Syracuse University

IST-623 Assignment#5 Firewalls

ThulasiRam RuppaKrishnan

IST 623

Professor Joon Park

Assignment#5 (Individual)

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)

Table 1.1 Firewall Packet Filtering Rules

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.

According to the rule described in **Table 1.1**, any external agent (Attacker) can send information through outbound service direction to internal clients on any port number above 1023 as permitted by the Rule D. Similarly, the external agent can receive information through Inbound service direction from any Internal clients to any destination port above 1023 as permitted by the Rule B.

Table 1.2 given below shows how these rules can be exploited by the Attacker using the destination port number 7000 and 8000 (>1023) for both Inbound and Outbound direction respectively.

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action	Status
Inbound	Outgoing	Internal	Attacker	TCP	7000	Permit (Rule B)	Attack Success
Outbound	Incoming	Attacker	Internal	TCP	8000	Permit (Rule D)	Attack Success

Table 1.2 Firewall Packet Filtering Rule Penetration by Attacker on Rule B and D

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).

By introducing additional filter in the packet filtering rules with source port number check, the attack described in Topic 1 can be foiled. **Table 1.3** given below shows the additional constraints added on top of the initial laid out in **Table 1.1.** Here the Rule B and D will invalidate the attack by checking the source port number in both Inbound and Outbound direction as shown in **Table 1.4**

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. 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)

Table 1.3 Advance Firewall Packet Filtering Rule (A1)

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action	Status
Inbound	Outgoing	Internal	Attacker	TCP	8000	7000	Permit (Rule B)	Attack Foiled
Outbound	Incoming	Attacker	Internal	TCP	7000	8000	Permit (Rule D)	Attack Foiled

Table 1.4 Advance Firewall Packet Filtering Rule (A1) preventing attack laid in Table 1.2

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.

An advance attacker who can control his machine with the capability of changing the port number can still penetrate the system using rule B and D as described in **Table 1.5.** In this case**,** the attacker chooses source port 80 for sending information to internal machine running on destination port 8000 using Rule D and change his machine's port number to 7000 (>1023) while receiving information from internal machine using Rule B

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action	Status
Inbound	Outgoing	Internal	Attacker	TCP	80	7000 (Attacker changed his port from 80 to 7000)	Permit (Rule B)	Attack Success
Outbound	Incoming	Attacker	Internal	TCP	80	8000	Permit (Rule D)	Attack Success

Table 1.5 Firewall Packet Filtering Rule Penetration by advanced attacker on Rule B and D

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).

By adding connection initiator as part for Firewall packet filtering rule, the successful attack described in **Table 1.5** can be foiled. In this case the first message sent by the attacker to internal machine will accompany ACK=0 which is not permitted in the Rule D and hence the attack is foiled as shown in **Table 1.7**

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. 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)

Table 1.6 Advance Firewall Packet Filtering Rule (A2)

Service Direction	Packet Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	ACK=1	Action
Outbound	Incoming	External	Internal	TCP	80	8000	No	Attack Foiled

Table 1.7 Advance Firewall Packet Filtering Rule (A2) preventing attack laid in Table 1.5