Εργαστήριο 1.1 – Ρύθμιση Τείχους Προστασίας

1. Επισκόπηση Εργαστηρίου

1.1 Περιγραφή Εργαστηρίου

Καλώς ήρθες στο πρώτο σου διαδραστικό εργαστήριο κυβερνοασφάλειας!

Σε αυτή την άσκηση θα μάθεις πώς να ενεργοποιείς και να ρυθμίζεις ένα βασικό τείχος προστασίας για να διασφαλίζεις το σύστημά σου από μη εξουσιοδοτημένη πρόσβαση. Είτε χρησιμοποιείς Windows είτε Linux, αυτό το εργαστήριο θα σε καθοδηγήσει στην ενεργοποίηση του firewall, στη διαμόρφωση κανόνων για να επιτρέπεις ή να απορρίπτεις συγκεκριμένη κίνηση, και στον έλεγχο της αποτελεσματικότητάς τους.

Μέχρι το τέλος του εργαστηρίου, θα έχετε κάνει το πρώτο βήμα για να ελέγχετε πώς εισέρχονται και εξέρχονται τα δεδομένα από το σύστημά σας—ένα θεμέλιο απαραίτητο για την άμυνα στον κυβερνοχώρο.

1.2 Εκπαιδευτικοί Στόχοι

Μετά την ολοκλήρωση αυτού του εργαστηρίου, θα μπορείτε να:

- Να κατανοείτε τον ρόλο και τη λειτουργία ενός τείχους προστασίας στην κυβερνοασφάλεια.
- Να ενεργοποιείτε και να διαχειρίζεστε τις ρυθμίσεις τείχους προστασίας σε Windows και Linux.
- Να δημιουργείτε κανόνες για να επιτρέπετε ή να μπλοκάρετε την κυκλοφορία δικτύου βάσει θυρών, διευθύνσεων IP ή υπηρεσιών.
- Να ελέγχετε την αποτελεσματικότητα του τείχους προστασίας με προσπάθειες SSH, ping και σάρωση με Nmap.
- Να αναγνωρίζετε τη σημασία των τειχών προστασίας τόσο σε προσωπικό όσο και σε επαγγελματικό περιβάλλον.

1.3 Προϋποθέσεις

Για να ολοκληρώσετε με επιτυχία αυτό το εργαστήριο, θα χρειαστείτε:

- Βασικές γνώσεις λειτουργικών συστημάτων υπολογιστών (Windows και/ή Linux).
- Πρόσβαση σε υπολογιστή με Windows ή σε εικονική μηχανή με Linux (συνιστάται Ubuntu).
- Δικαιώματα διαχειριστή στο σύστημα που χρησιμοποιείτε.
- Σύνδεση στο διαδίκτυο για να δοκιμάσετε την κίνηση δικτύου (ή δεύτερη συσκευή/εικονική μηχανή για δοκιμές SSH).
- Προαιρετικά: Εγκατάσταση του Nmap για δοκιμές σάρωσης θυρών.

