CSE 4512 [Computer Networks Lab]

Lab Final

Instructions

- Complete individual steps of each task **exactly in the given order**. Don't jump between the steps. Failing to complete a previous step might result in *failure of the successive steps*. So, follow the order of steps exactly as given in the task description.
- There are steps where you need to take a screenshot. Those steps will start with [ss] at the beginning. Take the screenshot *right at that step* before completing the next steps. And attach that screenshot in the given *template doc*. **Don't keep it until the end** because you might not get the expected output.
- *Pay close attention to each instruction in the task*. Otherwise, you might end up with a faulty configuration. First read the instructions in a step and then start doing that step.
- You've been given a pre-configured .pkt file where the network topology and routings are already done for your convenience. **Don't change any configuration** unless it's needed to complete the task.
- Submit the **.pkt file** and the **answer template doc file** after completion of the exam. Name the .pkt file as "*ID-Lab-Final-Task.pkt*" and template doc as "*ID-Template-Final-Exam-Lab-Report-CSE-4512.docx*".

Background Scenario

You're Lames Bond. You've been hired by CIA to protect their super-secret infrastructure from 'bad' hands. But this time your assignment is not traditional like infiltrate into enemy territory or spy on someone. This time you'll protect their digital infrastructure in the Matrix of Packet Tracer. Be aware, this time your enemies are invisible and spooky too. You need to be very vigilant about how you complete your mission.

To assist you, CIA has provided explicit instructions that you need to follow exactly as specified or else you might fall in the abyss of darkness. So, let's take you to the doorstep. From there you've to venture on your own. And as always, you'll put your signature on every step of your adventure.

Good Luck, Agent Bond!

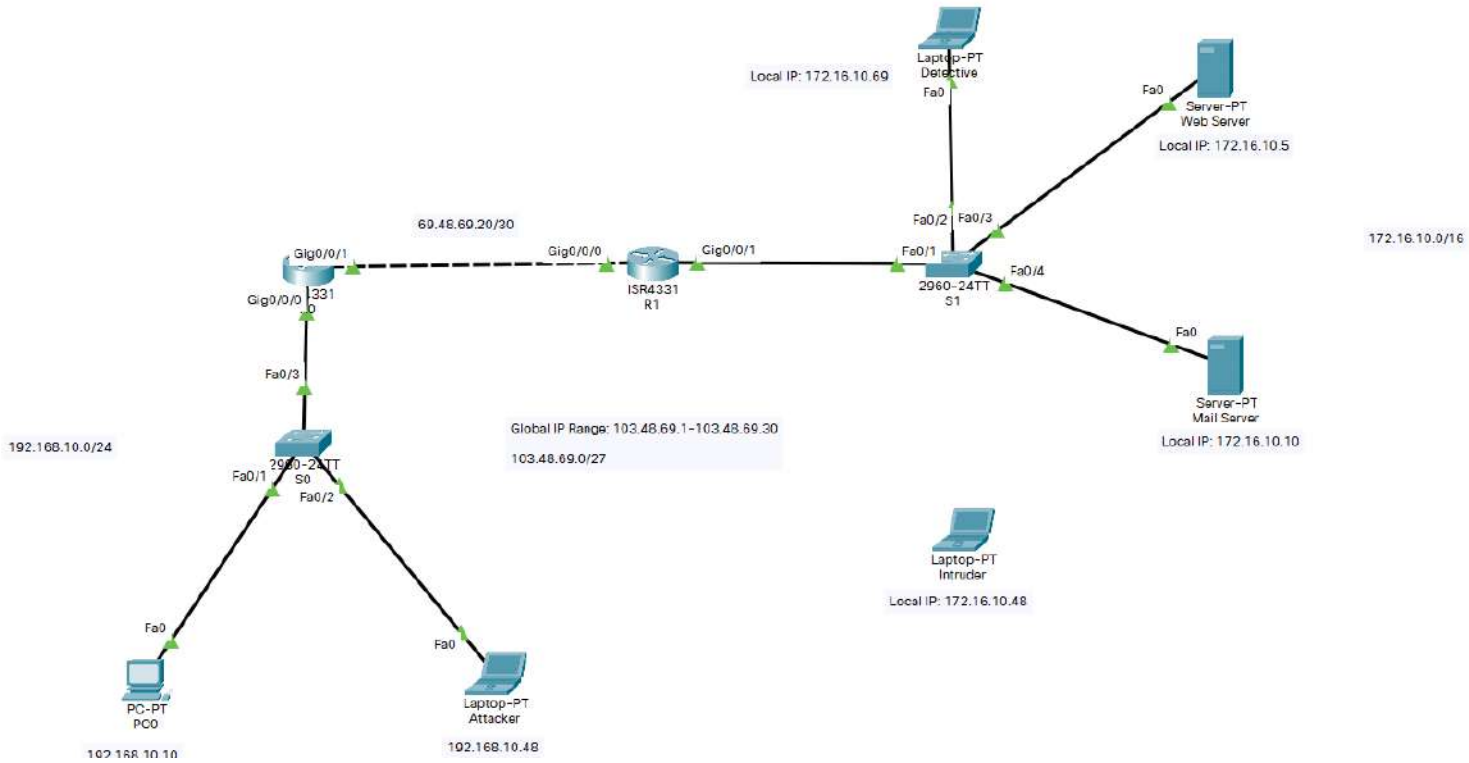

Figure 1:CIA Network

Task Description

Step 0:

- Rename the hostname of *R0, R1* and *S1* as *R0_XXX, R1_XXX* and *S1_XXX* respectively where *XXX* is the ***last 3 digits of your ID***.
- [ss] Ping *Web Server* from *PC0*. Take a screenshot of ping result and attach it in the doc. The ping should not be successful.

