# Ενότητα 1 – Τελικό Κουίζ: Εισαγωγή στην Κυβερνοασφάλεια

1 - Ποιος από τους παρακάτω ορισμούς περιγράφει καλύτερα την κυβερνοασφάλεια;

A) Η προστασία των υλικών αγαθών από κλοπή
B) Η διασφάλιση ψηφιακών συστημάτων, δικτύων και δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή επιθέσεις
C) Η εγκατάσταση λογισμικού προστασίας από ιούς σε προσωπικό υπολογιστή
D) Μόνο η προστασία προσωπικών δεδομένων στα κοινωνικά δίκτυα

2 - Ποιος χρειάζεται προστασία από τις απειλές στον κυβερνοχώρο;

A) Μόνο κυβερνήσεις και μεγάλες εταιρείες
B) Μόνο τράπεζες και χρηματοπιστωτικά ιδρύματα
C) Όλοι, από άτομα μέχρι παγκόσμιους οργανισμούς
D) Μόνο επαγγελματίες της πληροφορικής

3 - Ποιο από τα παρακάτω αποτελεί συνηθισμένο παράδειγμα κυβερνοεπίθεσης;

A) Μορφοποίηση ενός σκληρού δίσκου
B) Εγκατάσταση ενημερώσεων λογισμικού
C) Δόλιες ηλεκτρονικές επιστολές που ζητούν στοιχεία σύνδεσης
D) Διαγραφή προσωρινών αρχείων

4 - Τι είναι το ransomware;

A) Λογισμικό που εντοπίζει κακόβουλο λογισμικό στον υπολογιστή σας
B) Κακόβουλο λογισμικό που κλειδώνει αρχεία και απαιτεί λύτρα για την επαναφορά της πρόσβασης
C) Επίθεση ηλεκτρονικού ψαρέματος μέσω email
D) Επίθεση με δοκιμές κωδικών πρόσβασης

## 5 - Ποια από τις παρακάτω επιθέσεις στοχεύει τον ανθρώπινο παράγοντα της ασφάλειας;

A) Επίθεση Άρνησης Παροχής Υπηρεσιών (Denial-of-Service)
B) Επίθεση Brute-Force
C) Phishing και Κοινωνική Μηχανική
D) Εκμετάλλευση Zero-Day

## 6 - Τι σημαίνει το “C” στο τρίπτυχο CIA;

A) Έλεγχος
B) Κρυπτογράφηση
C) Εμπιστευτικότητα
D) Επικοινωνία

## 7 - Ποια αρχή διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο σε ό,τι είναι απολύτως απαραίτητο;

A) Πολυεπίπεδη Άμυνα
B) Ελάχιστα Δικαιώματα
C) Zero Trust
D) Ασφάλεια από τον Σχεδιασμό

### 8 - Με ποιον βασικό τρόπο προστατεύει ένα τείχος προστασίας το σύστημα;

A) Κρυπτογράφηση όλων των αρχείων στον υπολογιστή
B) Φιλτράρισμα εισερχόμενης και εξερχόμενης κίνησης βάσει κανόνων
C) Εντοπισμός και αφαίρεση ιών
D) Αποκλεισμός πρόσβασης σε ιστότοπους κοινωνικής δικτύωσης

### 9 - Ποια από τις παρακάτω ενέργειες πραγματοποιεί ένα πρόγραμμα προστασίας από ιούς;

A) Κρυπτογράφηση της διαδικτυακής κίνησης
B) Εντοπισμός και απομόνωση κακόβουλων αρχείων
C) Αποκλεισμός ύποπτων διευθύνσεων IP
D) Παρακολούθηση των κανόνων του τείχους προστασίας

## 10 - Γιατί συνιστάται συχνά να χρησιμοποιούμε και τείχος προστασίας και λογισμικό antivirus;

A) Κάνουν ακριβώς το ίδιο, οπότε η επανάληψη είναι χρήσιμη
B) Τα firewalls εμποδίζουν εισβολές, το antivirus απομακρύνει τις μολύνσεις
C) Το antivirus καθιστά τα firewalls περιττά
D) Τα firewalls λειτουργούν μόνο σε Linux, το antivirus μόνο σε Windows

## 11 - Ποια εντολή Linux ενεργοποιεί το firewall με το UFW;

A) sudo firewall ενεργοποίηση
B) ufw επιτρέπονται όλα
C) sudo ufw enable
D) ενεργοποίηση ufw firewall

