**Birla Institute of Technology & Science, Pilani**

**Work-Integrated Learning Programmes Division**

**Second Semester 2020-2021**

**Mid-Semester Test**

**(EC-2 Regular)**

Course No. : SS ZG575

Course Title : ETHICAL HACKING

Nature of Exam : Open Book

No. of Pages = 1

# No. of Questions = 6

Weightage : 30%

Duration : 2 Hours

Date of Exam : Saturday, 06/03/2021 (AN)

Note:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. What is Sniffing and how does sniffing work? How will you detect Sniffing? Names 3 popular tools used for Sniffing. [5]
5. What is vulnerability assessment? Describe the process of Vulnerability assessment. Name the two databases where you can find vulnerabilities of IT systems. [5]
6. What is Privilege Escalation and how does it work? Describe one method of privilege escalation you can use in Linux. [5]
7. Describe the structure of an Android App. How would you hack an Android App – explain with a tool example? [5]
8. Describe the Traceroute command along with various command options. How would you use Traceroute to create a network diagram of a target? [5]
9. Describe Nmap command in detail. How would you use Nmap to determine a vulnerable system or application in a target? [5]

\*\*\*\*\*\*\*