ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Ομαδική εργασία μαθήματος ***Ασφάλεια Δικτύων και Επικοινωνιών***

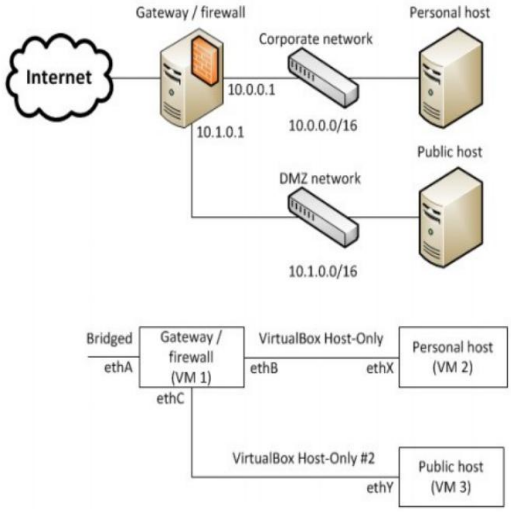
Εκφώνηση της άσκησης

(Α) 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, psfense ή οποιαδήποτε άλλη τεχνολογία firewall επιθυμείτε.**

1) Δημιουργία τοπολογίας δικτύου.

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



Θα χρειαστεί να δημιουργήσετε 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.

1

(3) Υλοποίηση πολιτικής ασφάλειας για το εσωτερικό δίκτυο ITZ: Μέσω του firewall, 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

Να πραγματοποιήσετε 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://kiloai.hashnode.dev/iptables-ddos-protection-the-best-rules-to-mitigate-ddos-attacks

[3] https://serverfault.com/questions/1105705/how-to-configure-iptables-against-ddos-attacks-or-others

[4] https://blog.cloudflare.com/how-to-drop-10-million-packets/

Περιεχόμενα

(Α ΜΕΡΟΣ) Πολιτική Ασφάλειας Δικτύου με τη χρήση firewall

1 Εισαγωγή και σχεδιασμός

1.1 Αντικείμενο και σκοπός

Αντικείμενο της παρούσας εργασίας είναι η σχεδίαση και η πρακτική υλοποίηση μιας ολοκληρωμένης δικτυακής υποδομής με έμφαση στην ασφάλεια. Μέσω της χρήσης εικονικών μηχανών (Virtual Machines), προσομοιώνεται ένα εταιρικό περιβάλλον το οποίο διαχωρίζεται σε ζώνες εμπιστοσύνης, ελεγχόμενες από έναν κεντρικό Gateway (Firewall).

Βασικός σκοπός είναι η θωράκιση των εσωτερικών συστημάτων από εξωτερικές απειλές, επιτρέποντας παράλληλα την λειτουργία των απαραίτητων υπηρεσιών (όπως Web και DNS) και τη δημοσίευση υπηρεσιών προς το Διαδίκτυο με ελεγχόμενο τρόπο.

1.2 Αρχιτεκτονική και τοπολογία δικτύου

Η τοπολογία που υλοποιήθηκε ακολουθεί το μοντέλο των τριών ζωνών:

1. Εξωτερικό Δίκτυο eth0 (WAN / Internet): Η πύλη προς τον έξω κόσμο, η οποία συνδέεται στη διεπαφή eth0 του Gateway.
2. Internal Trust Zone eth1 (ITZ): Το εσωτερικό δίκτυο της εταιρείας (VM2), όπου φιλοξενούνται οι σταθμοί εργασίας των χρηστών. Η πρόσβαση είναι περιορισμένη και ελέγχεται αυστηρά.
3. Demilitarized Zone eth2 (DMZ): Η ζώνη που φιλοξενεί τον δημόσιο Web Server (VM3). Είναι απομονωμένη από το εσωτερικό δίκτυο (ITZ), ώστε σε περίπτωση παραβίασης του Web Server, ο εισβολέας να μην αποκτήσει αυτόματα πρόσβαση στα εταιρικά δεδομένα.

Για την πιστή αναπαράσταση της τοπολογίας, παραμετροποιήθηκαν οι εικονικές κάρτες δικτύου του Gateway (VM1) μέσω του VirtualBox, ώστε να διαχωριστούν πλήρως τα κανάλια επικοινωνίας:

Adapter 1 (NAT): Ρυθμίστηκε σε κατάσταση NAT, συνδέοντας το VM1 με τον εξωτερικό κόσμο (Internet). Αυτή η κάρτα λαμβάνει αυτόματα διεύθυνση IP και χρησιμεύει ως η μοναδική πύλη εξόδου για όλο το εταιρικό δίκτυο.

Adapter 2 (Internal Network): Ρυθμίστηκε ως Internal Network με το όνομα "itz-net". Σε αυτόν τον προσαρμογέα συνδέθηκε αποκλειστικά το VM2(Adapter 1), δημιουργώντας ένα απομονωμένο κανάλι για το εσωτερικό δίκτυο της εταιρείας.

Adapter 3 (Internal Network): Ρυθμίστηκε ως Internal Network με το όνομα "dmz-net". Εδώ συνδέθηκε το VM3(Adapter 1), εξασφαλίζοντας ότι η κίνηση προς τον Web Server εδεν αναμιγνύεται με την κίνηση των χρηστών του ITZ.

1.3 Τεχνολογίες υλοποίησης

Για την υλοποίηση της εργασίας χρησιμοποιήθηκαν τα εξής εργαλεία:

- Hypervisor: VirtualBox για τη φιλοξενία και δικτύωση των εικονικών μηχανών.
- Λειτουργικό Σύστημα: Kali Linux και στις 3 εικονικές μηχανές
- Netfilter / iptables: Το υποσύστημα του πυρήνα Linux που χρησιμοποιήθηκε για το φιλτράρισμα των πακέτων (Filtering) και τη μετάφραση διευθύνσεων (NAT).

1.4 Σχεδιασμός διευθυνσιοδότησης

Για την αποφυγή συγκρούσεων και την ορθή δρομολόγηση, εφαρμόστηκε το παρακάτω σχήμα διευθυνσιοδότησης:

Μηχάνημα	Ρόλος	Δίκτυο	IP Διεύθυνση
VM1	Gateway / Firewall	WAN / ITZ / DMZ	10.0.2.15 / 10.0.0.1 / 10.1.0.1
VM2	Personal Host	ITZ	10.0.0.10
VM3	Public Host	DMZ	10.1.0.10

2 Υλοποίηση πολιτικής ασφάλειας και firewall

Σε αυτό το κεφάλαιο περιγράφεται η παραμετροποίηση του VM1 (Gateway) ως κεντρικού σημείου ελέγχου της κυκλοφορίας, εφαρμόζοντας κανόνες φιλτραρίσματος πακέτων και μετάφρασης διευθύνσεων.

2.1 Βασική αντιμετώπιση προβλημάτων

Ο πρώτος στόχος ήταν η διασφάλιση της βασικής επικοινωνίας μεταξύ των γειτονικών δικτύων για λόγους διάγνωσης.

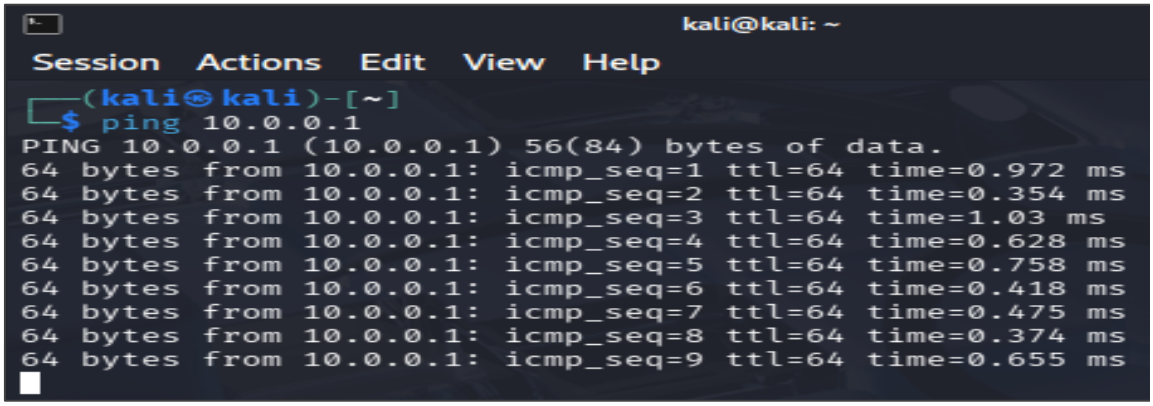
Επιτρέψαμε το πρωτόκολλο ICMP (ping) μεταξύ του VM1 και του VM2. (Εικόνα 1)

Εντολές (VM1):

- `sudo iptables -A INPUT -p icmp -i eth1 -j ACCEPT`

Επεξήγηση: Η παράμετρος -p icmp στοχεύει το πρωτόκολλο ελέγχου μηνυμάτων. Με την παράμετρο -i eth1, ορίζουμε ότι το VM1 θα δέχεται πακέτα μόνο από τη διεπαφή που είναι συνδεδεμένη στο εσωτερικό δίκτυο (itz-net).

Επειδή το VM3 είναι συνδεδεμένο στην eth2 (DMZ), τυχόν προσπάθεια ping από αυτό θα απορριφθεί από την προεπιλεγμένη πολιτική (Default Drop), καθώς δεν ταιριάζει με τον κανόνα της eth1.



