Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

Μπουρλάκης Γεώργιος

1054321

Ερωτήσεις κατανόησης:

1. Το φιλτράρισμα πακέτων πραγματοποιείται μόνο αν η υποστήριξη TCP/IP πακέτων είναι ενσωματωμένη στο λειτουργικό σύστημα, γιατί σε μονολιθικά συστήματα, όπως το linux, η επεξεργασία πακέτων γίνεται στον ίδιο χώρο διευθύνσεων που εκτελείται και ο πυρήνας του συστήματος. Επίσης, ο πυρήνας είναι ένα πολύ σημαντικό κομμάτι ολόκληρου του λειτουργικού συστήματος γι' αυτό και επεξεργάζεται άμεσα τα πακέτα.

2. Κάποιες από τις διαφορές είναι ότι το τείχος προστασίας φιλτραρίσματος πακέτων ελέγχει και φιλτράρει όλη την εισερχόμενη και εξερχόμενη κίνηση σε ένα τοπικό δίκτυο, φιλτράρει IP πακέτα και υλοποιείται στα επίπεδα δικτύου και μεταφοράς. Αντίθετα, το τείχος προστασίας διακομιστή μεσολάβησης διαχειρίζεται όλη την κίνηση σε ένα τοπικό δίκτυο που διέρχεται από αυτόν το διακομιστή, φιλτράρει αιτήματα πελατών για σύνδεση και υλοποιείται στο επίπεδο εφαρμογής. Μπορούν να λειτουργούν και τα 2 ταυτόχρονα για να προστατεύουν ένα δίκτυο σε έναν υπολογιστή.

3. Οι 4 πίνακες που διατηρούνται από τον πυρήνα linux για επεξεργασία εισερχόμενων και εξερχόμενων πακέτων είναι: filter, mangle, nat και raw.

4. Το μέρος του πακέτου που εξετάζεται είναι η κεφαλίδα του, από τον πυρήνα ώστε να το κατευθύνει στη συνέχεια στη σωστή αλυσίδα. Αν το πακέτο προορίζεται για το μηχάνημα στο οποίο επεξεργάζεται τότε περνάει στην input αλυσίδα. Αν το πακέτο προορίζεται για άλλη δικτυακή διεπαφή τότε περνάει στην forward αλυσίδα. Αν ο υπολογιστής θέλει να στείλει το πακέτο εκτός μηχανήματος τότε περνάει στην output αλυσίδα.

5. Εάν το πακέτο δεν πληροί τις προϋποθέσεις των κανόνων τότε ο πυρήνας ανάλογα την πολιτική αλυσίδας καθορίζει τι θα γίνει με το συγκεκριμένο πακέτο. Το πιο σύνηθες είναι να λέει η πολιτική στον πυρήνα να το κάνει drop. Η πολιτική αλυσίδας είναι μία πολιτική στην οποία εφόσον το πακέτο δεν έκανε σε καμία από τις 3 προηγούμενες αλυσίδες τότε εκτελείται μία προκαθορισμένη ενέργεια που συνήθως είναι η απόρριψη του πακέτου.

6. Η εντολή για απόρριψη όλων των εισερχόμενων SYN πακέτων είναι:
   sudo iptables -t mangle -A PREROUTING -p tcp -m tcp –tcp-flags SYN NONE -j DROP

7. Η εντολή για αρχικοποίηση όλων των αλυσίδων είναι:
   Αλυσίδα χρήστη: sudo iptables -F <όνομα αλυσίδας>
   Γενικά: sudo iptables -F
   Για τον mangle πίνακα: sudo iptables -t mangle -F

8. Η εμφάνιση της συμβολοσειράς <icmp type 255> σημαίνει ότι μπορεί να χρησιμοποιείται οποιοσδήποτε τύπος icmp μηνύματος, καθώς δεν έχει οριστεί από την IANA, σε αντίθεση με 3 χρησιμοποιούμενους τύπους: 0, 8, 11.

9. Ο τύπος icmp που σχετίζεται με το echo-request(ping) είναι ο 8, ενώ ο τύπος για τα πακέτα echo-reply(pong) είναι ο 0.

10. Ο καθορισμός εξαιρέσεων σημαίνει ότι ο πυρήνας αναγνωρίζει την κατάσταση διάφορων εισερχόμενων πακέτων που ανήκουν σε μία συνεχιζόμενη σύνδεση που είχε δημιουργηθεί και αποδεχθεί πριν οπότε γλιτώνει την περιττή επεξεργασία πακέτων. Όταν υπάρχουν raw πίνακες έχουν μεγαλύτερη προτεραιότητα από όλους τους υπόλοιπους. Η κατάσταση των πακέτων αυτών αναγνωρίζεται ως established.

