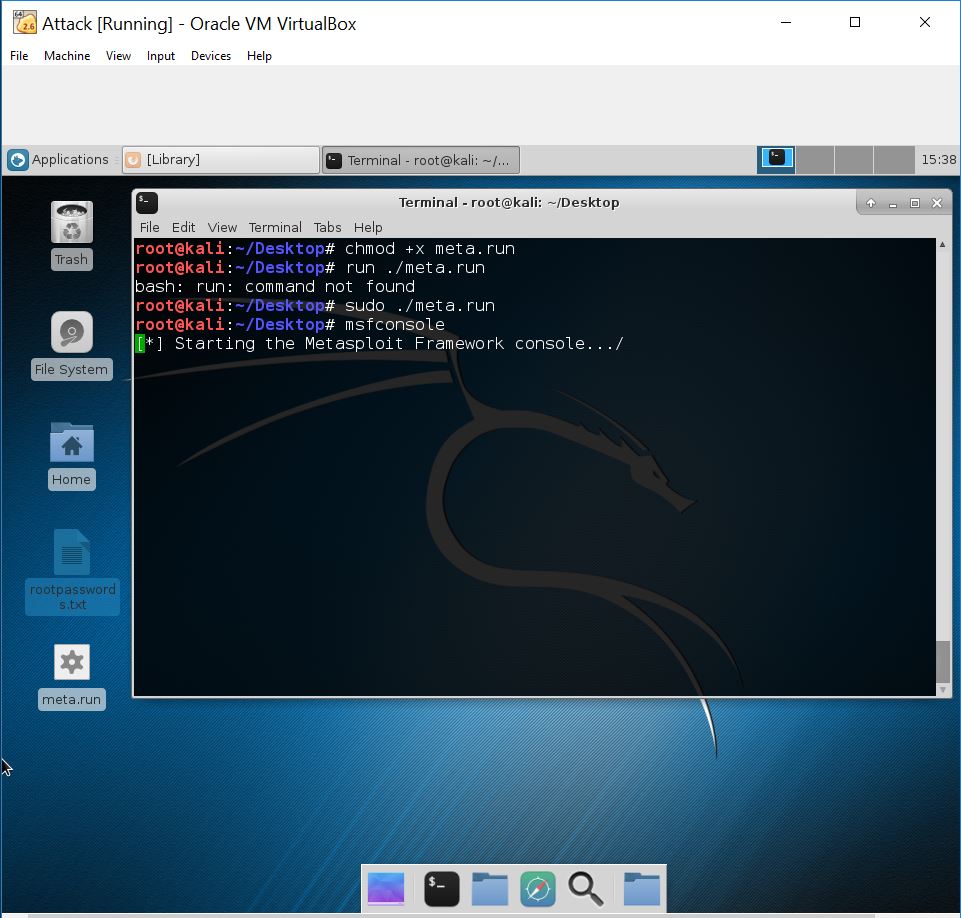
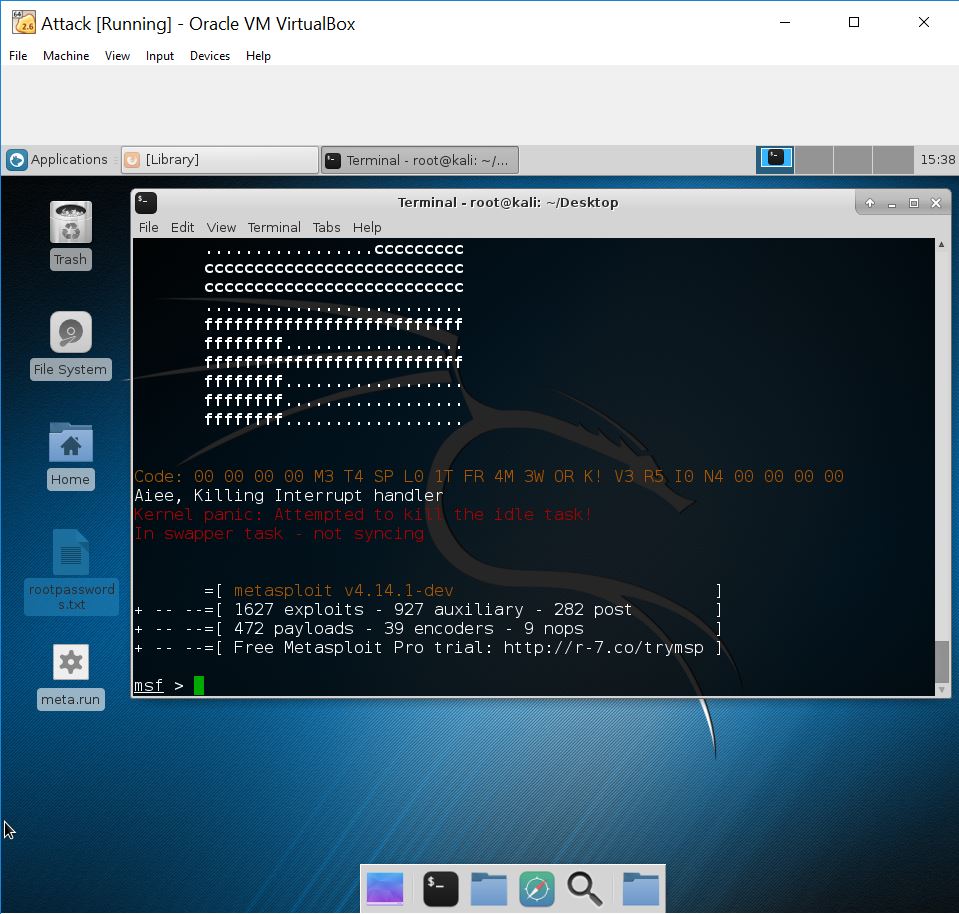
***שלב 4: תקיפת מכונת היעד***

בשלב הקודם השתמשנו במספרי הפורטים שמצאנו על מנת לפתוח את פורט 22 