Ενότητα 2 – Τελικό Κουίζ: Ασφάλεια Λειτουργικού Συστήματος & Δικτύου

1 - Ποιος είναι ο βασικός στόχος της ασφάλειας ενός λειτουργικού συστήματος;

A) Να αυξήσει την ταχύτητα του λειτουργικού συστήματος
B) Να προστατεύει το λειτουργικό σύστημα από μη εξουσιοδοτημένη πρόσβαση και ευπάθειες
C) Να επιτρέπει απεριόριστη διαχειριστική πρόσβαση
D) Να εξασφαλίζει ότι το λειτουργικό σύστημα έχει ελκυστική εμφάνιση

2 - Ποιο από τα παρακάτω αποτελεί παράδειγμα συχνής απειλής για την ασφάλεια ενός λειτουργικού συστήματος;

A) Εκδόσεις χωρίς τις τελευταίες ενημερώσεις και ελλιπή patches
B) Ενεργοποίηση σκοτεινής λειτουργίας
C) Συμπίεση αρχείων
D) Εγκατάσταση γραμματοσειρών

3 - Γιατί είναι τόσο σημαντικά τα patches και οι ενημερώσεις λογισμικού για την ασφάλεια του λειτουργικού συστήματος;

A) Κάνει το λειτουργικό σύστημα να φαίνεται πιο σύγχρονο
B) Προσθέτει νέους οδηγούς για υλικό
C) Εξαλείφει τα τρωτά σημεία ασφαλείας προτού τα εκμεταλλευτούν κακόβουλοι χρήστες
D) Είναι προαιρετικά και δεν σχετίζονται με την ασφάλεια

4 - Ποια μέθοδος χρησιμοποιείται συνήθως για να ελέγχεται ποιος μπορεί να εισέλθει σε ένα σύστημα;

A) Έλεγχος πρόσβασης
B) Συμπίεση αρχείων
C) Δικτυακή προσωρινή αποθήκευση
D) Αντίγραφα ασφαλείας δεδομένων

5 - Ποια μέθοδος ενισχύει την ασφάλεια απενεργοποιώντας υπηρεσίες που δεν χρειάζονται;

A) Λίστα επιτρεπόμενων εφαρμογών
B) Ενίσχυση του λειτουργικού συστήματος
C) Κρυπτογράφηση
D) Αντιικό λογισμικό

6 - Γιατί είναι σημαντικό να αφαιρούνται ή να περιορίζονται οι προεπιλεγμένοι λογαριασμοί;

A) Συχνά είναι ανασφαλείς και μπορούν να γίνουν στόχος επιθέσεων
B) Μειώνουν την απόδοση του συστήματος
C) Δεν συνεργάζονται με σύγχρονο λογισμικό
D) Καταλαμβάνουν περισσότερο χώρο στον δίσκο

7 - Τι σημαίνει η διαδικασία λευκής λίστας εφαρμογών;

A) Επιτρέπονται μόνο οι εφαρμογές που έχουν εγκριθεί
B) Αποκλεισμός όλων των εφαρμογών από προεπιλογή
C) Κρυπτογράφηση εφαρμογών κατά τη διάρκεια λειτουργίας
D) Απεγκατάσταση αχρησιμοποίητων εφαρμογών

8 - Ποια από τις παρακάτω μεθόδους βοηθά στον εντοπισμό ασυνήθιστης ή κακόβουλης δραστηριότητας του λειτουργικού συστήματος;

A) Ανασυγκρότηση δίσκου
B) Καταγραφή και παρακολούθηση
C) Εκκαθάριση δίσκου
D) Εικονικοποίηση

9 - Τι σημαίνει διαφθορά μνήμης;

A) Ένα πρόβλημα με αργή μνήμη RAM
B) Όταν οι εισβολείς εκμεταλλεύονται αδυναμίες στον τρόπο διαχείρισης της μνήμης
C) Σφάλμα αποθήκευσης στον σκληρό δίσκο
D) Λανθασμένη ρύθμιση ενημέρωσης του λειτουργικού συστήματος

