Linux Essentials 010-160 + Bonuses

קורס זה הינו שדרוג של ההסמכה המוכרת **Linux Essentials 010-160** בתוספת נושאים של **LPI 101(LPIC-1)** עם דגש על **אבטחת מידע והכנה ל-OSCP**.

קורס זה הינו בפיקוח של Linux Professional Institute (LPI) ומזכה את התלמיד בהנחה לבחינה הבינלאומית LPIC הנחשבת!

קורס זה מתאים לבני נוער ולחסרי רקע בעולם ה-Linux, Linux היא מערכת הפעלה הכרחית הן בעולם ניהול הרשת והן בעולם אבטחת המידע והסייבר.

בקורס הזה אנחנו נעבוד עם מערכת ההפעלה Kali Linux ו-Ubuntu.

שיעור – 6 – תקשורת נתונים ושירותי רשת

תקשורת נתונים ושירותי רשת הינם חיוניים מאוד בעת העבודה עם מערכת ההפעלה, ללא הגדרה נכונה של תקשורת הנתונים לא תוכלו לתקשר עם המכונות ברשת שלכם ולא תיהיה לכם גישה לאינטרנט.

ב-LPI 101 אלמד אתכם חישוב כתובות IP ואת המונח VLSM, ברמת החומר של LPI Essentials אנחנו נתייחס לכתובות ולמסכות הרשת בצורה בסיסית ביותר.

על מנת להציג את כתובת ה-ip של המכונה עלינו להשתמש באחת מהפקודות הבאות:

```
ifconfig eth0
iwconfig eth0
iwlist wlan0 scan
```

כדי לכבות את כרטיס הרשת ניתן להשתמש בפקודה הבא:

```
ifup eth0
ifdown eth0
```

או בפקודה המלאה:

```
ifconfig eth0 up
ifconfig eth0 down
```

בשנים האחרונות החליטו להחליף את הפקודה ifconfig הישנה והטובה בפקודה ip ובעתיד כנראה לא נראה יותר את הפקודה ifconfig שכבר היום לא מגיעה מותקנת במערכות לינוקס חדשות.

הפקודה החדשה נראית כך:

```
ip addr show eth0
ip link set eth0 down
ip link set eth0 up
```

כדי להציג את כתובת הdefault gateway נשתמש בפקודה route שגם פקודה זו הוחלפה בפקודה ip שתפקידה לנהל את כל הקשור תקשורת במכונה.

```
Route -n
```

בשיטה החדשה:

```
ip route show
```

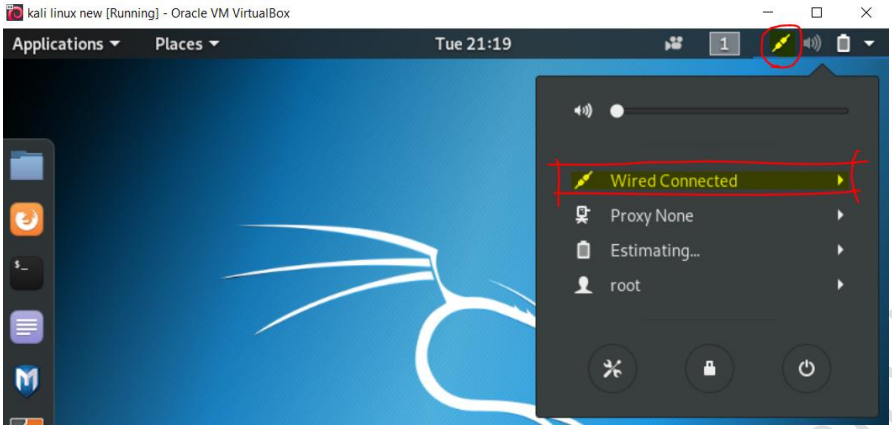
כדי להגדיר default gateway בשיטה הישנה:

```
route add default gw 192.168.1.1 eth0
```

