Modulo 3 – Quiz finale: crittografia e protocolli di sicurezza

1 - Qual è lo scopo principale della crittografia?

A) Ridurre le dimensioni dei dati per facilitarne l'archiviazione
B) Proteggere la riservatezza, l'integrità e l'autenticità delle informazioni
C) Accelerare il traffico di rete
D) Sostituire i sistemi di controllo degli accessi

2 - Quale delle seguenti definizioni descrive meglio la crittografia simmetrica?

A) Utilizza una chiave pubblica per crittografare e una chiave privata per decrittografare
B) Utilizza la stessa chiave segreta per la crittografia e la decrittografia
C) Memorizza le password in modo sicuro tramite hash
D) Firma i messaggi senza crittografia

3 - Quale delle seguenti definizioni descrive meglio la crittografia asimmetrica?

A) La stessa chiave è condivisa da entrambe le parti
B) Utilizza una coppia di chiavi: chiave pubblica (crittografia/verifica), chiave privata (decrittografia/firma)
C) Utilizzata solo per l'hashing
D) Rende superflui i controlli di integrità dei dati

4 - In pratica, perché i sistemi utilizzano la crittografia ibrida?

A) La crittografia a chiave pubblica è più veloce per i dati di grandi dimensioni
B) La crittografia simmetrica è più lenta ma più sicura
C) Combina la crittografia asimmetrica (per lo scambio di una chiave di sessione) con quella simmetrica (per i dati)
D) L'hashing è necessario per crittografare i dati

5 - Quale affermazione sulle funzioni hash è corretta?

A) Sono reversibili con la chiave giusta
B) Mappano l'input su un digest di dimensioni fisse e sono unidirezionali
C) Crittografano sempre i dati
D) Richiedono chiavi pubbliche/private

6 - Quale proprietà è più importante per l'hashing delle password?

A) Solo la resistenza alle collisioni
B) Essere veloce da calcolare
C) Essere lento e salato (ad esempio, con PBKDF2/bcrypt/Argon2)
D) Utilizzo della crittografia simmetrica

7 - Il salting delle password aiuta principalmente a:

A) Accelerare gli accessi
B) Prevenire gli attacchi rainbow table rendendo gli hash unici
C) Comprimere gli hash memorizzati
D) Sostituisci l'autenticazione a due fattori

8 - In che modo una firma digitale fornisce garanzie?

A) Solo riservatezza
B) Integrità e autenticazione dell'origine (e non ripudiabilità)
C) Anonimato
D) Compressione

6 - Che cos'è un certificato digitale?

A) Un file che memorizza la password di un utente
B) Una credenziale che associa una chiave pubblica a un'identità, firmata da una CA
C) Un backup delle chiavi private
D) Un file di configurazione dell'hashing

10 - Qual è il ruolo di un'autorità di certificazione (CA)?

A) Genera chiavi di sessione per TLS
B) Verifica le identità e firma i certificati per stabilire la fiducia
C) Archivia le e-mail crittografate
D) Instradamento sicuro del traffico di rete

11 - Quale delle seguenti non è una proprietà di un buon hash crittografico?

A) Resistenza alla preimmagine
B) Resistenza alla seconda preimmagine
C) Resistenza alla collisione
D) Facile reversibilità

12 - Cosa c'entra l'ASLR o il DEP con la crittografia?

A) Sono algoritmi di crittografia
B) Sono mitigazioni del sistema operativo; distinte dalla crittografia ma utili alla sicurezza
C) Sono algoritmi di hashing
D) Sono protocolli VPN

13 - Quale combinazione di protocolli garantisce la massima sicurezza durante la navigazione web?

A) HTTP + MD5
B) HTTPS (HTTP su TLS)
C) FTP su UDP
D) Telnet con AES

14 - Quale scenario giustifica maggiormente l'uso diretto della crittografia asimmetrica?

A) Crittografia di backup multi-GB locali su disco
B) Distribuzione sicura una tantum di un piccolo segreto a un nuovo utente
C) Crittografia video in streaming
D) Crittografia dell'intero disco su laptop

15 - Arriva un messaggio con una firma verificabile con la chiave pubblica di Alice, ma il testo cifrato era leggibile da chiunque. Quale livello di sicurezza è stato raggiunto?

A) Solo riservatezza
B) Integrità e autenticazione senza riservatezza
C) Solo disponibilità
D) Nessuna garanzia

Laboratorio 3.1 – Crittografia, hashing e firma dei file con GPG

16 - Quale comando genera una nuova coppia di chiavi in GPG?

A) gpg --gen-key
B) gpg --new-hash
C) gpg --make-cert
D) gpg --create-salt

17 - Per crittografare un file per un destinatario utilizzando la sua chiave pubblica, quale comando è corretto?

