Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

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

---

1) Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban
Εγκαταστήστε το πακέτο fail2ban στην εικονική μηχανή που έχετε φτιάξει. Ανατρέξτε στα φίλτρα (***/etc/fail2ban/filter/d/***) και στα αρχεία διαμόρφωσης ***fail2ban.conf*** και ***jail.conf*** που εγκαταστάθηκαν.
Το fai2ban πακέτο με την εγκατάσταση του αυτόματα ενεργοποιεί το φίλτρο προστασίας για ssh επιθέσεις.

- Ελέγξτε την κατάσταση των jails με την εντολή *fail2ban-client status* και *fail2ban-client status sshd*.
- τροποποιήστε το αρχείο για το φίλτρο ssh ώστε κλειδώνει τις συνδέσεις μετά από 5 λανθασμένες προσπάθειες στα τελευταία 10 λεπτά.
- Έχοντας δύο τερματικά ανοικτά, πραγματοποιείστε 5 προσπάθειες με λάθος κωδικό και δείτε το αποτέλεσμα με την εντολή fail2ban-client status sshd.
- Σε ποιο log αρχείο καταγράφονται οι συνδέσεις? Ανοίξτε και δείτε τις τελευταίες γραμμές που δείχνουν την ανεπιτυχή σύνδεση.
- Δείτε ξανά την έξοδο της fail2ban-client status sshd και ελέγξτε το firewall σας εάν απορρίπτει την IP διεύθυνση από την οποία κάνατε τις ανεπιτυχές συνδέσεις.
- Με ποια εντολή κάνουμε “unban” την IP?
- Σε ποιο αρχείο μπορούμε να προσθέσουμε IP που δεν επιθυμούμε να φιλτράρονται? Πχ (τις IP διευθύνσεις από το εσωτερικό LAN).
- Εγκαταστήστε και ρυθμίστε το πακέτο sendmail ώστε το fail2ban να σας στέλνει εμαιλ όταν μπλοκάρετε μια IP διεύθυνση. Οδηγίες για την εγκατάσταση και ρύθμιση του sendmail μπορείτε να βρείτε εδώ.

---

2) Χρήση Public Key Authentication
Στην εικονική μηχανή που τρέχει debian ενεργοποιείστε την ssh πρόσβαση μόνο με χρήση δημόσιου κλειδιού. Τα βήματα περιλαμβάνουν :

- την δημιουργία του κλειδιού (ssh-keygen) με τις σωστές παραμέτρους.
- την αντιγραφή του κλειδιού σε άλλο server (πχ το host υπολογιστή σας)
- τροποποίηση του αρχείου sshd config για πρόσβαση μόνο με το δημόσιο κλειδί.
- την επιτυχή δοκιμή σύνδεσης (χωρίς την χρήση συνθηματικού password).

---

3) Υλοποιήσει νέων φίλτρων για χρήση στο πακέτο fail2ban
Το log αρχείο δύο εφαρμογών joomla και nextcloud είναι όπως παρακάτω:

- *2020-10-06T16:27:16+00:00 INFO 150.140.139.252 joomlafailure Username and password do not match or you do not have an account yet.*

- *{"reqId":"VDEzZE0K2wITbT4fNrs1","level":2,"time":"2020-10-26T16:04:26+02:00","remoteAddr":"150.140.139.252","user":"--","app":"no app in*

context","method":"POST","url":"/nextcloud/index.php/login","message":"Login failed: username (Remote IP: 150.140.139.143)","userAgent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0","version":"19.0.4.2"}

1) Υλοποιείστε το “regular expression” για δύο νέα φίλτρα στο fail2ban που να λαμβάνει υπόψιν του τα παραπάνω αρχείο καταγραφής. Μπορείτε να χρησιμοποιήσετε το site αυτό: https://regex101.com/
2) Με ποια εντολή μπορούμε να δοκιμάσουμε (dry run) τα παραπάνω φίλτρα χωρίς να τα ενεργοποιήσουμε?
3) Φτιάξτε το αρχείο jail.local και ορίστε για τα παραπάνω φίλτρα τα: ports, protocols, iptable chain, findtime, bantime και retries.

Μπορείτε να βρείτε έναν πλήρης οδηγός για την χρήση του fail2ban εδώ.