HELLENIC CYBER SECURITY TEAM

UNIVERSITY OF PIRAEUS

ΠΑΝΕΛΛΗΝΙΟΣ ΜΑΘΗΤΙΚΟΣ ΔΙΑΓΩΝΙΣΜΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΥΛΗ ΔΙΑΓΩΝΙΣΜΟΥ

ΔΕΚΕΜΒΡΙΟΣ 2023

Περιεχομενα

ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο έχει σαν στόχο την περιγραφή της ύλης του Πανελλήνιου Μαθητικού Διαγωνισμού Κυβερνοασφάλειας. Η ύλη περιλαμβάνει το σύνολο των γενικών και ειδικών γνώσεις που μπορεί να χρειαστεί κάποιος για την επίλυση των δοκιμασιών ασφαλείας του διαγωνισμού. Η παρούσα ύλη αναπτύχθηκε χρησιμοποιώντας είναι ένα υποσύνολο της ύλης του ευρωπαϊκού διαγωνισμού κυβερνοασφάλειας (ECSC) και δίνοντας έμφαση στα πιο πρακτικά και απλά σημεία της ασφάλειας πληροφοριών πολλές φορές δίνοντας παραπάνω έμφαση στην χρήση εργαλείων για την μείωση της πολυπλοκότητας και απαίτηση τεχνικών γνώσεων.

Για την συμμετοχή τους στον διαγωνισμό δεν είναι υποχρεωτικό οι μαθητές να γνωρίζουν το σύνολο της ύλης. Κατά την διάρκεια του διαγωνισμού οι μαθητές θα έχουν τον χρόνο να αναζητήσουν πληροφορίες και να λάβουν γνώση για την επίλυση των δοκιμασιών. Υπενθυμίζεται πως οι δοκιμασίες που θα δοθούν θα έχουν διάφορα επίπεδα δυσκολίας (από πολύ εύκολες μέχρι πολύ δύσκολες), για να μπορούν να συμμετέχουν όλοι οι μαθητές ανεξάρτητα από τις γνώσεις τους.

Στο παράρτημα του παρόν εγγράφου αναφέρονται ενδεικτικά πηγές για εκπαίδευση χρηστών σε θέματα σχετικά της κυβερνοασφάλειας καθώς και προτεινόμενο λογισμικό για την επίλυση των δοκιμασιών.

ΒΑΣΙΚΕΣ ΔΕΞΙΟΤΗΤΕΣ ΚΑΙ ΓΕΝΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ

ΓΕΝΙΚΕΣ ΓΝΩΣΕΙΣ

Κωδικοποιήσεις

- Συστήματα αναπαράστασης των αριθμών: Δυαδικό (Binary), Οκταδικό (Octal), Δεκαδικό (Decimal), Δεκαεξαδικό (Hexadecimal)
- Πίνακας ASCII
- Βασική κατανόηση λειτουργίας QR code

Γλώσσες Προγραμματισμού

- Ικανότητα ανάγνωσης κώδικα C
- Ικανότητα ανάγνωσης και συγγραφής κώδικα Python
- Ικανότητα ανάγνωσης κώδικα JavaScript

ΚΡΥΠΤΟΓΡΑΦΙΑ

Εμπιστευτικότητα/Κρυπτογράφηση

- Κώδικες αντικατάστασης (αλγόριθμος κρυπτογράφησης του Καίσαρα, αλγόριθμος κρυπτογράφησης Vigenère, κρυπτογράφηση Pigpen, κώδικας Μορς κτλ.)
- Κρυπτογράφηση συμμετρικού κλειδιού και κρυπτογράφηση δημόσιου κλειδιού
- Ισχυρή κρυπτογράφηση και αδύναμη κρυπτογράφηση, μήκος κλειδιού και εξαντλητική αναζήτηση κλειδιού
- Σύγχρονοι αλγόριθμοι κρυπτογράφησης (AES, RSA)

Ακεραιότητα και έλεγχος αυθεντικότητας δεδομένων

- Συναρτήσεις Hash

Ταυτοποίηση/Αυθεντικοποίηση οντοτήτων

- Κωδικοί πρόσβασης, ισχυροί/αδύναμοι κωδικοί πρόσβασης

ΔΙΚΤΥΑ

Αρχιτεκτονική και Πρωτόκολλά Διαδικτύου

- Βασικές αρχές λειτουργίας TCP/IP
- Γενικές τεχνολογίες σύνθεσης: Ethernet, Wi-Fi
- Βασικά πρωτόκολλα υποδομών: DNS
- Βασικά πρωτόκολλα επιπέδου εφαρμογών: HTTP

