There are two tasks in this exercise. You need to attempt both and submit a report carrying screenshots, commands you ran and their descriptions.

Task 1

Requirements: Three virtual machines running Linux (e.g artix linux with no X window – a bare console setup with 256 MB RAM and single core). One of the VMs should have two (virtualized) network interface (in host only mode) and the other two could have two different interfaces. You could use any popular virtualization system.

The first task teaches you how to use Linux IPTables firewalls to do traffic filtering (a form for of network ACLs). You would require configuring the three VMs using the following configurational setup.

[VM1](interface 1) ←→ (interface 1) [VM2](interface 2)←→(interface 1) [VM3]

             10.0.0.0/8   20.0.0.0/8

       Client   Firewall   Server
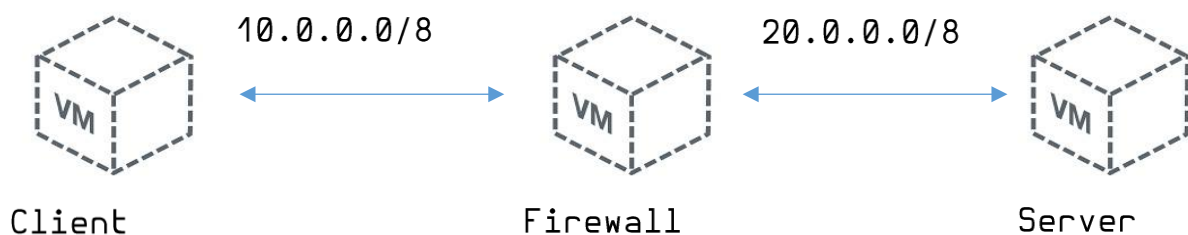
a. Assign private IP addresses to each interface, such that the VMs can ping one another. VM1 (iface1) and VM2 (iface1) should be in the same subnet. VM2(iface2) and VM3 (iface1) should be in the same subnet.

b. Setup IP forwarding on VM2 such that VM1 can ping both interfaces IPs of VM2 and VM3. Make sure traffic from VM1 to VM3 goes via VM2 (can be seen via traceroute).

c. On VM3 add another interface with which it can access the Internet. Install a HTTP server (e.g. Apache, lighttp or nginix) on the VM3. Create a web directory and add some files to it.

d. You need to use IPTables on VM2 and configure bi-directional Network Address Translation on VM2. Thus, when VM1 access the webserver on VM3, or when VM2 access the webserver on VM3, in both cases you should observe connections coming from VM2. Similarly when responses go back to VM1, it should appear that they are arriving from VM2 and not VM3. You need to show screenshot outputs taken from Wireshark, showing the bidirectional NATing.

e. Enable webserver process on port 80 and 443. Configure the firewall on VM2 to restrict access only to those ports and not allow anything else. To test correct functionality you could additionally install SSH server on VM3 and try to access it. Correct firewall functionality should restrict access to port 22 (SSH).

f. Configure the firewall such that only connections from VM1 are allowed on port 80 and 443 on the HTTP server on VM3. Access from VM2 should not be allowed.

The following links are some references I used to learn more about iptables (and netfilter):

https://www.cyberciti.biz/tips/linux-iptables-examples.html

https://help.ubuntu.com/community/IptablesHowTo

https://www.garron.me/en/linux/iptables-manual.html

https://netfilter.org/documentation/HOWTO//networking-concepts-HOWTO.txt

https://netfilter.org/documentation/HOWTO//NAT-HOWTO.txt

Task 2 (total points: 25)

This task requires setting appropriate file permissions on the VM3.

   a. On VM3 now you need to create one more user – temphttp. The web directory on the server should be onwed by temphttp with no permissions for the webserver process to read from it.

   b. Utilize the `setuid' bit to set the permissions of the web server process to be able to write to the webserver directory.

   c. Use Linux ACLs to grant specific access read access to the webserver process.

Useful links:

https://linuxconfig.org/how-to-manage-acls-on-linux

https://www.tecmint.com/secure-files-using-acls-in-linux/

https://bencane.com/2012/05/27/acl-using-access-control-lists-on-linux/