

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

CC-403 Information Security **BSCSF21 Morning (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 do you mean by Access control vulnerabilities? Mention its three types. [2]

B. Briefly differentiate between iterative and recursive DNS query by giving a command for each. [2]

C. Give the command to perform a TCP syn scan using `nmap`. Mention what happens behind the curtain. [2]

D. Mention the `msfconsole` commands in sequence that you will use to perform a scan by running `auxiliary/scanner/http/tomcat_mgr_login.rb` script on Metasploitable 2 machine. Assume you have `usernames.txt` file and `passwords.txt` file in the `pwd`. [2]

E. Precisely define a `meterpreter`. How do you differentiate it from a reverse TCP shell? [2]