ABU DHABI POLYTECHNIC

Information Security Engineering Technology Department

NCS-420 – Incident Handling and Response

Final Examination

Summer Semester 17-18

Exam Time: 2 hours

Instructor *Asad Raza*

Students answer on the question paper
Calculators, drawing kits and dictionaries are allowed
No additional materials are required

STUDENT NAME										
STUDENT NUMBER										
CRN	1	9	5	4	DEPARTMENT	**ISET**				

READ THESE INSTRUCTIONS CAREFULLY

Write your *name*, *number*, *CRN* and department **clearly** in the boxes above.

Answer **all** questions.

Show **all** your work, and use appropriate **units.** Otherwise, you may lose marks.

Answers not **clearly readable**, if any, will not be marked.

This exam consists of **4 parts** in 6 **pages**.

Question	Score	Outcome
1	/40	1-4
2	/10	5
3	/20	4,5
4	/30	3,6,7
Total	**/100**	

All mobile devices are not allowed during examination.

Abu Dhabi Polytechnic considers cheating or attempting to cheat a serious offense that will result in disciplinary action taken against involved individuals.

Abu Dhabi Polytechnic
Information Security Engineering Technology Department
NCS-420 Incident Handling and Response (CRN: 1954)
Final Exam
Instructor: *Asad Raza* Date: 25/6/2018 Exam Duration: 2 hours

Instructions

- This exam has 4 (Four) Parts. You are required to attempt all sections of all questions.
- Provide all the required components for full credit.
- Although not required, you may only use a simple and standard calculator.

Part 1: Fill in the correct answer(s) for each of the following questions (2 points each) [40 points]

1	2	3	4	5	6	7	8	9	10
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**

1. Which of the following TWO represents protect and forget response philosophy
    a. Focus on detection and logging
    b. Focus on identifying and apprehending the intruder
    c. Focus on preserving potential evidence for prosecution
    d. Focus on analysis of events to recover and prevent recurrence

2. The primary purpose of _____ phase is to limit the damage and prevent any further damage from happening.
    a. Preparing
    b. Containment
    c. Eradication
    d. Recovery
3. Which of the following terms describes the term "preventing concurrent recurrence" in eradication phase
    a. Preventing the occurrence of an incident
    b. Preventing the incident from happening again in future
    c. Preventing the occurrence of another similar incident in parallel to the first incident
    d. Preventing the incident of another different incident in parallel to the first incident
4. Which of the following statements BEST describe the primary objective Recovery phase
    a. Re-establishment of pre-incident status of all organization systems
    b. Re-establishment of some of the core organization systems
    c. Recovering the data from affected systems

d. Bring affected systems back into the production environment

5. Probing for the initial estimate of defensive state of networks and system is known as _____
    a. Fingerprinting
    b. Foot printing
    c. Reconnaissance
    d. Doorknob rattling
6. An event that triggers alarm and causes a false positive is known as
    a. Alert or Alarm
    b. False positive Alarm
    c. False Attack Stimulus
    d. False Negative Stimulus
7. Which of the following is Most rigorous, but also very risky testing methodology
    a. Parallel Testing
    b. Full interruption
    c. War Gaming
    d. Structured Walk-through
8. Which of the following types of users require more personalized type of incident response training
    a. Managers
    b. Technical Users
    c. Customers
    d. IT Staff
9. _____ is the third step of Incident Response Lifecycle.
    a. Detection
    b. Eradication
    c. Containment
    d. Recovery
10. Incident response _____is the anchor of an entire incident response effort.
    a. Manager
    b. Policy
    c. Procedure
    d. Team
11. Which one of the following is part of the second phase of Incident Response Lifecycle?
    a. Incident response policy
    b. Keep incident from spreading
    c. Postmortem analysis
    d. Log files
12. _____require(s) development of a variety of incident scenarios.
    a. Incident handling policy
    b. Mock exercises
    c. Business resumption
    d. Incident identification
13. Support for prosecution activity is generated in the _____ phase of Incident Response.
    a. Eradication
    b. Detection

c. Containment
d. Follow up

14. Benefits of having mock exercises in an organization include _____.
    a. Validation of procedures
    b. Practice makes perfect
    c. Record critical data and evaluate
    d. All of the above
15. Re-evaluation/modifying procedures on basis of lessons learned takes place in _____ phase.
    a. Recovery
    b. Preparation
    c. Follow up
    d. Detection
16. Profitability areas must be considered before taking extreme actions
    a. True
    b. False
17. The primary objective of any incident response strategy is to identify the attacking host.
    a. True
    b. False
18. Loss of availability is a NOT probable type if incident indicator
    a. True
    b. False
19. Incident Response procedures are preventive controls, not reactive measures.
    a. True
    b. False
20. The overall cost of the preventive maintenance action must be less than the overall cost of a corrective action.
    a. True
    b. False

Part 2: Match the following questions [10 Marks]

Incident Type	Match
1. Violation of Law	
2. Activates at unexpected time	
3. Unusual consumption of computing resources	
4. Adjusting for true noise	
5. Should be conducted at regular interval	

A. Definite indicator
B. Probable indicator
C. Possible Indicator
D. Tuning
E. Mock Exercise
F. Incident Handling

Part 3: Short Questions: Write short answers to the following questions (10 points each) [20 points]

Question 1)

What is the difference between an event, adverse event and incident? Briefly discuss the six stages in Incident Response life cycle?

Question 2)

During planning phase before the incident there are different testing methodologies that can be adopted by the IR team to make sure that there IR plan has no gaps. Discuss any 4 of these testing methodologies.

Part 3: Analyze the Scenario and answer the following questions. [30 points]

Scenario 1

You have been recently hired as a team leader of CSIRT (Computer Security Incident Response Team) in a government organization which is providing very important e-services to the UAE residents. On Thursday around 3 pm you started getting phone calls from staff who is working. They couldn't open some of the files they used daily that resided on a central server. Everyone is complaining that when they try to open the files they get a message that they need to pay 1000 $ if they want to access the files otherwise they will lose the files for ever. These files contain a lot of personal information and billing information about the customers and the organization cannot afford to lose these files.

Question 1) Being a team leader and keeping in view the incident describe your strategy for (10 Marks)

- Before this incident
- During this incident
- After this incident

Scenario 2

You are working in Abu Dhabi Commercial Bank (ADCB) as an Incident Response Specialist. The management has decided to outsource Incident handling to an MSSP (Managed Security Service provider), Dark Matter. You have to convince your management not to outsource incident handling.

Question 2) Write down the arguments that you will use to prevent this outsourcing. (10 Marks)

Scenario 3

Helpdesk operator Julie has been especially busy this morning. Aside from the normal calls she has received numerous complaints from one of the traveling salespeople (Frank) who just has returned

from being in the field. Frank logged several complaints saying that his computer system is not working properly. As an incident response technical expert you have been assigned to investigate this issue.
Frank explains that this morning he logged in the system and installed a stock exchange application. The application gave him a message that the system will be rebooted several times during the installation. So he went off and had a cup of coffee and checked with coworkers on latest news. Upon return to his computer it appeared to be done with its program but "acted" weird during the morning. Sometimes it would beep and sometimes the cd tray would eject and sometimes the system would show a blue screen of death.

Question 3) After listening to frank about the problems, what will be your course of actions in terms of eradication? (2 Marks)

Question 4) Did Frank violate any organizational policy, if yes then which one? (1 Marks)

Question 5) How can you make sure to prevent such incidents in future? (2 Marks)