Cyber Security Technologies

Session 7 – Midterm Study Guide

Shawn Davis

ITMS 448 – Spring 2016

Slides contain original content from Davis, S.

Midterm Details

- Our Midterm is on 2/29/15 here in this classroom.
- Class starts at 5:30pm and the Midterm starts at 5:40pm. 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.

Midterm Details

- You will have 2 hours to complete the Midterm which will be in the form of a Blackboard Test
- There will be between 60-80 questions on the exam

Midterm Details (cont.)

- The Midterm is closed book/closed notes.
- Do not attempt to start/take the midterm 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.

Midterm Details (cont.)

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

Respondus LockDown Browser

- Check to see if you have LockDown Browser icon on your physical Desktop
- Before the exam, you will need to:
  - Double-click that “LockDown Browser” from your desktop
  - Login to Blackboard and our course
  - Select the “Exams” folder and start the Midterm when 5:40pm hits

Midterm Study Guide

- The following slides are not all-inclusive but will provide study suggestions to prepare for the majority of the topics covered in the Midterm
- The majority of questions will be based on the lecture slides and labs and will cover Weeks 1-7

Week 1 – Security Overview

- Be able to define the important security concepts
- Be familiar with the core security principles
- Phishing/Email Header Analysis
- Understand how the BeEF lab worked
- Be familiar with how Tor works
- Common 5 Phases of an Attack and their defenses
- Understand the Recent Popular Security Threats

Week 2

- No Class

Week 3 – Malware Overview & Exploit Kits

- Be familiar with all malware types listed in the slides, their propagation methods, and common payloads
- Understand how botnets work
- Understand how Netcat backdoors work
    - Be able to pick the correct commands out of a list
- Understand basic malware detection and remediation techniques
- Understand the general chain of events and goal of web exploit kits

Week 3 (Cont.)

- Know the details about how Crimeboss and Blackhole work, payloads and signatures they use, etc.
- Understand how Wireshark is organized and how it was used in the lab
- Understand details about what the Crimeboss exploit kit did in the packet capture from the lab

Week 4 – Malware Analysis

- Understand steps for creating an isolated analysis environment
- Understand all types of static and dynamic malware analysis
- Understand what each analysis tool does, how it is used, and what type of malware analysis it performs (static or dynamic)
    - Be able to identify the tool based on a screenshot

Week 4 (Cont.)

- Understand what happened in the Windows Live Messenger lab
- Understand levels of abstraction

Week 5 – Attack Vectors & Mitigation Techniques

- Understand attacker taxonomy
- Understand types of social engineering attacks
- Be familiar with how the mentioned network protocols work
- Be able to identify DoS/DDoS attacks based on seeing screenshots of packet captures
- Be familiar with how buffer overflows work as well as the code involved (such as the in-class lab)

Week 5

- Understand how ARP Poisoning works and how to use arpspoof and the tools we used in class
    - Be able to pick the correct command out of a list
    - Be familiar with the diagrams
- Understand the defenses against the various attacks

Week 6 – Web App Attack Vectors & Mit Tech I

- Be familiar with the first three of the OWASP Top 10 (Injection, Broken Auth/Session Mgmt, XSS)
  - How each attack works
  - Goal of attacks
  - Defenses against attacks
  - Be able to identify an attack based on seeing a screenshot of a webpage
- Be able to identify correct database SQL queries out of a list

Week 6

- Make sure you can identify correct SQL or OS injection queries out of a list
- I would be familiar with most all topics in the week 6 slide deck
- However, the exam will **not** cover:
  - sqlmap slides
  - DOM Based XSS slides
  - Proxy Lab slides

Week 7 Web App Attack Vectors & Mit Tech II

- Be familiar with the remaining categories of the OWASP Top 10
  - How each attack works
  - Goal of attacks
  - Defenses against attacks
  - Be able to identify an attack based on seeing a screenshot of a webpage
- Understand the difference between LFI, RFI, and Directory Traversal

Week 7

- I would be familiar with most all topics in the week 7 slide deck
- However, the exam will **not** cover:
  - Nikto
  - Skipfish

Grade Weighting

- Homework/Labs = 50%
- Individual Project = 5%
- Attendance/Class Participation = 10%
- Midterm Exam = 15%
- Final Exam = 20%

Good Luck!

- Finish last week's HW6 right away so that you can dedicate your time to midterm study
- Don't want until the last second to complete HW6 and to study for the midterm
- My exams do require thinking but none of the questions are designed to trick you

- Any questions???