1. Dati le seguenti tecniche e scenari di attacco,
   1. Shadow server,
   2. Packet sniffing,
   3. Man-at-the-end
   4. APT

Spiegare come funzionano, indicare brevemente gli obiettivi che si potrebbero ottenere, e indicare possibili contromisure e controlli di sicurezza potrebbero limitarli

1. Spiegare cosa è il GDPR, quale è il suo obiettivo e indicare almeno 3 principi che lo caratterizzano
2. Cosa è Chacha20 256?
   1. La versione completa di un algoritmo di crittografia simmetrica di tipo stream con chiave 256 bit.
   2. Un algoritmo di crittografia simmetrica di tipo stream con blocco da 128 bit e chiave da 256 bit.
   3. Un algoritmo di crittografia simmetrica a blocchi con blocco da 128 bit e chiave da 256 bit.
   4. Un algoritmo di crittogragia simmetrica a blocchi con blocco da 256 bit e chiave 256 bit.
   5. Nessuna delle precedenti.
3. Spiegare come funziona IPsec (v2) ESP in tunnel mode e quali trasformazioni vengono fatte ai pacchetti IP.

Descrivere uno scenario di utilizzo, le ipotesi perché possa essere attuato e una tecnica per autenticare le parti ed uno specifico metodo di autenticazione ritenuto particolarmente sicuro (motivando).

Indicare quali proprietà di sicurezza possono essere applicate con questa tecnica. Per ognuna delle proprietà indicate, riportare se sono obbligatorie o opzionali e a quale parte del pacchetto IP originale si applicano.

1. Indicare e motivare brevemente quale controllo, tecnologia o architettura di sicurezza utilizzereste nel caso fosse necessario implementare della policy di sicurezza per:
   1. Impedire che dall’esterno della rete (es. internet) possano lanciare un attacco che sfrutti una vulnerabilità non ancora corretta (patch) ad un web service aziendale.
   2. Proteggere un server web dagli attacchi nella Top10 di OWASP
   3. Gestire da riga di comando un apparato di rete
   4. Permettere ad alcuni host, tutti noti e descritti mediante una lista di indirizzi IP, riescano a comunicare con un server interno
   5. Proteggere la rete aziendale ed un server che deve essere raggiungibile anche da chiunque da internet
   6. Permettere agli utenti nella sede di Torino di un’azienda di comunicare in maniera sicura con un’altra sede della stessa azienda di Bologna
2. Cosa è una KDF?
   1. È una finzione che permette di rallentare attaccanti che intendono svolgere dictionary attack perché li obbliga a chifrare password e sale per un numero elevato di iterazioni
   2. È una funzione usata per trasformare una password in dati casuali usando una stringa segreta detta sale.
   3. È una funzione che permette di generare chiavi crittografiche a partire da un sale crittografico random
   4. È una funzione che cifra un numero elevato di volte una password ed un sale random per generare delle chiavi crittografiche forti
   5. È una funzione che trasforma dati che non sono pseudo-random in chiavi forti usando l’entropia ottenuta da un sale crittografico generato mediante un processo random.
3. Spiegare cosa è e quale problema permette di risolvere l’Extensible Authentication Protocol (EAP) e quale importante servizio fornisce per rendere possibile la comunicazione.

Inoltre, spiegare cosa è l’EAP-TLS e valutarne l’efficacia.