1. Explique o que é o WPA. Enquadre os respetivos cenários em que pode ser utilizado. Identifique as suas fragilidades. Justifique devidamente.

O WPA é um protocolo de segurança criado pela Wi-Fi Alliance para garantir a segurança de redes wireless que utiliza o protocolo TKIP para encriptar os dados que são transmitidos, incluindo também, o método de segurança de Message Integrity Check que previne os ataques de alterarem e mandar de voltas os pacotes de dados, que coloca na mensagem um “tag” para provar a autenticidade da mensagem enviada.

Com a atualização para o WPA2, o CCMP (protocolo de encriptação) tornou-se um dos suportes obrigatórios para o WPA.

Na última atualização o WPA3 implementa, feita em janeiro de 2019, a encriptação de 128 bits e “forward secrecy” (protocolo que garante que as chaves de sessão não serão comprometidas, mesmo que a chave privada do servidor esteja comprometida).

O WPA foi inicialmente criado para substituir o WEP, mas que ainda conseguisse trabalhar com hardware wireless que utilizasse o seu predecessor, mas atualmente, é utilizado por todo o lado seja em redes domésticas, privadas, de empresas, etc.

O WPA tem algumas fragilidades, como password cracking (através de brute forcing) que é possível se as passwords forem de uma natureza fraca, a falta de “forward secrecy” nas versões mais antigas, possibilidade de fazer packet spoofing (injeção de pacotes maliciosos nas mensagens), entre mais algumas.