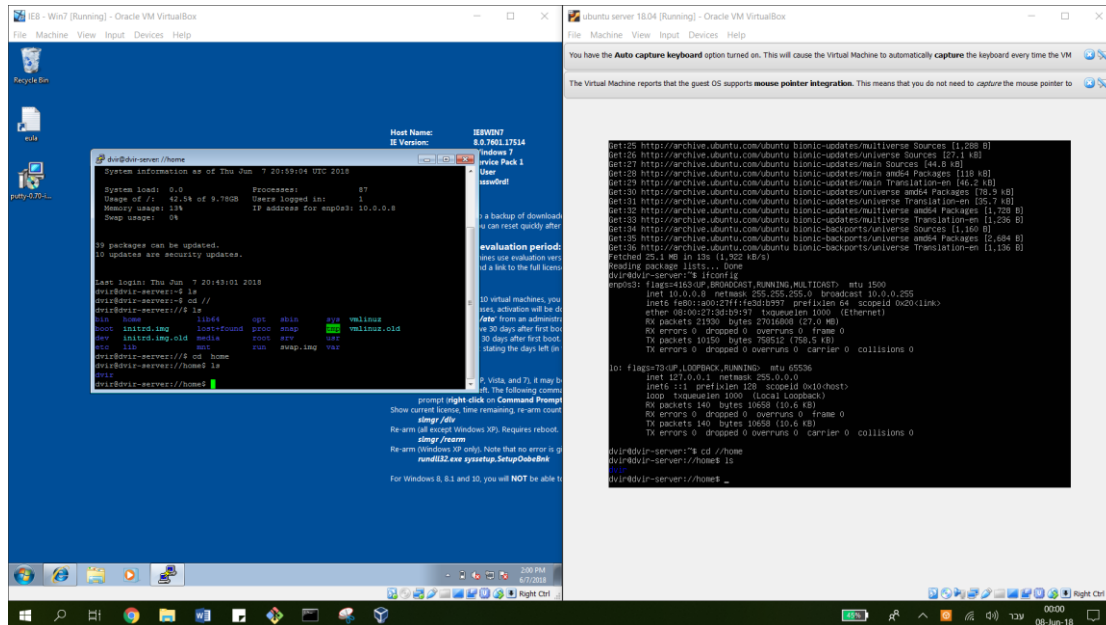


פתרון למטלה 4 – מעבדת סייבר הגנה

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 ב Windows 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 ה IP שלה לכולם.
- **NAT** – למכונה הוירטואלית תהיה כתובת IP משלה כמחשב נוסף בתוך הרשת ותוכל לגשת לאינטרנט. אולם מחוץ לרשת לא נוכל לגשת ישירות לכתובת ה IP של המחשב.

Phase 2

```

Administrator: Command Prompt
identifier          {bootmgr}
device             partition=C:
description        Windows Boot Manager
locale             en-US
inherit            {globalsettings}
default            {current}
resumeobject       {f74b4640-6094-11e5-a7be-8dfa37ab9638}
displayorder       {current}
toolsdisplayorder  {memdiag}
timeout            30

Windows Boot Loader
-----
identifier          {current}
device             partition=C:
path               \Windows\system32\winload.exe
description        Windows 7
locale             en-US
inherit            {bootloadersettings}
recoverysequence   {f74b4642-6094-11e5-a7be-8dfa37ab9638}
recoveryenabled    Yes
osdevice           partition=C:
systemroot         \Windows
resumeobject       {f74b4640-6094-11e5-a7be-8dfa37ab9638}
nx                 OptIn

C:\Windows\system32>

```

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

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

```

Administrator: Command Prompt
identifier          {bootmgr}
device             partition=C:

Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\IEUser>

