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 – 1 – התקנת מערכת ההפעלה ותפעול בסיסי

Linux הינה דוגמה מעולה ל-Open Source ולהבדיל מ-Windows הינה מערכת הפעלה חינמית. Linux היא מערכת Multi Users המאפשרת למשתמשים רבים לעבוד על אותה מערכת הפעלה בצורה נוחה ויעילה, מערכת הפעלה זו הינה נוחה מאוד לעבודה הן בממשק הגרפי שלה והן באמצעות פקודות ממשק CLI.

ישנן גרסאות רבות של למערכת ההפעלה Linux הניתנות להתאמה לכל סוג של צורך או חומרה וזו הסיבה שמכונות רבות בחרו במערכת ההפעלה זו (Embedded Systems).

ליונס טורבאלדס ריצ'רד מת'יו סטולמן

בשנת 1991, במהלך לימודיו, טורבאלדס ניסה למצוא אפשרות לעבוד ביוניקס גם מהבית, במחשב האישי שלו. האפשרות היחידה בתקופה ההיא הייתה מיניקס שלא נמכרה ברישיון חופש, טורבאלדס החליט לבנות גרסה משלו.

השכתוב של מיניקס הפך בהדרגה לפרויקט בפני עצמו שכבר לא היה קשור אל מיניקס באופן מיוחד, טורבאלדס פיתח את הליבה וכשהרגיש כי יש לו מספיק קוד, הוא פנה לרשימת הדיוור של מיניקס והכריז על כך. זמן קצר לאחר מכן הייתה לינוקס זמינה לכל דורש מספריה פרטית בשרת ה-FTP שהוקצה עבורה.

חשוב לציין שטורבאלדס ממשיך להיות המתחזק הראשי של ליבת לינוקס עד היום.

במקביל לליונס, ריצ'רד מת'יו סטולמן מתכנת אמריקאי יהודי. בשנת 1983 יזם את פרויקט GNU ליצירת מערכת הפעלה חופשית, דמוית יוניקס ומשמש מאז כארכיטקט המוביל שלה. העקרונות הרעיוניים אותם ביטא סטולמן כשייסד את GNU מהווים את התשתית לתנועה חברתית בשם תנועת Open Source.

Open Source

מוצר או תוכנה שהינה קוד פתוח משמע מאפשרים לכל הרוצה בכך לצפות בקוד המקור של התוכנה, להוריד את הקוד מקור ולבחון אותו, בעולם אבטחת המידע אנו משתמשים בקוד המקור של החברות על מנת לאתר ליקויי אבטחה בקוד ולדווח להם על כך.

בעולם הקוד הפותח לעיתים אף ניתן לשנות קוד מהקור של התוכנה ולהתאים אותה לצרכים האישיים של המתכנת, כיום פלטפורמת הקוד הפתוח הגדולה ביותר הינה GitHub וב-GitHub ניתן למצוא קוד מקור לפרויקטים שונים בכל העולמות התכנות בכלל ובסייבר כפרט.

לדוגמה לתוכנת קוד פתוח:

- Httpd & Apache - https://github.com/apache/httpd
- WordPress – https://github.com/WordPress/WordPress
- MySQL & MariaDB - https://github.com/mysql/mysql-server

מטרת מודול הקוד הפתוח הוא לשחרר קוד מקור של תוכנות בחינם לכל דורש. אך יחד עם זאת:

- התמיכה בקוד.
- בקשת פיצ'ר או שינוי בקוד.
- קורס או הסמכה בתוכנה.

חשוב לציין שלפי מודול הקוד הפתוח מצד אחד הקוד קריא וגלוי לכולם מצד שני לא כל תוכנות הקוד הפתוח מכילות את אותו הרישיון ומאשרות לכם לבצע שינויים בקוד ולהפיץ את התוכנה מחדש.

סוגי רישיונות בתחום הקוד הפתוח:

- **Copyright** – היא ההגנה שניתנת ליוצר או לבעלים של יצירה מפני שימוש בלתי מורשה ביצירה שהיא קניין רוחני שלו. למידע נוסף
- **Copyleft** – תוכן חופשי הוא שם כללי לתוכן (כתוב, תוכנה, תמונה, צליל וכדומה) שאין גוף יחיד עם שליטה מוחלטת על הפצתו ועל השימוש בו. השם מקובל כשם לתנועה חברתית אשר מבקשת לעודד שימוש בתוכן חופשי.

