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

Mid Term Examination Spring 2021

Course Title: Information Security	**Course Code: CS375**
Program: BSCS / BSIT	**Batch: BSCS F18 (A & B) BSIT F18**
Total Marks: 20	**Date & Time: 12-Apr-2021 (05:30pm till 08:30pm)**
Credit Hours: 03	**Teacher Name: Dr. Qaisar Javaid**

Q. No.	Marks Obtained
1	
2	
Mid-term Marks	

Student's Name: **Muhammad Abdullah Kamran**
Student's Registration Number: **4037-FBAS/BSCS4/F18(A)**

<u>Instructions for Students:</u>

Before starting your examination, please read and follow all the given below instructions carefully. You must affirm the honesty pledge given at the end:

1. Download the question paper titled as **"IS Question Paper.pdf" (pdf file)** and answer-sheet titled as **"IS_Answer-Booklet.docx" (MS Word document)** from the Google Classroom as per instructions of your teacher. You are required to write down the answers to each question in your own handwriting on neat white papers with blue pen.
2. **<u>Maximum time to download question paper, attempt and submit/ upload your answer sheets is 3 HOURS.</u>** As soon as you finish your paper, upload your answer booklet on priority basis.
3. You can only upload your exam response **ONCE.** You will be unable to re-upload an additional or amended version. If you fail to submit it within the due time, your paper will be considered canceled.

4. **How to submit(upload) your answer-booklet/paper**:

   After completing your answers, you need to:

   a. Mention your **Name**, **Registration Number**, **Page number** and **sign** each page of your handwritten answer-sheet.

b. Take pictures using mobile camera or Scan each page of your written answers /answer sheets via any scanning software (as guided in the video tutorial).

c. Insert all pictures or scanned images of your answer sheets into the **MS WORD** file titled as **“IS_Answer-Booklet.docx”** provided by the teacher in the Google Classroom.

d. After inserting all the images, save the **“IS_Answer-Booklet.docx”** file as a single PDF file **(Only PDF format is acceptable as your answer-booklet),** and upload it in the Google Forms (link of which is provided in the Google Classroom).

e. Please make sure you upload the correct document as you will not be able to change this, once it has been submitted.
(Please see the video tutorial regarding procedure to upload the examination responses, shared in the Google classroom and LMS, accessible on the link (https://lms.iiu.edu.pk/attempt-via-computer.mp4) for students using Computers for attempting Examination paper and on the link (https://lms.iiu.edu.pk/attempt-via-mobile.mp4) for students using mobile devices for attempting Examination paper).

