Introduction to Homeland Defense
Qualifier exam example question

Why was NORTHCOM formed? What are the two primary missions of NORTHCOM? How are NORTHCOM and DHS related? Describe the central issues related to each of NORTHCOM's missions. Has NORTHCOM made the country safer (why or why not)? Can NORTHCOM ever make the country completely safe (why or why not)? Are we better with or without NORTHCOM?

Understanding the Threat
Qualifier exam example question

Describe the specific threat posed by modern terrorism. Why is the terrorist threat more significant than natural disaster? Why is it difficult to classify terrorists? Broadly describe US counterterrorism strategy. Has US counter-terrorism strategy reduce or increased the threat of terrorism (why or why not)? Can we ever be entirely safe from terrorist attack?

Computer Communications
PhD Qualifier Example Questions

Problem 1. Hamming Coding

1) A n-bit codeword is a frame of m-bit data plus k-bit redundant check bits (n = m + k). What is the lower limit on the number of bits k needed to correct single-bit errors in a n -bit codeword? Explain your answer in details.

2) Perform hamming encoding for a 7-bit data sequence 1001000. Show major steps.

Problem 2. Subnetting

Suppose many departments in UCCS want to have their own LANs, each LAN with up to 100 hosts. Suppose the UCCS now has a class B address (16 host ID bits) with network address 150.100.0.0. Please design an appropriate subnet addressing scheme.

(1) How many bits you would use for the hostID in each subnet?

(2) How many subnets that your subnetting addressing scheme would allow UCCS to have?

(3) What IP mask would be?

(4) Please find the subnet for an incoming packet with destination IP address 150.100.12.176.

Please select two from the three questions below.

Problem 1. Cyber Attack

1. Buffer Overflow.
    a. What is the main purpose of those NOP instructions in the payload of the exploit?
    b. The last part of exploit payload consists of many same memory address.
        i. What is the memory address pointed to?
        ii. What part of stack components, the hackers would like to overwrite using this memory address?
        iii. How do they guarantee the memory alignment between that stack component and the memory address?
    c. How the canary guard works in the context of buffer overflow defense?
    d. Explain how dynamically changing the Instruction Set (how op codes are interpreted) can prevent buffer overflow attack.
2. What is ARP poisoning? How to prevent that? What is DNS poisoning? How to prevent that?

Problem 2. Cyber Defense

1. Web Security
    a. What is SQL injection attack?
    b. How to prevent SQL injection attacks?
    c. What is command injection attack?
    d. How to prevent command injection attacks?
2. Defense against Insider Attack.
   A disgruntled system admin can change the root password and block all accesses to an important server. Propose a scheme where the future OS allows multiple root accounts and can change the password of one root account when the majority of the root users agree. Discuss key privilege restriction of the root user for this defense to occur and the process where the majority of the root users can reach the concensus.

Problem 3. Encryption and Authentication

1. How can biotope provide the biometric-based authentication without compromising the privacy?
2. NIST CSCTG group is currently debating adopting EAX mode vs. CCM mode of AES for smart grids.
    a. What is this “mode” about? And how it is related to the AES standard?
    b. Give three common modes used with AES or 3DEC standards?

Applied Cryptography sample questions

1. Using the extended Euclidean algorithm, find the multiplicative inverse of:
a. 1234 mod 4321
b. 24140 mode 40902
c. 550 mod 1769

Reference for this question:
Chapter 4 of the Textbook: Cryptography and Network Security: Principles and Practice (5th Edition), by William Stallings
ISBN-10: 0136097049, ISBN-13: 978-0136097044

2. DSA (The Digital Signature Algorithm) specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?

Reference for this question:
Chapter 13 of the Textbook: Cryptography and Network Security: Principles and Practice (5th Edition), by William Stallings
ISBN-10: 0136097049, ISBN-13: 978-0136097044