10 - Ποια είναι η λειτουργία της Προστασίας Εκτέλεσης Δεδομένων (DEP);

A) Αποτρέπει τη χρήση της μνήμης για εκτέλεση κακόβουλου κώδικα
B) Κρυπτογραφεί όλα τα αρχεία του συστήματος
C) Διαγράφει αλλοιωμένη μνήμη
D) Δημιουργεί νέες κατατμήσεις μνήμης

11 - Ποιος είναι ο σκοπός της Τυχαιοποίησης Διάταξης Χώρου Διευθύνσεων (ASLR);

A) Για να κρύβονται οι λογαριασμοί χρηστών από επιτιθέμενους
B) Για να αναδιατάσσονται τυχαία οι διευθύνσεις της μνήμης, δυσκολεύοντας τις επιθέσεις
C) Για να κρυπτογραφείται η δικτυακή κίνηση
D) Για να αποκλείονται άγνωστες διευθύνσεις IP

12 - Ποιο από τα παρακάτω ΔΕΝ θεωρείται συνηθισμένη απειλή για την ασφάλεια δικτύου;

A) Επιθέσεις τύπου Man-in-the-Middle
B) Παρακολούθηση πακέτων
C) SQL injection
D) Ανασυγκρότηση σκληρών δίσκων

13 - Ποιος είναι ο σκοπός της χρήσης VPN;

A) Για τον αποκλεισμό διαφημίσεων σε ιστοσελίδες
B) Για τη δημιουργία κρυπτογραφημένης σήραγγας για ασφαλή μεταφορά δεδομένων
C) Για τη μείωση της ταχύτητας του διαδικτύου
D) Για σάρωση ιών

14 - Ποιο πρότυπο ασφάλειας για ασύρματα δίκτυα θεωρείται σήμερα το πιο ισχυρό;

A) WEP
B) WPA
C) WPA2
D) WPA3

15 - Γιατί θεωρείται επικίνδυνο το δημόσιο Wi-Fi;

A) Καταναλώνει περισσότερη μπαταρία
B) Συχνά έχει αδύναμη ή ανύπαρκτη κρυπτογράφηση, εκθέτοντας τα δεδομένα των χρηστών
C) Είναι πιο αργό σε σχέση με το ιδιωτικό Wi-Fi
D) Δεν υποστηρίζει μεγάλες λήψεις αρχείων

Εργαστήριο 2.1 – Ρύθμιση Πολιτικών Ασφαλείας σε Εικονική Μηχανή

16 - Γιατί οι εικονικές μηχανές είναι χρήσιμες για εξάσκηση σε εργαστήρια ασφάλειας;

A) Είναι πιο γρήγορες από τις φυσικές μηχανές
B) Απομονώνουν το περιβάλλον, μειώνοντας τους κινδύνους για το κύριο σύστημα
C) Εντοπίζουν και διορθώνουν αυτόματα τρωτά σημεία
D) Δεν απαιτούν επιπλέον υλικό εξοπλισμό

17 - Ποιο εργαλείο των Windows εφαρμόζει πολιτικές κωδικών πρόσβασης;

A) Επεξεργαστής Ομαδικής Πολιτικής
B) Διαχειριστής Εργασιών
C) Διαχειριστής Συσκευών
D) Εξερευνητής Αρχείων

18 - Στο Linux, ποιο αρχείο βοηθά στον καθορισμό πολιτικών κωδικών πρόσβασης;

A) /etc/login.defs
B) /etc/services
C) /etc/networks
D) /etc/hosts

19 - Ποιος είναι ο σκοπός του περιορισμού των διαχειριστικών δικαιωμάτων;

A) Για να αποφεύγονται οι περιττές ενημερώσεις λογισμικού
B) Για να μειώνεται ο κίνδυνος κακής χρήσης ή επιθέσεων αύξησης δικαιωμάτων

