Δημιουργία ασφαλούς περιβάλλοντος, για άσκηση σε θέματα δικτύων και ασφάλειας, με εικονικές μηχανές

Βασιλάκης Βασίλειος
vdvass@gmail.com
Καθηγητής Πληροφορικής ΠΕ19, 1ο ΕΠΑΛ Αργυρούπολης
Υπεύθυνος Τομέα Πληροφορικής 2ο Ε.Κ. Δ' Αθήνας

Περίληψη

Στην παρούσα εργασία παρουσιάζεται μία μέθοδος για τη δημιουργία ενός ασφαλούς περιβάλλοντος στο εργαστήριο πληροφορικής, όπου οι ασκούμενοι θα μπορούν να εργασθούν σε θέματα δικτύων και ασφάλειας, με τη βοήθεια εικονικών μηχανών. Οι εικονικές μηχανές θα είναι απομονωμένες από το υπόλοιπο εσωτερικό δίκτυο του Σχολείου, ενώ ταυτόχρονα θα μπορούν να έχουν πρόσβαση στο Διαδίκτυο αλλά και σε επιλεγμένους διακομιστές που προσφέρουν υπηρεσίες στο εσωτερικό τοπικό δίκτυο. Η υλοποίηση θα γίνει και αυτή με χρήση εικονικής μηχανής και ελεύθερου-ανοιχτού λογισμικού, με μηδενικό κόστος. Με τον τρόπο αυτό η εργασία των ασκούμενων δεν θα επηρεάσει τους υπόλοιπους υπολογιστές που συνδέονται στο δίκτυο του Σχολείου.

Λέξεις κλειδιά: Εργαστήριο Πληροφορικής, Εικονικές Μηχανές, Δίκτυα, Ασφάλεια, Τείχος Προστασίας

Εισαγωγή

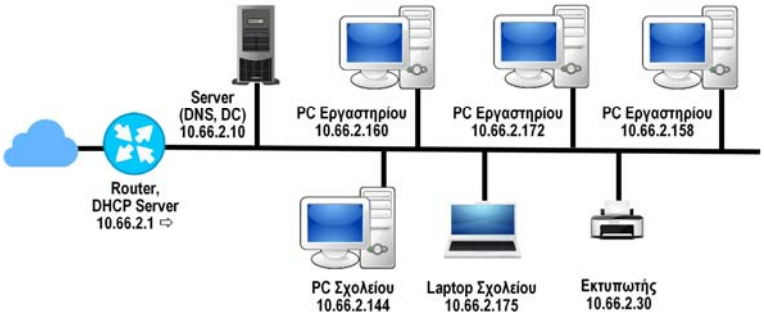
Τα νέα αναλυτικά προγράμματα πληροφορικής των ΕΠΑΛ, αλλά και οι σύγχρονες ειδικότητες των ΙΕΚ απαιτούν την άσκηση σε προχωρημένα θέματα δικτύων και ασφάλειας. Η τεχνολογία των εικονικών μηχανών δίνει τη λύση για την πραγματοποίηση ενεργειών που θα ήταν αδύνατο να γίνουν κάτω από τους περιορισμούς που επιβάλλει η τυπική διαμόρφωση των εργαστηρίων πληροφορικής (Βασιλάκης & Τζανάκης, 2013), αλλά και η ανάγκη για τη συνεχή και απρόσκοπτη λειτουργία τους.

Ωστόσο, η χρήση εικονικών μηχανών στο Εργαστήριο Πληροφορικής ενδέχεται να δημιουργήσει προβλήματα ασφάλειας, καθώς αυτές μπορούν να έχουν πρόσβαση σε υπολογιστές που συνδέονται στο τοπικό δίκτυο του Σχολείου και στα δεδομένα που αυτοί μπορεί να περιέχουν. Η κατάσταση αυτή επιδεινώνεται καθώς τα περισσότερα Σχολεία διαθέτουν πλέον ασύρματο δίκτυο στο οποίο συνδέονται και φορητές υπολογιστικές συσκευές καθηγητών διαφόρων ειδικοτήτων, που δεν έχουν πάντα τις απαραίτητες γνώσεις για να προστατευθούν από μη εξουσιοδοτημένη πρόσβαση.

Προκύπτει συνεπώς η ανάγκη περιορισμού της πρόσβασης των εικονικών μηχανών μόνο στους υπολογιστές του Σχολείου που παρέχουν κάποια απαραίτητη υπηρεσία (π.χ. Web Server). Ταυτόχρονα αυτό θα πρέπει να γίνεται με απλό και διαφανή τρόπο, χωρίς πολύπλοκες ρυθμίσεις που θα αποπροσανατολίσουν τους ασκούμενους από την πραγματική εκπαιδευτική διαδικασία. Σαν λύση προτείνεται η εγκατάσταση ενός Τείχους Προστασίας (firewall) μεταξύ των εικονικών μηχανών και των φυσικών υπολογιστών του Σχολείου. Για την υλοποίηση θα χρησιμοποιηθεί το IPCop, μια εξειδικευμένη διανομή Linux για τη δημιουργία Τείχους Προστασίας (Στέλλας, 2011). Πρόκειται για ελεύθερο λογισμικό ανοιχτού κώδικα που φυσικά διατίθεται δωρεάν.

