Blocking the Attacking Machine with IPTABLES in the Host Machine

Step 1:

Check the existing firewall rules in iptables:

`sudo iptables -L -v`

Step 2:

Adding an iptables rule to disable connection from one attacking machine (need to know the IP address of the machine; replace "10.0.2.2" with the target IP address)

`sudo iptables -A INPUT -s 10.0.2.2 -p tcp --destination-port 8000 -j DROP`

Try if you can still access or DoS the webserver from that machine

Step 3:

Removing the blocking rule from the iptables:

`sudo iptables -D INPUT 1` (assuming there is only one rule in the iptables)

Try if you can access or DoS the webserver again from that machine