Συγχρονες εφαρμογες Ασφαλειας

Ονοματεπώνυμο : Νικόλας Φιλιππάτος
AM: 1072754
Εργασία: 2η

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;***

   Με την ενσωματωμενη υποστηριξη TCP/IP, επειδη ο kernel ειναι monolithic, εκτελειται το φιλτραρισμα στην ιδια διευθυνση που ο ιδιος ο kernel εκτελειται, καθως εχει αμεση επικοινωνια με την κάρτα δικτυου .
2. ***Ποια είναι η διαφορά μεταξύ ενός τείχους προστασίας φιλτραρίσματος πακέτων και ενός τείχος προστασίας διακομιστή μεσολάβησης; Μπορούν τα δύο να χρησιμοποιηθούν μαζί;***

   Ενα τείχος προστασιας δικομιστη μεσολάβησης ειναι ενα προγραμμα το οποιο αποτελει ενα ενδιαμεσο βημα για τα αιτηματα απο clients που ζητανε resources απο αλλους servers. Ελεγχουν το περιεχομενο του πακετου, και προσφερουν μεγαλυτερη προστασια.
   Αντίθετα ενα τειχος προστασιας φιλτραρισματος πακετων βρισκεται μεσα στο εσωτερικο δικτυο, ελεγχει μονο τα headers και ειναι δυνατο να χρησιμοποιηθουν μαζι
3. ***Ποιοι είναι οι τέσσερις πίνακες που διατηρούνται από τον πυρήνα Linux για την επεξεργασία εισερχόμενων και εξερχόμενων πακέτων;***

   Υπαρχουν 4 πινακες που διατηρουνται απο τον πυρηνα Linux για την επεξεργασια εισερχομενων και εξερχομενων πακετων:
   - filter
   - mangle
   - nat
   - row
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 τειχος προστασιας που χρησιμοποιει iptables, κοιταζει το header καθε πακετου:

- Αν εισερχεται χρησιμοποιει τους κανονες αλυσιδας INPUT
- Εαν εξέρχεται χρησιμοποιει τους κανονες της αλυσιδας OUTPUT
- Εαν εινα δρομολογητης και στελνεται το πακετο σε καποιο αλλο μηχανημα εκτος αυτου τοτε αξιοποιει τους κανονες αλυσιδας FORWARD

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;***

Γενικα καθε κανονας εξεταζει το packet header, και αν οι συνθηκες του κανονα συμβαδιζουν με τις συνθηκες του header, εκτελειται η πραξη του κανονα , αλλιως προχωραει στον επομενο κανονα.
Εαν το πακετο φτασει στο τελος της αλυσιδας, τοτε το linux kernel κοιταει την Πολιτικη Αλυσιδας, που ειναι η default ενεργεια για τα πακετα.

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;***

```
iptables -F
```

Ειναι για να διαγραψει ολους του σκανονες
Με το `-t <table name>` προσδιοριζουμε απο ποιον πινακα θα κανει διαγραφη

```
iptables -F -t <table-name>
```

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

Ο κανονας αυτος λεει οτι κανει accept οποιοδηποτε ICMP type. Μπορει να χρησιμποιηθει και το "any"

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

- echo-request (ping) (code 0)
- echo-reply (pong) (echo 8)

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

Καθιστα ευκολο να καθορισει ενα connection tracking κανονα με την βοηθεια της επεκτασης "state"
Παιρνει προτεραιοτητα πανω απο ολα τα υπολοιπα tables.

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;***

Η παρακολουθηση ενος πακετου βασιζεται στην καταστση "state"

- Εαν ειναι το πρωτο που βρισκει το firewall το θεωρει στην καταστση state="NEW"
- Εαν ειναι κομματι απο μια υπαρχουσα συνδεση το θεωρει στην κατάσταση state="ESTABLISHED"
  Η καταστση γινεται assigned οταν διαβαζει το πακετο ο firewall.

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

Οι καταστασεις πακετων που αναγνωριζονται απο την καταστση της συνδεσης ειναι :

- 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 χρησιμοποιει τους κανονες που θελουμε, θα βαλουμε τους κανονες σε ενα αρχειο στο directory /etc/rc.local.

Εργασία:

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

1. ***Κανένας περιορισμός των πακέτων εξόδου.***

```
iptables -A OUTPUT -j ACCEPT
```

Στην αλυσιδα OUTPUT δεχομαστε ολα τα πακετα εξοδου .

2. ***Επιτρέψτε την ssh πρόσβαση (port22) μόνο από τις IP διευθύνσεις του εργαστηρίου Δικτύων (150.140.139.194 έως 150.140.139.255) με μιαν μόνο εντολή.***

```
iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 150.140.139.194-
150.140.139.255 -j ACCEPT
```

3. ***Επιτρέψτε την ssh πρόσβαση (port22) από το εσωτερικό δίκτυο (192.168.X.X) με μιαν μόνο εντολή.***

```
iptables -A INPUT -p tcp --dport 22 -s 192.169.0.0/16 -j ACCEPT
```

4. ***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 IPδιεύθυνση στο Διαδίκτυο να έχει πρόσβαση στο μηχάνημά σας για την HTTP υπηρεσία.***

```
iptables -A INPUT -p tcp --dport 80 ! -s X.X.X.X -j DROP
```

Κανουμε drop ολες τις διευθυνσεις που δεν ειναι αυτη που εχουμε προσδιορισει

5. ***Επιτρέψτε την χρήση της υπηρεσίας παράδοσης/αποστολής εμαιλ (SMTP over TLS, imap) που χρησιμοποιούν οι περισσότεροι διακομιστές μηνυμάτων ηλεκτρονικού ταχυδρομείου.***

```
iptables -A INPUT -p tcp --match multiport --dports 143,465 -j ACCEPT
```

6. ***Αποδεχτείτε όλα τα αιτήματα ICMP Echo (όπως χρησιμοποιείται από το ping) από το εξωτερικό δίκτυο.***

```
iptables -A INPUT ! -s 192.168.0.0/16 -p icmp --icmp-type echo-request -j
ACCEPT
```

Κανει accept ολα τα icmp echo requests απο ολες τις διευθυνσεις που δεν ειναι εσωτερικου δικτυου

7. ***Απαντήστε με TCP RST ή ICMP μη προσβάσιμο για εισερχόμενα αιτήματα για όλες τις αποκλεισμένες θύρες.***

```
iptables -A INPUT -p all -j REJECT --reject-with icmp-host-prohibited
```

```
# 1 no output restrictions
iptables -A OUTPUT -j ACCEPT

# 2 ssh accpet for labs only
iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 150.140.139.194-
150.140.139.255 -j ACCEPT

# 3 ssh accept from internal network
iptables -A INPUT -p tcp --dport 22 -s 192.169.0.0/16 -j ACCEPT

# 4 accept httpd from only one ip address
iptables -A INPUT -p tcp --dport 80 ! -s X.X.X.X -j DROP

# 5 email servers
iptables -A INPUT -p tcp --match multiport --dports 143,465 -j ACCEPT

# 6 accpet all icmp requests pings from outside the network
iptables -A INPUT ! -s 192.168.0.0/16 -p icmp --icmp-type echo-request -j
ACCEPT

# 7 not responsive
iptables -A INPUT -p all -j REJECT --reject-with icmp-host-prohibited
```