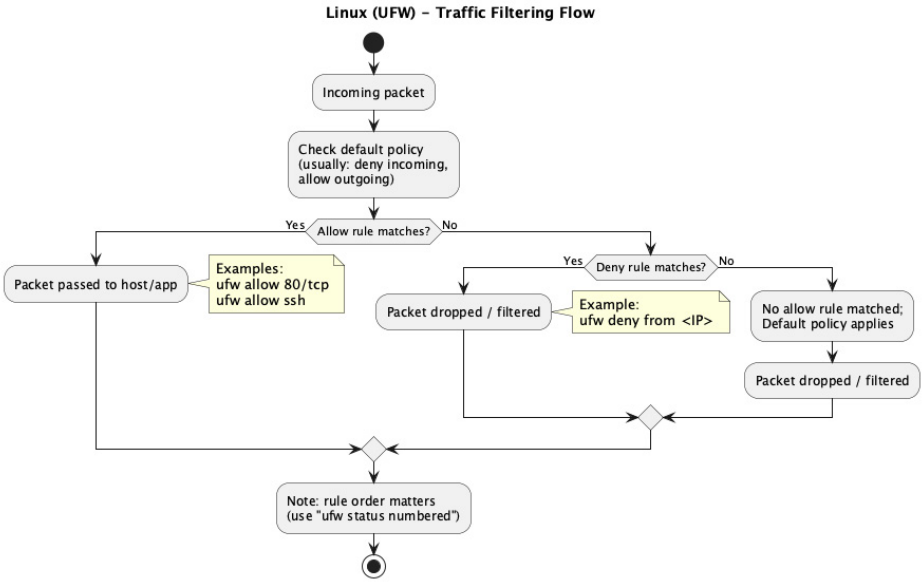
1.4 Εκτιμώμενος Χρόνος Ολοκλήρωσης

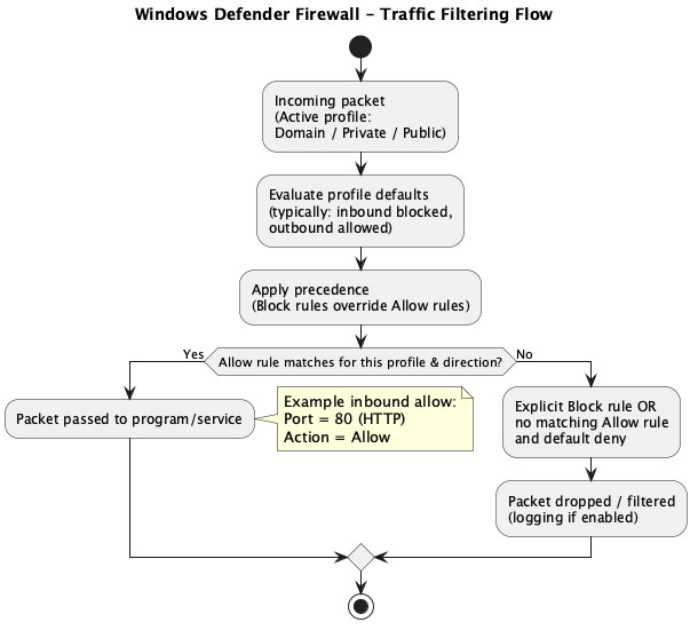
Δραστηριότητα	Εκτιμώμενη Διάρκεια
Μελέτη Οδηγιών & Εγκατάσταση Περιβάλλοντος	10 λεπτά
Ενεργοποίηση Τείχους Προστασίας (Windows ή/και Linux)	15 λεπτά
Ρύθμιση προσαρμοσμένων κανόνων (Εισερχόμενες/Εξερχόμενες, Θύρες, IP)	30 λεπτά
Έλεγχος της διαμόρφωσης (SSH, Ping, Nmap, Καταγραφές)	35 λεπτά
Σε βάθος: Προχωρημένες δυνατότητες του Windows Firewall (Προαιρετικό)	25 λεπτά
Ανάλυση πραγματικών σεναρίων: Χρήσεις και πιθανοί κίνδυνοι	25 λεπτά
Διαδραστική δοκιμασία: Επίτρεψε HTTP, απαγόρευσε τα υπόλοιπα	30 λεπτά
Καταγραφή και σύνταξη της αναφοράς διαμόρφωσης του τείχους προστασίας	10 λεπτά
Συνολικός εκτιμώμενος χρόνος	**3 ώρες**

2. Ξεκινώντας

2.1 Τι είναι το Firewall;

Ένα **firewall** είναι ένα σύστημα που επιβλέπει και διαχειρίζεται την εισερχόμενη και εξερχόμενη κίνηση δικτύου, σύμφωνα με προκαθορισμένους κανόνες. Λειτουργεί ως φραγμός ανάμεσα στο αξιόπιστο εσωτερικό σας δίκτυο και στο δυνητικά επικίνδυνο εξωτερικό δίκτυο (όπως το διαδίκτυο).





Υπάρχουν δύο βασικές κατηγορίες:

- **Προσωποποιημένα firewalls** (η έμφαση σε αυτό το εργαστήριο): Εγκαθίστανται σε μεμονωμένους υπολογιστές (όπως το laptop ή τον server σας).
- **Δικτυακά firewalls**: Τοποθετούνται σε επίπεδο δικτύου για να ελέγχουν την κίνηση μεταξύ πολλών συσκευών.

Γιατί έχει σημασία:

Τα firewalls αποτελούν από τα βασικά μέτρα προστασίας σε κάθε ασφαλές σύστημα—χρησιμοποιούνται από επιχειρήσεις, κυβερνήσεις και ιδιώτες για να αποτρέπουν επιθέσεις.

Γνωρίζατε ότι...

Τα περισσότερα λειτουργικά συστήματα διαθέτουν ενσωματωμένο τείχος προστασίας, το οποίο συνήθως είναι απενεργοποιημένο ή ρυθμισμένο ελάχιστα. Σε αυτό το εργαστήριο θα μάθετε πώς να το διαχειρίζεστε αποτελεσματικά.

Πριν ξεκινήσετε, βεβαιωθείτε ότι έχετε τα εξής έτοιμα:

Έναν λειτουργικό υπολογιστή με μία από τις εξής επιλογές:

- **Windows 10/11** με δικαιώματα διαχειριστή
- **Ubuntu Linux (22.04 ή νεότερο)** σε φυσικό ή εικονικό περιβάλλον

Πρόσβαση σε τερματικό (Linux) ή δικαιώματα διαχειριστή στο γραφικό περιβάλλον (Windows), σύνδεση στο διαδίκτυο για δοκιμές και εγκατάσταση εργαλείων, δυνατότητα εγκατάστασης λογισμικού (π.χ. Nmap, OpenSSH αν χρειαστεί) (Προαιρετικά) Δεύτερη συσκευή ή εικονική μηχανή για προσομοίωση εξωτερικής πρόσβασης SSH

2.3 Σημειώσεις για Χρήστες Windows και Linux

Αυτό το εργαστήριο υποστηρίζει **τόσο Windows όσο και Linux** χρήστες. Μπορείτε να ακολουθήσετε και τις δύο διαδρομές ή να επιλέξετε εκείνη που ταιριάζει στο σύστημά σας.

Συνιστούμε να ολοκληρώσετε και τις δύο για πιο ολοκληρωμένη κατανόηση.

Ενέργεια	**Linux (UFW)**	**Windows**
Ενεργοποίηση τείχους προστασίας	sudo ufw enable	Ανοίξτε **Ασφάλεια των Windows → Τείχος προστασίας & Δίκτυο**
Δημιουργία κανόνων	Εντολές ufw allow / ufw deny	Χρησιμοποιήστε **Προηγμένες Ρυθμίσεις Τείχους Προστασίας** στο γραφικό περιβάλλον
Έλεγχος λειτουργίας τείχους προστασίας	SSH, ping, Nmap	Ping, σάρωση θυρών, έλεγχος αποκλεισμένων εφαρμογών
Ορατότητα κανόνων	ufw status verbose	Λίστα κανόνων στο Windows Defender Firewall (GUI)

Συμβουλή: Αν δεν είστε σίγουροι ποιο λειτουργικό να επιλέξετε, ξεκινήστε με το **Linux UFW** και συγκρίνετέ το με τα Windows για πιο ολοκληρωμένη εμπειρία.

