Εργαστήριο 2.1 – Ρύθμιση Πολιτικών Ασφαλείας σε Εικονική Μηχανή

1. Επισκόπηση Εργαστηρίου

1.1 Περιγραφή Εργαστηρίου

Σε αυτό το εργαστήριο, θα εξασκηθείτε στη **θωράκιση συστήματος** διαμορφώνοντας πολιτικές ασφαλείας μέσα σε μια εικονική μηχανή (VM). Οι εικονικές μηχανές προσφέρουν ένα ασφαλές περιβάλλον δοκιμών, όπου μπορείτε να εφαρμόζετε πραγματικές πολιτικές χωρίς να διακινδυνεύετε το βασικό σας σύστημα.

Θα μάθετε να:

- Δημιουργήστε και διαχειριστείτε λογαριασμούς χρηστών με τα κατάλληλα δικαιώματα.
- Εφαρμόστε αυστηρές πολιτικές κωδικών πρόσβασης.
- Περιορίστε τα δικαιώματα διαχειριστή.
- Ενεργοποιήστε την καταγραφή συστήματος για παρακολούθηση και έλεγχο.

Μέχρι το τέλος αυτού του εργαστηρίου, θα έχετε ένα **ενισχυμένο στιγμιότυπο VM** — μια ασφαλή βάση στην οποία μπορείτε να επιστρέψετε όποτε χρειαστεί.

1.2 Στόχοι Μάθησης

Με την ολοκλήρωση του εργαστηρίου, θα είστε σε θέση να:

- Εξηγήστε γιατί η ενίσχυση της ασφάλειας του συστήματος είναι ζωτικής σημασίας στην κυβερνοασφάλεια.r>Στήστε ένα εικονικό περιβάλλον για να δοκιμάσετε πολιτικές ασφαλείας.r>Ρυθμίστε πολιτικές για ισχυρούς κωδικούς πρόσβασης σε Windows και Linux.r> Περιορίστε τα δικαιώματα διαχείρισης εφαρμόζοντας την αρχή της ελάχιστης πρόσβασης.r> Ενεργοποιήστε και ελέγξτε συστήματα καταγραφής και ελέγχου.r>Τεκμηριώστε και αποθηκεύστε ένα ασφαλές στιγμιότυπο της εικονικής μηχανής για μελλοντική χρήση.

1.3 Προαπαιτούμενα

Για να ολοκληρώσετε επιτυχώς το εργαστήριο, θα χρειαστείτε:

- Έναν υπολογιστή με **τουλάχιστον 8GB RAM** και **20GB ελεύθερου χώρου στο δίσκο**.

- Ένα εργαλείο εικονικοποίησης εγκατεστημένο (VirtualBox, VMware Workstation ή Hyper-V).
- Ένα αρχείο εγκατάστασης ISO για Windows (10/11) ή Linux (προτείνεται Ubuntu Server).
- Βασικές γνώσεις στη χρήση γραμμής εντολών (Linux) και διαχείρισης συστημάτων.
- Δικαιώματα διαχειριστή στο βασικό σας σύστημα (για εγκατάσταση/παραμετροποίηση εικονικών μηχανών).

1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης

Δραστηριότητα	**Εκτιμώμενος Χρόνος**
Ρύθμιση της εικονικής μηχανής (εγκατάσταση + δημιουργία χρηστών)	90 λεπτά
Διαμόρφωση πολιτικών πρόσβασης κωδικού	60 λεπτά
Περιορισμός δικαιωμάτων διαχειριστή	45 λεπτά
Ενεργοποίηση και επαλήθευση καταγραφής συμβάντων	45 λεπτά
Δοκιμασία εργαστηρίου: Στιβαρό στιγμιότυπο VM + ανάλυση	60 λεπτά
Συνολικός Εκτιμώμενος Χρόνος	**~5 ώρες**

Σημείο Ελέγχου

Πριν συνεχίσετε, βεβαιωθείτε ότι:

- Γνωρίζετε ότι αυτό το εργαστήριο διαρκεί περίπου 5 ώρες.
- Έχετε εγκαταστήσει την πλατφόρμα εικονικής μηχανής.
- Έχετε επιλέξει λειτουργικό σύστημα (Windows ή Linux) για εξάσκηση.

