Tema 3

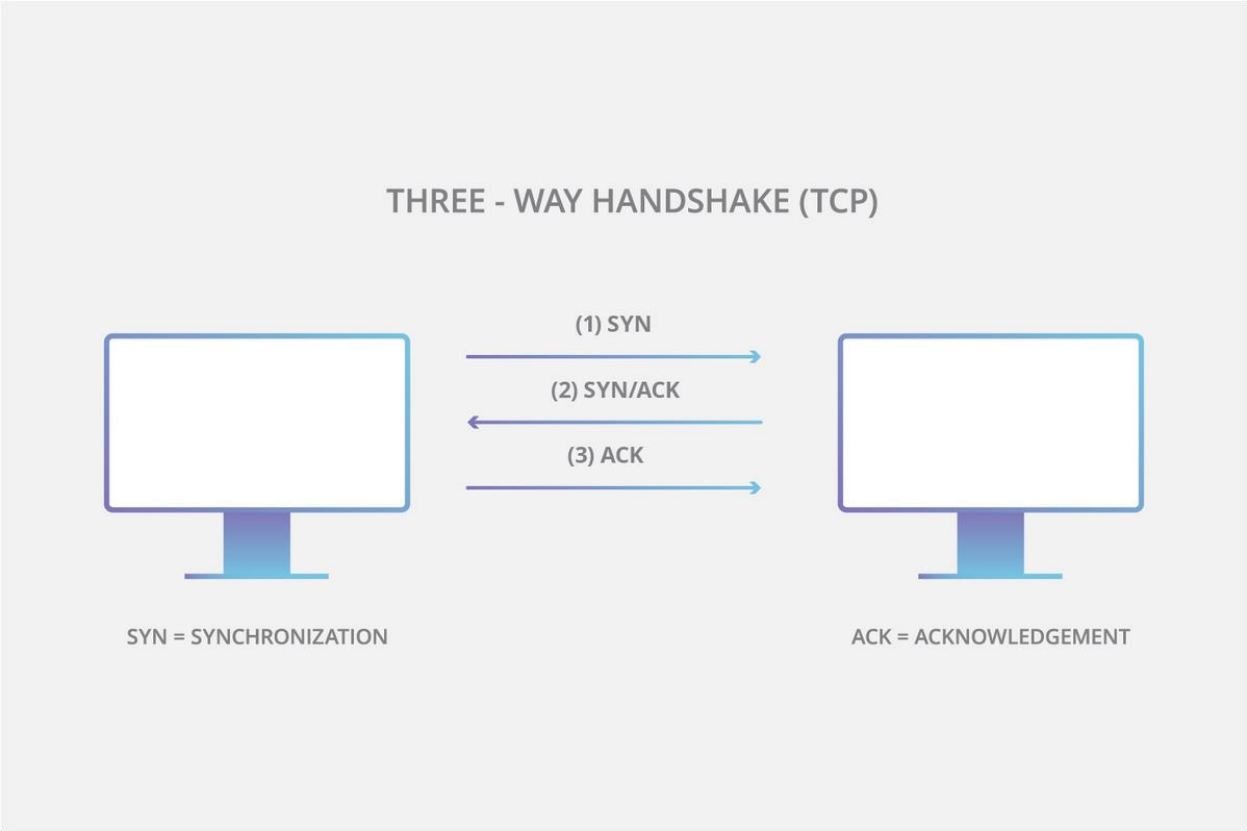
Stamate Valentin

Atacul Syn Flooding

Este un atac ce exploateaza modul cum clientii stabilesc o conexiune de tip TCP cu un server.

Three-Way Handshake:

- clientul trimite un packet de tip SYN pentru a initia conexiunea
- serverul trimite inapoi clientului un packet de tip SYN/ACK
- clientul trimite serverului un packet de tip ACK
- conexiunea TCP ramane deschisa si se pot primi/trimite mesaje

