**משימה ראשונהsyn flood attack –**

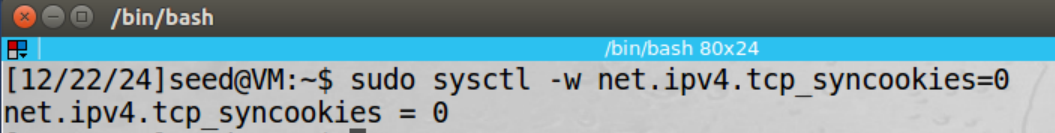
**מבוא:**

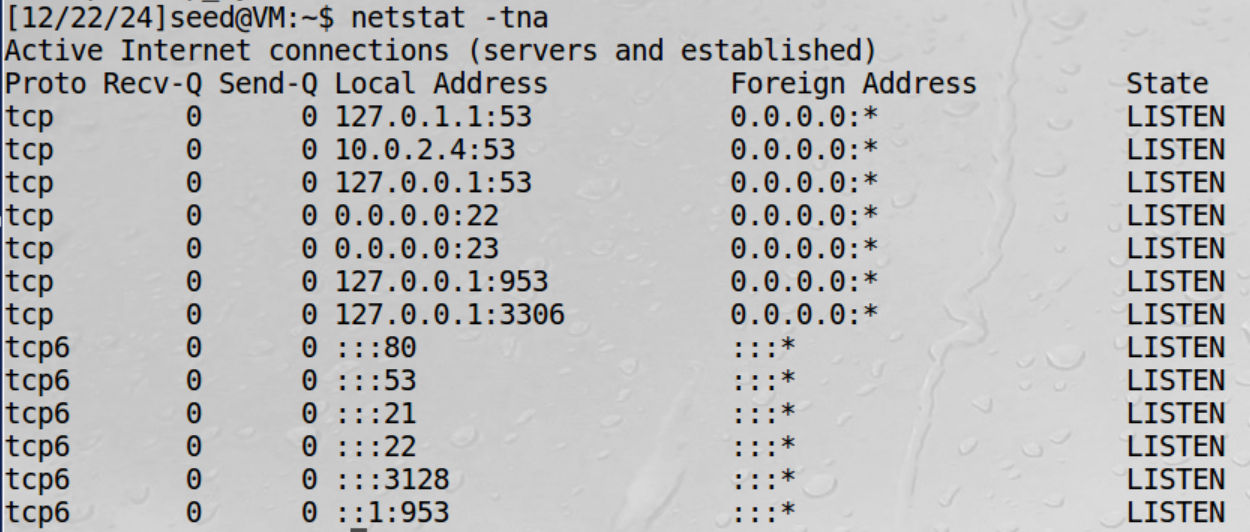
**Attacker: 10.0.2.15**

**Server: 10.0.2.4**

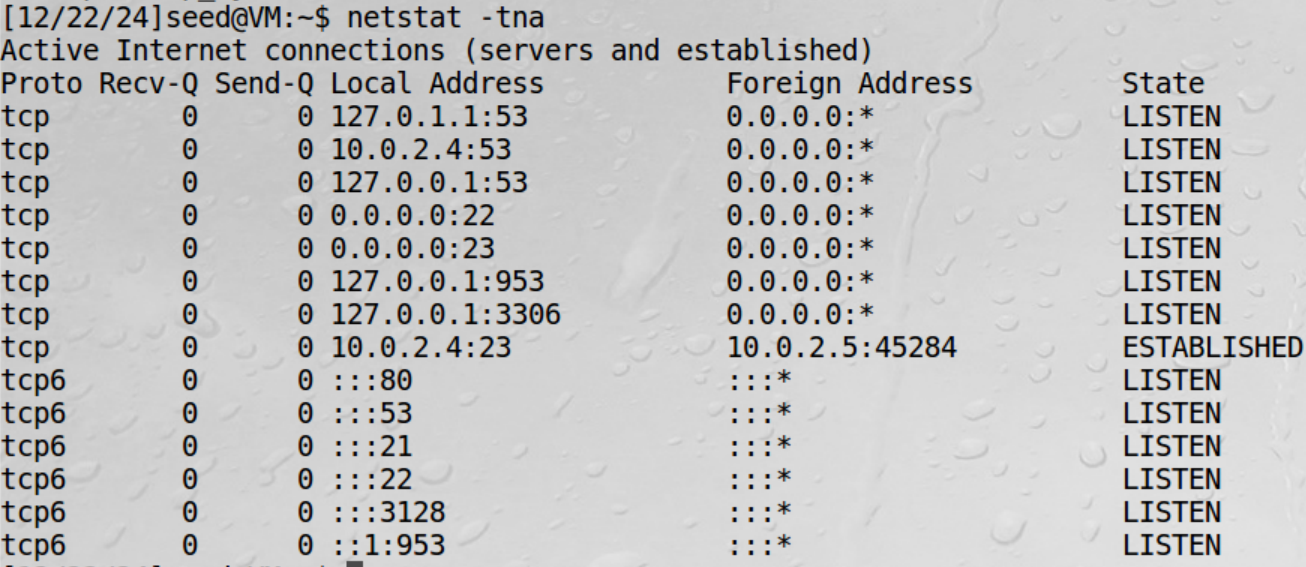
**Client: 10.0.2.5**

**ביצוע:**

**תחילה נבטל את ה-syn cookie כדי שנוכל לתקוף:**

**נבדוק ונראה שכל הפורטים במצב listening ולא מחוברים:**

**נתחבר לשרת:**

****

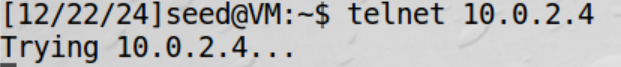
