מעבדה 2

CYBER SCHOOL

התקפת תקשורת DoS DDoS

הרצת Dos

CYBER SCHOOL

נושאי המעבדה

הבנת הדרך לביצוע מתקפת Dos בעזרת מערכת ההפעלה Kali Linux.

זמן מוערך

20-30 דקות

סביבת מעבדה

- VirtualBox
- Kali Linux
- Windows 10

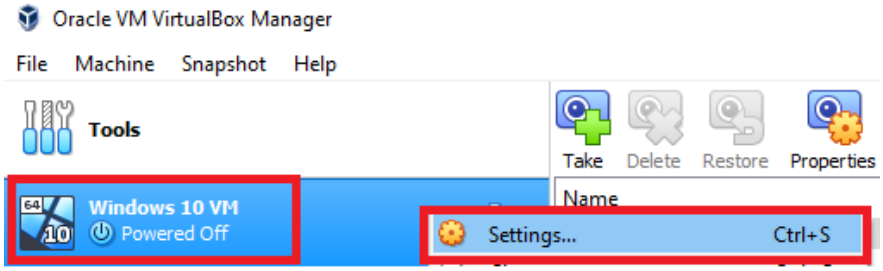
משימת מעבדה

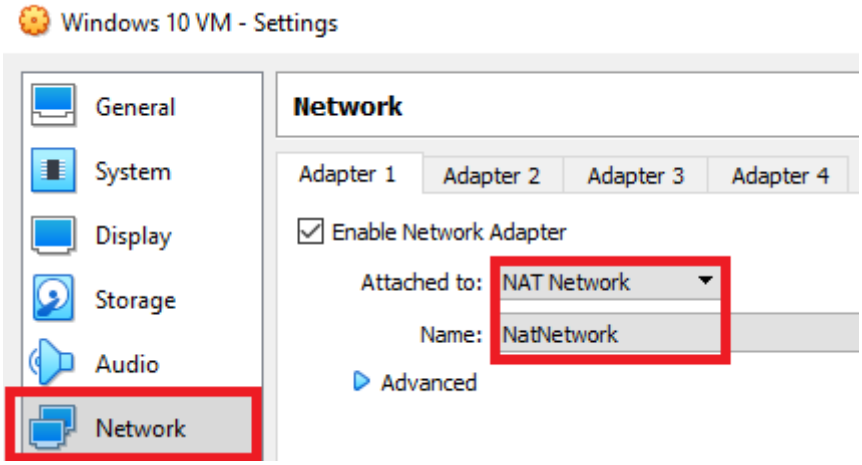
משימת מעבדה: ביצוע מתקפת arpspoof במחשב Windows

יש לבצע מתקפת מניעת שירות על המכונה הווירטואלית של Windows ולגרום למניעת שירות.

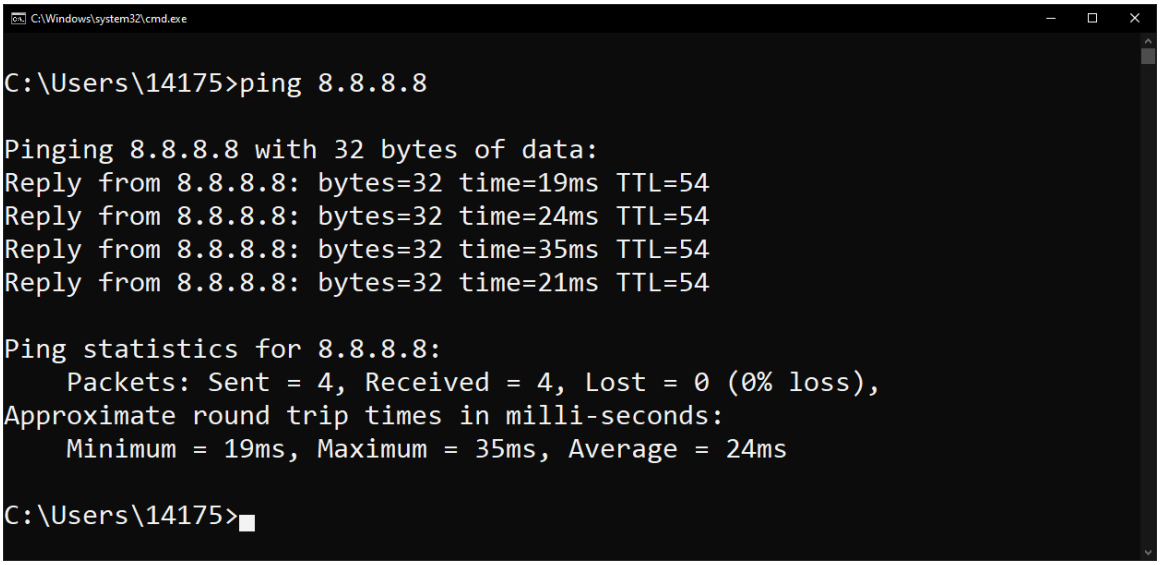
1 ב-Oracle VM VirtualBox Manager, יש ללחוץ על הלחצן הימני על שם המכונה ולבחור באפשרות **Settings**. יש לנווט למקטע **Network** ולוודא ששני המחשבים מוגדרים אל אותה רשת NAT.

