See 2016 final exams. Most of the questions are repeated

(in the end of this file)

**Our exam June 3, 2017:**

Q1. Viruses: Exactly same as Q1 of June 2016 exam

Q2. Authentication vs Authorization: Exactly same as Q2 of June 2016 exam

Q3. DMZ: Exactly same as Q**4** of June 2016 exam

Q4. He gives you the 8 design principles, then gives you statements and you need to specify which security principle that the statement follow (don’t remember exactly but at least the statements are close):

1. The use of write-once media to log information? You answer: principle of least privileges
2. Firewalls are easy to configure? Answer: Principle of psychological acceptability
3. Moving files require approval from *more than one* employee? Answer: Principle of separation of privilege
4. Don’t remember ☹ but maybe something is distributed on multiple servers: Principle of least common mechanism
5. … should know the minimum knowledge: answer: principle of least privileges

Q5. Goals of Intrusion detection system: Exactly same as Q6 of June 2016 exam

Q6. Was weird! The question is: after doing penetration testing, we discovered that the admin password for one of the routers in a room is admin. Write two generalizations of this flaw??

I even did not understand what he wants!! I answered that we should use strong passwords that are difficult to guess. Number 2 is we should change the passwords periodically and never use the default ones (did not understand the question so I am not sure if that is a correct answer or not)

Q7. ACM for the user classes and data classes: Exactly same as Q10 of June 2016 exam

Q8. XSS: same as Q6 in Oct 2016 exam. What is XSS? Give an example and what it can causes? How to prevent XSS?

Q9. True/False and you need to explain the answer (otherwise, give you zero). 20 marks (5 each branch). I am not sure from the answers so search more :P

1. All hosts in the internet must have domain name. my answer: true; because that is how the DNS works i.e. it maps names to IPs (not sure of the answer)
2. A Detection Manipulation Code is based on timestamp? My answer: False; it is based on other thing (you need to mention it) but not on the timestamp.
3. An attachment of extension .doc or .docx is safer than .txt (not exactly like this but I forgot)
4. A system use the misuse detection model will fail detecting a zero day attack. My answer: true, zero day attack means a hole that is unknown to vendor. Misuse model matches data against rule sets, so it cannot detect attacks unknown to developers of rule sets (No rules to cover them).

Q10. SCI: Exactly same as Q10 of June 2016 exam