**נתקוף את השרת:**

****

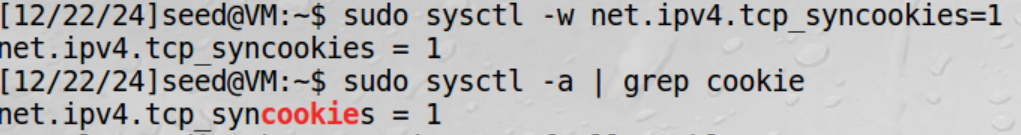
**פורט 23 התמלא:**

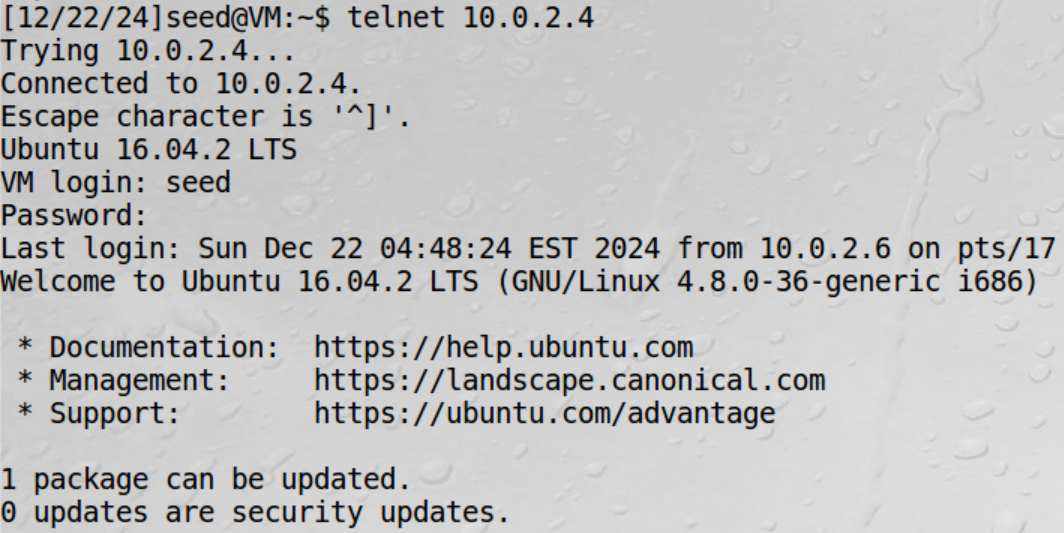


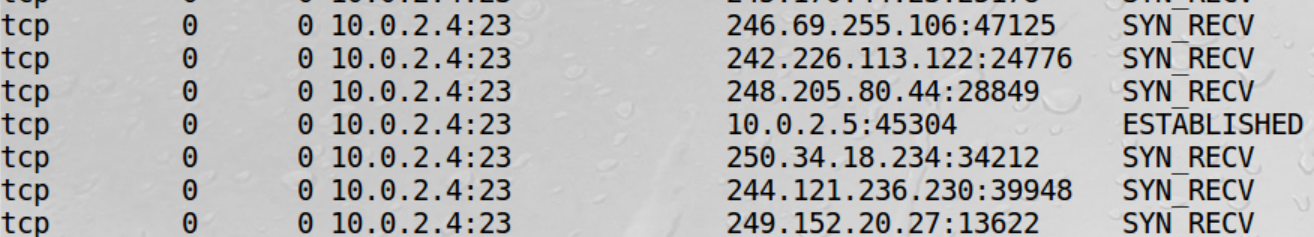
**והקליינט לא הצליח להתחבר:**



**הגנה עם החזרת syn cookie :**



**ננסה לתקוף שוב ללא הצלחה ונצליח להתחבר:**

****

**סיכום המשימה:**

אכן הצלחנו לבצע את המשימה, מה שלמדנו בתאוריה אכן קרה. הייתה בעיה אחת שלא הייתה תקשורת בין המכונה של התוקף לשרת ולקליינט. ונזכרתי שלא שיניתי את ההגדרות. וששיניתי הכל עבד כמו שצריך. (שיניתי ל-Nat network)

בס"ד

**משימה שניה** **TCP Reset Attack on Telnet connections–**

**מבוא:**

**מתקפת TCP Reset היא שיטה שמטרתה לנתק חיבורים בין שני צדדים המתקשרים בפרוטוקול .TCP**

**בעבודה נשתמש בכלי Wireshark ונבצע את המתקפה על ידי זיוף חבילת . reset (RST) נבחן את המתקפה בשני תרחישים: פעם אחת על חיבור Telnet ופעם נוספת על חיבור SSH בין הלקוח לשרת.**