הערה: יש לבצע את השלב הזה במכונה הווירטואלית של Kali Linux ושל Windows 10.

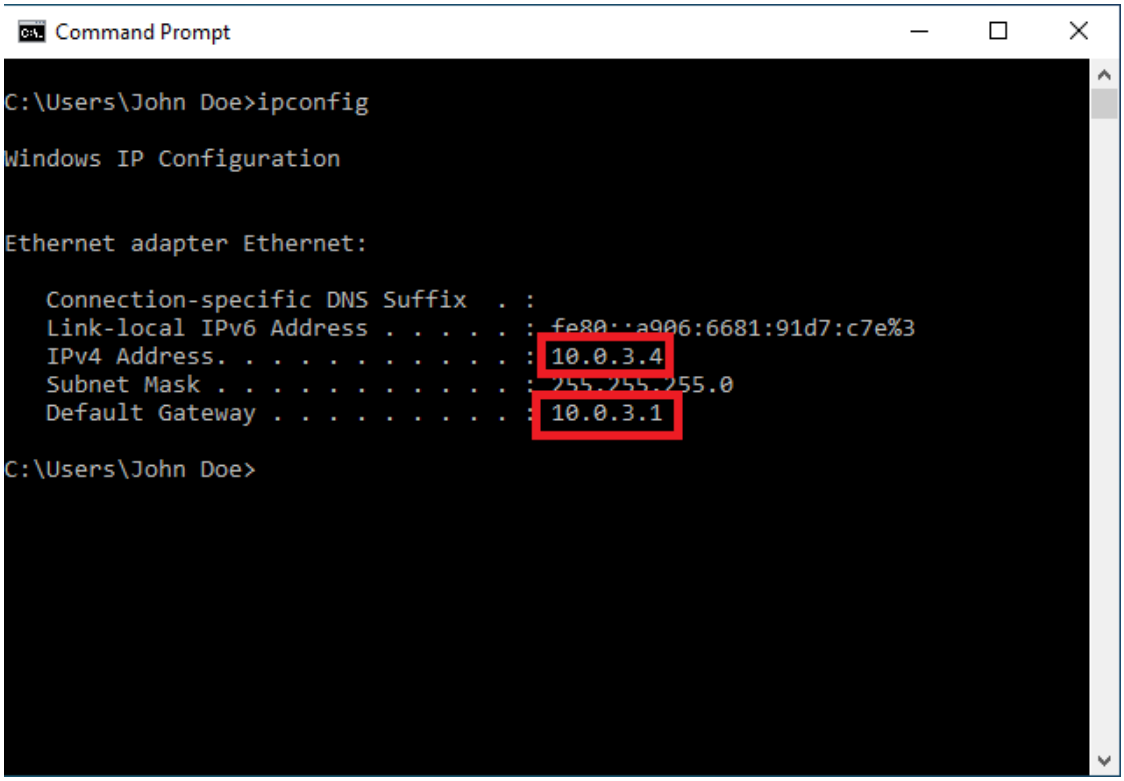




2 במחשב ה-Windows, יש להריץ פקודת ***ping*** אל ***8.8.8.8***, או להיכנס לאתר באמצעות הפקודה ***ping 8.8.8.8*** בדי לוודא שתקשורת רשת NAT פועלת בראוי.

