Quiz Guide

This material, if not specified, guides you at the level covered at lectures.

Quiz Specification

- Oct 17, 2019 at Class Time
- Closed book and closed note
- Question types:
  - 10 Short answer questions (ex. definitions)
    - 2 points each
  - 10 Yes/no questions
    - 2 points each
  - 10 Multiple choice questions
    - 2 points each
  - 2 Long answer questions
    - 20 points each
    - Each question is made up of several small questions
  - **All the answers written on the exam papers**

Topics

- Network vulnerabilities and penetration
  - the dangerous jungle
    - Basic understanding of network security and its importance
    - Virus, Worm, DDoS
  - major network attacks
    - Passive attack vs. active attack
    - The various attack weapons
  - Intrusion penetration (Lab 2)
    - Attack weapons, intrusion tools, penetration steps
    - The big picture
  - Penetration tools
    - The function of the tools and their simple usage examples

Topics

- Internet malware
  - Worm (strongly suggested to read the worm paper discussed in class)
    - Morris, Code Red I v1 and v2, Code RedII, Nimda, Slammer, Blast and Welchia, Walhol worm, flash worm, stealth worm
    - Hit-list scanning, Permutation scanning, Topological scanning
  - Buffer Overflow (Lab 1)
    - Stack buffer overflow
      - Manipulating return address
    - How to prevent buffer overflow
      - Methods
      - StackGuard, PointGuard
  - Lab 1 (buffer overflow), Lab 2 (metasploitable)

The following example questions are based on the **labs**.

Example Questions

- Part 1: Short-answer questions
  - In Lab 1, where does the buffer overflow happen? Stack or heap? Is the return address replaced by another address? Where is the new address pointing to?

Example Questions

- Part 2: True/False questions.
  - In Lab 2, nmap could help us find the victim machine is running a web service for tikiwiki.

Example Questions

- Part 3: Multiple-choice Single-answer questions
  - Which of the following was not true for Lab 2?
    - a. brute force key guessing attack was performed towards ssh_authorized_keys
    - b. a reverse shell attack was triggered by uploading a rerverse shell to the victim web application
    - c. the session obtained through the reverse shell was not root-level access
    - d. the key inside ssh_authorized_keys is a private key

Example Questions

- Part 4: Long-answer questions
  - Example 1: the steps of Lab 1
  - Example 2: the steps of Lab 2