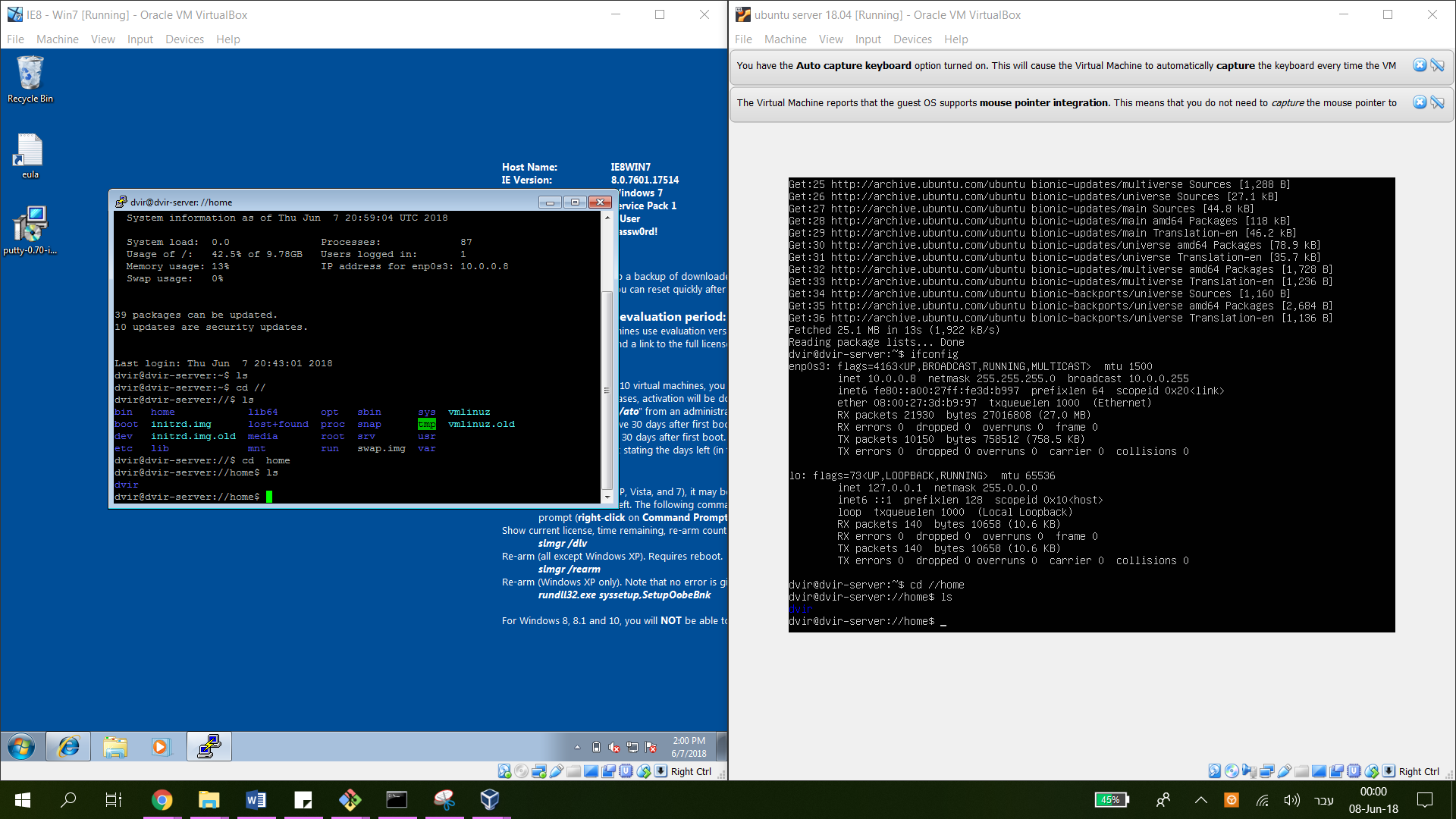
פתרון למטלה 4 – מעבדת סייבר הגנה

**Phase 1**

לאחר התקנת Virtual Box עם מכונה וירטואלית של Ubuntu Server הגדרתי את הגדרות הרשת של המכונה להיות על מצב Bridged והתחברתי דרך Putty בWindows - למכונה וירטואלית זו. בתמונה הבאה ניתן לראות שיצרתי תקייה בשם Dvir על המכונה ע"י חיבור דרך פורט 22.