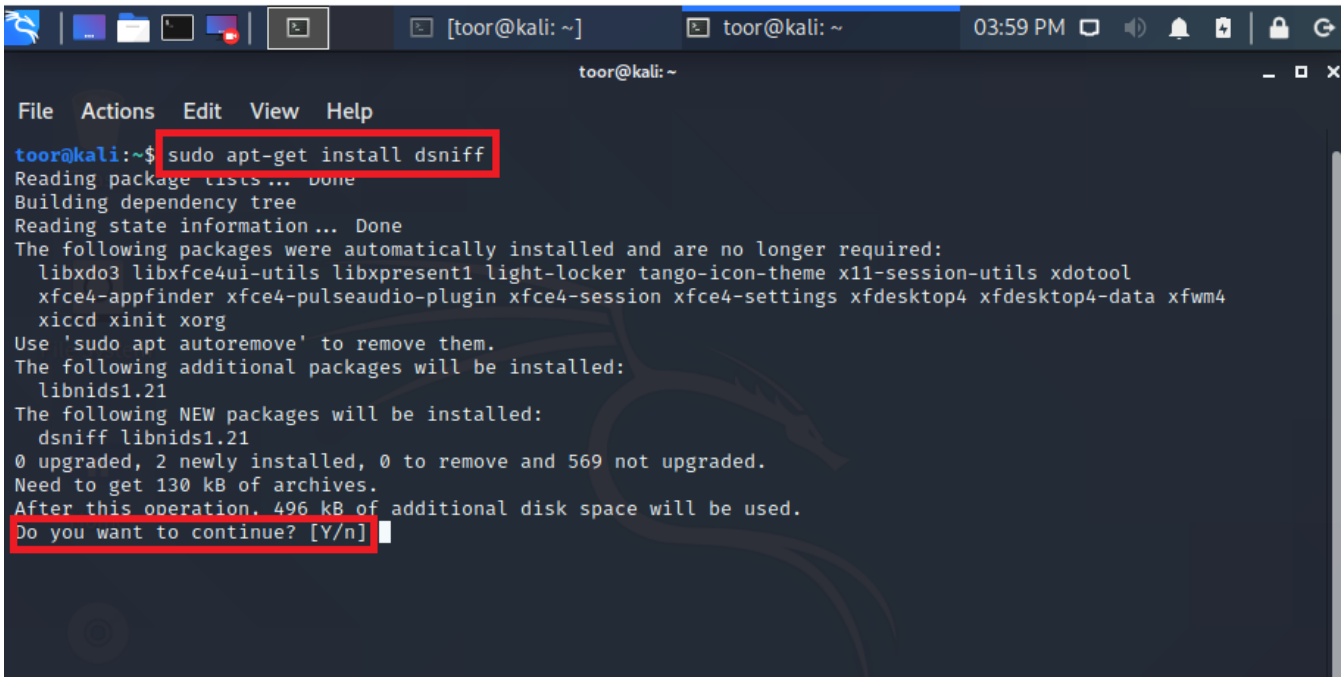


3 יש לשים לב לקונפיגורציית ה-IP של המכונה הווירטואלית Windows VM.
הערה: בדוגמה שלנו, כתובת ה-IP הוא ***10.0.3.4*** ושער ברירת המחדל הוא ***10.0.3.1***.



4 יש לפתוח את המסוף במחשב ה-Kali Linux.

5 יש להתקין את החבילה ***dsniff*** בעזרת הפקודה הבאה: ***sudo apt-get install dsniff*** ועם עליית חלונית ההנחיה, להזין ***y.***



6 בעזרת הכלי *arpspoof* במחשב ה-Linux, יש להרעיל את טבלת ה-ARP של Windows 10 מבלי להעביר הלאה מנות אל הנתב.

לצורך הדוגמה שלנו, ניתן להרעיל את טבלת ה-ARP של Windows 10 על ידי הוצאת הפקודה הבאה:***sudo arpspoof -i eth0 -t 10.0.3.4 10.0.3.1 -r***

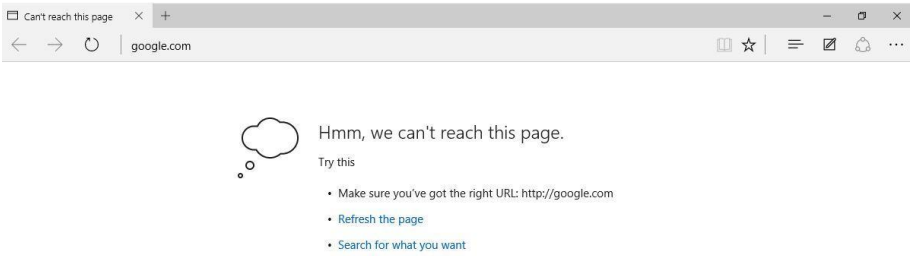
הערה: שער ברירת המחדל הוא רכיב רשת המאפשר להתקנים לצאת מהרשת המקומית (נתב).

מידע נוסף: התחביר של פקודה זו הוא: *sudo arpspoof -i eth0 -t <Windows VM IP> <Default Gateway IP> -r*

הפרמטרים של הפקודה:

- *arpspoof* - שם הכלי המשמש לביצוע ההתקפה
- *-i eth0* - משמש לציון ממשק האינטרנט; במקרה זה, eth0
- *-t <Windows VM IP>* – מציין את המטרה שתותקף על ידי כתובת ה-IP שלה; במקרה זה, המכונה הווירטואלית Windows 10 VM
- *<Default Gateway IP>* – מציין את כתובת ה-IP של המכונה שבעזרתן arpspoof מסווה אתכם; במקרה זה, כתובת ה-IP של שער ברירת המחדל של רשת NAT
- *-r* - משמש להרעיל את טבלאות ה-ARP של הכתובות שצוינו; במקרה זה, הן המכונה הווירטואלית Windows 10 VM והן שער ברירת המחדל של רשת ה-NAT

7 יש לנסות להשתמש באינטרנט במחשב ה-Windows. (יש לשלוח פינג אל ***8.8.8.8*** או להיכנס אל הדפדפן ולחפש את ***google.com***)




```
C:\Users\Dave>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Dave>
```

8 מה גרם לתקשורת הרשת להיכשל לאחר הרצת הפקודה ***arpspoof***?