Name: Enrolment No:	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2020

Course: Security in Mobile Computing **Semester: VIII**
Program: B.Tech CS with SPZ in Mobile Computing **Time 03 hrs.**
Course Code: CSIT 452 **Max. Marks: 100**

Instructions: Attempt all Questions

SECTION A

Instruction: Each of the following MCQ contains 2 Marks. **30*2 Marks**

1. Hackers cannot do which of the following after compromising your phone?
   a) Steal your information
   b) Rob your e-money
   c) Shoulder surfing
   d) Spying
2. DDoS in mobile systems wait for the owner of the _____ to trigger the attack.
   a) worms
   b) virus
   c) botnets
   d) programs
3. Mobile security is also known as _____
   a) OS Security
   b) Wireless security
   c) Cloud security
   d) Database security
4. _____ is the protection of smart-phones, phablets, tablets, and other portable tech-devices, & the networks to which they connect to, from threats & bugs.
   a) OS Security
   b) Database security
   c) Cloud security
   d) Mobile security
5. App permissions can cause trouble as some apps may secretly access your memory card or contact data.
   a) True
   b) False
6. Activate _____ when you're required it to use, otherwise turn it off for security purpose.
   a) Flash Light

b) App updates
c) Bluetooth
d) Rotation

7. Try not to keep _____ passwords, especially fingerprint for your smart-phone, because it can lead to physical hacking if you're not aware or asleep.
   a) Biometric
   b) PIN-based
   c) Alphanumeric
   d) Short
8. Which of the following tool is used for Blackjacking?
   a) BBAttacker
   b) BBProxy
   c) Blackburried
   d) BBJacking
9. BBProxy tool is used in which mobile OS?
   a) Android
   b) Symbian
   c) Raspberry
   d) Blackberry
10. Which of the following is not a security issue for PDAs?
    a) Password theft
    b) Data theft
    c) Reverse engineering
    d) Wireless vulnerability
11. Phishers often develop _____ websites for tricking users & filling their personal data.
    a) legitimate
    b) illegitimate
    c) genuine
    d) official
12. Which of the following type of data, phishers cannot steal from its target victims?
    a) bank details
    b) phone number
    c) passwords
    d) apps installed in the mobile
13. Algorithm-Based Phishing was developed in the year _____
    a) 1988
    b) 1989
    c) 1990
    d) 1991
14. Which among them has the strongest wireless security?
    a) WEP
    b) WPA

c) WPA2
d) WPA3

15. _____ is the central node of 802.11 wireless operations.
    a) WPA
    b) Access Point
    c) WAP
    d) Access Port
16. There are _____ types of wireless authentication modes.
    a) 2
    b) 3
    c) 4
    d) 5
17. Sniffing is also known as _____
    a) network-tapping
    b) wiretapping
    c) net-tapping
    d) wireless-tapping
18. Which of them is not an objective of sniffing for hackers?
    a) Fetching passwords
    b) Email texts
    c) Types of files transferred
    d) Geographic location of a user
19. Which of the following tech-concepts cannot be sniffed?
    a) Router configuration
    b) ISP details
    c) Email Traffic
    d) Web Traffic
20. Which of these is not a step followed by cyber-criminals in data breaching?
    a) Research and info-gathering
    b) Attack the system
    c) Fixing the bugs
    d) Exfiltration
21. What types of data are stolen by cyber-criminals in most of the cases?
    a) Data that will pay once sold
    b) Data that has no value
    c) Data like username and passwords only
    d) Data that is old
22. An attacker, who is an employee of your firm may _____ to know your system password.
    a) do peeping
    b) perform network jamming
    c) do shoulder surfing
    d) steal your laptop

23. ATM Skimmers are used to take your confidential data from your ATM cards.
    a) True
    b) False
24. _____ is the concept that tells us about the replacement of every alphabet by another alphabet and the entire series gets ‘shifted’ by some fixed quantity.
    a) Rolling Cipher
    b) Shift Cipher
    c) Playfair Cipher
    d) Block Cipher
25. _____ employs a text string as a key that is implemented to do a series of shifts on the plain-text.
    a) Vigenere Cipher
    b) Shift Cipher
    c) Playfair Cipher
    d) Block Cipher
26. In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.
    a) Block Cipher
    b) One-time pad
    c) Hash functions
    d) Vigenere Cipher
27. Password cracking in system hacking is of _____ types.
    a) 2
    b) 3
    c) 4
    d) 5
28. Which of the following is an example of passive online attack?
    a) Phishing
    b) Social Engineering
    c) Spamming
    d) Wire sniffing
29. Which of the following case comes under victims’ list of an active online attack?
    a) Strong password based accounts
    b) Unsecured HTTP users
    c) Open authentication points
    d) Logged in systems and services
30. _____ is a weakness that can be exploited by attackers.
    a) System with Virus
    b) System without firewall
    c) System with vulnerabilities
    d) System with a strong password

SECTION B

Instruction: Each of the following conventional questions carries 10. 10*4

Q.B.1 Explain and evaluate various web based and network based security threats in mobile security?

Q.B.2 Analyze various physical threats of stolen mobile devices.

Q.B.3 Elaborate various strategies for secure development in mobile computing.

Q.B.4 Analyze various cryptographic techniques used in mobile security

OR

Explain Hash function with a working example