Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

1η Εργασία
Ονοματεπώνυμο: Αγησίλαος Κολλιόπουλος
Αριθμός Μητρώου: 1072803
Τμήμα: ΗΜΤΥ

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

Απαντήστε στις παρακάτω ερωτήσεις κατανόησης:

1. Στα σύγχρονα δίκτυα υψηλής ταχύτητας, μπορεί να πραγματοποιηθεί φιλτράρισμα πακέτων μόνο εάν η υποστήριξη TCP / IP πακέτα είναι ενσωματωμένη απευθείας στο λειτουργικό σύστημα μιας μηχανής. Γιατί;

   Η υποστήριξη TCP/IP ενσωματώνεται στον πυρήνα του λειτουργικού συστήματος ώστε να γίνεται αποδοτικότερο το φιλτράρισμα των TCP/IP πακέτων. Αυτό συμβαίνει διότι ο πυρήνας του λειτουργικού έχει ”άμεση” επικοινωνία με την κάρτα δικτύου στην οποία φτάνουν τα πακέτα. Αντίθετα, αν το φιλτράρισμα των πακέτων γινόταν από μία εφαρμογή επιπέδου χρήστη, θα έπρεπε το σύστημα να προωθεί το πακέτο στην εν λόγω εφαρμογή και στην συνέχεια να εφαρμόσει ό,τι απαιτήσει η εφαρμογή, εισάγοντας έτσι μια σημαντική καθυστέρηση στο φιλτράρισμα του πακέτου. Γενικά, η ενσωμάτωση της υποστήριξης TCP / IP στο λειτουργικό σύστημα προσφέρει απόδοση, ασφάλεια και ευκολότερη διαχείριση για τα δίκτυα υψηλής ταχύτητας.

2. Ποια είναι η διαφορά μεταξύ ενός τείχους προστασίας φιλτραρίσματος πακέτων και ενός τείχος προστασίας διακομιστή μεσολάβησης; Μπορούν τα δύο να χρησιμοποιηθούν μαζί;

   Το τείχος προστασίας διακομιστή μεσολάβησης αποτελεί ένα ενδιάμεσο επίπεδο μεταξύ του εσωτερικού και του εξωτερικού δικτύου, καθώς ελέγχει τα πακέτα που προορίζονται για το εσωτερικό δίκτυο προτού αυτά φτάσουν στον προορισμό τους. Αντίθετα, ένα τείχος προστασίας φιλτραρίσματος πακέτων βρίσκεται εντός του εσωτερικού δικτύου. Επίσης, τα proxy firewalls μπορούν να ελέγξουν και το περιεχόμενο ενός πακέτου, σε αντίθεση με τα packet firewalls που ελέγχουν μόνο το header του πακέτου. Έτσι, μπορούν να προσφέρουν περισσότερη ασφάλεια στο εσωτερικό δίκτυο με αντάλλαγμα την χρονική καθυστέρηση που επιβάλλουν στην άφιξη του πακέτου στο εσωτερικό δίκτυο. Οι δύο αυτοί τύποι τειχών προστασίας είναι δυνατό και θεμιτό να συνδυαστούν.

3. Ποιοι είναι οι τέσσερις πίνακες που διατηρούνται από τον πυρήνα Linux για την επεξεργασία εισερχόμενων και εξερχόμενων πακέτων;

   filter, mangle, nat, raw.

4. Πώς αποφασίζει ένα τείχος προστασίας που χρησιμοποιεί iptables ως προς το ποια πακέτα θα προωθήσει στην INPUT αλυσίδα κανόνων, ποια στην αλυσίδα FORWARD και ποια στην αλυσίδα OUTPUT. Επιπλέον, ποιο μέρος ενός πακέτου εξετάζεται για αντιληφθεί εάν το πακέτο εμπίπτει ή όχι σε κάποια στη συνθήκη μιας εντολής των παραπάνω αλυσίδων?