3. Βήμα 1 – Ενεργοποίηση του Τείχους Προστασίας

Σε αυτή την ενότητα, θα ενεργοποιήσετε το προεπιλεγμένο τείχος προστασίας του υπολογιστή σας.

Θα μάθετε:

- Πώς να ενεργοποιήσετε το UFW (Uncomplicated Firewall) σε Linux.
- Πώς να ελέγξετε και να ενεργοποιήσετε το τείχος προστασίας μέσα από το Κέντρο Ασφαλείας των Windows.
- Πώς να επιβεβαιώσετε ότι το τείχος προστασίας προστατεύει πλέον το σύστημά σας.

3.1 Ενεργοποίηση Τείχους Προστασίας στα Windows

Βήμα-προς-Βήμα (Windows 10/11):

1. **Άνοιγμα του Κέντρου Ασφαλείας των Windows**
    - Κάντε κλικ στο **Μενού Έναρξης** ή πατήστε το **πλήκτρο Windows**
    - Πληκτρολογήστε: Windows Security
    - Πατήστε **Enter** ή επιλέξτε το πρώτο αποτέλεσμα
2. **Μεταβείτε στις Ρυθμίσεις Τείχους Προστασίας**
    - Στο αριστερό μενού, κάντε κλικ στο **«Τείχος προστασίας & Προστασία δικτύου»**
3. **Ελέγξτε την Κατάσταση για το Ενεργό Δίκτυο**
    - Στην **ενεργή σύνδεση δικτύου** (συνήθως Ιδιωτικό ή Τομέα), εντοπίστε το πράσινο σημάδι ελέγχου και την ένδειξη **«Το Τείχος προστασίας είναι ενεργό»**
    - Αν είναι **Ανενεργό**, κάντε κλικ και ενεργοποιήστε το τείχος προστασίας **Ενεργό**
4. **Επιβεβαίωση επιτυχίας**
    - Όταν το τείχος προστασίας είναι ενεργό, τα Windows εμφανίζουν ένα πράσινο σημάδι ελέγχου
    - Πλέον το σύστημά σας προστατεύεται με βασικό φιλτράρισμα από τοπικό τείχος προστασίας

Συμβουλή: Ορισμένα προγράμματα προστασίας από ιούς τρίτων μπορεί να απενεργοποιούν το Τείχος προστασίας των Windows. Αν δεν βλέπετε την επιλογή, ελέγξτε τις ρυθμίσεις του antivirus σας.

3.2 Ενεργοποίηση του Τείχους Προστασίας σε Linux (UFW)

Βήμα-προς-βήμα (συστήματα βασισμένα σε Ubuntu/Debian):

Οι οδηγίες αυτές προϋποθέτουν ότι χρησιμοποιείτε Ubuntu 22.04 LTS ή παρόμοια έκδοση.

1. **Ανοίξτε το Τερματικό**
    - Μπορείτε να χρησιμοποιήσετε **Ctrl + Alt + T** για να ανοίξετε το τερματικό
2. **Έλεγχος κατάστασης UFW (προαιρετικό)**
3. sudo ufw status
    - Αν το UFW είναι **ανενεργό**, συνεχίστε με την ενεργοποίησή του
    - Αν το UFW είναι **ενεργό**, μεταβείτε στην επόμενη ενότητα
4. **Ενεργοποίηση του Τείχους Προστασίας**
5. sudo ufw enable
    - Πληκτρολογήστε τον **κωδικό χρήστη** όταν σας ζητηθεί
    - Το UFW θα εμφανίσει: Το τείχος προστασίας είναι ενεργό και θα ξεκινά αυτόματα με το σύστημα
6. **Επιβεβαίωση κατάστασης**
7. sudo ufw status verbose
    - Εδώ θα δείτε αναλυτικά τους τρέχοντες κανόνες και την κατάστασή τους

Συμβουλή: Το UFW σημαίνει «Uncomplicated Firewall» — έχει σχεδιαστεί ώστε να είναι απλό και φιλικό για αρχάριους, διευκολύνοντας τη χρήση του μέσω γραμμής εντολών.

3.3 Σύντομη Ανασκόπηση: Ρυθμίσεις Windows & Linux

Λειτουργικό Σύστημα	Βήματα Ενεργοποίησης Τείχους Προστασίας
Windows	Έναρξη → Αναζήτηση για Ασφάλεια των Windows → Τείχος προστασίας & Προστασία δικτύου → Ενεργοποίηση
Linux	Άνοιγμα Τερματικού → sudo ufw enable → Έλεγχος με sudo ufw status verbose

Σημείο Ελέγχου

Πριν προχωρήσετε:

- Έχετε ενεργοποιήσει το τείχος προστασίας σας; **Μπορείτε να δείτε την έξοδο κατάστασης** που να επιβεβαιώνει ότι το τείχος προστασίας λειτουργεί;
- Είστε έτοιμοι να αρχίσετε να ορίζετε κανόνες;

4. Βήμα 2 – Διαμόρφωση Κανόνων Τείχους Προστασίας

Όταν το τείχος προστασίας ενεργοποιηθεί, παραμένει ουσιαστικά ανενεργό μέχρι να προσθέσετε κανόνες για να επιτρέπετε ή να μπλοκάρετε συγκεκριμένη δικτυακή κίνηση.