כדי להתחבר בSSH למחשב המטרה (המחשב של אדוארד).

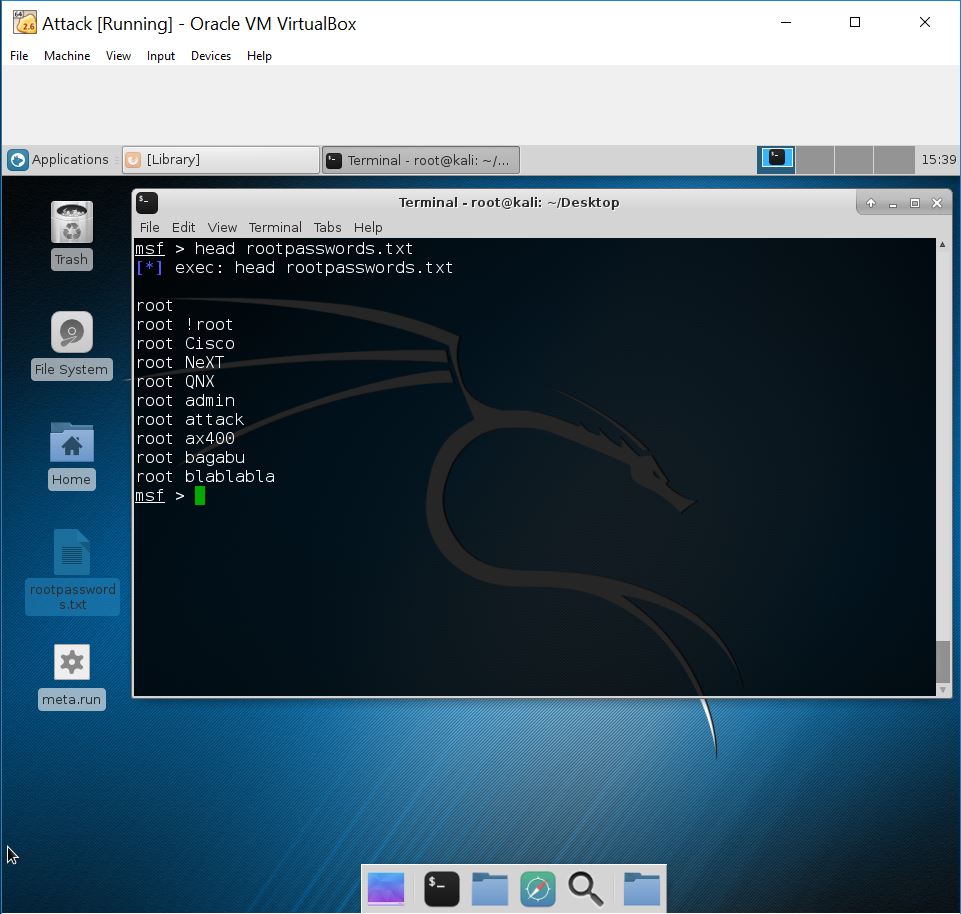
כמו כן, יש ברשותנו קובץ טקסט המכיל אוסף של שמות משתמש וססמאות מופרדים ברווחים וירידת שורה.