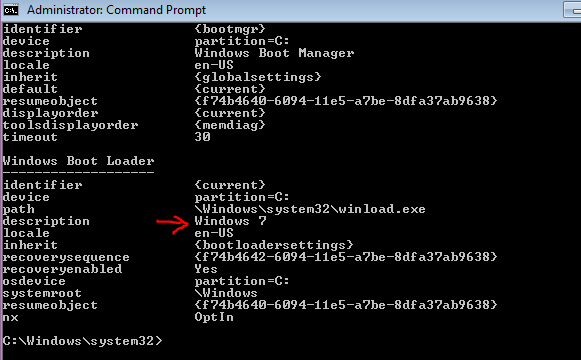


דרכים נוספות לשוטט בקבצים של מחשב אחר הן דרך הפרוטוקולים FTP ו-Telnet.

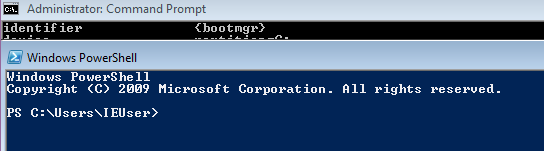
נבחן את ההבדלים בין הגדרות הרשת השונות במכונה וירטואלית:

* Host Only – משמעות הגדרה זו היא שהמכונה תקבל כתובת IP אך הכתובת תהיה נגישה רק למכונות שרצות על ה- VM. מחשבים אחרים לא יוכלו לתקשר עם המכונה שמוגדרת במצב זה.
* Bridged – במצב זה המכונה תתפקד כמחשב נוסף בתוך הרשת שלנו אך תהיה נגישה בכתובת הIP שלה לכולם.
* NAT – למכונה הוירטואלית תהיה כתובת IP משלה כמחשב נוסף בתוך הרשת ותוכל לגשת לאינטרנט. אולם מחוץ לרשת לא נוכל לגשת ישירות לכתובת הIP של המחשב.

**Phase 2**



לפי התיאור ניתן לראות שהשם והגרסה של הboot manager הוא Windows 7.

כפי שניתן לראות בתמונה, אני השתמשתי ב-Command Prompt Shell. אולם קיימים Shells נוספים. לדוגמא – Windows PowerShell: 

יצרתי קובץ Dvir.txt שמכילים חמש פסקאות שהעתקתי מהאתר Lorem ipsum וקראתי את התוכן שלו דרך ה-PowerShell בעזרת הפקודה get-content .\Dvir.txt

תיעוד של תהליך המחיקה של ה-kernel הנוכחי והתקנת kernel חדש:

עדכנתי את כל המאגרים של המערכת:

*sudo apt update*

ושדרגתי את כל החבילות:

*sudo apt upgrade –y*

לאחר מכן נעשה ריבוט למערכת כדי לוודא שכל השינויים יכנסו לתוקפם בעזרת הפקודה

*sudo reboot*

*וידאתי שלא קיימים עדכונים נוספים שעליי לעשות בעזרת הפקודה*

*sudo apt list –upgradeable*

ומכאן המשכתי לשדרוג ה-kernel שלי לאחד חדש.

בתמונה הבאה ניתן לראות מהי הגרסה של ה-kernel הנוכחי:



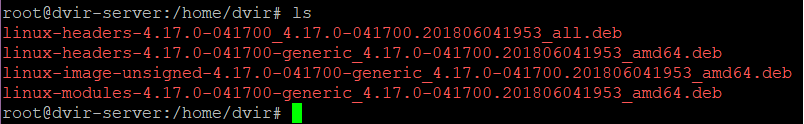
אחרי זה נכנסתי לאתר <http://kernel.ubuntu.com/~kernel-ppa/mainline/> ונכנסתי לגרסה העדכנית ביותר שיש – 4.17 והורדתי את הקבצים הנדרשים בעזרת הפקודות:

wget <http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.17/linux-headers-4.17.0-041700_4.17.0-041700.201806041953_all.deb>

wget <http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.17/linux-headers-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb>

wget <http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.17/linux-image-unsigned-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb>

wget <http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.17/linux-modules-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb>



כעת, בעזרת הפקודה *dpkg -i \*.deb אנו נתקין את ארבעת החבילות שהורדנו*.

בסיום ההתקנה נריץ את הפקודות:

*sudo update-grub  
sudo reboot*

אחרי כל זה, ניתן לראות שעדכנו את ה-kernel שלנו לגרסה החדשה ביותר 4.17.

