912. Ασφάλεια Δικτύων Υπολογιστών

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ			
ΤΜΗΜΑ	ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ			
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ			
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**912**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**9**	
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**Ασφάλεια Δικτύων Υπολογιστών**			
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**		**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διάφορες μορφές διδασκαλίας		4		5
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων			
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Δίκτυα Υπολογιστών			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική			
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι			
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ	eclass/courses/			

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Το μάθημα εστιάζει σε θέματα ασφάλειας δικτύων υπολογιστών και τεχνολογίες προστασίας της Ιδιωτικότητας. Για τον σκοπό αυτό, έχει επιλεγεί η προσέγγιση στην αρχιτεκτονική ασφάλειας δικτύων OSI/ISO και συγκεκριμένα στην αρχιτεκτονική ασφάλειας με βάση το διαδικτυακό μοντέλο TCP/IP.

Με την ολοκλήρωση του μαθήματος, οι φοιτητές:

- Έχουν αποκτήσει γνώση περί της ασφάλειας των δικτύων και των υπολογιστικών συστημάτων και αναπτύσσουν πολιτικές ασφάλειας σε δικτυακό περιβάλλον.
- Είναι ενήμεροι σε αναλυτικό βαθμό των διάφορων κατηγοριών απειλών, των σημείων ευπάθειας, των αντιμέτρων και των μεθόδων διασφάλισης.
- Γνωρίζουν τις τεχνολογίες και χρησιμοποιούν τις υπηρεσίες υποδομής δημόσιων κλειδιών.
- Εξοικειώνονται με τη σχετική ορολογία και τις βασικές τεχνολογίες προστασίας της Ιδιωτικότητας
- Έχουν μάθει τους τρόπους ένταξης της Ιδιωτικότητας κατά τη σχεδίαση πληροφοριακών συστημάτων σε τομείς του Ηλεκτρονικού Εμπορίου και της Ηλεκτρονικής Διακυβέρνησης.

Ο στόχος των εργαστηριακών εφαρμογών και μελετών περίπτωσης (ατομικές/ομαδικές εργασίες), που δρουν συμπληρωματικά στη θεωρία κάθε διδακτικής ενότητας, είναι η καθοδήγηση των φοιτητών στην αξιοποίηση με βέλτιστο τρόπο των παραπάνω μεθοδολογιών και τεχνολογιών ασφάλειας και προστασίας της Ιδιωτικότητας τόσο σε δικτυακό όσο και σε διαδικτυακό περιβάλλον.

Γενικές Ικανότητες

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
Αυτόνομη εργασία
Ομαδική εργασία
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Εισαγωγικά θέματα Ασφάλειας Δικτύων Υπολογιστών:

- Ορολογία,
- Κατηγορίες Απειλών,
- Σημεία Ευπάθειας,
- Αντίμετρα,
- Διασφάλιση.

Τεχνολογίες και Υπηρεσίες Υποδομής Δημόσιων Κλειδιών.

Αρχιτεκτονική Ασφάλειας Δικτύων OSI/ISO:

- Υπηρεσίες Ασφάλειας,
- Μηχανισμοί Ασφάλειας.

Αρχιτεκτονική Ασφάλειας στο μοντέλο TCP/IP του Internet:

- Ασφάλεια Επιπέδου Internet,
- Ασφάλεια Επιπέδου Μεταφοράς,
- Ασφάλεια Επιπέδου Εφαρμογής,
- Ασφάλεια υπεράνω του Επιπέδου Εφαρμογής.

Αναχώματα Ασφάλειας:

- Δυνατότητες και Περιορισμοί,
- Αρχιτεκτονική Αναχωμάτων Ασφάλειας,

- Αναχώματα Ασφάλειας Επιπέδου Δικτύου,
- Αναχώματα Ασφάλειας Επιπέδου Εφαρμογής,
- Υβριδικά Αναχώματα Ασφάλειας

Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολών. Ιδιωτικότητα:

- Ορολογία,
- Βασικές τεχνικές προστασίας της Ιδιωτικότητας,
- Η Ιδιωτικότητα κατά τη σχεδίαση πληροφοριακών συστημάτων,
- Εφαρμογές σε τομείς του Ηλεκτρονικού Εμπορίου και της Ηλεκτρονικής Διακυβέρνησης.

