ΠΜΣ «Προηγμένα Συστήματα Πληροφορικής»

Σχεδίαση Αρχιτεκτονικών Ασφάλειας

Μεθοδολογίες & Εργαλεία Αποτίμησης Ευπαθειών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Εισαγωγή

- Μεθοδολογίες & Πλαίσια Αποτίμησης Ευπαθειών
- Βασικές Φάσεις Υλοποίησης μιας Διαδικασίας Αποτίμησης Ευπαθειών
- Εργαστηριακές Ασκήσεις

Αποτίμηση Ευπαθειών (Α.Ε.)

- Διαδικασία αξιολόγησης της ασφάλειας ενός οργανισμού ανιχνεύοντας τις απειλές που θέτουν σε κίνδυνο τα αγαθά του οργανισμού
- Στόχος: εκτέλεση ελέγχων σε κάθε εξεταζόμενο αγαθό για την ανίχνευση αδυναμιών και την αξιολόγηση υπαρχόντων αντιμέτρων
  - Έλεγχος των εσωτερικών συστημάτων (π.χ. τοπικά δίκτυα, servers).
  - Έλεγχος της περιμέτρου (π.χ. dns)
- Τύποι ελέγχων
  - Black box testing
  - White box testing
  - Grey box testing

Μεθοδολογίες & Πλαίσια Αποτίμησης Ευπαθειών (1/2)

- Ορίζουν τον τρόπο διενέργειας μιας διαδικασίας Α.Ε. είτε σε βήματα είτε ως γενικευμένες οδηγίες
  - Εξεταζόμενα αγαθά
  - Αντιστοίχηση αγαθών με πιθανές ευπάθειες
  - Χρήση εργαλείων
- Προσεγγίσεις
  - Εστίαση σε τεχνικά θέματα
  - Εστίαση σε διαχειριστικά θέματα
  - Υβριδικές

Μεθοδολογίες & Πλαίσια Αποτίμησης Ευπαθειών (2/2)

- ISSAF
  - Information Systems Security Assessment Framework
- OSSTMM
  - Open-Source Security Testing Methodology Manual
- OWASP
  - Open Web Application Security Project
- WASC-TC
  - Web Application Security Consortium Threat Classification
- NIST SP800-42
  - Guideline on Network Security Testing
- NIST SP800-115
  - Technical Guide to Information Security Testing and Assessment