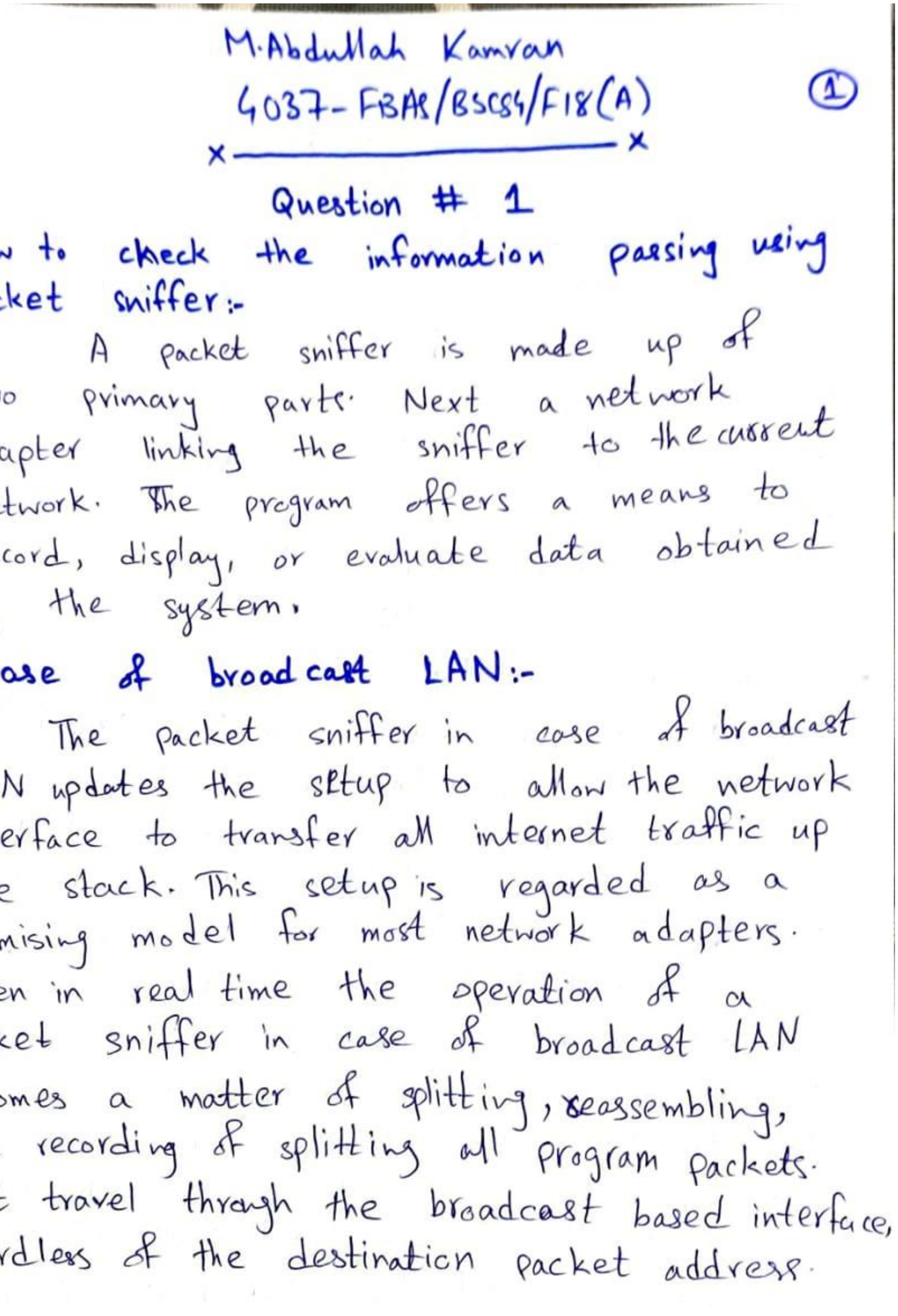
5. **The University views copying from one another's examination paper/ cheating, giving or receiving unpermitted aid, discussion/consultation, plagiarism, impersonation and submission of examination responses/answer sheets through the email IDs of other students as serious disciplinary offences, that fall under the category of Use of Unfair Means and will be dealt as per university rules for Unfair Means Control Committee (UMCC).**

6. Before you start the paper, you must agree to and sign the following pledge by clicking on the Student’s Affirmation check box **(it is mandatory to Tick the Checkbox):** (In case a student does not find the option to tick mark the checkbox, he/she can simply write down ‘Yes’ in the place of checkbox).

> ***“I hereby affirm that i) I shall solve this paper on my own and I shall not seek the help of any person(s) with any sort of aid (like telephonic/verbal help, attempted answers related to my examination etc.) while taking my paper, (ii) or will not provide assistance of any sort (verbal or written) to other fellow students. If I am found involved in i) cheating ii) impersonation, iii) or using plagiarized content in my writing, my case may be dealt as per university rules and procedures for using unfair means.”***

Student’s Affirmation: ☒

Q1.



