22	IO4	j	j1				
23	IO3	m	m2				
24	IO3	m	m2				
25	IO4	j	j1				
26	IO4	j	j2				
27	IO3	m	m2				
28a/b	IO3	m	m2				
29a/b	IO4	j	j1				
30a/b	IO4	j	j1				
31a/b	IO4	j	j2				
32a/b	IO3	m	m2				

OUTCOMES

MET	NOT MET

Staff Signature with date

Part – B (Answer any 5 questions) (5 x 4 = 20 Marks)

21. What is a security audit? What are the kinds of security audit?
22. What are the components of EISP?
23. Business continuity planning has broader scope than Incident Response Plan?
24. What are the types of penetration tests?
25. How to create a forensic copy?
26. What are the tamper resistant and privacy enhanced technologies?
27. Justify why asset management is essential for an organisation.

Part – C (Answer all the questions)(5 x 12 = 60 Marks)

28a. Explain in detail about Incident Response Plan?

[OR]

28b. Explain in detail about ROI on security.

29a. What do you mean by Security Domain? Briefly explain .

[OR]

29b. Why web system security plays an important role in today's day to day activity? Justify your views.

30a. Define attack? What are the types of attack?

[OR]

30b. Explain buffer overflow attack and its types? How to mitigate buffer overflow attack?

31a. Describe threat modelling in detail.

[OR]

31b. Discuss in detail about the various possible vulnerabilities in an organisation.

32a. Explain Cost – Benefit analysis method in detail

[OR]

32b. How computer investigation and Forensics is done in real time?

SRM University, Kattankulathur

Faculty of Engineering and Technology, Department of Information Technology

IT1021- INFORMATION ASSURANCE AND SECURITY

Cycle Test -2

Degree	: B.Tech	Specialisation: IT	
Year/Sem	: IV/7TH	Date	:26/10/2017
Duration	: 3hrs	Max Marks	: 100

Part – A (Answer all the following) (1 x20 = 20 Marks)

1.The person or group who develops strategies for incident response includes:

a.CISO b.CRO c.IRT d.IMT

2. Goals should be broken down to sub-goals as it

a. expedites system design
b. provides a convenient target to aim at during system design
c. is recommended by experienced analysts
d. is good idea to use

3. You are developing an Incident Response Plan. An executive order is that the network shall remain up, and intruders are to be pursued. Your first step is to…

a. Use commands off the local disk to record what is in memory
b. Use commands off of a memory stick to record what is in memory
c. Find a witness and log times of events
d. Call your manager and a lawyer in that order

4. During feasibility analysis it is necessary to examine several alternative solutions because

(i)a comparison of alternatives will lead to a cost-effective solution
(ii)a pre-conceived single solution may turn out to be unimplementable
(iii)it is always good to examine alternatives
(iv)management normally looks at alternatives

a. i and iii b. i and iv c. i and ii d. ii and iv

5. A cost-benefit analysis is performed to assess

a. economic feasibility b. operational feasibility
c. technical feasibility d. all of the above

6. The primary objective of cost-benefit analysis is

a. to find out direct and indirect cost of developing the information system
b. to determine the tangible benefits of the information system
c. to determine if it is economically worthwhile to invest in developing the information system
d. to determine the intangible benefits of the information system

7.A cost benefit analysis consists of

(i)finding the direct and indirect cost of developing, implementing and running the system
(ii)finding out the tangible and intangible benefit of the system
(iii)finding the investment to be made in the system
(iv)finding the profit which will accrue from the system

a. iii and iv b. i and iv c. ii and iii d. i and ii

8. A _____ is anything that can cause
a)Vulnerability b) threat c) spoof d)

9. A _____ is a small program embedded inside of a GIF image.
a)web bug. b cookie. c)spyware application. d)spam

10. A hacker contacts you my phone or email and attempts to acquire your password.
a)Spoofing b) phishing c) spamming d) bugging

11. The most important parts of a feasibility report are
(i)cost-benefit analysis
(ii)statement of the objective of the proposed system
(iii)who will supply equipment for implementing the system
(iv)organizational changes needed to successfully implement the system
a. i and ii b. i, ii and iii c. i and iv d. i, ii and iv

12. A potential violation of security is called _____
a) Attack b) threat c) risk d) vulnerability

13._____attacks are very difficult to detect.
a) active b) passive c) DOS d) replay

14. The PRIMARY reason for Triage is:
a. To coordinate limited resources
b. To disinfect a compromised system
c. To determine the reasons for the incident
d. To detect an incident

15. The types of buffer overflow are_____ and _____ based.
a.)Stack and heap b) static and dynamic c) text and data d) DoS and DDoS

16. What is NOT TRUE about forensic disk copies?
a. The first step in a copy is to calculate the message digest
b. Extraction and analysis for presentation in court should always occur on the original disk
c. Normalization is a forensics stage which converts raw data to an understood format
d. Forensic copies requires a bit-by-bit copy

17. Active attacks affect the _____of data.
a) Availability b. Integrity c. Authenticity d. Both a and b

18. A weakness in some aspect or feature of a system that makes a threat possible.
a) threat b) attack c) vulnerability d) exploit

19. In what scale the threats are rated in DREAD model.
a) 1-10 b) 1-5 c) 1-15 d) 1-20

20. Threat modelling is a _____process in an organisation.
a) Iterative b) static c) dynamic d) repetitive