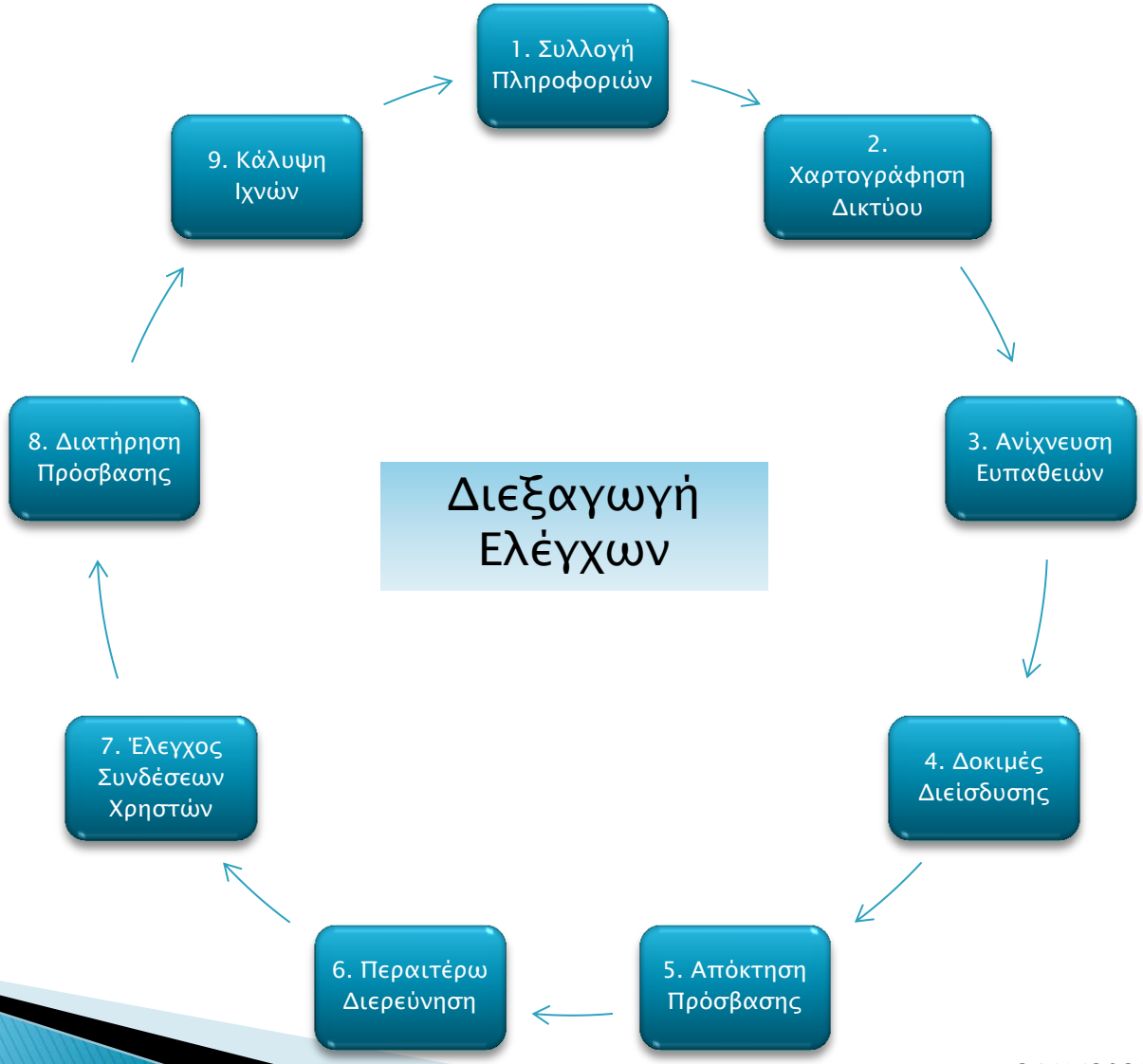
Φάσεις Υλοποίησης

- Η διαδικασία αποτίμησης χωρίζεται σε 3 φάσεις
  - Φάση 1η: Σχεδιασμός και Προετοιμασία
  - Φάση 2η: Αξιολόγηση
  - Φάση 3η: Αναφορά

Φάση 1η: Σχεδιασμός και Προετοιμασία

- Ανταλλαγή αρχικών πληροφοριών μεταξύ των εμπλεκόμενων μερών
- Καθορισμός νομικού πλαισίου κάτω από το οποίο θα εκτελεστεί όλη η διαδικασία
- Προσδιορισμός βασικών παραμέτρων της διαδικασίας ελέγχου
  - Μεθοδολογία ελέγχου
  - Χρονοδιάγραμμα (ημ/νίες διεξαγωγής – διάρκεια ελέγχου)
  - Σκοπός (ορισμός της υπό εξέτασης υποδομής)
  - Εμπλεκόμενες οντότητες
  - Λήψη τελικής έγκρισης

Φάση 2η: Αξιολόγηση



Συλλογή Πληροφοριών (1/2)

- Πλήρης επισκόπηση του στόχου Περιγραφή
  - Συλλογή όλων των πιθανών πληροφοριών για τον στόχο
    - Πληροφορίες για τους υπαλλήλους, συνεργάτες
    - Παρουσία στο Διαδίκτυο, Φυσική τοποθεσία
    - E-mails, αριθμοί τηλεφώνων
    - Τεχνικές Πληροφορίες
    - …
- Χρήση Δημόσιων Πηγών
  - Επισκόπηση της εταιρικής ιστοσελίδας
  - Αναζήτηση διαδικτυακών ιστοσελίδων με αναφορές στο στόχο
  - Χρήση μηχανών αναζήτησης (χρήση προηγμένων επιλογών αναζήτησης (π.χ. site:, link:)).
  - Αναζήτηση τεχνικών λεπτομερειών (π.χ. Διαδικτυακά Forum)
  - Εντοπισμός IP διευθύνσεων και domain names (http://www.robtex.com/)
  - Εκμετάλλευση των συλλεγόντων πληροφοριών (π.χ. τηλέφωνα) χρησιμοποιώντας τεχνικές κοινωνικής δικτύωσης (social engineering)

Συλλογή Πληροφοριών (2/2)

Εργαλεία	
Search Engine Tools	SEAT (Search Engine Assessment Tool)
	FOCA
	Metagoofil
	theHarvester
	Goog-mail
	Way‟BackMachine
	Curl
Document Metadata	SEAT (Search Engine Assessment Tool)
	Metagoofil
	FOCA
Meta-Search Engines	ixquick
	MetaCrawler
	Dogpile
	search.com
On-line Tools	Serversniff
	Domaintools
	Centralops
	Clez
	Robtex
	Webhosting
	Spoke