M.Abdullah Kamran
4037-FBAS/BSCS4/F18(A) ①

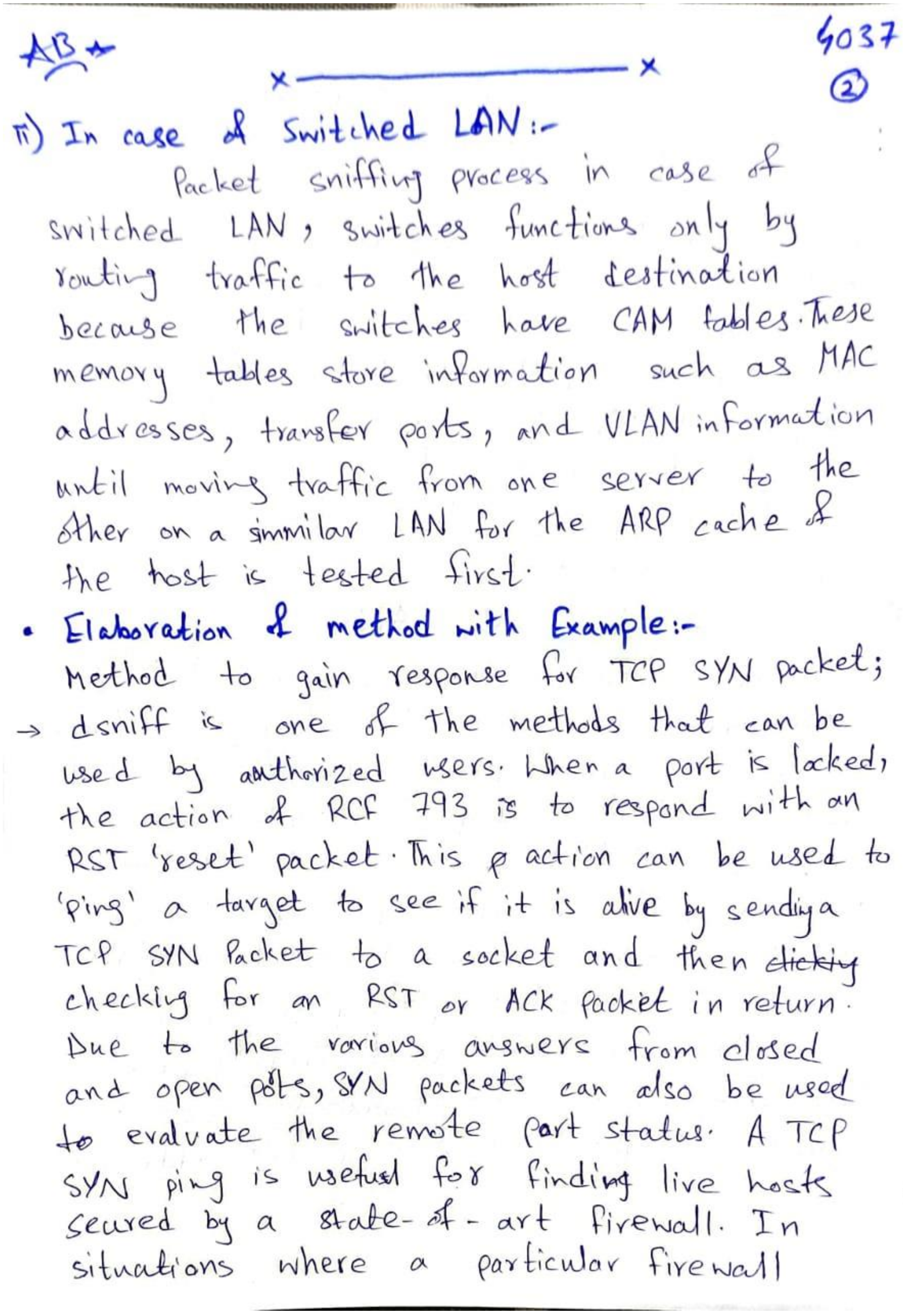
Question # 1

How to check the information passing using packet sniffer:-

A packet sniffer is made up of two primary parts. Next a network adapter linking the sniffer to the current network. The program offers a means to record, display, or evaluate data obtained by the system.

i) Case of broadcast LAN:-

The packet sniffer in case of broadcast LAN updates the setup to allow the network interface to transfer all internet traffic up the stack. This setup is regarded as a promising model for most network adapters. When in real time the operation of a packet sniffer in case of broadcast LAN becomes a matter of splitting, reassembling, and recording of splitting all program packets. that travel through the broadcast based interface, regardless of the destination packet address.