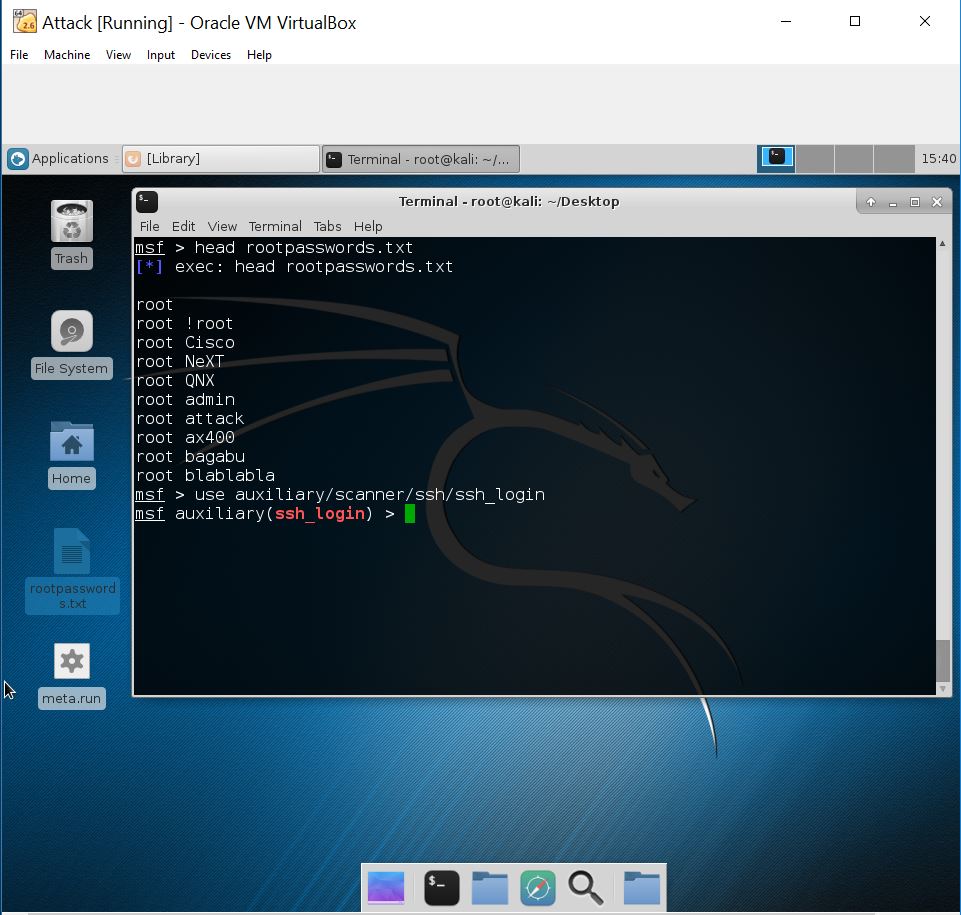
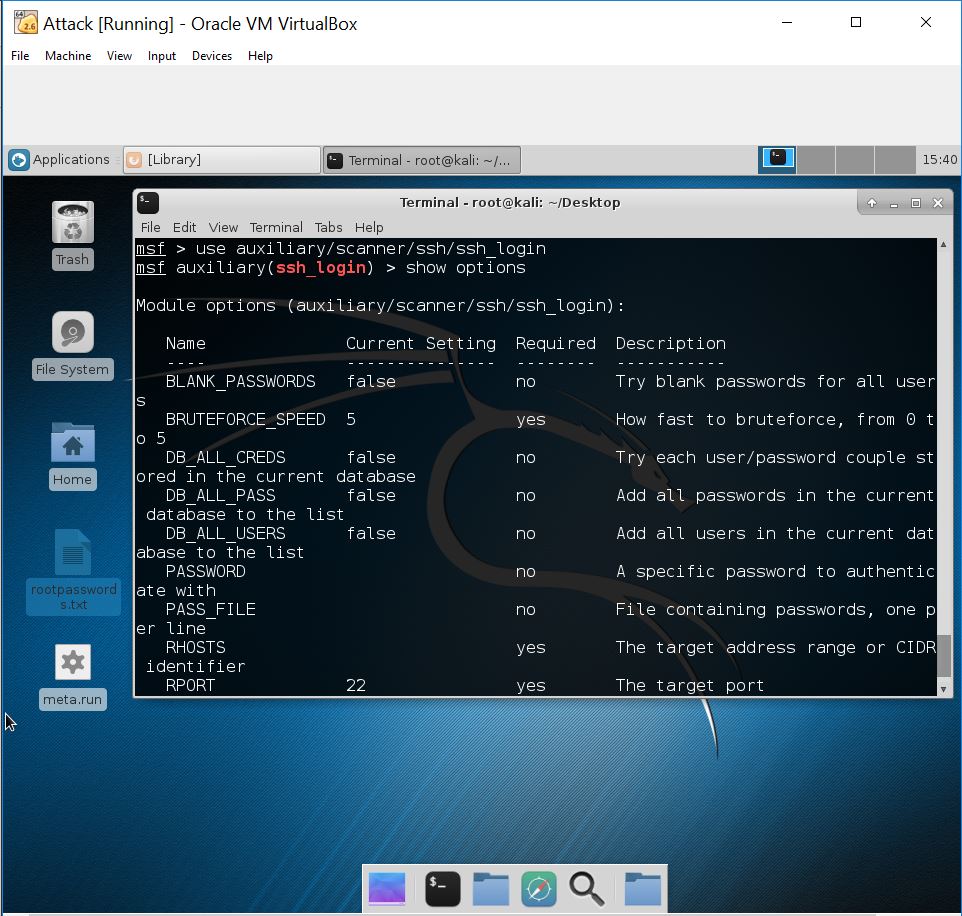
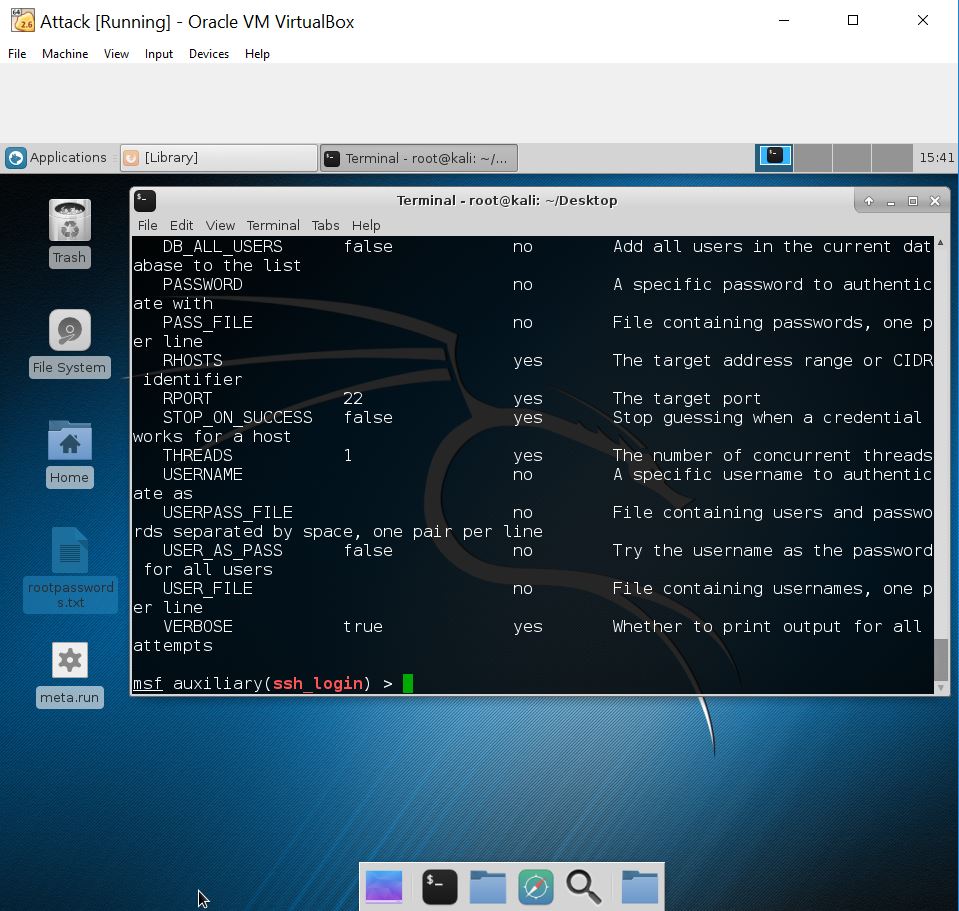
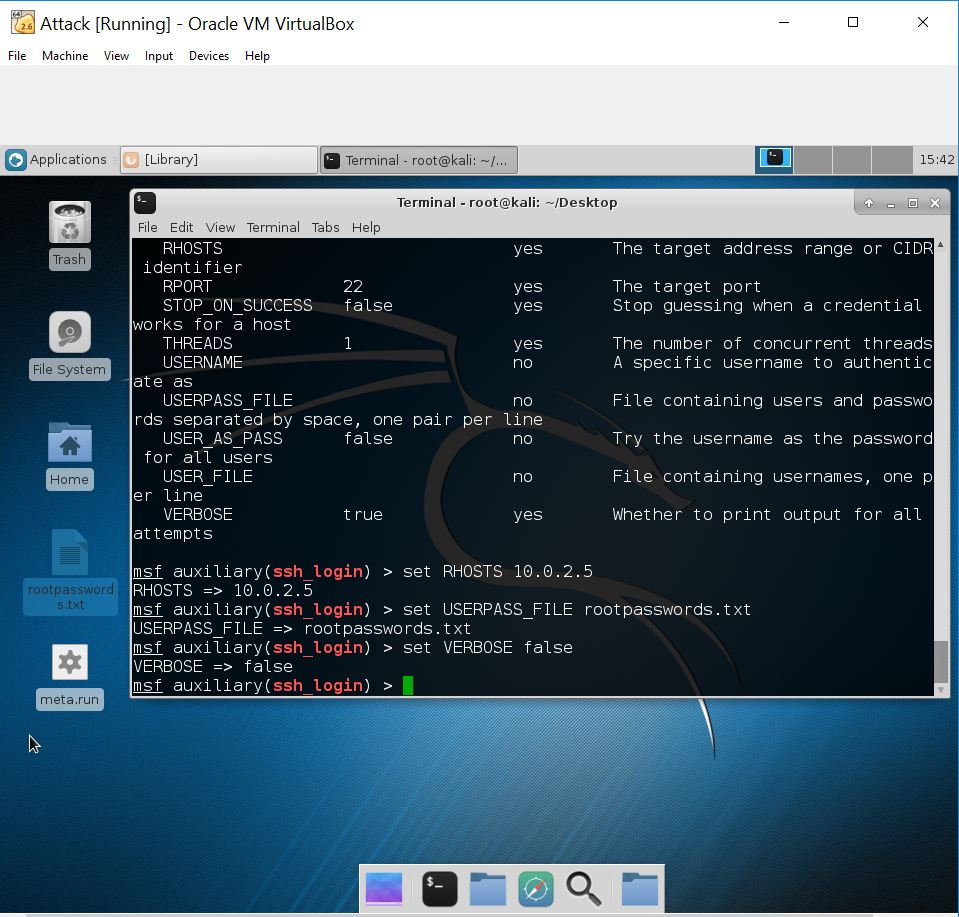
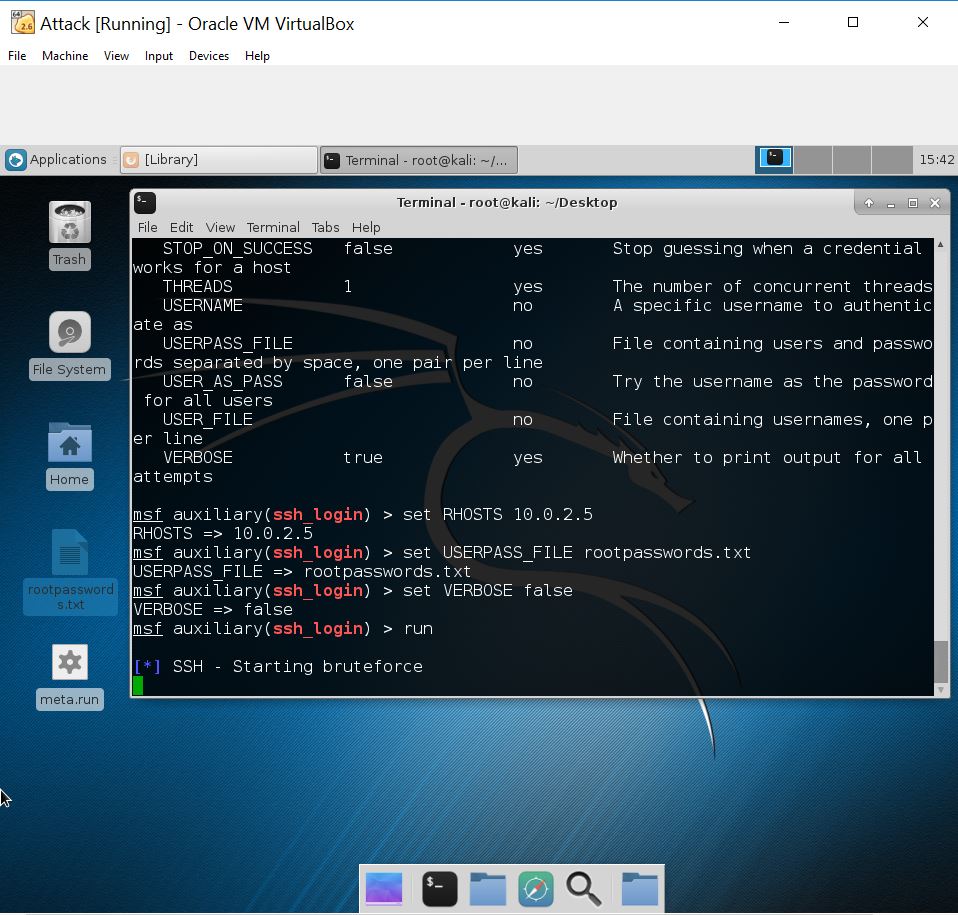
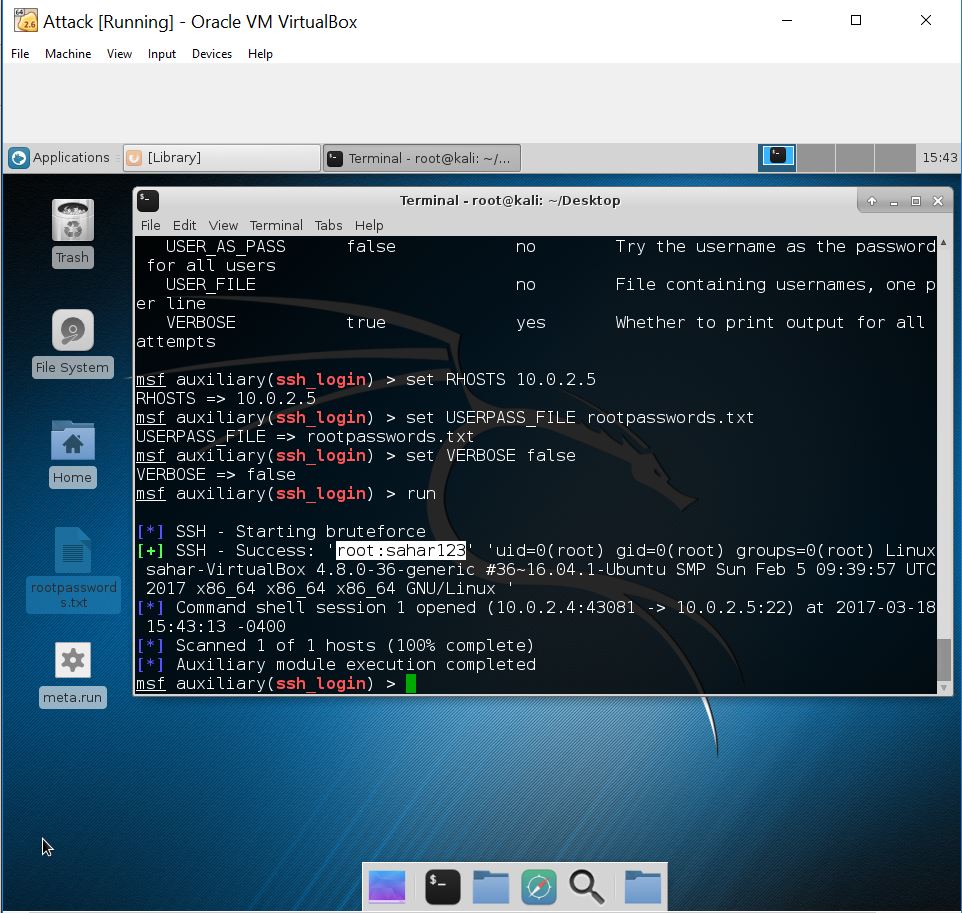