Σχεδίαση

Η τυπική δομή ενός Σχολικού Εργαστηρίου Πληροφορικής είναι αυτή που φαίνεται στο Σχήμα 1 (Θεοδωρόπουλος κ.α., 2013). Υπάρχει ένας δρομολογητής που αναλαμβάνει την επικοινωνία με τον έξω κόσμο και συνήθως αποτελεί και DHCP Server. Υπάρχει ακόμη και ένα μηχάνημα σε ρόλο Server που αποτελεί ταυτόχρονα DNS Server και Domain Controller (DC). Για τις ανάγκες του παραδείγματος έστω ότι το δίκτυο είναι το 10.66.2.0/24 με τον Router στην διεύθυνση 10.66.2.1 και τον Server στην 10.66.2.10. Οι υπολογιστές του εργαστηρίου αποτελούν μέρος του Domain, ενώ υπάρχουν και άλλοι που ανήκουν σε ομάδες εργασίας (γραφεία, διοίκηση, pc καθηγητών κ.α.).

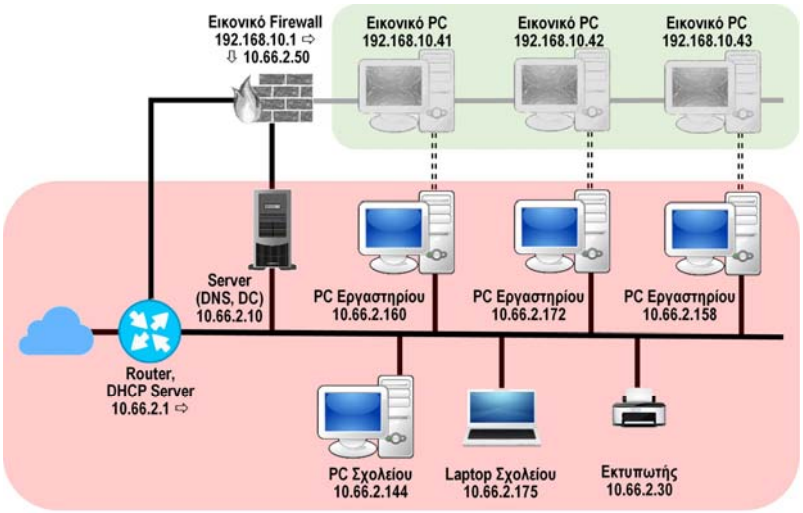


Σχήμα 1. Τυπική δομή Σχολικού Εργαστηρίου Πληροφορικής

Για την υλοποίηση του σχήματος ασφαλείας πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

1. Οι εικονικές μηχανές θα πρέπει να βρίσκονται σε ξεχωριστό δικό τους δίκτυο, έστω π.χ. το 192.168.10.0/24. Δεν θα πρέπει να έχουν πρόσβαση στους υπολογιστές του δικτύου του Σχολείου, παρά μόνο σε εκείνους που παρέχουν κάποια απαραίτητη υπηρεσία (π.χ. Web Server) και μόνο για τη υπηρεσία αυτή.
2. Οι εικονικές μηχανές θα πρέπει να έχουν πρόσβαση στο Διαδίκτυο αλλά και μεταξύ τους. Ο εκπαιδευτικός θα πρέπει να είναι σε θέση να ρυθμίζει τους δικτυακούς τόπους στους οποίους επιτρέπεται η πρόσβαση.

Μετά την παρεμβολή του Τείχους Προστασίας ανάμεσα στις εικονικές μηχανές και τους φυσικούς υπολογιστές, το δίκτυο θα έρθει στη μορφή του Σχήματος 2.



Σχήμα 2. Η δομή μετά την εγκατάσταση του Τείχους Προστασίας

Υλοποίηση

Το ISO της τελευταίας σταθερής έκδοσης του IPCop είναι διαθέσιμο στο δικτυακό τόπο http://www.ipcop.org/. Οι απαιτήσεις του IPCop είναι πολύ χαμηλές και προτείνεται η εγκατάσταση του στο Server ή σε υπολογιστή που μένει ανοιχτός καθ' όλη τη λειτουργία του εργαστηρίου.

Δημιουργία εικονικής μηχανής και εγκατάσταση

Αρχικά θα πρέπει να γίνει η δημιουργία μιας νέας εικονικής μηχανής με τη διαμόρφωση που φαίνεται στον Πίνακα 1.

