Cyber Security Technologies

Final Exam Study Guide

Shawn Davis
ITMS 448 – Spring 2016

Slides contain original content from Davis, S.

Final Details

- Our Final is in two weeks on 5/2 here in this classroom.
- Class starts at **5:00pm** and the Final starts as soon as I have taken attendance and give the okay to proceed. You will not be given additional time if you arrive late.
- No makeups will be given unless you have an extreme situation accompanied by a doctor's note.

Final Details

- You will have until 7pm (roughly two hours) to complete the Midterm which will be in the form of a Blackboard Test
- There will be around 65 questions on the final exam

Final Details (cont.)

- The Final is closed book/closed notes.

- Do not attempt to start/take the Final from outside of class. Attendance will be taken in class and any out of class attempts will result in a zero with no makeups allowed.

Final Details (cont.)

- Keep your eyes on your own screen during the exam.
- Any attempts at cheating will result in an automatic zero, dismissal from class, and an ADR filed
- No talking of any kind is permitted during the exam time period.
- Once you finish, please quietly leave the classroom

Respondus LockDown Browser

- Respondus is installed on each computer
- Before the exam, you will need to double-click "LockDown Browser" from your desktop
- Login to Blackboard and our course
- Select the "Exams" folder and start the final after attendance is taken and I say to begin

Final Study Guide

- The following slides are not all-inclusive but will provide study suggestions to prepare for the most all of the topics covered in the Final
- The majority of questions will be based on the lecture slides and labs and will cover the lectures after the Midterm Exam

Week 9 – Crypto I

- Know the terms on the “Terminology” slides
- Know the four goals of cryptographic ciphers
- Know the difference between symmetric and asymmetric key crypto
- Know the common stream and block ciphers
- Understand broadly how CrypTool was used to crack ciphers
- Understand how to manually decrypt ciphertext with the Caesar and Vigenere ciphers

Week 9 – Crypto II

- Understand the broad concept that Witfield Diffie came up with
- Understand how the key pairs work for Confidentiality and Authentication
- Understand how message integrity and authentication, and non-repudiation is achieved
- Be familiar with Digital Signatures, CAs, Digital Certificates, Etc.

Week 9 – Crypto II

- Be familiar with the email and web standards that offer all four goals of cryptographic ciphers
- Be familiar with the tools used in the in-class SSH lab

Week 11 – Stego / Firewalls

- Know details about overt and covert files
- Understand the common stego schemes (Image and Audio file carriers)
- Understands the differences between and how data is hidden in each method:
  - Insertion
  - Substitution
  - Generation

Week 11 – Stego / Firewalls

- Know the general steganalysis detection techniques
- Understand the commands for hiding and unhiding alternate data streams

Week 11 – Stego / Firewalls

- Understand the capabilities a Firewall needs to have
- Understand the difference between the two types of Firewalls (as well as the four sub-types)
- Know what header fields are always considered by packet filters when performing filtering
- Understand the difference between the default policy choices

Week 11 – Stego / Firewalls

- Understand how to read/explain as well as create a stateless packet filter rule
  - It won't have to be with iptables for this question and will be more general as shown in slides 31 and 33
  - That means you should know the port numbers of the 10 most common services
- Understand what header fields stateful packet filters evaluate

Week 11 – Stego / Firewalls

- Understand NAT and how it works
- Understand the difference between the iptables rule actions (ACCEPT, REJECT, DROP)
- Understand the difference between the NEW, ESTABLISHED, and RELATED states for ctstate in iptables
- Be able to read/explain a few iptables stateful chain rule entries

Week 12 – IDS/IPS

- Be able to define the six items on the "Terminology" slides
- Understand anomalies an IDS/IPS may detect
- Understand the difference between inline and passive sensors and what devices may be used for each
- Know the NIDS sensor placement choices and the advantages/disadvantages of each

Week 12 – IDS/IPS

- Know what a Honeypot is and its placement choices
- Understand Snort's two modes and submodes
- Be able to identify the header parts and option parts of a Snort rule

Week 13 – User Authentication & Access Control

- Understand the four means of authenticating a user
- Understand how traditional password authentication works
- Be able to define the five methods to crack a password
- Understand what a salt is and how it can prevent an attacker using lookup or rainbow tables
- Understand the current Unix/Linux shadow file format for password entries and why the shadow file is more secure

Week 13 – User Authentication & Access Control

- Know the difference between LM and NT hash generation and where they are both stored
- Know what the six general authentication security issues are
- Understand what components a Kerberos environment consists of
- Understand what a Ticket Granting Ticket (TGT) does

Week 13 – User Authentication & Access Control

- Understand how to change permissions via letters and numbers
  - You will need to provide the full command on a few scenarios for each
- Know why you would need to ever set an ACL in Linux

Week 14 – Computer Forensics

- Understand the three federal laws involving computer forensics
- Understand the differences between allocated/unallocated space and partitioned/non-partitioned space and what items may be found or not found in each
- Know the different types of evidence acquisition imaging methods and how they work

Week 14 – Computer Forensics

- Be able to explain the differences of Dead vs. Live Acquisitions
- Know some or the potential questions forensic analysis can answer
- Understand the main tasks we performed with EnCase
- Understand the differences in the registry and internet artifact tools
- Be familiar with common items found in memory captures

Week 15 – Wireless Network Security & Attacks

- Understand the difference between a Wireless Router and a Wireless Access Point
- Be able to define each of the IEEE 802.11 architecture terms
- Know the differences between the three wireless security protocols
- Be able to define each of the common wireless security threats

Good Luck!

- Make sure to review all of the slides, memorize the concepts and terms, and quiz yourself on the specific items listed in this study guide.
- The Final is 20% of your course grade.