**Server: 10.0.2.4**

**Client: 10.0.2.5**

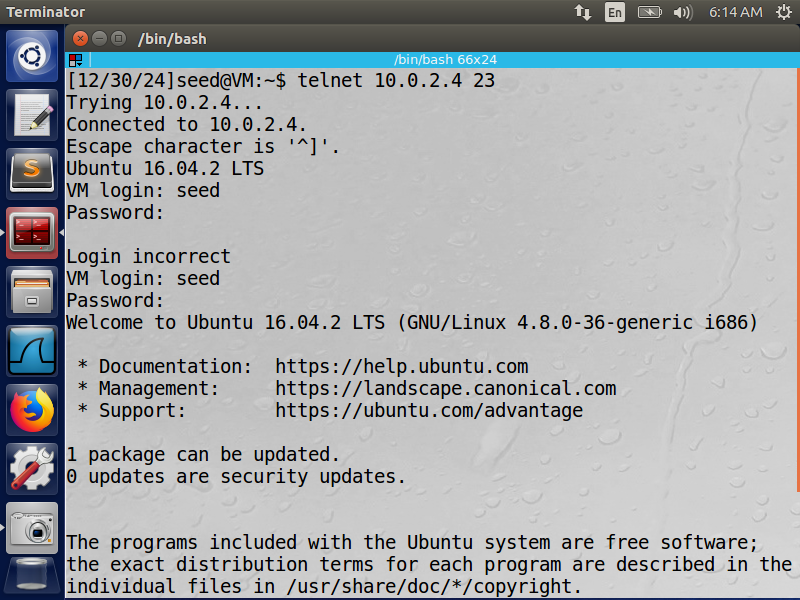
Tcp connection

RST packet

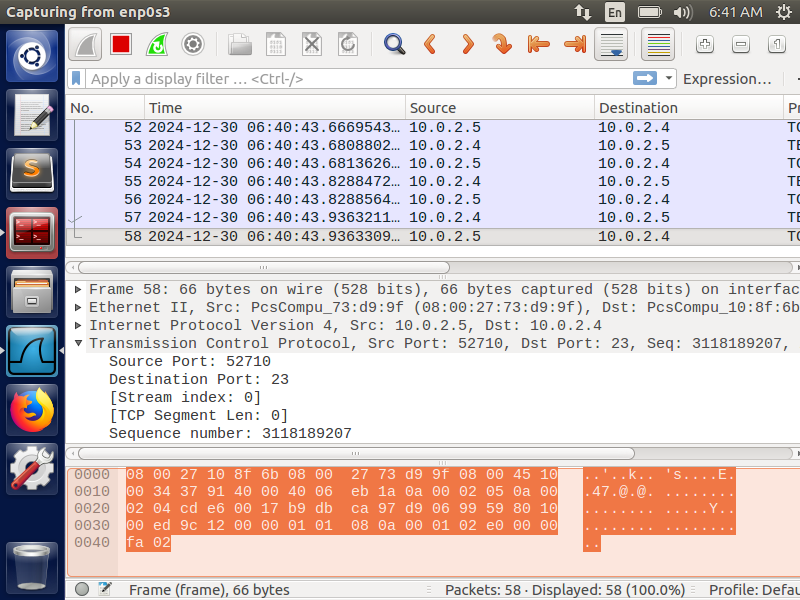
**Attacker: 10.0.2.6**

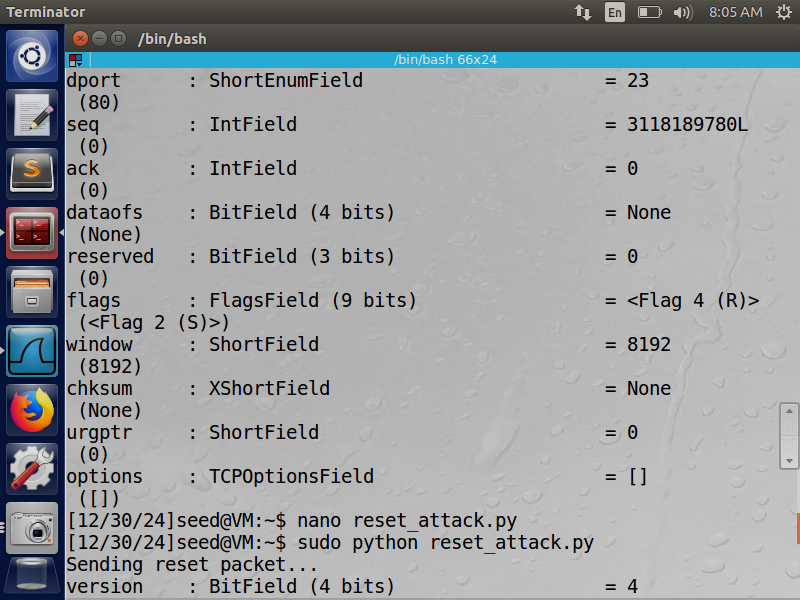
**ביצוע:**

**השתמשנו ב-Telnet כדי ליצור חיבור TCP לא מוצפן מהלקוח לשרת מרוחק ביציאה 23.**

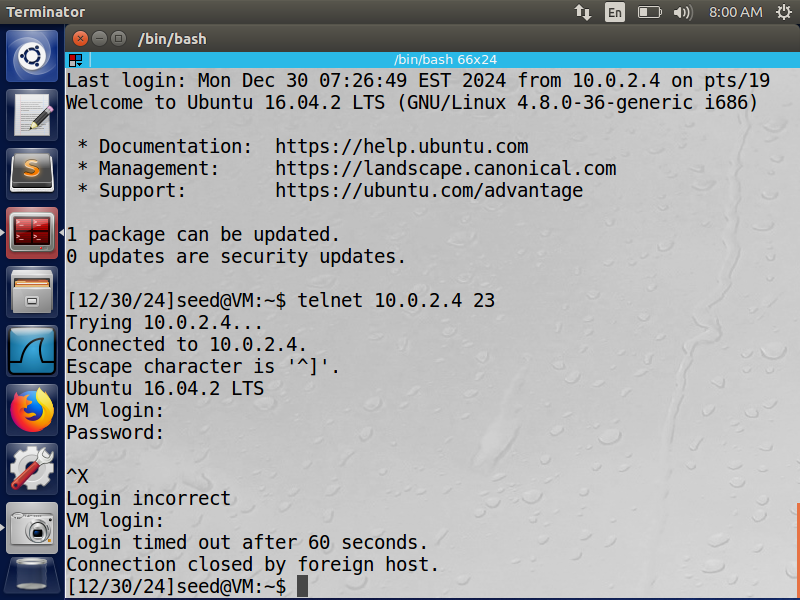


**כאן התוקף משיג את הפרטים של השרת והלקוח(כתובות, פורט, מספר רצף)**



**יצרנו קובץ reset attack