כעת נרצה להשתמש בMetasploit כדי לבדוק את הססמאות בBrute Force ולהשיג גישת root למכונה.

1. נפעיל את קונסול הMetasploit:



1. נבדוק שקובץ הססמאות נקרא בצורה תקינה על ידי Metasploit על ידי הפקודה:  
   Head <file\_name>.txt

  
הערה: חשוב להריץ את Metasploit כשאנחנו באותה תיקייה כמו הקובץ כדי שלא נהיה צריכים לספק את הנתיב המלא. בדוגמא הקובץ נמצא בdesktop (ניתן לעבור בין תיקיות על ידי הפקודה cd) .

1. נבחר את המודול המבצע Brute Force על login בSSH :  
   use auxiliary/scanner/ssh/ssh\_login  
   
2. נתבונן בפרמטרים שהמודול מקבל:  
   Show options  
   
3. כעת נגדיר 3 פרמטרים: קובץ הססמאות, מחשב היעד, ונבטל פירוט נוסף (כדי להקל על קריאת התוצאות).  
   <Set RHOST <target\_ip   
   Set USER\_PASSFILE meta.txt  
   Set VERBOSE false 
4. נפעיל את המודול על ידי הפקודה: Run
5. במידה והכל כשורה המודול יחזיר איזה משמות המשתמש והסיסמא הנכונים.
6. נשתמש בססמא על מנת להתחבר לSSH Client של מחשב היעד.

ssh root@<target\_ip>

בשלב זה השגנו גישה לroot - השלמנו את האתגר.