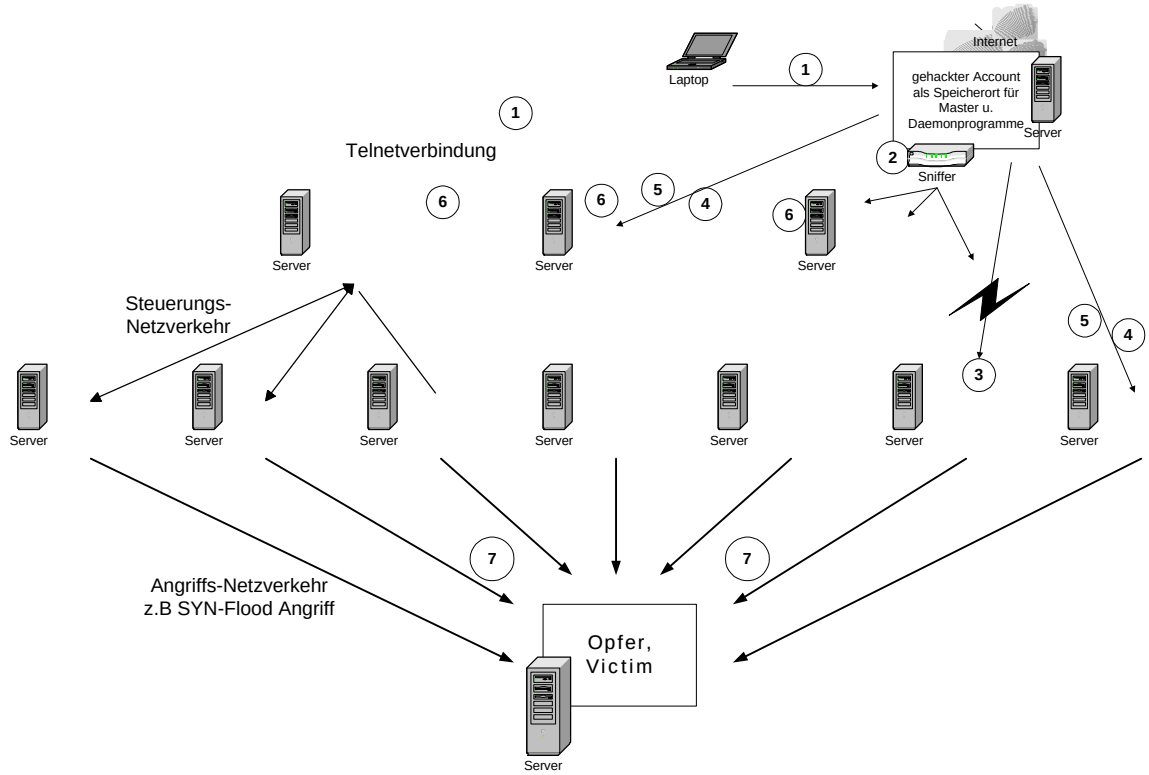


**Abbildung 3 : DDoS Angriffsszenario in 7 Schritten**

In der Beschreibung des Angriffsszenario wurde der Begriff Angriff nur im Zusammenhang mit dem Aufbau des Angriffs gebraucht und hat keinen Zusammenhang mit dem eigentlichen DDoS-Angriff.

## 1.6 Marktübersicht DDoS-Tools

Es existieren mittlerweile 6 Hauptbasen für Tools, die als Master- und Daemonsysteme fungieren. Sie unterscheiden sich durch grössere Änderungen in ihren Angriffsarten, ihrer Kommunikation oder andere zusätzliche Funktionen. Darüber hinaus gibt es eine Vielzahl weiterer Tools, die nur einige kleine Änderungen erhalten haben und im wesentlichen einem dieser Basistools entsprechen. Es besteht zudem die Möglichkeit, dass weitere neuartige Tools existieren, aber bisher noch nicht gefunden worden sind. Wie viele Systeme es im Internet gibt und wie viele schon verwendet wurden, lässt sich nur vermuten. In den folgenden Kapitel werden die wirkungsvollsten Tools beschrieben.

### 1.6.1 Trinoo

Der Angriff mit Trinoo erfolgt durch eine UDP-Flood-Attacke. Die Kommunikation zwischen Angreifer und Master erfolgt über eine TCP-Verbindung mit hoher Portnummer. Zwischen Master und Daemon, in beiden Richtungen, wird über eine UDP-Verbindung kommuniziert. Die Portnummern können leicht verändert werden und sind deshalb nicht immer gleich. Master und Daemon sind über ein Passwort geschützt und verhindern so die Übernahme durch andere. Das Passwort wird in Klartext übertragen und es besteht die Möglichkeit, ein Paket mit dem Passwort abzuhören. Dieser Nachteil wird bei anderen Tools durch verschlüsselte Passwortübertragung abgeschafft.

### 1.6.2 Trible Flood Network (TFN)

Mit TFN sind UDP-Flood-, TCP-SYN-Flood-, ICMP-Echo-Request- und ICMP-Broadcast-Storm-Attacken (smurf) möglich. TFN verfügt auch über die Möglichkeit, die IP-Adresse zu fälschen (IP-Spoofing). Die Kommunikation zwischen Angreifer und Master kann über verschiedene Remote-Shells erfolgen (TCP-, UDP-, oder ICMP-basierte Client/Server Shells). Zwischen Master und Daemon erfolgt die Kommunikation nur über ICMP-Echo-Reply-Pakete. Für den Master ist kein Passwort nötig, es braucht nur die Liste der Daemons.