עם הפרטים שהשגנו ונשתמש בפקודה sudo python reset\_attack.py כדי לשלוח את החבילה...** 

**אחרי ששלחנו את החבילה ראינו אצל הלקוח שאכן החיבור נותק עם השרת**



**סיכום המשימה:**

בסוף, הצלחנו את המתקפה וניתקנו את החיבור בין הלקוח לשרת באמצעות יצירת חבילת RST (Reset) עם הנתונים הנכונים שהשגנו.

הבעיה שנתקלנו שלא כתבנו נכון את sequence number

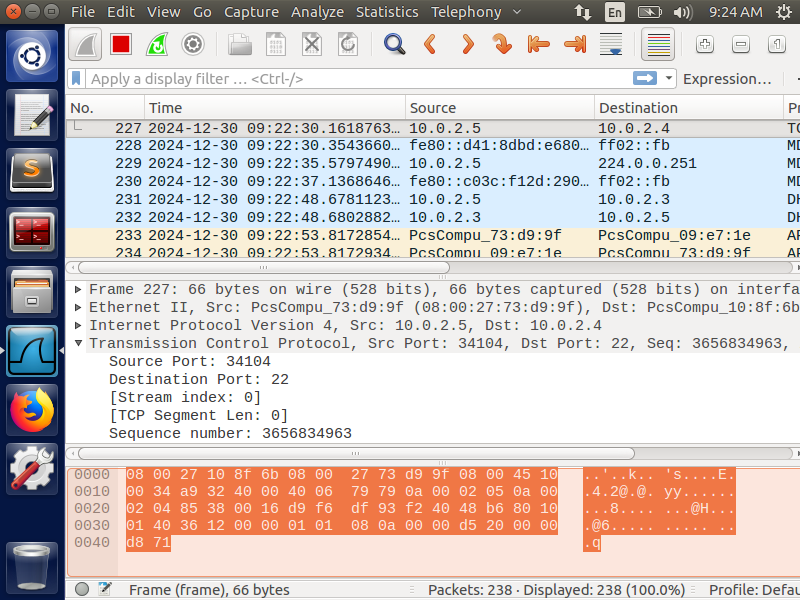
אחרי שתיקנו קיבלנו את השגיאה שהחיבור נותק מהצד של הלקוח וזה עבד.