Γ) Για να αυξηθεί η ταχύτητα της σύνδεσης

Δ) Για να δίνεται πλήρης έλεγχος του συστήματος στους χρήστες

20 - Ποιο από τα παρακάτω χρησιμοποιείται για την παρακολούθηση συστήματος στο Linux;

A) Προβολή Συμβάντων
B) Syslog
C) Διαχείριση Δίσκων
D) Επεξεργαστής Μητρώου

Εργαστήριο 2.2 – Ανάλυση Πακέτων με το Wireshark

21 - Ποιος είναι ο βασικός σκοπός της ανάλυσης πακέτων;

A) Ανασυγκρότηση σκληρών δίσκων
B) Εξέταση και κατανόηση της κίνησης στο δίκτυο
C) Απεγκατάσταση μη χρησιμοποιούμενων εφαρμογών
D) Επιτάχυνση της απόδοσης του συστήματος

22 - Όταν ξεκινάτε το Wireshark, τι πρέπει να επιλέξετε πρώτα;

A) Τύπος προγράμματος περιήγησης
B) Διεπαφή δικτύου για καταγραφή της κυκλοφορίας
C) Εργαλείο προστασίας από ιούς
D) Διαδρομή εξερευνητή αρχείων

23 - Ποιο φίλτρο του Wireshark θα χρησιμοποιούσατε για να εμφανίζετε μόνο την HTTP κίνηση;

A) dns
B) http
C) icmp
D) tcp.port == 22

24 - Γιατί είναι σημαντικό να εντοπίζουμε μη κρυπτογραφημένη κίνηση;

A) Αποκαλύπτει το ιστορικό ενημερώσεων του συστήματος
B) Βοηθά στον εντοπισμό ευαίσθητων δεδομένων που μπορεί να διαρρεύσουν σε επιτιθέμενους
C) Συμβάλλει στη βελτίωση της ταχύτητας του διαδικτύου
D) Αποτρέπει τη λήψη ανεπιθύμητων email

25 - Στη δοκιμασία του εργαστηρίου, τι είδους ερωτήματα καλούνται οι φοιτητές να συλλέξουν και να αναλύσουν;

A) Ερωτήματα FTP
B) Ερωτήματα DNS
C) Ερωτήματα SQL
D) Αρχεία καταγραφής VPN

Εργαστήριο 2.3 – Διαμόρφωση και Έλεγχος VPN

26 - Τι καλύπτει κυρίως ένα VPN από τρίτους;

A) Ιστορικό περιήγησης
B) Διεύθυνση IP και περιεχόμενο δικτυακής κίνησης
C) Εγκατεστημένες εφαρμογές
D) Χαρακτηριστικά υλικού υπολογιστή

27 - Ποια δοκιμή επιβεβαιώνει ότι το VPN σας προστατεύει την κίνηση DNS;

A) Έλεγχος ταχύτητας
B) Δοκιμή διαρροής DNS
C) Έλεγχος με antivirus
D) Έλεγχος ακεραιότητας αρχείων

28 - Ποια είναι η λειτουργία του «kill switch» σε ένα VPN;

A) Τερματίζει το VPN μετά από 1 ώρα
B) Αποτρέπει την πρόσβαση στο διαδίκτυο αν διακοπεί το VPN
C) Διαγράφει το ιστορικό περιήγησης μετά τη χρήση
D) Επιταχύνει τη σύνδεση του VPN

29 - Γιατί προτείνεται να συγκρίνουμε τα δεδομένα δικτύου με και χωρίς VPN;

A) Για να διαπιστώσουμε αν το VPN επιβραδύνει την περιήγηση
B) Για να επιβεβαιώσουμε ότι γίνεται κρυπτογράφηση της κυκλοφορίας
C) Για να ελέγξουμε την απόδοση του Wi-Fi
D) Για να μειώσουμε τη χρήση μνήμης

