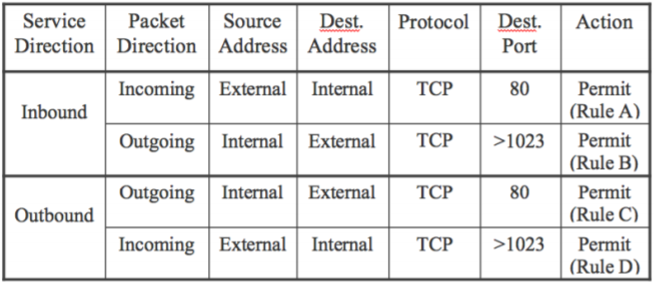
David Doman

IST 623

HW Assignment 5



**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.

***Answer:*** *The attacker can gain access through Rule D, where it can access the victims host machine at port 8000 through the firewall. As for the victim, Rule B allows the victims outgoing packet to be permitted through the firewall.*

**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).

***Answer:*** *Source port numbers not being checked is the main reason why the attacker was able to exploit Rule B & Rule D. Shown below, this attack can be defended by adding an additional parameter to the rule definitions. Adding source port numbers to the rules allows this check to be executed. Implementing this modification performs validation that the source port is coming from port 80 and not from somewhere else. The attack that happened in Topic 1 will now be unsuccessful as attacker port 7000 and victim port 8000 will now be denied based on the newly implemented modifications.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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) |

**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.

***Answer:*** *After the attacker has been denied in the scenario described in Topic 2, he/she becomes aware that new defenses have been implemented. As most hackers/attackers do, they learn of these new defenses and come up with additional ways to attack a system. In this scenario, the attacker masks their port number to be 80 to be able to pass the firewall as port 80. Rules C & D are susceptible to this type of attack and are therefore compromised.*

**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).

***Answer:*** *This scenario requires a new parameter to be added to the firewall rules we have already implemented. This new parameter will be one that checks the packet initiator ACK segment. The ACK bit is defaulted to 0 and is a 3-way interaction in TCP. The initial packet will be set to 0 and all following sequences will the ACK will be 1, which signifies a prior packet request.*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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) |  |