Ενότητα 3 – Τελικό Κουίζ: Κρυπτογραφία και Πρωτόκολλα Ασφαλείας

1 - Ποιος είναι ο βασικός σκοπός της κρυπτογραφίας;

A) Συμπίεση δεδομένων για αποθήκευση
B) Διασφάλιση εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των πληροφοριών
C) Επιτάχυνση της κυκλοφορίας στο δίκτυο
D) Αντικατάσταση συστημάτων ελέγχου πρόσβασης

2 - Ποιος ο καλύτερος ορισμός για τη συμμετρική κρυπτογράφηση;

A) Χρησιμοποιεί δημόσιο κλειδί για την κρυπτογράφηση και ιδιωτικό για την αποκρυπτογράφηση
B) Χρησιμοποιεί το ίδιο μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση
C) Αποθηκεύει τους κωδικούς με ασφαλή κατακερματισμό
D) Υπογράφει μηνύματα χωρίς να τα κρυπτογραφεί

3 - Ποιος ο καλύτερος ορισμός για την ασύμμετρη κρυπτογράφηση;

A) Το ίδιο κλειδί χρησιμοποιείται και από τις δύο πλευρές
B) Χρησιμοποιεί ζεύγος κλειδιών: δημόσιο κλειδί (κρυπτογράφηση/επαλήθευση), ιδιωτικό κλειδί (αποκρυπτογράφηση/υπογραφή)
C) Αφορά μόνο τη διαδικασία κατακερματισμού
D) Δεν απαιτούνται έλεγχοι ακεραιότητας δεδομένων

4 - Στην πράξη, γιατί τα συστήματα επιλέγουν υβριδική κρυπτογράφηση;

A) Η κρυπτογράφηση με δημόσιο κλειδί είναι πιο γρήγορη για μεγάλες ποσότητες δεδομένων
B) Η συμμετρική κρυπτογράφηση είναι πιο αργή αλλά προσφέρει μεγαλύτερη ασφάλεια
C) Συνδυάζουμε ασύμμετρη (για ανταλλαγή κλειδιού συνεδρίας) με συμμετρική (για τα δεδομένα)
D) Η διαδικασία κατακερματισμού απαιτείται για την κρυπτογράφηση των δεδομένων

5 - Ποια δήλωση για τις συναρτήσεις κατακερματισμού είναι σωστή;

A) Είναι αναστρέψιμες με το κατάλληλο κλειδί
B) Μετατρέπουν την είσοδο σε μια σύνοψη σταθερού μεγέθους και λειτουργούν μόνο προς μία κατεύθυνση
C) Κρυπτογραφούν πάντα τα δεδομένα
D) Απαιτούν δημόσια/ιδιωτικά κλειδιά

6 - Ποια ιδιότητα είναι πιο σημαντική για το κατακερματισμό κωδικών πρόσβασης;

A) Μόνο ανθεκτικότητα σε συγκρούσεις
B) Η γρήγορη εκτέλεση
C) Η αργή διαδικασία με προσθήκη salt (π.χ. PBKDF2/bcrypt/Argon2)
D) Η χρήση συμμετρικής κρυπτογράφησης αντί αυτού

7 - Ποια είναι η κύρια συμβολή του αλατιού στους κωδικούς πρόσβασης;

A) Επιτάχυνση της διαδικασίας σύνδεσης
B) Αποτροπή επιθέσεων με rainbow-table κάνοντας τα hash μοναδικά
C) Συμπίεση των αποθηκευμένων hash
D) Αντικατάσταση της ταυτοποίησης δύο παραγόντων

8 - Με ποιο τρόπο μια ψηφιακή υπογραφή παρέχει εγγύηση;

A) Μόνο εμπιστευτικότητα
B) Ακεραιότητα και επαλήθευση προέλευσης (και μη-αποποίηση ευθύνης)
C) Ανωνυμία
D) Συμπίεση

9 - Τι είναι το ψηφιακό πιστοποιητικό;

A) Ένα αρχείο που αποθηκεύει τον κωδικό πρόσβασης ενός χρήστη
B) Ένα διαπιστευτήριο που συνδέει ένα δημόσιο κλειδί με μια ταυτότητα και φέρει υπογραφή από μια Αρχή Πιστοποίησης (CA)
C) Ένα αντίγραφο ασφαλείας ιδιωτικών κλειδιών
D) Ένα αρχείο ρυθμίσεων κατακερματισμού

10 - Ποιος είναι ο ρόλος μιας Αρχής Πιστοποίησης (CA);

