Dear all,

First of all, please be informed that this assignment is an individual submission. Please **DO NOT POST** your comments in a public space. Instead, submit your individual report by Next Week's Live Session.

Assignment#5 (Individual)

- **Topics:** Answer the following questions based on the packet-filtering rules below. These rules are intended to allow only HTTP (using server port number 80) services between the internal and external machines.

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
Inbound	Incoming	External	Internal	TCP	80	Permit (Rule A)
	Outgoing	Internal	External	TCP	>1023	Permit (Rule B)
Outbound	Outgoing	Internal	External	TCP	80	Permit (Rule C)
	Incoming	External	Internal	TCP	>1023	Permit (Rule D)

Topic 1. Explain how an external attacker (using port number 7000) can have access to an internal machine (using port number 8000) based on the above rules. **Hint: The attacker needs only a couple of rules that allow his outgoing and incoming packets.

Topic 2. Explain how the attack (described in **Topic 1**) can be foiled by checking the source port numbers. Please describe the enforced rule(s).

Topic 3. Explain how an external attacker (using port number 80) can have access to an internal machine (using port number 8000) based on the above rules (described in **Topic 2**). **Hint: The attacker has control over his machine, including the port number change.

Topic 4. Explain how the above attack (described in **Topic 3**) can be foiled by checking the connection initiator. Please describe the enforced rule(s).

- **Deliverables:** Your answers for the topics above with clear and sufficient description (up to 100 words for each topic).
- **Submission:** Attach one PDF file.
- **Due Date: Submit your work by** Next Week's Live Session.

Best,
Dr. Park