ΔΟΚΙΜΗ ΔΙΕΙΣΔΥΣΗΣ ΚΑΙ ΨΗΦΙΑΚΗ ΣΗΜΑΝΣΗ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	7		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB204	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**Β'**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΔΟΚΙΜΗ ΔΙΕΙΣΔΥΣΗΣ ΚΑΙ ΨΗΦΙΑΚΗ ΣΗΜΑΝΣΗ**		

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	3	
Άσκηση Πράξης	2	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).	5	8

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης, γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	*Ανάπτυξης δεξιοτήτων, Ειδίκευσης*
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΚΑΝΕΝΑ
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά και Αγγλικά
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	UNIWA Open eClass | Digital Forensics and Penetratio...

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ
Πρώτο μέρος Στο πρώτο μέρος του μαθήματος διδάσκονται στους φοιτητές οι βασικές αρχές και πολλές από τις τακτικές, τις τεχνικές, τις διαδικασίες και τα εργαλεία που χρησιμοποιούνται από επαγγελματίες κατά την δοκιμή διείσδυσης σε windows συστήματα. Σκοπός του μαθήματος μεταξύ άλλων είναι να κατανοήσουν την απειλή και τον τρόπο δράσης των επιτιθέμενων. Οι φοιτητές θα μάθουν να εφαρμόζουν ολόκληρη τη διαδικασία δοκιμής διείσδυσης, συμπεριλαμβανομένου του σχεδιασμού, της συλλογής πληροφοριών από ανοικτές πηγές (OSINT – Open Source Intelligence), της αναγνώρισης συστημάτων, της σάρωσης, της αξιολόγησης ευπαθειών, της εκμετάλλευσης και της απόκτησης αρχικής πρόσβασης, τις ενέργειες και διαδικασίες μετά την αρχική πρόσβαση και της αναφοράς αποτελεσμάτων. Το μάθημα θα παρέχει τις βασικές τεχνικές πληροφορίες που σχετίζονται με καθεμία από τις μεθόδους που χρησιμοποιούνται από τους περισσότερους επαγγελματίες δοκιμής διείσδυσης. **Δεύτερο μέρος** Στο δεύτερο μέρος του μαθήματος οι φοιτητές θα διδαχθούν την διαδικασία διαχείρισης / αντιμετώπισης

κυβερνοεπιθέσεων σε ένα windows δίκτυο και την διαδικασία ψηφιακής εγκληματολογικής έρευνας ή διαφορετικά ψηφιακή σήμανση.

Το μάθημα διαχείρισης κυβερνοεπιθέσεων και ψηφιακής σήμανσης σε Windows OS καλύπτει συνολικά τις έξι φάσεις που ακολουθούνται στην διαδικασία διαχείρισης κυβερνοεπιθέσεων, καθώς και την διαδικασία ψηφιακής εγκληματολογικής έρευνας ή διαφορετικά ψηφιακής σήμανσης που περιλαμβάνει την συλλογή και ανάλυση μνήμης των Windows, την συλλογή και ανάλυση της registry, την συλλογή και ανάλυση του συστήματος αρχείων και την ψηφιακή ανάλυση εφαρμογών. Στο τέλος του μαθήματος οι φοιτητές θα έχουν την δυνατότητα να πραγματοποιούν διαχείριση κυβερνοεπίθεσης και ψηφιακή σήμανση χρησιμοποιώντας μια ποικιλία από δωρεάν, ανοιχτού κώδικα και εμπορικά εργαλεία. Θα μάθουν να προσδιορίζουν και να χειρίζονται σωστά

Τα ψηφιακά αποδεικτικά στοιχεία και να απαντούν σε κρίσιμα ερωτήματα σχετικά με την υπόθεση της ψηφιακής εγκληματολογίας. Ερωτήματα όπως τυχόν εκτέλεση υπόπτων εφαρμογών, παράνομη πρόσβαση σε αρχεία, κλοπής δεδομένων, χρήση ύποπτης εξωτερικής συσκευής, μεταφόρτωση υπόπτων αρχείων κλπ. Στο τέλος θα μάθουν πως να συντάσσουν ολοκληρωμένη αναφορά όπου θα παρουσιάζουν με τεκμηριωμένο τρόπο τα ευρήματά τους.

