Übungszettel 7

Gruppe 7
Jan Wolfram
Andreas Diesendorf
Artur Siubiak

Aufgabe 1

(1)

Bei einer TCP-Verbindung zwischen Client und Server, führt der Client
und der Server einen Threeway-Handshake durch um die Verbindung einzurichten.

Ablauf:

Client an Server: Paket mit Flag SYN, Abgleichen (synchronize).
Server an Client: Paket mit Flags SYN, ACK, Abgleichen bestätigt (synchronize acknowledge).
Client an Server: Paket mit Flag ACK, Bestätigt (acknowledge); Die Verbindung ist nun hergestellt.

Ein böswilliger Client kann die letzte ACK-Nachricht unterschlagen.
Dabei wartet der Server einige Zeit auf ein entsprechendes Paket, welches durch
Verzögerung erst später ankommen kann.

Während dieser Zeit werden sowohl die Adresse des Clients als auch der Status der noch
halb offenen Verbindung im Speicher des Netzwerkstacks vorrätig gehalten, um die
Verbindung später vollständig etablieren zu können.

Diese halb offene Verbindung belegt bei allen Betriebssystemen Ressourcen auf dem Server.
Ressourcen sind immer begrenzt. So kann es durch Flutung des Servers mit SYN-Nachrichten
dazu kommen, dass alle Ressourcen aufgebraucht sind.
Falls dies der Fall ist, können zum Server keine neuen Verbindungen aufgebaut werden. Dies
führt zur Zugriffsverweigerung (Denial of Service).

Bei diesem Angriff braucht der Verteidiger mehr Ressourcen zur Verteidigung als der
Angreifer zum Angriff.

(2)

Verfügbarkeit: Die Verfügbarkeit gestalltet sich schwierig durch SYN-Flooding, da der Angriff
die Kommunikation beeinträchtigt. Dadurch das der Angriiff den Server fast komplett beschäftigt
ist die Kommunikation fast unmöglich. Man hat so keinen Zugriff auf seine Daten.

Intergität: Wird nicht angegriffen

Vertraulichkeit: Wird nicht angegriffen

(3)
Der SYN-Cookies-Mechanismus

Die SYN-Cookies sind ein Fallback-Mechanismus, wenn die Backlog-Queue voll ist. Sie
erfordern keine Anpassungen bei den Clients, aus deren Sicht der Server weiterhin
normal antwortet.

Dabei speichert der Server keinerlei Informationen über ein SYN-Paket, sondern sendet
diese als Crypto-Cookie an den Client. Falls dieser nicht antwortet, hat der Server nur
kurze Rechenzeit investiert. Antwortet der Client, kommt das Cookie wieder und der Server
kann anhand der darin enthaltenden Informationen feststellen, dass er bereits mit diesem
Client kommuniziert hat. So stellt dann der Server die Verbindung her, auch ohne dass er
einen Eintrag in der Backlog-Queue dazu vorfindet.

Der Server verwendet seine Sequenznummer, die er sonst pseudozufällig erzeugt als Cookie.
Mit SYN-Cookies erstellt er aus Quell- und Ziel-Ports, den zugehörigen
IP-Adressen und einem Geheimnis einen MD5-Hash und schickt diesen als erste Sequenznummer

an den Client.

Kommt die Antwort, um den Dreiwege-Handshake zu komplettieren, enthält diese eine Bestätigung der Sequenznummer (ACK). Der Server bildet wiederum den MD5-Hash über das Geheimnis und die Adressen und Ports des ACK-Pakets und vergleicht diesen Wert mit der vom Client bestätigten Sequenznummer. Stimmen die beiden überein, weiss der Server, dass der Client das Cookie von ihm haben muss und stellt die Verbindung her.

(4)

/proc/sys/net/ipv4/tcp_synack_retries:

Anzahl der SYNACKs für einen passiven TCP-Verbindungsversuch die erneut übertragen werden. Sollte nicht höher als 255 sein. Standardwert ist 5, was 31 Sekunden bis zur letzten erneuten Übertragung entspricht mit der aktuellen anfänglichen RTO von 1 Sekunde. Damit ist die letzte Auszeit die für eine passive TCP-Verbindung passieren wird nach 63 Sekunden.

/proc/sys/net/ipv4/tcp_max_syn_backlog:

Maximale Anzahl von gespeicherten Verbindungsanfragen (SYN_RECV), die keine Bestätigung vom verbindenden Client erhalten haben.
Dies ist eine Beschränkung pro Hörer.
Der Mindestwert ist 128 für Computer mit geringem Arbeitsspeicher
Zunahme im Verhältnis zum Speicher der Maschine.
Wenn der Server überlastet ist, erhöhen Sie diese Zahl.

/proc/sys/net/ipv4/tcp_syncookies:

Nur gültig, wenn der Kernel mit CONFIG_SYN_COOKIES kompiliert wurde
Sendet Syncookies aus, wenn die Syn-Backlog-Warteschlange eines Sockets überläuft. Dies soll vor dem häufigen "SYN-Flood-Angriff" schützen
Voreinstellung: 1

Syncookies ist Fallback-Funktion.
Wenn Sie SYN-Flutwarnungen sehen
in Ihren Protokollen, aber die Untersuchung zeigt, dass sie auftreten
wegen überlastung mit legalen verbindungen, solltest du
weitere Parameter abstimmen bis diese Warnung verschwindet.

Wenn man testen möchten, welche Effekte Syncookies auf die Netzwerkverbindung haben, können Sie diesen Regler auf 2 stellen um Bedingungslose Erzeugung von Syncookies zu Aktivieren.

(5)
/proc/sys/net/ipv4/tcp_synack_retries: 5

/proc/sys/net/ipv4/tcp_max_syn_backlog: 256

/proc/sys/net/ipv4/tcp_syncookies: 1

(6)
/proc/sys/net/ipv4/tcp_synack_retries: 1(niedrig lassen)

/proc/sys/net/ipv4/tcp_max_syn_backlog: 256: hoch lassen

/proc/sys/net/ipv4/tcp_syncookies: auf 2 stellen

Aufgabe 3

1)

Router 1:

Ziel	Weg zum Ziel
Default	IP vom Router via Netzwerkkarte 1 (10.168.100.3)
50.18.160.101	Netzwerkkarte 2 (50.18.120.99)

Router 1:

Ziel	Weg zum Ziel
Default	IP vom Router via Netzwerkkarte 1 (10.168.100.3)
50.18.120.100	Netzwerkkarte 2 (50.18.120.99)

Router 2:

Ziel	Weg zum Ziel
Eigene IP/Subnetz	Netzwerkkarte 1 (15.145.101.1)