**Dosing the Dos Attack**

1.Are there problems with any of her precautions? If so, what are the problems?

* Blocking all incoming ICMP packets can assist in reducing specific types of DoS attacks, such as ICMP floods. However, this action may impede critical network diagnostic and troubleshooting tasks like ping requests and error messaging, making it difficult to promptly identify and resolve network issues. Moreover, the implementation of SYN cookies on the web server effectively addresses SYN flood attacks by validating connection requests. Nevertheless, this measure can escalate server overhead and latency, particularly during peak traffic periods, potentially resulting in reduced server performance and delayed response times for legitimate users. Consequently, while these precautions are intended to bolster network security, they have the potential to inadvertently compromise network functionality and server efficiency. It is imperative for network administrators, such as Runa, to carefully evaluate these possible drawbacks and explore alternative strategies for mitigating DoS attacks without causing disruptions to network operations.

2. What additional steps would you recommend to Runa?

* I recommend that Runa installs systems that can detect and stop suspicious activity right away. Also, using networks that spread out the load on our web server can help avoid it getting overwhelmed during attacks. Plus, Runa should divide our network into sections and control who can access them, stopping attacks from spreading. These extra steps will make it much harder for DoS attacks to cause problems and keep our network safe.