DoS – Attacken

Thomas Perteneder

27. Mai 2014

Zusammenfassung

In dieser Mini-Seminararbeit werden grundlegende Konzepte von Denial-of-Service (DoS) und Distributed-Denial-of-Service (DDoS) Attacken beschrieben, Motive und Hintergründe weshalb diese durchgeführt werden beleuchtet und fundamentale Techniken der Abwehr diskutiert.

1 Einführung

Die Einführung des Internet und seinem meist genutztem Dienst, dem WWW (World-Wide-Web), revolutionierte die Computerwelt. Durch die hochgradige Vernetzung von Computersystemen auf der ganzen Welt, wurden ungeahnte Möglichkeiten der Kommunikation und des Informationsaustausches geschaffen. Bezogen auf die Sicherheit von Computersystemen stellt der ungehinderte und anonyme Datenfluss jedoch eine große Bedrohung dar und genau dort setzen die sogenannten DoS-Attacken an. DoS-Attacken sind der Netzwerkgemeinde schon seit den 1980er bekannt, wobei mit der Geburt des Internet dieser Art des Angriffs völlig neue Möglichkeiten eröffnet wurden. DoS (*Denial-of-Service*) Angriffe zielen darauf ab, einen verfügbaren Service (Dienst), wie etwa eine herkömmliche Webseite oder einen Onlineserver so zu beeinträchtigen, dass dessen Nutzung für legitime User nur noch sehr eingeschränkt oder gar nicht mehr möglich ist. Man spricht von einem Denial-of-Service (DoS), da der Zugriff auf eine ansonsten verfügbare Ressource verweigert („denied“) wird. Ist diese Überlastung des Systems mutwillig provoziert worden, so spricht man von einer DoS-Attacke. Sind mehrere Benutzer oder ein ganzes Botnetz [1] involviert, wird dies als DDoS-Attacke (*Distributed-Denial-of-Service*) bezeichnet.

2 Hintergründe

Die Motive für DoS-Attacken und DDoS-Attacken sind vielfältig und reichen von politischem Protest über Cyberwar und Hacktivismus bis hin zu organisierter Kriminalität [4]. So wurden in der Vergangenheit DoS-Attacken eingesetzt, um Webseiten von Politkern

[1] Netzwerk an korrumpierten Devices (Bots) unter Kontrolle des Angreifers

unerreichbar zu machen, wie etwa die des georgischen Präsidenten Micheil Saakaschwili [2]. Und auch die Internetbewegung Anonymous setzt DoS-Techniken gezielt im Rahmen ihrer Protestaktionen ein. So auch im Jahr 2012, als namhafte Zahlungsinstitute wie MasterCard, Postfinance und PayPal als Reaktion auf die Sperrung von Wikileaks Konten angegriffen wurden [3]. Besonders im Bereich des computergestützten Protestes, dem sogenannten Hacktivismus, gewinnen DoS-Attacken an Bedeutung, da sie aufgrund vieler kostenlos verfügbarer Tools wie etwa der LOIC (Low-Orbit-Ion-Cannon), einer Open-Source Software um Lasttests für Netzwerkanwendungen zu generieren, auch ohne Expertise durchführbar sind.

3 Typen

3.1 DoS – Denial of Service

DoS-Attacken sind dadurch gekennzeichnet, dass ein Angreifer ganz gezielt bestimmte Ressourcen eines Systems (Internetzugang, Netzwerkverbindungen, Betriebssystemressourcen, ...) blockiert. Zwei grundlegende Techniken sind das SYN-Flooding und die Smurf-Attacke .