### 1.6.3 TFN2K

TFN2K ist eine Erweiterung des TFN. Es wählt die Verbindungsart automatisch aus und verschlüsselt sie mit einem CAST-256 Algorithmus. Die Befehle werden hier nicht stringbasiert, sondern in der Form "+<id>+<data>" übertragen. Id ist der Befehl und ein Byte lang. Data sind die zugehörigen Parameter.

quelle: http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt

### 1.6.4 Stacheldraht

Stacheldraht besitzt die gleichen Angriffsmöglichkeiten wie TFN. Neu ist die verschlüsselte Kommunikationsverbindung. Somit ist ein Session hijacking (Übernahme einer Verbindung) nicht mehr möglich. Die Verbindung zwischen Angreifer und Master erfolgt über eine Telnet ähnliche Verbindung, welche durch einen Passwortsatz gesichert und verschlüsselt ist. Die Kommunikation zwischen Master und Daemon ist mittels Blowfish (symmetrischer Verschlüsselungsalgorithmus) verschlüsselt. Der Master kommuniziert mit dem Daemon über eine TCP-Verbindung, im Gegensatz sendet der Daemon seine Nachrichten als ICMP-Echo-Reply-Pakete. Zusätzlich können die Daemons automatisch aktualisiert werden.
Stacheldraht läuft nur auf Solaris und Linux, hat aber eine weitere Finesse eingebaut: Über einen Befehl kann der Master auf allen bereits infizierten Rechnern eine neue Version des

Clients installieren. Neuen Funktionen und Tarnmöglichkeiten sind so praktisch keine Grenzen mehr gesetzt.

quelle: http://www.etdv.ruhr-uni-bochum.de/dv/lehre/seminar/

### 1.6.5 Shaft

Die Kommunikation ist bei Shaft gleich wie bei Trinoo. Angreifer zu Master Kommunikation über TCP und Master zu Daemon Kommunikation und umgekehrt über UDP. Der Angreifer kontaktiert den Master über einen Telnetclient und loggt sich mit einem Passwort ein. Die Daten werden somit im Klartext übertragen. Shaft kann UDP-, TCP- und ICMP-Attacken einzeln oder in Kombination durchführen.

Quelle: http://www.royans.net/insync/ddos/bugtraq_ddos3.shtml

### 1.6.6 Mstream

Die Kommunikation zwischen Master und Daemon erfolgt über UDP. Der Angreifer meldet sich über TCP beim Master. Die Daten zwischen den einzelnen Komponenten werden nicht verschlüsselt. Mstream verfügt über TCP-SYN-Attacken, welche die Angriff-Ports jedesmal zufällig auswählt.

Quelle: http://packetstorm.securify.com/advisories/iss/iss.00-05-02.mstream

## 1.7 DDoS in Zahlen und Fakten

| Jahr | Name | Besonderheit |
|---|---|---|
| Herbst 1996 | SYN-Flooding | SYN-Flooding: TCP-Verbindungen, "Three-Way-Handshake" , SYN-Paket, Handshake, eine falsche Absenderadresse; Der Trick beim SYN-Flooding besteht darin, diese Zeit bis zum Abbruch (Timeout) damit zu nutzen, das Opfer mit SYN-Paketen zu fluten |
| Oktober 1997 | SMURF | Ping auf Broadcastadresse mit IP-Spoofing; Das Problem war unter dem Namen ICMP Storm schon länger bekannt, seit Oktober 1997 gab es dann aber das einfach zu bedienende Tool SMURF |
| Anfang 1997 | Ping of Death | Der Ping of Death war die erste Attacke, mit der man ein Opfer mit einem einzigen Schuß erledigen konnte: "Ping -l 65510 astalavista.com". Funktioniert heute nicht mehr |
| 7.Mai.1997 | OOB-Angriff (Out of Band) | OOB-Angriff: NetBios Port 139; Das erste OOB-Tool war WinNuke und erblickte am 7.Mai.1997 die Welt. Durch das IRC fand WinNuke sehr schnell Verbreitung. Selbst Anfang 1998 konnte man noch DAU's abschießen, jedoch haben die OOB-Attacken zunehmend Ihre Bedeutung verloren, da Win98 gegen solche Angriffe gefeilt ist. |
| Ende 1997 | Land | Land: SYN DoS-Attacke Eine Besonderheit von Land ware jedoch, daß die weit verbreiteten und oft an zentralen Knotenpunken der Netze installierten CISCO-Router von dem Tool betroffen waren |
| 1988 | Morris-Wurm | Die erste bedeutende Denial-of-Service-Attacke war der Morris-Wurm. Schätzungen zufolge waren etwa 5.000 Rechner für einige Stunden betriebsunfähig. Zu jener Zeit (1988) war es eine Katastrophe für akademische- und Forschungseinrichtungen, hatte aber nur wenig Auswirkung auf den Rest der Welt. Heutzutage könnte eine vergleichbare DoS- Attacke Verluste in Millionenhöhe nach sich ziehen. |
| | | |