Σε αυτήν την ενότητα θα δείτε:

- Πώς να επιτρέπετε πρόσβαση σε βασικές υπηρεσίες (όπως SSH ή HTTP).
- Πώς να αποτρέπετε ανεπιθύμητες συνδέσεις (π.χ. από συγκεκριμένες IP διευθύνσεις).
- Πώς να χρησιμοποιείτε τόσο εργαλεία γραμμής εντολών (Linux) όσο και γραφικά εργαλεία (Windows).

4.1 Linux – Διαχείριση Κανόνων με UFW

Παράδειγμα 1: Ενεργοποίηση Πρόσβασης SSH

Επιτρέψτε εισερχόμενες συνδέσεις στη θύρα 22 (προεπιλογή για SSH):

```
sudo ufw allow ssh
```

Αυτό επιτρέπει την απομακρυσμένη σύνδεση μέσω SSH.

Παράδειγμα 2: Ενεργοποίηση Κίνησης Ιστοσελίδας (HTTP)

Αποδεχθείτε την κίνηση του web server στη θύρα 80:

```
sudo ufw allow 80/tcp
```

Αυτή η ενέργεια είναι συχνή για φιλοξενία ή πρόσβαση σε ιστοσελίδες.

Παράδειγμα 3: Αποκλεισμός Συγκεκριμένης Διεύθυνσης IP

Αποκλείστε εισερχόμενες συνδέσεις από ύποπτες ή κακόβουλες διευθύνσεις IP:

```
sudo ufw deny from 192.168.1.100
```

Αντικαταστήστε με οποιαδήποτε διεύθυνση IP θέλετε να μπλοκάρετε.

Παράδειγμα 4: Έλεγχος όλων των ενεργών κανόνων

Δείτε τους ενεργούς κανόνες και τη διαμόρφωση του firewall:

```
sudo ufw status numbered
```

ή για περισσότερες λεπτομέρειες:

```
sudo ufw status verbose
```

Σημείωση: Οι κανόνες εφαρμόζονται με τη σειρά που εμφανίζονται. Μπορείτε αργότερα να διαγράψετε ή να τροποποιήσετε συγκεκριμένους κανόνες χρησιμοποιώντας τον αριθμό τους.

4.2 Windows – Δημιουργία κανόνων με το Προχωρημένο Τείχος Προστασίας

Βήμα 1: Άνοιγμα Ρυθμίσεων για Προχωρημένους του Τείχους Προστασίας

1. Ανοίξτε **το μενού Έναρξης**
2. Αναζήτηση: Windows Defender Firewall με Προηγμένη Ασφάλεια
3. Πατήστε για να εμφανίσετε τον πίνακα ρυθμίσεων για προχωρημένους

Βήμα 2: Δημιουργία Νέου Κανόνα Εισερχόμενης Κίνησης

1. Στο αριστερό μενού, επιλέξτε **Κανόνες Εισερχόμενης Κίνησης**
2. Στα δεξιά, κάντε κλικ στο **Νέος Κανόνας...**
3. Επιλέξτε **Θύρα**, μετά πατήστε **Επόμενο**
4. Εισάγετε μια θύρα (π.χ. 80), επιλέξτε **Να επιτρέπεται** ή **Να αποκλείεται**
5. Εφαρμόστε στον κατάλληλο τύπο προφίλ (Τομέας, Ιδιωτικό, Δημόσιο)
6. Ονομάστε τον κανόνα σας (π.χ. “Να επιτρέπεται το HTTP”) και ολοκληρώστε

Βήμα 3: Εναλλακτικοί Τύποι Κανόνων

Μπορείτε ακόμη να:

- Να επιτρέπετε ή να αποκλείετε συγκεκριμένα προγράμματα
- Να φιλτράρετε βάσει διευθύνσεων IP
- Να επιλέγετε μεταξύ TCP ή UDP
- Να ορίζετε συνθήκες με βάση την ταυτοποίηση ή τις υπηρεσίες

Συμβουλή: Μπορείτε να αντιγράψετε και να επεξεργαστείτε υπάρχοντες κανόνες για να δημιουργήσετε γρήγορα προσαρμοσμένες παραλλαγές.

4.3 Σύντομη Ανασκόπηση: Περίληψη Κανόνων Ασφαλείας

Πλατφόρμα	Ενέργεια	Εντολή / Βήματα
Linux (UFW)	Επιτρέψτε SSH	`sudo ufw allow ssh`
Linux (UFW)	Επιτρέψτε HTTP	`sudo ufw allow 80/tcp`
Linux (UFW)	Αποκλεισμός διεύθυνσης IP	`sudo ufw deny from 192.168.1.100`
Linux (UFW)	Έλεγχος κανόνων	`sudo ufw status verbose`
Windows	Άνοιγμα προχωρημένων ρυθμίσεων	Έναρξη → Αναζήτηση Windows Defender Firewall με προχωρημένη ασφάλεια
Windows	Άνοιγμα θύρας (π.χ. HTTP)	Εισερχόμενοι κανόνες → Νέος κανόνας → Θύρα → 80 → Επίτρεψη
Windows	Αποκλεισμός συγκεκριμένης εφαρμογής ή διεύθυνσης IP	Νέος κανόνας → Πρόγραμμα / Προσαρμοσμένο → Αποκλεισμός

Σημείο ελέγχου

Πριν συνεχίσετε:

- Έχετε δημιουργήσει τουλάχιστον δύο κανόνες (έναν **επιτρεπτικό** και έναν **αποκλεισμού**);
- Δοκιμάσατε να δημιουργήσετε κανόνες και στις **δύο πλατφόρμες**, αν ισχύει;
- Γνωρίζετε πώς να **δείτε και να διαχειριστείτε** τους υπάρχοντες κανόνες;

5. Βήμα 3 – Δοκιμή του Τείχους Προστασίας σας

Η δημιουργία κανόνων για το τείχος προστασίας είναι μόνο η μισή δουλειά — πρέπει επίσης να **δοκιμάσετε** ότι λειτουργούν όπως πρέπει.