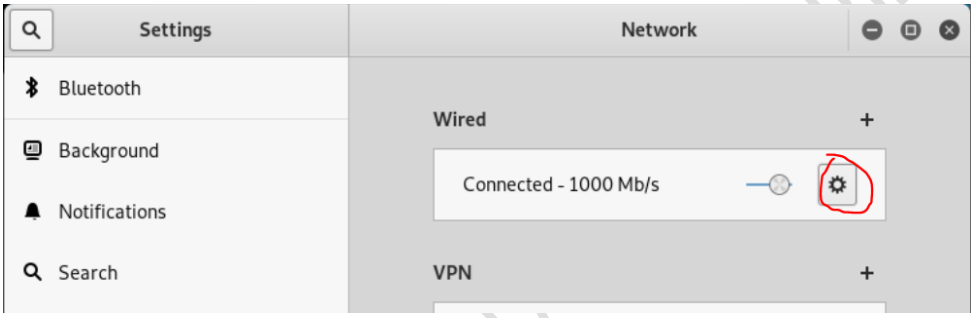
בשיטה החדשה:

```
ip route add default via 192.168.50.100
```

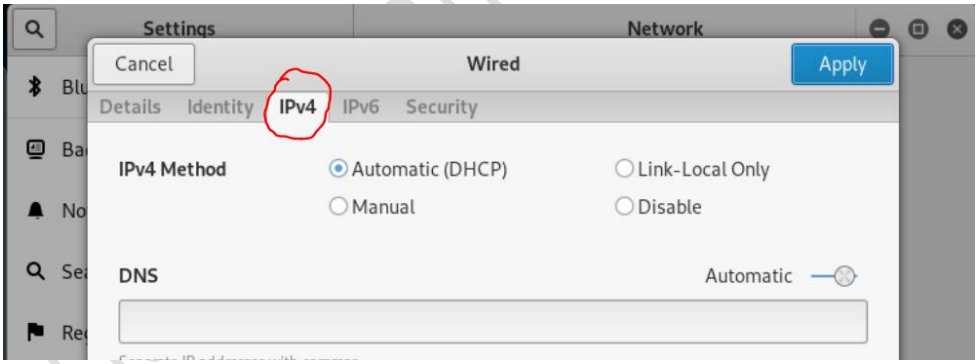
בעולם הלינוקס קיים שירות הנקרא **NetworkManager** הוא אחראי על הגדרות כרטיס הרשת כאשר יש לכם מנוע גרפי (Desktop) והגדרה צריכה להתבצע דרכו בלבד. על מנת להשתמש בשירות נלחץ פה:



ולאחר מכן נגדיר את כרטיס הרשת מכאן:



ואז יש ללחוץ על IPv4:



בחלון הזה ישנם מספר הגדרות ושירותים שעלינו להכיר, נתחיל משני שירותי הרשת הבאים:

DHCP (Dynamic Host Configuration Protocol) – תפקיד השירות להגדיר את כרטיס הרשת בצורה אוטומטית והוא מוגדר כברירת המחדל ברוב כרטיסי הרשת הן בלינוקס והן ב-windows.

כאשר שירות זה אינו מצליח לתת לנו כתובת נקבל את הכתובת 169.254.X.X מה שנקרא APIPA שזו כתובת אוטומטית שתאפשר לכל המכונות שקיבלו APIPA לתקשר ברשת הפנימית בלבד מבלי לצאת לאינטרנט.

כדי לבקש משירות ה-DHCP כתובת עלינו להשתמש בפקודה:

```
dhclient eth0
```

DNS (Domain Name System) – שירות שתפקידו לתרגם שם לכתובת IP, השירות יתרגם את שם האתר לדוגמה www.google.co.il לכתובת ה-IP שלו מכיוון שהתקשורת בפועלת מתבצעת באמצעות כתובות IP.

על מנת לפנות לשירות זה אנו משתמשים בפקודות הבאות:

```
host www.google.com
dig www.google.com
nslookup www.google.com
```

שימו לב שאם בחרתם בהגדרה ידנית (Manual) עליכם להגדיר את כל הנתונים בצורה נכונה אחרת לא תוכלו לגלוש באינטרנט.

הגדרת כתובת IP בצורה זמנית

במהלך העבודה עם מערכת ההפעלה לפעמים עלינו לשנות את כתובת ה-IP לצורך בדיקה כלשהי או שאנחנו מנסים להתחזות לעמדה אחרת ברשת. במקרים אלו נרצה להחליף את כתובת ה-IP בצורה זמנית.

בשיטה הישנה:

```
ifconfig eth0 192.168.0.1 netmask 255.255.255.0
```

בשיטה החדשה:

```
ip addr del 192.168.0.1/24 dev eth0
ip addr add 192.168.0.1/24 dev eth0
ip addr add 192.168.0.1/255.255.255.0 dev eth0
```

במידה ויש צורך לשנות גם את הכתובות הפיזית נצטרך לבצע את הפעולות הבאות.