בס"ד

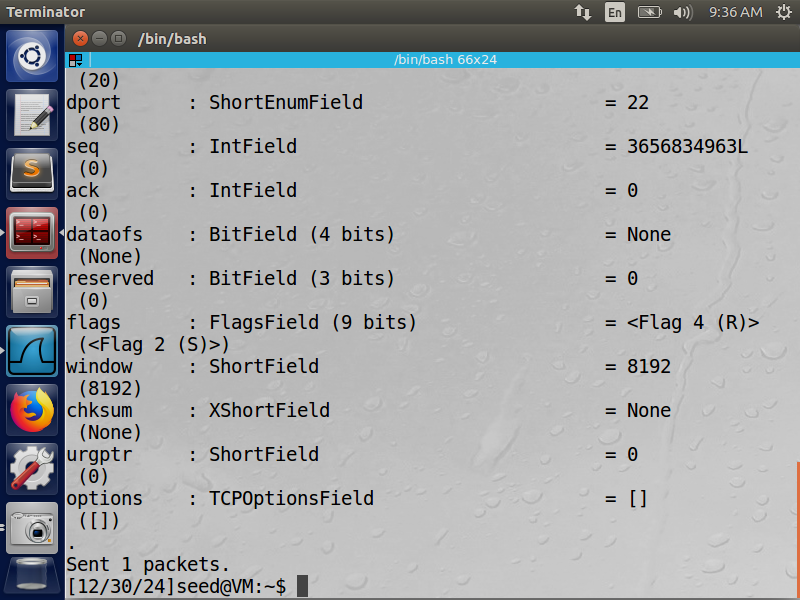
**משימה שלישית-** **TCP Reset Attack on SSH connections**

**ביצוע:**

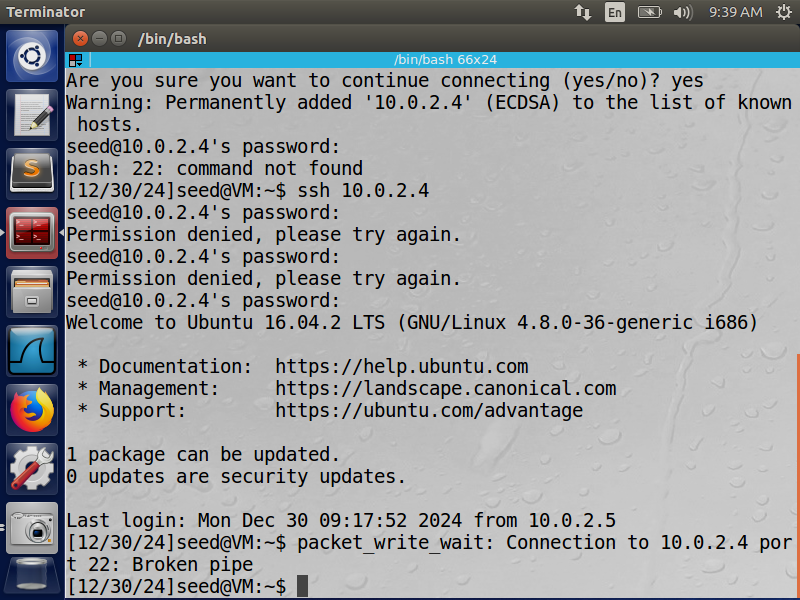
**בדיוק כמו המשימה הקודמת רק הפעם נשתמש בSSH כדי ליצור חיבור בין הלקוח לשרת. ונחליף את מספר הפורט מ-23 (Telnet) ל-22 (SSH).**