Σε αυτή την ενότητα θα:

- Δοκιμάσετε σύνδεση μέσω SSH και δείτε πώς αντιδρά το τείχος προστασίας.
- Χρησιμοποιήσετε ping για να ελέγξετε τη βασική πρόσβαση στο δίκτυο.
- Εκτελέσετε μια **Nmap** σάρωση για να δείτε ποια ports είναι ορατά από το εξωτερικό.

Σημείωση: Ίσως χρειαστεί να χρησιμοποιήσετε μια δεύτερη συσκευή ή εικονική μηχανή για να προσομοιώσετε εξωτερική πρόσβαση. Η δοκιμή είναι πιο αποτελεσματική όταν το ένα σύστημα προστατεύεται από το τείχος προστασίας και το άλλο λειτουργεί ως "εξωτερικός πελάτης" ή "επιτιθέμενος".

5.1 Δοκιμή Αποκλεισμού SSH

Στόχος:

Ελέγξτε αν η πρόσβαση SSH περιορίζεται ή επιτρέπεται από τους κανόνες του firewall σας.

Βήματα:

1. Στον **δεύτερο υπολογιστή**, ανοίξτε ένα τερματικό ή έναν SSH client.
2. Δοκιμάστε να συνδεθείτε με:

```
ssh το-όνομα-χρήστη@η-ip-του-server-σας
```

3. Αν το SSH είναι **μπλοκαρισμένο**, θα δείτε:
    - Η σύνδεση απορρίφθηκε
    - Λήξη χρονικού ορίου
    - Δεν υπάρχει διαδρομή προς τον υπολογιστή
4. Αν η πρόσβαση SSH είναι **επιτρεπτή**, θα σας ζητηθεί ο κωδικός πρόσβασής σας και θα μπορέσετε να συνδεθείτε.

Συμβουλή: Σε Linux, μπλοκάρετε το SSH με την εντολή sudo ufw deny ssh και προσπαθήστε να συνδεθείτε ξανά.

5.2 Δοκιμή Ping (Επιτευξιμότητα ICMP)

Σκοπός:

Επαληθεύστε αν το σύστημά σας ανταποκρίνεται σε βασικά **αιτήματα ICMP echo** (ping).

Βήματα:

1. Σε άλλο υπολογιστή, ανοίξτε το τερματικό.
2. Εκτελέστε:

```
ping your-server-ip
```

3. Παρατηρήστε το αποτέλεσμα:
    - Απαντήσεις = Το ICMP είναι **επιτρεπτό**
    - Λήξη χρονικού ορίου αιτήματος = Το ICMP είναι **μπλοκαρισμένο**

Σημείωση: Ορισμένα συστήματα μπλοκάρουν το ICMP από προεπιλογή· αυτή η ρύθμιση μπορεί να τροποποιηθεί μέσω προχωρημένων επιλογών τείχους προστασίας.

5.3 Έλεγχος θυρών με το Nmap

Σκοπός:

Χρησιμοποιήστε **Nmap** για να εντοπίσετε ανοιχτές θύρες και να δείτε ποιες υπηρεσίες είναι προσβάσιμες.

Βήματα:

1. Στο δεύτερο σύστημα (ή από υπολογιστή σάρωσης), εγκαταστήστε το Nmap εάν δεν υπάρχει ήδη:

```
sudo apt install nmap        # Σε διανομές Debian/Ubuntu
brew install nmap            # Σε macOS
```

2. Σάρωση του προστατευμένου συστήματος:

```
nmap η-ip-του-server-σας
```

3. Ελέγξτε τα αποτελέσματα:
    - Επιτρεπόμενες θύρες (π.χ. 22, 80) θα εμφανίζονται ως **ανοιχτές**
    - Οι μπλοκαρισμένες θύρες δεν θα εμφανίζονται ή θα φαίνονται ως **φιλτραρισμένες**
4. Για περισσότερες πληροφορίες:

```
nmap -v η διεύθυνση IP του διακομιστή σας
```

Συμβουλή Ασφαλείας: Οι επιτιθέμενοι χρησιμοποιούν εργαλεία όπως το Nmap. Εξασκηθείτε να ελέγχετε τα δικά σας συστήματα για να προστατευτείτε από σάρωση και ανίχνευση.

Πίνακας Ανασκόπησης 5.4 – Μέθοδοι Ελέγχου Τείχους Προστασίας

Δοκιμή	Εντολή ή Ενέργεια	Αναμενόμενο Αποτέλεσμα αν ο Κανόνας Ισχύει
Δοκιμή Αποκλεισμού SSH	`ssh user@ip`	Η σύνδεση απορρίφθηκε / έληξε ο χρόνος
Δοκιμή Ping	`ping στη διεύθυνση του διακομιστή σας`	Απαντήσεις (επιτρέπεται) ή λήξη χρόνου (αποκλεισμένο)
Σάρωση θυρών με Nmap	`nmap στη διεύθυνση του διακομιστή σας`	Εμφανίζονται μόνο οι επιτρεπόμενες θύρες (π.χ. 22, 80)
Αναλυτική σάρωση με Nmap	`nmap -v η διεύθυνση IP του διακομιστή σας`	Λεπτομερής λίστα με φιλτραρισμένες/μπλοκαρισμένες υπηρεσίες

Σημείο Ελέγχου

Επιβεβαίωσε πριν συνεχίσεις:

- Έκανες δοκιμή σε **τουλάχιστον μία μπλοκαρισμένη και μία επιτρεπόμενη θύρα**;
- Κατάφερες να επαληθεύσεις τη λειτουργία του τείχους προστασίας με **ping ή SSH**;
- Δοκίμασες **σάρωση θυρών** με το Nmap;

6. Σημασία στην Πραγματική Ζωή

Η ρύθμιση ενός firewall ίσως φαίνεται απλή υπόθεση, όμως αποτελεί ένα από τα πιο **κομβικά βήματα για την προστασία συστημάτων στην πράξη** — από φορητούς υπολογιστές μέχρι μεγάλα εταιρικά data centers.

