1η Εργασία στις σύγχρονες εφαρμογές ασφάλειας δικτύων

Όνομα: Γεώργιος

Επώνυμο: Βέργος

Αριθμός Μητρώου: 1072604

Τμήμα: ΤΜΗΥΠ(CEID)

Ημερομηνία: 27/10/2022

Εξάμηνο σπουδών: 7ο

1) Ερωτήσεις κατανόησης

a)

Τα δίκτυα υψηλής ταχύτητας απαιτούν ελάχιστες καθυστερήσεις στην επεξεργασία της πληροφορίας οπότε και καθυστερήσεις στην επεξεργασία των πακέτων. Όταν η υποστήριξη για tcp/ip είναι ενσωματωμένη απευθείας στον πυρήνα του λειτουργικού και φτάσει ένα πακέτο σε κάποια δικτυακή διεπαφή , ο πυρήνας μπορεί άμεσα να αποφασίσει τι θα γίνει με το πακέτο αυτό. Έτσι η επεξεργασία του γίνεται πολύ πιο γρήγορα σε αντίθεση π.χ με τη περίπτωση που το πακέτο προωθούταν από τον πυρήνα σε κάποια

διεργασία για να το επεξεργαστεί(που αυτό θα γεννούσε αρκετές καθυστερήσεις).

b)

Με ένα τείχος προστασίας διακομιστή μεσολάβησης όλη η κίνηση δικτύου για τους

υπολογιστές ενός τοπικού δικτύου δρομολογείται μέσω ενός διακομιστή μεσολάβησης.

Αυτό επιτρέπει στον διακομιστή να ελέγξει όλη την κίνηση του δικτύου.

Με ένα τείχος προστασίας φιλτραρίσματος πακέτων εκμεταλλευόμαστε την ενσωματωμένη υποστήριξη του πυρήνα(για λίνουξ συνήθως)

για το tcp/ip. Ναι μπορούν να χρησιμοποιηθούν μαζί.

c) Οι 4 πίνακες που διατηρούνται από τον πυρήνα του linux για την επεξεργασία εισερχόμενων και εξερχόμενων πακέτων είναι οι : filter ,mangle,nat,raw.

d) Όταν φτάσει το πακέτο στο σύστημα που αναφερόμαστε μέσω κάποιας δικτυακής

διεπαφής ο πυρήνας κοιτά την διεύθυνση προορισμού του πακέτου.

Αν προορίζεται για την μηχανή τότε το πακέτο προωθείται στην input αλυσίδα κανόνων.

Αν το εισερχόμενο πακέτο προορίζεται για άλλη δικτυακή διεπαφή στο ίδιο μηχάνημα τότε προωθείται

στην forward αλυσίδα. Αν γίνει αποδεκτό από την forward αλυσίδα τότε στέλνεται στο αντίστοιχο interface.

Αν κάποια διεργασία θέλει να στείλει ένα πακέτο στον έξω κόσμο, το πακέτο προωθείται στην output αλυσίδα.

Γενικά κάθε κανόνας σε μία αλυσίδα εξετάζει τη κεφαλίδα του πακέτου και αν η συνθήκη του κανόνα ταιριάζει

με τη κεφαλίδα του πακέτου η αντίστοιχη πράξη του κανόνα εκτελείται. Αλλιώς το πακέτο πηγαίνει στον επόμενο κανόνα.

e)

Αν ένα πακέτο φτάσει στο τέλος της αλυσίδας τότε ο πυρήνας κοιτά τη πολιτική αλυσίδας για να δει

τι θα κάνει με το πακέτο. Η πολιτική αλυσίδας ορίζει τι θα πάθουν τα πακέτα εφόσον δεν πληρούν κανέναν προηγούμενο κανόνα.

f) Η εντολή θα είναι:

sudo iptables -A INPUT -p tcp –syn -m state –state NEW -j DROP

g)

Η εντολή για να αρχικοποιήσει όλες τις αλυσίδες στον πίνακα είναι : sudo iptables -F. Η αρχικοποιήση ‘’σβήνει’’ όλες τις αλυσίδες που προηγουμένως είχαμε προσθέσει στον πίνακα.

h)

Το icmp-type 255 αναφέρεται σε όλα τα είδη icmp πακέτων(π.χ icmp echo requests(8) ,icmp echo reply(0) κλπ). Οι υπόλοιποι τύποι φαίνονται στην παρακάτω εικόνα:

```
Valid ICMP Types:
        any
        echo-reply (pong)         (type 0)
        destination-unreachable   (type 3)
           network-unreachable       (code 0)
           host-unreachable          (code 1)
           protocol-unreachable      (code 2)
           port-unreachable          (code 3)
           fragmentation-needed      (code 4)
           source-route-failed       (code 5)
           network-unknown           (code 6)
           host-unknown              (code 7)
           network-prohibited        (code 8)
           host-prohibited           (code 9)
           TOS-network-unreachable   (code 10)
           TOS-host-unreachable      (code 11)
           communication-prohibited (code 12)
           host-precedence-violation
           precedence-cutoff
        source-quench             (type 4)
        redirect                  (type 5)
           network-redirect
           host-redirect
```



```
           TOS-network-redirect
           TOS-host-redirect
        echo-request (ping)       (type 8)
        router-advertisement      (type 9)
        router-solicitation       (type 10)
        time-exceeded (ttl-exceeded)(type 11)
           ttl-zero-during-transit    (code 0)
           ttl-zero-during-reassembly (code 1)
        parameter-problem         (type 12)
           ip-header-bad
           required-option-missing
        timestamp-request         (type 13)
        timestamp-reply           (type 14)
        address-mask-request      (type 17)
        address-mask-reply        (type 18)     ]
```

i)

