Hands-on A1: Examine Data Breaches

In this exercise, the student studies some of the biggest data breaches using the following link then reports on the issues & impact associated with the case study you have chosen.

Open your web browser and enter the link (also the link available on the stream site):
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Click Hide Filter to display a visual graphic of the data breaches. Scroll down the page to view the data breaches. Note that the size of the breach is indicated by the size of the bubble. Click Read a bit more. Click to see the original report.

Select at least THREE data breaches, read about them (If necessary do a further research on the topic), and answer the following questions:

Deliverables [3 Marks]

Please hand-in a short report detailing:

1. What is the breach about, including the victim and impact of damage?
2. What was the method of leak (if necessary, consult to today's lecture note)?
3. Which technology could have prevented the leak (if necessary, consult to today's lecture note)?

Hands-on A2: Looking for vulnerabilities

The National Vulnerability Database (NVD) is one of the most well-known vulnerability repositories. NVD provides a lot of information relate to vulnerability discovered daily. In this exercise, the student uses the NVD search engine to find details of some of the recent vulnerabilities.

The NVD search engine is available at: https://web.nvd.nist.gov/view/vuln/search

The overview of CVSS is here: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Complete the following table according to the NVD information: (use CVSS version 3) and answer the following questions.

Deliverables [3 Marks]

Please hand-in a short report detailing:

1. Submit the completed table below.
2. Explain the meaning of CVSS base score, impact score, exploitability score, attack vector, attack complexity.
3. In your opinion, which vulnerability is most severe and why?

Environment	CVE identifier	Description of Summary	Date (dd/mm/yyyy)	CVSS base score	CVSS impact score	CVSS exploitability score	CVSS attack vector	CVSS attack complexity	Status of Fix
Apple	CVE-2020-6528								

Microsoft	CVE-2019-1111								
Huawei	CVE-2020-9102								
Google	CVE-2020-6527								
Facebook	CVE-2019-3563								

Hands-on A3: Setting up a simple firewall

Packet Tracer is one of the most popular network simulation tools that are used to simulate the feasibility of organisations' network configuration. In this exercise, the student learns the basic of setting up a firewall using the Packet Tracer. Your instructor will explain the details of how to use Packet Tracer.

For this exercise:

Create the 1st PC with an IP address: 192.168.1.1

Create the 2nd PC with an IP address: 192.168.1.2

A switch connects these two PCs.

Create a server with an IP address: 192.168.2.1

Set up a firewall (in the form of a router) that allows the host with IP address 192.168.1.1 to path through the organisation's firewall to send packets to the server with the IP address 192.168.2.1.

Use the router interfaces as following:

Gateway interface from the PCs: 192.168.1.254

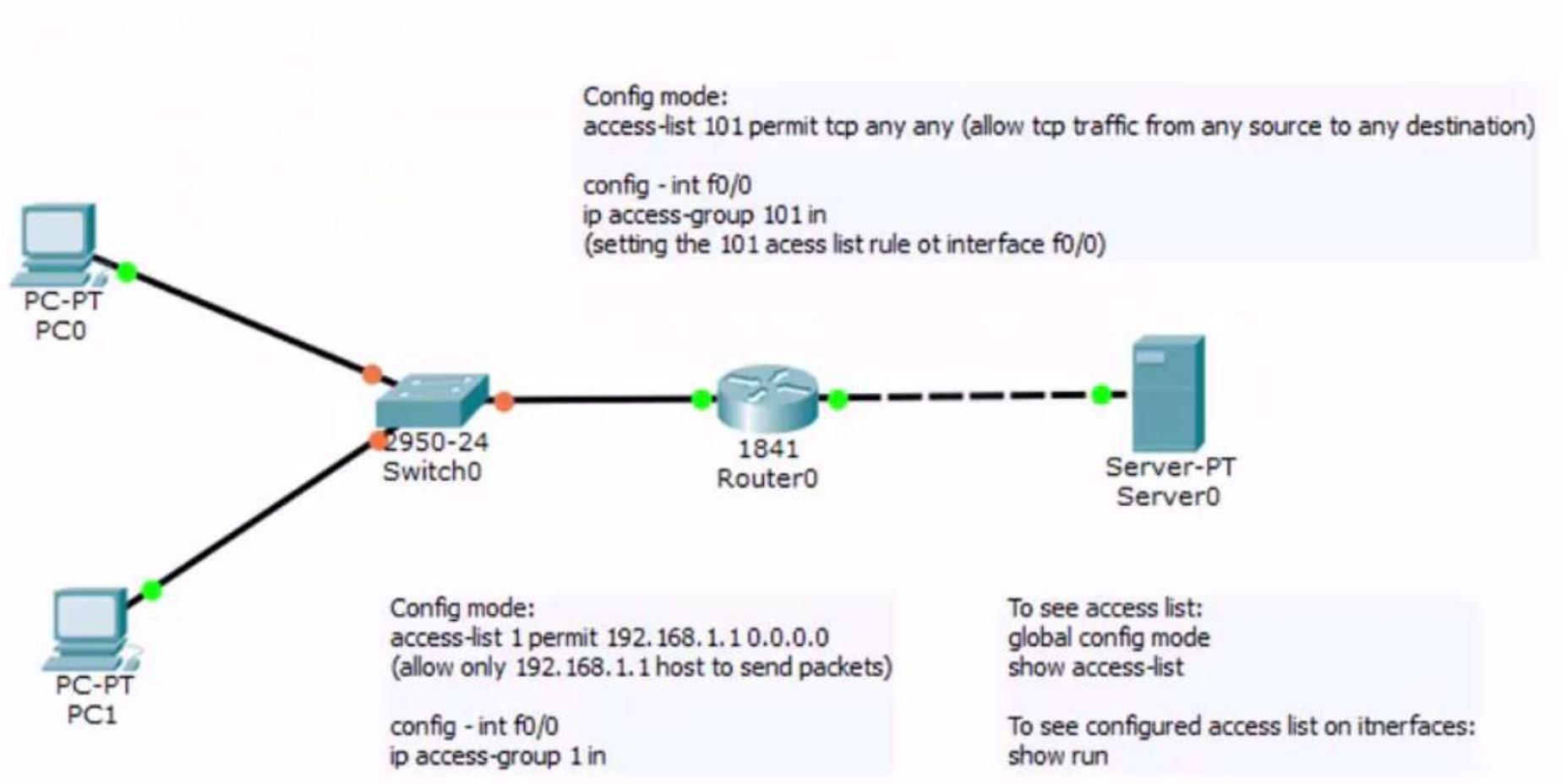
Gateway interface from the server: 192.168.2.254

Deliverables [4 Marks]

Please hand-in a short report detailing:

1. Describe what is a firewall (if necessary, consult to today's lecture note)?
2. What is the firewall trying to protect in this exercise?
3. Submit your packet tracer file.

PS: Your simulation should look like the below.


Config mode:
access-list 101 permit tcp any any (allow tcp traffic from any source to any destination)
config - int f0/0
ip access-group 101 in
(setting the 101 acess list rule ot interface f0/0)
PC-PT
PC0
2950-24
Switch0
1841
Router0
Server-PT
Server0
PC-PT
PC1
Config mode:
access-list 1 permit 192.168.1.1 0.0.0.0
(allow only 192.168.1.1 host to send packets)
config - int f0/0
ip access-group 1 in
To see access list:
global config mode
show access-list
To see configured access list on itnerfaces:
show run