CS-239 Exam Revision Topics (Lecture and Labs)

Week	**Topics Included**	**Topics Excluded**	**Exam Tips**
Week 1	Definitions of security. Readings 1 and 2 both are highly relevant for definitions and a range of examples.		Focus on the precise terminology of basic definitions. The range of examples in the readings could be useful to help illustrate the basic concepts when you are asked for them.
Week 2	Basic concepts in security and how they are related to each other. A basic understanding of the V-model. Basic notation of an AD Tool.	Readings 1 and 2 are excluded.	Examples provided in the lab sheet including entering a room and denial of service attack could be useful to show for an example attack tree.
Week 3	Key attributes to characterise a threat, including the tables to assign values to those threats. Also, a basic understanding of the notions of attribution and stealthy threats. From the lab, attack potential calculation.	Readings 1 and 2 are excluded.	The lab examples of entering a room and emergency braking from the lab could be useful to help understand how attack potential is calculated. The lecture example of Android weather and contacts app could also be useful for explaining stealth.
Week 4	From the lecture, only topics of risk management and threat analysis are included. From the lab, only asset, damage and threat scenarios.	Excluded are all definitions of automotive technologies (only useful if you wish to give an automotive example). Data Flow Diagrams are excluded.	Asset and Damage scenarios are most useful here to help understand what could be targets of an attack, and what are the implications of damage to such assets.
Week 5	From the lecture, under topics of risk assessment, impact ratings and attack potential are included. Risk value determination is also included.	Any details of automotive systems as examples could be excluded (unless you want to use it an example to help clarify a concept). Data Flow Diagrams are excluded.	In the lab, threat attributes from week 3 and risk impact are useful topics to pay close attention to.
Week 6	Definitions in Slides 1-3 are important. A basic understanding of the relationship between safety and security would suffice. Definitions of types of risks from Reading 1 could be useful.	The topic of "Risk as uncertainty" is entirely excluded, alongwith business risk taxonomy and scenarios for risk perception. The rest of reading 1 and the entire Reading 2 are excluded. From the lab, attack defences are excluded.	Pay attention to the various types of risks and impact categories as the most important topics in this week.

Week 7	Basic definitions of software testing and security testing. A basic introduction to the Model-based security testing (MBST) technique.	Most sections in Reading 2 apart from section 4.3 Security Testing (which has been covered in the lecture)	Focus on the similarities and differences between software testing and security testing. Understand the applicability of different security testing techniques with respect to SDLC. Understand the basic steps of MBST. Practice the provided example to challenge your understanding.
Week 8	A basic introduction to other security testing techniques including manual/automatic code review, tainted analysis, pen-testing, and fuzzing.	Readings 1 and 2 are excluded.	Focus on understanding each techniques such as what are the input, output and steps. Practice all the examples provided in the lecture and reflect them against your understanding.
Week 9	All definitions in the lecture. Top three reading articles could help offer some examples	From the lecture, "software bug" is excluded. Readings on computer bug and security economics are excluded.	Legal or economic details are not needed, only the basic descriptions are presented in the slides.
Week 10	Vulnerability management, risk of exploitation and disclosure.	Readings 1 and 2 are excluded.	You may wish to use any other vulnerability (drawn from any domain) as an example, if asked to explain any of this week's topics, just to help illustrate your point.