11. Οι εντολές για να δέχεται ο server εισερχόμενα αιτήματα σύνδεσης για τον sshd διακομιστή και να απορρίπτει όλα τα άλλα πακέτα αιτήματος σύνδεσης από απομακρυσμένους πελάτες είναι:
    sudo iptables -A INPUT -p tcp –destination-port 22 -j ACCEPT
    sudo iptables -A INPUT -j DROP

12. Connection tracking γίνεται όταν έχουμε ξεκινήσει εμείς μία σύνδεση με κάποιον και αυτός μας στέλνει πίσω κάποια πακέτα. Το connection tracking αναφέρεται στην ουσία στην κατάσταση που βρίσκεται ένα πακέτο, μία χρήσιμη μονάδα επέκτασης. Το firewall αν δει κάποιο πακέτο για πρώτη φορά θεωρεί την κατάσταση του ως new, ενώ αν το πακέτο είναι μέρος ήδη γνωστής σύνδεσης ή ροής τότε θεωρεί ότι βρίσκεται σε κατάσταση established και το αποδέχεται αυτόματα.

13. Οι διαφορετικές καταστάσεις πακέτων που αναγνωρίζονται από το connection tracking είναι: new(για νέα σύνδεση), established(για υπάρχουσα σύνδεση), related(για σχετιζόμενα πακέτα με τη σύνδεση χωρίς να είναι μέρος τους, όπως ένα icmp error) και invalid(για πακέτα που δεν έχουν αναγνωριστεί).

14. Οι εντολές για να υλοποιεί το Debian κάθε φορά που εκκινεί τα iptables είναι:
    sudo iptables -A input -j DROP
    sudo iptables-save > /etc/iptables.rules
    vi /etc/network/if-pre-up.d/firewall
    στο αρχείο που ανοίγει προσθέτουμε:
    #!/bin/bash
    /sbin/iptables-restore < /etc/iptables.rules
    μετά αποθηκεύουμε το αρχείο και εκτελούμε την εντολή:
    chmod +x /etc/network/if-pre-up.d/firewall
    έπειτα σε κάθε επανεκκίνηση με την εντολή:
    sudo iptables -L

θα βλέπουμε τα αποτελέσματα των εντολών που είχαμε αποθηκεύσει, στην περίπτωση μας την εντολή: sudo iptables -A input -j DROP

Εργασία:

- sudo iptables -A OUTPUT -j ACCEPT
- sudo iptables -A INPUT -p tcp --destination-port 22 -m iprange --src-range 150.140.139.194 - 150.140.139.255 -j ACCEPT
- sudo iptables -A INPUT -p tcp -s 192.168.0.0/16 --dport 22 -j ACCEPT
- sudo iptables -A INPUT -p tcp -s 10.0.0.1 --dport 80 -j ACCEPT
- 1.sudo iptables -A OUTPUT -p tcp --sport 25 -j ACCEPT
  2. sudo iptables -A INPUT -p tcp --dport 25 -j ACCEPT
- sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
- 1. sudo iptables -A INPUT -p tcp --tcp-flags RST RST -j DROP
  2. sudo iptables -A INPUT -p icmp –icmp-type 8 -j DROP

Παρατίθενται κάποια screenshots μετά από όλους τους κανόνες για τα iptables:

```
File  Edit  View  Terminal  Tabs  Help
root@debian:/home/george# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh source IP range 150.140.139.194-150.140.139.255
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp dpt:ssh
ACCEPT     tcp  --  10.0.0.1             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:smtp
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
DROP       tcp  --  anywhere             anywhere             tcp flags:RST/RST
DROP       icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:smtp
root@debian:/home/george#
```

```
root@debian:/home/george# sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m iprange --src-range 150.140.139.194-150.140.139.255 -j ACCEPT
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 10.0.0.1/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags RST RST -j DROP
-A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
-A OUTPUT -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 25 -j ACCEPT
root@debian:/home/george#
```

```
root@debian:/home/george#
root@debian:/home/george# sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       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     tcp  --  *      *       192.168.0.0/16       0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       10.0.0.1             0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:25
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x04/0x04
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  864  100K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:25
root@debian:/home/george#
root@debian:/home/george#
```