Ο τύπος icmp-echo-request (type 8) αφορά το ping ενώ

ο icmp-echo-reply(type 0) αφορά το pong.

j)

Με τον raw πίνακα μπορούμε να επεξεργαζόμαστε πακέτα προτού ο πυρήνας του λειτουργικού αρχίσει να καταγράφει την κατάσταση τους(new,established κλπ).

k)

sudo iptables -A INPUT -p tcp -s 0/0 --dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT

και με policy:

sudo iptables -P INPUT DROP(ή REJECT)

l)

Η Παρακολούθηση σύνδεσης πρόκεται για μία μέθοδο η οποία αποθηκεύει πληροφορίες για τις συνδέσεις στον πίνακα του iptables. Έτσι μπορεί να αναγνωρίζει ποιο πακέτο ανήκει σε ποια σύνδεση. Όταν ένα πακέτο είναι το πρώτο για το οποίο το τείχος προστασίας γνωρίζει , βρίσκεται σε κατάσταση NEW. Αν ήταν ήδη μέρος

μίας ήδη εγκατεστημένης σύνδεσης βρίσκεται σε κατάσταση established.

m) Οι διαφορετικές καταστάσεις πακέτων που αναγνωρίζονται από το connection tracking του iptables είναι:

NEW,ESTABLISHED,RELATED,INVALID

n)

Για να κρατάει σε κάθε εκκίνηση το iptables όλους τους κανόνες που του όρισα(τους πιο πρόσφατους) κάνω το εξής:

Προσθέτω τις ακόλουθες γραμμές στο αρχείο /etc/network/interfaces:

auto ens33

iface ens33 inet dhcp

pre-up iptables-restore < /etc/iptables/rules.v4

post-down iptables-save > /etc/iptables/rules.v4

2) Εργασία

a)

Εφόσον δεν έχουμε κανέναν περιορισμό στα πακέτα εξόδου θα έχουμε την εντολή :

sudo iptables -P OUTPUT ACCEPT

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

b) Επιτρέπω πρόσβαση στον υπολογιστή μέσω ssh μόνο στις

διευθύνσεις 150.140.139.194-150.140.139.255:

sudo iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 150.140.139.194-150.140.139.255 -m state --state NEW,ESTABLISHED -j ACCEPT :

```
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
  source IP range 150.140.139.194-150.140.139.255 state NEW,ESTABLISHED
```

Και βάζω ως πολιτική αλυσίδας : sudo iptables -A INPUT DROP. Έτσι αν μία μη επιτρεπτή ip διεύθυνση πραγματοποιήσει ssh με το μηχάνημα μου δε θα ταιριάξει με τον πρώτο κανόνα και λόγω πολιτική αλυσίδας θα απορριφθεί.

c) Επιτρέπω ssh στον υπολογιστή από το εσωτερικό δίκτυο (192.168.X.X)

sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.0.0/16 -m state --state NEW,ESTABLISHED -j ACCEPT :

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp dpt:ssh state NEW,ESTABLISHED
```

d) Επιτρέπω μόνο σε μία διεύθυνση ip στο διαδίκτυο να συνάπτει σύνδεση http(και https) με τον υπολογιστή που τρέχει υπηρεσία httpd:

sudo iptables -A INPUT -p tcp -s 8.8.8.8(ή οποιαδήποτε μοναδική διεύθυνση) -m multiport --dports 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT

```
    0     0 ACCEPT     tcp  --  any    any     8.8.8.8              anywhere             multiport d
ports http,https state NEW,ESTABLISHED
```

e)

Επιτρέπω την παράδοση/αποστολή(στην αποστολή είμαστε καλυμμένοι λόγω μη περιορισμών στα πακέτα εξόδου):

sudo iptables -A INPUT -p tcp -m multiport --dports 25,143,993,465,587 -m state --state NEW,ESTABLISHED -j ACCEPT

```
Chain INPUT (policy DROP 460 packets, 40108 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             multiport d
ports smtp,imap2,imaps,submissions,submission state NEW,ESTABLISHED
```

f) Αποδέχομαι όλα τα μηνύματα icmp echo requests:

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp dpt:ssh state NEW,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
```

g)

Απορρίπτω για τις υπόλοιπες θύρες τα πακέτα με μήνυμα icmp-host-unreachable

sudo iptables -A INPUT -j REJECT --reject-with icmp-host-unreachable

Αυτός ο κανόνας μπαίνει τελευταίος στην αλυσίδα και έτσι για όλες τις υπόλοιπες θύρες που δε μας ενδιαφέρουν (άρα τις αποκλεισμένες) απορρίπτουμε το πακέτο με το μήνυμα icmp-host-unreachable: