**Sicurezza dei sistemi informativi - appello 16 giugno 2022**

1. Cosa è AES-192?
   1. Un algoritmo di crittografia asimmetrica
   2. Un algoritmo di hash con digest a 192 bit
   3. Un algoritmo di crittografia simmetrica a blocchi con chiave e blocco da 192 bit
   4. Un algoritmo di crittografia simmetrica di tipo stream con chiave e nonce da 192 bit
   5. Nessuna delle precedenti
2. Spiegare quali sono i principali approcci metodolodici per la stima dei rischi, in altre parole, come dai dati di assessment e di framing si ottengono gli impatti. Per ognuno di questi approcci spiegare da quali dati si parte, quali informazioni vengono derivate o usate e come si stimano, infine, gli impatti dei rischi
3. Spiegare cosa. Sono il GCM e l’H-MAC, quali proprietà di sicurezza permettono di garantire e, brevemente, come vengono implementati. Indicare quando ha senso usarli e quali sono i vantaggi che portano ad utilizzarli
4. Spiegare cosa è il processo di reverse engineering e come gli strumenti noti come disassembler e decompiler permettono di effettuarlo su binari. In particolare, indicare cosa questi tool producono in output e quali sono le loro principali limitazioni.
5. Cosa è un a KDF?
   1. È una funzione che trasforma chiavi crittografiche speudo-random in chiavi più forti usando l’entropia ottenuta da un sale crittografico generato mediante un processo random
   2. È una funzione che cifra un numero elevato di volte una password con un sale random per generare delle chiavi crittografiche forti
   3. È una funzione che permette di rallentare attaccanti che intendono svolgere dictionary attack obbligando la ripetizione di operazioni crittografiche su un sale per un numero elevato di iterazioni
   4. È una funzione che permette di ottenere dati pseudo-casuali forti a partire da stringhe di testo
6. Un’azienda dotata dalla sua rete privata aziendale vuole esporre al pubblico due servizi (HTML e posta elettronica) da due server aziendali (fisici, di proprietà dell’azienda).

Approfittando delle modifiche, hanno deciso di dividere la rete aziendale in due parti a diversi livelli di sicurezza. La parte rede della rete aziendale a livello di sicurezz più elevato dovrà attraversare la parte di rete a livello di sicurezza intermedio per poter accedere ad internet.

Progettare una soluzione che permetta di implementare una politica di autorizzazione di rete, indicando quali security control vorreste usare e come questi sarebbero collegati alle varie reti e ai due server

1. Elencare tutte le informazioni ed i dati che vengono scambiati mediante il TLS Handshake Protocol. Per ognuno di essi indicare come lo scambio viene effettuato e a cosa servono ai fini del protocollo TLS i dati scambiati