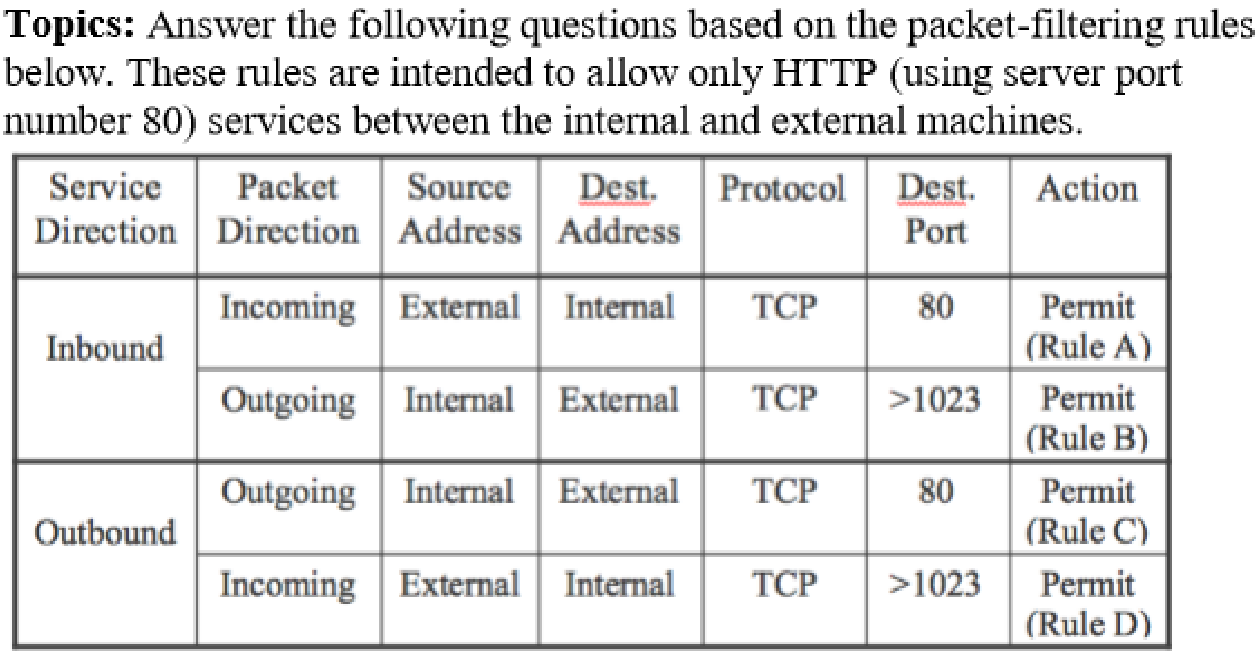
IST 623 - Intro to Information Security

Homework Assignment 5

Ryan Timbrook
NetID: RTIMBROO
Term: Winter, 2020
Date: 3/15/2020
Topic: Packet Filtering Rules

Table of Contents

Packet Filtering Rules Table:



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)

1 Topics

1.1 Topic 1

Question: 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.

An external attacker can exploit Rule's D and B shown in the above packet-filtering rules table. The attacker satisfies these rules based on the following:

The originating attacker exploits Rule D where it's permitted passed the firewall to the vitims host machine at port 8000. The victim's outgoing packet response is permitted through the firewall by exploiting Rule B. This is shown in Table T1.1 below.

Table T1.1: Firewall Rule Actions Permitted - The Attack is successful!

Packet Dir	Source Addr	Dest. Addr.	Protcol	Dest. port	Action
Incoming	External	Internal	TCP	8000	**Permit (Rule D)**
Outgoing	Internal	External	TCP	7000	**Permit (Rule B)**

1.2 Topic 2

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

The attack described in Topic 1 was possible because the attacker was able to exploit the rule set rule D and rule B because in that senario we weren't checking the source port numbers.

By adding a new parameter to our rules definitions, shown below in table T2.1 highlighted in red, we can now check the source port numbers. Now we've refined the conditions for the packet filtering rules to validate the source port is coming from an HTTP service port 80 as intended for these rules. And based on the attacker port of 7000 and the victim port of 8000, these port numbers are now denied based on the modified Rule B and Rule D source port configurations. The packets are now denied, therefor the attack is foiled. This is represented in Table T2.2 shown below.

Table T2.1: Updated Firewall Rules Configuration

Service Dir.	Packet Dir.	Source Addr.	Dest. Addr.	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)**
Default	Either	Any	Any	Any	Any	Any	Deny (Rule E)

Table T2.2: Firewall Rule Actions Denied

Packet Dir.	Source Addr.	Dest. Addr.	Protocol	Source Port		Dest. Port	Action
Incoming	External	Internal	TCP	**7000**		8000	**Deny (Rule E)**
Outgoing	Internal	External	TCP	**8000**		7000	**Deny (Rule E)**

1.3 Topic 3

Question: 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.

In this scenario the attacker has learned that the firewall rules are checking the source ports to be HTTP 80 service ports. Based on this learned knowledge, the attacker masks their source port as 80 to mimic the request is originating from an HTTP services on port 80. This configuration change would be permitted by firewall rules, Rule C and D shown in Table T3.1 below. The attack has exploited these rules, therefor the attack is successful.

Table T3.1: Firewall Rule Actions Permitted

Packet Dir.	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	Action

Incoming	External	Internal	TCP	**80**	8000	**Permit (Rule D)**
Outgoing	Internal	External	TCP	8000	**80**	**Permit (Rule C)**

1.4 Topic 4

Question: 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 scenario we've added another new firewall rule condition column that checks the packet initiator (ACK) segment. The ACK bit, of the three-way handshake in TCP, is defaulted to 0. Only in the very first packet for the entire session is ACK equal to 0. In all subsiquent session sequences the ACK bit will equal 1, signifing the acknologment of the prior packet request.

As the external attacker host who's the originator targeting port 8000 of the internal victims host, this message segments ACK will be 0. Shown in Table T4.2 below, an ACK segment of 0 is denied by Rule E because it did not satisfy any of the prior filewall rules, specifically Rule D.

Table: T4.1: Updated Firewall Rule - Including Initiator ACK Condition

Service Dir.	Packet Dir.	Source Addr.	Dest. Addr.	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)**
Default	Either	Any	Any	Any	Any	Any	Any	Deny (Rule E)

Table T4.2: Firewall Rule Denied Action

Packet Dir.	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK=1	Action
Incoming	External	Internal	TCP	80	8000	**No**	**Deny (Rule E)**