Σε αυτή την ενότητα θα ανακαλύψετε:

- Γιατί τα firewalls έχουν αξία στον πραγματικό κόσμο.
- Πώς οι επιθέσεις αποτρέπονται με σωστά ρυθμισμένους κανόνες.
- Πού εφαρμόζονται τα firewalls, στο σπίτι και στην εργασία.

6.1 Γιατί τα Firewalls είναι Απαραίτητα στην Κυβερνοασφάλεια

Τα firewalls δεν είναι προαιρετικά. Αποτελούν **απαραίτητα εργαλεία άμυνας** που χρησιμοποιούνται σχεδόν σε κάθε ασφαλές σύστημα σήμερα.

Τα firewalls προστατεύουν τα συστήματα ως εξής:

- Αποκλείουν μη εξουσιοδοτημένες σαρώσεις και προσπάθειες σύνδεσης.
- Αποτρέπουν την πρόσβαση σε ευάλωτες υπηρεσίες.
- Φιλτράρουν κακόβουλη κίνηση **πριν** φτάσει στο σύστημα.

6.2 Firewalls στην Πράξη – Παραδείγματα Χρήσης

Οικιακός Χρήστης:

- Ο οικιακός σου δρομολογητής διαθέτει ενσωματωμένο firewall που αθόρυβα μπλοκάρει το μεγαλύτερο μέρος της εισερχόμενης διαδικτυακής κίνησης.
- Έτσι, οι συσκευές σου (laptop, τηλεόραση, κινητό) προστατεύονται αποτελεσματικά από άμεσες επιθέσεις.

Εταιρικά Συστήματα:

- Μεγάλες επιχειρήσεις χρησιμοποιούν **πολλαπλά επίπεδα firewall** για να χωρίσουν τα εσωτερικά τους δίκτυα και να ελέγχουν την πρόσβαση σε βάσεις δεδομένων, εφαρμογές και συσκευές εργαζομένων.
- Αυτά τα firewall παρακολουθούνται στενά και ενημερώνονται διαρκώς.

Προσωπικές Συσκευές:

- Τα firewalls σε φορητούς υπολογιστές ή σταθμούς εργασίας εμποδίζουν επικίνδυνες εφαρμογές, αποτρέπουν κρυφές προσβάσεις και απομονώνουν κακόβουλο λογισμικό.

6.3 Οπτική Σύνοψη – Το Firewall ως Ασπίδα

Η λειτουργία του firewall σε 3 απλά βήματα:

1. **Ελέγξτε** όλη την εισερχόμενη και εξερχόμενη κίνηση.
2. **Συσχετίστε** την κίνηση με τους κανόνες που έχουν ρυθμιστεί.
3. **Επιτρέψτε ή αποκλείστε** ανάλογα με την πολιτική ασφαλείας.

Σημείο Ελέγχου

Σκεφτείτε το σύστημά σας:

- Ποιες υπηρεσίες θέλετε να είναι **διαθέσιμες** στο διαδίκτυο;
- Ποιες υπηρεσίες πρέπει πάντα να είναι **αποκλεισμένες**;
- Με ποιον τρόπο θα μπορούσε ένα λάθος στη ρύθμιση του τείχους προστασίας να εκθέσει το σύστημά σας;

7. Εργαστηριακή Πρόκληση

7.1 Σενάριο: Επιτρέψτε HTTP, Αποκλείστε Όλα τα Υπόλοιπα

Η Αποστολή σας:

Ρυθμίστε το σύστημά σας ώστε **μόνο η κυκλοφορία HTTP (θύρα 80)** να επιτρέπεται — όλη η άλλη εισερχόμενη κίνηση πρέπει να μπλοκάρεται.

Αυτό προσομοιώνει ένα απλό σενάριο web server, όπου θέλετε οι χρήστες να έχουν πρόσβαση στην ιστοσελίδα σας αλλά να μπλοκάρεται κάθε άλλη πρόσβαση (SSH, ping κ.λπ.).

Οδηγίες για Linux (UFW)

1. **Ορίστε την προεπιλεγμένη πολιτική ώστε να μπλοκάρεται όλη η εισερχόμενη κίνηση:**

```
sudo ufw default deny incoming
```

2. **Επιτρέψτε μόνο την κίνηση HTTP (θύρα 80):**

```
sudo ufw allow 80/tcp
```

3. **(Προαιρετικό) Απορρίψτε όλα τα άλλα services ξεχωριστά:**

```
sudo ufw deny ssh
```

4. **Ελέγξτε τους κανόνες σας:**

```
sudo ufw status verbose
```

Οδηγίες για Windows

1. **Ανοίξτε τις προηγμένες ρυθμίσεις του Firewall**
2. **Δημιουργήστε νέο κανόνα εισερχόμενης κίνησης:**
    - Τύπος: **Θύρα**
    - Θύρα: 80
    - Ενέργεια: **Επιτρέπεται**
    - Όνομα: Επιτρέπεται HTTP
3. **Αποκλείστε όλη την υπόλοιπη εισερχόμενη κίνηση (προαιρετικό):**

