

Department of Data Science
Faculty of Computing and Information Technology
University of the Punjab

CC-403 Information Security **BSDSF22 Afternoon (Term Spring 25)** Student ID: _____

Quiz 02

Time: 12 mins

Marks: 10

Quiz will be cancelled if any student is found looking at his/her neighbor's paper or writing after the expired time.

QUESTION # 1

- A. What is a Trojan Horse? Give two examples of a Trojan. [2]
- B. What is `netdiscover` is used for, and how can we use it for passive as well as active information gathering. [2]
- C. Differentiate between CWE and CVE by giving one example of each. [2]
- D. Mention the `msfconsole` commands in sequence that you will use to perform a brute-force login on the Tomcat service running at port 8180 using `auxiliary/scanner/http/dir_scanner.rb` script on Metasploitable 2 machine. [2]
- E. In order to exploit the `vsftpd 2.3.4` service running on Metasploitable 2 machine. Describe the attack vector and show the set of shell commands you can practically use on Kali terminal to exploit this vulnerability. [2]