ΠΑΝΕΛΛΗΝΙΟΣ ΜΑΘΗΤΙΚΟΣ ΔΙΑΓΩΝΙΣΜΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Α. ΠΕΡΙΟΧΕΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΠΟΥ ΚΑΛΥΠΤΟΥΝ ΟΙ ΠΡΟΚΛΗΣΕΙΣ

Οι δοκιμασίες (προκλήσεις) που θα κληθούν οι μαθητές/-τριες να επιλύσουν θα καλύπτουν δημοφιλείς περιοχές της κυβερνοασφάλειας, όπως αυτές κατηγοριοποιούνται σε παρόμοιους ευρωπαϊκούς διαγωνισμούς. Επιπλέον, οι δοκιμασίες θα έχουν διαμορφωθεί ειδικά για το διαγωνισμό και θα είναι πλήρως προσαρμοσμένες στις ανάγκες της ηλικιακής ομάδας στην οποία απευθύνονται. Ο βαθμός δυσκολίας των δοκιμασιών θα εκτείνεται από πολύ εύκολες μέχρι και δύσκολες, με σκοπό την συμμετοχή όλων των μαθητών με ενδιαφέρον στην ασφάλεια υπολογιστών.

1. Κρυπτογραφία (Cryptography)

Δοκιμασίες σχετικές με κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών και απόκρυψη μηνυμάτων. Σκοπός των δοκιμασιών αυτών είναι να παρέχουν στον χρήστη γνώσεις λειτουργίας κρυπτογραφικών αλγορίθμων και αναγνώριση ευπαθειών σε αυτούς.

2. Παγκόσμιος Ιστός (Web)

Δοκιμασίες σχετικές με την λειτουργία και ασφάλεια διαδικτυακών εφαρμογών. Σκοπός των δοκιμασιών αυτών είναι να παρέχουν στον χρήστη γνώσεις λειτουργίας, μηχανισμών αυθεντικοποίησης και ασφάλειας σε ιστοσελίδες και διακομιστές στον παγκόσμιο ιστό.

3. Αντίστροφη Μηχανική (Reverse Engineering)

Δοκιμασίες σχετικές με την ανάλυση εκτελέσιμων προγραμμάτων σε γλώσσα μηχανής. Σκοπός των δοκιμασιών αυτών είναι η κατανόηση λειτουργίας δυαδικών προγραμμάτων και εκτέλεσής τους από το εκάστοτε λειτουργικό σύστημα.

4. Ψηφιακή Εγκληματολογία (Digital Forensics)

Δοκιμασίες σχετικές με την ανάλυση πληροφοριών με σκοπό την αναγνώριση και ανάκτηση ηλεκτρονικών αποδεικτικών στοιχείων. Σκοπός των δοκιμασιών αυτών είναι η παροχή γνώσεων τηλεπικοινωνιών και πρωτοκόλλων, καθώς και μεθόδων ανάλυσής τους για την ανάκτηση πληροφοριών.

5. Εκμετάλευση αδυναμιών (Pwn/Binary exploitation)

Δοκιμασίες που απαιτούν την εκμετάλλευση αδυναμιών σε εκτελέσιμα αρχεία, οι συμμετέχοντες συνήθως παρέχονται με ένα ευάλωτο δυαδικό πρόγραμμα και τους ζητείται να εντοπίσουν και να εκμεταλλευτούν ευπάθειες μέσα σε αυτό για να αποκτήσουν έλεγχο ή να εξάγουν ευαίσθητες πληροφορίες.

6. Στεγανογραφία (Steganography)

Δοκιμασίες σχετικές με την ανάλυση πληροφοριών και ανάκτηση κρυμμένων μηνυμάτων. Σκοπός των δοκιμασιών αυτών είναι η παροχή γνώσεων πάνω σε τεχνικές στεγανογραφίας, αλλά και τεχνικές κωδικοποίησης πληροφοριών.

7. Συλλογή Πληροφοριών από Ανοικτές Πηγές (Open Source Intelligence, OSINT)

Δοκιμασίες που απαιτούν την εκμετάλλευση δημόσια διαθέσιμων πληροφοριών για την εύρεση κρυμμένων δεδομένων, λύση προβλημάτων ή εύρεση ευπαθειών. Ο στόχος είναι να αξιοποιηθούν πηγές ανοικτής πληροφορίας όπως δημόσια ιστοσελίδες, μέσα κοινωνικής δικτύωσης, φόρουμ και άλλες δημόσιες πλατφόρμες για την απόκτηση πληροφοριών.

