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**.

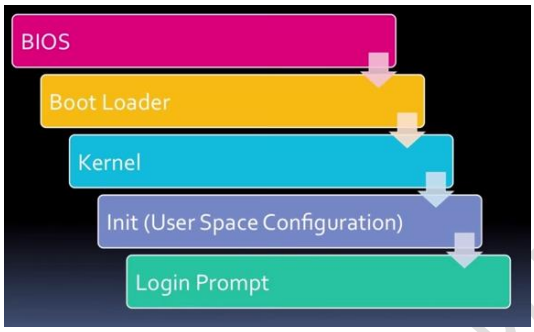
קורס זה הינו בפיקוח של Linux Professional Institute (LPI) ומזכה את התלמיד בהנחה לבחינה הבינלאומית LPIC הנחשבת!

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 – 5 – תהליכים לוגים ואתחול מערכת ההפעלה

תהליך ה-boot של המערכת

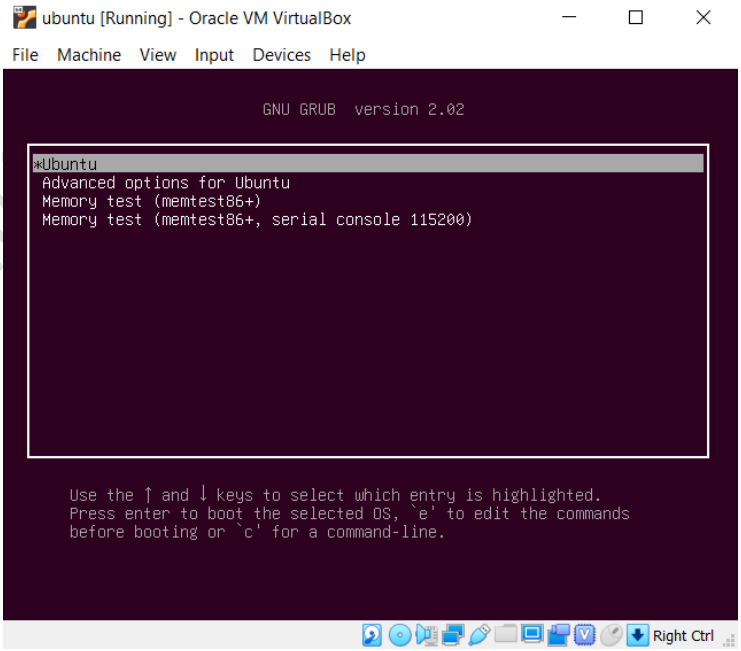


Boot the system

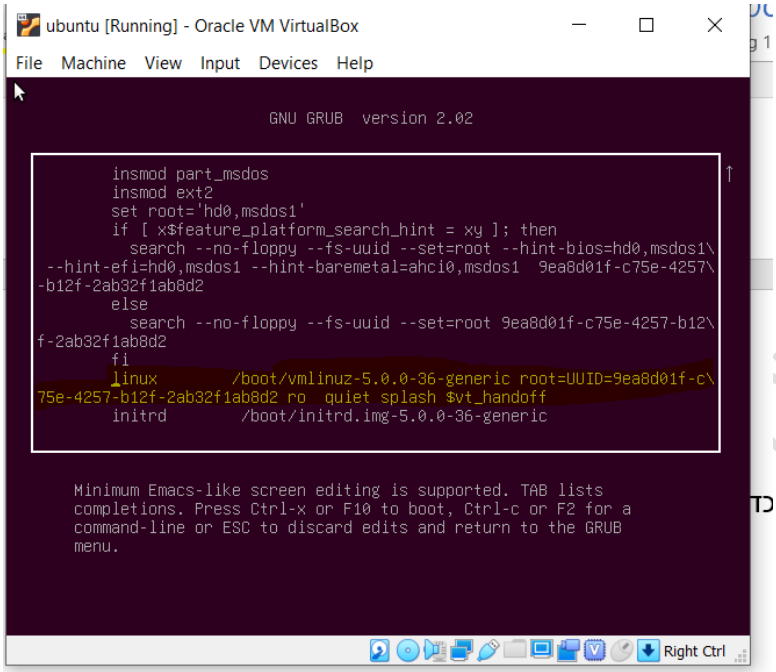
במערכת חלונות ישנו bootloader הנקרא NT Bootloader ותפקידו להכניס את המחשב למצבים שונים כגון – מצב בטוח, מצב פקודה בלבד, מצב בטוח ללא אינטרנט וכו'...