Πίνακας 1. Ρυθμίσεις εικονικής μηχανής

Ιδιότητα	Ρύθμιση
Λειτουργικό Σύστημα	Unix / Linux (έκδοση πυρήνα ≥ 2.6)
Μνήμη RAM	256 έως 384 MB
Μέσα αποθήκευσης	HD 8.00GB, IDE CD-ROM
Δίκτυο	Δύο κάρτες δικτύου σε γεφύρωση (bridged) με τη φυσική κάρτα δικτύου του υπολογιστή.

Η εγκατάσταση του IPCop στην εικονική μηχανή είναι τυπική Linux και γίνεται σε περιβάλλον κειμένου. Στο τελευταίο της στάδιο γίνονται οι δικτυακές ρυθμίσεις. Το IPCop μπορεί να υποστηρίξει μέχρι τέσσερις ζώνες. Η κόκκινη (RED) είναι το εξωτερικό/αναξιόπιστο δίκτυο (εδώ το τοπικό δίκτυο του Σχολείου και το Διαδίκτυο). Η πράσινη (GREEN) είναι το εσωτερικό/έμπιστο δίκτυο (εδώ οι εικονικές μηχανές), η πορτοκαλί (ORANGE) η ζώνη αποστρατικοποίησης (DMZ) και η μπλε (BLUE) για σύνδεση κυρίως ασύρματων συσκευών σε διαφορετικό δίκτυο. Κάθε μία από αυτές χρειάζεται τη δική της δικτυακή διασύνδεση (interface). Για τις ανάγκες του παρόντος χρειάζονται μόνο η κόκκινη και η πράσινη. Η κόκκινη διασύνδεση ορίζεται σαν στατική (Static) με τις τιμές που φαίνονται στον Πίνακα 2. Δεν πρέπει να γίνει ενεργοποίηση του DHCP Server για την πράσινη ζώνη, ώστε να μην υπάρχουν δύο DHCP Server στο ίδιο φυσικό δίκτυο.

Πίνακας 2. Δικτυακές ρυθμίσεις του IPCop

Διασύνδεση	Διεύθυνση IP	Μάσκα Υποδικτύου	Πρωτεύων DNS	Δευτερεύων DNS	Προεπιλεγμένη Πύλη
RED	10.66.2.50	255.255.255.0	10.66.2.10	194.63.239.164	10.66.2.1
GREEN	192.168.10.1	255.255.255.0			

Τέλος, ζητείται η εισαγωγή τριών συνθηματικών, για τους χρήστες root, admin και backup. Ο πρώτος είναι για σύνδεση στο Login της διανομής, ο δεύτερος για σύνδεση στην ιστοσελίδα διαχείρισης και ο τρίτος για λήψη αντίγραφου ασφαλείας των ρυθμίσεων. Όταν η εγκατάσταση τελειώσει μπορεί να γίνει σύνδεση σαν root και δοκιμή τη συνδεσιμότητας προς όλα τα δίκτυα αλλά και το Διαδίκτυο με την εντολή ping. Αν έχει γίνει λάθος σε κάποια ρύθμιση αυτό μπορεί να διορθωθεί με την εντολή *setup*.

Δημιουργία κανόνων Τείχους Προστασίας

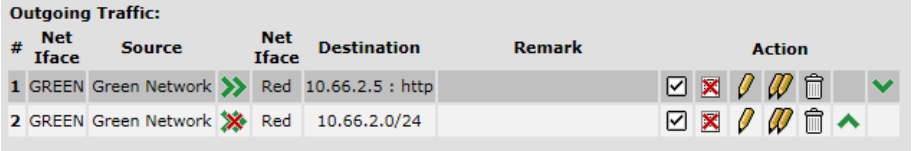
Αφού ξεκινήσει το IPCop σειρά έχει η δημιουργία μιας εικονική μηχανής με στατική IP διεύθυνση στην πράσινη ζώνη και DNS και Προεπιλεγμένη πύλη την διεύθυνση της πράσινης διασύνδεσης (192.168.10.1). Από εκεί μέσω ενός φυλλομετρητή παρέχεται πρόσβαση στην ιστοσελίδα ρύθμισης στη διεύθυνση https://192.168.10.1:8443.

Ακολουθεί η δημιουργία δύο κανόνων ασφαλείας από την επιλογή Firewall/Rules/Outgoing Traffic. Ο ένας θα απαγορεύει την πρόσβαση στο δίκτυο του Σχολείου, ενώ ο άλλος θα επιτρέπει την πρόσβαση σε έναν Web Server στη διεύθυνση 10.66.2.5. Οι ρυθμίσεις περιγράφονται στον πίνακα 3.

Χρειάζεται προσοχή στο ότι το IPCop εφαρμόζει τους κανόνες με τη σειρά που εμφανίζονται στον κατάλογο. Ο κανόνας της απαγόρευσης πρόσβασης θα πρέπει να είναι ο τελευταίος και αυτοί που επιτρέπουν την πρόσβαση να προηγούνται. Η σειρά των κανόνων στον κατάλογο μπορεί να αλλάξει από τα βέλη ▲ και ▼.

Πίνακας 3. Κανόνες Τείχους Προστασίας

Πεδία	Άρνηση Πρόσβασης στο Δίκτυο του Σχολείου	Πρόσβαση σε Web Server
Source	Default Networks: Green Network	Default Networks: Green Network
Destination	Destination IP or Net: 10.66.2.0/24	Destination IP or Net: 10.66.2.5
Use Service	-	http (80)
Additional	Rule Enabled, Rule Action: DROP	Rule Enabled, Rule Action: ACCEPT



Σχήμα 3. Ο κατάλογος των κανόνων του Τείχους Προστασίας

Ρυθμίσεις εικονικών μηχανών

Σε κάθε εικονική μηχανή θα πρέπει να δοθεί στατική IP διεύθυνση στο δίκτυο 192.168.10.0/24, με DNS και Προεπιλεγμένη Πύλη το 192.168.10.1. Επίσης θα πρέπει να απενεργοποιηθεί το IPv6 στα λειτουργικά συστήματα που από προεπιλογή το εγκαθιστούν, καθώς μπορεί να υπάρχει πρόσβαση σε κάποιες υπηρεσίες μέσω αυτού (π.χ. Περιοχή Δικτύου στα Windows Vista και μεταγενέστερα).

Επεκτάσεις

Οι δυνατότητες του IPCop δεν σταματούν εδώ. Υπάρχει δυνατότητα λεπτομερούς παραμετροποίησης του που μπορεί να καλύψει σχεδόν οποιαδήποτε ανάγκη (Clancey et al., 2014). Εκτός από το IPCop υπάρχουν και άλλες διανομές που μπορούν να υλοποιήσουν Τείχος Προστασίας όπως οι IPFire, pfSense, ClearOS κ.α., με παρόμοια εγκατάσταση και παραμετροποίηση.

Συμπεράσματα

Το IPCop, μπορεί να χρησιμοποιηθεί για να απομονώσει τις εικονικές μηχανές που δημιουργούν οι ασκούμενοι στο Εργαστήριο Πληροφορικής από το υπόλοιπο δίκτυο του Σχολείου, εξασφαλίζοντας έτσι ότι η εργασία σε αυτές δεν θα θέσει σε κίνδυνο την ασφάλεια των δεδομένων των φυσικών υπολογιστών που συνδέονται σε αυτό. Επιπλέον προσφέρει τη δυνατότητα λεπτομερούς ρύθμισης των θέσεων στις οποίες η κάθε εικονική μηχανή μπορεί να έχει πρόσβαση, διευκολύνοντας έτσι το έργο του εκπαιδευτικού. Τέλος, λόγω των πολύ χαμηλών απαιτήσεων του σε υλικό και επεξεργαστική ισχύ, μπορεί να λειτουργήσει και το ίδιο μέσα σε εικονική μηχανή, χωρίς ιδιαίτερη επιβάρυνση του υπολογιστή που θα το φιλοξενήσει και με μηδενικό ουσιαστικά κόστος.

Αναφορές

Clancey, C., Goldschmitt, H., Kastner, J., Oberlander, E., Walker, P., Sondermann, M. (2014), IPCop v2.0.0 administration manual, Retrieved 10 January 2016 from http://www.ipcop.org/2.0.0/en/admin/html/index.html

Βασιλάκης, Β., Τζανάκης, Δ. (2013). Αξιοποίηση της τεχνολογίας των εικονικών μηχανών στην επαγγελματική εκπαίδευση και την κατάρτιση πληροφορικής, Στο *Πρακτικά Εργασιών 3ου Πανελλήνιου Συνεδρίου «Ένταξη των ΤΠΕ στην Εκπαιδευτική Διαδικασία»*, Πειραιάς.

Θεοδωρόπουλος, Θ., Σιάχος, Γ., Παπαναγιώτου Ι. (2013). Εγκατάσταση ΣΕΠΕΗΥ με Windows 2008 Server & Windows 7, Ανακτήθηκε στις 20 Ιανουαρίου 2016 από http://ts.sch.gr/docs/cat_view/60-odhgies-egkatastashs-diaxeirishs

Στέλλας, Ι. (2011). Αποκτήστε με ΕΛ/ΛΑΚ ένα φύλακα ασφαλείας (guard) στο εργαστήριό σας. Στο *Η Πληροφορική στην Εκπαίδευση: Πρακτικά Εργασιών 3rd Conference on Informatics in Education*, σελ. 38-45, Πειραιάς.