AB ★

4037

②

×————×

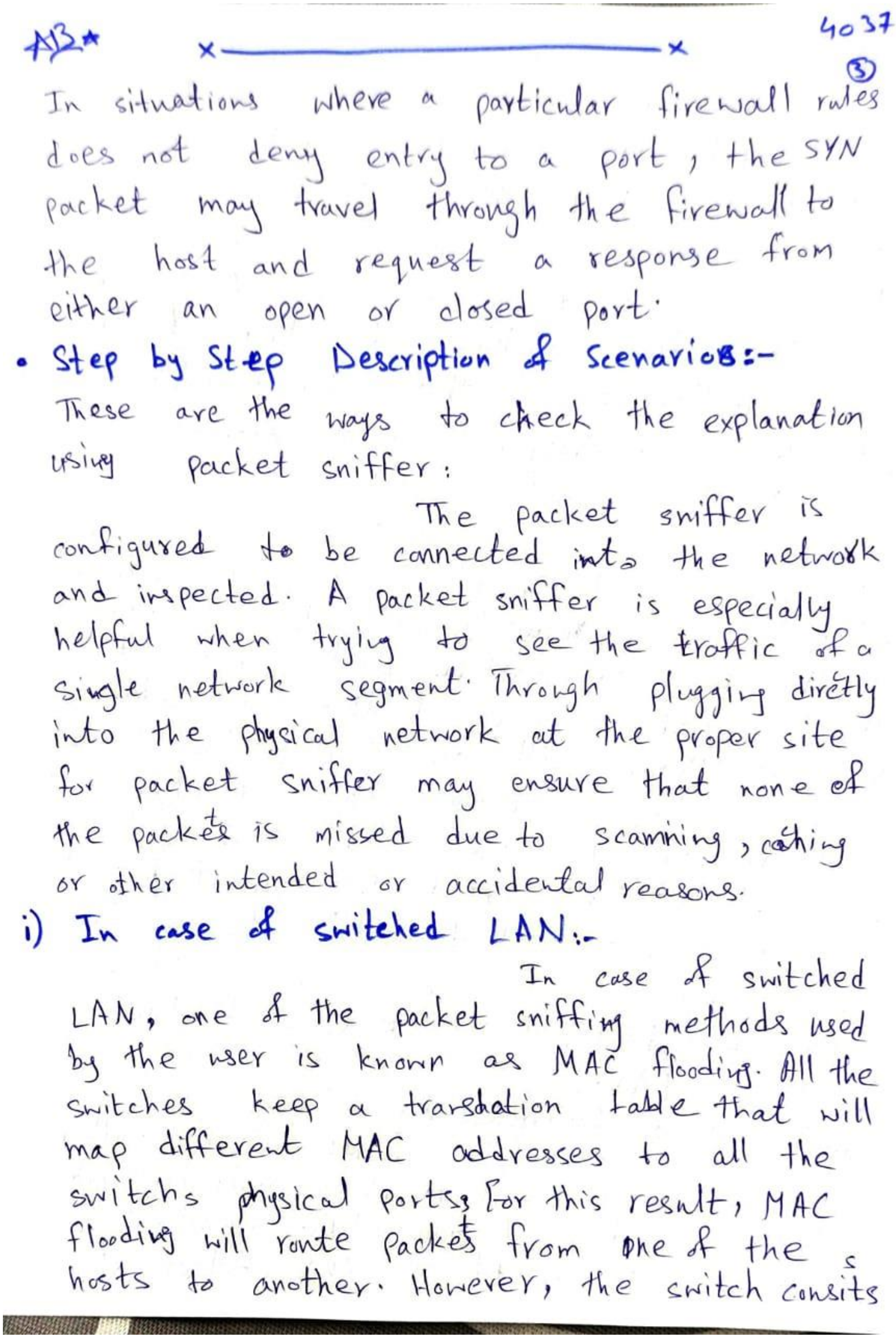
ii) In case of Switched LAN:-

Packet sniffing process in case of switched LAN, switches functions only by routing traffic to the host destination because the switches have CAM tables. These memory tables store information such as MAC addresses, transfer ports, and VLAN information until moving traffic from one server to the other on a simmilar LAN for the ARP cache of the host is tested first.

- Elaboration of method with Example:-

Method to gain response for TCP SYN packet;

→ dsniff is one of the methods that can be used by authorized users. When a port is locked, the action of RCF 793 is to respond with an RST 'reset' packet. This ~~p~~ action can be used to 'ping' a target to see if it is alive by sending a TCP SYN Packet to a socket and then ~~clicking~~ checking for an RST or ACK packet in return. Due to the various answers from closed and open ports, SYN packets can also be used to evaluate the remote part status. A TCP SYN ping is useful for finding live hosts secured by a state-of-art firewall. In situations where a particular firewall



A3*

4037

3

In situations where a particular firewall rules does not deny entry to a port, the SYN packet may travel through the firewall to the host and request a response from either an open or closed port.

- **Step by Step Description of Scenarios:-**

These are the ways to check the explanation using packet sniffer:

The packet sniffer is configured to be connected into the network and inspected. A packet sniffer is especially helpful when trying to see the traffic of a single network segment. Through plugging dirctly into the physical network at the proper site for packet sniffer may ensure that none of the packets is missed due to scanning, caching or other intended or accidental reasons.

i) In case of switched LAN:-

In case of switched LAN, one of the packet sniffing methods used by the user is known as MAC flooding. All the switches keep a translation table that will map different MAC addresses to all the switchs physical ports; For this result, MAC flooding will route packets from one of the hosts to another. However, the switch consists

AB.* x———————————x 4037

of a limited amount of memory fo bombardig (4) the switch that consists of fake MAC addreses till the switched LAN cannot sope up with the network process. Sometimes the user can use the arpwatch to moniter the ARP cache of the main machine to find out there is a duplication in the switched LAN. Sometimes the DHCP can trigger a false Alarm.

ii) In case of Broadcast LAN:-

In case of broadcast LAN majority of the people use the ping method to transfer ping requests with the IP address of the suspected machine which is part of the suspeted machime of the main address. None of them will see the packet because each of the broadcast LAN addapters will be rejected because it does not match the MAC address. However, if the suspected machine is operating a packet sniffer because it will not be bothering the rejected packers with different destination adresses of the broadcast LAN.

