B. E. (Comps) (sem -VII) (CBCGS)
(R-2016)
Advance System Security & Digital forensics

University of Mumbai
Examinations Summer 2022

Time: 2 hour 30 minutes   Max. Marks: 80

Q1.	Choose the correct option for following questions. All the Questions are compulsory and carry two marks each.
1.	The small, 1x1 pixel cookies implanted in banner ads are called:
Option A:	Devil Cookies
Option B:	Web scum
Option C:	Web bugs
Option D:	Backdoor
2.	How do you know if the information transmitted between the web browser and the web server is secured
Option A:	The browser usually displays a padlock icon, it may also display a green address
Option B:	A pop-up window with SSL information comes up but it may also display a green address bar.
Option C:	There is no way to know if their connection is secured
Option D:	The SSL Certificate is displayed every time a secure website is loaded
3.	Your organization has become worried about recent attempts to gain unauthorized access to the R&D facility. Therefore, you are asked to implement a system that will require individuals to present a password and enter a PIN at the security gate before gaining access. What is this type of system called?
Option A:	Authorization
Option B:	Authentication
Option C:	Two factor Associationn
Option D:	Three factor privacy
4.	The choice of whether to use low-overhead cryptography versus heavy-duty cryptography in a micropayment scheme represents a tradeoff between:
Option A:	Security and cost
Option B:	cost and performance
Option C:	security and convenience
Option D:	security, cost and performance
5.	Poorly designed social networking sites are especially vulnerable to
Option A:	Buffer overflow attacks
Option B:	SQL injection attacks
Option C:	Non-persistent cross-site scripting attacks
Option D:	Persistent cross-site scripting attacks
6.	What is the challenge from the network (MSC) to authenticate the SIM card?
Option A:	the random number generated by the MSC
Option B:	IMSI number generated by the MSC
Option C:	the sequence number
Option D:	the integrity check key generated by the MSC
7.	_____ has the worst wireless security encryption standard?
Option A:	WPA
Option B:	WEP
Option C:	WPA3
Option D:	WPA2

8.	A new way to process milk so that there is no fat in any cheese made from it, is covered under
Option A:	Patent
Option B:	Copyright
Option C:	Trade secret
Option D:	Trademark
9.	To transfer encrypted data from victim machine to forensic machine which tool is used.
Option A:	AEScat
Option B:	cryptcat
Option C:	md5cat
Option D:	netcat
10.	In many countries which of the following key principle used in evolution of computer crime laws
Option A:	All members of the United Nations have agreed to uniformly define and prosecute computer crime.
Option B:	Existing laws against embezzlement, fraud, and wiretapping cannot be applied to computer crime.
Option C:	The definition of property was extended to include electronic information.
Option D:	Unauthorized acquisition of computer-based information without the intent to resell is not a crime.

Q2	
A	**Solve any two** **(5 marks each)**
i.	Explain the difference between "live acquisition" and "post mortem acquisition".
ii.	Explain different Targeted malicious code
iii.	Explain in brief Account Harvesting.
B	**Solve any one** **(10 marks each)**
i.	Explain with diagram Federated Identity Management.
ii.	How do phishing and pharming attacks take place? Discuss different solutions to avoid phishing and pharming attack?.

Q3	
A	**Solve any two** **(5 marks each)**
i.	List the Unix operating system vulnerabilities
ii.	Differentiate between DAC and MAC models.
iii.	Discuss the first generation of wireless security
B	**Solve any one** **(10 marks each)**
i.	Explain Linearization attack with example.
ii.	Explain how security is provided in UMTS.

Q4	
A	**Solve any two** **(5 marks each)**
i.	Write short note on Windows Registry.
ii.	Compare and contrast copyright and patent
iii.	Explain how Defense in Depth security strategy is used to stop advanced cyber attacks.
B	**Solve any one** **(10 marks each)**
i.	Discuss ethical and legal issues in computer security.
ii.	Explain volatile data collection procedure for Unix system.