ΥΣ13 Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**ΥΣ13**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	8
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ *σε περίπτωση που οι πιστωτικές μονάδες απονέμονται σε διακριτά μέρη του μαθήματος π.χ. Διαλέξεις, Εργαστηριακές Ασκήσεις κ.λπ. Αν οι πιστωτικές μονάδες απονέμονται ενιαία για το σύνολο του μαθήματος αναγράψτε τις εβδομαδιαίες ώρες διδασκαλίας και το σύνολο των πιστωτικών μονάδων*	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις-Φροντιστήριο	4(3+1)	6
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (4).		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	ειδίκευσης γενικών γνώσεων
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Λειτουργικά Συστήματα
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Διδασκαλία στα Ελληνικά, εξέταση στα Αγγλικά
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://hackintro.github.io/

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος.

Συμβουλευτείτε το Παράρτημα Α

- *Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με το Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης*
- *Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και το Παράρτημα Β*
- *Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων*

Βασικό υπόβαθρο για να ξεκινήσει ο/η φοιτητής/τρια μια καριέρα στην ασφάλεια υπολογιστικών συστημάτων είτε με περισσότερες σπουδές στην συνέχεια (μεταπτυχιακό/διδακτορικό) είτε με μετάβαση στην βιομηχανία. Οι γνώσεις, δεξιότητες και ικανότητες που θα αποκτήσει ο/η φοιτητής/φοιτήτρια στον τομέα της ασφάλειας υπολογιστών ολοκληρώνοντας το μάθημα είναι κοντά σε μεταπτυχιακό επίπεδο (ανώτατα σημεία του επιπέδου 6, αρχές επιπέδου 7).

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής/η φοιτήτρια θα είναι σε θέση να:

- Αναφέρει και εξηγεί βασικές έννοιες/λεξιλόγιο της ασφάλειας
- Αναφέρει και εφαρμόζει βασικές τεχνικές άμυνας και επίθεσης σε υπολογιστικά συστήματα (λογισμικό, κρυπτογραφία, δίκτυα, forensics)
- Συζητά για state-of-the-art τεχνολογίες και λύσεις ασφαλείας

Γενικές Ικανότητες

Λαμβάνοντας υπόψη τις γενικές ικανότητες που πρέπει να έχει αποκτήσει ο πτυχιούχος (όπως αυτές αναγράφονται στο Παράρτημα Διπλώματος και παρατίθενται ακολούθως) σε ποια / ποιες από αυτές αποσκοπεί το μάθημα;.

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών

Προσαρμογή σε νέες καταστάσεις

Λήψη αποφάσεων

Αυτόνομη εργασία

Ομαδική εργασία

Εργασία σε διεθνές περιβάλλον

Εργασία σε διεπιστημονικό περιβάλλον

Παραγωγή νέων ερευνητικών ιδεών

Σχεδιασμός και διαχείριση έργων

Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα

Σεβασμός στο φυσικό περιβάλλον

Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και ευαισθησίας σε θέματα φύλου

Άσκηση κριτικής και αυτοκριτικής

Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

……

Άλλες…

Επίλυση προβλημάτων
Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
Προσαρμογή σε νέες καταστάσεις
Λήψη αποφάσεων
Αυτόνομη εργασία
Ομαδική εργασία
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα καλύπτει τις ακόλουθες έννοιες και θεματικές ενότητες:

1. Βασικές αρχές ασφαλείας σε συστήματα υπολογιστών, ορισμός adversary, threat models, TCB. 2. Βασικά εργαλεία για ασφάλεια, debuggers (gdb, web dev tools), docker, python. 3. x86 assembly, buffer overflows, format-strings attacks, CVEs and CWEs, mitigations and Return-Oriented Programming. 4. Access control, Mandatory, Discretionary, Role-Based, ACLs and Capabilities. Reference Monitors. 5. Cryptographic concepts, randomness and pseudorandomness, One-Time Pad, Perfect Secrecy. 6. Encryption Modes, Block ciphers, MACs and Integrity Checking, MAC Constructions. 7. Hash Functions, weak and strong collision resistance, oracles and security games. 8. Authenticated encryption and asymmetric cryptography. RSA, Signatures and certificates. 9. Web security and attacks: XSS, CSRF, Cookie tampering, SSRF, SQL Injections, Command Injections. 10. Network fundamentals, DOS/DDOS attacks, Firewalls and Intrusion Detection/Prevention. 11. Privacy, policy and usability. 12. Hands-on exploit development and experience with binary/web exploitation, cryptography analysis, reverse engineering, and forensics.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Site του μαθήματος: https://hackintro.github.io/ Καταγραφή διαλέξεων μέσω του: https://delos.uoa.gr Επικοινωνία με τους φοιτητές μέσω email και της πλατφόρμας Piazza για ανακοινώσεις και συζητήσεις. Ανάθεση και υποβολή εργασιών μέσω GitHub. Χειρισμός ημερολογίου και ερωτηματολογίων μέσω Google Suite. Χρήση Kahoot για ερωτήσεις κατανόησης σε εβδομαδιαία βάση. Εικονικές μηχανές για την επίλυση ασκήσεων κυβερνοασφάλειας.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ *Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.* *Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ.* *Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης σύμφωνα με τις αρχές του ECTS*	Το θεωρητικό μέρος του μαθήματος διδάσκεται με χρήση διαφανειών και διαδραστικής συζήτησης, ερωτήσεων και επίλυσης προβλημάτων με τους/τις φοιτητές/φοιτήτριες. Ώρες γραφείου προσφέρονται για ερωτήσεις που δεν καλύφθηκαν την ώρα της διάλεξης. Οι φοιτητές/φοιτήτριες υποβάλλουν εργασίες κατά την διάρκεια του εξαμήνου, όπου καλούνται να επιλύσουν προβλήματα κυβερνοασφάλειας. Το μάθημα εξετάζεται γραπτά στην τελική εξέταση και το υπόλοιπο της βαθμολογίας προκύπτει από τις εργασίες (δες και την αξιολόγηση παρακάτω). **_Δραστηριότητα_** | **_Φόρτος Εργασίας Εξαμήνου_** Διαλέξεις | 52 Εργασίες / Μελέτη | 98 **Σύνολο Μαθήματος** | **150**

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Ο τελικός βαθμός προκύπτει από τα ακόλουθα:
Περιγραφή της διαδικασίας αξιολόγησης *Γλώσσα Αξιολόγησης, Μέθοδοι αξιολόγησης, Διαμορφωτική ή Συμπερασματική, Δοκιμασία Πολλαπλής Επιλογής, Ερωτήσεις Σύντομης Απάντησης, Ερωτήσεις Ανάπτυξης Δοκιμίων, Επίλυση Προβλημάτων, Γραπτή Εργασία, Έκθεση / Αναφορά, Προφορική Εξέταση, Δημόσια Παρουσίαση, Εργαστηριακή Εργασία, Κλινική Εξέταση Ασθενούς, Καλλιτεχνική Ερμηνεία, Άλλη / Άλλες* *Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.*	

Αξιολόγηση	***Αριθμός***	***Ποσοστό***
Γραπτή εξέταση	1	50%
Εργασίες	4	50%

- Η γραπτή εξέταση περιλαμβάνει ερωτήσεις που εξετάζουν την κριτική σκέψη και την εφαρμογή της για την επίλυση θεμάτων κυβερνοασφάλειας.
- Η βαθμολογία των εργασιών προκύπτει από την εξέταση της λειτουργικότητας των λύσεων που υπεβλήθησαν, σε συνδυασμό με την γραπτή αναφορά που υποβλήθηκε.

Η γλώσσα αξιολόγησης είναι τα Αγγλικά.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- W. Stallings, L. Brown. «Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές».
- Σ. Κάτσικας, Σ. Γκρίτζαλης, Κ. Λαμπρινουδάκης. «Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο».
- Pfleeger P. Charles, Pfleeger Shari Lawrence, Margulies Jonathan. «. Ασφάλεια Πληροφοριακών Συστημάτων».
- R. Anderson. https://github.com/tpn/pdfs/blob/master/Security%20Engineering%20-%20Ross%20Anderson%20(v1).pdf