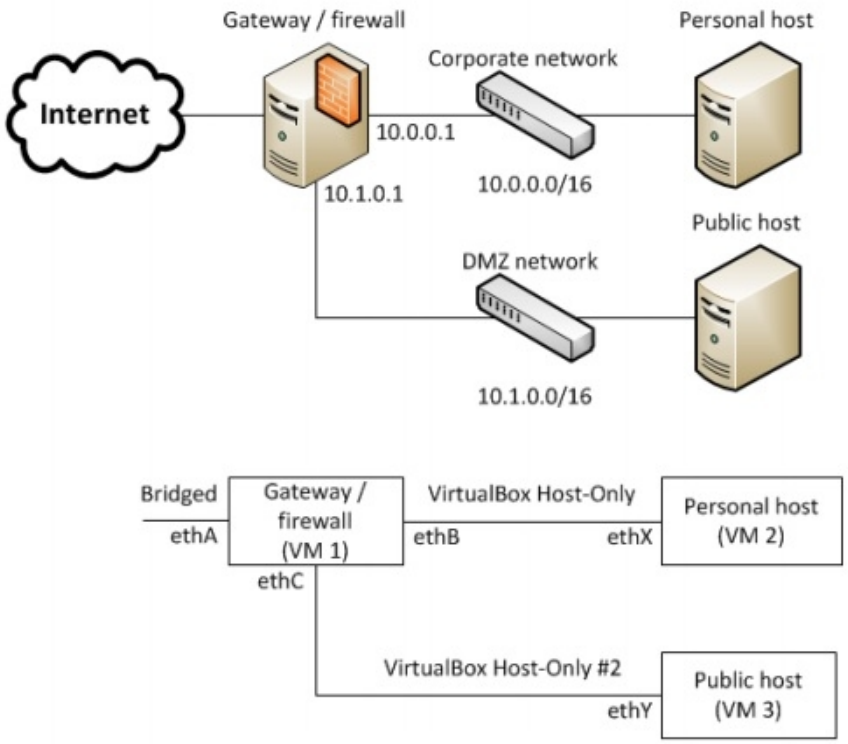
(A) Πολιτική Ασφάλειας Δικτύου με τη χρήση firewall

Στόχος είναι να υλοποιήσετε πολιτική ασφάλειας δικτύου με τη χρήση firewall. Για την υλοποίηση μπορείτε να χρησιμοποιείστε iptables ή οποιαδήποτε άλλη τεχνολογία firewall επιθυμείτε (πχ pfsense).

1) Δημιουργία τοπολογίας δικτύου.

Δημιουργήστε με τη χρήση εικονικών μηχανών τοπολογία δικτύου αντίστοιχη με αυτή της παρακάτω εικόνας.



Θα χρειαστεί να δημιουργήσεστε 3 VM: Το VM1 θα έχει το ρόλο του κεντρικού firewall/gateway. Το VM2 θα έχει το ρόλο του εσωτερικού δικτύου (ITZ) και το VM3 το ρόλο του εξωτερικά προσβάσιμου δικτύου (DMZ). Επιπλέον, στα VM2 και VM3 πρέπει επίσης να ρυθμιστεί η προεπιλεγμένη πύλη (gateway) προκειμένου η κίνηση να δρομολογείται από το VM στο ρόλο του gateway.

2) Υλοποίηση πολιτικής

Οι επιχειρησιακοί κανόνες που πρέπει να υλοποιήσετε ως κανόνες firewall πρέπει να εκτελούν τα ακόλουθα:

> (1) Βασική αντιμετώπιση προβλημάτων δικτύου: Επιτρέψτε στα γειτονικά VM του δικτύου VM 1 και 2 να κάνουν ping (ICMP τύπου) μεταξύ τους.
>
> (2) Ενεργοποίηση της εταιρικής κίνησης δικτύου στο Internet: Για να επιτρέψετε στους υπολογιστές να φτάσουν σε υπηρεσίες Internet, πρέπει να εξουσιοδοτήσετε τις διευθύνσεις του δικτύου τους για να προωθηθούν και να ενεργοποιήσετε το NAT για

όλα τα πακέτα που φθάνουν από αυτό το δίκτυο. **Hint:** Η λειτουργία NAT πρέπει να οριστεί στον πίνακα NAT της αλυσίδας POSTROUTING.

(3) Υλοποίηση πολιτικής ασφάλειας για το εσωτερικό δίκτυο ITZ: Μέσω iptables (pfsense ή άλλης αν, να υλοποιήσετε μία πολιτική ασφάλειας δικτύου για το σύστημα που προσομοιώνει το εταιρικό δίκτυο. Θα πρέπει να διαμορφώσετε το firewall ώστε:

- Να επιτρέπεται το loopback.
- Να επιτρέπεται κίνηση DNS ανάλογα με το πρωτόκολλό του.
- Να επιτρέπεται η εξερχόμενη κίνηση προς HTTP/HTTPS.
- Να γίνεται logging των εισερχόμενων πακέτων και να καταγράφει πληροφορίες σύνδεσης για κάθε "ύποπτη" κίνηση (log and drop policy),
- Απαγορεύστε όλη την κίνηση που δεν επιτρέπεται ρητά (default deny).

