1η Άσκηση: *Μελέτη Ασφάλειας Πληροφοριακού Συστήματος*

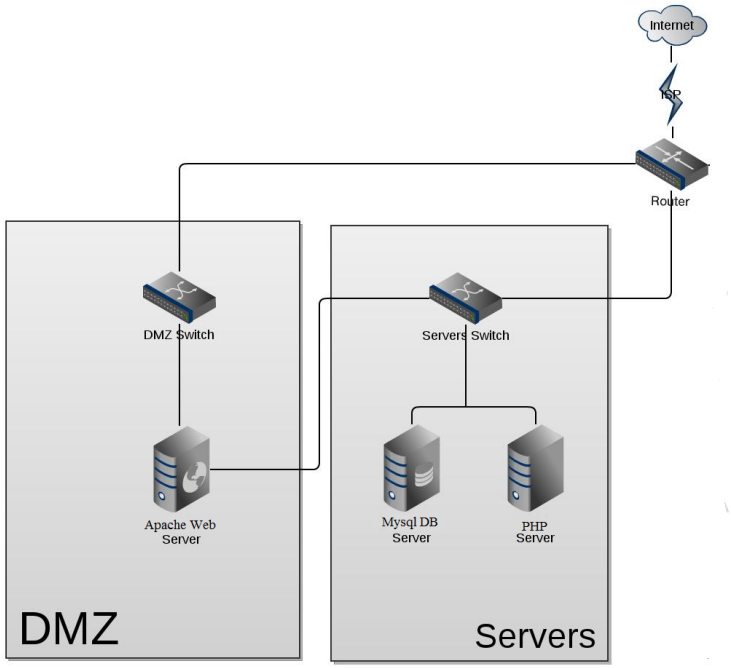
Με βάση το παρακάτω παράδειγμα, καλείστε να πραγματοποιήσετε καταγραφή των υπηρεσιών και των αγαθών του ΠΣ (web εφαρμογής) το οποίο θα χρησιμοποιήσετε για την εργασία του μαθήματος, καθώς και μία αρχική μελέτη ασφάλειας του συστήματος.

Παράδειγμα περιγραφής συστήματος

Ένα μικρό ηλεκτρονικό κατάστημα παρέχει τις παρακάτω on-line ***υπηρεσίες***:

1. ***Αναζήτηση προϊόντων:*** Παρέχεται η δυνατότητα σε όλους τους χρήστες (εγγεγραμμένους ή όχι) να αναζητήσουν στον κατάλογο προϊόντων του καταστήματος, μέσα από πεδίο αναζήτησης ή πατώντας σε συνδέσμους κατηγοριών – υποκατηγοριών των προϊόντων.
2. ***Εγγραφή χρηστών***: οι χρήστες εγγράφονται για τις υπηρεσίες του ηλεκτρονικού καταστήματος μέσω web φόρμας, παρέχοντας στοιχεία όπως όνομα, διεύθυνση επικοινωνίας, e-mail κτλ. Το η-κατάστημα έχει αυτή τη στιγμή περίπου 1.000 εγγεγραμμένους χρήστες. Οι χρήστες δημιουργούν ένα μοναδικό κωδικό πρόσβασης, ο οποίος διατηρείται ανανεώνεται κάθε 2 έτη το αργότερο.
3. ***Ηλεκτρονικές αγορές (on-line payments):*** Οι εγγεγραμμένοι χρήστες έχουν τη δυνατότητα να πραγματοποιήσουν ηλεκτρονικές αγορές των προϊόντων. Πριν την 1η αγορά τους ζητείται να δώσουν στοιχεία πιστωτικής κάρτας, τα οποία αποθηκεύονται στη βάση σε κρυπτογραφημένη μορφή. Η αποστολή των στοιχείων της πιστωτικής κάρτας κρυπτογραφείται με τη χρήση του πρωτοκόλλου SSL/TLS (λεπτομέρειες έκδοσης ssl/tls αναφέρονται παρακάτω). Η διεκπεραίωση της πληρωμής γίνεται μέσα από συνεργαζόμενη τράπεζα.

