EXAM CYBER SECURITY MANAGEMENT 201500018/201500041

FEBRUARY 1, 2018; 13.30H -16.30H

- This exam contains 23 questions for a total of 74 points.
- The case description at the beginning of the exam applies to multiple questions.
- Please answer in ENGLISH
- We wish you good luck!

Case description

The densely populated country Atlantis lies below sea level. To protect its citizens from a flood, the country's government has invested in the Zeta works. This is a set of construction works, including dams, flood barriers, dykes and storm surge barriers that are used to control the level of sea water in Atlantis' rivers, canals, and other waterway infrastructure. Each of the Zeta works has an office building a few km away from it, which hosts a control room for the SCADA system responsible for controlling that Zeta work. Each office also hosts 2 system administrators who are responsible for all things IT-related. The offices use up-to-date software, while the waterworks still have legacy systems, developed by third party companies, to ensure operational continuity. The waterworks themselves have full time staff controlling the access gates. Employees are required to wear protective clothing, an ID badge, and need an appointment to enter the facility. The Zeta Commission is a group of experts commissioned by the government to oversee the Zeta works.

Governance and Risk Management

1. **(4 points)** How is the information security governance of the Zeta works best organized and why? Complete the table below by filling in the roles and responsibilities (1 point per correct role, 4 in total)

Roles	**Responsibilities**
	Accountability, high-level understanding of risk, endorsement, alignment with the Zeta works' objectives
	Sounding board of affected stakeholders, ensuring alignment of information security with the business objectives and culture
	Day-to-day operations supporting the implementation of information security governance
	Creation and effectiveness of information security program, establishing communication channels and obtaining senior management commitment

2. **(3 points)** Describe 3 improvements for the Zeta works in organizing their third-party risk management related to cyber security. Include (a) people, (b) processes, and (c) technology in your answer (3 points in total: 1 point per a, b, c)
3. Risk management often starts by categorizing known or expected risks in terms of likelihood and impact.
    a. **(1 point)** Give an example of a highly likely, low impact risk that might strike Zeta works.
    b. **(1 point)** Give an example of an unlikely, high impact risk that might strike Zeta works.
    c. **(1 point)** Given your knowledge of cyber risk management, if you only had budget to implement security countermeasures against one of these risks, which would you choose, and why?

Industrial Control Systems (ICS)

4. **(3 points)** The Purdue Model for Control Hierarchy describes a notion of 5 levels of hierarchy in the ICS architecture concept. Enumerate all levels. For each, explain its role and which components can be found at this level.
5. **(3 points)** Describe why there is a need to connect IT with OT (Operational Technology). Describe what a DMZ is, how it changes the traffic flow and what components can be found there.
6. **(4 points)** A new RCE exploit in SMB is published with Proof of Concept code which affects nearly all Windows versions since XP. The Zeta Commission asks you for your view on your proposed patching/mitigation strategy for the SCADA systems (L3-L1). Also, describe any constraints, priorities and assumptions you make.

Physical and Social Security

7. **(2 points)** When is the right time to do Open Source Intelligence and overall reconnaissance?
8. **(2 points)** Which measures would you advise Zeta take to improve their resilience against these types of reconnaissance? Name two.
9. **(2 points)** What is the difference between penetration testing and red teaming? Name at least two differences and their consequences for a business that is commissioning a test.
10. **(2 points)** Explain the human condition and the “Parent, Adult, Child” relationship. How does this apply to Social Engineering?

Monitoring and Detection

11. After much lobbying by the security manager, the Zeta Commission has finally agreed to invest in an in-house cyber security monitoring capability. They have asked you to make a plan for setting it up. Based on the case description and your knowledge of security monitoring:
    a. (1 point) Which part of the IT landscape would you start monitoring first, and why?
    b. (4 points) For this part of the landscape, which data would you want to ingest, and for which anomalies would you monitor? Give two example use cases, e.g. for external and internal threats.
    c. **(1 point)** Would you (first) use a HIDS or a NIDS setup, and why?
    d. (2 points) How would you set up the SOC? Specifically, where would you locate it (centrally in Atlantis, in the capitol of Atlantis, offshore it to India, etc.), and how would you staff it (business hours, 24/7, redundant staffing, etc.)? What are the pros and cons of your approach?

