Hall Ticket Number:

Code No. : 13110 IUBP

VASAVI COLLEGE OF ENGINEERING (Autonomous), HYDERABAD
B.E. (CBCS) III-Semester Main Examinations, December-2017

Internet Usage Best Practices

Time: 3 hours   Max. Marks: 70

Note: Answer ALL questions in Part-A and any FIVE from Part-B

Part-A (10 × 2 = 20 Marks)

1. Sarbanes-Oxley Act (SOX) is concerned with Information Integrity Regulations. Define them.

2. Draw a neat diagram to illustrate the working of a DMZ.

3. Define the 3 types of Viruses?

4. How do we prevent from Information Threat? Give a common approach adopted for preventing this.

5. Differentiate Monitoring vs Audit in the perspective of countermeasures.

6. Define the role of Post Incident Analysis.

7. Who are WhistelBlowers (WBS)? What is their relation with Espionage? Name one WBS.

8. List the Mobile malware that have infected the iOS and Android in 2016.

9. Define Zero day attack and give an example of it.

10. Define a DoS attack and differentiate this with DDoS.

Part-B (5 × 10 = 50 Marks)

11. a) Human Resources and Workplace Issues are a integral part of any Business. Explain the steps to be implemented to address these.   [4]

    b) Email and Spam management are one of the most common inbound threats. Describe how Spam Filtering is done on the Network.   [6]

12. a) Differentiate between the following Attacks : Phishing, Vishing, SMSing, Smear Phishing? Give examples for each one of them.   [4]

    b) Give the structure and functions of countermeasures to defend against internet threats.   [6]

13. a) Elaborate on the various tasks that must be performed to MAINTAIN a variety of countermeasures.   [4]

    b) Information loss is possible through growing threats in the internet. List the concerns and describe how on Nimda, Code Red were successful in achieving this?   [6]

14. a) Assume a company "Primus Software" has a new application development project,   [5]
    with projected revenues of $1,200,000. Using the following table, calculate the ARO
    and ALE for each threat category that "Primus Software" faces for this project.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per six months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year

   b) Assume a year has passed and XYZ has improved security by applying a number of   [5]
   controls. Using the information from the above table and the following table,
   calculate the post-control ARO and ALE for each threat category listed

Threat Category	Cost per Incident	Frequency of Occurrence	Cost of Control	Type of Control
Programmer mistakes	$5,000	1 per month	$20,000	Training
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security
Web defacement	$500	1 per quarter	$10,000	Firewall
Theft of equipment	$5,000	1 per 2 years	$15,000	Physical security

15. a) "Non-Malware's are a greater threat for organizations". Justify the following   [4]
    statement by taking the examples of KRACK, Heartbleed?

   b) In addition to firewalls, boundary routers and other devices that are appearing in the   [6]
   near perimeters, define the new complex network measures.

16. a) What can organizations do to protect themselves in the purview of Intellectual   [4]
    Property rights/Industry Espionage

   b) Determine the steps that address the challenges associated with Mobile devices   [6]

17. Answer any *two* of the following:
    a) Explain some of the well known authorities which look after the privacy regulations?   [5]
    b) List the specific Outbound threats present in any business organization.   [5]
    c) How can content on corporate and government networks be categorized into?   [5]
       Explain the future of content protection

CRCRCRSRSRSRS