Ο στόχος του μαθήματος είναι να διδάξει τους φοιτητές πώς να εκτελούν την διαδικασία διαχείρισης μιας κυβερνοεπίθεσης, ακολουθώντας ένα σχέδιο διαχείρισης καθώς και πως να εφαρμόζουν μια ολοκληρωμένη ψηφιακή εγκληματολογική έρευνα σε ένα Windows σύστημα.

(1)Γενικές Δεξιότητες / Γνώσεις.

- Κατανόηση της κυβερνοαπειλής και του τρόπου δράσης των επιτιθέμενων στον κυβερνοχώρο.
- Κατανόηση των τακτικών, τεχνικών, διαδικασιών και των εργαλείων που εφαρμόζουν και χρησιμοποιούν οι ελεγκτές ασφαλείας (penetration testers) και οι κόκκινες ομάδες (Read Teams).
- Διεξαγωγή ολοκληρωμένης διαδικασίας δοκιμής διείσδυσης
- Πρακτική εφαρμογή της διαδικασίας διαχείρισης μιας κυβερνοεπίθεσης ακολουθώντας τις έξι φάσεις αντιμετώπισης.
- Πρακτική διεξαγωγή μιας ολοκληρωμένης ψηφιακής εγκληματολογικής έρευνας.

3. **ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ**

Τα περιεχόμενα της κάθε μιας εκ των 13 διαλέξεων περιλαμβάνουν:

1. Εισαγωγή στη αξιολόγηση Δοκιμής Διείσδυσης και κόκκινης ομάδας (Penetration Testing and Red Teaming assessment)
   α. Τι είναι αξιολόγηση Δοκιμής Διείσδυσης και κόκκινης ομάδας (penetration test and red team assessment)
   β. Μεθοδολογία Δοκιμής διείσδυσης (Penetration Test Methodology)
   γ. Προετοιμασία διεξαγωγής Δοκιμής διείσδυσης (Penetration test Essentials Pre-engagement)
   δ. Πεδίο εφαρμογής, Δεοντολογικές απαιτήσεις και νομικά ζητήματα
   ε. Δομή και εξαρτήματα της έκθεσης δοκιμής διείσδυσης
   στ. Δημιουργία εργαστηρίου δοκιμών διείσδυσης
   ζ. Προετοιμασία, ανάπτυξη υποδομής OSINT και ανωνυμίας.
2. Συλλογή πληροφοριών
   α. Αναγνώριση (αναγνώριση DNS TCP, UDP, συνδέσεις)
   β. OSINT (Νοημοσύνη ανοιχτού κώδικα)
   γ. Μεθοδολογία σάρωσης
   δ. Σάρωση συστήματος και δικτύου, Σάρωση με χρήση nmap
3. Αξιολόγηση ευπαθειών (vulnerability assessment)
   α. Netcat

