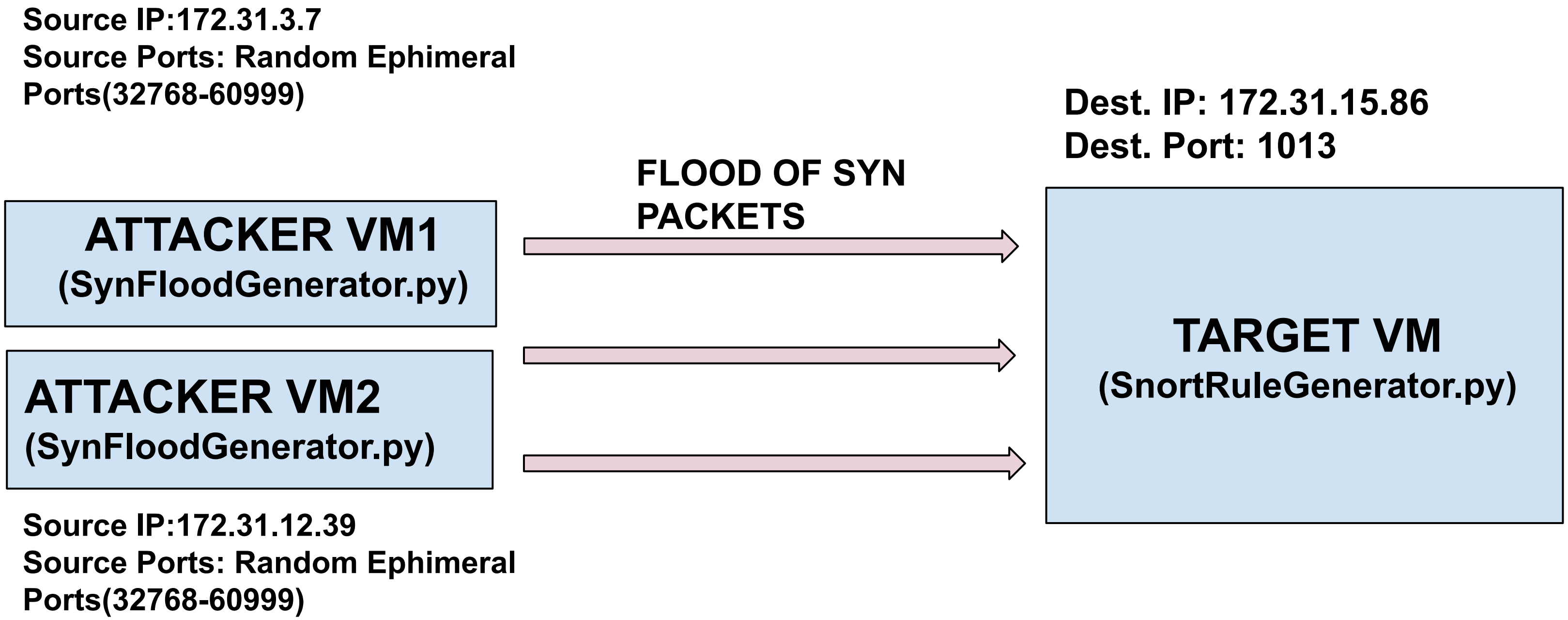
PYSNORTLINGS 2.0 HIGH LEVEL OVERVIEW



Source IP:172.31.3.7
Source Ports: Random Ephimeral
Ports(32768-60999)

ATTACKER VM1
(SynFloodGenerator.py)

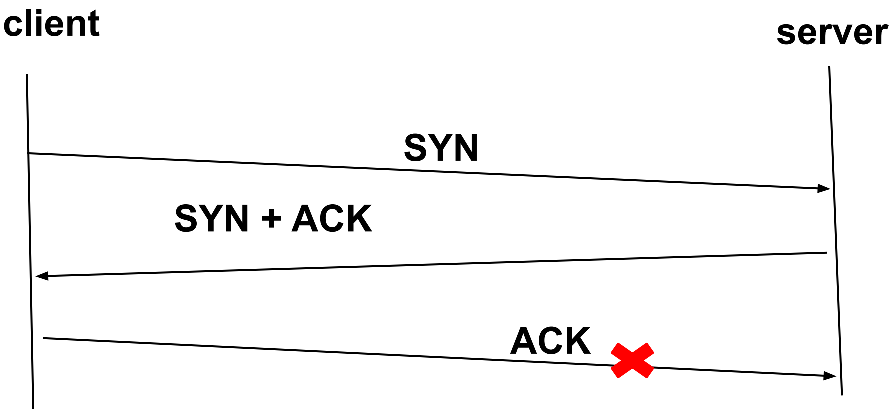
ATTACKER VM2
(SynFloodGenerator.py)

Source IP:172.31.12.39
Source Ports: Random Ephimeral
Ports(32768-60999)

FLOOD OF SYN
PACKETS

Dest. IP: 172.31.15.86
Dest. Port: 1013

TARGET VM
(SnortRuleGenerator.py)



Client sends a flood of SYN packets and Server sends SYN-ACK for every SYN packet, waiting for the ACK to open a connection. But it never happens, resulting in keeping the server unnecessarily busy and not serving legitimate connections.