



Università
degli Studi
della Campania
Luigi Vanvitelli

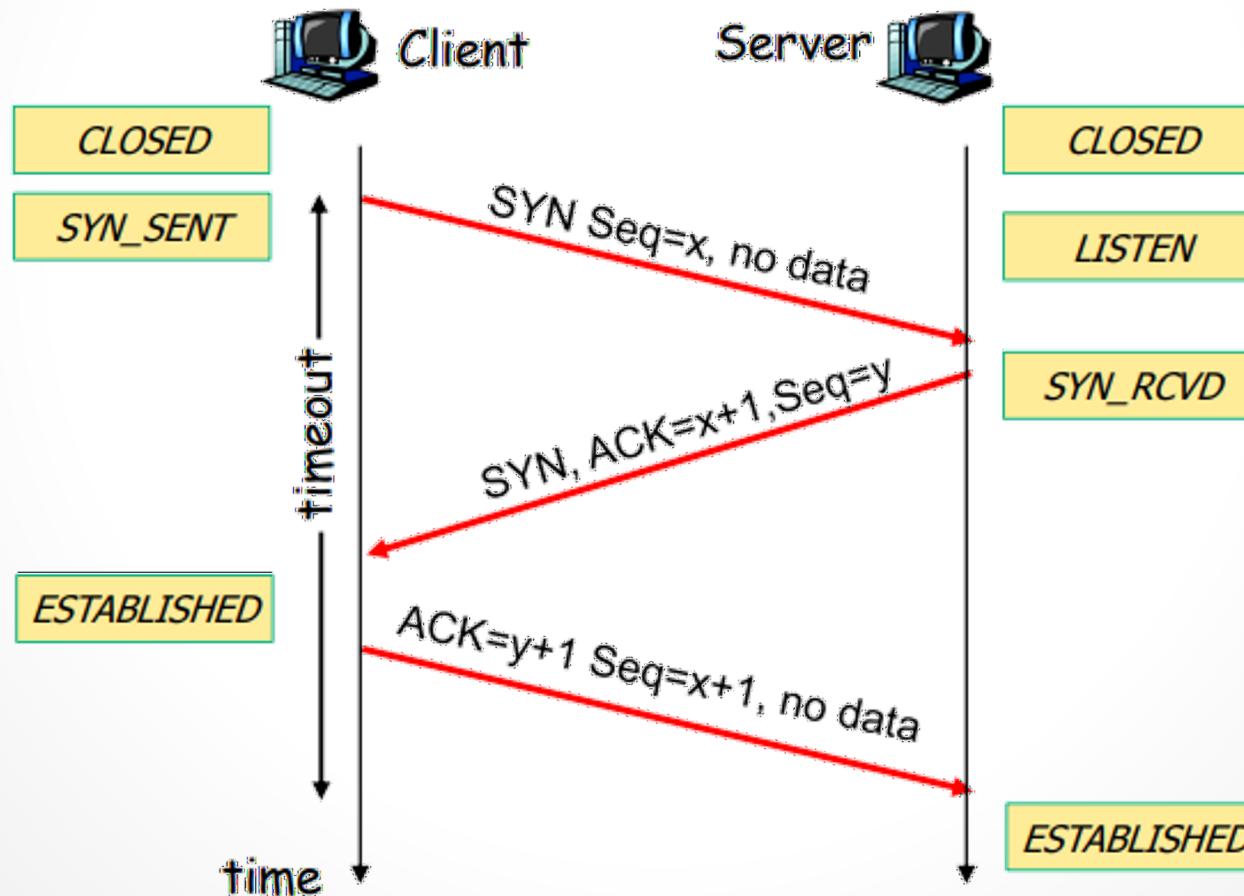
Reti di Calcolatori e Cybersecurity

TCP – Syn Flood

Ing. Vincenzo Abate

TCP avvio connessione

- 3 way-handshake
- Il client prende l'iniziativa inviando il primo segmento



TCP avvio connessione

Il three-way handshake serve a questo:

Il client invia un pacchetto SYN al server.- “Ciao, vorrei configurare una connessione con voi.”

Il server risponde con un pacchetto SYN/ACK e prepara una struttura di dati chiamata “Transmission Control Block” (TCB) per la connessione nel backlog del SYN.- “OK, con piacere. Ti prego di usare i seguenti parametri di connessione.”

Il client risponde al pacchetto SYN/ACK con un pacchetto ACK e finisce in questo modo l’handshake.

Da questo momento in poi la connessione è pronta e i dati possono essere inviati in entrambe le direzioni. Da parte del server, il Transmission Control Block verrà rimosso dal backlog del SYN.- “Fantastico, grazie. Andiamo!”

↓ Quello che ha memorizzato a connessione stabilita non serve più. Quello serve a tenerla in memoria
per un po'.