Η αρχιτεκτονική του δικτύου δίδεται στο παρακάτω σχήμα:



Οι τεχνολογίες πάνω στις οποίες έχει υλοποιηθεί η παραπάνω υπηρεσία είναι οι ακόλουθες:

- Λειτουργικό Σύστημα: Debian 10.13
- Εξυπηρετητής Ιστού: Apache v. 2.4.39 με υποστήριξη OpenSSL
- Εξυπηρετητής εφαρμογής: php v. 5.3.7
- Εξυπηρετητής βάσης δεδομένων: MySQL v. 8.1.0
- Πλαίσιο υλοποίησης (framework): Joomla v. 4.2
- Πρωτόκολλο ασφάλειας SSL/TLS: TLS v1.2. Υλοποίηση με τη χρήση της βιβλιοθήκης Openssl v 3.0.11
- Κλειδί εξυπηρετητή: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Ερωτήματα:

(1) Καταγραφή του υπό μελέτη συστήματος. Να πραγματοποιήσετε **για το δικό σας ΠΣ** μία αρχική καταγραφή των υπηρεσιών και της αρχιτεκτονικής του συστήματος. Να περιγράψετε τουλάχιστον **3 υπηρεσίες του ΠΣ**. *(1-2 σελίδες με βάση το παραπάνω ενδεικτικό παράδειγμα και ανάλογα με το δικό σας Πληροφοριακό Σύστημα)*

(2) Δημιουργία μοντέλου αγαθών (asset model). Για κάθε υπολογιστικό σύστημα που αποτελεί μέρος του ΠΣ που έχετε περιγράψει στο προηγούμενο βήμα, να μοντελοποιήσετε αναλυτικά όλα τα αγαθά του υπολογιστικού συστήματος (H/W, S/W, Network, Data). Να καταγράψτε το μοντέλο αγαθών **για 3 υπολογιστικά συστήματα**. Για την μοντελοποίηση μπορείτε να χρησιμοποιήσετε τον παρακάτω πίνακα για την μοντελοποίηση των αγαθών κάθε Υπολογιστικού Συστήματος.

(Παράδειγμα: στο Πληροφοριακό Σύστημα του ηλεκτρονικού καταστήματος που δόθηκε ως παράδειγμα προηγουμένως, τα υπολογιστικά συστήματα μπορεί να περιλαμβάνουν τον Web Server, Application Server, Database Server, Administrator PC κτλ)

Όνομα Υπολογιστικού Συστήματος:		
HW	Server (μοντέλο, χαρακτηριστικά)	...
	Τοποθεσία (κτήριο, δωμάτιο)	...
SW	Λειτουργικό Σύστημα (πυρήνας, έκδοση)	...
	Λογισμικό Εφαρμογών	...
	Άλλο Λογισμικό	...
Network	Περιοχή Δικτύου (network zone)	...
	Σημείο σύνδεσης (Gateway)	...
Data	Δεδομένα διαμόρφωσης (Configuration data)	...
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	...
	Άλλα δεδομένα	...

(3) Αντιστοίχηση υπηρεσιών και υπολογιστικών συστημάτων. Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αντιστοιχίσετε τα υπολογιστικά συστήματα που χρησιμοποιούνται για την παροχή της υπηρεσίας (από αυτά που περιγράψατε στο βήμα 2). Είναι πιθανό ένα υπολογιστικό σύστημα να χρησιμοποιείται για την παροχή περισσότερων από μία υπηρεσιών.

(4) Αποτίμηση συνεπειών ή επιπτώσεων ασφάλειας (impact assessment). Για κάθε μία υπηρεσία που παρέχει το υπό μελέτη σύστημα, όπως τις έχετε περιγράψει στο βήμα 1, να αποτιμήσετε τις πιθανές συνέπειες ασφάλειας (security impact) από την πιθανή παραβίαση της ασφάλειας των αγαθών που συμμετέχουν στην κάθε υπηρεσία, ως εξής:

- Συνέπειες μη διαθεσιμότητας της υπηρεσίας (unavailability / loss of Availability).
- Συνέπειες αποκάλυψης των δεδομένων που διαχειρίζεται η υπηρεσία (disclosure / loss of Confidentiality).