Σκιαγράφηση (1/2)

- Βασικός στόχος αποτελεί ο προσδιορισμός των τεχνικών χαρακτηριστικών των αγαθών του οργανισμού.
  - Εξερεύνηση των ορίων των δικτύων (Network Mapping)
  - Απαρίθμηση και σκιαγράφηση συστημάτων.
  - Προσδιορισμός των Λειτουργικών συστημάτων (OS fingerprinting)
  - Ανίχνευση διαθέσιμων θυρών (Port Scanning)
  - Αναγνώριση και σκιαγράφηση υπηρεσιών.
  - Πληροφορίες δρομολόγησης και υποστηριζόμενα πρωτόκολλα.
  - Καταγραφή υποστηριζόμενων τεχνολογιών.
- Συλλογή πληροφοριών απαραίτητων για τη δημιουργία μιας αξιόπιστης και ρεαλιστικής τοπολογίας της εξεταζόμενης δικτυακής υποδομής.

Σκιαγράφηση (2/2)

Εργαλεία

- Δικτυακή απαρίθμηση (Network Enumeration
  - Εξέταση DNS υπηρεσίας (DNS Interrogation).
  - Προσδιορισμός δρομολόγησης (Route Identification).
  - Αποτύπωση Firewall.
  - Ανίχνευση συστημάτων (Hosts Identification).
  - Σαρωτές (Port & Service Scanner).
- Ενεργή Σκιαγράφηση Λειτουργικών Συστημάτων (Active OS Fingerprinting.
- Παθητική Σκιαγράφηση (Passive fingerprint.
- Σκιαγράφηση εξυπηρετητών (Web & Application Server Fingerprint).

Προσδιορισμός Ευπαθειών

- Βασικός στόχος αποτελεί ο εντοπισμός και η καταγραφή πιθανών ευπαθειών της εξεταζόμενης υποδομής.
  - Βήμα 1: Αναζήτηση γνωστών αδυναμιών
    - Αναζήτηση σε ευρέως διαδεδομένες «βάσεις γνώσεις» (π.χ. Security Focus [SecFocus], BugTraq [BT], NTBugTraq [NTBT], Full Disclosure [FD], ISS‟ Xforce [ISSxForce], NIST‟s National Vulnerability Database [NVD], Common Vulnerability and Exposures [CVE)]
  - Βήμα 2: Εντοπισμός αδυναμιών
    - Χρήση αυτοματοποιημένων ή μη εργαλείων για την ανίχνευση αδυναμιών. Η φύση του υπό ελέγχου αγαθού καθορίζει την υιοθέτηση και εφαρμογή των απαιτούμενων ελέγχων.

Βήμα 2: Εντοπισμός αδυναμιών

Έλεγχοι

- Έλεγχος Μηχανισμών Ελέγχου Πρόσβασης: ορθότητα και αποτελεσματικότητα των εφαρμοζόμενων μηχανισμών ελέγχου πρόσβασης.
- Έλεγχος Μηχανισμών Ανίχνευσης Εισβολών: απόδοση και ευαισθησία των μηχανισμών ανίχνευσης εισβολών.
- Έλεγχος Μηχανισμών Αντιμετώπισης Κακόβουλου Λογισμικού: αποτελεσματικότητα των εφαρμοζόμενων μηχανισμών.
- Έλεγχος Ισχύος κωδικών πρόσβασης: ανθεκτικότητα των κωδικών πρόσβασης.
- Έλεγχος Ασφάλειας Ασύρματου Δικτύου: εντοπισμός πιθανών αδυναμιών ασφάλειας στην υπάρχουσα υποδομή του ασύρματου δικτύου.
- Έλεγχος Ασφάλειας Τείχους Προστασίας (Firewall): παραμετροποίηση του τείχους προστασίας ώστε να διασφαλιστεί ότι η ασφαλή πρόσβαση μεταξύ δικτύων.
- Έλεγχος Ασφάλειας Δικτυακού Εξοπλισμού (Router/Switch): εντοπισμός ευπαθειών οι δρομολογητές που είναι συνδεδεμένοι στο δίκτυο του οργανισμού.
- Έλεγχος Ασφάλειας Εξυπηρετητών (Servers): εντοπισμό ενδεχόμενων ευπαθειών.

