Tutorial Session 10

1. Consider a simplified scenario in which a computer program has a buffer that can store a maximum of N bytes. An attacker attempts to overflow the buffer by providing a payload of P bytes.
   i. Express the condition for a buffer overflow to occur mathematically, taking into account the buffer size N and the payload size P.
   ii. If the buffer size N is 128 bytes and the attacker's payload size P is 150 bytes, determine whether a buffer overflow would occur based on the condition from question i.
   iii. Calculate the number of bytes by which the payload exceeds the buffer size if a buffer overflow occurs as per the conditions in question ii.

2. Suppose a software development team is implementing a defense mechanism to prevent buffer overflow attacks in a C program. They have decided to use stack canaries as one of the defense measures.
   i. Let C be the canary value, which is placed between the buffer and the return address on the stack. Express the condition for a successful buffer overflow attack to occur mathematically, considering the canary value C and the values overwritten by the attacker during the attack.
   ii. Assume that the attacker attempts to overwrite the canary value C during a buffer overflow attack, and the canary value C is set to a randomly generated 32-bit integer. Calculate the probability of a successful buffer overflow attack if the attacker has no knowledge of the canary value C.
   iii. If the canary value C is a 32-bit integer, how many possible values can it take? Calculate the number of possible canary values.
   iv. Calculate the probability of a successful buffer overflow attack if the attacker has only one chance to guess the canary value C correctly.