Final Exam Guide

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

Final Exam Specification

- 1 hour long
- Closed book, closed sheet
  - **No reference sheet**
- Question types:
  - 10 Short answer questions (ex. definitions)
    - 3 points each
  - 10 Yes/no questions
    - 3 points each
  - 10 Multiple choice questions
    - 3 points each
  - 1 Long answer questions
    - 10 points each
    - Each question can be 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 and Lab 3)
    - 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

Topics

- Firewall
  - Firewall basics
  - Packet filtering
    - Use the example to understand how to use the TCP 3-way handshake to deny traffic
  - Proxying vs. Packet Filtering (difference)
  - Stateful Packet Filtering
  - Architectures
  - iptables

Topics

- Intrusion detection system (IDS)
  - Intrusion types
  - Idea of HIDS, NIDS, AIDS
  - HIDS
    - Session Level Intrusion Detection
      - The haystack algorithm
    - System Call Level Intrusion Detection
  - NIDS
    - Signature-based NIDS: Snort and rules
  - Anomaly detection vs. signature-based detection

Topics

- Authentication
  - passwords (one time password, challenge-response authentications)

Topics

- Labs
  - Lab 1 (buffer overflow)
  - Lab 2 (metasploitable)
  - Lab 3 (pentesting)
  - Lab 4 (heartbleed)
  - Lab 5 (SQL injection) (understand what is called SQL)
  - Lab 6 (XSS attack) (understand what is called XSS)

Example Questions

- Part 1: Short-answer questions (4 points each)
  - What is done by this iptables rule: “iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP”? Can we still ping localhost?
  - Why do we need to use keyed hash function, not just normal hash function, in AH protocol?

Example Questions

- Part 2: True/False questions (4 points each). If false, please also explain why.
  - Packet filter firewalls check both the header information and content of a packet.
  - Fragmentation attacks may bypass packet filter firewalls.

Example Questions

- Part 3: Multiple-choice questions (4 points each)
  - Given A =Alice; KpubA = Alice's public Key; KprivA =Alice's private Key; KprivCA = Private Key of a Certification Authority. KpubCA = Public Key of the Certification Authority. In the following notation X{Y} means using X to perform an operation (encryption/decryption/signing/verification) on Y. Which of the following cryptographic notations most closely represents what Alice's certificate is like?
    - a. KprivA., A, CA, KprivCA {KpubA., A, CA}
    - **b. KpubA., A, CA, KprivCA {KpubA., A, CA}**
    - c. KpubA., A, CA, KpubCA {KpubA., A, CA}
    - d. KprivA., A, CA, KprivCA {KprivA., A, CA}

Example Questions

- Part 4: Long-answer questions (20 points each)
  - Based on the following figure, please carefully design a set of rules for a packet filter firewall, so that 1) no incoming telnet service should be processed; 2) outgoing telnet request are OK; 3) Computer 132.28.6.4 can NOT do Telnet; 4) UDP packets are not allowed. Please also give a brief explanation what's the rationale that you design each rule.
  - Ex: For each rule, you should have: Direction (incoming/outgoing), Source Addresses, Destination Addresses, Type (TCP/UDP), Source Port, Destination Port, ACK (1/0), Action (Deny/Permit)