```

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

```

Host Name: IESWIN7
IE Version: 8.0.7601.17514

PS C:\Users\IEUser\Desktop> ls

Directory: C:\Users\IEUser\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----        6/7/2018   2:23 PM           2452 Dvir.txt
-a-----        9/21/2015   2:19 AM             826 eula.lnk
-a-----        6/7/2018   1:56 PM       2942464 putty-0.70-installer.msi

PS C:\Users\IEUser\Desktop> start .\Dvir.txt
PS C:\Users\IEUser\Desktop> get-content .\Dvir.txt
Why you do this?
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec condimentum lobortis felis, quis dignissim orci facilisi
s sit amet. Praesent tellus leo, tincidunt non pretium vel, placerat ac est. Etiam hendrerit eros neque, aliquet sceler
isque est tempore nec. Sed vitae rhoncus odio. Nullam ligula odio, tempus vel maxinus ac, tempus quis lacus. Aliquam por
titor elit vitae mauris dictum varius. Aliquam sed justo non tortor sagittis mattis nec a sapien. Cras nec elit ac tor
tor faucibus imperdiet. Morbi et ultrices ni. Sed ultricies dolor nunc, a volutpat nulla tempus eu. Donec tristique luc
tus iaculis.

Mauris sit amet sollicitudin est, vitae mollis nunc. Aliquam sed nibh porta, feugiat ligula vel, venenatis mi. Lorem ip
sum dolor sit amet, consectetur adipiscing elit. Nunc faucibus non elit laoreet laoreet. Nunc non turpis metus. Pellent
isque sodales urna metus, quis tincidunt felis volutpat at. In ante augue, pretium tincidunt elit quis, feugiat pulvina
r dui. Curabitur dictum molestie dapibus. Vestibulum quis lorem erat. Fusce vestibulum, enim et efficitur venenatis, ve
lit enim malesuada nisl, ut viverra lectus sapien in est.

Donec vestibulum accumsan condimentum. Nam euismod pretium ipsum, ut fermentum est dignissim nec. Phasellus mattis cons
equat lobortis. Suspendisse in dictum risus, et feugiat tellus, Suspendisse vel sem eget ligula tristique malesuada a e
t ligula. Suspendisse justo metus, tincidunt a mollis vitae, tincidunt nec tortor. Ut a mauris quis dui molestie finibu
s. Nunc varius tellus ut ante dictum, molestie tristique dui fringilla. Suspendisse sit amet arcu non orci tristique ma
lesuada quis ut augue.

Proin nec tortor at lacus blandit fermentum a ut tortor. Integer in accumsan nisi. Praesent vel vulputate augue, eget t
empore ante. Proin vitae cursus diam, id vestibulum nibh. Nam sed eleifend enim, id euismod urna. Nullam efficitur diam
nec scelerisque elementum. Aliquam et bibendum lectus. Proin vehicula nisl sed augue vestibulum sagittis. Nulla facilis
i.

Pellentesque vitae purus eget tellus blandit sollicitudin. Suspendisse potenti. Fusce suscipit arcu eu tortor posuere e
uismod. Praesent rhoncus, metus sed ultricies sodales, mauris augue mollis elit, vitae tristique erat metus sit amet di
am. Vestibulum sapien dolor, interdum id tellus id, varius tempus tortor. Cras at turpis nec nisl tincidunt porta sed n
on mi. Suspendisse varius ultricies justo ac vehicula.
  
```

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:

```
root@dvir-server:/home/dvir# uname -msr
Linux 4.15.0-22-generic x86_64
```

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
```

```
root@dvir-server:/home/dvir# ls
linux-headers-4.17.0-041700_4.17.0-041700.201806041953_all.deb
linux-headers-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb
linux-image-unsigned-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb
linux-modules-4.17.0-041700-generic_4.17.0-041700.201806041953_amd64.deb
root@dvir-server:/home/dvir#
```

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.

```
dvir@dvir-server:~$ uname -msr
Linux 4.17.0-041700-generic x86_64
```

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 בטעות את הגרסה שבה אנחנו משתמשים כרגע.

נתקין את byobu:

```
sudo apt install byobu
```

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

```
dpkg -l | grep linux-image
```

```
root@dvir-server:/home/dvir# dpkg -l | grep linux-image
ii linux-image-4.15.0-20-generic          4.15.0-20.21
    amd64 Signed kernel image generic
ii linux-image-4.15.0-22-generic          4.15.0-22.24
    amd64 Signed kernel image generic
ii linux-image-generic                    4.15.0.22.23
    amd64 Generic Linux kernel image
ii linux-image-unsigned-4.17.0-041700-generic 4.17.0-041700.201806041953
    amd64 Linux kernel image for version 4.17.0 on 64 bit x86 SMP
```

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 kernel 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:

```
root@dvir-server:~/home# ls
ariel  dvir
```

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

```
root-1:x:1002:1006:root-1,root-1,,:/home/root-1:/bin/bash
```

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

```
shadow:17690:0:99999:7:::
dvir:$6$c90mB1LJRQ/kqgY9$TXDi20yxYFYzy9HsgUWW8pDLAfgJvJTCN3ea80/I204QR1pesLdcfe1TXlhV4jLzEW60yFr171F454y.EDK0:17680:0:99999:7:::
ariel:$6$BwedW1BuShdXXBqgHfdQz2UqDZxrU1F3yLDuzKHChEVzkm.EFZExQ4KeJ.vu.ywCQ21enJ.C9gasPOJnuKmRChel510Vwj/:17690:0:99999:7:::
root-1:$6$MXMaB5x1$KeNaDwn1SbnBSHjmKRBjL3vRrT0unEb74qkDQ9NIvs3/LyyYBJq0T53jDPw9wRSqt/EONr1zwTxVsqXd.q3rP0:17690:0:99999:7:::
root@dvir-server:~/etc#
```

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:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
ariel   ALL=(ALL:ALL) ALL
```