Εικόνα 1: VM-2 ping VM-1 (10.0.0.10 ping 10.0.0.1)

2.2 Ενεργοποίηση εταιρικής κίνησης στο Internet

Για να αποκτήσουν πρόσβαση στο Διαδίκτυο οι εσωτερικοί υπολογιστές, υλοποιήσαμε τη δρομολόγηση και τη μετάφραση διευθύνσεων.

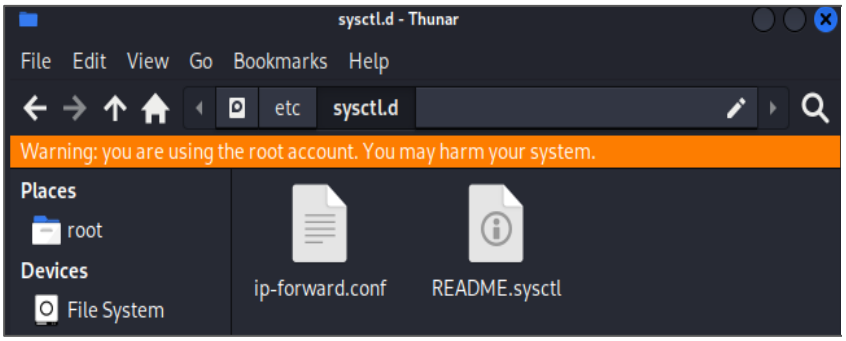
2.2.1 IP Forwarding

Από προεπιλογή, ο πυρήνας (Kernel) του Linux έχει τη λειτουργία προώθησης πακέτων απενεργοποιημένη για λόγους ασφαλείας. Η παράμετρος net.ipv4.ip_forward λειτουργεί ως ένας ψηφιακός διακόπτης:

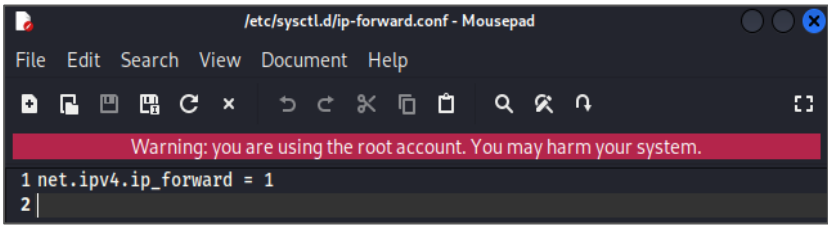
- Όταν η τιμή είναι 0 (Default): Το VM1 λειτουργεί ως "αδιέξοδο". Αν λάβει ένα πακέτο που δεν προορίζεται για την IP του, το απορρίπτει.
- Όταν η τιμή είναι 1 (Ενεργό): Το VM1 λειτουργεί ως γέφυρα. Επιτρέπεται στον πυρήνα να λαμβάνει πακέτα από μία διεπαφή (π.χ. το εσωτερικό δίκτυο ITZ στην eth1) και να τα προωθεί σε μια άλλη (π.χ. το Internet στην eth0).

Για να διασφαλίσουμε ότι θα παραμείνει έτσι ακόμα και μετά από επανεκκίνηση του συστήματος, ακολουθήσαμε τα εξής βήματα:

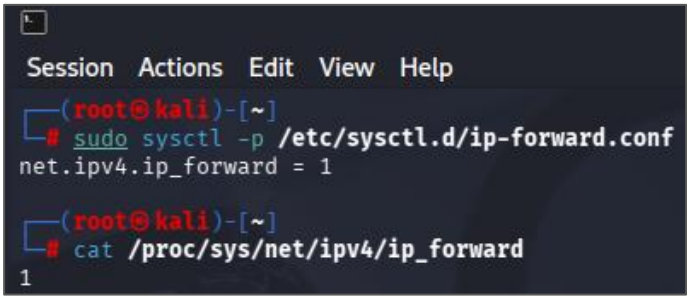
- Τροποποίηση αρχείου: Δημιουργήσαμε κεντρικό αρχείο ρυθμίσεων στη διαδρομη /etc/sysctl.d/ ip-forward.conf (Εικόνα 2)
- Ενεργοποίηση ρύθμισης: Προσθέσαμε τη γραμμή net.ipv4.ip_forward=1 και την ενεργοποιήσαμε. Η ονομασία της παραμέτρου αναφέρεται ιεραρχικά στο δίκτυο (net), στο πρωτόκολλο IPv4 και στη λειτουργία προώθησης (forward). (Εικόνα 3)
- Άμεση εφαρμογή: Για να μην χρειαστεί επανεκκίνηση, εκτελέσαμε την εντολή: sudo sysctl -p Η εντολή αυτή αναγκάζει το σύστημα να διαβάσει το αρχείο και να ενημερώσει άμεσα τις ρυθμίσεις του στη μνήμη RAM. (Εικόνα 4)
- Επαλήθευση: Επιβεβαιώσαμε την αλλαγή διαβάζοντας την τρέχουσα τιμή απευθείας από το σύστημα αρχείων του πυρήνα: cat /proc/sys/net/ipv4/ip_forward. Η εμφάνιση της τιμής 1 επιβεβαίωσε ότι ο Gateway είναι πλέον έτοιμος να δρομολογήσει την κίνηση από τα VM2 και VM3 προς το εξωτερικό δίκτυο. (Εικόνα 4)



Εικόνα 2: Δημιουργία αρχείου ρυθμίσεων



Εικόνα 3: Παράμετρος για forwarding



Εικόνα 4: Αποτελέσματα και επαλήθευση

2.2.2 Εργαλείο netfilter-persistent

Οι κανόνες που ορίζονται μέσω της εντολής iptables αποθηκεύονται προσωρινά στη μνήμη RAM. Αυτό σημαίνει ότι σε περίπτωση επανεκκίνησης του VM1, το firewall θα επέστρεφε σε κενή κατάσταση, διακόπτοντας την πρόσβαση στο Internet για όλο το

δίκτυο. Για να αποφύγουμε τη χειροκίνητη επανεισαγωγή των κανόνων, χρησιμοποιήσαμε το εργαλείο netfilter-persistent.

Το netfilter-persistent είναι ένα εργαλείο που τρέχει κατά την εκκίνηση του συστήματος. Η εγκατάστασή του είναι απαραίτητη εξ αρχής σε έναν Gateway, καθώς επιτρέπει στο σύστημα να διαβάζει τους αποθηκευμένους κανόνες από ένα αρχείο ρυθμίσεων και να τους εφαρμόζει αυτόματα στον πίνακα Netfilter του πυρήνα.

Πριν προχωρήσουμε στην εισαγωγή των κανόνων, έπρεπε να βεβαιωθούμε ότι η υπηρεσία είναι εγκατεστημένη και ενεργή. (Εικόνα 5)

- Έλεγχος Εγκατάστασης: Με την εντολή dpkg -l | grep netfilter-persistent επιβεβαιώσαμε ότι το πακέτο είναι παρόν στο σύστημα.
- Ενεργοποίηση Υπηρεσίας: Χρησιμοποιήσαμε την εντολή sudo systemctl enable netfilter-persistent. Με αυτή την ενέργεια, προετοιμάσαμε το πρόγραμμα ώστε να είναι έτοιμο να λειτουργήσει.

Εικόνα 5: Ενεργοποίηση του netfilter-presistent

2.2.3 Εφαρμογή κανόνων

Για την υλοποίηση της πρόσβασης στο Διαδίκτυο, χρησιμοποιήθηκαν δύο βασικές εντολές του εργαλείου iptables. (Εικόνα 8) Παρακάτω αναλύεται κάθε τμήμα τους:

Α. Η εντολή του NAT (Network Address Translation)

- `sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`

Επεξήγηση:

- **iptables**: Το εργαλείο διαχείρισης του firewall και του NAT στο Linux.
- **-t nat**: Ορίζει τον πίνακα (table) στον οποίο θα γίνει η παρέμβαση. Ο πίνακας nat χρησιμοποιείται αποκλειστικά για τη μετάφραση διευθύνσεων.
- **-A**: Σημαίνει Append (προσθήκη). Προσθέτει τον κανόνα στο τέλος της συγκεκριμένης αλυσίδας.
- **POSTROUTING**: Η αλυσίδα (chain) που επεξεργάζεται το πακέτο μετά τη δρομολόγηση, ακριβώς πριν αυτό εγκαταλείψει τον Gateway. Είναι το κατάλληλο σημείο για να αλλάξουμε την IP του αποστολέα.
- **-o eth0**: Ορίζει την έξοδο (output interface). Ο κανόνας θα ισχύει μόνο για πακέτα που φεύγουν μέσω της κάρτας eth0, η οποία είναι συνδεδεμένη στο Internet.
- **-j**: Σημαίνει Jump. Ορίζει τι θα συμβεί αν το πακέτο ταιριάζει με τα παραπάνω κριτήρια (τον στόχο - target).
- **MASQUERADE**: Ο στόχος του NAT. Αντικαθιστά την ιδιωτική IP του εσωτερικού VM με την IP της eth0. Ονομάζεται έτσι γιατί ο Gateway παρουσιάζει τα πακέτα των άλλων VM σαν να είναι δικά του.

