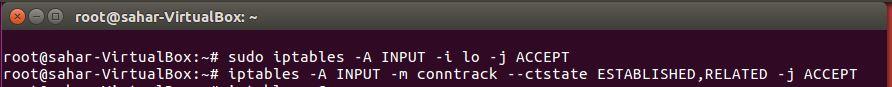
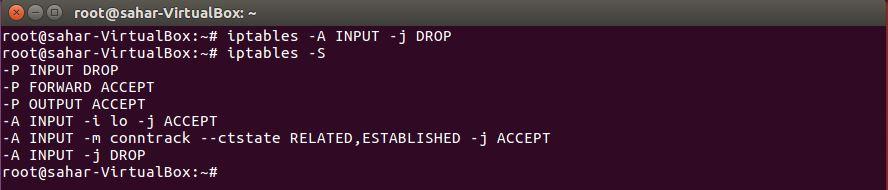
***שלב 3: הקמה של שירות הPort Knocking***

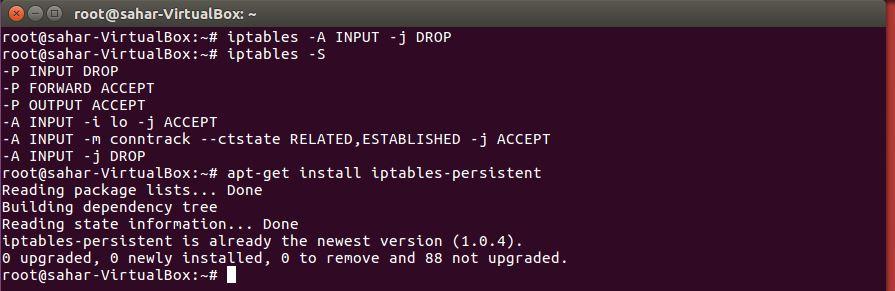
בשלב זה נתקין את מנגנון ההאזנה לPort Knocking על גבי מכונת ההגנה.

1. נאכלס את טבלת ההוראות של הFIREWALL לא לאפשר תקשורת בSSH

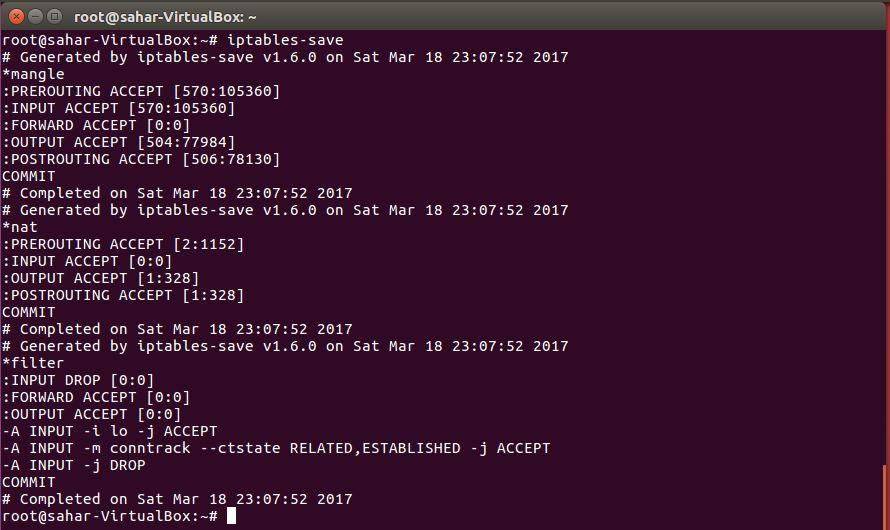




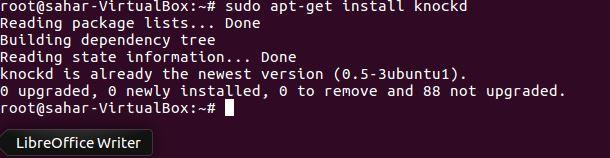
1. נתקין את שירות הIPPERSISTENT שדואג לעדכן את ההוראות במידה והשרת נפל.



1. נשתמש בשירות לשמור את ההוראות.