לאחר שעברנו לגרסה העדכנית ביותר אנו יכולים למחוק את הגרסה הישנה שבה השתמשנו לפני העדכון, גרסה 4.15:

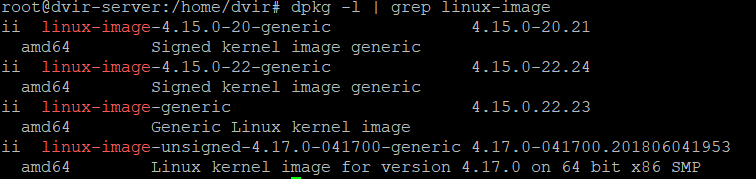
ע"מ להסיר את הגרסה הישנה נשתמש בשורת הפקודה של **byobu** , שבעזרתה נוכל לבצע את התהליך בצורה בטוחה בלי למחוק בטעותאת הגרסה שבה אנחנו משתמשים כרגע.

נתקין את byobu:

*sudo apt install byobu*

אחרי שאנו מסיימים להתקין, נבדוק איזה גרסאות ישנות יש לנו על המחשב בעזרת הפקודה

*dpkg -l | grep linux-image*



בתמונה זו נוכל לראות שיש גם את הגרסה הישנה שהייתה לנו 4.15, וגם את הגרסה החדשה שהורדנו 4.17.

אם נריץ את הפקודה

*sudo purge-old-kernels*

אנו נמחק את כל הגרסאות הישנות שיש ברשותנו, מלבד ה-2 האחרונות (כך מוגדר להיות כברירת מחדל, כדי להיות בטוחים שאם הkernel החדש נכשל אזי יהיו לנו 2 גרסאות נוספות לחזור אליהן).

--

בחלק זה נעזרתי במדריך המפורט: <https://www.howtoforge.com/tutorial/how-to-upgrade-linux-kernel-in-ubuntu-1604-server/>

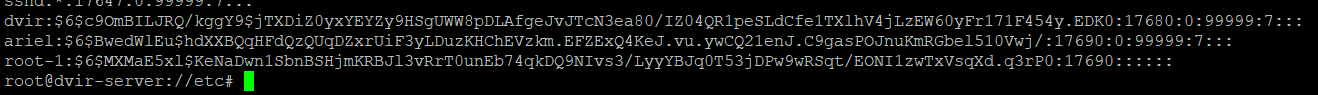
**Phase 3**

יצרתי משתמש חדש בשם ariel:



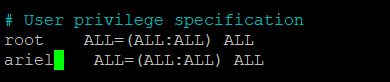
כמו כן, יצרתי משתמש נוסף בשם root-1 באופן ידני ע"י עריכת הקובץ passwd: 

ולאחר מכן הוספתי סיסמה בעזרת הפקודה passwd root-1 , ניתן לראות בתמונה הבאה שהתווספה שורה עם הסיסמה המוצפנת בסוף הקובץ shadow:

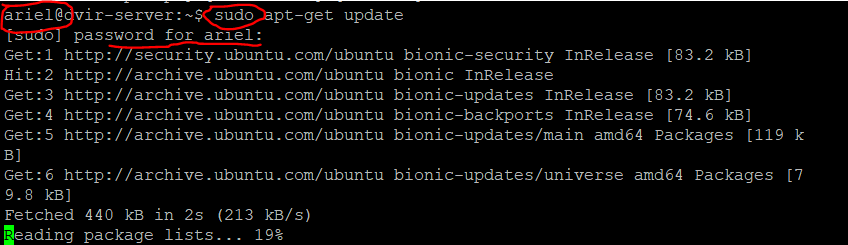


הרשאת sudo למשתמש ariel:

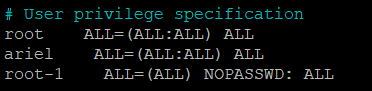
נריץ בהרשאת ה-root הנוכחית את הפקודה sudo visudo ונערוך את הקובץ תחת הכותרת User privilege specification כך שגם למשתמש ariel יהיו הרשאות:



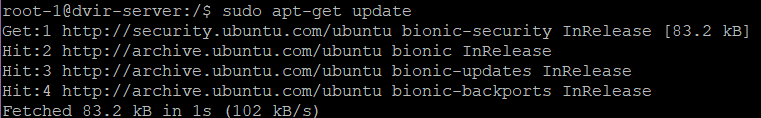
ואחרי ששמרנו אנו יכולים להתחבר למשתמש ariel ולהשתמש בsudo:



כדי לאפשר למשתמש root-1 להשתמש בפקודות sudo ללא צורך בהזנת סיסמה עלינו להזין שוב את הפקודה sudo visudo ולהוסיף את השורה הבאה (נעשה את זה מהמשתמש ariel, בשביל הקטע):