בלינוקס ישנם שניים כאלה **lilo** או **grub**, grub הוא נפוץ יותר ונכנסים אליו על ידי לחיצה על shift בעת הפעלת המכונה או על ידי לחיצה על esc.

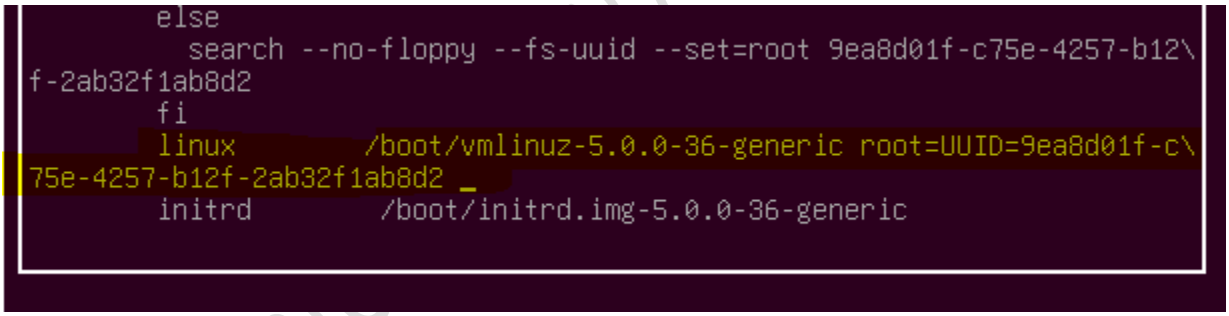
מה שיראה כך:



על מנת לערוך את ה-grub יש ללחוץ על e וכדי להפעיל את המכונה ללא סיסמא נבצע את העדכון הבא:



מוחקים את כל ההגדרות עד ל-ro כולל! מה שיראה כך:



וכתובים את הפקודה הבאה:

rw init=/bin/bash

כדי להפעיל את המערכת לוחצים על ctrl+x.

קח ניתן להתחבר לכל מכונת לינוקס שלא הגדירו בה סיסמא ב-grub, הגדרת הסיסמא הינו חומר של LPI 102.

לידע כללי ה-grub נמצא בתיקייה boot/grub/ וההגדרה שלו מתבצעת על ידי אחד הקבצים הבאים:

- grub.cfg
- menu.lst

תהליכים בעולם הלינוקס

כדי לראות את כל התהליכים במערכת

```
ps aux
```

a- כולם

u- משתמשים User

x- מראה גם פקודות שפועלות מחוץ ל-terminal הנוכחי

```
ps -aux
```

מציג את כל התהליכים של המשתמש x ולכן בעצם מניח שטעיתם בפקודה

```
ps -auroot
```

כיום משתמשים נהוג להשתמש בפקודה הבאה במקום הפקודה הקודמת, כמו כן שימו לב שלכל תהליך יש מספר מה שנקרא pid ולו יש גם הורה מה שנקרא ppid:

```
ps -ef
ps -p 4146
```

מה שיראה כך:

```
root@roman-VirtualBox:/home/roman# ps -ef
UID          PID  PPID  C STIME TTY          TIME CMD
root           1     0  0 08:45 ?        00:00:03 /sbin/init splash
root           2     0  0 08:45 ?        00:00:00 [kthreadd]
root           3     2  0 08:45 ?        00:00:00 [rcu_gp]
root           4     2  0 08:45 ?        00:00:00 [rcu_par_gp]
root           6     2  0 08:45 ?        00:00:00 [kworker/0:0H-kb]
root           7     2  0 08:45 ?        00:00:00 [kworker/u2:0-ev]
root           8     2  0 08:45 ?        00:00:00 [mm_percpu_wq]
root           9     2  0 08:45 ?        00:00:00 [ksoftirqd/0]
root          10     2  0 08:45 ?        00:00:00 [rcu_sched]
root          11     2  0 08:45 ?        00:00:00 [migration/0]
```

כדי לאתר את מספר התהליך אנו יכולים להשתמש גם בפקודות הבאות:

```
pidof sleep
```

או הפקודה

```
pgrep sleep
```

מבצעות את אותו הדבר.

