Department of Computer Science

Faculty of Computing and Information Technology

University of the Punjab

CC-403 Information Security **BSCSF23 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. Precisely give the objectives of Scanning and Vulnerability Analysis. **[2]**

B. Differentiate between active and passive information gathering techniques, by giving three sample tools used in each type. **[2]**

C. Give commands to perform the following tasks: **[2]**

   a. Use `nmap` to perform a version scan on ports 20-50, 80 and 500-530 on a machine having IP address of 10.0.2.7

   b. Run a script named `special-script.nse` to perform a scan on Metasploitable 2 machine

D. Mention the names of the seven modules of Metasploit Framework and give a single line description of any two of them. **[2]**

E. You performed scans on your target machine and have come to know that it is running `vsftpd 2.3.4` service at port 21. Mention four different sources which you will check to find out if this service is vulnerable and if there exist an exploit for this vulnerable service. **[2]**