Β. Η εντολή προώθησης (Forwarding Approval)

- `sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT`

Επεξήγηση:

- **-A FORWARD**: Προσθήκη κανόνα στην αλυσίδα FORWARD. Αυτή η αλυσίδα διαχειρίζεται πακέτα που ο Gateway απλώς «μεταφέρει» (δεν προορίζονται για τον ίδιο).
- **-i eth1**: Ορίζει την είσοδο (input interface). Αφορά πακέτα που έρχονται από το εσωτερικό δίκτυο ITZ μέσω της κάρτας eth1.
- **-o eth0**: Ορίζει την έξοδο (output interface). Αφορά πακέτα που κατευθύνονται προς το Internet μέσω της eth0.

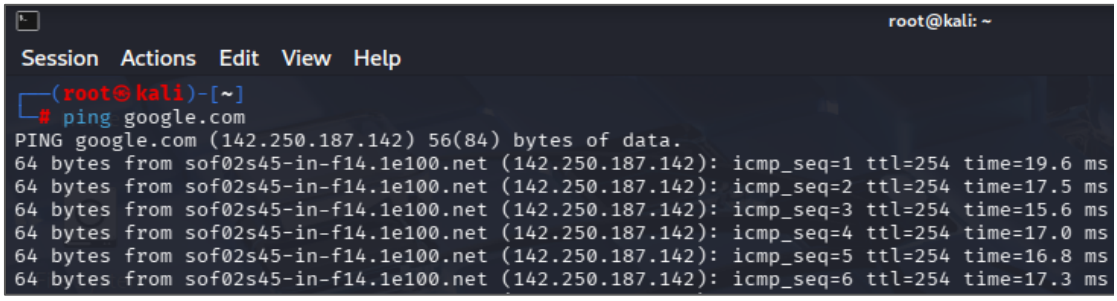
- **-j ACCEPT**: Ο στόχος είναι η αποδοχή. Δίνει τη ρητή άδεια στο firewall να αφήσει αυτά τα πακέτα να περάσουν. Χωρίς αυτή την εντολή, ακόμα και αν το NAT ήταν σωστό, το firewall θα μπορούσε να "κόψει" την κυκλοφορία.

2.2.4 Επαλήθευση και Ανάλυση Πακέτων (Live Testing)

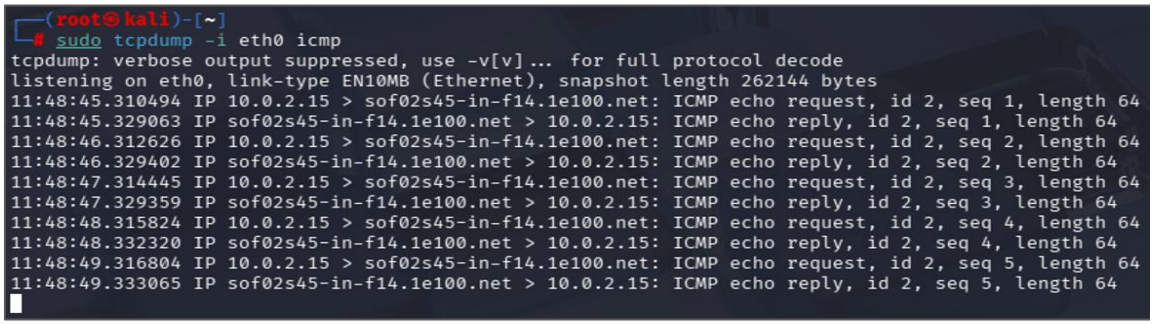
Πριν προχωρήσουμε στην οριστική αποθήκευση των κανόνων, πραγματοποιήσαμε έναν έλεγχο σε πραγματικό χρόνο για να βεβαιωθούμε ότι ο Gateway (VM1) μεταφέρει και μεταφράζει σωστά την κίνηση από το εσωτερικό δίκτυο προς το Διαδίκτυο.

Ο έλεγχος βασίστηκε στον συνδυασμό δύο ενεργειών σε διαφορετικά μηχανήματα:

- Στο VM2 (Client): Εκτελέσαμε την εντολή ping google.com. Το VM2 προσπάθησε να επικοινωνήσει με έναν εξωτερικό διακομιστή, στέλνοντας πακέτα ICMP. (Εικόνα 6)
- Στο VM1 (Gateway): Ταυτόχρονα, τρέξαμε την εντολή: sudo tcpdump -i eth0 icmp. (Εικόνα 7)



Εικόνα 6: VM2 ping google.com



Εικόνα 7: VM1 κίνηαη στην eth0

Όπως φαίνεται, η εντολή tcpdump κατέγραψε επιτυχώς την κίνηση στην εξωτερική κάρτα (eth0). Η ανάλυση της εξόδου μας δίνει δύο κρίσιμα συμπεράσματα:

- Επαλήθευση Forwarding: Το γεγονός ότι είδαμε πακέτα ICMP (Echo requests και Echo replies) στην eth0, ενώ αυτά ξεκίνησαν από το VM2, αποδεικνύει ότι ο Gateway προωθεί σωστά την κίνηση από την εσωτερική κάρτα (eth1) στην εξωτερική.
- Επαλήθευση NAT (Masquerading): Στην έξοδο του tcpdump παρατηρούμε ότι η IP που φαίνεται να στέλνει τα αιτήματα είναι η 10.0.2.15 (η IP του VM1) και όχι η 10.0.0.10 (η εσωτερική IP του VM2).

2.2.5 Οριστική αποθήκευση

Εκτελέσαμε την εντολή: sudo netfilter-persistent save.

Με αυτή την ενέργεια, οι κανόνες που δοκιμάσαμε αποθηκεύτικαν μόνιμα στο αρχείο /etc/iptables/rules.v4. Με την εντολή cat /etc/iptables/rules.v4, εμφανίσαμε το περιεχόμενο του αρχείου αποθήκευσης. Εκεί πιστοποιείται ότι οι κανόνες FORWARD και MASQUERADE έχουν εγγραφεί επιτυχώς. Πλέον, ακόμα και αν το VM1 υποστεί απώλεια ισχύος ή επανεκκίνηση, το δίκτυο θα επανέλθει αυτόματα στην ασφαλή και λειτουργική κατάσταση που ορίσαμε. (Εικόνα 8)

Εικόνα 8: Εφαρμογή και αποθήκευση κανόνων

2.3 Πολιτική ασφάλειας εσωτερικού δικτύου (ITZ)

Η υλοποίηση της πολιτικής ασφάλειας έγινε αποκλειστικά στον Gateway (VM1), ο οποίος ελέγχει την πρόσβαση του VM2 προς τον έξω κόσμο.

2.3.1 Ενεργοποίηση Loopback

Κάθε σύστημα Linux χρειάζεται να επικοινωνεί με τον εαυτό του για να λειτουργούν σωστά οι εσωτερικές του υπηρεσίες. Χωρίς αυτόν τον κανόνα, πολλές τοπικές διεργασίες του Gateway θα κατέρρεαν.

- `sudo iptables -A INPUT -i lo -j ACCEPT`

Επεξήγηση:

- **-A INPUT**: Προσθήκη (Append) του κανόνα στην αλυσίδα των εισερχομένων.

- **-i lo** (Interface Loopback): Η εικονική διεπαφή του ίδιου του υπολογιστή (localhost).
- **-j ACCEPT**: Ορίζει τον στόχο (Jump) ως αποδοχή. Επιτρέπουμε στο VM1 να "μιλάει" στον εαυτό του.

2.3.2 Διασφάλιση πρόσβασης στο διαδίκτυο (DNS & Web)

Για να μπορεί το VM2 (Εταιρικό δίκτυο) να λειτουργεί, πρέπει να μπορεί να μεταφράζει ονόματα (DNS) και να βλέπει ιστοσελίδες (HTTP/HTTPS).

Α. Υπηρεσία DNS

- `sudo iptables -A FORWARD -i eth1 -p udp --dport 53 -j ACCEPT`

Επεξήγηση:

- **-A FORWARD**: Αφορά την κίνηση που περνάει μέσα από το VM1.
- **-i eth1**: Το πακέτο έρχεται από το εσωτερικό δίκτυο (ITZ).
- **-p udp**: Το DNS χρησιμοποιεί το πρωτόκολλο UDP για γρήγορες ερωτήσεις.
- **--dport 53**: Η παγκόσμια θύρα (Port) για την υπηρεσία DNS.

Β. Υπηρεσίες Web (HTTP/HTTPS)

- `sudo iptables -A FORWARD -i eth1 -p tcp -m multiport --dports 80,443 -j ACCEPT`

Επεξήγηση:

- **-p tcp**: Το Web απαιτεί αξιόπιστη σύνδεση μέσω του πρωτοκόλλου TCP.
- **-m multiport**: Χρήση ενός πρόσθετου "module" που μας επιτρέπει να ορίσουμε πολλές θύρες μαζί.
- **--dports 80,443**: Οι θύρες για το απλό Web (80) και το κρυπτογραφημένο Web (443).

2.3.3 Καταγραφή και Έλεγχος (Logging)

Σύμφωνα με την απαίτηση της άσκησης για τη δημιουργία μιας πολιτικής "Log and Drop", υλοποιήσαμε δύο ξεχωριστούς κανόνες καταγραφής. Αυτό έγινε για να μπορούμε να διακρίνουμε αν μια ύποπτη δραστηριότητα προέρχεται από το εσωτερικό δίκτυο ή αν πρόκειται για εξωτερική επίθεση στον Gateway.