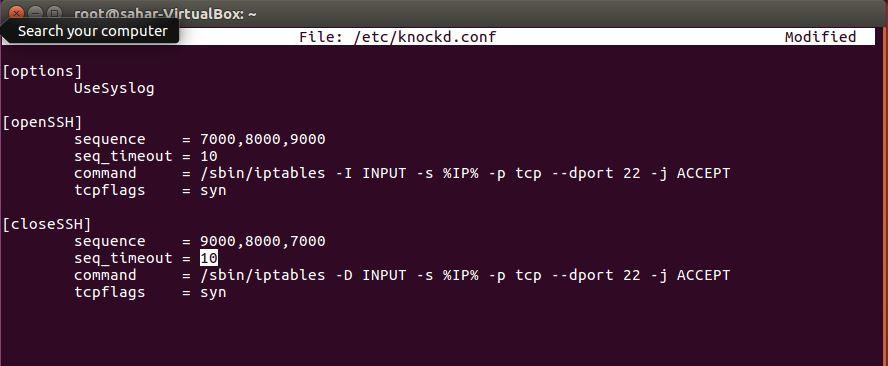
1. נתקין את שירות הKNOCKD שאחראי להאזין לנקישות ולפעול בהתאם להגדרות שנגדיר בהמשך.



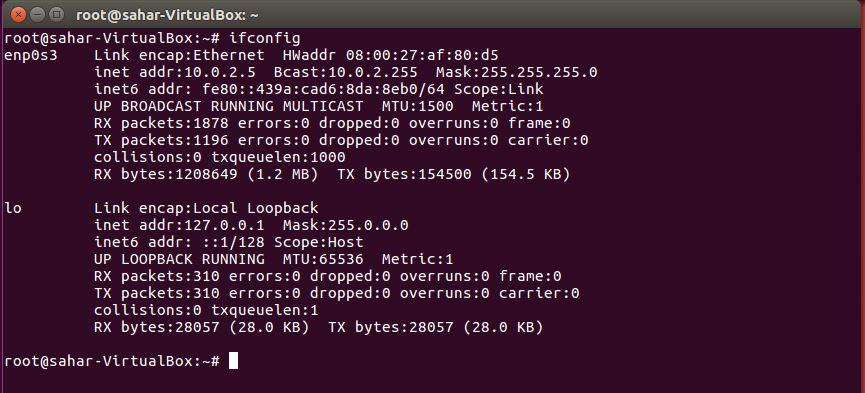
1. נערוך את קובץ הקונפיג של KNOCKD בשביל לקבוע את הגדרות הפורטים של הנקישות.



1. בחרנו שנקישה על פורטים 7000 8000 9000 בסדר עולה, גורמת לפקודה שפותחת את פורט 22. סדר הפוך סוגר את הפורט.



1. נריץ את הפקודה IFCONFIG בשביל לדעת מה הINTERFACE שעליו נאזין לנקישות.

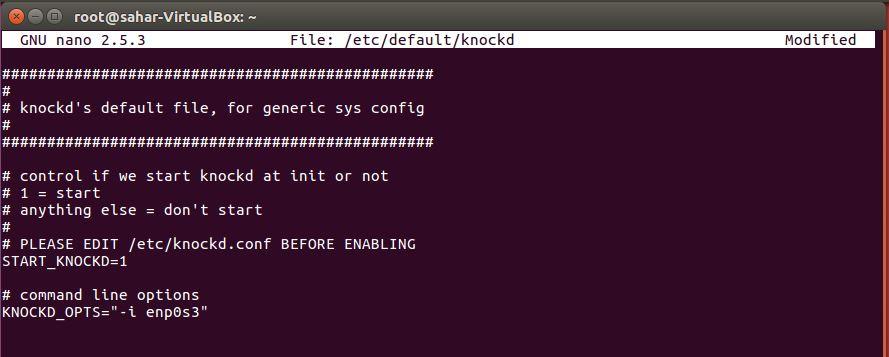


1. נערוך את ההגדרות של הרצת KNOCKD

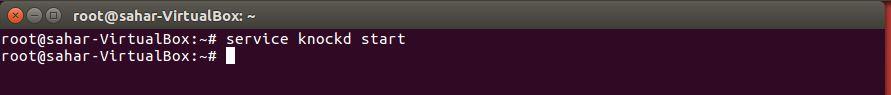
C:\Users\Daniel\AppData\Local\Microsoft\Windows\INetCache\Content.Word\8.jpg

1. שינינו את START\_KNOCKD ל1.

שינינו את KNOCKD\_OPTS לכתובת שמצאנו למעלה (enp0s3). בררת המחדל היא eth0.



1. נתחיל את השירות. לאחר הרצת פקודה זו השירות יאזין לנקישות ויפעל לפי הפקודות בהגדרות.



מדריכים בהם נעשה שימוש:

1. <https://www.digitalocean.com/community/tutorials/how-to-use-port-knocking-to-hide-your-ssh-daemon-from-attackers-on-ubuntu>
2. https://www.howtoforge.com/tutorial/how-to-use-port-knocking-to-hide-the-ssh-port-from-attackers-on-ubuntu/