2. Ξεκινώντας

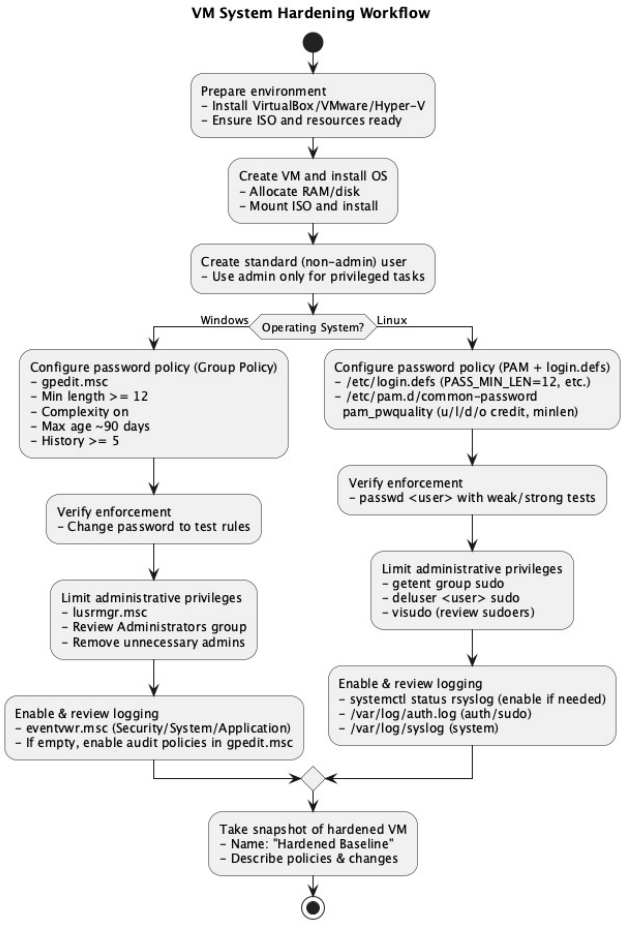
2.1 Τι είναι η Ενίσχυση Ασφαλείας Συστήματος;

Η θωράκιση συστήματοςείναι η διαδικασία ενίσχυσης της ασφάλειας ενός υπολογιστικού συστήματος, περιορίζοντας τις ευάλωτες πλευρές του. Αυτό περιλαμβάνει τη διαγραφή περιττών λογαριασμών, την εφαρμογή αυστηρών πολιτικών και την ενεργοποίηση λειτουργιών παρακολούθησης για τον έγκαιρο εντοπισμό ύποπτης δραστηριότητας.

Παραδείγματα ενεργειών θωράκισης:

- Επιβολή **ισχυρών κωδικών πρόσβασης**
- Περιορισμός **δικαιωμάτων διαχειριστή**
- Ενεργοποίηση **καταγραφής και ελέγχου**
- Αφαίρεση ή απενεργοποίηση μη χρησιμοποιούμενων υπηρεσιών

Βασική Αρχή: Όσο λιγότερα «αδύναμα σημεία» έχει ένα σύστημα, τόσο πιο δύσκολο είναι για έναν επιτιθέμενο να πετύχει.



2.2 Γιατί να χρησιμοποιήσουμε εικονικές μηχανές στα εργαστήρια ασφάλειας;

Οι εικονικές μηχανές (VMs) προσφέρουν ένα **ασφαλές περιβάλλον δοκιμών** για εξάσκηση στην κυβερνοασφάλεια:

- **Απομόνωση** – Οι αλλαγές σας δεν επηρεάζουν το κεντρικό σας σύστημα.
- **Δυνατότητα επαναφοράς** – Μπορείτε να επιστρέψετε σε ένα αποθηκευμένο στιγμιότυπο αν κάτι πάει στραβά.
- **Υποστήριξη πολλών λειτουργικών** – Εξασκηθείτε στην ενίσχυση τόσο σε Windows όσο και σε Linux.
- **Ρεαλισμός** – Οι εικονικές μηχανές λειτουργούν σαν πραγματικά συστήματα, ώστε οι δεξιότητές σας να μεταφέρονται απευθείας σε παραγωγικά περιβάλλοντα.

2.3 Λίστα ελέγχου για την εγκατάσταση του εργαστηρίου

Πριν ξεκινήσετε, βεβαιωθείτε ότι διαθέτετε:

Εγκατάσταση λογισμικού εικονικοποίησης

- VirtualBox (δωρεάν, συμβατό με όλα τα λειτουργικά)
- VMware Workstation Player (δωρεάν για προσωπική χρήση)
- Hyper-V (περιλαμβάνεται στα Windows Pro/Enterprise)

Αρχείο ISO λειτουργικού συστήματος

- Windows 10/11 (αρκεί και η δοκιμαστική έκδοση)
- Ubuntu Server (ελαφριά επιλογή Linux)

Απαιτήσεις συστήματος υπολογιστή

- Ελάχιστες απαιτήσεις: 8 GB RAM και 20 GB ελεύθερος χώρος στο δίσκο
- Σύνδεση στο διαδίκτυο (για ενημερώσεις και λήψεις)

Βασικά βήματα ρύθμισης VM ολοκληρωμένα

- Δημιουργήθηκε νέα εικονική μηχανή
- Εγκαταστάθηκε το επιλεγμένο λειτουργικό σύστημα
- Δημιουργήθηκε τουλάχιστον **ένας βασικός (μη διαχειριστής) λογαριασμός χρήστη**

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Έχετε προετοιμάσει ένα λειτουργικό περιβάλλον εικονικής μηχανής;
- Έχετε εγκαταστήσει Windows ή Linux μέσα στη VM;
- Δημιουργήσατε έναν **κανονικό λογαριασμό χρήστη** (όχι μόνο admin/root);

3. Ρύθμιση της Εικονικής Σας Μηχανής

3.1 Επιλογή Πλατφόρμας Εικονικοποίησης

Χρειάζεστε λογισμικό εικονικοποίησης για να εκτελέσετε την εικονική σας μηχανή. Δημοφιλείς επιλογές:

- **VirtualBox** (δωρεάν, συμβατό με όλα τα λειτουργικά)
- **VMware Workstation Player** (δωρεάν για προσωπική χρήση)
- **Hyper-V** (ενσωματωμένο στα Windows Pro/Enterprise)

Συμβουλή: Αν δεν είστε σίγουροι, προτιμήστε το **VirtualBox** — είναι ευρέως υποστηριζόμενο και εύχρηστο.