Α. Καταγραφή κάθε απόπειρας του εσωτερικού δικτύου (VM2) να επικοινωνήσει με το Internet μέσω μη εξουσιοδοτημένων θυρών (δηλαδή οτιδήποτε άλλο εκτός από DNS και HTTP/HTTPS)

- `sudo iptables -A FORWARD -i eth1 -j LOG --log-prefix "ITZ_SUSPICIOUS: " --log-level 4`

Επεξήγηση:

- **FORWARD:** Η αλυσίδα που ελέγχει τα πακέτα που διέρχονται από το VM1 (π.χ. από το VM2 προς το Internet).
- **LOG**: Ο Gateway κάνει μια εγγραφή στο αρχείο /var/log/syslog.
- **--log-prefix "ITZ_SUSPICIOUS: "**: Προσθέτει αυτό το κείμενο στην εγγραφή, ώστε να το βρίσκουμε εύκολα.
- **--log-level 4**: Ορίζει την κρισιμότητα της εγγραφής (επίπεδο Warning).

Β. Προσφέρει προστασία έναντι εξωτερικών απειλών, καθώς καταγράφει απόπειρες για hacking, brute-force επιθέσεις στο SSH ή σάρωση θυρών που στοχεύουν τον δρομολογητή της εταιρείας.

- `sudo iptables -A INPUT -j LOG --log-prefix "IN_ATTEMPT: " --log-level 4`

Επεξήγηση:

- **sudo iptables -A**: (Όπως παραπάνω) Προσθήκη κανόνα στο firewall.
- **INPUT:** Η αλυσίδα που ελέγχει τα πακέτα που έχουν ως τελικό προορισμό το ίδιο το VM1 (π.χ. κάποιος που προσπαθεί να συνδεθεί στο VM1 από το Internet).

- **--log-prefix "IN_ATTEMPT: ":** Προσθέτει αυτή την ετικέτα για να γνωρίζει ο διαχειριστής ότι κάποιος προσπαθεί να εισβάλει ή να επικοινωνήσει απευθείας με τον Gateway.
- **Απουσία του -i**: Επειδή δεν γράψαμε -i eth1, ο Gateway θα καταγράφει οτιδήποτε προσπαθεί να συνδεθεί πάνω του, είτε αυτό έρχεται από το Internet (eth0), είτε από το εσωτερικό δίκτυο (eth1)

Παρόλο που οι κύριες απαιτήσεις αφορούν το εσωτερικό δίκτυο (ITZ), κρίθηκε απαραίτητη η προσθήκη του κανόνα: sudo iptables -A INPUT -j LOG --log-prefix "IN_ATTEMPT: " --log-level 4. Η εντολή αυτή υλοποιήθηκε για προληπτικούς λόγους. Ο Gateway (VM1) αποτελεί το μοναδικό σημείο εισόδου για το δίκτυο ITZ. Εάν ένας επιτιθέμενος καταφέρει να παραβιάσει τον Gateway, θα αποκτήσει άμεση πρόσβαση και στους εσωτερικούς κόμβους (VM2, VM3). Συνεπώς, η καταγραφή κάθε ύποπτης απόπειρας προς τον ίδιο τον δρομολογητή είναι κρίσιμη, καθώς λειτουργεί ως ένα σύστημα έγκαιρης προειδοποίησης για επερχόμενη επίθεση στο ITZ.

Γ. Για κίνηση από Internet προς VM2

- `sudo iptables -A FORWARD -i eth0 -o eth1 -j LOG --log-prefix "FROM_NET_TO_VM2: " --log-level 4`

Επεξήγηση:

- **sudo iptables -A FORWARD**: Προσθέτει τον κανόνα στην αλυσίδα προώθησης. Αφορά πακέτα που ο Gateway (VM1) λαμβάνει για να τα στείλει κάπου αλλού.
- **-i eth0 (In-interface)**: Δηλώνει ότι το πακέτο μπαίνει από την κάρτα που είναι συνδεδεμένη στο Internet.
- **-o eth1 (Out-interface)**: Δηλώνει ότι το πακέτο προσπαθεί να βγει από την κάρτα που οδηγεί στο εσωτερικό δίκτυο (ITZ), όπου βρίσκεται το VM2.

2.3.4 Ενεργοποίηση Stateful Inspection

Κατά την εφαρμογή της πολιτικής καθολικής απαγόρευσης (Default DROP) στην αλυσίδα FORWARD, διαπιστώθηκε ότι παρόλο που επιτρέπονταν οι εξερχόμενες συνδέσεις από το εσωτερικό δίκτυο (ITZ) προς το Διαδίκτυο (DNS, HTTP, HTTPS), οι απαντήσεις των εξωτερικών διακομιστών απορρίπτονταν.

Αυτό συμβαίνει επειδή το firewall, χωρίς μηχανισμό παρακολούθησης συνδέσεων, λειτουργεί ως stateless φίλτρο. Δηλαδή δεν αναγνωρίζει ότι τα εισερχόμενα πακέτα αποτελούν απαντήσεις σε ήδη επιτρεπτές εξερχόμενες συνδέσεις.

Για τον λόγο αυτό ενεργοποιήθηκε μηχανισμός Stateful Inspection μέσω του υποσυστήματος conntrack του Netfilter:

- `sudo iptables -I FORWARD 1 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`

Επεξήγηση:

• -I FORWARD 1: Εισαγωγή του κανόνα στην πρώτη θέση της αλυσίδας FORWARD.
• -m conntrack: Χρήση του μηχανισμού παρακολούθησης συνδέσεων.
• --ctstate ESTABLISHED,RELATED: Επιτρέπει πακέτα που ανήκουν σε ήδη καθιερωμένες ή σχετιζόμενες συνδέσεις.
• -j ACCEPT: Αποδοχή των πακέτων.

Η τοποθέτηση του κανόνα στην πρώτη θέση είναι κρίσιμη, καθώς το iptables εφαρμόζει σειριακή αξιολόγηση (first-match logic). Με αυτόν τον τρόπο, οι νόμιμες απαντήσεις από το Διαδίκτυο προς το ITZ επιτρέπονται άμεσα, πριν ελεγχθούν από τους κανόνες καταγραφής και την τελική πολιτική DROP.

Με την προσθήκη αυτή, το firewall μετατρέπεται από stateless σε stateful, επιτρέποντας ασφαλή λειτουργία των εξερχόμενων υπηρεσιών χωρίς να παραβιάζεται η πολιτική “Log and Drop”.

2.3.5 Καθολική απαγόρευση

Αφού ολοκληρώσαμε τις ρυθμίσεις των επιμέρους υπηρεσιών, ενεργοποιήσαμε την τελική γραμμή άμυνας του Firewall.
Οι εντολές:

- `sudo iptables -P INPUT DROP`
- `sudo iptables -P FORWARD DROP`

Με την κίνηση αυτή, ορίσαμε ότι κάθε πακέτο που δεν ταιριάζει σε κάποιον από τους κανόνες ACCEPT που γράψαμε παραπάνω, απορρίπτεται αυτόματα.

2.4 Υλοποίηση πρόσβασης στον Web Server (DMZ - VM3)

Σε αυτό το στάδιο, υλοποιήσαμε τη φιλοξενία μιας υπηρεσίας Web στο VM3 (Kali) και ρυθμίσαμε τον Gateway ώστε να επιτρέπει την πρόσβαση σε αυτήν από το εξωτερικό δίκτυο.

2.4.1 Εγκατάσταση Apache

Η εγκατάσταση του Web Server στο VM3 πραγματοποιήθηκε σε συγκεκριμένο χρονικό σημείο για να διασφαλιστεί η λήψη των απαραίτητων πακέτων από τα αποθετήρια του Kali:

- Η εγκατάσταση έγινε αμέσως μετά την ενεργοποίηση του NAT (Masquerade) στον Gateway, αλλά πριν την επιβολή της αυστηρής πολιτικής FORWARD DROP. Με αυτόν τον τρόπο, το VM3 είχε προσωρινά πλήρη πρόσβαση στο Διαδίκτυο για να επικοινωνήσει με τα Kali Rolling Repositories.
- Εκτέλεση στο VM3: 1. sudo apt update: Συγχρονισμός με τους servers του Kali. 2. sudo apt install apache2 -y: Εγκατάσταση του Apache. 3. sudo systemctl start apache2: Εκκίνηση της υπηρεσίας.

2.4.2 Παραμετροποίηση του Gateway

Με τον Web Server ενεργό στο VM3, προχωρήσαμε στη ρύθμιση του Gateway (VM1) χρησιμοποιώντας το εργαλείο iptables. Οι εντολές εκτελέστηκαν με την εξής σειρά:

A. Destination NAT (DNAT)

- `sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.1.0.10:80`

Επεξήγηση:

Η εντολή αυτή λέει στον Gateway ότι οποιοδήποτε πακέτο φτάνει από το Internet (-i eth0) και ζητάει τη θύρα 80, πρέπει να “μεταφραστεί” και να προωθηθεί στην

εσωτερική IP του VM3 (10.1.0.10). Η αλλαγή αυτή συμβαίνει στο στάδιο PREROUTING, δηλαδή πριν το λειτουργικό σύστημα αποφασίσει για την πορεία του πακέτου.

