IPTables

מהו IP TABLE?

זהו כלי (CLI) שמאפשר לתפעל את NetFillter ע"י יצירת חוקים כלליים או נקודתיים וכך למנוע מחבילות מיעד "זדוניות" לחדור למערכת.

NetFilter- זהו Stateful Firewall מובנה בלינוקס.

המנגנון שמסופק על ידי Iptables מאורגן בשלושה סוגים של מבנים:

Tables (טבלאות)

הטבלאות מאפשרות להגדיר כיצד לטפל בחבילות:

- **Filter table** - הטבלה משמשת כ- Firewall ומשמשת כטבלת ברירת המחדל.
- **Raw table** - Iptables מתפקד כ- stateful firewall ולכן מבצע מעקב אחר החבילות כדי לדעת לאיזה connection שייכת כל חבילה. Raw table מאפשר **לבטל מעקב** אחר חבילות מסוימות.
- **Mangle table** - מאפשרת לשנות את ה- Packet Header. לדוגמא לשנות את ערך ה- TTL.
- **Nat table** - הטבלה מאפשרת ביצוע NAT.

Chains (שרשראות)

השרשראות מגדירות באיזה נקודה לבדוק את החבילות.

- **INPUT chain** - מטפלת בחבילות שנכנסים למערכת.
- **OUTPUT chain** - מטפלת בחבילות שיוצאים מהמערכת.
- **FORWARD chain** - מטפלת בחבילות שמיועדים לניתוב (עוברות דרך המערכת).
- **PREROUTING chain** - מטפלת בחבילות לפני הניתוב.

POSTROUTING chain - מטפלת בחבילות אחרי הניתוב.

פקודות בסיסיות לשימוש בכלי:

sudo iptables -t {table} -L {chain}

-t (table), ציין איזה טבלה להציג.
-L (list), ציין איזה שרשרת להציג. -L ללא פרמטר נוסף, יציג כל השרשראות בטבלה.

```
elior@elior-virtual-machine:~/Desktop$ sudo iptables -t filter -L
[sudo] password for elior:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
elior@elior-virtual-machine:~/Desktop$
```

בדוגמא שלהלן הרצתי את הפקודה תחת טבלת FILTER ולא ציינתי איזה סוג שרשרת תחת הטבלה.

כלומר פקודה זאת מציגה את כל השרשראות שיש תחת טבלת FILTER.

כמו כן הפוליסה הדפולטיבית כאן היא ACCEPT. כלומר אם לא צוין אחרת, הכל מאופשר.

על מנת לשנות את הפוליסה הדיפולטיבית של שרשרת מסויימת נבצע את הפקודה הבאה:

sudo iptables **-P** {CHAIN} {TARGET}

```
elior@elior-virtual-machine:~/Desktop$ sudo iptables -P INPUT DROP
elior@elior-virtual-machine:~/Desktop$ sudo iptables -t filter -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
elior@elior-virtual-machine:~/Desktop$
```

הוספת חוק

דוגמה לחסימת חבילה נכנסת: גיליתם שהכתובת 60.46.124.52 מנסה לתקוף את השרת שלכם. כדי לחסום אותה, נוסיף חוק אל chain **INPUT** של filter table. כלומר הכתובת לא תצליח להגיע (INBOUND). ברגע שהיא תגיע לשרת היא תקבל DROP.

```
elior@elior-virtual-machine:~/Desktop$ sudo iptables -A INPUT -s 60.46.124.52 -j DROP
elior@elior-virtual-machine:~/Desktop$ sudo iptables -t filter -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  60.46.124.52         anywhere
elior@elior-virtual-machine:~/Desktop$
```

- **-A** השרשרת אליה החוק יתווסף.
- **-s** כתובת המקור. ניתן להגדיר כתובת רשת (60.46.124.0/24).
- **-j** הגדרת סוג הפעולה (target).