Το firewall αποφασίζει ποια είναι η κατάλληλη αλυσίδα κανόνων βάσει τον προορισμό του πακέτου. Πιο συγκεκριμένα, αν ένα πακέτο εισέρχεται στον υπολογιστή, ακολουθούνται οι κανόνες της αλυσίδας INPUT. Όταν ένα πακέτο εξέρχεται από τον υπολογιστή χρησιμοποιείται η αλυσίδα OUTPUT, ενώ όταν ένα πακέτο προωθείται εντός του υπολογιστή χρησιμοποιείται η αλυσίδα FORWARD. Για την επιλογή της αλυσίδας, το firewall εξετάζει το header του πακέτου για IP διευθύνσεις, θύρες προέλευσης/προορισμού κ.α.

5. Καθώς ένα πακέτο υποβάλλεται σε επεξεργασία από μια αλυσίδα κανόνων, τι συμβαίνει στο πακέτο εάν δεν πληροί τις προϋποθέσεις των κανόνων; Τι σημαίνει πολιτική αλυσίδας;

   Όταν ένα πακέτο δεν πληροί τις προϋποθέσεις ενός κανόνα, αυτό προωθείται για έλεγχο από τον επόμενο κανόνα. Αν δεν πληροί ούτε τις προϋποθέσεις του τελευταίου κανόνα, τότε εκτελείται η ενέργεια που καθορίζει η πολιτική της αλυσίδας. Πολιτική αλυσίδας ουσιαστικά σημαίνει μια προεπιλεγμένη ενέργεια που θα εκτελεστεί όταν ένα πακέτο ελεγχθεί από όλους τους κανόνες της αλυσίδας και δεν πληροί τις προϋποθέσεις κανενός από αυτών (ώστε να εκτελεστεί η ενέργεια που καθορίζει κάποιος κανόνας).

6. Δείξτε πώς θα χρησιμοποιήσετε την εντολή iptables για να απορρίψετε όλα εισερχόμενα πακέτα SYN που προσπαθούν να ανοίξουν μια νέα σύνδεση με το μηχάνημά σας;

   iptables -A INPUT -p tcp -m tcp --syn -j DROP

7. Ποια είναι η επιλογή που δίνεται στην εντολή iptables να αρχικοποιήσει (flush) όλες τις αλυσίδες που ορίζονται από τον χρήστη σε έναν πίνακα; Πώς αρχικοποιούνται όλοι οι κανόνες σε έναν πίνακα;

   Είναι η επιλογή --flush, -F. Η αρχικοποίηση γίνεται με την παρακάτω εντολή:

   iptables -F -t <TABLE NAME>, όπου **TABLE NAME**: {filter, mangle, nat, raw}

8. Εάν δείτε τη συμβολοσειρά «icmp type 255» στο τέλος μιας γραμμής που παράγεται από την έξοδος της εντολής «iptables -L», τι σημαίνει αυτό?

   Σημαίνει ότι ο κανόνας που βρίσκεται σε αυτήν την σειρά αφορά ICMP μήνυμα οποιουδήποτε τύπου. (χρησιμοποιείται ως “wildcard”)

9. Ποιοι είναι οι τύποι icmp που σχετίζονται με το echo-request (ping) και με τα πακέτα echo-reply (pong);

   Είναι οι τύποι 0 (echo-reply) και 8 (echo-request)

10. Ο αρχικός (raw) πίνακας χρησιμοποιείται για τον καθορισμό εξαιρέσεων από τη παρακολούθηση της σύνδεση (connection tracking). Τι σημαίνει αυτό?

    Σημαίνει ότι ο πίνακας raw εκμεταλλευόμενος την προτεραιότητά του σε σχέση με το

conntrack είναι σε θέση να αποκλείσει κάποια πακέτα έτσι ώστε αυτά να εξαιρεθούν από το connection tracking. Αυτό χρησιμεύει σε περιπτώσεις όπου υπάρχει πολλή κίνηση σε ένα router και είναι επιθυμητή η αποσυμφόρησή του ή όταν θέλουμε να χειριστούμε συγκεκριμένα πακέτα διαφορετικά.

