Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

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;
2. Ποια είναι η διαφορά μεταξύ ενός τείχους προστασίας φιλτραρίσματος πακέτων και ενός τείχος προστασίας διακομιστή μεσολάβησης; Μπορούν τα δύο να χρησιμοποιηθούν μαζί;
3. Ποιοι είναι οι τέσσερις πίνακες που διατηρούνται από τον πυρήνα Linux για την επεξεργασία εισερχόμενων και εξερχόμενων πακέτων;
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?
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;
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;
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;
8. Εάν δείτε τη συμβολοσειρά «icmp type 255» στο τέλος μιας γραμμής που παράγεται από την έξοδος της εντολής «iptables -L», τι σημαίνει αυτό?
9. Ποιοι είναι οι τύποι icmp που σχετίζονται με το echo-request (ping) και με τα πακέτα echo-reply (pong);
10. Ο αρχικός (raw) πίνακας χρησιμοποιείται για τον καθορισμό εξαιρέσεων από τη παρακολούθηση της σύνδεση (connection tracking). Τι σημαίνει αυτό?
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.
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;
13. Ποιες είναι οι διαφορετικές καταστάσεις πακέτων που αναγνωρίζονται από την κατάσταση της σύνδεσης (connection tracking) του iptables;
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.

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 εργαστηρίπυ Δικτύων (150.140.139.194 έως 150.140.139.255) με μιαν μόνο εντολή.
- Επιτρέψτε την ssh πρόσβαση (port22) από το εσωτερικό δίκτυο (192.168.X.X) με μιαν 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 IPδιεύθυνση 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.