A) Δημιουργεί κλειδιά συνεδρίας για TLS
B) Επαληθεύει ταυτότητες και υπογράφει πιστοποιητικά για την εδραίωση εμπιστοσύνης
C) Αποθηκεύει κρυπτογραφημένα email
D) Δρομολογεί με ασφάλεια την κίνηση δικτύου

11 - Ποια δεν είναι ιδιότητα ενός καλού κρυπτογραφικού κατακερματισμού;

A) Αντοχή στην εύρεση προεικόνας
B) Αντοχή στη δεύτερη προεικόνα
C) Αντοχή σε συγκρούσεις
D) Εύκολη αντιστρεψιμότητα

12 - Τι σχέση έχουν η ASLR ή η DEP με την κρυπτογραφία;

A) Είναι αλγόριθμοι κρυπτογράφησης
B) Πρόκειται για μετριασμούς λειτουργικού συστήματος, διαφορετικοί από την κρυπτογραφία, αλλά βοηθούν στην ασφάλεια.
C) Είναι αλγόριθμοι κατακερματισμού
D) Είναι πρωτόκολλα VPN

13 - Ποιος συνδυασμός πρωτοκόλλου ασφαλίζει με μεγαλύτερη ακρίβεια την περιήγηση στο διαδίκτυο;

A) HTTP + MD5
B) HTTPS (HTTP μέσω TLS)
C) FTP μέσω UDP
D) Telnet με AES

14 - Ποιο σενάριο δικαιολογεί καλύτερα την άμεση χρήση ασύμμετρης κρυπτογράφησης;

A) Κρυπτογράφηση αντιγράφων ασφαλείας πολλών GB τοπικά στον δίσκο
B) Εφάπαξ ασφαλής διανομή ενός μικρού μυστικού σε έναν νέο χρήστη
C) Κρυπτογράφηση ροής βίντεο
D) Κρυπτογράφηση πλήρους δίσκου σε φορητούς υπολογιστές

15 - Ένα μήνυμα φτάνει με υπογραφή που επαληθεύεται με το δημόσιο κλειδί της Alice, αλλά το κρυπτογράφημα ήταν αναγνώσιμο από όλους. Ποια ασφάλεια επιτεύχθηκε;

A) Μόνο εμπιστευτικότητα
B) Ακεραιότητα και ταυτοποίηση χωρίς εμπιστευτικότητα
C) Μόνο διαθεσιμότητα
D) Καμία εγγύηση

Εργαστήριο 3.1 – Κρυπτογράφηση, δημιουργία κατακερματισμών και υπογραφή αρχείων με το GPG

16 - Ποια εντολή δημιουργεί ένα νέο ζεύγος κλειδιών στο GPG;

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

17 - Ποια είναι η σωστή εντολή για να κρυπτογραφήσετε ένα αρχείο για κάποιον παραλήπτη χρησιμοποιώντας το δημόσιο κλειδί του;

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

18 - Ποια εντολή ελέγχει την ακεραιότητα ενός αρχείου με SHA-256 (συνήθη εργαλεία GNU);

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

19 - Τι είναι μια αποσυνδεδεμένη υπογραφή στο GPG;

A) Υπογραφή που βρίσκεται ενσωματωμένη μέσα στο κρυπτογραφημένο αρχείο
B) Υπογραφή που αποθηκεύεται ξεχωριστά (π.χ. file.txt.sig)
C) Αρχείο χωρίς υπογραφή
D) Πιστοποιητικό κλειδιού που έχει ανακληθεί

20 - Ποια εντολή ελέγχει μια αποσυνδεδεμένη υπογραφή;

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

Εργαστήριο 3.2 – Πρακτική εξερεύνηση του HTTPS και των Ψηφιακών Πιστοποιητικών

21 - Το λουκέτο του προγράμματος περιήγησης δείχνει κυρίως:

A) Ο ιστότοπος είναι ασφαλής και αξιόπιστος
B) Η σύνδεση με τον ιστότοπο είναι κρυπτογραφημένη και έχει πιστοποιηθεί
C) Ο ιστότοπος δεν παρουσιάζει ευπάθειες
D) Ο ιστότοπος έχει εγκριθεί από τις αρχές

22 - Κατά τον έλεγχο ενός πιστοποιητικού, ποια πεδία βοηθούν περισσότερο στην επιβεβαίωση της ταυτότητας;

A) Μέγεθος αρχείου και άθροισμα ελέγχου
B) Όνομα υποκειμένου και ονόματα κεντρικού υποκειμένου (SAN)
C) Μήκος λίστας αλγορίθμων κρυπτογράφησης
D) Πλήθος key pinning

23 - Ποιο είναι ένα συνηθισμένο σφάλμα πιστοποιητικού που εμφανίζει προειδοποίηση;