TCP Syn Flood

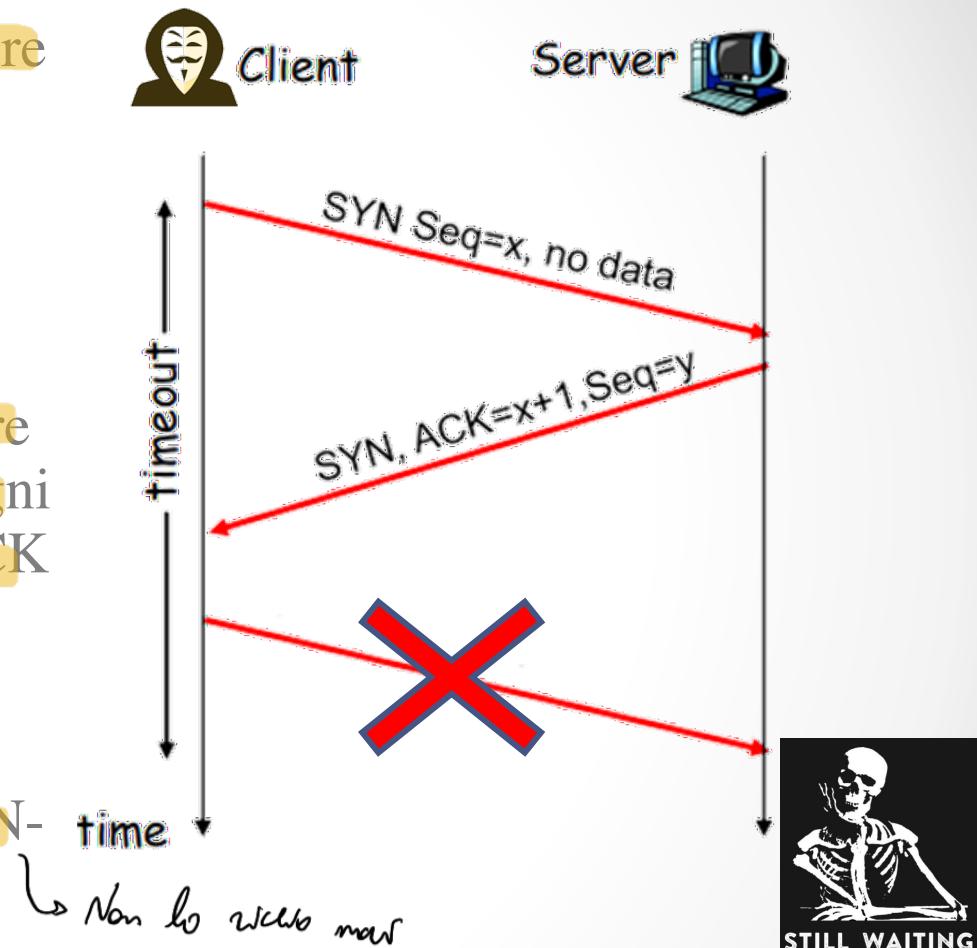
- TCP SYN flood è un tipo di attacco DDoS (Distributed Denial of Service) che sfrutta parte del three-way handshake TCP per consumare risorse sul server target e renderlo non reattivo.
- Essenzialmente, con i DDoS SYN flood, l'autore dell'attacco invia le richieste di connessione TCP più velocemente di quanto il computer target le possa elaborare (possa farle decadere), causando la saturazione della rete.

Idea: fino a quando non mando ACK 3°, server ha tempo salvare su chet nella Transmission Control Block
⇒ Salvo al TCB. Le richieste che non si chiudono sono di più di quelle che posso arrivare.

TCP Syn Flood

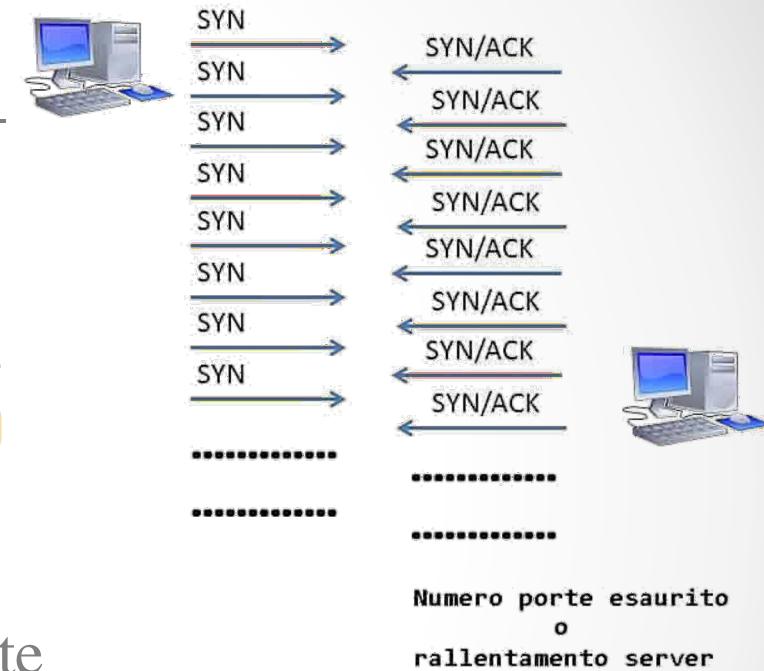
In un attacco SYN flood, l'aggressore invia pacchetti SYN ripetuti a ogni porta del server mirato, spesso utilizzando un indirizzo IP falso. Il server, inconsapevole dell'attacco, riceve richieste multiple, apparentemente legittime, di stabilire una comunicazione. Risponde ad ogni tentativo con un pacchetto SYN-ACK da ogni porta aperta.