(4) Ανακατεύθυνση επισκεψιμότητας σε υπηρεσία web στο DMZ: Καλείστε να εγκαταστήστε ένα Web Server στο VM 3 και να βάλετε τους απαραίτητους κανόνες στο firewall για την ασφαλή πρόσβαση στην υπηρεσία web από το εξωτερικό δίκτυο. Μεταξύ άλλων, το firewall θα πρέπει να λαμβάνει αποφάσεις βάσει της κατάστασης των συνδέσεων (stateful inspection).

(5) Αυτόματη εκκίνηση κανόνων: Να ενεργοποιείστε αυτόματη φόρτωση των κανόνων του firewall κατά την εκκίνηση του VM1.

(6) Application Layer Firewall. Για προστασία του web server σε επίπεδο εφαρμογής, εγκαταστήστε και διαμορφώστε κάποιο open source Web Application Firewall της επιλογής σας.

3) Επαλήθευση κανόνων

Καλείστε να κάνετε ενδεικτική δοκιμή και επαλήθευση των πολιτικών που εφαρμόσατε. Δηλαδή να δημιουργήσετε δοκιμαστική κίνηση ώστε να επαληθεύσετε ότι οι κανόνες του ερωτήματος 2 είναι σωστοί.

4) Δοκιμή επιθέσεων και υλοποίηση κανόνων αποτροπής

Στο βήμα αυτό καλείστε να υλοποιήσετε μία επίθεση δικτύου (π.χ. port/service scanning, DDoS κτλ) και να υλοποιήσετε τους κανόνες αντιμετώπισης της επίθεσης.

(1) Υλοποίηση επίθεσης: Μπορείτε να χρησιμοποιήσετε εργαλεία όπως το nmap για την υλοποίηση επιθέσεων τύπου scanning ή εργαλεία DDoS, π.χ. [1].

(2) Αποτροπή επίθεσης μέσω κανόνων στο firewall: Υλοποιήστε και δοκιμάστε τους κατάλληλους κανόνες αντιμετώπισης της επίθεσης, π.χ. [2].