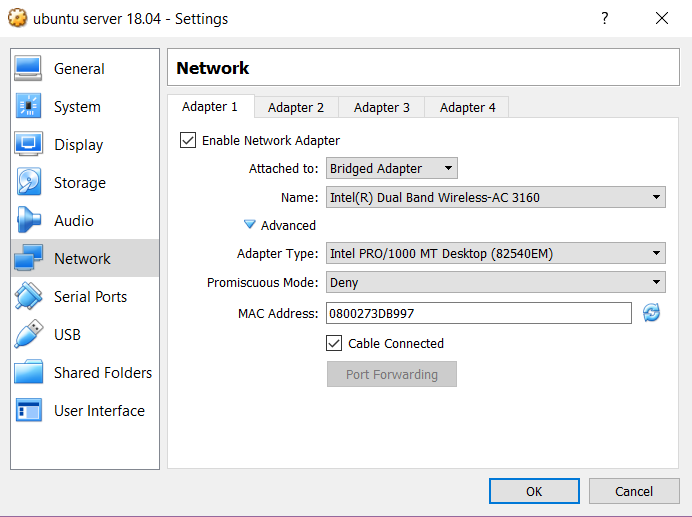


לאחר שמירת השינויים, נוכל להתחבר למשתמש root-1 ולהשתמש בפקודות sudo ללא צורך בהזנת סיסמה:

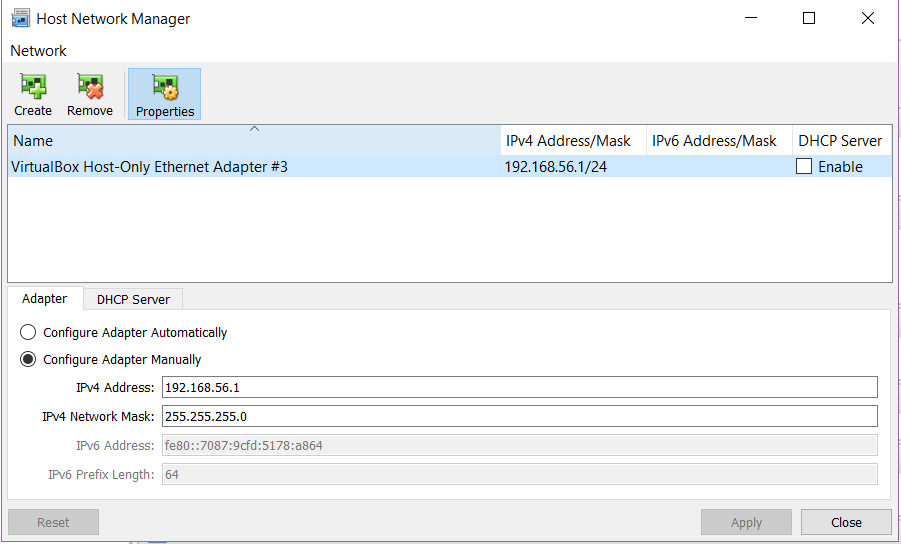


**Phase 4**

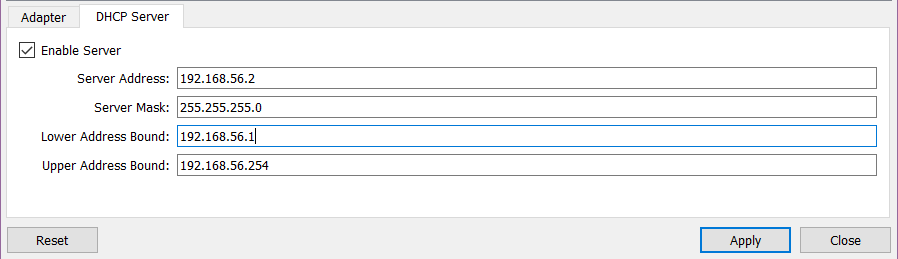
ניתן לשנות את כתובת הMAC כפי שניתן לראות בתמונה:



לאחר השינוי קיבלתי כתובת MAC חדשה: 080027B3A88F

ובמצב רשת Host-Only נשנה את הכתובת IP באופן ידני (ה-DHCP במצב Enable): 

נאפשר לDHCP להעניק למכונות כתובת IP בתחום קבוע, וכך הכתובת תוכל להשתנות מפעם לפעם שאנו מתחברים לרשת:



כמו כן נוכל להוסיף למכונה ממשקים נוספים לרשת כך שלכל ממשק תהיה כתובת IP משלו וכך לאותה מכונה יהיו כמה כתובות IP.