B. Forward ACCEPT (Stateful)

• `sudo iptables -I FORWARD 2 -i eth0 -o eth2 -p tcp -d 10.1.0.10 --dport 80 -m conntrack --ctstate NEW -j ACCEPT`

Επεξήγηση:

Εφόσον έχουμε επιβάλει γενική απαγόρευση (FORWARD DROP), το πακέτο που προορίζεται για το VM3 θα κοβόταν. Με αυτή την εντολή, δημιουργούμε μια εξαίρεση αποκλειστικά για νέες (NEW) TCP συνδέσεις από το εξωτερικό δίκτυο (eth0) προς το DMZ (eth2) και τη θύρα 80 του Web Server.

Η χρήση του μηχανισμού conntrack διασφαλίζει ότι επιτρέπονται μόνο νέες συνδέσεις προς την υπηρεσία HTTP, ενώ οι απαντήσεις του Web Server επιτρέπονται μέσω του κανόνα ESTABLISHED,RELATED που έχει ήδη οριστεί στην κορυφή της αλυσίδας FORWARD.

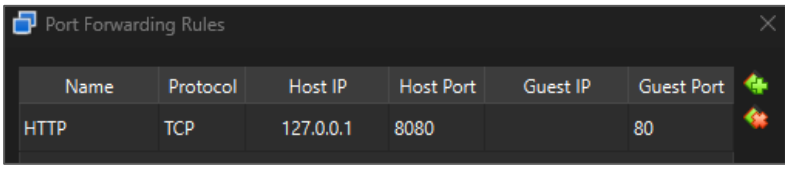
Οποιαδήποτε άλλη προσπάθεια επικοινωνίας με το VM3 (π.χ. SSH στη θύρα 22) απορρίπτεται αυτόματα από την προεπιλεγμένη πολιτική.

2.4.3 Δοκιμή μέσω Windows Host

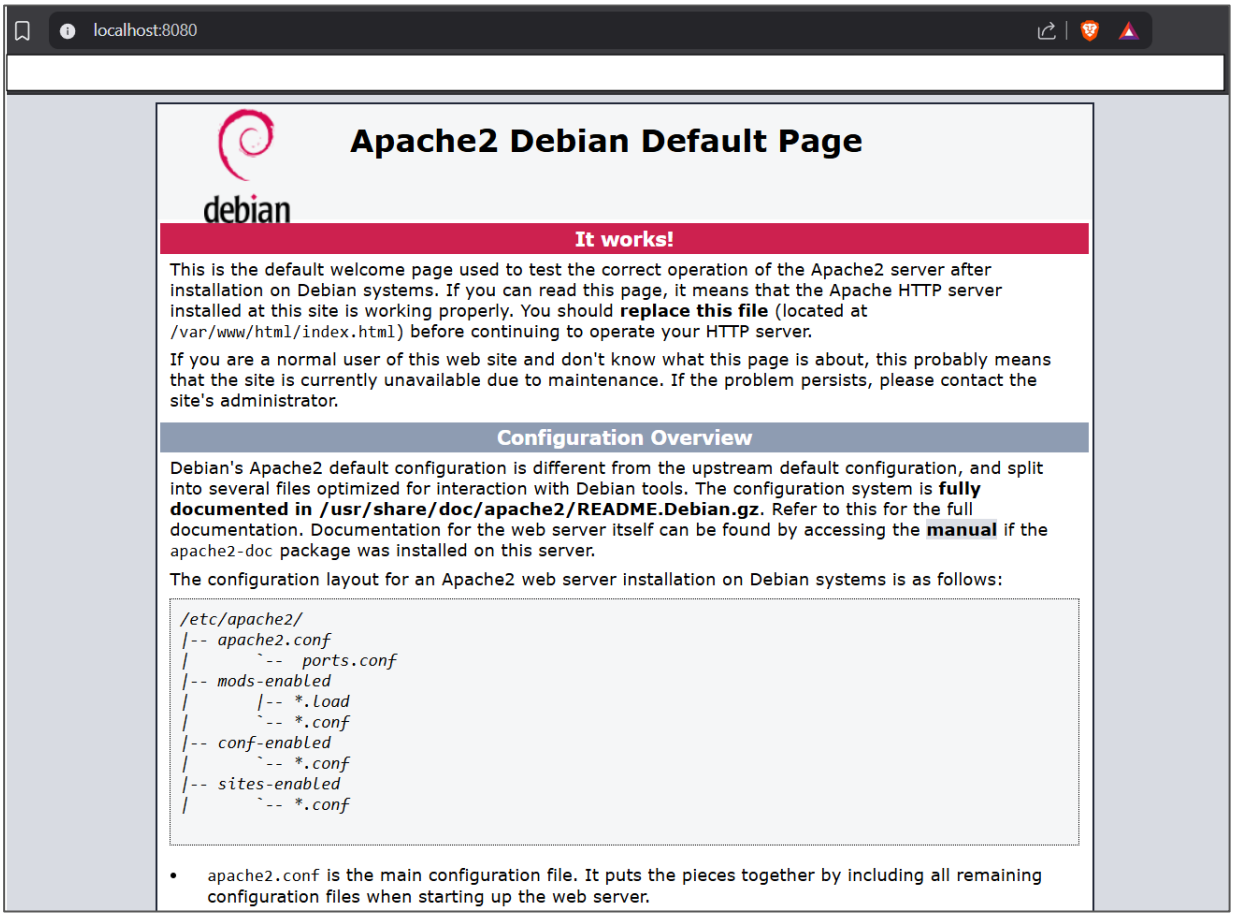
Για την επαλήθευση της σωστής λειτουργίας, χρησιμοποιήσαμε τον φυσικό υπολογιστή (Windows Host) ως εξωτερικό χρήστη:

- VirtualBox Port Forwarding: Στις ρυθμίσεις του VM1 (Network -> Port Forwarding), αντιστοιχίσαμε τη θύρα 8080 του Host με τη θύρα 80 του Guest (VM1). (Εικόνα 9)

- Τελικός Έλεγχος: Ανοίγοντας έναν browser στα Windows και πληκτρολογώντας http://127.0.0.1:8080, η σελίδα "Apache2 Kali Linux Default Page" εμφανίστηκε επιτυχώς. (Εικόνα 10)



Εικόνα 9: Ρύθμιση port forwarding στο VirtualBox για VM1



Εικόνα 10: Εμφάνιση Apache στον browser του Windows Host

2.5 Αυτόματη φόρτωση κανόνων Firewall

Για την υλοποίηση της αυτόματης εκκίνησης των κανόνων, χρησιμοποιήθηκε το εργαλείο netfilter-persistent. Όπως προαναφέρθηκε, το συγκεκριμένο εργαλείο είχε εγκατασταθεί στον Gateway από την έναρξη της εργαστηριακής άσκησης, ώστε να διασφαλίζεται η μόνιμη αποθήκευση κάθε νέου κανόνα που προστίθετο σταδιακά.

- Διαδικασία: Σε κάθε κρίσιμο στάδιο της παραμετροποίησης (π.χ. μετά την εφαρμογή του NAT ή των κανόνων πρόσβασης στο DMZ), εκτελούσαμε την εντολή: sudo netfilter-persistent save

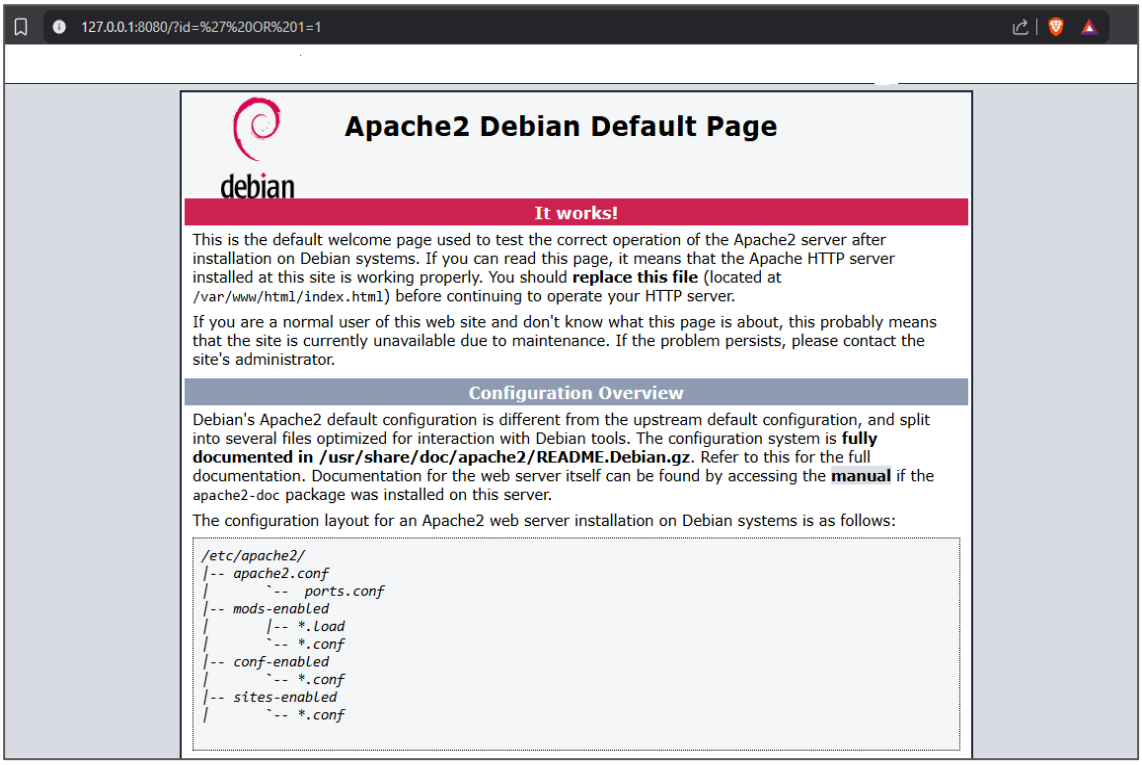
- Μηχανισμός: Η εντολή αυτή παγώνει την τρέχουσα κατάσταση των κανόνων από τη μνήμη και την εγγράφει στο αρχείο ρυθμίσεων του συστήματος. Με αυτόν τον τρόπο, σε κάθε επανεκκίνηση (reboot) του Kali Linux, οι κανόνες φορτώνονται αυτόματα πριν ξεκινήσει η διακίνηση δεδομένων στο δίκτυο.

