2013-02-27

Reading instructions for Stallings: "Computer Security" and other course material in the course EDA263 – rev7

These notes are reading instructions for the first edition of the text book and are only supplied as is. The officially recommended book is the second edition and the course / exam is going to be based on the material in the second edition. It will be continuously updated during the course so please always download the last version.

Lecture number:

L01: Introduction; Threats, Vulnerabilities, Protection
Chapter 1 (except §1.4, pp.22-26)
Chapter 13 (overviewish) -- Physical security
DL1:Targeted Trojan Email Attacks

L02 - UNIX:
Chapter 23 -- Linux Security: all (23.7 for the interested)
Chapter 4 -- Access Control (UNIX): Only Section 4.4
DL 2: UNIX Security 1 (corresponds to Ch 23 in edition one of book)
DL 3: UNIX Security 2 (corresponds to Ch 23 in edition one of book)

L02 - Malware I (L02) + Malware II (L04):
Chapter 7 -- Malware: (for interested: Digital Immune System)
Chapter 11 -- Buffer Overflows: all
DL 4: Salami attack

L03: Chapter 3 (except: "Markov Model" p.85-88). (Overviewish: §§ 3.7-3.8, pp. 101-105)
Chapter 4 (except: § 4.4 - in L02; RBAC Reference Model, The NIST RBAC Model and Static Separation of Duty Relations, pp. 128-134)
(Overviewish: §4.6, pp. 135-136)
DL2: Testing biometric methods
DL3: Bank card skimming
DL4: Password trading
DL12: Password guessing

L04 Malware I (L02) + Malware II (L04):
Chapter 7 -- Malware: (for interested: Digital Immune System)
Chapter 11 -- Buffer Overflows

L05: An introduction to cryptology

Chapter 2	Cryptographic Tools
Chapter 19.1	Symmetric Encryption Principles (not: Feistel Cipher Structure)
Chapter 19.2	Data Encryption Standard
(Chapter 19.3	for interested students, read as an overview: AES)
Chapter 19.5	Cipher Block Modes
Chapter 19.7	Key Distribution
Chapter 22.3	Public-Key Infrastructure
OP2-3	

L06: Malware defences, Firewalls, Link encryption, Operating Systems Security:
DL7 (p. 1-7) -- Malware defences
§§ 9.1-9.5 -- Firewalls
§ 19.6 -- Link encryption
§ 10.3 -- Reference Monitor

L07: NW attacks, Denial-of-Service Attacks, Kerberos
Chapter 8 -- Denial-of-Service-attacks, spoofing
§ 22.1, OP4 – Kerberos NW authentication scheme

L08: Intrusion Detection Systems, Intrusion Tolerance
Chapter 6 -- Intrusion Detection
§ 9.6 -- Intrusion Prevention Systems
OP5 -- Intrusion tolerance (FRS system)

L09: Security Policies and Models

Chapter 4.1	Access Control Principles
Chapter 4.2	Subjects, Objects, and Access Rights
Chapter 4.3	Discretionary Access Control
Chapter 10.1	The Bell-LaPadula Model Section "Abstract Operations" only as an overview. Section "Implementation Example – Multics" is not included.
Chapter 10.2	Other formal models for computer security the Certification and Enforcement rules on page 316 are only as an overview

L10: Defensive Programming and Database Security
§§ 5.1-5.5 (where 5.1-5.3 is database introduction. Should only be read
to the extent necessary to understand the rest of the chapter, note that this edition misses the discussion on cloud security, part of course and part of the second edition)
Chapter 12

L11: Security and Dependability Modeling, Risk Analysis, Key Escrow
Lecture slides
§ 16.4 -- Risk Analysis
§§ 16.1-3 overviewish -- Risk Analysis
DL9 -- The Risks of Key Recovery

L12: Security Metrics, Organisational issues, Human factors
Lecture slides
§ 14.2-14.4 -- Organisational issues, Human factors, Security policy
§§ 14.1 overviewish -- Organisational issues, Human factors, Security policy
§§ 17.3 - 17.5 -- Security plan
§§ 17.1 - 17.2 (overviewish) -- Security plan
DL8 -- A Framework for Security Metrics
DL10 – Why Cryptosystems Fail

L13: Key Escrow Systems, Common Criteria, Spam Economics, Computer Forensics
DL13 – Key Escrow Systems Taxonomy, DL9 – The Risks of Key Recovery
§10.6-7 – Common Criteria (Fig. 10.15 overviewish)
DL 11: Common Criteria – Introduction and General Model (§1-9, A1-A3, B1-B3, C1-C2, D1)
DL14: Spamalytics

L14: Side-channel attacks, Ethics (+catchup)
Chapter 18.4
DL 15: Introduction to Side-Channel Attacks; DL5: Data remanence
OP1: Pfleeger, Ethics;

L15: Guest Lecture, Examination