Step 1 (NAT):

In this step you'll have to configure **Network Address Translation (NAT)** on the *192.168.10.0/24* Network. Configure the NAT in such a way that the internal hosts will automatically get an IP from the dynamic address pool. Use the following information to configure NAT appropriately.

- The global IP range for the dynamic NAT will be from *103.48.69.1* upto *103.48.69.30*.
- Network for global IP is *103.48.69.0/27*. You can figure out the `netmask` from this.
- Name the nat pool as **Final_XXX** where *XXX* is the last *3 digits of your ID*.
- While defining access-list, *access_list_number* will be **XX** where *XX* is the last two digits of your ID.

- [ss] After you're done configuring NAT, ping the *Web Server* from *PC0*. The ping should work now. Now, take a screenshot of the ping result and attach it in the doc.
- [ss] Now, take screenshot of the output of command "**`show ip nat translations`**" right after the above ping is done and attach it in the doc.
- [ss] Then, ping *Mail Server* from *Attacker* laptop after configuring NAT. The ping should work. Take screenshot of ping result and attach in the doc.
- [ss] Now, take screenshot of the output of command "**`show ip nat translations`**" right after the above ping is done and attach it in the doc.

Step 2 (Switch Port Security):

Now's the time for action. As a first layer of defense, you'll enable **Switch Port Security** on S1. This will effectively block any unwanted device from accessing the super-secret CIA infrastructure. Follow the below steps for securing the S1 switch:

1. **Disable all unused ports**.
2. [ss] Take screenshot of the output of command **"show ip interface brief"** and attach it in the doc.
3. Configure port security on the port connected with *Web Server* so that it's the only allowed device on that port.
4. Configure port security on the port connected with *Mail Server* so that it's the only allowed device on that port.
5. Configure port security on the port connected with *Detective* laptop so that it's the only allowed device on that port.

6. Configure port security on the port connected with *R1* router so that router's MAC address will be saved to NVRAM after saving the running-config to startup-config.
7. [ss] Take screenshot of the output of command **"show port-security"** and attach it in the doc.
8. [ss] Take screenshot of the output of command **"show port-security address"** and attach it in the doc.
9. Remove *Detective* laptop and attach *Intruder* laptop on interface *fa0/2* of **S1** (use *Copper Straight-Through cabling*).
10. [ss] Ping *Web Server* from *Intruder* laptop. Take screenshot of whole topology after the ping and attach it in the doc.
11. [ss] Take screenshot of the output of command **"show port-security"** and attach it in the doc.
12. [**Must Do**] Remove *Intruder* laptop. Attach *Detective* laptop on *fa0/2*. Re-enable interface *fa0/2* by sequentially executing the following commands:

```
Switch(config)# interface fa0/2
  Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

Step 3 (SPAN):

Now that you've built the first defense, you want to analyze enemy footsteps so that you can understand them better. That's why you'll setup **Switch Port Analyzer (SPAN)** to monitor traffic on the port connected to your most important resource i.e., *Mail Server*. So, setup SPAN on *S1* for the port connected to *Mail Server*. Use the following information to configure SPAN accordingly.

- Mirrored traffic would go to the *Detective* laptop.
- The *session id* would be **XX** where *XX* is the last two digits of your ID.
- [ss] Take screenshot of the output of command **"show monitor"** after configuring SPAN and attach it in the doc.

Step 4 (ACL):

Great Agent Bond! You've finally found the hidden attacker that's been jeopardizing your entire secret infrastructure. Seems like that SPAN in the last step paid off. You figured out that the attacker is residing in the *103.48.69.0/27* network. To be extra-safe, you want to block the entire *103.48.69.0/27* network. So, define an **ACL** on **R1** by using the following information so that no device from the *103.48.69./27* network can access your super-secret network.

- The *access_list_number* would be **XX** where *XX* is the last two digits of your ID.
- Be careful while calculating the `wildcard mask`.
- Make sure that only the mentioned network is blocked and hosts from other networks can access the network. You don't want the CIA HQ from Langley to be denied access.
- [ss] Ping *Mail Server* from *Attacker* laptop. *Attacker* should not be able to ping *Mail Server* now. Take a screenshot of the ping result and attach it in the doc.
- [ss] Take screenshot of the output of command **"show access-lists"** and attach it in the doc.

*** Congrats Agent! You've successfully completed your mission by thwarting dangerous cyber attackers from damaging the super-secret CIA infrastructure. We'll be looking forward to working with you in more adventurous missions like this in future. Till then, au revoir! ***