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

**Work-Integrated Learning Programmes Division**

**Second Semester 2020-2021**

**Comprehensive Examination**

**(EC-3 Regular)**

Course No. : SS ZG575

Course Title : ETHICAL HACKING

Nature of Exam : Open Book

Weightage : 50%

No. of Pages = 1

# No. of Questions = 8

Duration : 2 Hours

Date of Exam : Saturday, 01/05/2021 (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. You have been retained by an organization to analyze a security incident that occurred in their environment. The organization usage a DHCP for dynamically allocating IP addresses to the devices connecting to the network. One morning the network administrator found that their normal DHCP was inundated with connection requests and due to this a number of users connected to network through another DHCP server which had appeared suddenly. Explain:
   1. What actually happened to the original DHCP server? What is this attack called [3]
   2. How the attacker setup a secondary server which was able to convince user devices to connect to it? [3]
5. Describe step by step process to setup and use Kismet tool to exploit wi-fi activity around you? [8]
6. What is an Evil Twin Attack? Describe in detail the process of setting up an Evil Twin attack.

[6]

1. How does a VPN server work? Describe various different VPN protocols [6]
2. What is privilege escalation and types of privilege escalation? What are various methods of privilege escalation? [6]
3. You connected to a public wi-fi network offered by Starbucks Coffee at a public place. However after some time you realized that some of the mails you sent using Starbucks wi-fi network have been hacked. To your dismay, you found that there is no Starbucks outlet nearby the place you connected to the so called Starbucks wi-fi.

Describe what is this type of attack and how is this executed? [6]

1. In Apr 2020, Zoom video conferencing system was subjected to an attack called ZoomBombing. Describe in detail what is ZoomBombing and the safeguards for this attack? [6]
2. What is DNS enumeration process? Describe various techniques & tools used for DNS enumeration? [6]

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