IP Tables

Adrianna Holden-Gouveia
Website: `https://aholdengouveia.name`
in: aholdengouveia
: aholdengouveia
: aholdengouveia

Complete the following problems

References, a video, a PowerPoint and some notes are available at my website https://www.aholdengouveia.name/LinuxAdmin/iptables.html

Go through both servers and complete the following problems.

Write scripts or statements to modifying firewall rules (IPtables) for specific purposes, make sure you include wireshark screenshots to prove your command/script/statements work.

1. Deal with web server (open needed ports, and forward port 80 traffic to 8080)
2. Deal with MySQL service (open needed ports)
3. Deal with SSH service (allow incoming and outgoing SSH, second script to deny SSH)
4. Script to allow/block specific hosts, MAC addresses
5. A script/command to block telnet, and another one to block ping

Write the specs for how you think you could prevent a DDOS attack using IPtables. Can you write a script for this? Cite your sources!

Deliverables

Target Market is someone trying to take care of your server that hasn't used IPTables before, assume some technical knowledge but not expertise. Screenshots are helpful to go with your descriptions.

Include documents for BOTH servers clearly labeled with what the document is and which server it's for

- A text document including the answers to each question, (scripts or statements or commands are fine) but explain why you choose what you choose. Include any assumptions made about what you consider "dealing with" as well as the screenshots showing Wireshark to prove your script/statement/command works.
- Documentation of your IPtables for each of your servers should include a list of changes to the chains you've made including which table you think needs to be changed, when the change was made. Include a copy of your original IPtable and your updated IPtable at the end of this assignment.
- A short document explaining how you think you could prevent a DDOS attack using IPtables. Cite at least 2 sources.