11. Ποια είναι η εντολή iptables εάν θέλετε ο server σας, να αποδέχεται εισερχόμενα αιτήματα σύνδεσης για τον sshd διακομιστή και να απορρίπτει όλα τα άλλα πακέτα αιτήματος σύνδεσης από απομακρυσμένους πελάτες.

    iptables -A INPUT -p tcp ! --destination-port 22 -j DROP

12. Τι είναι η παρακολούθηση σύνδεσης (connection tracking); Πώς ένα firewall που χρησιμοποιεί τα iptables γνωρίζει ότι όλα τα εισερχόμενα πακέτα ανήκουν στην ίδια συνεχιζόμενη σύνδεση;

    Είναι μια μέθοδος του iptables(μεταξύ άλλων) που αποθηκεύει τις εισερχόμενες συνδέσεις σε έναν πίνακα ούτως ώστε να μπορούν οι διαχειριστές του συστήματος να τις ελέγξουν βάσει της κατάστασης στην οποία ανήκουν. Το firewall είναι σε θέση να γνωρίζει ποια πακέτα σχετίζονται με την ίδια σύνδεση μέσω των καταστάσεων established, related, που αποδίδονται από το conntrack.

13. Ποιες είναι οι διαφορετικές καταστάσεις πακέτων που αναγνωρίζονται από την κατάσταση της σύνδεσης (connection tracking) του iptables;

    NEW, ESTABLISHED, RELATED, INVALID

14. Μελετήστε το παράδειγμα χρήσης iptables για χρήση στον προσωπικό σας υπολογιστή και υιοθετήστε το στην εικονική μηχανή που τρέχει debian που έχετε δημιουργήσει. Ρυθμίστε την εικονική σας μηχανή να τα χρησιμοποιεί/υλοποιεί κάθε φορά που εκκινεί.

    Για να μπορέσουμε να κάνουμε την εικονική μας μηχανή να χρησιμοποιεί τους κανόνες που θέλουμε να θέσουμε, χρησιμοποιούμε το αρχείο rc.local (Full path: /etc/rc.local), το οποίο κάνουμε executable και τρέχει αυτόματα κάθε φορά που κάνει boot η συσκευή.

```
  GNU nano 7.2                          /etc/rc.local
#!/bin/sh -e
#
# rc.local
# This script is executed at the end of each multiuser runlevel

iptables-restore < /home/agiskallas/labfirewall.bk

exit 0
```

Εικόνα 1: Αρχείο rc.local

Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Εργασία:
Σχεδιάστε ένα τείχος προστασίας χρησιμοποιώντας τα iptables με τους παρακάτω κανόνες:

- Κανένας περιορισμός των πακέτων εξόδου.
- Επιτρέψτε την ssh πρόσβαση (port22) μόνο από τις IP διευθύνσεις του εργαστηρίου Δικτύων (150.140.139.194 έως 150.140.139.255) με μίαν μόνο εντολή.
- Επιτρέψτε την ssh πρόσβαση (port22) από το εσωτερικό δίκτυο (192.168.X.X) με μίαν μόνο εντολή.
- Υποθέτοντας ότι χρησιμοποιείτε έναν διακομιστή HTTPD εγκατεστημένο σε δικό σας υπολογιστή που δίνει πρόσβαση στο home directory σας στο εξωτερικό κόσμο. Γράψτε έναν κανόνα iptables που να επιτρέπει μόνο μία IP διεύθυνση στο Διαδίκτυο να έχει πρόσβαση στο μηχάνημά σας για την HTTP υπηρεσία.
- Επιτρέψτε την χρήση της υπηρεσίας παράδοσης/αποστολής εμαιλ (SMTP over TLS, imap) που χρησιμοποιούν οι περισσότεροι διακομιστές μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Αποδεχτείτε όλα τα αιτήματα ICMP Echo (όπως χρησιμοποιείται από το ping) από το εξωτερικό δίκτυο.
- Απαντήστε με TCP RST ή ICMP μη προσβάσιμο για εισερχόμενα αιτήματα για όλες τις αποκλεισμένες θύρες.

