INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD
FACULTY OF BASIC & APPLIED SCIENCES
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Online Mid Term Examination Spring Semester 2021

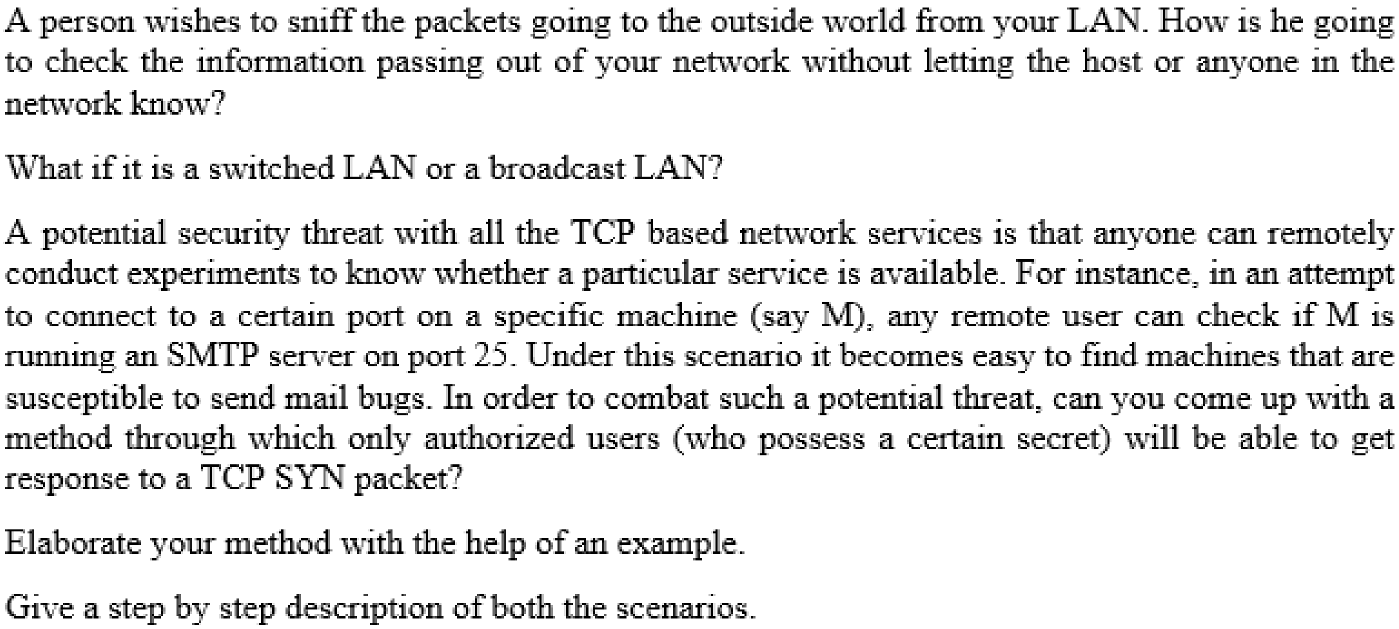
Course Title:	CS375 Information Security	**Batch:**	**BSCS F18 (A & B), BSIT F18**
Total Marks:	20	**Max Time Allowed:**	3 hours
Course Instructor:	Dr. Qaisar Javaid	**Date:**	12/4/2021

Instruction for Students:

Before starting your open book examination, please read all the given below instructions carefully, and must follow these instructions carefully.

1. Attempt all the questions by hand on white sheets.
2. Total time allowed for ***solving 1.5 Hours*** and for ***uploading 1.5 Hours*** manage accordingly.
3. Download the file IS_Midterm-Answer.docx file (File attached in the Midterm Activity in Google Classroom).
4. Type in your name and registration number on the first page of the word file in the space provided.
5. Take screens shots of the answer sheets.
6. Embed those screenshots in the file IS_Midterm-Answer.docx
7. Save the IS_Midterm-Answer.docx as pdf document.
8. Upload the IS_Midterm-Answer.pdf file on the link provided in the Google Classroom on the question paper. Submissions will only accepted in respective Google Form uploaded in Midterm Exam activity. ***No submissions will be accepted on personal emails, Google Classrooms, WhatsApp or any other social network***.
9. Make sure you have **2** pages in question paper including this one.
10. No extra time will be awarded for uploading answer-booklet manage accordingly.

Question 1: [10 points]



A person wishes to sniff the packets going to the outside world from your LAN. How is he going to check the information passing out of your network without letting the host or anyone in the network know?

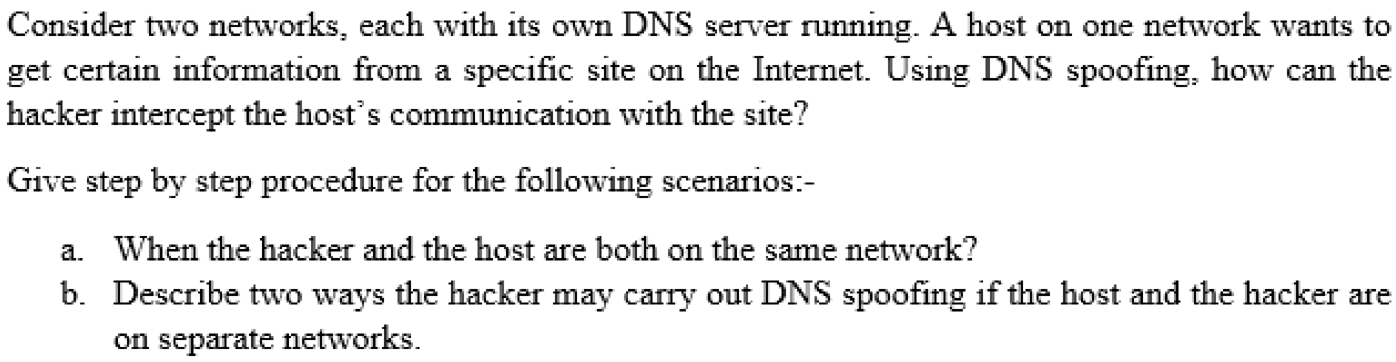
What if it is a switched LAN or a broadcast LAN?

A potential security threat with all the TCP based network services is that anyone can remotely conduct experiments to know whether a particular service is available. For instance, in an attempt to connect to a certain port on a specific machine (say M), any remote user can check if M is running an SMTP server on port 25. Under this scenario it becomes easy to find machines that are susceptible to send mail bugs. In order to combat such a potential threat, can you come up with a method through which only authorized users (who possess a certain secret) will be able to get response to a TCP SYN packet?

Elaborate your method with the help of an example.

Give a step by step description of both the scenarios.

Question 2: [10 points]



Consider two networks, each with its own DNS server running. A host on one network wants to get certain information from a specific site on the Internet. Using DNS spoofing, how can the hacker intercept the host's communication with the site?

Give step by step procedure for the following scenarios:-

a. When the hacker and the host are both on the same network?
b. Describe two ways the hacker may carry out DNS spoofing if the host and the hacker are on separate networks.

Good Luck ☺