AMERICAN COLLEGE

CSC225 NETWORK SECURITY II

ECTS Course Syllabus

Code CSC225	Title Network Security II	
ECTS Credits 6	**Department** Computer Science	**Instructor**
Semester Spring	**Cycle** First	**Language of Instruction** Greek

Description

Το μάθημα Ασφάλεια Δικτύων ΙΙ αποσκοπεί στο να παρουσιάσει τις προηγμένες έννοιες σχετικά με το ethical hacking, όπως η εταιρική κατασκοπεία, η συγγραφή κωδικών ιών, η εκμετάλλευση γραφής και η αντίστροφη μηχανική. Γίνεται ανάλυση πακέτων δικτύου, ασφάλειας των διακομιστών IIS και Apache, διαχείριση του συστήματος των Windows χρησιμοποιώντας το PowerShell, την βάση δεδομένων Hacking SQL & Oracle. Παρέχει πρακτική εξάσκηση στην τάξη για τη σάρωση, δοκιμή, αφαίρεση και προστασία συστημάτων και εφαρμογών. Η εκτεταμένη πορεία για την ηθική hacking με πρόσφατους τομείς ασφάλειας δίνει στους συμμετέχοντες σε βάθος γνώση και πρακτική προσέγγιση στο σημερινό βασικό σύστημα ασφαλείας.

Learning outcomes

Με το πέρας αυτού του μαθήματος οι καταρτιζόμενοι πρέπει να:

- κατανοούν τα θέματα για το χειρισμό της ασφάλειας πληροφοριών με περισσότερη σαφήνεια
- κατανοούν τις λεπτότερες αποχρώσεις των Trojans, Backdoors και Countermeasures
- κατανοούν των IDS, Firewalls, Honeypots και Wireless Hacking
- εξειδικευτούν σε προηγμένες έννοιες όπως η αναβάθμιση του πακέτου δικτύου, η διασφάλιση των διακομιστών Web IIS & Apache, η διαχείριση του συστήματος των Windows με το Powershell, η Hacking SQL & Oracle
- αποκτήσουν γνώση σε προηγμένες έννοιες Hacking - hacking Κινητές συσκευές & έξυπνα τηλέφωνα, εταιρική κατασκοπεία, γραφή κωδικών για ιούς, εκμετάλλευση εγγράφων & αντίστροφης μηχανικής.

Prerequisite(s): CSC218

Learning methods and educational activities

Διαλέξεις, φροντιστήρια και εργαστήρια, πρακτική εξάσκηση, συζήτηση ερωτήσεων και ασκήσεων, προετοιμασία εργασιών με την ενεργό συμμετοχή των καταρτιζόμενων.

Teaching hours: 39

Assessment methods and weight

Ενδιάμεση Εξέταση:	20%
Ασκήσεις και Διαγνωστικά:	30%
Τελική Εξέταση:	50%

Grading system

90-100	**A**	85-89	**B+**	80-84	**B**	75-79	**C+**
70-74	**C**	65-69	**D+**	60-64	**D**	0-59	**F**

Required book(s)

Title:	Certified Ethical Hacker V9 Study Guide
Author(s):	Sean-Philip Oriyano
Publisher:	John Wiley & Sons ISBN: 978-1-119-25224-5
Edition:	Version 9
Year:	2016

Title:	ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ
Author(s):	Κάτσικας Σωκράτης
Publisher:	ΠΕΔΙΟ ISBN 9789605464158
Edition:	1st
Year:	2014

Επιπρόσθετα θα δίνονται σημειώσεις από τον καθηγητή.

Recommended book (s)

Title:	Network Security Essentials
Author(s):	Willian Stallings
Publisher:	Pearson
Edition:	6th
Year:	2016

Title:	TCP/IP Protocol Suite
Author(s):	Behrouz A. Forouzan
Publisher:	McGraw-Hill Education
Edition:	4th
Year:	2011

Title:	CompTIA Linux+ Study Guide
Author(s):	Christine Bresnahan, Richard Blum
Publisher:	Sybex
Edition:	4η
Year:	2019

Content

Week 1	**Introduction to Ethical Hacking - System Fundamentals.** Το μάθημα αυτό καλύπτει το σκοπό του Ethical Hacking, ορίζει τον ηθικό χάκερ και περιγράφει πώς να ξεκινήσετε την εκτέλεση Ελέγχου ασφαλείας. Επίσης παρουσιάζει τα διάφορα συστατικά στοιχεία που αποτελούν ένα σύστημα και τον τρόπο με τον οποίο επηρεάζονται από την ασφάλεια Εισαγωγή στο Linux

Week 2	**Foot printing: Understanding the steps of Ethical Hacking, what is Foot printing – Terminology, threats and Foot printing process.** Σε αυτό το μάθημα, θα μάθετε πώς να λαμβάνετε πληροφορίες από ένα στόχο χρησιμοποιώντας παθητικές και ενεργές μεθόδους..Nmap-Linux

Week 3	**Scanning: What is Scanning, checking for "live" systems and ports, The family tree of scans, OS fingerprinting, countermeasures, vulnerability scanning, mapping the network.** Αυτό το μάθημα σάς δείχνει πώς μπορείτε να αποκτήσετε πληροφορίες σχετικά συσκευές σε ένα δίκτυο, καθώς και τι σημαίνει η κάθε πληροφορία. Vulnerability Scanner in Linux.