3.2 Δημιουργία Νέας Εικονικής Μηχανής

Ακολουθήστε τον οδηγό «Νέας Εικονικής Μηχανής» της πλατφόρμας σας. Τα συνήθη βήματα είναι:

1. **Ονομασία και Επιλογή Λειτουργικού Συστήματος**
    - Παράδειγμα: «Ubuntu Ενισχυμένη VM» ή «Εργαστήριο Ασφαλείας Windows»
    - Επιλέξτε τον τύπο και την έκδοση του λειτουργικού συστήματος

2. **Κατανομή Πόρων**
    - Μνήμη: τουλάχιστον **2 GB για Linux**, **4 GB για Windows**
    - Δίσκος: τουλάχιστον 20 GB

3. **Σύνδεση μέσου εγκατάστασης**
    - Τοποθετήστε το αρχείο ISO για την εγκατάσταση των Windows ή του Linux

4. **Εγκατάσταση λειτουργικού συστήματος**
    - Εκκινήστε τη VM και ακολουθήστε τα συνηθισμένα βήματα εγκατάστασης του λειτουργικού συστήματος

3.3 Δημιουργία Λογαριασμών Κανονικών Χρηστών

Αφού εγκαταστήσετε το λειτουργικό σύστημα στη VM σας:

- **Στα Windows**
  - Ανοίξτε **Ρυθμίσεις → Λογαριασμοί → Οικογένεια & άλλοι χρήστες**
  - Δημιουργήστε νέο **κανονικό χρήστη** (μη διαχειριστή)
  - Χρησιμοποιείτε τον λογαριασμό διαχειριστή μόνο για εργασίες με προνόμια
- **Στο Linux**
  - Προσθέστε νέο χρήστη με:
  - sudo adduser studentuser
  - Όταν σας ζητηθεί, ορίστε έναν κωδικό πρόσβασης
  - Επιβεβαιώστε ότι ο λογαριασμός λειτουργεί πραγματοποιώντας είσοδο

Αρχή της Ελάχιστης Αναγκαίας Πρόσβασης: Για καθημερινές εργασίες, χρησιμοποιείτε πάντα λογαριασμούς χρήστη χωρίς διαχειριστικά δικαιώματα.

Πρόσβαση διαχειριστή/root να χρησιμοποιείται μόνο όταν είναι απολύτως απαραίτητο.

3.4 Ανακεφαλαίωση: Βασικά σημεία ρύθμισης VM

Βήμα	Windows	Linux
Δημιουργία VM	Οδηγός VirtualBox/VMware/Hyper-V	Οδηγός VirtualBox/VMware/Hyper-V
Εγκατάσταση λειτουργικού συστήματος	Windows 10/11	Ubuntu Server/Desktop
Δημιουργία λογαριασμού απλού χρήστη	Ρυθμίσεις → Λογαριασμοί → Προσθήκη χρήστη	`sudo adduser studentuser`
Επιβεβαίωση περιορισμένων δικαιωμάτων	Σύνδεση ως απλός χρήστης, όχι διαχειριστής	Βεβαιωθείτε ότι η πρόσβαση στο sudo είναι περιορισμένη

Σημείο ελέγχου

Πριν προχωρήσετε:

- Έχετε εγκαταστήσει και εκκινήσει το VM σας;
- Υπάρχει τουλάχιστον ένας **λογαριασμός απλού χρήστη**;
- Μπορείτε να συνδεθείτε χωρίς να χρησιμοποιήσετε λογαριασμό διαχειριστή/root;

4. Εφαρμογή Πολιτικής Κωδικών Πρόσβασης

Οι κωδικοί πρόσβασης αποτελούν συχνά την πρώτη γραμμή προστασίας ενάντια σε εισβολείς. Αδύναμοι κωδικοί θέτουν σε κίνδυνο ακόμα και τα πιο ασφαλή συστήματα. Σε αυτή την ενότητα, θα υιοθετήσετε κανόνες που επιβάλλουν τη χρήση ισχυρότερων και πιο ασφαλών κωδικών.