אחרי ששמרנו אנו יכולים להתחבר למשתמש ariel ולהשתמש ב-sudo:

```
ariel@dvir-server:~$ sudo apt-get update
[sudo] password for ariel:
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [83.2 kB]
Hit:2 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [83.2 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [119 kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [79.8 kB]
Fetched 440 kB in 2s (213 kB/s)
Reading package lists... 19%
```

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):

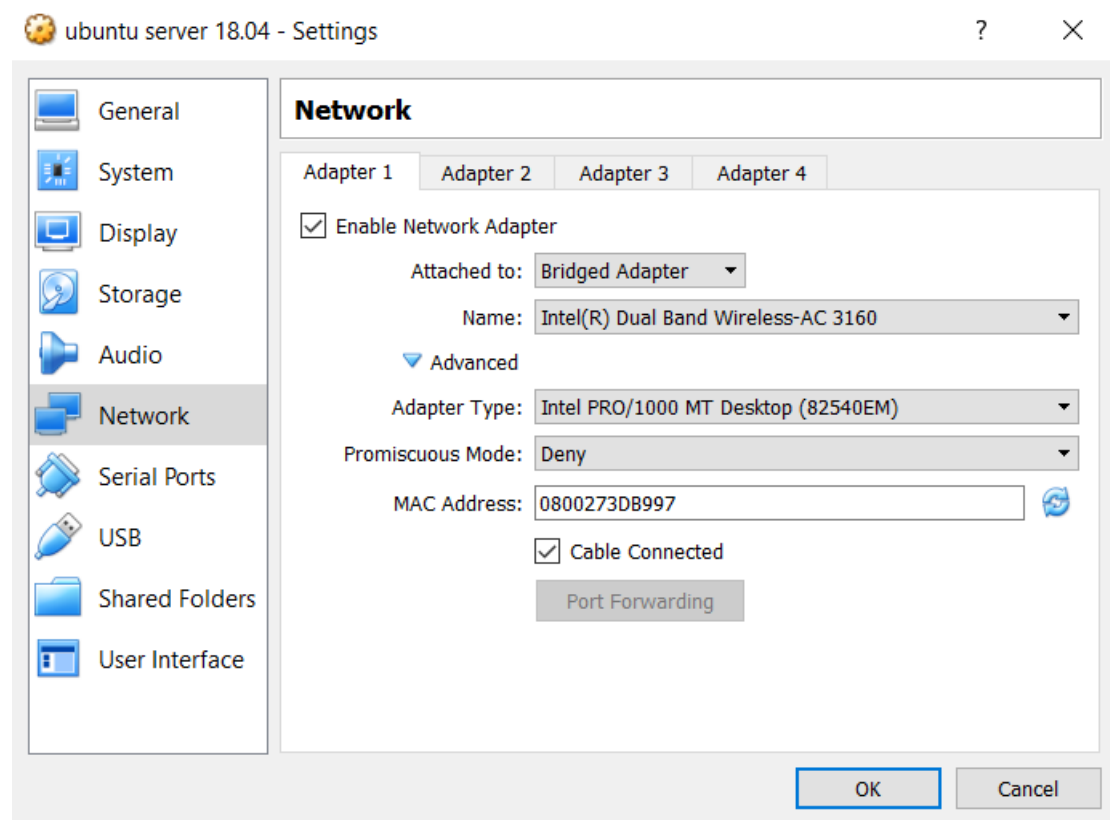
```
# User privilege specification
root    ALL=(ALL:ALL) ALL
ariel   ALL=(ALL:ALL) ALL
root-1  ALL=(ALL) NOPASSWD: ALL
```

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

```
root-1@dvir-server:/$ sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [83.2 kB]
Hit:2 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Fetched 83.2 kB in 1s (102 kB/s)
```

Phase 4

ניתן לשנות את כתובת ה-MAC כפי שניתן לראות בתמונה:



לאחר השינוי קיבלתי כתובת MAC חדשה: B3A88F080027

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

Host Network Manager

Network

Create Remove Properties

Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter #3	192.168.56.1/24		<input type="checkbox"/> Enable

Adapter DHCP Server

☐ Configure Adapter Automatically

☒ Configure Adapter Manually

IPv4 Address: 192.168.56.1

IPv4 Network Mask: 255.255.255.0

IPv6 Address: fe80::7087:9cfd:5178:a864

IPv6 Prefix Length: 64

Reset Apply Close

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

Adapter DHCP Server

☒ Enable Server

Server Address: 192.168.56.2

Server Mask: 255.255.255.0

Lower Address Bound: 192.168.56.1

Upper Address Bound: 192.168.56.254

Reset Apply Close

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