במידה ואחד התהליכים אינו מגיב, אנו יכולים להפסיק את פעילותו באמצעות הפקודה הנפוצה kill, הפקודה שולחת סיגנל לתהליך ומציינת מה היא רוצה שהוא יעשה:

```
kill [process id]
kill -1 -9 -15
```

reset – 1

force – 9

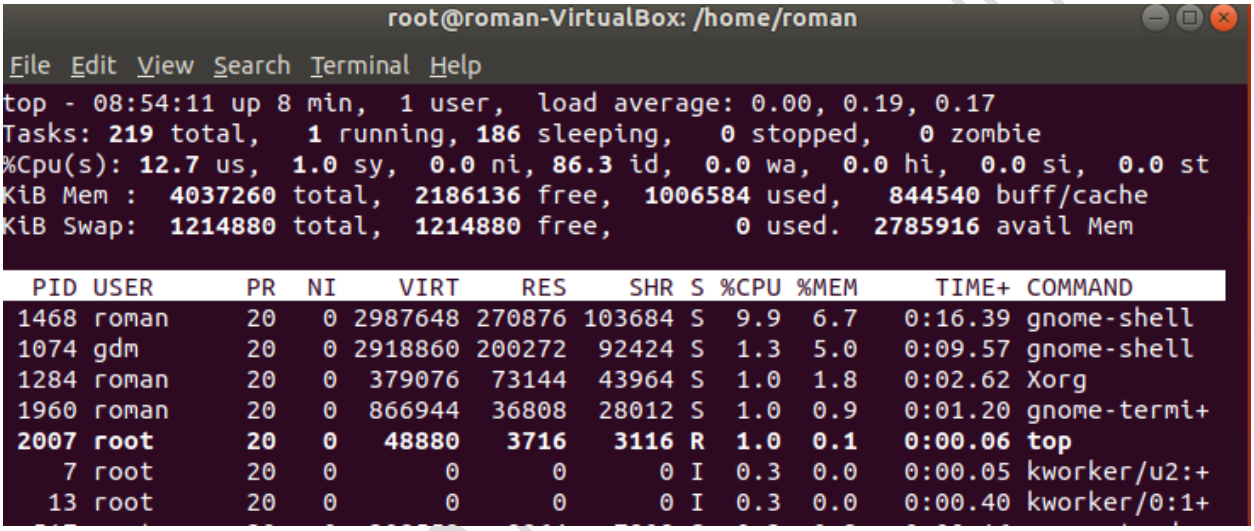
close and cleanup – 15 **(default).**

במידה ויש מספר פקודות שיצאו משליטה ניתן להפסיק את פעילותן לפי שם:

```
killall sleep
```

על מנת לקבל מידע מפורט יותר

```
top
```



h – תפריט הפקודות האפשריות.

< > – סינון על פי עמודה שונה.

k – כדי להפסיק תהליך מעבודות.

m – מצב הזיכרון במכונה.

u – כדי לבחור משתמש כלשהו ולצפות בתהליכים שלו.

אם נרצה לראות נתונים של תהליך אחד ספציפי נבצע את הפקודה:

```
top -p 1324
```

כלי נוסף עם ממשק יותר נוח הינו htop:

```
apt install htop
```

תרגיל

1. הריצו 5 פעמים את התוכנה Wireshark מאחורי הקלעים באותו ה-bash.
2. תהרגו את ה-bash שהריץ את כל ה-Wireshark שהוא בעצם תהליך האבא שלהם, מה קרה לתהליכי ה-Wireshark האם הם נסגרו?
3. תהרגו תהליך Wireshark כלשהו מתוך ה-5 תהליכים.
4. תהרגו את כל 4 תהליכי ה-Wireshark בפקודה אחת.

כדי לקבל מידע על המערכת ולהבין כמה זמן השרת פעיל אנו משתמשים בפקודה uptime בצורה הבאה:

```
uptime
```

תוצאת הפקודה תראה כך:

```
15:17:03 up 3 days,  2:14,  2 users,  load average: 0.00, 0.00, 0.00
```

ניתן לראות בתצוגה את השעה הנוכחית, כמה זמן השרת למעלה, כמה משתמשים מחוברים ואת מצב העומס על השרת על פי הדקה, חמש דקות והחמש עשרה הדקות האחרונות.

free

כדי לצפות בזיכרון אנו משתמשים בפקודה free, תוכנות עם ממשקים גרפיים בדרך כלל מבזבזות יותר זיכרון ולכן עדיף פחות לעבוד עם תוכנות בעלי ממשק גרפי.

הפקודה free מראה כמה ram בשימוש על ידי המערכת והאם ה-swap בשימוש (הסבר מפורט על swap הינו חומר של LPI 101).