### 12 - Στα εργαλεία antivirus, η καραντίνα ενός αρχείου σημαίνει:

A) Αυτόματη οριστική διαγραφή
B) Κρυπτογράφηση με ισχυρό κωδικό πρόσβασης
C) Απομόνωση ώστε να μην βλάπτει το σύστημα
D) Αποστολή σε εφεδρικό διακομιστή

## 13 - Λαμβάνετε ένα email από την «τράπεζά» σας που σας ζητά να επιβεβαιώσετε τον κωδικό πρόσβασής σας μέσω ενός συνδέσμου. Ποια έννοια σας βοηθά να αναγνωρίσετε ότι αυτό είναι phishing;

A) Εμπιστευτικότητα
B) Πολυεπίπεδη Άμυνα
C) Ευαισθητοποίηση για Κοινωνική Μηχανική
D) Αρχή της Μη Εμπιστοσύνης

14 - Ποιο από τα παρακάτω αποτελεί το καλύτερο παράδειγμα Αρχιτεκτονικής Zero Trust;

A) Οι εργαζόμενοι έχουν απεριόριστη πρόσβαση μόλις μπουν στο δίκτυο
B) Οι συσκευές και οι χρήστες πρέπει να επαληθεύονται συνεχώς πριν αποκτήσουν πρόσβαση σε πόρους
C) Η εταιρεία χρησιμοποιεί μόνο ένα ισχυρό firewall
D) Όλη η ασφάλεια βασίζεται αποκλειστικά σε σαρώσεις antivirus

15 - Τα αρχεία καταγραφής του firewall εμφανίζουν επανειλημμένες προσπάθειες από άγνωστη διεύθυνση IP στη θύρα 22 (SSH). Ποια είναι η καλύτερη άμεση ενέργεια;

A) Αγνόησέ το, μάλλον είναι απλός «θόρυβος»
B) Απόκλεισε τη διεύθυνση IP και έλεγξε τους κανόνες του firewall για SSH
C) Απεγκατάστησε το firewall και εγκατάστησε ξανά το antivirus
D) Επίτρεψε τη σύνδεση για να δεις τι θα συμβεί

## Εργαστήριο 1.1 – Ερωτήσεις για το Firewall

16 - Ποια από τις παρακάτω επιλογές περιγράφει καλύτερα ένα firewall;

A) Ένα εργαλείο για κρυπτογράφηση αρχείων
B) Ένα «τείχος» που ελέγχει την κυκλοφορία δεδομένων στο δίκτυο με βάση κανόνες
C) Ένας σαρωτής που εντοπίζει ιούς
D) Ένα πρόγραμμα που παρακολουθεί τη χρήση του επεξεργαστή

## 17 - Ποιο εργαλείο των Windows χρησιμοποιείται για τη ρύθμιση προχωρημένων κανόνων firewall;

A) Διαχείριση Εργασιών
B) Γραμμή Εντολών
C) Windows Defender Firewall με Προηγμένες Ρυθμίσεις Ασφαλείας
D) Διαχείριση Συσκευών

## 18 - Ποιος είναι ο λόγος που μπλοκάρουμε τη θύρα 22 (SSH) στη ρύθμιση του τείχους προστασίας;

A) Για να αποτρέψουμε την αποστολή ανεπιθύμητων email
B) Για να σταματήσουμε μη εξουσιοδοτημένες απομακρυσμένες συνδέσεις
C) Για να απενεργοποιήσουμε την περιήγηση στο διαδίκτυο
D) Για να βελτιώσουμε την απόδοση του συστήματος

### 19 - Ποια εντολή εμφανίζει τους ενεργούς κανόνες του τείχους προστασίας στο Linux UFW;

A) ufw κανόνες λίστας
B) sudo ufw status
C) λίστα firewall
D) netstat --ufw

## 20 - Στην εργαστηριακή δοκιμασία (επιτρέψτε το HTTP, αποκλείστε τα υπόλοιπα), ποια θύρα πρέπει να παραμείνει ανοιχτή;

A) 22
B) 25
C) 80
D) 443

### Εργαστήριο 1.2 – Ερωτήσεις για το Αντιβιοτικό Λογισμικό

## 21 - Ποιο είναι το πρώτο βήμα πριν ξεκινήσετε μια σάρωση για ιούς;

A) Απενεργοποιήστε το τείχος προστασίας σας
B) Ενημερώστε τις βάσεις δεδομένων ιών
C) Επανεγκαταστήστε το πρόγραμμα προστασίας από ιούς
D) Εκτελέστε επαναφορά συστήματος