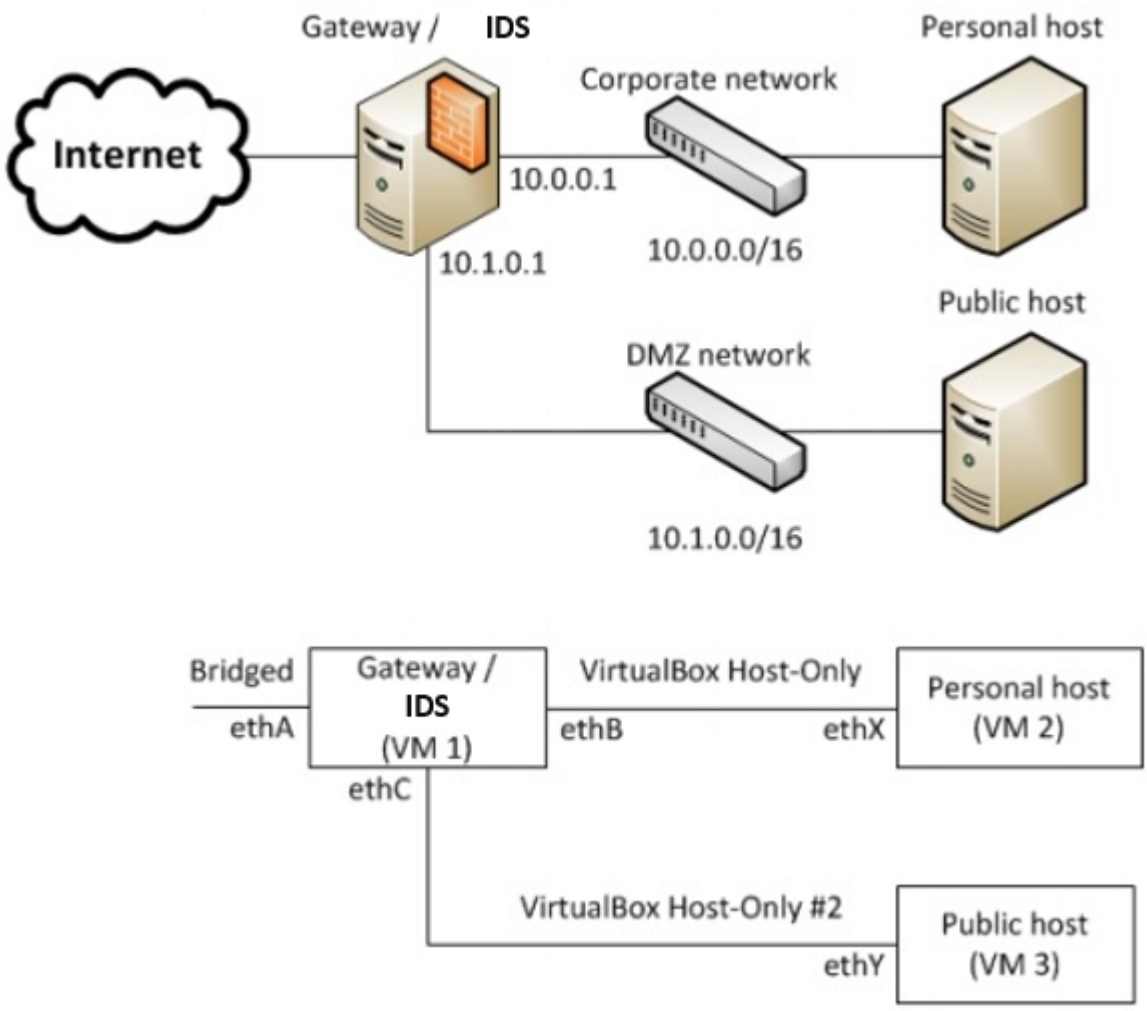
Χρήσιμες πηγές

[1] https://thehackerstuff.com/top10-powerfull-ddos-tools-linux-windows/

[2] https://javapipe.com/blog/iptables-ddos-protection/

(B) Ανίχνευση επιθέσεων με τη χρήση IDS

Σε συνέχεια του (A) μέρους, στόχος είναι να υλοποιήσετε μία πολιτική ανίχνευσης επιθέσεων δικτύου με τη χρήση IDS. Για την υλοποίηση μπορείτε να χρησιμοποιείστε snort ή οποιαδήποτε άλλη τεχνολογία IDS επιθυμείτε (πχ suricata).



Χρησιμοποιήστε την τοπολογία της προηγούμενης εργασίας (σχετικά με τα firewall) στην οποία θα εγκαταστήσετε σύστημα IDS της επιλογής σας, στο VM1.

Στη συνέχεια καλείστε:

- Να εγκαταστήσετε στο public host μηχάνημα έναν xampp server. https://www.apachefriends.org/index.html)
    - Μέσω του apache που εμπεριέχεται στο xampp θα κάνετε host ένα απλό HTML page.
    - Θα ενεργοποιήσετε επίσης και τον FileZilla server, για την περίπτωση του Brute force attack.

- Ρυθμίστε το IDS ώστε να εντοπίζει και αποτρέπει τις παραπάνω επιθέσεις (BruteForce, HTTP Flood Attack). Μπορείτε να χρησιμοποιήσετε υπάρχοντα σετ κανόνων ή να δημιουργήσετε τους δικούς σας κανόνες που θα αποτρέπουν τις παραπάνω επιθέσεις.
    - Εάν χρησιμοποιήσετε έτοιμο πακέτο κανόνων πρέπει να βρείτε τον κανόνα ή τους κανόνες που αποτρέπουν τις συγκεκριμένες επιθέσεις και να τον εξηγήσετε. *Οι κανόνες μπορεί ήδη να περιέχονται στο πακέτο κανόνων που είναι διαθέσιμα κατά την εγγραφή στο snort.org.*
    - Εάν δημιουργηθεί καινούργιος κανόνας, εξηγείστε ακριβώς τι κάνει και πως αποτρέπει την επίθεση.
    - Σε περίπτωση χρήσης του Snort για να αποτρέψει τις παραπάνω επιθέσεις θα πρέπει να είναι σε IDS mode(-Q). Επιλέξτε το κατάλληλο module μέσω του snort.conf αρχείου. Προτείνονται τα afpacket-nfq. Το ipfw σε pfsence interaction.

- Μέσω του kali linux καλείστε να εκτελέσετε επιθέσεις στο Windows μηχάνημα τύπου:
    - FTP BruteForce attack στα credentials του FileZilla server χρησιμοποιώντας κάποιο wordlist.Πιθανά Εργαλεία:
        - **Medusa** (https://www.hackingarticles.in/comprehensive-guide-on-medusa-a-brute-forcing-tool/), **XHydra**(https://github.com/frizb/Hydra-Cheatsheet), **Ncrack**(https://nmap.org/ncrack/man.html).
    - HTTP Flood Attack στο HTML page ως προς το content της σελίδας. Ενδεικτικά εργαλεία:
        - Python Useful Libraries:
            - Requests(https://pypi.org/project/requests/),
            - Molotov(https://molotov.readthedocs.io/en/stable/)
        - Apache Jmeter (https://jmeter.apache.org/download_jmeter.cgi)
        - Low Orbit Ion Cannon (https://github.com/NewEraCracker/LOIC).
- Πραγματοποιήστε επανάληψη των επιθέσεων για να επαληθεύσετε την λειτουργικότητα των κανόνων. (logs, screenshots)

Βοηθητικά link:

https://github.com/codecat007/snort-rules/blob/master/snortrules-snapshot-29150/rules/server-apache.rules

http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html

https://stackoverflow.com/questions/47742405/using-snort-suricata-i-want-to-generate-an-ssh-alert-for-every-failed-login-to

https://www.debuggex.com/cheatsheet/regex/pcre

https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/#article

https://blog.joelesler.net/2010/03/offset-depth-distance-and-within.html

https://www.computersecuritystudent.com/SECURITY_TOOLS/Metasploit/lesson19/index.html