Il client malevolo non invia l'ACK previsto oppure, se l'indirizzo IP è stato spoofed, non riceve mai il SYN-ACK. In entrambi i casi, il server sotto attacco aspetterà per qualche tempo la conferma del suo pacchetto SYN-ACK.



TCP Syn Flood

Un server sotto un attacco di SYN flood continuerà ad attendere un pacchetto SYN-ACK per ogni richiesta di connessione, poiché il ritardo potrebbe essere normale e legato alla congestione della rete. Tuttavia, poiché un pacchetto SYN-ACK non arriva mai per nessuna delle richieste di connessione; il numero massiccio di connessioni semiaperte riempie rapidamente la tabella TCB del server prima che possa effettuare qualsiasi connessione. Questo processo continua per tutto il tempo in cui continua l'attacco di flood.



TCP Syn Flood

I principali modi in cui avvengono gli attacchi di tipo SYN flood sono

Attacco diretto In questo tipo di attacco, l'attaccante invia richieste SYN multiple e in rapida successione, senza neanche nascondere il suo indirizzo IP.

Attacco distribuito L'attacco distribuito (Distributed direct attacks) è un tipo di attacco che permette all'attaccante di utilizzare non più una singola macchina, ma fare affidamento a N macchine. Questo permette ad ogni singola macchina di sferrare un attacco diretto ricorrendo anche alla tecnica dello spoofing, con conseguente difficoltà da parte della vittima di difendersi da vari attacchi SYN flood. Al giorno d'oggi questi attacchi sono possibili poiché esistono reti di molte macchine, le cosiddette Botnet, che permettono ai vari cyber criminali di sferrare attacchi senza esser riconosciuti.

Spoofing attack un utente malintenzionato può anche contraffare l'indirizzo IP in ciascun pacchetto SYN inviato per inibire gli sforzi di mitigazione e rendere più difficile la propria identificazione. Pur potendo essere contraffatti, tali pacchetti possono essere eventualmente ricondotti alla loro origine. Svolgere questo tipo di indagine è difficile ma non impossibile, soprattutto se i provider di servizi Internet (ISP) sono disposti a collaborare..

TCP Syn Flood

Contromisure possibili:

- Aumentare la capacità del backlog del SYN
- Far cadere le connessioni in entrata se l'IP effettua più di N connessioni alla porta XXX entro tot secondi
- Bloccare pacchetti Bogus
- SYN cache e SYN cookie

→ comprendiamo le informazioni e salvo solo l'hash dei determinati parametri

SYN cache e SYN Cookie

L'idea alla base di una **SYN cache** è semplice: invece di salvare un **Transmission Control Block** (TBC) completo nel backlog del SYN per ogni connessione semi-aperta, si mantiene soltanto un TBC minimo. Questa tecnica utilizza una funzione hash per impedire all'aggressore di indovinare le informazioni crittografiche della connessione. La SYN cache si è rivelata una tecnica efficace.

L'invenzione dei **SYN cookies** nel 1996 ha permesso di sviluppare ulteriormente il concetto di **SYN cache**. Qui si rinuncia del tutto all'utilizzo del **Transmission Control Block** come struttura di dati. Al suo posto si codificano i parametri rilevanti di connessione nella sequenza numerica del pacchetto SYN/ACK. La funzione crittografica di hash garantisce che l'aggressore non riesca a indovinare facilmente la sequenza numerica. Un client legittimo risponde al pacchetto SYN/ACK con un pacchetto ACK e ricorre a una sequenza numerica particolare. Il server utilizza la sequenza numerica del pacchetto ACK per verificare la crittografia della connessione e stabilire la connessione. L'utilizzo di **SYN cookies** rappresenta una protezione efficace da attacchi SYN flood. In casi particolari, però, può portare a una riduzione delle prestazioni. Entrambe le tecniche sono utilizzate anche in combinazione. Normalmente si usa la **SYN cache**. Se la **SYN cache** si riempie, si passa ai **SYN cookies**. In questo modo si combinano gli aspetti positivi delle due tecniche.

Crittografia serve a nascondere agli elementi intermedii cosa c'è dentro.

SYN Cookie

