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.

- An external attacker can exploit Rule's D and B. The attacker satisfies these rules based on the following:
    - The originating attacker exploits Rule D, which allows the firewall to be passed to the victim's host machine at post 8000. The victim's outgoing packet response is permitted through the firewall by exploiting Rule B shown in the table below.

Table 1

Packet Direction	Source Address	Destination Address	Protocol	Destination Port	Action
Incoming	External	Internal	TCP	8000	Permit- Rule D
Outgoing	Internal	External	TCP	7000	Permit- Rule B

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).

- Since the user in this situation is not checking the source port numbers, the attacker was able to exploit rule D and rule B, allowing the attack to take place. The user can now check the source port numbers by adding a new parameter to the rule definitions, as shown in table 2.1. The modified packet filtering rules' requirements is to ensure that the source port is an HTTP service port 80 as intended for these rules. The new rule B and rule D source port configurations now deny these port numbers based on the attacker port of 7000 and the victim port of 8000. The packets are now denied; therefore, the attack is foiled shown in Table 2.2.

Table 2.1

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

Default	Either	Any	Any	Any	Any	Any	Deny-Rule E

Table 2.2

Packet Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
Incoming	External	Internal	TCP	7000	8000	Deny-Rule E
Outgoing	Internal	External	TCP	8000	7000	Deny- Rule E

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).

- The attacker has discovered that the firewall rules are inspecting the source ports for HTTP 80 service ports in this case. Based on this information, the attacker disguises their source port as 80 to make it appear as if the request is coming from an HTTP service on port 80. The firewall rules, rule C and D, as indicated in table 3, would allow this configuration change. As a result of exploiting these rules, the attack was successful.

Table 3

Packet Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
Incoming	External	Internal	TCP	80	8000	Permit-Rule D
Outgoing	Internal	External	TCP	8000	80	Permit-Rule C

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).

- In this case, we've added a new condition column to the firewall rule that checks the packet initiator ACK section. In TCP, the ACK bit of the three-way handshake is set to 0. ACK=0 is only included in the first packet of the whole session. The ACK bit will be set to 1 in all following session sequences, indicating that the previous packet request has been acknowledged. This message segment ACK will be 0 as the external attacker host whose originator is targeting port 8000 of the internal victim's host, as stated in table 4.2. Rule E denies the ACK segment of 0 since it does not comply with any of the previous firewall rules, particularly rule D.

Table 4.1

Service Direction	Packet Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK=1	Action
Inbound	Incoming	External	Internal	TCP	>1023	80	Any	Permit-Rule A
	Outgoing	Internal	External	TCP	80	>1023	Yes	Permit-Rule B
Outbound	Outgoing	Internal	External	TCP	>1023	80	Any	Permit-Rule C
	Incoming	External	Internal	TCP	80	>1023	Yes	Permit-Rule D
Default	Either	Any	Any	Any	Any	Any	Any	Deny-Rule E

Table 4.2

Packet Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK=1	Action
Incoming	External	Internal	TCP	80	8000	No	Deny-Rule E