## 22 - Στο Microsoft Defender, ποια επιλογή προσφέρει τον πιο ολοκληρωμένο έλεγχο;

A) Γρήγορη σάρωση
B) Προσαρμοσμένη σάρωση
C) Πλήρης σάρωση
D) Έλεγχος ιστορικού

## 23 - Ποια εντολή Linux ενημερώνει τη βάση δεδομένων ιών του ClamAV;

A) sudo freshclam
B) sudo update-av
C) clamav --update
D) av-refresh

## 24 - Εάν το antivirus εντοπίσει ένα ύποπτο αρχείο, ποια είναι η πιο ασφαλής πρώτη ενέργεια;

A) Διαγραφή αμέσως χωρίς έλεγχο
B) Μετακίνηση σε καραντίνα για αποτροπή εκτέλεσης
C) Αγνόηση της προειδοποίησης αν φαίνεται ακίνδυνο το αρχείο
D) Αποστολή σε όλους τους συναδέλφους για έλεγχο

## 25 - Ποια ενέργεια θεωρείται βέλτιστη πρακτική μετά την επανεξέταση των αποτελεσμάτων σάρωσης από το antivirus;

A) Απενεργοποιήστε το antivirus για εξοικονόμηση πόρων
B) Ελέγξτε τα αρχεία καταγραφής και επιβεβαιώστε τυχόν ψευδώς θετικά πριν προχωρήσετε
C) Εκτελέστε μόνο μία σάρωση τον χρόνο
D) Υποθέστε ότι δεν απαιτείται περαιτέρω ενέργεια

## Λύσεις Απαντήσεων

1. **B** – Κυβερνοασφάλεια = προστασία ψηφιακών συστημάτων και δεδομένων.
2. **C** – Η κυβερνοασφάλεια αφορά όλους.
3. **C** – Τα phishing emails είναι κλασικές επιθέσεις στον κυβερνοχώρο.
4. **B** – Το ransomware κλειδώνει αρχεία και απαιτεί λύτρα.
5. **C** – Η κοινωνική μηχανική στοχεύει τους ανθρώπους, όχι τα μηχανήματα.
6. **C** – "C" = Εμπιστευτικότητα.
7. **B** – Ελάχιστα δικαιώματα = μόνο όσα είναι απολύτως απαραίτητα.
8. **B** – Τα firewalls φιλτράρουν την κυκλοφορία, όχι τα αρχεία.
9. **B** – Το antivirus ανιχνεύει και απομονώνει κακόβουλα αρχεία.
10. **B** – Συμπληρώνουν το ένα το άλλο: εισβολή vs μόλυνση.
11. **C** – Η σωστή εντολή: sudo ufw enable.
12. **C** – Καραντίνα = απομόνωση ύποπτων αρχείων.
13. **C** – Η γνώση της κοινωνικής μηχανικής αποτρέπει το phishing.
14. **B** – Zero Trust = συνεχής επαλήθευση.
15. **B** – Καλύτερη ενέργεια: μπλόκαρε το IP, έλεγξε τους κανόνες firewall.
16. **B** – Firewall = φίλτρο κυκλοφορίας.
17. **C** – Εργαλείο των Windows: Defender Firewall με Προηγμένη Ασφάλεια.
18. **B** – Το μπλοκάρισμα SSH αποτρέπει απομακρυσμένες συνδέσεις.
19. **B** – Η εντολή sudo ufw status εμφανίζει ενεργούς κανόνες.
20. **C** – Το HTTP χρησιμοποιεί τη θύρα 80.
21. **B** – Πάντα ενημέρωσε πρώτα τους ορισμούς ιών.
22. **C** – Ο Πλήρης Έλεγχος είναι ο πιο διεξοδικός.
23. **A** – Η εντολή sudo freshclam ενημερώνει τη βάση δεδομένων του ClamAV.
24. **B** – Πρώτα απομόνωση, μετά έλεγχος.
25. **B** – Πάντα έλεγξε τα logs και επιβεβαίωσε πριν διαγράψεις.