2.6 Υλοποίηση Web Application Firewall (WAF)

Για την ενίσχυση της ασφάλειας του Web Server που βρίσκεται στο DMZ (VM3), υλοποιήθηκε Web Application Firewall (WAF) με τη χρήση του **ModSecurity** σε συνδυασμό με το **OWASP Core Rule Set (CRS)**.

Στόχος ήταν η προστασία του Web Server από επιθέσεις επιπέδου εφαρμογής (Layer 7), όπως SQL Injection, Cross-Site Scripting (XSS) και άλλες κακόβουλες εισαγωγές δεδομένων.

Προτού προχωρήσει η εγκατάσταση, έγινε δοκιμή SQL injection από τον windows host με url: http://127.0.0.1:8080/?id=' OR 1=1 και πράγματι όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 11) ανοίγει κανονικά την σελίδα "Apache2 Kali Linux Default Page" γεγονός που πρέπει απαγορευτεί.



Εικόνα 11: Επιτυχής εμφάνιση σελίδας με sql injection

2.6.1 Εγκατάσταση ModSecurity και CRS

Η εγκατάσταση πραγματοποιήθηκε στο VM3 (Web Server) με τις εντολές:

- `sudo apt update`
- `sudo apt install libapache2-mod-security2 modsecurity-crs -y`

Στη συνέχεια ενεργοποιήθηκε ο μηχανισμός επιβολής κανόνων (Enforcement Mode) τροποποιώντας το αρχείο:

- `/etc/modsecurity/modsecurity.conf`

και αλλάζοντας την παράμετρο:

- `SecRuleEngine DetectionOnly`

σε :

- `SecRuleEngine On`

Για τη σωστή λειτουργία του CRS με το αρχείο ρυθμίσεων:

- `/etc/modsecurity/crs/crs-setup.conf`

έγινε σύνδεση των κανόνων του CRS μέσω του αρχείου:

- `/etc/apache2/mods-enabled/security2.conf`

με τη γραμμή:

- `IncludeOptional /usr/share/modsecurity-crs/*.load`

Τέλος, πραγματοποιήθηκε επανεκκίνηση του Apache:

- `sudo systemctl restart apache2`

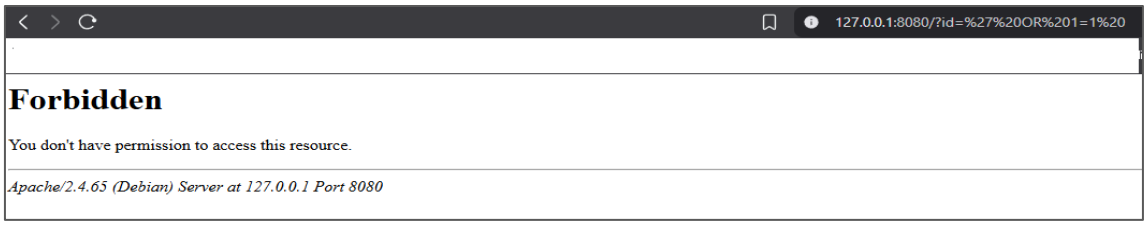
2.6.2 Δοκιμή λειτουργίας WAF

Για την επαλήθευση της σωστής λειτουργίας του WAF πραγματοποιήθηκε ελεγχόμενη δοκιμή SQL Injection μέσω του browser από τον windows host όπως παραπάνω.

Η δοκιμή έγινε με την ακόλουθη URL:

- `http://127.0.0.1:8080/?id=' OR 1=1`

Κατά τη δοκιμή με κακόβουλο URL, το αίτημα δεν εκτελέστηκε κανονικά, αλλά διακόπηκε από το Web Application Firewall. (Εικόνα 12)

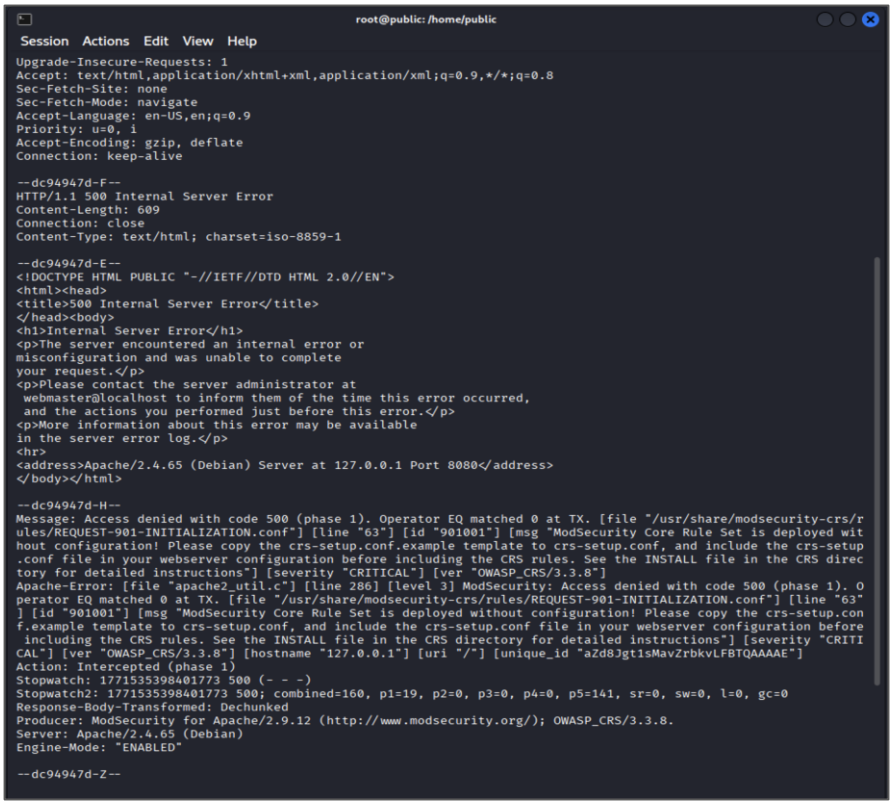


Εικόνα 12: Αποτυχημένη δοκιμή sql injection

Επιπλέον και όπως φαίνεται παρακάτω (Εικόνα 13) με την εντολή

- `sudo tail -f /var/log/apache2/modsec_audit.log`

ο server επέστρεψε σφάλμα HTTP 500, γεγονός που δείχνει ότι το ModSecurity εντόπισε ύποπτη είσοδο και μπλόκαρε το αίτημα πριν αυτό φτάσει στην εφαρμογή.



Εικόνα 13: Σφάλμα http 500 από webserver

Η καταγραφή που εμφανίζεται επιβεβαιώνει ότι οι κανόνες του OWASP CRS είναι ενεργοί και εφαρμόζονται κανονικά.Η συμπεριφορά αυτή αποδεικνύει ότι ο Web Server προστατεύεται από κακόβουλες προσπάθειες εκμετάλλευσης μέσω URL.

3 Επαλήθευση κανόνων

3.1 Ενδοδικτυακή επικοινωνία

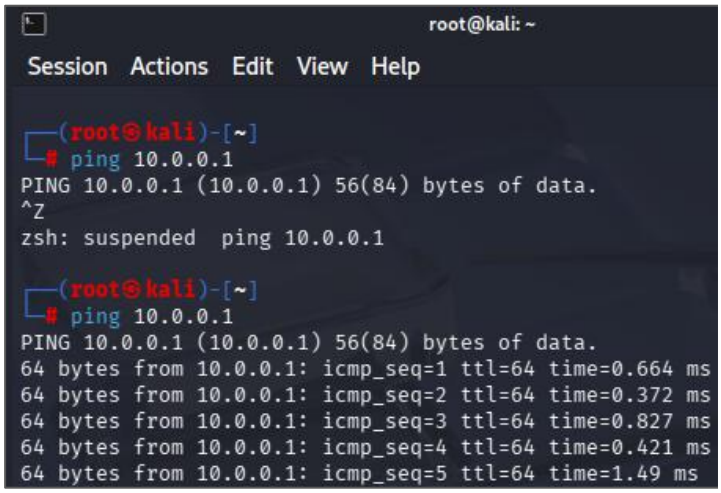
Σύμφωνα με την απαίτηση (1), πρέπει τα VM1 και VM2 να επικοινωνούν μεταξύ τους.

Από το τερματικό του VM2, εκτελούμε ping 10.0.0.1 (διεύθυνση του Gateway).