בעת שימוש בתוכן חופשי יש למשתמשים את החופש ל:

- להשתמש בתוכן ולהפיק ממנו תועלת
- ללמוד את התוכן וליישם את מה שנלמד
- ליצור ולהפיץ עותקים של התוכן
- לשנות ולשפר את התוכן ולהפיץ עבודות נגזרות לו

למידע נוסף

- **GNU General Public License(GPLv3)** – הוא רישיון **copyleft** שיצירות נגזרות תחת אותם תנאי רישיון. מעניק לתוכנת מחשב זכויות של תוכנה חופשית ומשתמש ב-**copyleft** כדי להבטיח שהחירות תישמר, גם אם העבודה שונתה או שודרגה. **(קוד המקור של התוכנה חייב להיות נגיש לכולם ולא ניתן לרשום עליו פטנט)**

- **Apache License** – רישיון שחובר על ידי החברה apache, כל התוכנות שהופצו על ידי מוסד זה או על ידי אחד מהפרויקטים שלה, רשומים תחת רישיון זה. יש לציין שרישיון זה אינו **copyleft** והוא מרשה שימוש והפצה של קוד המקור בתוכנות קוד פתוח וסגור. **(כל אחד יכול לקחת את הקוד ולבנות ממנו תוכנה בקוד סגור ולמכור אותה, אבל הוא לא יכול לרשום פטנט על הקוד או על הרעיון).**

- **MIT License** – רישיון של המכון הטכנולוגי MIT, הוא רישיון חופשי מתירני ומאפשר שימוש חוזר גם בתוכנה קניינית, בתנאי שעותק של הרישיון יצורף לעותקי התוכנה. כמו כן רישיון זה מאפשר המרה לרישיון GPL והפצצת התוכנה. **(כל אחד יכול לקחת את הקוד ולבנות ממנו תוכנה בקוד סגור ולמכור אותה, בגדול רישיון זה אומר תעשה מה שאתה רוצה עם הקוד).**

- **Unlicensed** – תוכנה חסרת רישיון הינה תוכנה מסוכנת מכיוון שלא ניתן לדעת מי כתב את התוכנה והינה יכולה לגרום לנזק למחשב.

כדי לעשות לכם סדר הנה אתר מעולה שמסביר בצורה מקיפה על כל הרישיונות בצורה קלילה לחץ כאן

סוגים שונים של מערכות Linux

בקורס זה אנו נעבוד עם מערכת ההפעלה Ubuntu ו-Kali Linux שהיא בפועל (Debian) שהותקנו עליו מספר כלי האקינג צורך נוחות.

בעולם הלינוקס קיימים מספר רב של אפשרויות למערכות הפעלה לדוגמה:

- **Server** – מערכת הפעלה ללא ממשק גרפי וכל העבודה עם מערכת ההפעלה מתבצעת באמצעות פקודות בלבד.
- **Desktop** – מערכת הפעלה גרפית דמוי מערכת ההפעלה Windows אשר ניתן לתפעל ללא שימוש בפקודות כלל.
- **Embedded System** – מערכת הפעלה ליצירת חומרה מותאמת לדוגמה Raspberry Pi/Arduino נהוג להשתמש במערכת הפעלה זו בעת פיתוח מוצר חכם לדוגמה מצלמת IP.

Linux Distributions

בעולם הלינוקס קיימים אינספור הפצות שונות ומשונות שעונות על צרכים שונים, להלן רשימת הפצות בעולם הלינוקס.

ההפצות המובילות והמוכרות הן:

- Debian, Ubuntu(LTS), Kali Linux
- Gentoo
- Red Hat, CentOS, Fedora
- Raspberry Pi, Raspbian
- Android

מונחת נוסף שיש להכיר לפני שנתחיל ללמוד את מערכת ההפעלה לינוק הינו **Distribution Life Cycle**, לכל הפצה שתורידו יכולים להיות מספר גרסאות:

- **Release** – הגרסה היציבה של התוכנה עבור המשתמש הפשוט.
- **Pre-Release**
  - **Alpha** – גרסה חדשה מלאה בבאגים עבור מפתחים שמעוניינים להקדים את ולהוציא עדכון לתוכנה שלהם עוד לפני שתצא גרסת ה-release.
  - **Beta** – גרסה יותר יציבה מ-Alpha כאשר רוב הבאגים תוקנו בגרסה, בשלב הזה על המפתח לבדוק את הקוד שהוא כתב ב-Alpha לפני שהוא יצא ביחד עם ה-**release**.
- **Rolling Release Schedule** – עדכונים שוטפים שמגיעים למערכת ההפעלה, בדרך כלל מדובר בעדכוני security ו-bug fix.
- **Support Versions**
  - Short-term – גרסת ביניים
  - Long-term – LTS גרסה יציבה מאוד לאורך תקופה ארוכה
  - End of Life – אין יותר תמיכה

השוואה בין מערכות הפעלה שונות:

- **Windows**
  - 90% of home users
  - Widely-available and widely-supported
  - Most prone to malware
  - Requires a license
  - GUI-based
- **Mac OSX**
  - 7% of home users
  - Free but only works on Apple systems
  - GUI-based
- **Linux**
  - Less than 2% of home users
  - More than 75% of enterprise server environments
  - Known as the OS for computer experts and hackers
  - Source code is available for modification
  - Open source
  - Can run from the command line only

התקנת מערכת ההפעלה Linux:

אתם יכולים לבחור באחת מתוך שלושת אפשרויות ההתקנה:

- **Oracle VirtualBox and Virtualization** – להתקין את מערכת ההפעלה בסביבה וירטואלית ולא כמערכת ההפעלה המרכזית שלכם, זו השיטה הקלה והנוחה ביותר. לכן, בקורס זה בחרנו להתקין את מערכת ההפעלה בסביבה וירטואלית.

- **LiveCD** – שיטה זו מאפשרת להריץ את הלינוקס מבלי להתקין אותו באופן ישיר מתוך דיסק און קי.
- **Full Installation** – התקנה מלאה של מערכת ההפעלה על הדיסק הקשיח של המחשב.

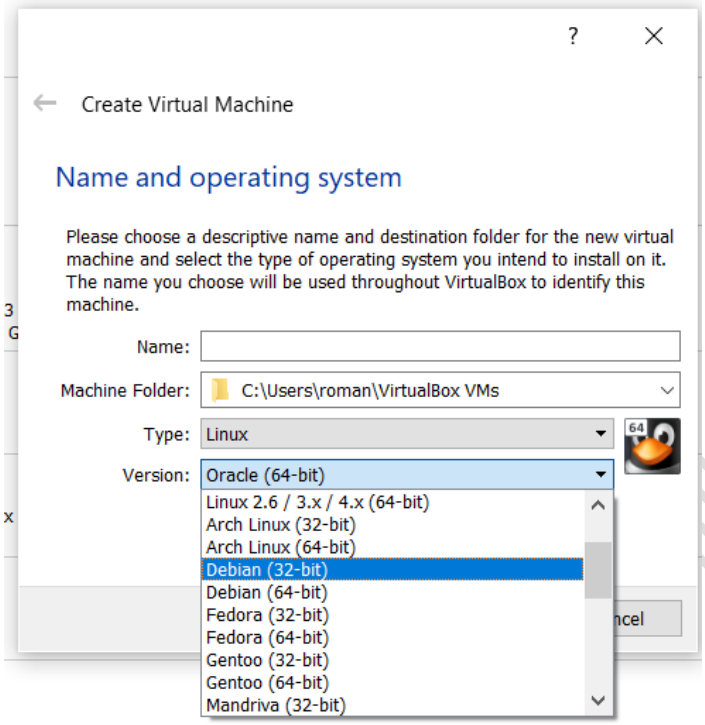
בקורס אנו נעבוד עם **Ubuntu** ו-**Kali Linux**, הורידו את 2 המכונות מהאתרים הבאים:

- Ubuntu
- Kali

אנו נתקין את המכונות באמצעות תוכנה מכונה וירטואלית – Oracle Virtual Box שניתן להוריד מכאן.

שימו לב שיש להפעיל וירטואליזציה ב-BIOS של המחשב שלכם בהתאם לדגם של המחשב, לכן בקורס זה אנו נעשה מעקף ונתקין מכונות 32bit בלבד.

במידה והתוכנה מאפשרת לכם להתקין מכונות 64bit אז הכל תקין אצלכם במידה ואתם רואים רק אפשרויות של 32bit תדעו שיש לפתוח את הווירטואליזציה ב-BIOS.



לאחר התקנה יש לשים לב שאתם אמורים לעבוד במשתמש root על ידי אחת מ-2 האפשרויות הבאות:

1. לבצע את הפקודה sudo su
2. לבצע את הפקודה sudo לפני כל פקודה שדורשת הרשאות לדוגמה:

```
sudo apt install vim
```

אם יש לכם בעיית צבעים, כפי שמוצג בסרטון יש לבצע את הפקודה:

```
alias ls="ls --color=auto"
```

תוכנות נפוצות ועבודה עם מערכת ההפעלה.

בעולם ה-Linux יש לכם את היכולת לבחור באיזה תצורת מסך תבחרו קיימים סוגים שונים:

- **Unity**
- **KDE**
- **Gnome**
- **Cinnamon**
- **Xface**
- **LXQt**
- לרשימה המלאה

תוכנות נפוצות שיש להכיר למשתמש הפשוט:

- **Librawriter** – תוכנה זו מחליפה את ה-Office Word.
- **Libracalc** – תוכנה זו מחליפה את ה-Office Excel.
- **Libraoffice express** – תוכנה זו מחליפה את ה-Office PowePoint.
- **Vlc** – נגן סרטים.
- **Gimp** – תוכנה המחליפה את ה-Photoshop.
- **Kdenlive** – תוכנה המחליפה את ה-Windows Movie Maker.
- **Audacitiy** – תוכנה להקלטת Sound.
- **Firefox** – הדפדפן המומלץ בעולם הלינוקס.