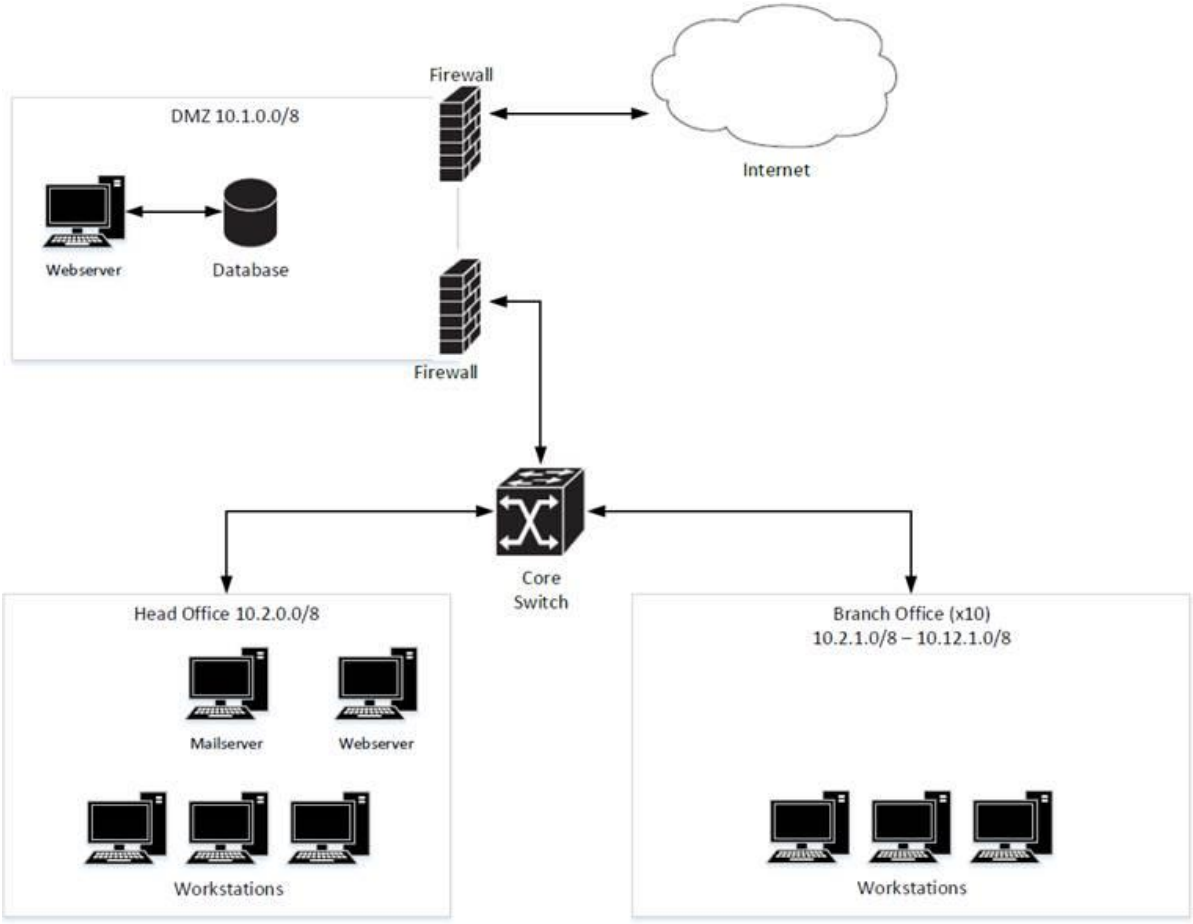
e. **(1 point)** Would your SOC use a SIEM? If yes, what would it be used for; if no, why not?

Incident Response

12. **(2 points) Name** the 4 different phases of the NIST Incident Response process. Also indicate the relationships between the 4 phases and any feedback loops that might exist.

You – the security manager - are notified about a suspected incident. You are getting the incident response team together.

13. **(2 points)** Can you describe the decision-making and communication parameters that need to be defined before the team starts to conduct the actual analysis?



14. **(6 points)** For this question, see the network diagram shown above. The incident deals with suspected data theft from one of the file servers that is supposedly only accessible for employees. Please formulate 3 hypotheses on how the data could have been stolen and describe a short analysis plan how you want to prove or disprove each hypothesis.

Managed Security Services

15. **(2 points)** What are the drivers of make-or-buy decisions in the security practice? How would these drivers explain a growing willingness to buy security as a service rather than to do it in-house?
16. The Zeta Commission is considering outsourcing part or all of its cyber security capability in hopes of saving money (including the monitoring capability you just set up in one of the questions above). Outsourcing of IT security as well as OT security is on the table, but the final decision has not been made yet. They have asked you to provide them with input as to **which aspects** they should consider before making the final decision.
    a. **(2 points)** Name one argument for and one argument against outsourcing the entire security capability. Would the pros and cons be different in a situation without OT?
    b. **(2 points)** If the security capability would be partially outsourced, which parts of it would you recommend for outsourcing, and which would you want to keep in-house? Name one of each, and indicate why you chose them.
    c. **(2 points)** Based on what you know about the Zeta works, which of the aforementioned options (i.e. outsource everything, outsource some parts, keep everything in-hosue) would you advise them to go with, and why?

Identity and Access Management (IAM)

17. **(5 points)** Based on the case description as well as your knowledge of cyber security, describe 3 vulnerabilities related to the physical and logical access security of the Zeta works. For each vulnerability, describe an access security control on how to mitigate it.
18. **(2 point)** We distinguish 3 authentication types (or: authentication factors). Name 2 of these, and provide an example for each in the context of Zeta works.
19. **(3 points)** In the lecture of IAM, we discussed the U2F standard. Elaborate on how U2F would be beneficial for Zeta works. Provide 1 concrete example.

Crisis Management and Business Continuity

20. **(3 points)** What is the difference between an incident and a crisis? Name at least 3 key elements.
21. **(2 points)** Explain what group think is, and how it can affect the decision making process during crises.
22. **(2 point)** Explain why communication is a critical function in crisis management, especially in the case of the Zeta works.
23. **(2 points)** How do social media affect the crisis management landscape? When handling a Zeta works-related crisis, how would you apply social media (or not), given your knowledge of crisis management theory?