→dSniff method Explanation :-

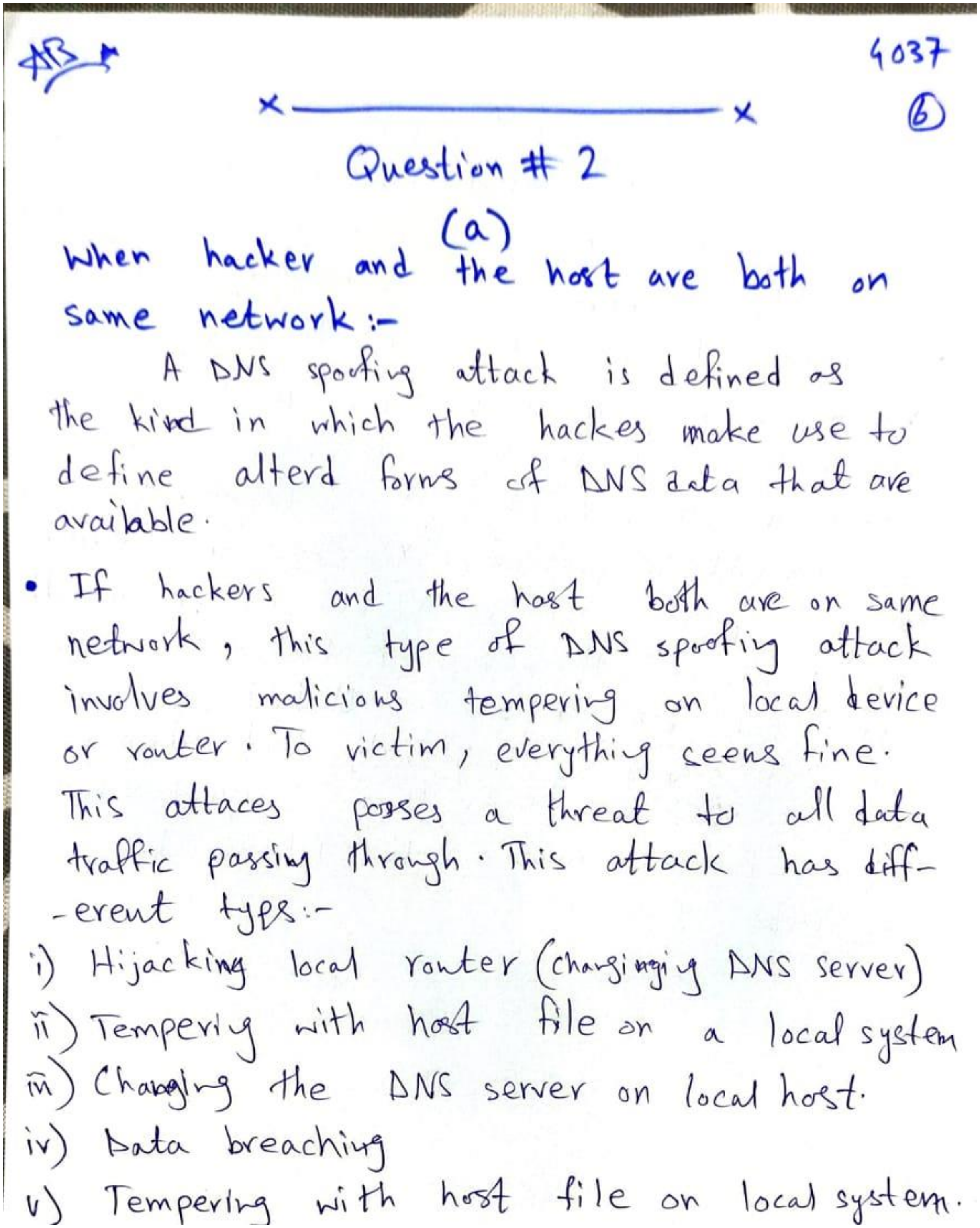
dsniff is the colletion of tools used for networking andicting which moniters confidential data like email, passwords. or other files. dSniff use SYN packets to