- Μεταβείτε στις **Εισερχόμενοι Κανόνες** → Επιλέξτε **Νέος Κανόνας**
- Τύπος: **Όλα τα Προγράμματα**
- Ενέργεια: **Αποκλεισμός**
- Εύρος: Εφαρμόστε σε όλες τις θύρες ή συγκεκριμένες, όπως η 22 για SSH

4. **Αναπροσαρμόστε ή διορθώστε τυχόν αντικρουόμενους κανόνες αν χρειάζεται**

7.2 Λίστα Ελέγχου – Τα Καταφέρατε;

Ενέργεια	**Ολοκληρώθηκε;**
Ορίστε προεπιλεγμένη απόρριψη για εισερχόμενη κίνηση	[ ]
Επιτρέπεται μόνο HTTP (θύρα 80)	[ ]
Έγινε επαλήθευση κατάστασης/εξόδου κανόνα	[ ]
Επιβεβαιώθηκε ότι το SSH ή το ping είναι μπλοκαρισμένο	[ ]
Επιβεβαιώθηκε ότι η θύρα 80 είναι ανοικτή (μέσω Nmap)	[ ]

7.3 Προαιρετικές Δοκιμές

Δοκιμάστε να συνδεθείτε στο σύστημά σας από άλλη συσκευή ή εικονική μηχανή:

- Μεταβείτε στη διεύθυνση http://your-server-ip → Αν τρέχει web υπηρεσία, θα πρέπει να φορτώσει
- Δοκιμάστε SSH ή Nmap → Θα πρέπει να μπλοκάρονται

Δεν έχετε web server; Δοκιμάστε:

sudo apt install apache2 sudo

systemctl start apache2

7.4 Ερωτήσεις Αναστοχασμού

Απαντήστε σε αυτές στο εργαστηριακό σας τετράδιο ή υποβάλετέ τες στην αναφορά σας:

1. Ποια εντολή ή βήματα ακολουθήσατε για να ρυθμίσετε το firewall σας;

2. Πώς διασφάλισες ότι όλη η μη HTTP κίνηση έχει μπλοκαριστεί;
3. Υπήρχαν υπηρεσίες που παρέμειναν προσβάσιμες χωρίς να το θέλεις;
4. Τι επιπτώσεις θα μπορούσε να έχει αν κατά λάθος άφηνες ανοιχτή μια ευάλωτη θύρα;

Η πρόκληση ολοκληρώθηκε!

Προσομοιώσατε το προφίλ firewall ενός **διαδικτυακού διακομιστή με δημόσια πρόσβαση** — ένα από τα πιο συνηθισμένα σενάρια στις επιχειρήσεις κυβερνοασφάλειας.

8. Ανασκόπηση και Επόμενα Βήματα

8.1 Κύρια Συμπεράσματα

Συγχαρητήρια — ολοκλήρωσες το πρώτο σου εργαστήριο κυβερνοασφάλειας!

Αυτά κατάφερες σε αυτή τη συνεδρία:

Ενεργοποίησες ένα τοπικό τείχος προστασίας τόσο σε Linux (UFW) όσο και σε Windows.

Δημιούργησες κανόνες εισερχόμενης και εξερχόμενης κίνησης για να επιτρέπεις ή να αποκλείεις δεδομένα.

Δοκιμάσατε τους κανόνες χρησιμοποιώντας εργαλεία όπως SSH, ping και Nmap.

Εξερευνήσατε πρακτικές εφαρμογές των firewalls σε οικιακά και εταιρικά δίκτυα.

Ρυθμίσατε ένα περιορισμένο προφίλ firewall για να προσομοιώσετε έναν web server στη δοκιμασία.

Γιατί αυτό έχει σημασία:

Κάθε ασφαλές σύστημα, από το προσωπικό σας laptop έως τις υποδομές cloud παγκοσμίως, βασίζεται σε σωστά ρυθμισμένα firewalls. Κάνατε ένα επαγγελματικό βήμα προς την κατανόηση και τον έλεγχο της ψηφιακής ασφάλειας.

8.2 Δεξιότητες που αποκτήσατε

Με την ολοκλήρωση αυτού του εργαστηρίου, απέκτησες πρακτική εμπειρία σε:

- Ρυθμίσεις ασφαλείας σε επίπεδο λειτουργικού συστήματος.
- Εργαλεία δικτύωσης μέσω γραμμής εντολών (ufw, ping, ssh, nmap).
- Αμυντική σκέψη: περιορισμός της επιφάνειας επίθεσης μέσω ελεγχόμενης πρόσβασης.
- Διαχείριση firewall μέσω γραφικού περιβάλλοντος και ορισμός κανόνων (Προηγμένο Firewall των Windows).

Αυτές οι δεξιότητες θα σου φανούν χρήσιμες σε όλη τη διαδρομή σου στην κυβερνοασφάλεια — σε εργαστήρια, διαγωνισμούς ή στο χώρο εργασίας.

8.3 Επόμενο βήμα: Εργαστήριο Ανίχνευσης Κακόβουλου Λογισμικού

Τώρα θα αλλάξουμε κατεύθυνση και θα δούμε **πώς εντοπίζουμε και απομακρύνουμε κακόβουλο λογισμικό** από ένα σύστημα με τη βοήθεια εργαλείων antivirus.