Γενικοί κανόνες αλυσίδας για κάθε bullet point:

- **iptables -A OUTPUT -j ACCEPT**
- **iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 150.140.139.194-150.140.139.255 -j ACCEPT**
- **iptables -A INPUT -p tcp –dport 22 -s 192.168.0.0/16 -j ACCEPT**
- **iptables -A INPUT -p tcp –dport 80 ! -s X.X.X.X -j DROP**
- **iptables -A INPUT -p tcp –match multiport --dports 143,587 -j ACCEPT**
- **iptables -A INPUT ! -s 192.168.0.0/16 -p icmp --icmp-type echo-request -j ACCEPT**
- **iptables -A INPUT -p all -j REJECT --reject-with icmp-host-prohibited** (ICMP unreachable)
- **iptables -A INPUT -p tcp -j REJECT --reject-with tcp-reset** (TCP RST)

Αρχείο labfirewall.sh, που περιλαμβάνει τους κανόνες:

```
# Initialise
iptables -t filter -F
iptables -t filter -X

iptables -t filter -N labfirewall.rules

# No restrictions on outbound packets
iptables -A OUTPUT -j ACCEPT

# Allow for SSH access(port 22) only from the lab IP addresses '150.140.139.193/26'
iptables -A labfirewall.rules -p tcp --dport 22 -m iprange --src-range 150.140.139.194-150.140.139.

# Allow SSH access(port 22) from the internal network '192.168.X.X'
iptables -A labfirewall.rules -p tcp --dport 22 -s 192.168.0.0/16 -j ACCEPT

# Allow a sinlge IP address in the internet access to the machine for the HTTP service
#iptables -A labfirewall.rules -p tcp --dport 80 ! -s X.X.X.X -j DROP

# Permit access to the mail service(SMTP over TLS: port 587, IMAP: port 143)
iptables -A labfirewall.rules -p tcp -m multiport --dport 143,587 -j ACCEPT

# Accept all ICMP Echo (used by ping) coming from external network
iptables -A labfirewall.rules ! -s 192.168.0.0/16 -p icmp --icmp-type echo-request -j ACCEPT

# Respond with TCP RST or ICMP unreachable for incoming requests for blocked ports
# For ICMP unreachable
iptables -A labfirewall.rules -p all -j REJECT --reject-with icmp-host-unreachable
# For TCP RST:
# iptables -A labfirewall.rules -p tcp -j REJECT --reject-with tcp-reset

iptables -I INPUT -j labfirewall.rules
iptables -I FORWARD -j labfirewall.rules
```

Εικόνα 2: Αρχείο labfirewall.sh

Παρακάτω φαίνεται το τείχος προστασίας αμέσως μετά την εκκίνηση της συσκευής:

```
Last login: Mon Oct 30 09:50:27 EET 2023 on tty1
agiskallas@debian-agis:~$ sudo iptables -nL -v
[sudo] password for agiskallas:
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    76 labfirewall.rules  0    --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 labfirewall.rules  0    --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   180 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0

Chain labfirewall.rules (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
source IP range 150.140.139.194-150.140.139.255
    0     0 ACCEPT     6    --  *      *       192.168.0.0/16       0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           multiport d
ports 143,587
    0     0 ACCEPT     1    --  *      *      !192.168.0.0/16       0.0.0.0/0           icmptype 8
    1    76 REJECT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with
 icmp-host-unreachable
agiskallas@debian-agis:~$
```

Εικόνα 3: Κατά την εκκίνηση

Για λόγους επιβεβαίωσης της ορθής λειτουργίας, έχω κάνει comment τον κανόνα που επιτρέπει πρόσβαση στη συσκευή από το διαδίκτυο (HTTP), καθώς δεν έχω δώσει συγκεκριμένη διεύθυνση IP. Γι' αυτό δεν φαίνεται στην Εικόνα 3.