A) gpg --sign file.txt
B) gpg --encrypt --recipientalice@example.com file.txt
C) gpg --hash sha256 file.txt
D) gpg --export-secret-keys

18 - Quale comando verifica l'integrità di un file tramite SHA-256 (strumenti GNU tipici)?

A) sha256sum file.txt
B) gpg --verify file.txt
C) gpg --armor file.txt
D) openssl enc -aes-256-cbc -in file.txt

16 - Che cos'è una firma separata in GPG?

A) Firma inclusa all'interno del file crittografato
B) Firma memorizzata separatamente (ad esempio, file.txt.sig)
C) Un file non firmato
D) Un certificato chiave revocato

20 - Quale comando verifica una firma separata?

A) gpg --verify file.txt.sig file.txt
B) gpg --decrypt file.txt.sig
C) gpg --list-keys file.txt.sig
D) gpg --clearsign file.txt

Laboratorio 3.2 – Esplorazione pratica di HTTPS e certificati digitali

21 - Il lucchetto del browser indica principalmente che:

A) Il sito è sicuro e affidabile
B) La connessione al sito è crittografata e il certificato è stato convalidato
C) Il sito non presenta vulnerabilità
D) Il sito è approvato dal governo

22 - Quando si controlla un certificato, quali campi aiutano maggiormente a confermare l'identità?

A) Dimensione del file e checksum
B) Nomi host del soggetto e del nome alternativo del soggetto (SAN)
C) Lunghezza dell'elenco delle suite di cifratura
D) Numero di key pinning

23 - Qual è un errore di certificato comune che attiva un avviso?

A) Segretezza perfetta in avanti abilitata
B) Certificato scaduto o nome host non corrispondente
C) CA ampiamente affidabile
D) TLS 1.3 in uso

24 - Cosa mostra la catena di fiducia nel visualizzatore di certificati di un browser?

A) Cronologia dell'algoritmo hash
B) Percorso da certificato server → certificati intermedi → CA radice
C) Tutti i precedenti proprietari del dominio
D) Elenco dei cookie crittografati

25 - Se un sito mostra il messaggio "La tua connessione non è privata" a causa di un emittente non attendibile, qual è l'azione più sicura da intraprendere?

A) Ignorare il messaggio e procedere con la navigazione sul sito
B) Aggiungere immediatamente un'eccezione permanente
C) Non procedere; verificare l'URL/certificato e riprovare più tardi
D) Disattiva la modalità solo HTTPS

Risposte

1. **B** – La crittografia protegge la riservatezza, l'integrità e l'autenticità.
2. **B** – Simmetrica = stessa chiave segreta in entrambe le direzioni.
3. **B** – Asimmetrica utilizza una coppia di chiavi pubblica/privata.
4. **C** – Utilizzare la crittografia asimmetrica per scambiare una chiave di sessione simmetrica, quindi crittografare i dati in modo simmetrico.
5. **B** – L'hashing è una mappatura unidirezionale su un digest di dimensioni fisse.
6. **C** – L'hashing delle password lento, con salt e memory-hard impedisce il cracking.
7. **B** – I salt sconfiggono gli attacchi precalcolati/rainbow table.
8. **B** – Le firme dimostrano l'integrità e l'origine (e supportano la non ripudiabilità).
9. **B** – I certificati legano una chiave pubblica a un'identità tramite la firma CA.
10. **B** – La CA convalida le identità e firma i certificati per stabilire la fiducia.
11. **D** – Gli hash validi *non* sono reversibili.
12. **B** – DEP/ASLR sono misure di mitigazione del sistema operativo, separate dalla crittografia.
13. **B** – HTTPS = HTTP su TLS per un traffico web sicuro.
14. **B** – L'asimmetria è ideale per la distribuzione iniziale di piccoli segreti/chiavi.
15. **B** – Firma verificata → integrità/autenticazione, ma nessuna riservatezza.
16. **A** – gpg --gen-key crea una coppia di chiavi.
17. **B** – Crittografare con la chiave pubblica del destinatario.
18. **A** – sha256sum produce/verifica i digest SHA-256.
19. **B** – La firma separata viene memorizzata separatamente dal file.
20. **A** – gpg --verify sig file controlla una firma separata.
21. **B** – Lucchetto = connessione crittografata + certificato valido (non "sito sicuro").
22. **B** – Oggetto/SAN devono corrispondere al dominio.
23. **B** – La scadenza e la mancata corrispondenza del nome host sono errori classici dei certificati.
24. **B** – Mostra server → intermediario/i → percorso radice attendibile.
25. **C** – Non procedere; verificare l'URL/certificato prima di fidarsi.