4.1 Windows: Μέσω του Επεξεργαστή Ομαδικής Πολιτικής

1. **Άνοιγμα του Επεξεργαστή Ομαδικής Πολιτικής**
    - Πατήστε **Windows key + R**
    - Πληκτρολογήστε:
    - gpedit.msc
    - Πατήστε **Enter**
2. **Μετάβαση στις Ρυθμίσεις Κωδικού Πρόσβασης**
    - Διαμόρφωση Υπολογιστή → Ρυθμίσεις Windows → Ρυθμίσεις Ασφαλείας → Πολιτικές Λογαριασμού → Πολιτική Κωδικού Πρόσβασης
3. **Ορίστε ισχυρούς κανόνες**
    - Ελάχιστο μήκος κωδικού πρόσβασης: **12 χαρακτήρες**
    - Ο κωδικός πρόσβασης πρέπει να πληροί τις απαιτήσεις πολυπλοκότητας (κεφαλαία, πεζά, αριθμοί, σύμβολα)
    - Μέγιστη διάρκεια κωδικού πρόσβασης: **90 ημέρες**
    - Ελάχιστη διάρκεια κωδικού πρόσβασης: **1 ημέρα**
    - Ενεργοποίηση ιστορικού κωδικών: **αποθήκευση των 5 τελευταίων κωδικών**

Συμβουλή: Μετά την εφαρμογή των αλλαγών, αποσυνδεθείτε και δοκιμάστε να δημιουργήσετε νέο κωδικό για να ελέγξετε την εφαρμογή των ρυθμίσεων.

4.2 Linux: Ρύθμιση PAM και login.defs

Το Linux αξιοποιεί **PAM (Pluggable Authentication Modules)** για τον έλεγχο ταυτοποίησης.

Α. Επεξεργασία του /etc/login.defs

1. Άνοιξε το αρχείο με έναν επεξεργαστή κειμένου:
2. sudo nano /etc/login.defs
3. Τροποποίησε τις παρακάτω ρυθμίσεις:
4. PASS_MAX_DAYS 90
5. PASS_MIN_DAYS 1
6. PASS_MIN_LEN 12
7. PASS_WARN_AGE 7
    - **PASS_MAX_DAYS** = υποχρεωτική αλλαγή κωδικού μετά από 90 ημέρες
    - **PASS_MIN_LEN** = ελάχιστο μήκος κωδικού

Β. Επεξεργασία πολιτικών κωδικού PAM

1. Άνοιγμα ρυθμίσεων κωδικού PAM:
2. sudo nano /etc/pam.d/common-password
3. Προσθέστε ή τροποποιήστε την παρακάτω γραμμή:
4. password requisite pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
    - minlen=12 → Ελάχιστο μήκος 12 χαρακτήρες
    - ucredit=-1 → Απαιτείται τουλάχιστον ένα κεφαλαίο γράμμα
    - lcredit=-1 → Απαιτείται τουλάχιστον ένα πεζό γράμμα
    - dcredit=-1 → Απαιτείται τουλάχιστον ένα ψηφίο
    - ocredit=-1 → Απαραίτητος τουλάχιστον ένας ειδικός χαρακτήρας

Δοκιμάστε το: Δοκιμάστε να αλλάξετε έναν κωδικό με το passwd studentuser — αδύναμοι κωδικοί θα απορρίπτονται.

4.3 Κατευθυντήριες Οδηγίες για Ισχυρούς Κωδικούς

Ακόμη και με αυστηρούς κανόνες, υπενθυμίστε στους χρήστες καλές πρακτικές:

- Προτιμήστε **φράσεις-κωδικούς** αντί για μία μόνο λέξη.
- Αποφύγετε λέξεις λεξικού ή εύκολα προβλέψιμα μοτίβα.
- Μην χρησιμοποιείτε τον ίδιο κωδικό σε διαφορετικούς λογαριασμούς.
- Επιλέξτε **διαχειριστή κωδικών** για ασφαλή αποθήκευση.

4.4 Πίνακας Ανακεφαλαίωσης: Πολιτικές Κωδικών ανά Πλατφόρμα

Πολιτική	**Windows (Ομαδική Πολιτική)**	**Linux (PAM/login.defs)**
Ελάχιστο Μήκος	12 χαρακτήρες	PASS_MIN_LEN 12 / pam_pwquality minlen=12
Σύνθετος Κωδικός	Απαραίτητα κεφαλαία, πεζά και σύμβολα	pam_pwquality με ucredit/lcredit/dcredit/ocredit
Μέγιστη Διάρκεια	90 ημέρες	PASS_MAX_DAYS 90
Ιστορικό Κωδικών	Απομνημόνευση των 5 τελευταίων κωδικών	Διαχείριση μέσω PAM modules

Σημείο ελέγχου

Πριν συνεχίσετε:

- Έχετε ρυθμίσει τις πολιτικές κωδικών σε Windows ή Linux;
- Δοκιμάσατε την εφαρμογή αλλάζοντας κάποιον κωδικό;
- Κατανοείτε τη σημασία της λήξης και της πολυπλοκότητας των κωδικών;

5. Περιορισμός Διοικητικών Δικαιωμάτων

Δεν είναι απαραίτητο όλοι οι χρήστες να έχουν πλήρη πρόσβαση στο σύστημα. Η **αρχή της ελάχιστης προνομιακής πρόσβασης** σημαίνει ότι δίνουμε στους χρήστες μόνο τα δικαιώματα που χρειάζονται για τη δουλειά τους. Έτσι μειώνεται ο κίνδυνος για ακούσιες λανθασμένες ρυθμίσεις ή κακόβουλες ενέργειες.