Το ping αποτυγχάνει (Εικόνα 14) λόγω της πολιτικής INPUT DROP στον Gateway, και έτσι πρέπει να προστεθεί ο κανόνας:

- `sudo iptables -A INPUT -p icmp -s 10.0.0.10 -j ACCEPT`

Η εντολή εκτελείται στον Gateway και όπου 10.0.10 είναι η ip του VM2. Έπειτα επαναλμβάνουμε την δοκιμή και πραγματοποιείται επιτυχως η επικοινωνία. (Εικόνα 14)



Εικόνα 14: Αποτυχής και έπειτα επιτυχής επικοινωνία

3.2 Κίνηση DNS και εξερχόμενη κίνηση HTTP/HTTPS

Ανάλυση Ονομάτων (DNS):

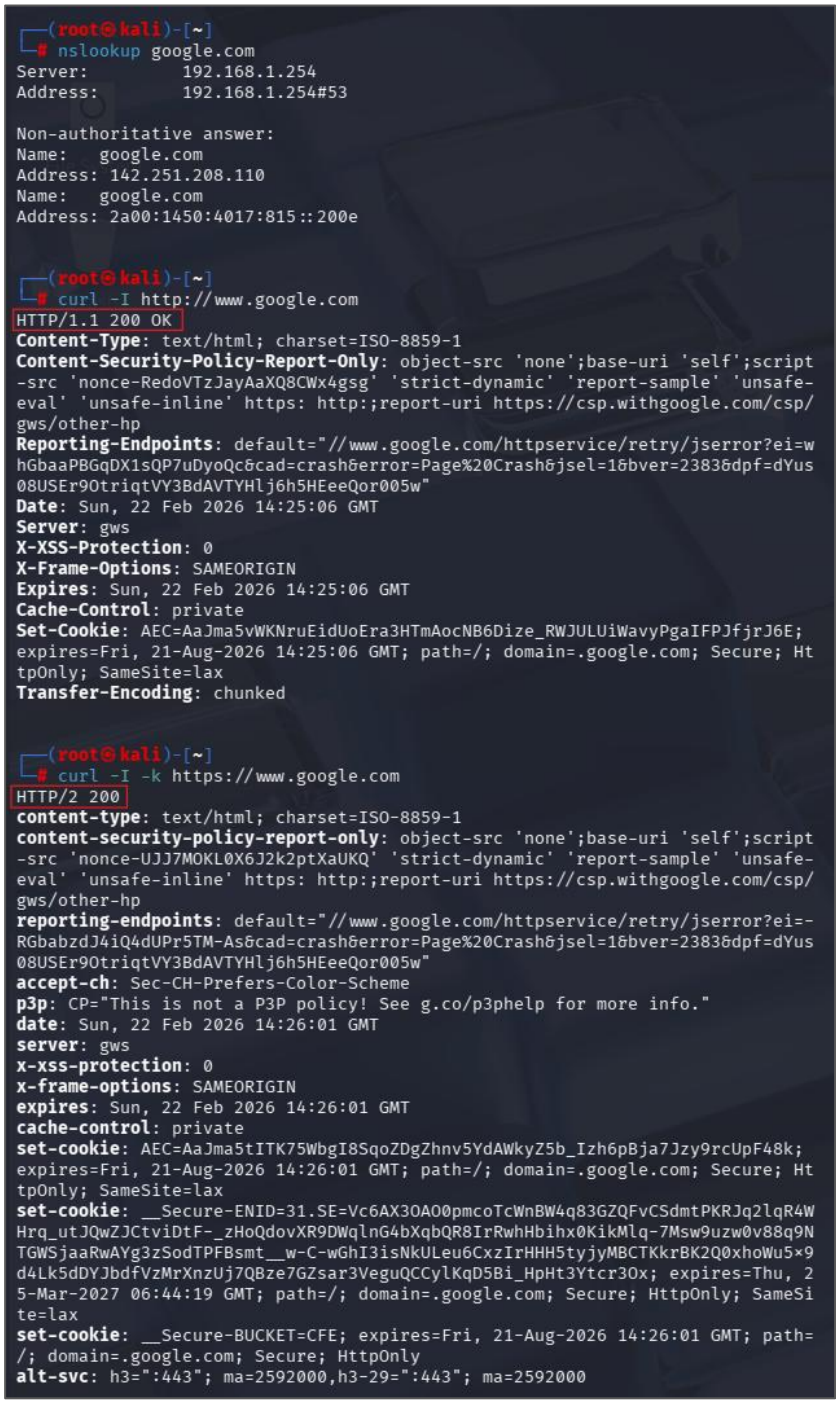
Χρησιμοποιήθηκε η εντολή nslookup google.com. Η επιτυχής επιστροφή της IP διεύθυνσης επιβεβαιώνει ότι οι κανόνες στην αλυσίδα FORWARD για τη θύρα 53 (UDP/TCP) λειτουργούν σωστά. (Εικόνα 15)

Πρωτόκολλο HTTP (Port 80):

Εκτελέστηκε η εντολή curl -I http://www.google.com. Η λήψη της απόκρισης **HTTP/1.1 200 OK** αποδεικνύει ότι ο Gateway επιτρέπει την έξοδο στη θύρα 80 και πραγματοποιεί επιτυχώς τη μετάφραση διευθύνσεων (NAT/Masquerade). (Εικόνα 15)

Πρωτόκολλο HTTPS (Port 443):

Εκτελέστηκε η εντολή curl -I -k https://www.google.com. Η επιτυχής ολοκλήρωση της σύνδεσης επιβεβαιώνει τη λειτουργία του κανόνα για τη θύρα 443. Η παράμετρος -k χρησιμοποιήθηκε για την παράκαμψη τυχόν σφαλμάτων πιστοποιητικών στο εργαστηριακό περιβάλλον, εστιάζοντας αποκλειστικά στη συνδεσιμότητα. (Εικόνα 15)



Εικόνα 15: Κίνηση DNS και εξερχόμενη κίνηση HTTP/HTTPS

3.3 Loopback

Η πολιτική ασφάλειας που υλοποιήθηκε στον Gateway (VM1) περιλαμβάνει ρητό κανόνα που επιτρέπει την κίνηση στη διεπαφή loopback (lo). Η διεπαφή αυτή είναι εικονική και χρησιμοποιείται από το λειτουργικό σύστημα για την επικοινωνία μεταξύ εσωτερικών διεργασιών στην τοπική διεύθυνση 127.0.0.1.

Διαδικασία Επαλήθευσης στο ITZ (VM2)
Για να επιβεβαιωθεί ότι οι περιοριστικοί κανόνες του firewall δεν επηρεάζουν την εσωτερική λειτουργία του συστήματος, εκτελέστηκε η παρακάτω δοκιμή στο VM2:

Εντολή:

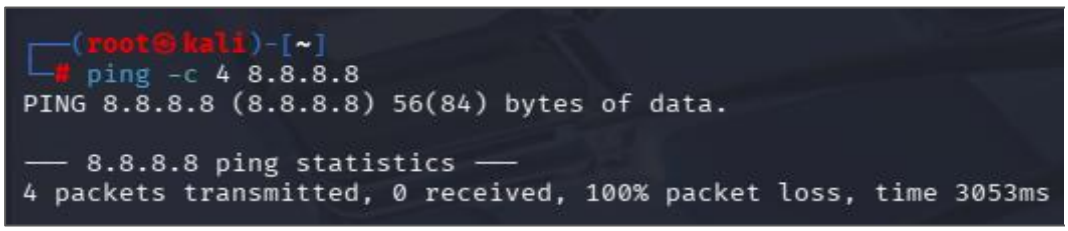
- `ping -c 4 127.0.0.1`

Παράμετρος -c 4: Χρησιμοποιήθηκε για τον περιορισμό της δοκιμής σε τέσσερα πακέτα, επιτρέποντας την αυτόματη εξαγωγή στατιστικών στοιχείων.

3.4 Καταγραφή και απόρριψη ύποπτης κίνησης (Logging)

Σύμφωνα με την πολιτική ασφάλειας του εσωτερικού δικτύου (ITZ), κάθε πακέτο που δεν επιτρέπεται ρητά από τους κανόνες (DNS, HTTP, HTTPS) πρέπει να καταγράφεται και στη συνέχεια να απορρίπτεται. Η διαδικασία αυτή υλοποιήθηκε μέσω του μηχανισμού Logging του iptables στον Gateway (VM1).