30 - Ποια από τις παρακάτω επιλογές είναι ένα συνηθισμένο προαιρετικό χαρακτηριστικό στους πελάτες VPN;

A) Αυτόματη σύνδεση κατά την εκκίνηση
B) Συμπίεση αρχείων
C) Λειτουργία εξοικονόμησης ενέργειας
D) Χρώμα φόντου εφαρμογής

Λύσεις Ερωτήσεων

1. **B** – Η ασφάλεια λειτουργικού συστήματος σημαίνει προστασία από μη εξουσιοδοτημένη πρόσβαση και ευπάθειες.
2. **A** – Οι ξεπερασμένες ενημερώσεις αποτελούν μεγάλο κίνδυνο.
3. **C** – Οι ενημερώσεις διορθώνουν κενά ασφαλείας πριν τα εκμεταλλευτούν κακόβουλοι χρήστες.
4. **A** – Ο έλεγχος πρόσβασης διαχειρίζεται συνδέσεις και δικαιώματα χρηστών.
5. **B** – Η σκλήρυνση συστήματος απενεργοποιεί άχρηστες λειτουργίες/υπηρεσίες.
6. **A** – Οι προεπιλεγμένοι λογαριασμοί είναι ευάλωτοι αν δεν περιοριστούν.
7. **A** – Η λευκή λίστα επιτρέπει μόνο τις εγκεκριμένες εφαρμογές να εκτελούνται.
8. **B** – Τα αρχεία καταγραφής εντοπίζουν ασυνήθιστη δραστηριότητα.
9. **B** – Παραμόρφωση μνήμης είναι σφάλμα στη διαχείριση της μνήμης.
10. **A** – Το DEP αποτρέπει την εκτέλεση από μη ασφαλείς περιοχές μνήμης.
11. **B** – Το ASLR τυχαία διαμορφώνει τη δομή της μνήμης.
12. **D** – Η ανασυγκρότηση δεν αποτελεί απειλή για το δίκτυο.
13. **B** – Τα VPN διασφαλίζουν την κυκλοφορία μέσω κρυπτογράφησης.
14. **D** – Το WPA3 είναι το πιο ισχυρό πρότυπο για Wi-Fi.
15. **B** – Τα δημόσια δίκτυα Wi-Fi συχνά δεν έχουν κρυπτογράφηση.
16. **B** – Οι εικονικές μηχανές απομονώνουν τα εργαστήρια και προστατεύουν το βασικό σύστημα.
17. **A** – Πολιτικές κωδικών πρόσβασης: μέσω Group Policy Editor.
18. **A** – Το αρχείο /etc/login.defs διαχειρίζεται τις ρυθμίσεις κωδικών.
19. **B** – Η αρχή της ελάχιστης προνομίας μειώνει τον κίνδυνο κατάχρησης.
20. **B** – Τα syslog και auth.log είναι εργαλεία παρακολούθησης στο Linux.
21. **B** – Η ανάλυση πακέτων αφορά την εξέταση της κυκλοφορίας δικτύου.
22. **B** – Πρέπει να επιλεγεί μια διεπαφή δικτύου.
23. **B** – Το φίλτρο “http” εμφανίζει τα HTTP πακέτα.
24. **B** – Μη κρυπτογραφημένη κίνηση μπορεί να αποκαλύψει ευαίσθητα δεδομένα.
25. **B** – Πρόκληση: ανάλυση DNS ερωτημάτων.
26. **B** – Το VPN κρύβει τη διεύθυνση IP και κρυπτογραφεί την κίνηση.
27. **B** – Τα τεστ διαρροής DNS επιβεβαιώνουν την προστασία της ιδιωτικότητας.
28. **B** – Το kill switch διακόπτει την κυκλοφορία εάν το VPN πέσει.
29. **B** – Η σύγκριση δείχνει την επίδραση της κρυπτογράφησης.
30. **A** – Η αυτόματη σύνδεση είναι συχνή ρύθμιση στα VPN.