8. Διάφορα (Miscellaneous)

Δοκιμασίες σχετικές με την επίλυση γρίφων και προβλημάτων. Σκοπός των δοκιμασιών αυτών είναι η εκπαίδευση του χρήστη στην επίλυση προβλημάτων, αλλά και η εξοικείωσή του με τεχνολογίες σχετικές με την κυβερνοασφάλεια.

Σκοπός του διαγωνισμού είναι η ευαισθητοποίηση των μαθητών/-τριών του λυκείου σε θέματα κυβερνοασφάλειας και η παροχή σε αυτούς/αυτές γνώσεων κυβερνοασφάλειας. Επιπλέον, δίνεται η δυνατότητα στους εκπαιδευτικούς να χρησιμοποιήσουν το υλικό του διαγωνισμού για την διεξαγωγή επιπλέον δραστηριοτήτων με τους μαθητές/-τριες με σκοπό την μόρφωσή τους σε θέματα κυβερνοασφάλειας, μιας και μετά το πέρας του διαγωνισμού θα δοθούν αναλυτικές οδηγίες επίλυσης της κάθε δοκιμασίας.

Β. ΕΝΔΕΙΚΤΙΚΕΣ ΠΕΡΙΓΡΕΣ ΠΡΟΚΛΗΣΕΩΝ

Με σκοπό την ευαισθητοποίηση των μαθητών/-τριών του λυκείου και την παροχή γνώσεων πάνω στην κυβερνοασφάλεια, στο πλαίσιο του Πανελλήνιου Σχολικού Διαγωνισμού Κυβερνοασφάλειας (ΠΜΔΚ) 2024 θα δοθούν στους/στις μαθητές/-τριες μια σειρά από ανεξάρτητες προκλήσεις πάνω στην Κυβερνοασφάλεια.

Για την προετοιμασία τους, οι ενδιαφερόμενοι μαθητές/-τριες μπορούν να δοκιμάσουν να λύσουν τις δοκιμασίες που δόθηκαν στους μαθητές κατά την διεξαγωγή του Πανελλήνιου Μαθητικού Διαγωνισμού Κυβερνοασφάλειας 2023 οι οποίες είναι διαθέσιμες στο GitHub του Εργαστηρίου Ασφάλειας Συστημάτων. Μαζί με τις εκφωνήσεις και τα αρχεία των δοκιμασιών αυτών δίνονται και οι ενδεικτικές λύσεις τους, δίνοντας έτσι και την δυνατότητα στους μαθητές/-τριες να ακολουθήσουν βήμα-βήμα την διαδικασία επίλυσής τους ανεξάρτητος του επιπέδου γνώσεων τους στην Κυβερνοασφάλεια.

Ακολουθεί περιγραφή ενδεικτικών προκλήσεων, που μπορεί να κληθούν να επιλύσουν οι μαθητές/-τριες κατά την διάρκεια του διαγωνισμού:

- Ανάκτηση και ανάλυση πηγαίου κώδικα ιστοσελίδων (π.χ. ανάγνωση πηγαίου κώδικα μιας ιστοσελίδας)
- Παράκαμψη αυθεντικοποίησης σε ευπαθής διαδικτυακή εφαρμογή (π.χ. επίθεση με SQL injection σε ιστοσελίδα)
- Ανάκτηση και ανάλυση πηγαίου κώδικα εκτελέσιμων προγραμμάτων με σκοπό την

παράκαμψη μηχανισμών ασφαλείας (π.χ. εύρεση κωδικού που ζητά ένα εκτελέσιμο πρόγραμμα)

- Αποκρυπτογράφηση κρυπτογραφημένου μηνύματος με ή χωρίς κλειδί (π.χ. αποκρυπτογράφηση μηνύματος σε Κώδικα του Καίσαρα)
- Ανάλυση και αποκωδικοποίηση μηνυμάτων (π.χ. αποκωδικοποίηση base64)
- Ανάλυση διαδικτυακής ροής (π.χ. ανάλυση ροής πακέτων με Wireshark)
- Σπάσιμο κωδικών (π.χ. ανάκτηση κωδικού σε συμπιεσμένο αρχείο zip)
- Ανάκτηση κρυμμένων μηνυμάτων (π.χ. ανάκτηση μηνύματος από φωτογραφεία)
- Εκμετάλλευση ευπαθειών σε κρυπτογραφικά συστήματα (π.χ. εύρεση αδύναμου ιδιωτικού κλειδιού)
- Ανακατασκευή/διόρθωση κατεστραμμένου αρχείου (π.χ. διόρθωση κατεστραμμένης φωτογραφίας)
- Εύρεση δημόσια διαθέσιμων πληροφοριών στο διαδίκτυο (π.χ. εύρεση λογαριασμού ατόμου σε μέσα κοινωνικής δικτύωσης)