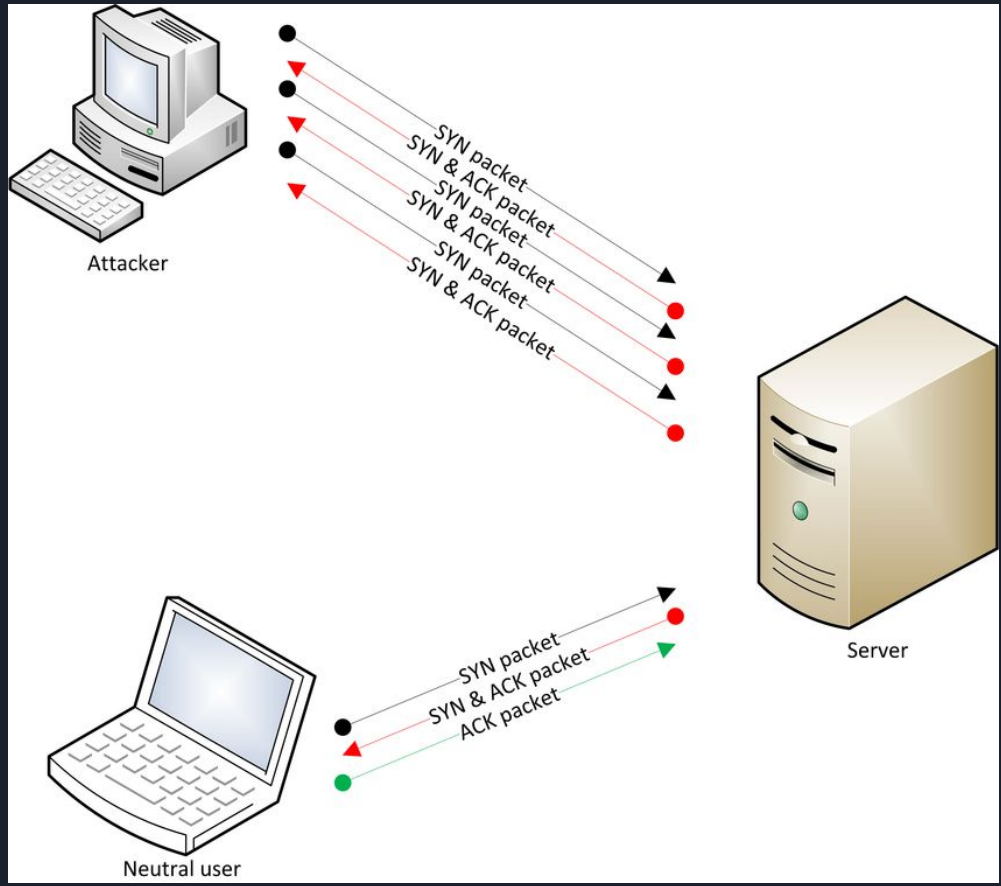
TCP-SYN-FLOOD ATTACK MITIGATION WITH RYU AND SNORT

Bartłomiej Gdowski
Michał Jaworski
Beniamin Paś
Michał Piróg

Sieci Sterowane Programowo 2021/22

TCP SYN FLOOD

- DoS/DDoS ATTACK
- MULTIPLE CONNECTION REQUESTS WITHOUT “THIRD HANDSHAKE”
- MALFUNCTION OR CRASH OF SERVER



SNORT

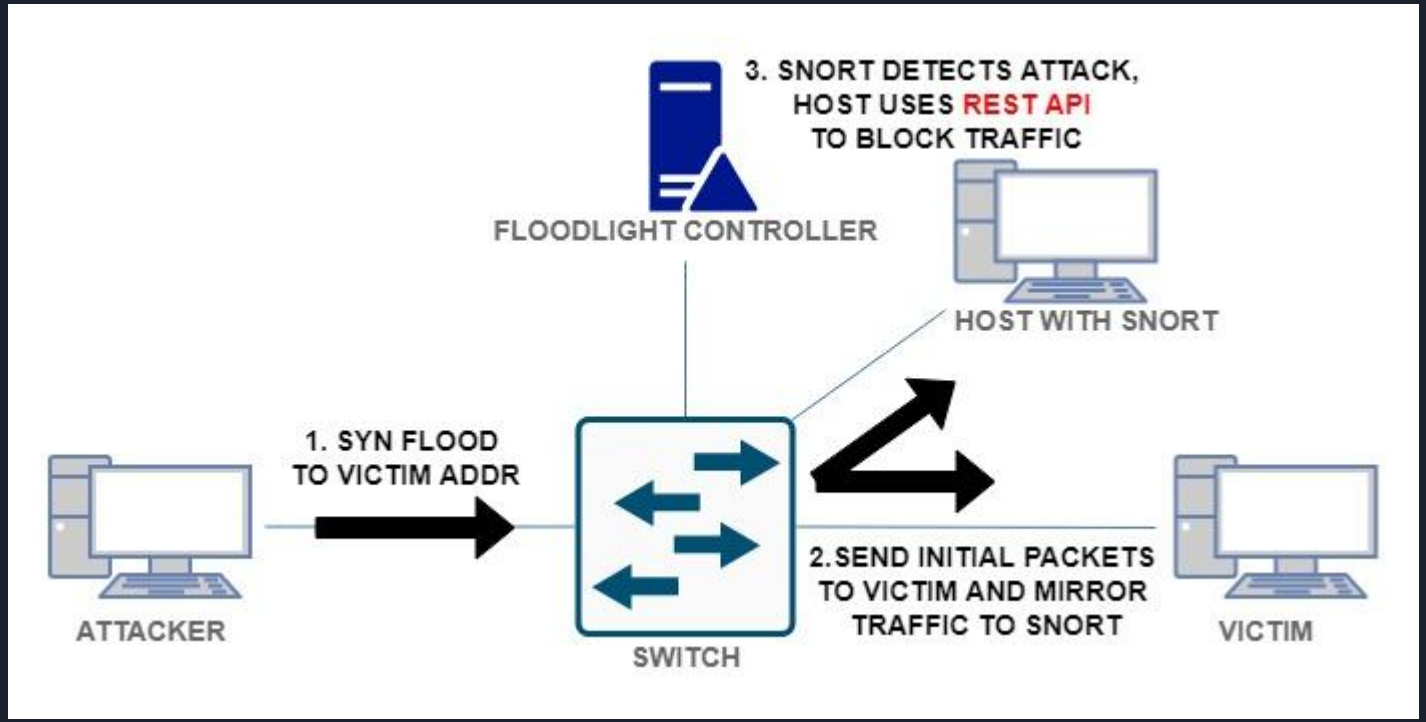
- NETWORK INTRUSION DETECTION SYSTEM
- OPEN SOURCE
- RULE LANGUAGE

```
alert tcp any any -> $HOME_NET 80 (flags: S; msg:"SYN FLOOD WARNING"; flow: stateless;
detection_filter: track by_src, count 30, seconds 10;)
```

RYU

- RYU MEANS ‘FLOW’ IN JAPANESE
- COMPONENT-BASED SDN FRAMEWORK
- OPEN SOURCE
- WELL DEFINED API
- OPEN-FLOW, NETCONF, OF-CONFIG, ETC.
- SNORT INTEGRATION

WHY NOT FLOODLIGHT?



LIVE DEMO