Βασικές αρχές ασφάλειας δικτύων

- Συνήθεις απειλές και επιθέσεις: Υποκλοπή πακέτων (Sniffing)

Πρακτική ασφάλεια δικτύων

- Ασφάλεια ασύρματων δικτύων: Wi-Fi

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

Βασικές Αρχές Λειτουργικών Συστημάτων

- Λειτουργικά συστήματα: Windows, Linux
- Σύστημα αρχείων, δικαιώματα πρόσβασης σε αρχεία και φακέλους
- Κονσόλα (Shell), Γραφική Διεπαφή Χρήστη (GUI)
- Εικονικές μηχανές (VM)

ΑΝΘΡΩΠΙΝΟΙ ΠΑΡΑΓΟΝΤΕΣ

Συλλογή και αναγνώριση πληροφοριών

- Τεχνικές συλλογής πληροφοριών με τη βοήθεια τεχνολογίας (μηχανή αναζήτησης, δημόσιες βάσεις δεδομένων κτλ.)

Επιθέσεις

- Αδύναμοι κωδικοί πρόσβασης (προεπιλεγμένοι κωδικοί πρόσβασης, αδύναμοι κωδικοί πρόσβασης: λίστες κωδικών, δημοφιλής κωδικοί πρόσβασης)
- Επιθέσεις εξαντλητικής αναζήτησης / brute force κωδικοί πρόσβασης
- Επιθέσεις hash cracking για ανάκτηση κωδικών πρόσβασης

ΕΙΔΙΚΕΣ ΓΝΩΣΤΙΚΕΣ ΠΕΡΙΟΧΕΣ

ΔΙΑΔΙΚΤΥΟ (WEB)

Αρχές Ανάπτυξης Εφαρμογών Διαδικτύου

- Βασικές αρχές εφαρμογών διαδικτύου (π.χ. μοντέλο πελάτη διακομιστή, δομή URL, πηγαίος κώδικας ιστοσελίδων)
- Εργαλεία για προγραμματιστές σε περιηγητές διαδικτύου (Browser Developer Tools)
- Γλώσσες προγραμματισμού διαδικτύου (π.χ. HTML, CSS, JavaScript)
- Κωδικοποιήσεις (π.χ. κωδικοποίηση URL, κωδικοποίηση base64)
- Χειροκίνητη επιθεώρηση διαδικτυακής κίνησης (π.χ. Developer Tools Network, Burp)

Συνήθη Προβλήματα και Ευπάθειες

- Παράκαμψη μηχανισμών αυθεντικοποίησης / Εσφαλμένος έλεγχος ταυτότητας
- Εσφαλμένη παραμετροποίηση: προεπιλεγμένες ρυθμίσεις, προεπιλεγμένοι κωδικοί πρόσβασης

- Διαχείριση συνεδρίας (session management)
- Επικύρωση εισόδου, επιθέσεις injection (SQL injection, Command injection)

Αξιολόγηση και εκμετάλλευση ευπαθειών διαδικτυακών εφαρμογών

- Δοκιμή προεπιλεγμένα κωδικών πρόσβασης (π.χ. admin:admin)
- Ανίχνευση και εκμετάλλευση των πιο κοινών ευπαθειών ιστού:
  - SQL injection (SQLi)
  - Χειρισμός διαχείρισης συνεδρίας (π.χ. Cookies)
  - Εργαλεία για την επισκόπηση κίνησης δικτύου: Wireshark

ΑΝΤΙΣΤΡΟΦΗ ΜΗΧΑΝΙΚΗ (REVERSE ENGINEERING)

Βασικές γνώσεις αντίστροφης μηχανικής

- deobfuscation κώδικα
- αντίστροφη μηχανική προγραμμάτων από κώδικα μηχανής
- αποσφαλμάτωση προγραμμάτων

ΤΕΧΝΙΚΕΣ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ

ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΣΥΛΛΟΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

Παθητική συλλογή πληροφοριών

- Google Dorks / Google Hacking

Δημόσια Διαθέσιμη Γνώση (Open-Source Intelligence)

- Χρήση εργαλείων για OSINT: Μηχανές Αναζήτησης (π.χ. Google), ψηφιακά αρχεία Παγκόσμιου Ιστού (π.χ. Wayback Machine)

