Roll No: | | | | | | | | | | | | |

B. TECH
(SEM III) THEORY EXAMINATION 2020-21
COMPUTER SYSTEM SECURITY

Time: 3 Hours   *Total Marks: 100*

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1.   Attempt *all* questions in brief.   **2 x 10 = 20**

Q no.	Question	Marks	CO
a.	What are the roles of a) cypher and b) key in cryptography?	2	
b.	What are some of the advantages and limitations of UNIX?	2	
c.	What is a privilege and discuss any two secure architecture principles	2	
d.	What is SSL and how does it work?	2	
e.	Discuss two problems associated with using ptrace	2	
f.	What are covert channels and what are their disadvantages?	2	
g.	When changing effective user ids, distinguish between ways to drop privileges	2	
h.	Why would you recommend using DNSSEC?	2	
i.	What are the goals of confidentiality policies?	2	
j.	Explain advanced anti-XSS tools	2	

SECTION B

2.   Attempt any *three* of the following: **10 x 3 = 30**

a.	Define the logout process, its steps and potential problems. Also, define session hijacking and discuss steps to mitigate session-tokens theft.	10
b.	Define Network-based IDS. What are its strengths?	10
c.	Discuss a)SQL injection b)CSRF c)XSS d)Sessions e) Four HTTP auth Problems	10
d.	Define role-based access control its major properties and why would you use it?	10
e.	Discuss session fixation attacks, steps to perform an attack and how can it be prevented?	10

SECTION C

3.   Attempt any *one* part of the following: **10 x 1 = 10**

a.	Discuss how vulnerabilities can be exploited in web applications.	10
b.	Define identity-based access control. What are the problems associated with it?	10

4.   Attempt any *one* part of the following: **10 x 1 = 10**

a.	Discuss single vs public-key cryptography	10
b.	Define knark. What are its features and why is it used?	10

5.   Attempt any *one* part of the following: **10 x 1 = 10**

a.	Define any five of the LRK v4 trojans: ifconfig, login, ls, passwd, ps, rshd, syslogd	10
b.	Discuss any three digital signatures and what are the steps to use them in the real world?	10

6.   Attempt any *one* part of the following: **10 x 1 = 10**

a.	Discuss DoS attacks and briefly discuss various methods for mitigation of DoS attacks.	10
b.	Discuss any three Real-World Protocols and what are the steps to use them in the real world?	10

7.   Attempt any *one* part of the following: **10 x 1 = 10**

a.	Compare access control in Windows with the access control in UNIX	10
b.	What is DNS and how does it work?	10