5.1 Windows: Διαχείριση Τοπικών Χρηστών και Ομάδων

1. **Άνοιγμα Τοπικών Χρηστών και Ομάδων**
    - Πατήστε **το πλήκτρο Windows + R**
    - Πληκτρολογήστε:
    - lusrmgr.msc
    - Πατήστε **Enter**
2. **Ελέγξτε τα μέλη της ομάδας Διαχειριστών**
    - Στο αριστερό πάνελ, επιλέξτε **Ομάδες**
    - Κάντε διπλό κλικ στους **Διαχειριστές**
    - Ελέγξτε ποιοι λογαριασμοί εμφανίζονται στη λίστα
3. **Αφαιρέστε τους περιττούς διαχειριστές**
    - Επιλέξτε οποιονδήποτε χρήστη δεν πρέπει να έχει δικαιώματα διαχειριστή
    - Κάντε κλικ στο **Αφαίρεση**
4. **Επαλήθευση τυπικών χρηστών**
    - Βεβαιωθείτε ότι ο **λογαριασμός καθημερινής χρήσης** ανήκει μόνο στην ομάδα **Χρήστες** και όχι αλλού

Συμβουλή: Πάντα να έχετε έναν λογαριασμό έκτακτης ανάγκης ως διαχειριστή ενεργό, αλλά να μην τον χρησιμοποιείτε για καθημερινές εργασίες.

5.2Linux: Διαμόρφωση αρχείου sudoers

1. **Έλεγχος τρεχόντων χρηστών με δικαιώματα sudo**

```
# Εμφανίζει όλους τους χρήστες με προνόμια sudo
getent group sudo
```

2. **Αφαίρεση περιττών δικαιωμάτων sudo**

```
#Για να αφαιρέσετε έναν χρήστη από την
ομάδα sudo: sudo deluser username sudo
```

3. **Επεξεργασία αρχείου sudoers (εάν χρειάζεται)**

```
# Ανοίξτε με visudo (πιο ασφαλές από την
απευθείας επεξεργασία) sudo visudo
```

4. Βεβαιωθείτε ότι μόνο αξιόπιστοι λογαριασμοί έχουν δικαιώματα ALL=(ALL:ALL) ALL

Συμβουλή: Να διατηρείτε πάντα έναν λογαριασμό διαχειριστή — αλλά να χρησιμοποιείτε **ξεχωριστό απλό λογαριασμό** για καθημερινή εργασία.

5.3 Βέλτιστες Πρακτικές για τη Διαχείριση Δικαιωμάτων Πρόσβασης

Δημιουργήστε ξεχωριστούς **λογαριασμούς διαχειριστή και απλού χρήστη**.

Χρησιμοποιείτε **δικαιώματα διαχειριστή μόνο όταν είναι απαραίτητο**.

Ελέγχετε τακτικά τους λογαριασμούς διαχειριστή.

Απενεργοποιήστε ή διαγράψτε λογαριασμούς που δεν χρησιμοποιούνται.

Μην μοιράζεστε ποτέ λογαριασμούς διαχειριστή με άλλους χρήστες.

5.4 Ανακεφαλαίωση: Έλεγχος Πρόσβασης Διαχειριστή

Έλεγχος Δικαιωμάτων Διαχειριστή ανά Πλατφόρμα		**Περιορισμός Δικαιωμάτων Διαχειριστή**
Windows	lusrmgr.msc → Ομάδες → Διαχειριστές	Αφαιρέστε χρήστες που δεν χρειάζονται από την ομάδα Διαχειριστών
Linux	getent group sudo	sudo deluser username sudo / visudo

Σημείο Ελέγχου

Πριν συνεχίσετε:

- Ελέγξατε ποιοι έχουν δικαιώματα διαχειριστή/sudo;
- Αφαιρέσατε τους περιττούς λογαριασμούς διαχειριστή;
- Έχετε πλέον τουλάχιστον έναν απλό λογαριασμό για καθημερινή χρήση;

6. Ενεργοποίηση Καταγραφής και Παρακολούθησης

Τα αρχεία καταγραφής είναι το σύστημα έγκαιρης ειδοποίησής σας. Καταγράφουν δραστηριότητες του συστήματος, όπως συνδέσεις, σφάλματα και συμβάντα ασφαλείας, ώστε να εντοπίζετε επιθέσεις ή παραβιάσεις πολιτικής.

Σε αυτήν την ενότητα, θα ενεργοποιήσετε και θα ελέγξετε την καταγραφή τόσο στα **Windows** όσο και στα **Linux**.