β. Nessus
γ. OpenVas

4. Πλατφόρμες διεξαγωγής ελέγχου διείσδυσης (Penetration test frameworks)
   α. Metasploit
   β. Poshc2
   γ. Covenant
   δ. Mythic
5. Βασική γνώση στην ασφάλεια ενός windows λειτουργικού συστήματος
   α. Εσωτερικοί μηχανισμοί ασφαλείας ενός Windows
   β. Πολιτικές ασφαλείας (Security policies)
   γ. Συσκευές και λογισμικά ασφαλείας (Security software and devices)
6. Τεχνικές απόκτησης αρχικής πρόσβασης (Gaining initial access)
   α. Εισαγωγή στις επιθέσεις των windows
   β. Brute forcing
   γ. Απομακρυσμένη εκμετάλλευση ευπαθειών
   δ. Επιθέσεις τελικού χρήστη
   ε. Πλατφόρμες και επιθέσεις phishing (Spear-phishing / phishing / κλοπή έγκυρων διαπιστευτηρίων)
7. Τεχνικές και διαδικασίες επιθέσεων μετά την αρχική πρόσβαση σε ένα Windows δίκτυο (post exploitation techniques)
   α. Επαύξηση δικαιωμάτων privilege escalation)
   β. Εσωτερική δικτυακή μετακίνηση (Password Spraying, AV, EDR evasion)
   γ. Powershel για penetration testers
   δ. Επιθέσεις Active Directory (Kerberos Authentication, Domain enumeration, Domain attacks, Kerberoasting attack, Golden ticket, Pass the hash attack, pass the ticket, over pass the hash)
8. Διαχείριση κυβερνοεπιθέσεων (Incident handling process)
   α. Εισαγωγή στην Διαχείριση κυβερνοεπιθέσεων
   β. Σχέδιο Διαχείρισης κυβερνοεπιθέσεων (Incident handling plan)
9. Διαδικασία ψηφιακής σήμανσης (Digital Forensics process)
   α. Μεθοδολογία ψηφιακής σήμανσης (Digital Forensics methodology)
   β. Δημιουργία ενός υπολογιστή ανάλυσης ψηφιακής ευρημάτων (Building a forensics analysis station).
   γ. Δημιουργία ενός εργαστηρίου ψηφιακής σήμανσης (Building a forensics lab).
10. Ανάλυση μνήμης ενός Windows συστήματος (memory forensics)
   α. Εισαγωγή στην μνήμη ενός windows λειτουργικού (Memory Essentials)
   β. Συλλογή μνήμης (Dumping the memory)
   γ. Ανάλυση της μνήμης (Memory analysis
11. Ψηφιακή ανάλυση μητρώου (Windows registry forensics)
   α. Εισαγωγή στην Registry Essentials
   β. Συλλογή της registry
   γ. Ανάλυση της Registry
12. Ψηφιακή σήμανση αρχείου συστήματος (Windows file system forensics)
   α. Εισαγωγή στο windows file system
   β. Συλλογή των αρχείων συστματος (Gathering file system relative to case information)
   γ. Ανάλυση του File system
   δ. Ανάλυση των Windows event log
13. Ψηφιακή σήμανση Windows εφαρμογών (application forensics)
   α. Browser Forensics
   β. Email forensics

γ. Usb forensics
δ. Σύνταξη αναφοράς ψηφιακής σήμανσης

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ – ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	*Πρόσωπο με πρόσωπο, Εξ αποστάσεως*
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	***Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση και στην Επικοινωνία με τους Φοιτητές***
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*	**Δραστηριότητα** — **Φόρτος Εργασίας Εξαμήνου** Διαλέξεις — 39 Εργαστηριακή Άσκηση — 26 Συγγραφή εργασίας — 40 Μελέτη — 60 Ανάλυση βιβλιογραφίας — 35 Σύνολο Μαθήματος — ***200***
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ *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.*	*Η αξιολόγηση των φοιτητών πραγματοποιείται με γραπτή εργασία, καθώς και με την πρακτική διεξαγωγή ελέγχου διείσδυσης ή ολοκληρωμένης ψηφιακής εγκληματολογικής ανάλυσης ενός παραβιασμένου windows λειτουργικού συστήματος.*

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- *The Hacker Playbook 3: Practical Guide To Penetration Testing*, ***Peter Kim***, *2018, Red Team Book.*
- *Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting, by Roberto Martínez, 2022, Packet Publishing.*
- Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, by Harlan Carvey, 2009

Recommended

- *Harlan Carvey, Investigating Windows Systems 1st Edition , Elsevier*
- *File System Forensic Analysis 1st Edition by Brian Carrier, 2005. Addison-Wesley Professional*
- *Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition by Daniel Teixeira (Author), Abhinav Singh (Author), Monika Agarwal (Author), 2018, Packt Publishing*
- *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey. 2011*
- *Penetration Tester's Open Source Toolkit 4th Edition, Kindle Edition by Jeremy Faircloth, 2016, Singress.*