**שלחנו את החבילה resetעם השינויים עם אותה פקודה כמו מקודם..**



**אחכ חזרנו ללקוח וראינו שהחיבור של הלקוח והשרת נותק בהצלחה**



**סיכום:**

הצלחנו לבצע מתקפת  **TCP Reset Attack** על חיבורי **SSH** באמצעות יצירת חבילת RST עם כתובות פורט וכו נכונים. למרות שהחיבור מוצפן, ההצפנה מגנה רק על תוכן הנתונים ולא על המידע שבכותרת החבילה, ולכן המתקפה הצליחה. כתוצאה מכך, הצלחנו לנתק את החיבור בין הלקוח לשרת.

**משימה רביעית - TCP Session Hijacking**

**מבוא:**

**בתקיפה זו בעזרת ה-wireshark נתפוס את הפקטה האחרונה בחיבור ה-telnet שניצור בין הקליינט לסרבר. וניצור פקטה בשם הקליינט כדי שהסרבר ישלח את התוכן של הקובץ הסודי לתוקף.**

**Attacker: 10.0.2.6**

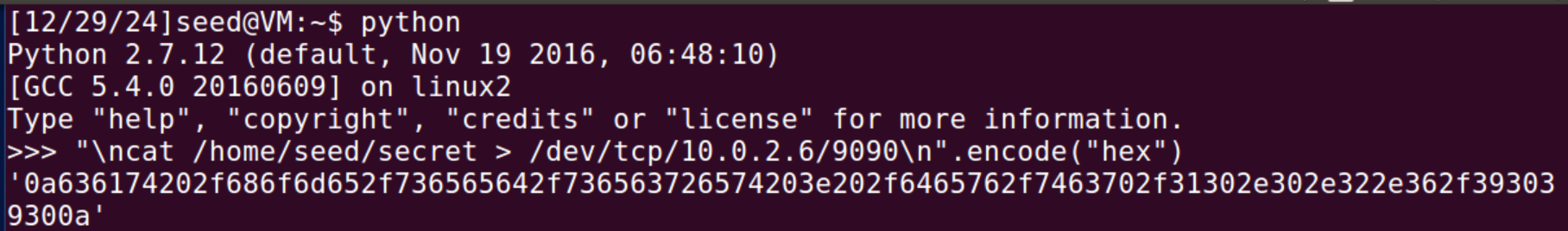
**Server: 10.0.2.4**

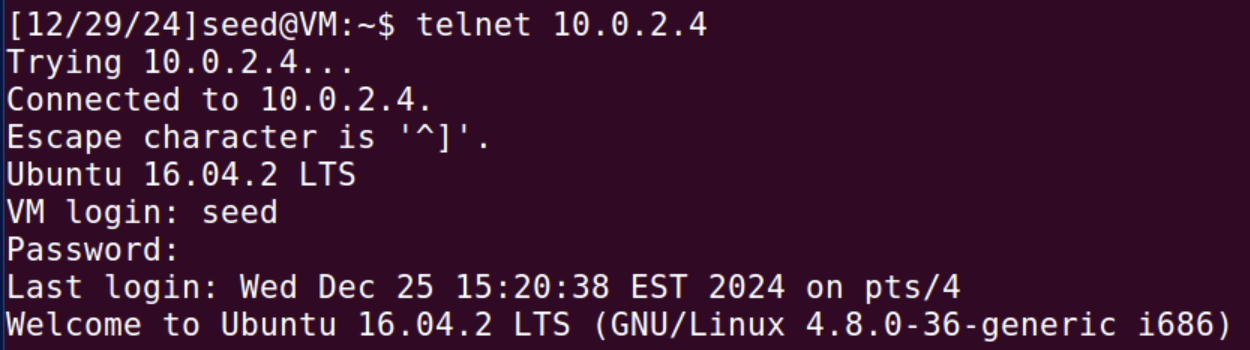
