NETWORK THREATS

Task 1. Watch the video "Denial of Service (DoS)" and choose only the correct statements

1. According to the video, a DoS attack is designed to make a system or data unavailable to people who need it.

2. In the video, the speaker describes browser redirection as the second method that can be used to carry out a denial of service attack.

3. The video explains that in a browser redirection attack, a user who requests a webpage is sent to a different page instead.

4. According to the video, a hacker performing a closing connections attack could shut down an open port to prevent a user from accessing a database.

5. In the video, the speaker states that deleting files can cause a "resource not found" error when someone tries to access that file.

6. According to the video, a DDoS attack differs from a standard DoS attack because it involves a hacker taking control of multiple computers.

7. In the video, the speaker explains that a resource exhaustion attack works by having a hacker request access to a resource just once but with an extremely large file.

8. The video indicates that if an application is vulnerable to injection attacks, a hacker can remove an entire database table to cause a denial of service.

9. According to the video, the speaker identifies exactly five different methods that can be used to carry out a denial of service attack.

10. In the video, the speaker mentions that repeatedly reloading a page can overload a web application, causing it to slow down or crash.

Task 2. Watch the video "GReAT Security Moments – Mobile Malware Evolution" and choose the correct answer to the questions

1. What is the speaker's main point about mobile devices?
A. They are less powerful than desktop computers and therefore less useful.
B. They should only be used for basic tasks to avoid security risks.
C. They are fully functional computers that face the same security threats as other devices.
D. They are more secure than traditional computers because of their design.

2. Why do cybercriminals tend to target Android devices more than other platforms?
A. Android devices are easier to physically steal and harder to track.
B. Android has a large user base and offers built-in flexibility that criminals can also exploit.
C. Android apps are not reviewed before being published, making attacks straightforward.
D. Android users are less aware of security risks than users of other platforms.

3. What does the speaker suggest about the overall trend in mobile malware between 2017 and 2018?
A. The number of malicious apps increased significantly, causing widespread damage.
B. Fewer malicious apps were found, but the actual number of attacks using them went up.
C. Both the number of malicious apps and the number of attacks dropped considerably.
D. More malicious apps were discovered, but they caused fewer successful attacks.

4. What does the phrase "the path of least resistance" mean?
A. Cybercriminals prefer to attack systems that are already protected by outdated software.
B. Cybercriminals choose targets that are the easiest and most rewarding to exploit.
C. Cybercriminals avoid mobile devices because they are too difficult to compromise.
D. Cybercriminals focus on attacking small businesses rather than individual users.

5. What precaution does the speaker recommend regarding financial transactions on mobile devices?
A. Users should avoid doing any banking on mobile devices under any circumstances.
B. Users should install a separate banking app that provides additional encryption.
C. Users should only carry out sensitive transactions on networks they trust.
D. Users should update their banking apps regularly to prevent unauthorized access.