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	• Πρόσωπο με πρόσωπο θεωρητική διδασκαλία. • Εργαστηριακή εκπαίδευση με ειδικό λειτουργικό σύστημα που φέρει πλήθος εφαρμογών διενέργειας επιθέσεων και ελέγχου ευπάθειας, συστημάτων, εφαρμογών κλπ. • Ανάθεση ατομικών/ομαδικών εργασιών σε διάφορες κατηγορίες απειλών και σε ενδεδειγμένες τεχνικές/μεθοδολογίες ελέγχου ευπαθειών.
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	Χρήση λογισμικού παρουσιάσεων διαφανειών (Power point presentations). Επικοινωνία με τους φοιτητές μέσω ηλεκτρονικής πλατφόρμας ασύγχρονης τηλεκπαίδευσης.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	***Δραστηριότητα*** | ***Φόρτος Εργασίας Εξαμήνου*** Διαλέξεις | 39 Εργαστηριακές Ασκήσεις (υποχρεωτική παρουσία) | 13 Εκπόνηση εργαστηριακών εργασιών/τεχνικών αναφορών σε μικρές ομάδες | 13 Ατομική Μελέτη | 58 Εξετάσεις | 3 ***Σύνολο Μαθήματος*** | ***126***
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	I. Γραπτή τελική εξέταση (ΓΕ) (60%) - Επίλυση προβλημάτων -Δοκιμασία Πολλαπλής Επιλογής, Ερωτήσεις Σύντομης Απάντησης. II. Ατομικές και ομαδικές εργασίες (ΑΠ) (40%) - Αναφορές - Δημόσιες Παρουσιάσεις Ο βαθμός του μαθήματος (ΓΕ*0,60 + ΑΠ*0,40) πρέπει να είναι τουλάχιστον πέντε (5). Τα κριτήρια αξιολόγησης είναι προσβάσιμα στους φοιτητές από την ηλεκτρονική σελίδα του μαθήματος.

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία :

Ελληνικά ή μεταφρασμένα διδακτικά συγγράμματα:

1. Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και Πρότυπα, William Stallings, έκδοση 3η, 2008 (μετάφραση).
2. Ασφάλεια υπολογιστών: Αρχές και πρακτικές, William Stallings, Lawrie Brown, 3η έκδοση, 2016 (μετάφραση).
3. W. Stallings, L. Brown, Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές, Έκδοση 3η Αμερικανική, ISBN 978-960-461-668-8, Εκδόσεις Κλειδάριθμος, 2016.
4. Georgia Weidman, Penetration Testing - A hands-on introduction to Hacking, 2014, ISBN: 978-1-59327-564-8.
5. P. Kim, The Hacker Playbook: Practical Guide to Penetration Testing, 2014, ISBN: 978-1494932633.
6. Davidoff S., Ham, J., Network Forensics: Tracking Hackers through Cyberspace, Prentice Hall, 2012.
7. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 2012.
8. Bill Blunden, The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, 2012.
9. D. Stuttard, M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2011, ISBN: 978-1118026472.
10. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni, Metasploit: The Penetration Tester's Guide, 2011, ISBN: 978-1-59327-288-3
11. Stewart J. M., Network Security, Firewalls, and VPNs, Jones & Bartlett Learning, 2010.
12. Stallings W., Cryptography and Network Security: Principles and Practice, Prentice Hall, 2010.
13. N. Ferguson, Cryptography Engineering: Design Principles and Practical Applications, 2010, ISBN: 978-0470474242.
14. Jon Erickson, Hacking: The Art of exploitation, 2nd edition, 2008.
15. Edward Skoudis, Tom Liston, Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2nd Ed., 2006.
16. OWASP Testing Guide v4.