1) Which of the following actions is an attacker not able to perform when gaining root access on a device, thus introducing a novel attack if managing to complete it?

a. Install and run a malicious app

b. Modify system files and configurations

c. Perform a software update for increased security

2) Specify which of the following attack scenarios is less common:

a. NFC Hacking

b. Phishing Attacks

c. Malicious App Downloads

3) Assuming the attacker can lure the victim to visit an arbitrary URL, which attack would not be able to complete?

a. Remote Device Takeover

b. Drive-By Downloads

c. Phishing Attack

4) If an attacker successfully runs code in the kernel of a mobile device, which attacks cannot he complete?

a. Rootkit Installation

b. Privilege Escalation

c. Complete Remote Control

5) Which of the following statements accurately describes the process of exploitation in cybersecurity?

a. Exploitation is the process of "taking advantage" of a vulnerability so that an attacker can perform unintended actions.

b. Exploitation is the process of enhancing system performance and efficiency.

c. Exploitation is the process of identifying and patching vulnerabilities in software.

6) When assessing the severity and relevance of a bug, what factors play a crucial role in determining its impact?

a. The combination of the "type" of bug and "where" it is (i.e., which component is affected).

b. The programming language used to develop the software.

c. The target victim device.

7) Among the following ones, select which is NOT an EOP attack

(where EOP = Escalation Of Privilege, I write it for you to remember)

a. Remote attacker ⇒ local attacker

b. Attacker with code execution with app's sandbox ⇒ write files in its private directory

c. Attacker with code execution with app's sandbox ⇒ system user/root

What does the term "attack surface" refer to in the context of cybersecurity?

8) What does the term "attack surface" refer to in the context of cybersecurity?

a. The sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.

b. The level of encryption used to protect sensitive data.

c. The total number of physical servers in an organization's data center.