תחילה יש לכבות את כרטיס הרשת עם פקודת down, לשנות את הכתובת ואז להפעיל את כרטיס הרשת עם פעולת up.

```
ifconfig eth0 hw ether 00:00:00:00:11:22
```

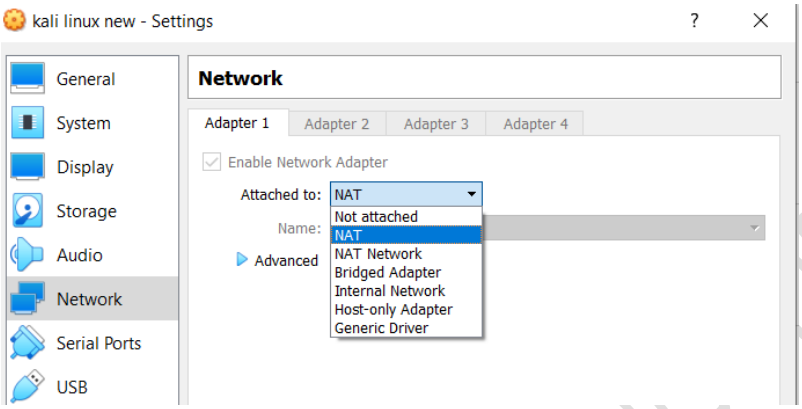
או בשיטה החדשה:

```
ip link set dev eth0 address 00:00:00:00:11:22
```

לכל כרטיס רשת בעולם ישנה כתובת ייחודית המשמשת כתעודת זהות של הכרטיס, מבנה הכתובת מתחל ל-2 חלקים **AA:AA:AA:BB:BB:BB** ומכיל 6 זוגות של תווים בתווך ה-Hexadecimal (0-F).

1. 3 זוגות בצד שמאל החלק האפור בדוגמה, מהווים את החלק שמאפיין את החברה שיצרה את כרטיס הרשת.
2. 3 הזוגות בצד ימין החלק הצהוב בדוגמה, מהווה המספר הסידורי של הכרטיס הספציפי שנוצר על ידי אותה החברה.

הגדרת כרטיס רשת ב-Oracle VirtualBox:



NAT – המחשב יהיה מבודד מהרשת שלכם אבל יכול לגלוש באינטרנט.
NAT Network – רשת מחשבים מבודד מהרשת שלכם שמאפשרת למחשבים ברשת לתקשר זה עם זה.
Bridged Adapter – המחשב יהיה חלק מהרשת שלכם ותוכלו לתקשר מולו.
Internal Network – רשת סגורה לחלוטין שרק המחשבים באותה רשת יכולים לתקשר זה עם זה.
Host-only Adapter – המחשב שלכם יכול לתקשר עם המכונה הווירטואלית והמכונה לא יכולה לצאת לאינטרנט.

הצגת כל השירותים הפעילים במכונה

על מנת לצפות בכל השירותים במכונה אנו משתמשים בפקודה netstat עם הדגלים הבאים

```
netstat -tunalp
```

הדגלים הם:

- -t tcp
- -u udp
- -n number
- -a all

הפקודה גם כן הוחלפה בפקודה:

```
ss
ss -l
```

ובפועל משתמשים בפקודה מהחומר של lpi 102 הנקראת lsof:

```
lsof -i
```

מדובר בפקודה מתקדמת יחסית אשר יכולה לתת לנו מידע רב על תהליכים והקבצים שהם משתמשים בהם, יותר על הפקודה בהסמכה lpi 101.

כאשר נרצה לבדוק האם יש תקשורת למכונה נשתמש בפקודה ping בצורה הבאה:

```
ping 10.0.0.1
```

קבצים הקשורים ל-networking

כדי לשנות את שם העמדה עלינו לשנות בקובץ

```
/etc/hostname
```

כדי להגדיר dns בדומה לקובץ Host של Microsoft

```
/etc/hosts
```

הגדרת שרת הdns של הארגון לצרכי גלישה

```
/etc/resolv.conf
```

הגדרה חיפוש הdns איפה הציוד יחפש קודם חומר מתקדם של lpi 101

```
/etc/nsswitch.conf
```

ניתן לראות שקודם המכונה תחפש בקובץ hosts ולאחר מכן יפנה לשרת הdns כמובן שניתן לשנות זאת.