A) Ενεργοποιημένο το τέλειο εμπιστευτικό κανάλι
B) Το πιστοποιητικό έληξε ή υπάρχει ασυμφωνία στο όνομα του διακομιστή
C) Η Αρχή Πιστοποίησης είναι ευρέως αξιόπιστη
D) Χρησιμοποιείται TLS 1.3

24 - Τι παρουσιάζει η αλυσίδα εμπιστοσύνης στον προβολέα πιστοποιητικών ενός προγράμματος περιήγησης;

A) Ιστορικό αλγορίθμων κατακερματισμού
B) Διαδρομή από το πιστοποιητικό διακομιστή → ενδιάμεσοι → ριζική αρχή έκδοσης
C) Όλοι οι προηγούμενοι κάτοχοι του domain
D) Λίστα με κρυπτογραφημένα cookies

25 - Αν εμφανιστεί το μήνυμα «Η σύνδεσή σας δεν είναι ιδιωτική» λόγω μη αξιόπιστου εκδότη, ποια είναι η πιο ασφαλής ενέργεια;

A) Αγνοήστε και συνεχίστε στην ιστοσελίδα
B) Προσθέστε αμέσως μόνιμη εξαίρεση
C) Μην συνεχίσετε· ελέγξτε το URL/πιστοποιητικό και δοκιμάστε ξανά αργότερα
D) Απενεργοποιήστε τη λειτουργία μόνο HTTPS

Λύσεις Εξετάσεων

1. **B** – Η κρυπτογραφία διασφαλίζει το απόρρητο, την ακεραιότητα και τη γνησιότητα.
2. **B** – Συμμετρική: ίδιο μυστικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.
3. **B** – Ασύμμετρη: ζεύγος δημόσιου/ιδιωτικού κλειδιού.
4. **C** – Αξιοποιούμε ασύμμετρη μέθοδο για ανταλλαγή συμμετρικού κλειδιού συνεδρίας και μετά κρυπτογραφούμε τα δεδομένα συμμετρικά.
5. **B** – Το hashing είναι μονόδρομος που παράγει αποτύπωμα σταθερού μεγέθους.
6. **C** – Αργό, με αλάτι και με απαιτήσεις μνήμης hashing κωδικών αποτρέπει παραβιάσεις.
7. **B** – Τα salts ακυρώνουν τις επιθέσεις προϋπολογισμένων/“rainbow-table”.
8. **B** – Οι ψηφιακές υπογραφές πιστοποιούν ακεραιότητα και προέλευση (και ενισχύουν την μη-άρνηση).
9. **B** – Τα πιστοποιητικά συνδέουν δημόσιο κλειδί με ταυτότητα μέσω υπογραφής ΑΠ (CA).
10. **B** – Η ΑΠ επαληθεύει ταυτότητες και υπογράφει πιστοποιητικά για να θεμελιώσει εμπιστοσύνη.
11. **D** – Τα σωστά hashes *δεν* γυρίζουν πίσω στο αρχικό.
12. **B** – DEP/ASLR είναι μέτρα του λειτουργικού συστήματος, άσχετα με την κρυπτογραφία.
13. **B** – HTTPS = HTTP πάνω από TLS για ασφαλή διακίνηση στο Web.
14. **B** – Η ασύμμετρη κρυπτογράφηση είναι ιδανική για αρχική διανομή μικρών μυστικών/κλειδιών.
15. **B** – Επικυρωμένη υπογραφή σημαίνει ακεραιότητα/ταυτοποίηση, όχι απόρρητο.
16. **A** – gpg --gen-key δημιουργεί ζεύγος κλειδιών.
17. **B** – Κρυπτογράφηση με το δημόσιο κλειδί του παραλήπτη.
18. **A** – sha256sum παράγει/ελέγχει αποτυπώματα SHA-256.
19. **B** – Η αποσυνδεδεμένη υπογραφή αποθηκεύεται ξεχωριστά από το αρχείο.
20. **A** – gpg --verify sig file ελέγχει αποσυνδεδεμένη υπογραφή.
21. **B** – Το λουκέτο σημαίνει κρυπτογραφημένη σύνδεση + έγκυρο πιστοποιητικό (όχι «ασφαλής ιστότοπος»).
22. **B** – Το Subject/SAN πρέπει να ταιριάζει με το domain.
23. **B** – Λήξη και ασυμφωνία domain είναι κλασικά σφάλματα πιστοποιητικών.
24. **B** – Εμφανίζει διαδρομή διακομιστή → ενδιάμεσων → έμπιστης ρίζας.
25. **C** – Μην συνεχίσετε· ελέγξτε το URL/πιστοποιητικό πριν εμπιστευτείτε.