Week 4	**Enumeration: What is Enumeration, Windows and Linux basic enumeration, Enumeration with SNMP & SMTP, LDAP and directory service enumeration.** Σε αυτό το μάθημα, θα μάθετε πώς να διερευνήσετε τις διάφορες υπηρεσίες σε έναν συγκεκριμένο κεντρικό υπολογιστή και πώς να επεξεργαστείτε τις πληροφορίες και πώς να τις χρησιμοποιήσετε για μεταγενέστερες ενέργειες.

Week 5	**Malware: Over and covert channels.** Αυτό το μάθημα καλύπτει τις ποικιλίες κακόβουλου λογισμικού και τον τρόπο με τον οποίο μπορεί να γίνει ο καθένας δημιουργεί, χρησιμοποιεί ή υπερασπίζεται.

Week 6	**Sniffers: Understanding sniffers, using a sniffer, Switched Network Sniffer.** Αυτό το μάθημα ασχολείται με τη χρήση παγίδων πακέτων για τη συλλογή πληροφοριών που ρέει στο δίκτυο. Packet Sniffing through Linux

Week 7	**Social Engineering: What is Social Engineering, gather information, commonly employed threats,**

	identify theft. Αυτό το μάθημα καλύπτει τον χειρισμό ανθρώπων προκειμένου να αποκτήσουν ευαίσθητες πληροφορίες.

Week 8	**Επανάληψη για την Ενδιάμεση Εξέταση; Ενδιάμεση Εξέταση.**

Week 9	**Denial of Service: Understanding DoS & DDoS, DoS Tools, DoS Defensive strategies, DoS Pen-Testing Considerations.** Αυτό το μάθημα περιλαμβάνει μια ανάλυση των επιθέσεων που είναι σχεδιασμένο για προσωρινή ή μόνιμη διακοπή ενός στόχου.

Week 10	**Session Hijacking: Understanding Session Hijacking, Exploring Defensive strategies.** Αυτό το μάθημα καλύπτει τον τρόπο διακοπής της επικοινωνίας, καθώς και να αναλάβουν νόμιμες συνεδριάσεις μεταξύ δύο μερών. Session hijacking attacks exploit -Linux

Week 11	**Web Servers and Applications: Exploring Client – Server Relationship.** Αυτό το μάθημα εξηγεί πώς να εισέλθετε σε διακομιστές και εφαρμογές ιστού, καθώς και τις διάφορες μεθόδους επίθεσης.

Week 12	**SQL Injection: Introducing SQL Injection. Hacking Wi-Fi and Bluetooth: What is Wireless Network.** Σε αυτό το μάθημα, θα μάθετε πώς να επιτίθενται βάσεις δεδομένων και αποθήκευση δεδομένων χρησιμοποιώντας ένεση SQL για να αλλάξετε, να παρακολουθήσετε, να προβάλετε ή να καταστρέψετε πληροφορίες. Επίσης θα μάθετε πώς να στοχεύετε, να αναλύσετε, να διακόψετε και να τερματίσετε τα ασύρματα δίκτυα προσωρινά ή μόνιμα. Hack WPA/WPA2 WiFi Using Linux

Week 13	**Evasion: Honeypots, IDSs and Firewalls. Cloud Technologies and Security. Physical Security.** Αυτό το μάθημα καλύπτει τον τρόπο αντιμετώπισης της κοινής προστασίας τα μέτρα που μπορεί να λάβει ένας διαχειριστής συστήματος · Αυτά τα μέτρα περιλαμβάνουν τα συστήματα ανίχνευσης εισβολής (IDS), τα τείχη προστασίας και τα honeypots. Επίσης, θα μάθετε πώς να διασφαλίσετε τεχνολογίες cloud καθώς επίσης και τις πτυχές τις φυσικής ασφάλειας. Ρύθμιση Linux για Τείχος προστασίας

Student workload

Activity	**Hours**
Lab attendance	18
Lab activities	19.5
Independent Study	30
Assignments Preparation	29
Mid-term Preparation	22
Mid-term Examination	1.5
Final Exam Preparation	28
Final Examination	2
Total	**150**