Για να επιβεβαιωθεί η λειτουργία, εκτελέστηκε από το VM2 κίνηση που παραβιάζει την πολιτική (π.χ. ping 8.8.8.8) (Εικόνα 16) . Καθώς το πρωτόκολλο ICMP δεν



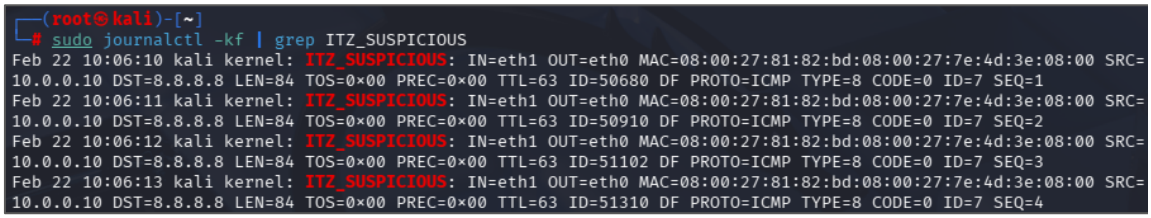
Εικόνα 16: ping 8.8.8.8 από VM2

περιλαμβάνεται στις εξουσιοδοτημένες υπηρεσίες, το πακέτο προωθήθηκε στον κανόνα Logging.
Η ανάκτηση των δεδομένων έγινε στον Gateway (Εικόνα 17) με την εντολή:

- `sudo journalctl -k | grep ITZ_SUSPICIOUS`

Τα αποτελέσματα επιβεβαίωσαν την ορθή λειτουργία, καθώς καταγράφηκαν τα εξής στοιχεία:

- Source (SRC): 10.0.0.10 (Η IP του VM2 που επιχείρησε την κίνηση).
- Protocol (PROTO): ICMP (Το πρωτόκολλο που μπλοκαρίστηκε).
- Action: Το πακέτο καταγράφηκε και στη συνέχεια απορρίφθηκε από το Default DROP της αλυσίδας

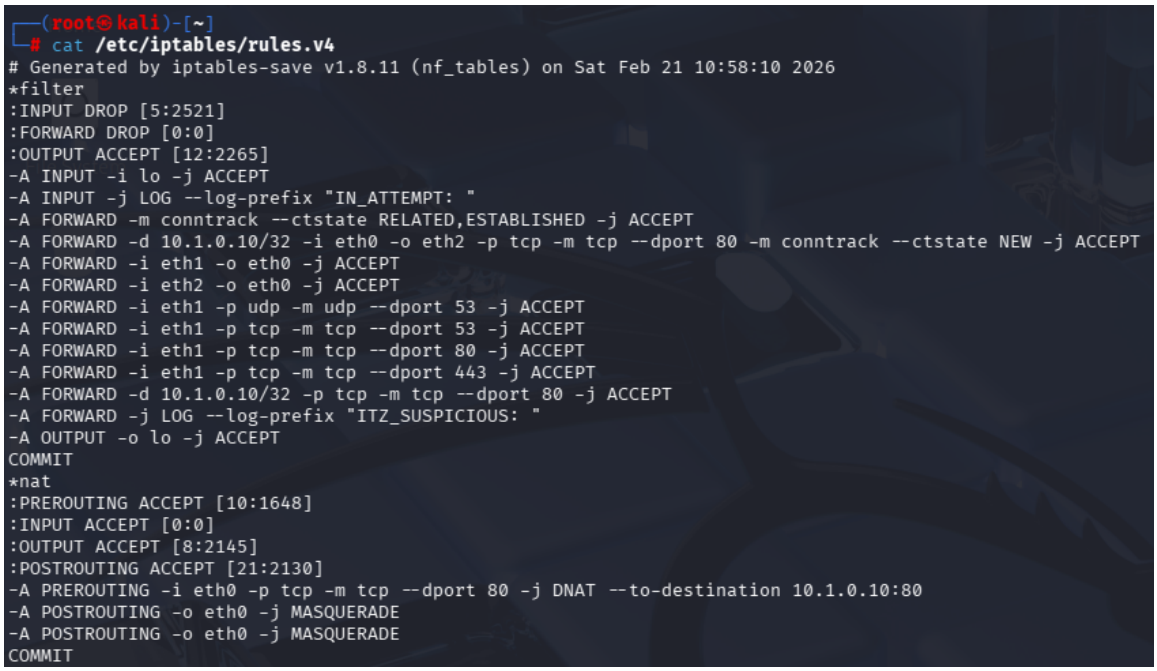


Εικόνα 17: Καταγραφή κίνησης από τον Gateway

Επισημαίνεται ότι όλοι οι υπόλοιποι κανόνες που περιγράφονται στο ερώτημα 2 επαληθεύθηκαν επιτυχώς κατά τη διάρκεια της υλοποίησής τους στα προηγούμενα στάδια.

3.4 Τελική κατάσταση αρχείου ρυθμίσεων

Η τελική μορφή του αρχείου /etc/iptables/rules.v4, όπως διαμορφώθηκε μετά την ολοκλήρωση όλων των βημάτων της άσκησης. (Εικόνα 18)



Εικόνα 18: Τελική κατάσταση αρχείου ρυθμίσεων

4 Δοκιμή επιθέσεων και υλοποίηση κανόνων αποτροπής

Στο βήμα αυτό πραγματοποιήθηκε δοκιμή επίθεσης δικτύου τύπου **DoS (SYN Flood)** προς τον Web Server (VM3), και στη συνέχεια υλοποιήθηκαν κανόνες στο firewall του Gateway (VM1) για την αποτροπή της.

4.1 Υλοποίηση επίθεσης (SYN Flood με hping3)

Για την προσομοίωση επίθεσης χρησιμοποιήθηκε το εργαλείο **hping3**, το οποίο επιτρέπει τη δημιουργία μεγάλου αριθμού TCP πακέτων με καθορισμένες σημαίες (flags).

Η επίθεση στόχευσε τη δημοσιευμένη HTTP υπηρεσία του Web Server (VM3), μέσω της εξωτερικής διεπαφής του Gateway.

Εντολή επίθεσης:

- `hping3 -S --flood -p 80 <IP_Gateway>`

Επεξήγηση:

- **-S**: ενεργοποιεί το SYN flag, δηλαδή την αρχική φάση δημιουργίας νέας TCP σύνδεσης.
- **--flood**: αποστέλλει πακέτα με τη μέγιστη δυνατή ταχύτητα.
- **-p 80**: στοχεύει τη θύρα HTTP.
- **<IP_Gateway>**: η εξωτερική IP του Gateway (VM1), μέσω της οποίας γίνεται προώθηση (DNAT) προς τον Web Server (VM3).

Κατά την εκτέλεση της επίθεσης παρατηρήθηκε αυξημένος αριθμός νέων TCP αιτημάτων προς τον Web Server, με αποτέλεσμα καθυστέρηση ή προσωρινή αδυναμία εξυπηρέτησης νόμιμων αιτημάτων.

4.2 Υλοποίηση κανόνων αποτροπής στο firewall (VM1)

Για την αντιμετώπιση της επίθεσης, προστέθηκαν δύο διαδοχικοί κανόνες στην αλυσίδα **FORWARD** του Gateway. Οι κανόνες αυτοί περιορίζουν τον ρυθμό νέων TCP συνδέσεων προς τη θύρα 80 του Web Server.

Οι κανόνες τοποθετήθηκαν αμέσως μετά τον κανόνα RELATED,ESTABLISHED, ώστε να διασφαλίζεται πρώτα η κανονική λειτουργία των ήδη εγκατεστημένων συνδέσεων.

Α. Περιορισμός ρυθμού νέων SYN πακέτων

Εντολή:

- `sudo iptables -I FORWARD 2 -i eth0 -o eth2 -p tcp -d 10.1.0.10 --dport 80 --syn -m limit --limit 20/second --limit-burst 40 -j ACCEPT`

Επεξήγηση:

- **-I FORWARD 2**: εισαγωγή του κανόνα στη δεύτερη θέση της αλυσίδας FORWARD.
- **-i eth0 -o eth2**: αφορά αποκλειστικά κίνηση από το εξωτερικό δίκτυο προς το DMZ.
- **-d 10.1.0.10 --dport 80**: στοχεύει τον Web Server στη θύρα HTTP.

- **--syn**: φιλτράρει μόνο νέα TCP αιτήματα σύνδεσης.
- **-m limit --limit 20/second --limit-burst 40**: επιτρέπει έως 20 νέα SYN ανά δευτερόλεπτο (με προσωρινή αιχμή έως 40).
- **-j ACCEPT**: επιτρέπει την κίνηση που βρίσκεται εντός των επιτρεπτών ορίων.

Με τον κανόνα αυτό διασφαλίζεται ότι η κανονική χρήση της υπηρεσίας δεν επηρεάζεται, ενώ περιορίζεται η υπερβολική δημιουργία νέων συνδέσεων.

Β. Απόρριψη υπερβολικών νέων συνδέσεων

Εντολή:

- `sudo iptables -I FORWARD 3 -i eth0 -o eth2 -p tcp -d 10.1.0.10 --dport 80 --syn -j DROP`

Επεξήγηση:

Ο κανόνας αυτός απορρίπτει όλα τα SYN πακέτα που υπερβαίνουν το όριο του προηγούμενου κανόνα.

Εφόσον ένα SYN δεν έγινε δεκτό από τον κανόνα περιορισμού ρυθμού, θεωρείται ύποπτο και απορρίπτεται. Με τον τρόπο αυτό αποτρέπεται η μαζική δημιουργία νέων TCP συνδέσεων, η οποία αποτελεί βασικό χαρακτηριστικό επιθέσεων τύπου SYN Flood.

4.3 Επαλήθευση λειτουργίας

Η ορθή τοποθέτηση και λειτουργία των κανόνων επιβεβαιώθηκε με την εντολή:

- `sudo iptables -L FORWARD -n -v`

Κατά την εκτέλεση της επίθεσης παρατηρήθηκε αύξηση στους μετρητές (counters) του κανόνα DROP, γεγονός που επιβεβαιώνει ότι η επιθετική κίνηση απορρίπτεται από το firewall, ενώ τα νόμιμα αιτήματα συνεχίζουν να εξυπηρετούνται κανονικά.

Με την υλοποίηση των παραπάνω κανόνων επιτεύχθηκε βασική προστασία έναντι επιθέσεων τύπου SYN Flood, χωρίς να διαταράσσεται η κανονική λειτουργία της δημοσιευμένης HTTP υπηρεσίας.