Στο **Εργαστήριο 1.2 – Ανίχνευση Κακόβουλου Λογισμικού**, θα μπορέσεις να:

- Εκτελέστε έναν έλεγχο με ενσωματωμένα ή ανοιχτού κώδικα εργαλεία.
- Παρατηρήστε πώς λειτουργεί και καλύπτεται το κακόβουλο λογισμικό.
- Δείτε πώς γίνεται στην πράξη ο εντοπισμός και η αντιμετώπιση απειλών.

Συμβουλή προετοιμασίας: Φροντίστε να έχετε έτοιμο ένα πρόγραμμα ανίχνευσης κακόβουλου λογισμικού (Windows Defender, ClamAV κ.ά.) και να πραγματοποιήσετε τόσο γρήγορους όσο και πλήρεις ελέγχους σε δοκιμαστικά αρχεία.

Επόμενα βήματα

- Απάντησε στις **ερωτήσεις αναστοχασμού** από την πρόκληση.
- Υπέβαλε το **αρχείο ή την αναφορά διαμόρφωσης τείχους προστασίας** αν χρειάζεται.
- Ξαναδές τις **εντολές που χρησιμοποίησες** — προσπάθησε να τις επαναλάβεις από μνήμης.
- Άρχισε να προετοιμάζεις το σύστημά σου για **έλεγχο για κακόβουλο λογισμικό**.

Έχεις δημιουργήσει μια ασπίδα — τώρα ήρθε η ώρα να μάθεις πώς να εντοπίζεις εισβολείς.

9. Παράρτημα

9.1 Αναφορά Εντολών Linux (UFW)

Εντολή	Περιγραφή
`sudo ufw status`	Εμφάνιση βασικής κατάστασης του τείχους προστασίας
`sudo ufw status verbose`	Εμφάνιση αναλυτικών ρυθμίσεων κανόνων
`sudo ufw enable`	Ενεργοποίηση του τείχους προστασίας
`sudo ufw disable`	Απενεργοποίηση του τείχους προστασίας
`sudo ufw default deny incoming`	Απόρριψη όλων των εισερχόμενων συνδέσεων από προεπιλογή
`sudo ufw default allow outgoing`	Επιτρέπονται όλες οι εξερχόμενες συνδέσεις
`sudo ufw allow ssh`	Επιτρέπεται η πρόσβαση SSH (θύρα 22)
`sudo ufw allow 80/tcp`	Επιτρέψτε HTTP (θύρα 80)
`sudo ufw deny from [IP]`	Αποκλεισμός όλης της κυκλοφορίας από συγκεκριμένη διεύθυνση IP
`sudo ufw delete [rule-number]`	Διαγραφή συγκεκριμένου κανόνα με βάση τον αριθμό του

9.2 Συμβουλές για το Τείχος Προστασίας των Windows

- Ανοίξτε τον πίνακα **Για Προχωρημένες Ρυθμίσεις** για πλήρη έλεγχο στους κανόνες.
- Να **δοκιμάζετε πάντα τους νέους κανόνες** πριν τους εφαρμόσετε σε κρίσιμα περιβάλλοντα.
- **Χρησιμοποιήστε "Προσαρμοσμένους" κανόνες** για ακριβή στόχευση θυρών, εφαρμογών ή πρωτοκόλλων.
- **Οι προκαθορισμένες προφίλ** (Τομέας, Ιδιωτικό, Δημόσιο) ενδέχεται να λειτουργούν διαφορετικά — ελέγχετε πάντα ποιο είναι ενεργό.
- Για να παρακολουθείτε αποκλεισμένες/επιτρεπόμενες συνδέσεις, χρησιμοποιήστε **Προβολή Συμβάντων > Αρχεία Καταγραφής Ασφαλείας** (για προχωρημένους χρήστες).

9.3 Επίλυση Συνηθισμένων Προβλημάτων

Πρόβλημα	Πιθανή Αιτία	Λύση
Δεν είναι δυνατή η σύνδεση μέσω SSH	Κανόνας μπλοκάρει τη θύρα 22	sudo ufw allow ssh ή έλεγχος κανόνα στα Windows
Το ping επιστρέφει "Έληξε ο χρόνος αίτησης"	Το ICMP είναι απενεργοποιημένο	Ενεργοποιήστε το ICMP (για προχωρημένους) ή ελέγξτε αν το δίκτυο είναι προσβάσιμο
Το Nmap εμφανίζει όλα τα ports κλειστά ή φιλτραρισμένα	Όλες οι θύρες είναι μπλοκαρισμένες ή το firewall είναι ενεργό	Επιτρέψτε συγκεκριμένες θύρες ανάλογα με τις ανάγκες σας
Ο κανόνας των Windows δεν εφαρμόζεται	Έχει επιλεγεί λάθος προφίλ (Ιδιωτικό/Δημόσιο)	Ελέγξτε το ενεργό προφίλ δικτύου και επιβεβαιώστε ότι εφαρμόζεται το σωστό
Το τείχος προστασίας δεν λειτουργεί στο Linux	Το UFW δεν είναι ενεργοποιημένο ή λείπει	Εκτελέστε sudo ufw enable και βεβαιωθείτε ότι έχει εγκατασταθεί

9.4 Επιλογές Εργαλείων & Πόροι

🛠 Προτεινόμενα Εργαλεία

- **Nmap** – https://nmap.org
- **Wireshark** – https://www.wireshark.org
- **ClamAV (Linux antivirus)** – https://www.clamav.net

Περαιτέρω Πηγές

- Οδηγός UFW: man ufw ή https://help.ubuntu.com/community/UFW
- Microsoft Defender Firewall: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall
- OWASP Οδηγός Τείχους Προστασίας: https://owasp.org/www-community/Firewalls