- Συνέπειες τροποποίησης των δεδομένων που διαχειρίζεται η υπηρεσία (modification / loss of Integrity).

Ο **Τύπος Συνέπειας** θα έχει μία ή περισσότερες από τις παρακάτω επιλογές:

- Άμεσες οικονομικές απώλειες
- Παρεμπόδιση λειτουργιών
- Δυσφήμιση
- Νομικές Κυρώσεις

Ο **Βαθμός Συνέπειας** θα έχει μία από τις παρακάτω τιμές:

1. Χαμηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος μέχρι €1000/περιστατικό.
2. Μέτρια: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος από €1001 μέχρι €10.000/περιστατικό.
3. Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €10.001 μέχρι €100.000/περιστατικό.
4. Πολύ Υψηλή: Η εκτιμώμενη άμεση ή έμμεση ζημία θα έχει κόστος πάνω από €100.000/περιστατικό.

Η αποτίμηση συνεπειών θα γίνει, για κάθε υπηρεσία με τη βοήθεια του παρακάτω πίνακα:

Όνομα Υπηρεσίας:	**…**		
	Τύπος Συνέπειας	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)			
(2) Αποκάλυψη δεδομένων (disclosure)			
(3) Τροποποίηση δεδομένων (modification)			

(5) Αποτίμηση απειλών(threat assessment). Να αξιολογήσετε τις παρακάτω απειλές για κάθε ένα από τα 3 υπολογιστικά συστήματα που καταγράψατε στο βήμα 2:

- Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access).
- Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware).
- Παραποίηση ιστοσελίδας (Web Defacement).
- Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection).
- Άρνηση υπηρεσίες (Denial of Service).

Η αποτίμηση κάθε απειλής για κάθε ένα από τα 3 υπολογιστικά συστήματα που μελετάτε, θα γίνει με βάση την κλίμακα:

0. Δεν εφαρμόζεται (not applicable): Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.
1. Χαμηλή πιθανότητα (Low likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%.
2. Μέτρια πιθανότητα (Medium likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 30%.
3. Υψηλή πιθανότητα (High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.
4. Πολύ υψηλή πιθανότητα (Very High likelihood): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

(6) Αποτίμηση αδυναμιών (vulnerability assessment). Να γίνει αποτίμηση αδυναμιών **για όλα τα αγαθά λογισμικού** των τριών υπό μελέτη υπολογιστικών συστημάτων (Λειτουργικό Σύστημα, λογισμικό εφαρμογών). Να χρησιμοποιήσετε διαθέσιμες βάσεις αδυναμιών π.χ. τη βάση αδυναμιών ασφάλειας του NIST (http://nvd.nist.gov/). Στην έρευνά σας θα πρέπει να συγκεντρώσετε και να περιγράψετε τις βασικότερες αδυναμίες ασφάλειας που υπάρχουν για τις συγκεκριμένες εκδόσεις λογισμικού που περιλαμβάνονται στα υπό μελέτη υπολογιστικά συστήματα.

(7) Αποτίμηση κινδύνων (risk assessment). Με βάση τα παραπάνω βήματα να αναφέρετε και να αιτιολογήσετε τους σημαντικότερους κινδύνους ασφάλειας για το υπό μελέτη ΠΣ.

(8) Επανεκτίμηση αδυναμιών μετά την υλοποίηση των μέτρων ασφάλειας (vulnerability post assessment). Μετά την ολοκλήρωση της υλοποίησης των μέτρων ασφάλειας, να πραγματοποιήσετε επανεκτίμηση των αδυναμιών ασφάλειας που είχατε αποτιμήσει στο βήμα (6), κάνοντας χρήση του εργαλείου CVSS V3. Για την επανεκτίμηση των αδυναμιών θα πρέπει να τροποποιήσετε κατάλληλα το temporal score και το environmental score για κάθε υπό μελέτη αδυναμία ασφάλειας, τεκμηριώνοντας ποια από τα επιπρόσθετα μέτρα ασφάλειας που υλοποιήσατε επηρέασαν την απόφασή σας.