6.1 Windows: Ρύθμιση του Event Viewer

1. **Άνοιγμα του Event Viewer**
    - Πατήστε **Windows key + R**
    - Πληκτρολογήστε:
    - eventvwr.msc
    - Πατήστε **Enter**
2. **Ελέγξτε τα αρχεία καταγραφής Ασφαλείας, Συστήματος και Εφαρμογών**
    - Ανοίξτε το αριστερό μενού και αναπτύξτε **Windows Logs**
    - Έλεγχος:
        - **Ασφάλεια** (απόπειρες σύνδεσης, χρήση δικαιωμάτων)
        - **Σύστημα** (προειδοποιήσεις/σφάλματα λειτουργικού)
        - **Εφαρμογές** (δραστηριότητα προγραμμάτων)
3. **Βεβαιωθείτε ότι η καταγραφή ασφαλείας είναι ενεργή**
    - Αν τα αρχεία καταγραφής ασφαλείας είναι κενά, ίσως δεν έχει ενεργοποιηθεί η παρακολούθηση.
    - Για να ενεργοποιήσετε την παρακολούθηση, ανοίξτε: gpedit.msc → Ρύθμιση Υπολογιστή → Ρυθμίσεις των Windows → Ρυθμίσεις Ασφαλείας → Εκτεταμένη Διαμόρφωση Πολιτικής Ελέγχου → Πολιτικές Ελέγχου

Συμβουλή: Δώστε προσοχή σε διαδοχικές αποτυχημένες προσπάθειες σύνδεσης — μπορεί να είναι ένδειξη επίθεσης με δοκιμή κωδικών.

6.2 Linux: Syslog και Auth.log

Τα συστήματα Linux συνήθως χρησιμοποιούν **rsyslog** ή **syslog-ng** για τη διαχείριση των αρχείων καταγραφής.

1. **Έλεγχος λειτουργίας του rsyslog**

2. sudo systemctl status rsyslog

    - Αν δεν είναι ενεργό, ξεκινήστε το: sudo systemctl start rsyslog
      sudo systemctl enable rsyslog

3. **Προβολή αρχείων καταγραφής ταυτοποίησης**

    - Εδώ καταγράφονται οι προσπάθειες σύνδεσης και οι ενέργειες με sudo:

    - sudo less /var/log/auth.log

4. **Προβολή Γενικών Καταγραφών Συστήματος**

    - Εδώ αποθηκεύονται τα γενικά συμβάντα του συστήματος:

    - sudo less /var/log/syslog

Συμβουλή: Χρησιμοποιήστε το grep για να αναζητήσετε στα αρχεία καταγραφής, π.χ.:

grep "Failed password" /var/log/auth.log

6.3 Γιατί Είναι Σημαντικά τα Αρχεία Καταγραφής

- **Ανίχνευση**: Αποτυχημένες προσπάθειες σύνδεσης ή προσπάθειες αύξησης δικαιωμάτων ξεχωρίζουν εύκολα.
- **Έρευνα περιστατικών**: Τα αρχεία καταγραφής προσφέρουν αποδείξεις μετά από κάποιο συμβάν.
- **Συμμόρφωση**: Πολλά πρότυπα (ISO 27001, PCI DSS) επιβάλλουν την καταγραφή συστήματος.

6.4 Πίνακας Ανασκόπησης: Βασικά Αρχεία Καταγραφής για Παρακολούθηση

Πλατφόρμα – Αρχεία Καταγραφής προς Έλεγχο	**Σκοπός**
Windows Ασφάλεια, Σύστημα, Εφαρμογές	Παρακολούθηση συνδέσεων, σφαλμάτων και ενεργειών εφαρμογών
Linux /var/log/auth.log	Συνδέσεις και δραστηριότητα sudo

Καταγραφή Πλατφόρμας προς Έλεγχο		Σκοπός
Linux	/var/log/syslog	Γενικά συμβάντα συστήματος

Σημείο ελέγχου

Πριν συνεχίσετε:

- Έχετε ενεργοποιήσει και ελέγξει τη λειτουργία καταγραφής στο VM σας;
- Μπορείτε να εντοπίσετε τις **προσπάθειες σύνδεσης** στα αρχεία καταγραφής σας;
- Καταλαβαίνετε γιατί τα logs είναι απαραίτητα για την ανίχνευση επιθέσεων;

7. Δοκιμασία Εργαστηρίου

Ήρθε η ώρα να συνδυάσεις όλα όσα έμαθες. Θα εφαρμόσεις πολιτικές για ισχυρούς κωδικούς, θα περιορίσεις τα δικαιώματα διαχειριστή, θα ενεργοποιήσεις την καταγραφή συμβάντων και θα αποθηκεύσεις το ενισχυμένο σύστημά σου ως ένα επαναχρησιμοποιήσιμο στιγμιότυπο.

7.1 Ενίσχυση της Εικονικής Μηχανής σου

Εφάρμοσε τις παρακάτω αλλαγές στην εικονική σου μηχανή:

- Εφάρμοσε αυστηρές **πολιτικές κωδικών πρόσβασης** (μήκος, πολυπλοκότητα, λήξη).
- Περιορισμός **διαχειριστικών δικαιωμάτων** ώστε μόνο αξιόπιστοι λογαριασμοί να έχουν αυξημένα προνόμια.
- Ενεργοποίησε και επιβεβαίωσε τη **καταγραφή και παρακολούθηση** (Event Viewer στα Windows, auth.log και syslog στα Linux).

