

choose one: Received Received help from:
(or more) no help Collaborated with: _____

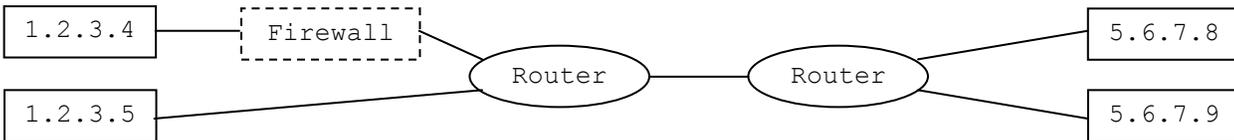
Homework: /SI110/The Cyber Battlefield/Firewalls

0. From the Tuesday talk: What is Kevin Mitnick's "favorite hack"?

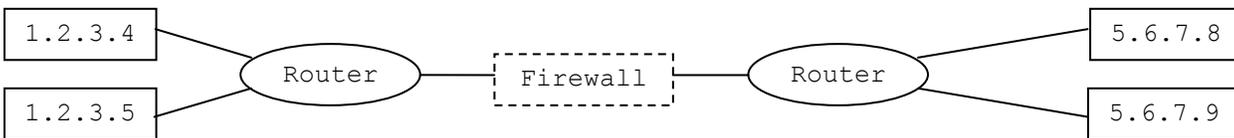
10/8/6/0

1. Consider Configuration A, B, and C pictured below:

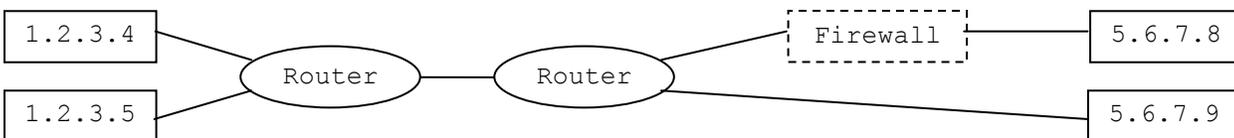
Configuration A:



Configuration B:



Configuration C:



If the firewall is configured to drop all packets with destination port 22, then ...

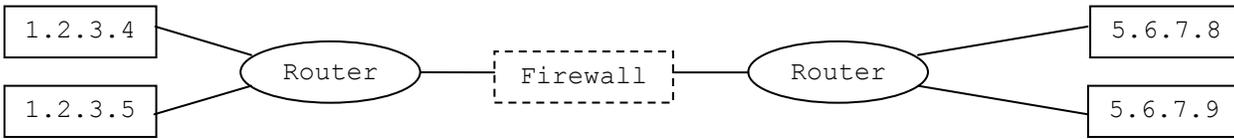
i. Configuration ____ stops host 1.2.3.4 from connecting via SSH to any host. Explain!

10/8/6/0

ii. Configuration ____ stops any host from connecting to host 5.6.7.8 via SSH. Explain!

10/8/6/0

2. Suppose we have the following network configuration, in which the firewall drops all traffic with destination port equal to 80, and forwards everything else:



a. Can host 5.6.7.8 access a DNS name server running on host 1.2.3.5? Explain!

15/12/9/0

b. Can host 5.6.7.8 access a web server running on host 5.6.7.9? Explain!

15/12/9/0

c. Can host 5.6.7.8 access a web server running on host 1.2.3.4? Explain!

15/12/9/0

d. Suppose host 5.6.7.8 has an SSH connection to host 1.2.3.5 running in its terminal window. If the command `nc 1.2.3.4 80` was typed into that terminal window, would the connection to 1.2.3.4 on port 80 be made, or would the firewall prevent it? Explain!

15/12/9/0

3. Consider these two versions of an ACL for a firewall:

Version 1:

Drop packets from 22.10.133.8 going to TCP port 15000 on 87.52.8.125
Forward packets from Any IP going to TCP port 15000 on 87.52.8.125

Version 2:

Forward packets from Any IP going to TCP port 15000 on 87.52.8.125
Drop packets from 22.10.133.8 going to TCP port 15000 on 87.52.8.125

Which of the two versions allows all hosts other than 22.10.133.8 to connect via TCP to Host 87.52.8.125 on port 15000? Explain!

10/8/6/0