4037

5

to identify the remote port state. A TCP SYN ping is indeed useful for finding live hosts secured by a state-of-art firewall. In situations where a particular firewall rule doesnot restrict acces to a ports the SYN packet may travel via firewall to the host and request response either from a closed or open port. When a state-of-the-art firewall is present, SYN pings ar preffered to Ack pings since a state-of-art firewall usually drops all unsolicited ACK packets since dsniff not part of an established or new link. TCP SYN pings frequently fail when a stateless ACL or firewall is designed to protect the incomming packet buffer to the port.

Q2.



AB

4037

6

Question # 2

(a)

When hacker and the host are both on same network :-

A DNS spoofing attack is defined as the kind in which the hackes make use to define alterd forms of DNS data that are available.

- If hackers and the host both are on same network, this type of DNS spoofing attack involves malicious tempering on local device or router. To victim, everything seems fine. This attaces posses a threat to all data traffic passing through. This attack has different types:-

i) Hijacking local router (changinging DNS server)
ii) Tempering with host file on a local system
iii) Changing the DNS server on local host.
iv) Data breaching
v) Tempering with host file on local system.

AB *

4037
7

x———————x

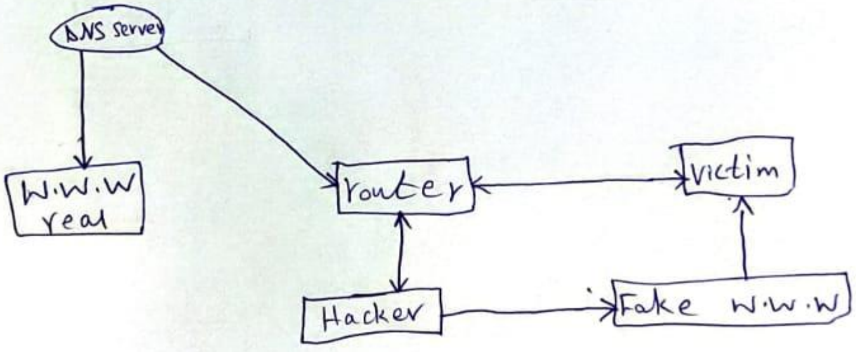
(b)

When hacker and host are on separate network :-

i) DNS spoofing is possible with an external network if attacker find victims DNS server, he may be able to poison cache there and control data traffic. This is also tricking the server into accepting a false IP address for a domain. The server places the malicious entry in its cache and begins to poison it.

Example:-

If victim and hacker are conneted via switches with different port with different will still route the packed even if it is still impossible that the router gets the packet from same interface.



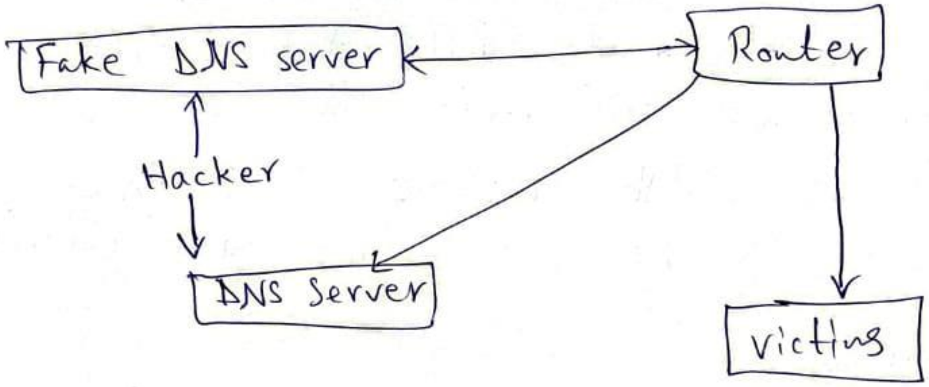
AB

4037
8

ii) Hatker can bombard victim with resolved queries form a previouely setup DNS server orfake DNS server whose queries are forgot. Hacker request to update a specific entry in victims DNS server.

Example :-

If victim and hacker ar conneted on or via switch with different parts. If hacker spoofs a network, the router will still lost the packets even if it is still impossible that router gets a packet from hacker.


Fake DNS server
Router
Hacker
DNS Server
victins