Security Apps with P4 Programmable Switches

Detecting and mitigating SYN flood attacks in P4

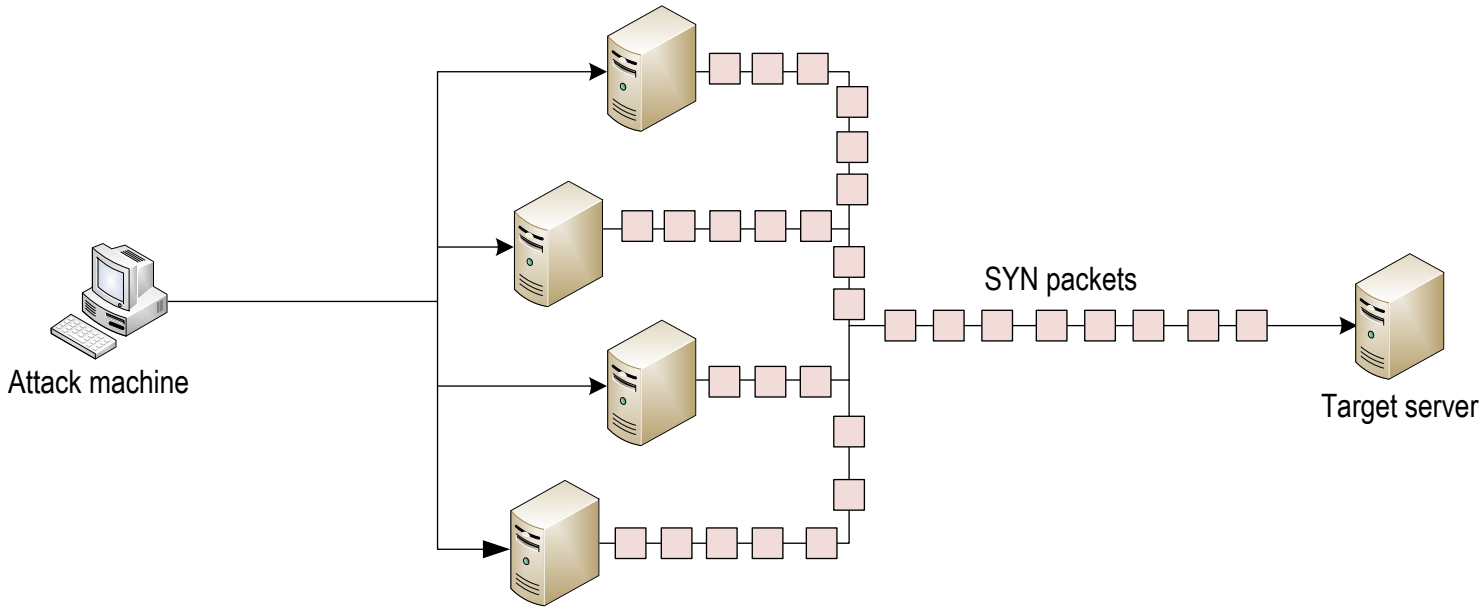
Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

University of South Carolina (USC)
Energy Sciences Network (ESnet)

September 18, 2023

SYN Flood Attack

- Massive amount of TCP SYN requests with spoofed IP addresses are sent to the server
- These connections consume the server's resources, making it unresponsive to legitimate traffic
- Server start "half-open" connections
- Connections build up until queue is full and all additional requests are blocked

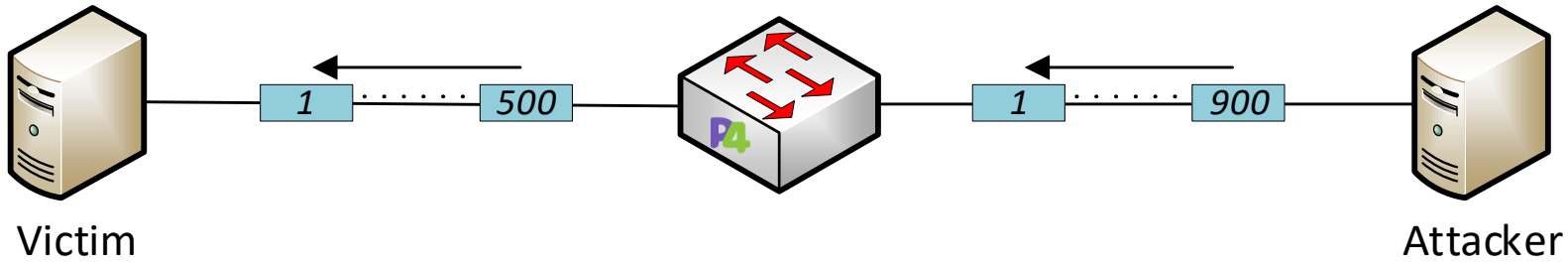


SYN Flood Detection in P4

- Count the number of SYN packets per second in the data plane
- When the count exceeds a predefined threshold, the switch starts dropping SYN packets
- The dropping percentage is configured by the administrator from the control plane

SYN Flood Detection in P4

- Assuming that the attacker is generating 900 SYN packets per second
- The SYN count detection threshold is 100 packets per second
- Assume that the drop percentage is 50%
- The number of packets that will be forwarded is:
  - $100 + (900 - 100) * 50/100 = 100 + \frac{800}{2} = 500$



SYN packets threshold: 100

Dropping percentage: 50%