- Έλεγχος Ασφάλειας Διαδικτυακών Εφαρμογών: εύρεση γνωστών αδυναμιών που μπορεί να οδηγήσει στη διακύβευση της ασφάλειάς τους:
  - Εξέταση Μηχανισμών Αυθεντικοποίησης: κατανόηση και εξέταση της διαδικασίας αυθεντικοποίησης.
  - Διαχείριση Συνόδων: η διαχείριση των συνόδων στην εξεταζόμενη εφαρμογή.
  - Εξέταση Μηχανισμών Εξουσιοδότησης: κατανόηση και έλεγχος των μηχανισμών εξουσιοδότησης που υλοποιούνται από την εφαρμογή.
  - Επιχειρησιακή Λογική: εντοπισμό αδυναμιών στην επιχειρηματικής της λογική.

- Έλεγχος και Επικύρωση Δεδομένων: τα δεδομένα τα οποία δέχεται σαν είσοδο η εξεταζόμενη εφαρμογή ελέγχονται και επικυρώνονται προτού ξεκινήσει η διαδικασία της επεξεργασίας τους.
  - Cross Site Scripting (XSS): τροποποίηση των παραμέτρων που δέχεται ως είσοδο η εφαρμογή μπορεί να οδηγήσει σε αποκάλυψη ευαίσθητων πληροφοριών.
  - SQL Injection: εισαγωγή δεδομένων στην εφαρμογή με στόχο την εκτέλεση SQL ερωτημάτων στη Βάση Δεδομένων (ΒΔ).
  - LDAP Injection: αποκάλυψη, τροποποίηση ή εισαγωγή ευαίσθητων πληροφοριών οι οποίες βρίσκονται σε υποδομές LDAP.
  - XML Injection: εισαγωγή XML εγγράφου με σκοπό την παραποίηση δεδομένων στην εφαρμογή.
  - SSI Injection: εξέταση του κώδικα των HTML σελίδων με σκοπό να διαπιστωθεί η δυνατότητα εισαγωγής κώδικα μέσα σε αυτές καθώς και η δυνατότητα εκτέλεσης του κώδικα από απόσταση.
  - XPATH Injection: εισαγωγή δεδομένων στην εφαρμογή με σκοπό την εκτέλεση κατάλληλα διαμορφωμένων από τους χρήστες ερωτημάτων XPath.
  - IMAP/SMTP Injection: εισαγωγής εντολών IMAP/SMTP και εκτέλεσης τους στους mail servers.
  - Code Injection: εισαγωγή συγκεκριμένου τμήματος κώδικας το οποίο θα εκτελεστεί στον εξυπηρετητή .

- Operation System (OS) Commanding: εισαγωγή εντολών λειτουργικού συστήματος ως δεδομένα εισόδου και εκτέλεση τους στον εξυπηρετητή που φιλοξενεί το “server-side” της εφαρμογής.
- Buffer overflow Έλεγχοι: έλεγχος ως προς διαφορετικούς τύπους αδυναμιών που σχετίζονται με απειλές buffer overflow (Heap overflow αδυναμίες, Stack overflow αδυναμίες, Format string αδυναμίες).
- Έλεγχος Ασφάλειας Βάσεων Δεδομένων: οι συγκεκριμένοι έλεγχοι πραγματοποιούνται για την εξέταση της εξασφάλισης της ασφάλειας/διαθεσιμότητας των Β.Δ.
- Έλεγχοι Υπηρεσιών Ιστού (Web Services):
  - Έλεγχος Συμμόρφωσης ΥΙ: έλεγχος συμμόρφωσης των τεχνολογιών και των προτύπων των ΥΙ ως προς τις αντίστοιχες προδιαγραφές.
  - Έλεγχος εγγράφων XML: εξέταση των μηχανισμών διαχείρισης των εγγράφων XML ώστε να διαπιστωθεί ότι οι μηχανισμοί αυτοί σέβονται τόσο τη σημασιολογία του περιεχομένου όσο και τη δομή των εγγράφων.
  - Έλεγχος Επιθέσεων Επανάληψης (Replay Attacks): Εξέταση της εφαρμογής για να διαπιστωθεί η ανθεκτικότητα της σε επιθέσεις τύπου Επανάληψης

Προσδιορισμός Ευπαθειών

- Βήμα 3: Δημιουργία λίστας με όλες τις αδυναμίες που εντοπίστηκαν
- Βήμα 4: Επισκόπηση των εντοπισμένων αδυναμιών για την εύρεση ψευδώς θετικών αδυναμιών
- Βήμα 5: Δημιουργία της τελικής λίστας με τις αδυναμίες που εντοπίστηκαν
- Βήμα 7: Προσδιορισμός σεναρίων