- *SYN-Flooding*: Bei dieser Attacke beutet der Angreifer eine Schwäche des Transmission-Control-Protocol (TCP), den sogenannten Dreiwege-Handshake, aus, um Dienste oder Rechner in einem Netzwerk vorübergehend unerreichbar zu machen. Ein böswilliger Angreifer sendet dabei zahlreiche SYN-Anfragen (synchronize/start), unterschlägt dem Server jedoch das abschließende ACK (acknowledge). Dies führt zu zahlreichen halboffenen Verbindungen, die im Speicher des Netzwerkstacks gehalten werden und Ressourcen verbrauchen. In Abbildung 1 ist der Ablauf schematisch dargestellt. Werden alle Ressourcen durch Flutung mit SYN-Anfragen aufgebraucht, können keine neuen Anfragen verarbeitet werden und es kommt zur Dienstverweigerung (DoS). [3]

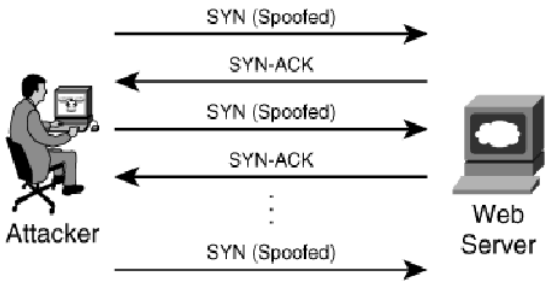

Abbildung 1: SYN-Flood Attacke [1]

[2] http://www.spiegel.de/netzwelt/web/hack-attacke-auf-georgien-ehrenamtliche-angriffe-a-572033.html
[3] http://www.n24.de/n24/Nachrichten/Politik/d/1168136/-wikileaks-gegner--von-hackern-bombardiert.html

- *Smurf-Angriff*: Im Gegensatz zum SYN-Flooding werden bei dieser Attacke sogenannte Ping-Pakete an eine Broadcast-Adresse eines Netzwerks gesendet. Diese ICMP-Pakete des Typs Echo-Request (*ping*) müssen von den Hosts sofern sie das Protokoll unterstützen mit ICMP Echo-Reply (*pong*) beantwortet werden. Zusätzlich wird mit Hilfe von IP-Spoofing (Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse) das Opfer als Absender der Pakete eingetragen. Im Zielnetz wird die Broadcast-Anfrage nun an alle Geräte im lokalen Netzwerk weitergeleitet. In Abhängigkeit der Anzahl an Clients ergibt sich ein enormer Antwortstrom, der auf das Opfer gerichtet wird. In Abbildung 2 schematisch dargestellt. Angriffe dieser Art gehören zur Gruppe der *Amplifier-Attacken*, da mit nur einem ICMP-Paket eine Flut an Antworten generiert werden kann. Der Angreifer wird damit befähigt seine eigene Bandbreite um ein Vielfaches verstärkt auf ein Opfer richten zu können. Rechnernetze, die gerichtete Broadcast-Anfragen lokal weiterleiten werden als sogenannte *Smurf-Amplifier* bezeichnet. [2]

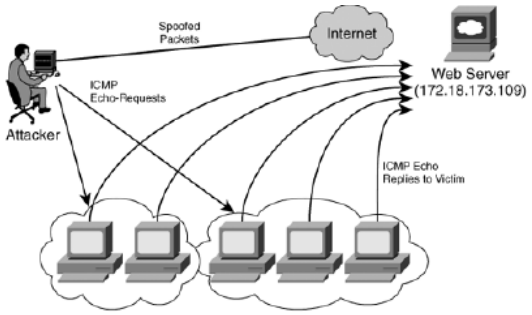

Abbildung 2: Smurf-Attacke [1]

3.2 DDos – Distributed Denial of Service

DDoS-Attacken, also verteilte Denial-of-Service Angriffe, werden von zahlreichen Angreifern simultan ausgeführt. Dabei kommt ein sogenanntes Botnetzwerk zum Einsatz. Ein Botnetz stellt ein Netzwerk an korrumpierten Devices (*Bots*) dar, deren Ressourcen vom Betreiber (*Master*) eines Botnetzes genutzt werden können. Zwischen Bots und Master stehen die sogenannten *Handler*, welche eine Kommunikation zwischen Master und Bots ermöglichen. Welche Funktionalität die Bots dem Master zur Verfügung stellen, hängt von der Malware ab, mit welcher ein Device infiziert wurde. D.h. Botnetze können unterschiedliche Funktionalitäten zur Verfügung stellen und sind somit nicht auf die Ausführung von DDos-Attacken limitiert. [4]