תוכנות ניהול רשת:

- **Wireshark** – תוכנת ניתור רשת
- **Gparted** – תוכנה לעבודה עם הדיסק הקשיח של המכונה.
- **Timeshift** – תוכנת גיבוי מעולה כמו system restore ב-windows.
- **Atom** – זה ה++notepad של ה-Linux
- **gedit** – גרסה נוספת של כתבן נוח ופשוט יותר בסגנון של notepad.
- **Putty** – תוכנה לניהול השרתים שלנו.

שפות תכנות כלליות ושימוש שלהם:

- **PHP** – שפת צד שרת בעולם האינטרנט.
- **JavaScript** – שפת פיתוח בצד לקוח בעולם האינטרנט
- **Python** – שפת הסקריפטינג המומלצת בתחומי אבטחת המידע וההייטק.
- **Bash** – שפת התכנות בעולם ה-Linux.
- **Java** – שפה שימושית לפיתוח תוכנה עם מנוע גרפי שתעבוד על כל סוגי מערכות ההפעלה.
- **C** – אחת השפות הראשונות לפיתוח תוכנה בעלת ביצועיים גבוהים.

Package Management and Installation

ב-Linux לא מורידים תוכנות מהאתרים של החברות כמו שעושים ב-Windows, בשביל זה יש package manager (חנות אפליקציות כמו במובייל).

חנות האפליקציות של מערכת ההפעלה Ubuntu נקראת - Ubuntu Software Store.

- חשוב לציין שלהתקנות יש תלות בעוד תוכנות בLinux לכן ה-package manager מתקין הכל בשבילנו שלא נצטרך להוריד עכשיו 10 תוכנות כדי לגרום לתוכנה לעבוד.

- כמו שאפליקציה באנדרואיד היא עם סיומת **apk.** אז תוכנה בלינוקס היא עם סיומת **deb.** או **rpm.**
  - **deb.** – מסמן הפצה מסוג debian.
  - **rpm.** – מסמן הפצה סמוג red hat חומר LPI101.
  - **tgz.** – סתם universal linux format, יותר דומה להורדת תוכנה בפורמט דחוס כמו zip.

- <u>תהליך ההתקנה מתבצע בצורה הבאה:</u>
  - מריצים פקודת התקנה
  - הפקודה מחפש את כל ה-dependencies ומתקינה אותם
  - מתקינים את התוכנה המתבקשת

- אחד היתרונות המשמעותיים ביותר בלינוקס בעת התקנת תוכנות הוא עדכון התוכנות הכללי שמתבצע במערכת, אין צורך לעדכן תוכנה בודדת. **ניתן לעדכן את כולם בפקודה אחת.**

apt-get command

פקודות אפשריות לפקודה **apt-get** או **apt**:

- **dist-upgrade** משדרג חבילות שבשביל לשדרג אותם יש צורך בהתקנת חבילות חדשות, בפקודה זו משדרגים את מערכת ההפעלה.
- **upgrade** משדרג את כל החבילות המותקנות
- **install** מתקין חבילה, ניתן גם להתקין גרסה מסוימת עבור חבילה כלשהי אמצעות השווה vsftpd=2.3
- **remove** מוחק חבילה בלבד לא נוגע בקבצי ההגדרות ובתלות
- **purge** מוחק גם את החבילה וגם את קבצי ההגדרה
- **autoremove** מוחק גם את התלות, אם מריצים בלי שום חבילה מוחק את כל התלויות והחבילות הפגומות.
- **update** מעדכן את ה-repositories
- **download** מוריד ולא מתקין חבילה
- **check** ללא שם תוכנה בודק האם יש חבילות שחסרה לה תלות והם לא יעבדו
- **build-dep** מתקין את כל התלויות שוב עבור חבילה כלשהי

דוגמה:

```
apt update
apt install ssh
apt autoremove --purge ssh
```

פרמטרים נוספים:

--download-only source

```
apt --download-only source ssh
```

תרגיל

הורידו את התוכנות הבאות למכונת ה-Ubuntu שלכם:

1. git
2. nmap
3. ssh

Repositories

את התוכנות אנו מתקינים מתוך ה-repositories, אשר נמצא בקובץ הבא:

```
/etc/apt/sources.list
```

deb – חבילות מוגדרות לשימוש

deb-src – קוד המקור של החבילות למפתחים במידת הצורך.

בעולם ה-**red-hat** הפקודה apt מתחלפת בפקודה **yum**.