**Client: 10.0.2.5**

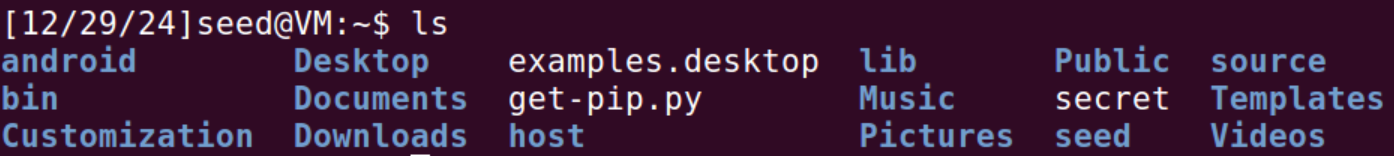
**ביצוע:**

**יצירת קובץ סודי ב-server: (בעיה 1 לא היה קיים קובץ כזה אז יצרנו אותו):**

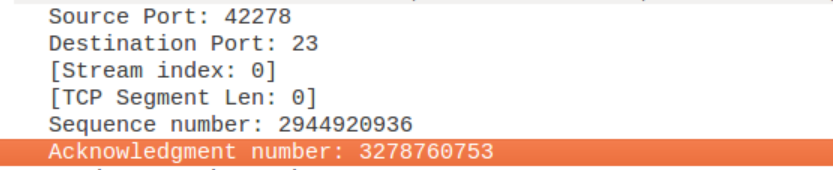
****

**המרת הפקודה הרצויה ל-hex:**

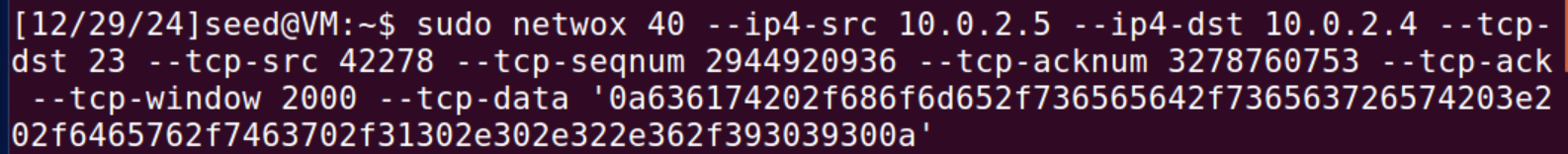
**פתיחת חיבור telnet בין הלקוח לשרת + שליחת פקודה ב-telnet:**

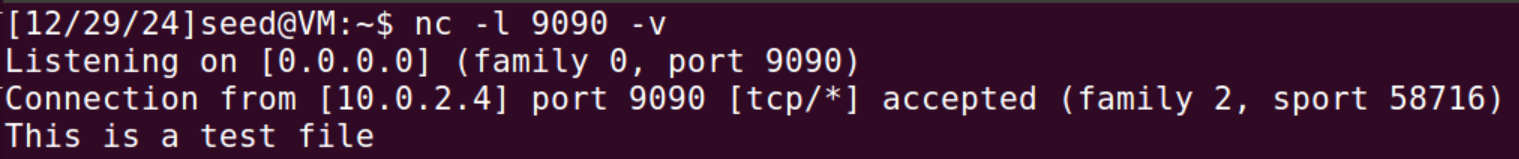


**תפיסת הפקטה האחרונה לאחר פתיחת תקשורת TCP ולקיחת הנתונים ממנה.**



**יצירת הפקטה:**

****

**קבלת ההודעה מהקובץ:**

**סיכום משימה:**

גילינו שבעזרת Wireshark אפשר לזהות פקטה ולדמות בקשה. הבעיה שהיתה לי זה ביצירת הקובץ שבסוף רשמתי פקודה שתיצור אותו כולל תוכן.

בנוסף היתה לי בעיה ביצירת הפקודה ואז שמתי לב שהיה צריך לרשום \n בהתחלה ובסוף.