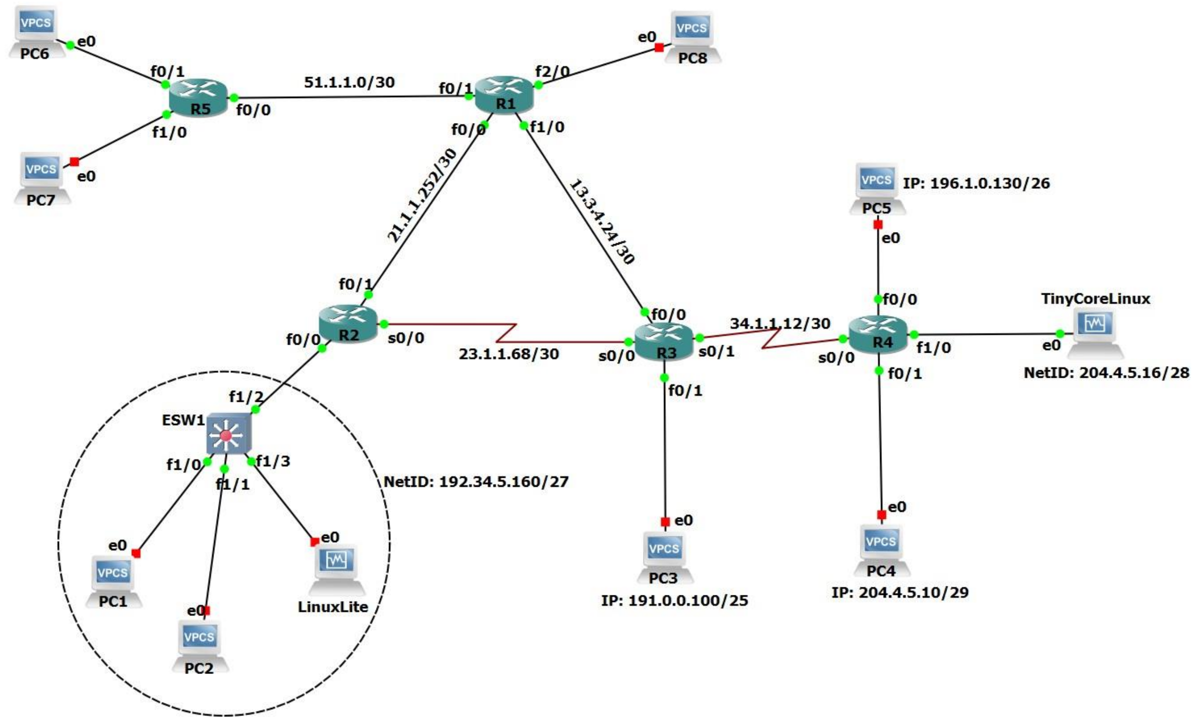
CECS 303 NETWORKS AND NETWORK SECURITY

<u>Netlab 5</u>: ACLs in GNS3

<u>Purpose:</u> In this Lab exercise, you will add more devices to the previous lab topology and apply ACLs to filter and secure traffic flow.

Part 1 Procedure

Add to the project one LinuxLite (or LinuxLiteClient) and one TinyCore (or LinuxLiteServer) VM appliances. Connect them to the routers as depicted in the topology. Configure both VMs. Note that the TinyCore or LinuxLiteServer is connected to a new network, so, adjust the routing and DHCP configuration accordingly.



Notes:

1.- We will refer to the LinuxLite or LinuxLiteClient as the "**ClientVM**" and the TinyCoreLinux or LinuxLiteServer as the "**ServerVM**".

2.- Before starting the Linux VM, edit their configuration:

Right-click❼configure❼Network tab❼Check-off "Allow GNS3 to use any configured

VirtualBox adapter"
3.- Login credentials for the VMs are: username: tc and pass: netlab2020

4.- If you are using TinyCoreLinux VM, you need to update the password for the user ***tc***. In a CLI window apply the command: sudo passwd tc (enter the password **netlab2020**) . If you are using the LinuxLiteServer VM, you don't need to do apply this.

Part 1

Start a packet capture in the link connecting the ServerVM. Apply the filter **tcp**. From the ClientVM open a CLI window and execute the command: ftp [*ServerVM IP address*] and enter any password. Even though the server will not authenticate you, the packets have been sent and captured in Wireshark.

Q1. In the packet capture, can you see the username and password in cleartext? Explain

Yes. I am able to see the username and password using the tcp. It is reflected in the FTP protocol exchange.

Q2. What are the protocols used and destination port number? Explain

Source: 45874, destination port: 21

Now from the ClientVM CLI window, execute the command: sftp tc@[*ServerVM IP address*] and enter the password **netlab2020**

Q3. In the packet capture, can you see the username and password in cleartext? Explain

No, the packet is encrypted because the VM uses SSHv2.

Q4. What are the protocols used and destination port number? Explain

SSH protocol V2 and TCP

Destination port: 56862

Part 2

Apply the following ACL rules to the topology: (refer to IOS Commands Sheet 2)

1.- PC7 should not be able to ping the ServerVM

2.- PC1 should not be able to ping the ServerVM but PC2 should

3.- ClientVM can connect the ServerVM using SSH and SFTP but it cannot ftp

4.- PC8 cannot ping the ClientVM, but ClientVM can ping PC8

5.- R5 should not be able to ping the ServerVM

Sniff the traffic with Wireshark in all necessary links to verify your ACLs are working and the packets are being sent and/or dropped.

All captures have been uploaded.

Part 3

In the ClientVM open a web browser and try to open the ServerVM webserver. It should open without a problem. Add an ACL to block http traffic from CLientVM. Confirm with Wireshark. Q. In the packet capture, do you see the three-way handshake completed? Explain.

I am not able to see the three-way handshake. The traffic is denied and the request is timed out.

Save all your configurations and post the project on OneDrive. Do not forget to submit your Lab paper with your answers. All ACL must be in place for full credit.