Swap זהה ל-page file במערכת ההפעלה Windows, זהו הזיכרון שהמערכת משתמש בו כאשר לא נשאר זיכרון ב-ram.

כדי לקבל את כל המידע משתמשים בפקודה:

```
free -h
```

בעיה נפוצה בתכנות נקראת memory leak, תוכנה שפשוט משתמשת בכל הזיכרון, ניתן לאתר כאלו באמצעות הפקודה top ולחיצה על M.

בסופו של דבר עם ייגמר הזיכרון המכונה לא תקרוס מה שיקרה זה שה-kernel יהרוג את התהליך הבזבזני.

Logs

במכונות לינוקס פועלים תהליכים רבים ולמרבית התהליכים אין ממשק משתמש והם רצים מאחורי הקלעים.

תהליך המתבצע מאחורי הקלעים בלינוקס נקרא demon והוא המקביל ל-service ובגלל שאין לו ממשק הוא שומר לוגים במערכת על מנת שנוכל לקבל אינדיקציה על המתרחש במכונה.

הלוגים במכונת לינוקס נמצאים בתיקיה /var/log ובתיקיה זו ניתן לראות את הלוגים הבאים:

```
root@kali:/var/log# ls
alternatives.log  dpkg.log        macchanger.log  speech-dispatcher
apache2           exim4           messages        sslsplit
apt               faillog         mysql           stunnel4
auth.log          fontconfig.log  nginx           syslog
boot.log          gdm3            ntpstats        sysstat
bootstrap.log     inetsim         openvpn         unattended-upgrades
btmp              kern.log        postgresql      user.log
daemon.log        lastlog         private         wtmp
debug             live            samba           Xorg.0.log
```

רשימת הלוגים בתיקיה:

/var/log/messages – מכיל הודעות כלליות שנשמרו בקובץ במהלך תהליך ה-boot של המערכת, בנוסף הקובץ מכיל גם הודעות של – mail, cron, daemon, kern, auth וגם לוגים של dmesg.

/var/log/dmesg – מכיל מידע על ה-kernel ring buffer, הכוונה לכל המידע שמודפס בעת ההפעלה של המכונה ובו בעיקר תקשורת חומרה תוכנה ומידע על המערכת. אפשר להציג קובץ זה גם באמצעות הפקודה **dmesg**.

/var/log/auth – מכיל מידע על גישה והרשאות המשתמש, מי התחבר למערכת ובאיזו צורה.

/var/log/boot – קובץ נוסף ששומר מידע על המכונה בעת ההפעלה.

/var/log/daemon – מכיל מידע על תהליכים הרצים במכונה מאחורי הקלעים כגון services של windows.

/var/log/kern – מכיל מידע על ה-kernel module מסתכלים בקובץ הזה אם חומרה לא עובדת כראוי לאחר הפעלת המכונה.

/var/log/lastlog – קובץ בינארי לא ASCII שמכיל את כל ניסיונות ההתחברות, את הקובץ קוראים עם הפקודה **last**.

/var/log/btmp – ניסיונות התחברות כושלים, הפקודה **lastb** מסתכלת על הקובץ הזה.

/var/log/faillog – ניסיון התחברות כושלים, את הקובץ ניתן לקרוא עם הפקודה **faillog**.

/var/log/maillog – מכיל לוגים מתהליכי המייל במכונה.

/var/log/user – מיכל מידע כללי על המשתמשים.

/var/log/Xorg.x.log – לוגים של ה-X Server (המנוע הגרפי של הלינוקס) והודעות הקשורות ל-Desktop של המשתמש.

/var/log/wtmp – מי מחובר כרגע למכונה, הפקודה who או w מסתכלת על הקובץ הזה, לפעמים שם הקובץ הינו **utmp**.

/var/log/cups – לוגים השייכים לשרת המדפסות.

/var/log/cron – לוגים השייכים לפעולות מתוזמנות המוגדרות על ידי crontab.

/var/log/secure – פעולות הקשורות בהרשאות וברמת השירותים במכונה לדוגמה התחברות ל-sshd או ניסיון bruteforce יופיע פה.

Syslog

שירות האחראי על שמירת לוגים עבור התוכנות השונות במערכת ומנהל את רמת המידע שיישמר בלוגים, הגדרת syslog הינו חומר של lpi 101 וקובץ הגדרות של השירות נמצא ב-**/etc/syslog.conf.**

במערכות הפעלה חדשות החליפו את השירות ב-**systemd** שהוא המחליף של ה-**init** (חומר של lpi 102).