7.2 Δημιουργία στιγμιότυπου του ενισχυμένου σας VM

Τα στιγμιότυπα σάς επιτρέπουν να αποθηκεύετε την τρέχουσα κατάσταση του VM. Αν γίνει κάποιο λάθος στη συνέχεια, μπορείτε εύκολα να επιστρέψετε στο ασφαλές σας σημείο αναφοράς.

Βήματα (παράδειγμα με VirtualBox):

1. Τερματίστε ή θέστε σε παύση το VM σας.
2. Στο VirtualBox, κάντε δεξί κλικ στο VM → **Λήψη στιγμιότυπου**.
3. Ονομάστε το: *Ενισχυμένη Βάση*
4. Προσθέστε μια περιγραφή (π.χ. «Εφαρμογή πολιτικών κωδικών, περιορισμοί διαχειριστή και ενεργοποιημένη καταγραφή»).

Στο VMware ή το Hyper-V, χρησιμοποιήστε τη λειτουργία **Snapshot/Checkpoint** για αποθήκευση.

7.3 Ερωτήσεις για προβληματισμό

Καταγράψτε τις απαντήσεις σας στο εργαστηριακό σας σημειωματάριο ή υποβάλετέ τες αν αυτό ζητηθεί:

1. Ποιους κανόνες για τους κωδικούς εφαρμόσατε και με ποιον τρόπο τους ελέγξατε;

2. Ποιοι λογαριασμοί έχουν δικαιώματα διαχειριστή ή sudo μετά τις αλλαγές σου;
3. Ποια αρχεία καταγραφής εξέτασες και ποια γεγονότα εντόπισες;
4. Πώς θα διευκόλυναν τα στιγμιότυπα τη διαχείριση της ασφάλειας σε πραγματικές συνθήκες;
5. Ποιο θα ήταν το **επόμενο βήμα για την ενίσχυση της ασφάλειας** αν αυτό το VM επρόκειτο να χρησιμοποιηθεί σε παραγωγικό περιβάλλον;

Η πρόκληση ολοκληρώθηκε!

Τώρα διαθέτετε ένα **ενισχυμένο στιγμιότυπο VM** — ένα ασφαλές και επαναχρησιμοποιήσιμο σημείο αναφοράς, στο οποίο μπορείτε να επιστρέψετε όποτε χρειαστεί. Αυτή η διαδικασία ακολουθείται από επαγγελματίες IT κατά τη δημιουργία «χρυσών εικόνων» για εταιρικές υλοποιήσεις.

8. Ανασκόπηση και Επόμενα Βήματα

8.1 Σημαντικά Σημεία

Σε αυτό το εργαστήριο, **θωρακίσατε με επιτυχία μια εικονική μηχανή** εφαρμόζοντας πρακτικές πολιτικές ασφαλείας. Συγκεκριμένα, πραγματοποιήσατε:

Διαμορφώσατε ένα ασφαλές περιβάλλον VM με χρήση VirtualBox, VMware ή Hyper-V.

Εφαρμόσατε **ισχυρούς κανόνες κωδικών πρόσβασης** για την προστασία των λογαριασμών.

Περιορίσατε **τα δικαιώματα διαχειριστή** μόνο σε αξιόπιστους χρήστες.

Ενεργοποιήσατε και επιβεβαιώσατε **την καταγραφή συμβάντων του συστήματος** για καλύτερη παρακολούθηση και έγκαιρη ανίχνευση επιθέσεων.

Δημιουργήσατε ένα **στιγμιότυπο της εικονικής μηχανής** — τη σταθερή σας βάση για τα επόμενα εργαστήρια.

8.2 Δεξιότητες που Αποκτήσατε

Ολοκληρώνοντας αυτό το εργαστήριο, πλέον μπορείτε:

- Να εξηγήσετε την αρχή του **ελάχιστου δικαιώματος** και να την εφαρμόσετε.
- Να διαμορφώσετε **πολιτικές κωδικών πρόσβασης** σε Windows και Linux.
- Να διαχειριστείτε **λογαριασμούς διαχειριστή και απλών χρηστών** αποτελεσματικά.
- Να χρησιμοποιείτε το **Event Viewer** (Windows) και το /var/log (Linux) για ασφάλεια και παρακολούθηση.
- Να δημιουργείτε και να τεκμηριώνετε **στιγμιότυπα** ώστε να διατηρείτε την ενισχυμένη ρύθμιση.

Αυτές είναι βασικές διαχειριστικές δεξιότητες που κάθε επαγγελματίας στον τομέα της κυβερνοασφάλειας οφείλει να κατέχει.

8.3 Επόμενο Θέμα: Βασικές Αρχές Ασφάλειας Δικτύων

Αφού θωρακίσατε το εικονικό σας μηχάνημα, το επόμενο βήμα είναι να διασφαλίσετε τις **συνδέσεις του με τον έξω κόσμο**.

Στην επόμενη ενότητα **Βασικές Αρχές Ασφάλειας Δικτύων**, θα ανακαλύψετε:

- Τι είναι τα βασικά πρωτόκολλα δικτύου και πώς μπορούν να τα εκμεταλλευτούν οι επιτιθέμενοι.
- Τι μέτρα προστασίας υπάρχουν, όπως τα firewalls, IDS/IPS και ο διαχωρισμός δικτύου.
- Διαδραστικά εργαστήρια όπου θα αναλύσετε κίνηση δικτύου και θα ασφαλίσετε την επικοινωνία σας.