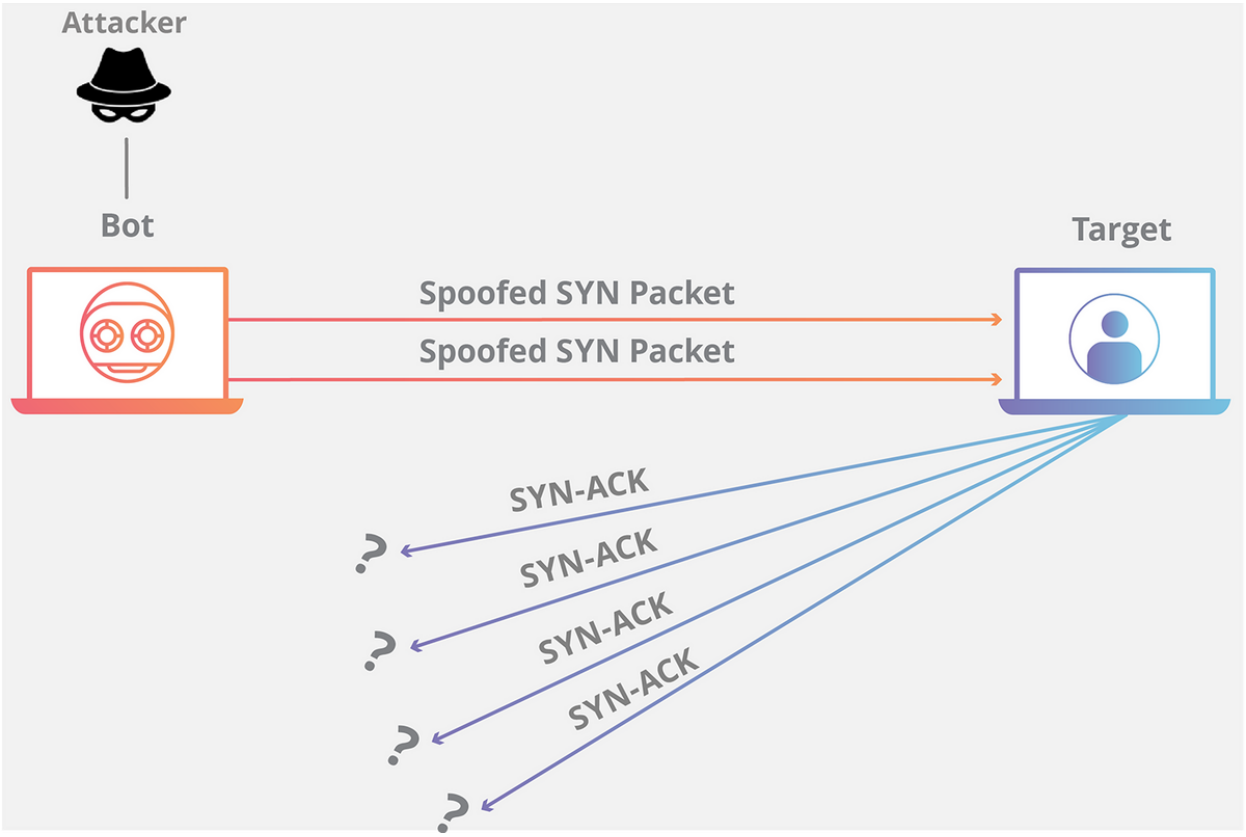


Acest atac se foloseste de faptul ca, atunci cand este trimis un packet de tip SYN, serverul raspunde cu unul sau mai multe packete de tip SYN/ACK si mentine o conexiune deschisa pe o perioada de timp pentru primirea packetului.

Cum se desfasoara atackul?

Atacatorul trimite un numar mare de packete de tip SYN cu o adresa ip invalida. Serverul raspunde la fierare dintre ele si pentru ca de la nici unul nu primeste raspuns inapoi, conexiunile create raman deschise temporar. Totodata, serverul are un numar limitat de conexiuni deschise pe care le poate intretine, asa ca, in urma volumului mare, sistemul va functiona anormal.

De asemenea, acest tip de atac se mai numeste si atac de tip DDoS(denial-of-service).



Cum se poate realiza un astfel de atac?

- Atac Direct: atacatorul nu-si ascunde adresa ip si pentru ca foloseste un singur device el este in pericol de a fi descoperit.
- Atac Ascuns: atacatorul isi ascunde adresa ip. Cu toate acestea, el inca poate fi descoperit.
- Atac Distribuit: atacul este creat de unul sau mai multe sisteme de tip botnet, ceea ce face depistarea atacatorului aproape imposibila.

Cum se poate preveni un astfel de atac?

- Cresterea numarului de conexiuni deschise.
- Scrierea peste cea mai veche conexiune deschisa.
- Folosirea uniu cookie pentru conexiunile a caror packet SYN/ACK a fost trimis.

Detectarea atacului:

- Numarul mare de packete SYN primite
- Variatia de timp e foarte mica intre packete
- Fiecare packet arata o alta adresa IP
- Numarul de packete de tip SYN/ACK este foarte mic

Bibliografie:

- Atacul SYN Flood : https://www.cloudflare.com/en-gb/learning/ddos/syn-flood-ddos-attack/
- Atacul DDoS : https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/
- Botnet : https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-botnet/
- Detectarea atacului : https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html