Final

Logistics

- 10 choices
- 10 fill in the blanks
- 4 descriptive questions
- 4 will be from the previous exams

Familiarity

Chapter 2

- Access control
    - Get familiar with group-based control.
    - The structuring access control.
    - The tree-like diagram on slides with orange nodes:
        - y1 students, y2 students.
        - For each specific group, the rights can be customized.
        - All students have read; y1 has write.
        - y2 has read and write rights.
        - Understand the relationship between the groups and rights.
- Biometric auth
    - FMR, FNMR, EER stuff.
    - Know all of these whats, hows, and whys.
    - Relation with threshold.
    - The graph needs to be done.
    - Understand stuff around that.

Chapter 3

- Block cipher
    - Cipher block chaining mode: (not OFB)
        - Encryption and all.
- RSA
    - Check the integrity authentication example.
    - If users receive the key, what's the security guarantee, as well as vice versa.
    - Which key should be used for encryption and decryption.
    - Make sure to show the work and thought process for answers.
    - Check both Alice and Bob scenarios for confidentiality.
    - Who's the who.
    - Whose key is used.

from new content

Chapter 4

System Security

- Understand the process of boot sequence:
    - Check if CPU and memory are ready; if not, cause an error message.
    - Find the place where the OS will be stored, so it can be loaded and started.
    - Load the boot program.
    - If not, refer to the "post again" slide.
- **Security Issues 1**
    - Understand two security issues:
        - *(Details missing)*
- **Password Salt**
    - With and without salt.
    - Search space growth.
    - Understand these two questions.
- **ACE, ACL**
    - Linux permissions:
        - Check the strategies in the "different systems" slide.
        - Linux permissions:
            - File system:
                - Groups.
                - Categories.
                - Permissions for different categories.
            - Understand the comments and how they are read. Refer to the slide with those comments.
            - There is a question somewhere around this; understand how to answer it.
    - For Windows:
        - What is the difference in security, file systems, and all?
- **Buffer Overflow Attack**
    - Understand the whole process:
        - Partition of address.
        - Permission of the shell code.
        - Partition of the malicious code.
    - Level L1 attack and lower:
        - New return address can be any from the "lob"?
        - You don't need the exact prediction, just an estimate of where to put it.
        - Process is the key part, and the "low, lob?" *(unclear)*.
        - *(No clue what was said)*.
- Done with system security.
- Tthe porcess to start OS.

- two security issues. hybernation attack or something.
- file systesm: liunux and windows, commens and difference. comments and reader comments.
- salting
- ACE, ACL - some concepts in file systems
- importance in buffer overflow attack
- the nop sled

Software Security

- **Security and Reliability**
  - How they are related and interrelated connections.
  - Reliability can't guarantee security.
    - How the attacker benefits from that.
  - Security can guarantee reliability.
- **Input Validation**
  - Exploit Unicode bug:
    - Unicode character, how `/` and similar characters matter.
    - Check examples around slides 16-18.
    - Signed integer.
    - Unsigned integer.
    - Understand computing with integers:
      - Why specific outputs occur.
      - If the number of bits for an integer is signed or unsigned, consider two cases:
        - Overflow or not.
        - How the calculations happen.
      - Know the result for each output.
      - Understand the standalone code (simple one on slide):
        - Which iteration the code will stop at.
        - How many times the loop runs or how to count the iterations.
- **SQL Injections**
  - Malicious input.
  - Expected output and related details.
  - Check the slide for examples.
  - Another example is on the differences.
  - Two categories of defense:
    - Detection.
    - Prevention (e.g., filtering).

Key Topics

1. Input validation.

2. Loop example (while code example).
3. Integer examples (signed, bits, and unsigned bits).
4. Concept of security and reliability:
    - Security features: detection and prevention.
    - Which feature is for what (example: mobility).
5. Determining in software.
6. Double free attack.
7. SQL injection:
    - Commands (if provided, know them accordingly).
    - Definition.
    - Ways to achieve the injection (e.g., comment-out symbol).

Network Security

- **Attacks**

    - ARP spoofing.
    - ICMP attack.
    - SYN flood.
    - DNS.

- **Understanding Attacks**

    - Be clear on ARP, ping, smurf, SYN, session hijacking, and DNS poisoning attacks.
    - Understand how these attacks are done and their associated layers:
        - ARP: Link layer.
        - ICMP/ping/smurf: Network layer.
        - SYN, hijacking: Transport layer.
        - DNS: Application layer (working process).
            - To solve it, refer to "divssec."

- **Defense/Firewall**

    - About firewalls, positioning, goals, and different types:
        - Packet filtering.
        - Stateful.
        - Application-level.
    - Understand the differences between them.
    - Reasons why ARP, smurf, and similar attacks work.
    - Check slides on ARP spoofing:
        - Depends on the machine's trust.
    - Check other attacks as well and ensure understanding.

- **DNS**

    - Security check guaranteed by QID or something similar.
    - If the attacker guesses the QID:
        - The attack will be quicker, and the attacker's answers will be saved in the cache.
        - Otherwise, the attack will fail.

- Two conditions for attack success:
    1. The guess is correct.
    2. The attacker's answer is faster than the legal name server's response.
- If the attacker fails:
    - They must wait until the TTL time expires.
    - The next attack should be launched after that time.
- Check the "DNS attack next try" slide:
    - The attacker won't need to wait.
    - Understand the process and how it works in case of failure or success.