Δοκιμές Διείσδυσης

- Βασικός στόχος αποτελεί η επιβεβαίωση των αδυναμιών. Οι δοκιμές διείσδυσης εκτελούνται με βάση τα σενάρια που έχουν προσδιοριστεί στο τέλος του προηγούμενου σταδίου:
  - Επιβεβαίωση των ευρημάτων με την απευθείας εξέταση των αγαθών που βρίσκονται υπό έλεγχο για τη διασταύρωση των αποτελεσμάτων.
  - Προσομοίωση επιθέσεων σε επίπεδο δικτύου, λειτουργικών συστημάτων, εξυπηρετητών κ.τ.λ. ώστε να διαπιστωθεί ότι οι αδυναμίες είναι εκμεταλλεύσιμες:
    - Με χρήση αυτοματοποιημένων εργαλείων εκτέλεσης επιθέσεων.
    - Με την εκτέλεση κακόβουλου scripting κώδικα που μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των συστημάτων.

Απόκτηση Πρόσβασης

- Βασικός στόχος αποτελεί η απόκτηση πρόσβασης σε αγαθά της υπό εξέταση υποδομής ως αποτέλεσμα των δοκιμών διείσδυσης:
  - Βελτίωση των δικαιωμάτων πρόσβασης στο σύστημα (με την απόκτηση δικαιωμάτων διαχειριστή/συστήματος)

Περαιτέρω Διερεύνηση

- Βασικός στόχος αποτελεί η συγκέντρωση περαιτέρω πληροφοριών για την υπό εξέταση υποδομή οι οποίες μπορούν να ληφθούν μέσω των ελεγχόμενων αγαθών:
  - πληροφορίες χρηστών
  - κωδικοί πρόσβασης χρηστών
  - δικτυακές πληροφορίες (ανίχνευση διαδρομών και άλλων δικτύων)
  - …

Επέκταση Πρόσβασης

- Βασικός στόχος αποτελεί η επέκταση της πρόσβασης και σε άλλα αγαθά της υπό εξέταση υποδομής εκμεταλλευόμενοι τις πληροφορίες που συγκεντρώθηκαν στο προηγούμενο στάδιο:
  - Domain Controllers
  - Workstations/Servers
  - Routers/Switches
  - Εφαρμογές
  - …

Διατήρηση Πρόσβασης

- Βασικός στόχος αποτελεί η διατήρηση της πρόσβασης στα αγαθά της υπό εξέταση υποδομής:
  - Convert channels
  - Backdoors
  - …

Κάλυψη Ιχνών

- Βασικός στόχος αποτελεί η κάλυψη όλων των στοιχείων τα οποία ενδέχεται να οδηγήσουν στην αποκάλυψη ότι η ασφάλεια ενός συστήματος έχει παραβιαστεί:
  - Τοποθέτηση των κακόβουλων αρχείων σε κρυφούς φακέλους
  - Τοποθέτηση των κακόβουλων αρχείων σε μη-προσβάσιμους φακέλους
  - Μετονομασία των καταλήξεων των αρχείων σε κατάληξη άσχετη με το σκοπό του.
  - Καθαρισμός των αρχείων καταγραφής γεγονότων (log files)
  - …

Φάση 3η: Αναφορά

- Αναφορά και αξιολόγηση των αποτελεσμάτων που προέκυψαν από τον έλεγχο.
  - Σκοπός και εύρος δοκιμών.
  - Εργαλεία που χρησιμοποιήθηκαν.
  - Ημερομηνίες εκτέλεσης των δοκιμών.
  - Τα αποτελέσματα των ελέγχων συμπεριλαμβανομένων των αναφορών όπως αυτά δημιουργήθηκαν από τα εργαλεία ασφάλειας που χρησιμοποιηθήκαν.
  - Μια λίστα με τις ευπάθειες οι οποίες εντοπίστηκαν.
  - Μια λίστα με προτεινόμενες λύσεις οι οποίες πρέπει να υιοθετηθούν για την διευθέτηση των ζητημάτων που εντοπίστηκαν.
- Καθαρισμός των υπό εξέταση συστημάτων από τα δεδομένα που δημιουργήθηκαν κατά τη διάρκεια του ελέγχου

Ευχαριστώ!!!!!!!!!

Ενημέρωση:

http://athina.cs.unipi.gr/security-lab

http://gunet2.cs.unipi.gr/eclass/courses/TME135/