Ahmad Abdullah
i22-1609

Networks | Cyber II
Online Task

Question #1

Feature	WPA2	WPA3	Improvements in WPA3
Encryption Protocol	AES with CCMP	AES with GCMP-256	WPA3 uses stronger encryption protocol offering better security
Password guessing resistance	Prone to get more offline dictionary attacks	Better at resisting dictionary attacks	Mutual authentication makes brute-force attacks significantly harder
Configuration	Easier to configure but less secure	Slightly more complex to configure but	Prioritizes Security over ease of setup
Protected Management Frames (PMF)	Optional	Mandatory	Mandatory PMF in WPA3 protects better from de-Auth and disassociation attack.

Question #2

WEP: Wired Equivalent Privacy (WEP) is the first security protocol for WIFI-networks as part of IEEE 802.11

Weaknesses of WEP: WEP uses 24-bit Initialization Vector (IV). The short length IV means it is repeated frequently. Attackers can capture enough packets to find duplicate IV. This makes WEP highly vulnerable to IV collision attacks.

- WEP does not check data integrity making it less reliable protocol.
- WEP relies on single shared key that is manually configured on each device.

Vulnerabilities of WEP:

- IV Reuseability Vulnerability
- Easily cracked Encryption
- Replay Attacks.

Improvements in WPA & WPA2:

- Stronger Encryption with TKIP in WPA and AES in WPA2
- Improved Key Management in both WPA/WPA2
- Integrity check with MIC