Mit Hilfe von Botnetzen lassen sich die angeführten DoS-Attacken (siehe Abschnitt 3.1) in vielfach verstärkter Form realisieren, indem alle Bots gleichzeitig angreifen. Eine weitere sehr verheerende DDoS-Technik, die enorme Datenflut generieren kann, ist die DNS Amplification Attacke.

- *DNS Amplification Attacke*: Bei dieser Form des Angriffs wird ein DNS (Domain Name Server) dazu missbraucht, um ein Opfer mit großen Datenströmen zu überfluten. Da-

bei bedient man sich der Tatsache, dass Nameserver auf kurze Anfragepakete (queries) mit sehr langen Antwortpaketen antworten können und erreicht damit eine vielfache Vergrößerung der Datenmenge. Durchgeführt wird der Angriff indem mit Hilfe eines Botnetzes, welches der Angreifer unter seiner Kontrolle hat, zahlreiche Anfragen an einen DNS gesendet werden und dessen Antworten mit Hilfe von IP-Spoofing an das Opfer umgelenkt werden. Als Verstärkungsserver werden häufig offene Resolver verwendet, also DNS, welche nicht auf Anfragen mit bestimmter Quelladresse beschränkt sind. Aufgrund der Anonymisierung mittels IP-Spoofing lässt sich der Angriff sehr schwer zurückverfolgen, da nur die IP-Adresse des Nameserver sichtbar ist. [1]

4 Gegenmaßnahmen

So vielfältig die Techniken des Angriffs, so auch die der Verteidigung. Nachfolgend ein kurzer Überblick an grundlegenden Konzepten.

- *SYN-Cookies*: Werden verwendet um SYN-Flood Angriffe zu neutralisieren. Diese nutzen eine Schwäche des TCP-Protokolls und generieren zahlreiche offene Serververbindungen, für die Ressourcen gebraucht werden. SYN-Cookies erweitern das TCP-Protokoll, sodass zusätzliche Informationen kodiert werden können, die ansonsten im Netzwerkstack abgelegt werden müssten. Somit wird verhindert, dass halboffene Verbindungen Ressourcen verschlingen können. [1]
- *Ingress/Egress Filterung*: Diese Technik wird angewandt, um gespoofte Pakete, also Pakete mit gefälschter IP-Adresse, die bei DoS und DDoS Attacken zum Einsatz kommen, herauszufiltern. [4]
- *D-WARD*: Jene Methode basiert auf Monitoring des aktuellen Datenverkehrs. Die erhobenen Werte werden mit vordefinierten Flow-Modellen abgeglichen. Bei nicht Übereinstimmung werden die abnormalen Datenströme gefiltert. [4]

Literaturverzeichnis

[1] Muhammad Aamir und Mustafa Ali Zaidi. „DDoS Attack and Defense: Review of Some Traditional and Current Techniques“. In: *CoRR* abs/1401.6317 (2014).

[2] F. Lau u. a. „Distributed denial of service attacks“. In: *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*. Bd. 3. 2000, 2275–2280 vol.3. DOI: 10.1109/ICSMC.2000.886455.

[3] R.R. Rejimol Robinson und C. Thomas. „Evaluation of mitigation methods for distributed denial of service attacks“. In: *Industrial Electronics and Applications (ICIEA), 2012 7th IEEE Conference on*. 2012, S. 713–718. DOI: 10.1109/ICIEA.2012.6360818.

[4] Saman Taghavi Zargar, James Joshi und David Tipper. „A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks“. In: *IEEE Communications Surveys and Tutorials* 15.4 (2013), S. 2046–2069.