ΚΡΥΠΤΑΝΑΛΥΣΗ

Αυτοματοποιημένη Κρυπτανάλυση

- Κρυπτανάλυση κρυπτογραφήσεων βασισμένες σε κώδικες αντικατάστασης (αλγόριθμος κρυπτογράφησης του Καίσαρα, αλγόριθμος κρυπτογράφησης Vigenère)

ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΚΑΙ ΑΝΑΛΥΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Βασικές Γνώσεις Ψηφιακής Εγκληματολογίας

- Εγκληματολογία αρχείων, κωδικοποίηση, κεφαλίδες αρχείων, μαγικοί αριθμοί (magic numbers), μεταδεδομένα (metadata)

- Εγκληματολογία δικτύου, ανάλυση pcap αρχείων (Wireshark), ανάλυση ροής πακέτων
- Στεγανογραφία

ΠΑΡΑΡΤΗΜΑ

Δοκιμασίες Προηγούμενων Διαγωνισμών

Στον παρακάτω πίνακα μπορείτε να βρείτε τον σύνδεσμο με τις δοκιμασίες από τον προηγούμενο διαγωνισμό μαζί με τις ενδεικτικές λύσεις τους. Οι δοκιμασίες αυτές μπορούν να χρησιμοποιηθούν για εκπαίδευση και προπόνηση των μαθητών.

Δοκιμασίες και ενδεικτικές λύσεις για τον 1ο Πανελλήνιο Μαθητικό Διαγωνισμό Κυβερνοασφάλειας (2023)	https://github.com/UniPiSSL/pmdk-2023

Πηγές Εκπαίδευσης

Στον παρακάτω πίνακα αναφέρονται πηγές σχετικές με την εκπαίδευση χρηστών πάνω σε θέματα κυβερνοασφάλειας με δωρεάν περιεχόμενο (μερικές πηγές μπορεί να περιέχουν επιπλέον επί πληρωμή υλικό). Οι διοργανωτές του διαγωνισμού δεν υποστηρίζουν και δεν προωθούν καμία από τις πηγές αναφέροντάς τες στον παρακάτω πίνακα. Οι πηγές που αναφέρονται στον παρακάτω πίνακα παρουσιάζονται με αλφαβητική σειρά.

BugBountyHunter Learn how to test for security vulnerabilities on web applications	https://www.bugbountyhunter.com/
CyberDefenders Training platform focused on the defensive side of cybersecurity	https://cyberdefenders.org/
CyberSecLabs Training labs to learn and practice penetration testing	https://www.cyberseclabs.co.uk/
Cybrary Cybersecurity training	https://www.cybrary.it/
HackMyVM Platform for vulnerable machines	https://hackmyvm.eu/
Hacker Test Online hacker simulation	http://www.hackertest.net/
Hacker101 Class for web security	https://www.hacker101.com/
Hacksec Bug bounty Training platform	https://www.hacksec.in/
Hackthebox Online cybersecurity training platform	https://www.hackthebox.com/
Hackxor Realistic webapp hacking game	https://hackxor.net/
LetsDefend Hands-on experience on blue team	https://letsdefend.io/

Overthewire – Bandit Εκμάθηση Τερματικού Linux	https://overthewire.org/wargames/bandit/
PentesterLab Web penetration testing exercises	https://pentesterlab.com/
picoCTF Computer security education program	https://picoctf.org/
Portswigger Web Security Academy Online training center for web application security	https://portswigger.net/web-security
Root Me Platform to test and improve knowledge in computer security	https://www.root-me.org/
Try2hack Game based on the real hacker attacks	https://try2hack.me/
TryHackMe Online platform for learning cyber security	https://tryhackme.com/
VulnHub Materials to gain hands-on experience with digital security	https://www.vulnhub.com/
Vulnmachines Cybersecurity learning platform	https://www.vulnmachines.com/

Προτεινόμενο Λογισμικό

Λογισμικά για εικονικές μηχανές

Virtual Box	https://www.virtualbox.org/wiki/Downloads
VMware Workstation Player	https://customerconnect.vmware.com/downloads/

Εξειδικευμένα λειτουργικά συστήματα για επιθέσεις κυβερνοασφάλειας

Kali Linux	https://www.kali.org/get-kali/
Parrot OS	https://www.parrotsec.org/download/

Phone Number
+30 210 4142773

E-mail
ecsc@unipi.gr

Address
University of Piraeus, Karaoli
and Dimitriou 80, Piraeus 185 34