Επόμενα Βήματα

- Αποθηκεύστε ή υποβάλετε τις απαντήσεις της εργαστηριακής σας ανασκόπησης.
- Διατηρήστε το **στιγμιότυπο Hardened VM** για χρήση σε μελλοντικά εργαστήρια.
- Ετοιμαστείτε για το **Network Security Fundamentals** module.

Έχεις δημιουργήσει μια ισχυρή και ασφαλή βάση στο επίπεδο του συστήματος. Επόμενο βήμα είναι να μάθεις πώς να διασφαλίζεις την προστασία του συστήματος όταν επικοινωνεί μέσω δικτύου.

9. Παράρτημα

9.1 Βασικές εντολές Linux

Εντολή	Σκοπός
sudo adduser όνομα_χρήστη	Δημιουργία νέου βασικού χρήστη
sudo deluser όνομα_χρήστη sudo	Αφαίρεση χρήστη από την ομάδα sudo (διαχειριστών)
sudo nano /etc/login.defs	Επεξεργασία προεπιλογών πολιτικής κωδικών πρόσβασης
sudo nano /etc/pam.d/common-password	Ρύθμιση πολύπλοκων κωδικών μέσω PAM
sudo visudo	Ασφαλής επεξεργασία του αρχείου sudoers
sudo systemctl status rsyslog	Έλεγχος αν η υπηρεσία καταγραφής λειτουργεί
sudo less /var/log/auth.log	Ανασκόπηση αρχείων σύνδεσης ταυτοποίησης
sudo less /var/log/syslog	Επισκόπηση γενικών αρχείων καταγραφής συστήματος
grep "Failed password" /var/log/auth.log	Αναζήτηση αποτυχημένων προσπαθειών σύνδεσης στα αρχεία καταγραφής

9.2 Γρήγορες διαδρομές πρόσβασης στα Windows

Εργασία	Διαδρομή / Εργαλείο
Άνοιγμα Επεξεργαστή Πολιτικής Ομάδας	gpedit.msc → Διαμόρφωση Υπολογιστή → Ρυθμίσεις των Windows → Ρυθμίσεις Ασφαλείας → Πολιτικές Λογαριασμού → Πολιτική Κωδικών
Διαχείριση Τοπικών Χρηστών και Ομάδων	lusrmgr.msc → Ομάδες → Διαχειριστές / Χρήστες
Προβολή Αρχείων Καταγραφής Ασφαλείας	eventvwr.msc → Αρχεία Καταγραφής των Windows → Ασφάλεια
Ενεργοποίηση Προηγμένων Πολιτικών Ελέγχου	gpedit.msc → Ρυθμίσεις Ασφαλείας → Διαμόρφωση Προηγμένων Πολιτικών Ελέγχου

9.3 Συμβουλές για Επίλυση Προβλημάτων

Πρόβλημα	Πιθανή Αιτία	Λύση
Η πολιτική κωδικού δεν εφαρμόζεται (Windows)	Λάθος εύρος πολιτικής / δεν έχει εφαρμοστεί ακόμα	Εκτελέστε gpupdate /force για να εφαρμοστεί η Ομαδική Πολιτική
Γίνονται δεκτοί ακόμα αδύναμοι κωδικοί (Linux)	Η διαμόρφωση της ενότητας PAM δεν έχει ρυθμιστεί σωστά	Επιβεβαιώστε ότι το αρχείο common-password περιλαμβάνει το pam_pwquality
Ο απλός χρήστης συνεχίζει να έχει πρόσβαση σε λειτουργίες διαχειριστή	Ο χρήστης παραμένει στην ομάδα Administrators ή sudo	Αφαιρέστε τον χρήστη με lusrmgr.msc (Windows) ή deluser (Linux)
Τα αρχεία καταγραφής είναι κενά (Windows)	Ο έλεγχος ασφάλειας δεν έχει ενεργοποιηθεί	Ρυθμίστε τις πολιτικές ελέγχου στον Επεξεργαστή Ομαδικής Πολιτικής
Δεν υπάρχει αρχείο auth.log στο Linux	Η υπηρεσία καταγραφής είναι απενεργοποιημένη	Ενεργοποιήστε το rsyslog: sudo systemctl enable --now rsyslog

9.4 Επιπλέον Πόροι

Τεκμηρίωση

- Microsoft Docs – Ρυθμίσεις Πολιτικής Κωδικών: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- Τεκμηρίωση Ασφαλείας Ubuntu: https://ubuntu.com/security
- Οδηγός PAM Password Quality Module: http://www.linux-pam.org/Linux-PAM-html/sag-pam_pwquality.html

Εργαλεία & Βέλτιστες Πρακτικές

- CIS Benchmarks (πρότυπα ασφάλειας για επιχειρήσεις): https://www.cisecurity.org/cis-benchmarks
- Οδηγίες Κωδικών NIST (SP 800-63): https://pages.nist.gov/800-63-3/sp800-63b.html