University Göttingen
GWDG/AG-C
Julian Kunkel

Exercise 1 / October 17, 2023
HPC System Administration / 2023/24
20 Minutes Total

Firewall

Perform all the following tasks and discuss them in your group.

Contents

Task 1: Configure the Firewall (20 min)

Beware: do not remove the rule regarding SSH, otherwise you are locked out from your VM.

Steps

1. Discuss the provided ruleset in your study group.
2. Check the ruleset using `nft -c -f ruleset.nft` - counters are very useful for debugging!
3. Check the open ports with `nmap`
4. Load the ruleset using `nft -f ruleset.nft`
5. Check the open ports with `nmap`
6. Modify the rules to reject instead and investigate response of `nmap` and `wget`
7. Check the output of the logfiles
8. Access an invalid port and see its impact on the logfile
9. Remove the rules using flush
10. Discuss what ports you would open for a service of your choice! How can you identify which ports to open in this case.

Hints

- Make sure that SSH is still accepted
- If you try to access the ports from localhost (instead from another node), there is a rule that will accept all traffic
- To reject, try this rule `reject with icmp type admin-prohibited`
- Use `tail -f LOGFILE` to get the newest log messages.

Optional Task 2: NAT with nftables (20 min)

This is a difficult **additional** task which will support your understanding in the topic.

Imaginge you have to set up a DMZ. On the firewall, you want to transparently redirect HTTP traffic to a target address using NAT. Thus, the clients of the web server will not realize that their network packets are altered.

Steps

1. Check that no firewall rule is active.
2. Check the links below for information on the topic
3. On your login node, create a ruleset that redirects any HTTP and HTTPS traffic to GWDG's web server.
4. On a worker node, retrieve data from the IP of the login node.

With a few modifications, this could be modified to forward any TCP/UDP request of all worker nodes correctly to any server in the WWW. In that case, you would have to modify the default route and must ensure the DNS resolver of the worker nodes work as intended.

Hints

- Use counter to be able to debug the usage.
- Create chains for the prerouting and postrouting hooks.
- You can also modify any outgoing (output) request on the node and can test on a single node, therefore, you must use the output chain.

Further Reading

- NAT `https://jensd.be/1086/linux/forward-a-tcp-port-to-another-ip-or-port-using-nat-with-nftables`
- NAT redirection `https://ungleich.ch/u/blog/nftables-magic-redirect-all-ports-to-one-port/`