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 – 7 – משתמשים והרשאות

בשיעור זה אלמד אתכם לעבוד עם הרשאות ומשתמשים.

על מנת לצפות בכל המשתמשים שיש לנו במכונה נפתח את הקובץ המפורסם /etc/passwd.

```
cat /etc/passwd
```

קובץ זה נראה כך:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
.
.
sddm:x:114:117:Simple Desktop Display Manager:/var/lib/sddm:/bin/false
avahi:x:115:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
roman:x:1000:1000:roman,,,:/home/roman:/bin/bash
```

הראשון הוא תמיד המשתמש root מכיוון שזה המשתמש הראשון שנוצר במערכת, בנוסף ניתן לראות שכמעט לכל שירות שמתקינים יש משתמש מטעמי אבטחה.

ברגע שכל שירות רץ עם משתמש משלו יש הפרדת הרשאות וסביבות ואם השירות ייפרץ הוא יקבל את ההרשאות של המשתמש שהשירות רץ איתו.

החלוקה של הקובץ, מתבצעת בצורה הבאה:

```
roman:x:1000:1000:roman,,,:/home/roman:/bin/bash
  1    2    3    4    5            6           7
```

1. **username** – שם המשתמש
2. **password** – בדרך כלל נראה x במקום הסיסמא וזה מציין שהסיסמא שמורה בקובץ shadow.
3. **uid** – המספר הסידורי של המשתמש אשר מחולק בצורה הבאה:
   a. 0 – המשתמש root
   b. 1 – 999 שירות מערכת
   c. 1000+ משתמש רגיל במערכת
4. **gid** – המספר הסידורי של הקבוצה אליה משויך המשתמש, בעת יצרית משתמש הוא משויך לקבוצה של עצמו.
5. **Info** – הערה כללית כלשהי
6. **home dir** – תיקיית הבית של המשתמש או התיקייה ממנה פעול השירות.
7. **shell** – לאיזה shell אנו מתחברים בעת התחברות למשתמש
   a. **/bin/false** – משתמש נעול
   b. **/bin/nologin** – משתמש נעול
   c. **/bin/sh** – shell ישן וקל
   d. **/bin/bash** – ברירת מחדל

<u>על מנת ליצור משתמש אנו משתמשים בפקודות:</u>

- **useradd** – פקודה סטנדרטית להוספת משתמשים
- **adduser** – סקריפט עזר ליצירת משתמשים אינטרקטיבי.

<u>הדגלים של **useradd**:</u>

- -m יצירת תיקיית בית למשתמש
- -d להגדיר איפה יהיה ה-home directory במידה והוא שונה משם המשתמש.
- -c תיאור כללי למשתמש

- g- מספר הקבוצה של המשתמש
- G- הוספת המשתמש לקבוצה במידה וקיימת
- u- הגדרת user id
- s- הגדרת ה-shell של המשתמש

דוגמה:

```
useradd -G "HELPDESK" -m -c "my user" -s "/bin/bash" -d "/home/cool" roman
passwd roman
```

ניתן גם להגדיר שלמשתמש לא תהיה סיסמא כך:

```
useradd roman && passwd -d roman
```

או לבצע יצירת משתמש מהירה אטרקטיבית.

```
adduser roman
```

בנוסף לקובץ **/etc/passwd** ישנם עוד 3 קבצים חשובים:

- **/etc/shadow** – כל המידע הקשור לסיסמא כולל תוקף סיסמא וכל הפרטים שיש בפקודה **chage**
- **/etc/group** – מידע על הקבוצות במערכת
- **/etc/gshadow** – קובץ שאינו בשימוש כרגע והוא מכיל מידע על סיסמאות קבוצה

עריכת משתמש לאחר שהוא נוצר באמצעות הפקודה:

```
usermod
```

c- הערה חדשה

```
usermod -c "new comment" roman
```

d- מחליף תיקיית

```
usermod -d /home/newperson newperson
```

L- נעילת משתמש
U- פתיחת משתמש
G- הוספת משתמש לקבוצה
m- העברת התוכן לתיקייה חדשה

במידה ונרצה למחוק את המשתמש נשתמש בפקודה **userdel**

```
userdel -r roman
```

r- מחק גם את הקבצים בתיקיית הבית
f- גם אם יש שם קבצים שהם לא שלו

כדי להכריח משתמש להחליף סיסמא ניתן לעשות זאת באמצעות (חומר של LPI 101)

```
chage roman
chage -d 0 roman
```

l- מידע על מתי תוקף הסיסמא פג
E- הגדרת תוקף לחשבון המשתמש

```
chage -E 2011-07-19 roman
```

כדי להציג מידע על chage של משתמש נשתמש בפקודה כך:

```
chage -l roman
```

כדי לצפות בכל הקבוצות במערכת משתמשים בפקודה:

```
cat /etc/group
getent group
```

ליצור קבוצה:

```
groupadd [groupname]
```

למחוק קבוצה:

```
groupdel [groupname]
```

לשייך משתמש לקבוצה:

```
adduser [user] [group]
deluser [user] [group]
```

צפייה באלו קבוצות נמצא משתמש –

```
groups roman
```

תרגיל

1. תצורו את המשתמש helpdesk ואל תשכחו להגדיר למשתמש תיקיית בית.
2. הכניסו את המשתמש לקבוצת sudo.
3. בצעו את הפקודה

```
sudo vi /etc/passwd
```

4. שנו את ה-id של המשתמש helpdesk ל-0 והתחברו למשתמש.

כדי להריץ פקודות מנהל (root) -

```
sudo [username] shutdown -r now
sudo roman shutdown -r now
```

אם אתם לא מצליחים לבצע את פקודת sudo סימן שאתם לא בקבוצה sudo ולכן נשתמש בפקודה:

```
adduser roman sudo
```

אבטחה בסיסית

כדי לקבל מידע על המשתמש הנוכחי נבצע את הפקודות הבאות:

- **id** – הפקודה מציגה את ה מזהים של המשתמש שאיתו אתם מחוברים מה שנראה כך:

```
uid=0(root) gid=0(root) groups=0(root)
```

- **whoami** – מי המשתמש שאליו אתם מחוברים

כדי לדעת מי מחובר כרגע למכונה:

- **w** – מי מחובר כרגע למכונה ובאיזה חלון
- **who** – מי מחובר כרגע למכונה ומאיזה IP הוא הגיע + מתי הוא התחבר.

כדי לקבל מידע על ניסיונות התחברות וכישלונות:

- **last** – מי הצליח להתחבר למכונה ומתי
- **lastb** – ניסיונות התחברות מרחוק שנכשלו (ssh)

הרשאות

נתחיל בפקודה ls -l ומשמאל אנו יכולים לראות את ההרשאות:

```
-rw-r--r--   1  root root          1264 Oct 26 2019     roman.file
```

בתצוגה אנו רואים שלושה זוגות:

- השלישייה הראשונה מתייחסת לowner
- השלישייה הבאה מתייחסת לgroup
- השלישייה האחרונה מתייחסת לכל השאר

שימו לב, ההרשאות מתחלקות לסוגים, הרשאות תיקייה או הרשאות לקובץ

תיקייה:

- x – כדי להיכנס בפנים
- w – כדי ליצור קבצים
- r – כדי להציג את התוכן והשלמת פקודות כשאני בפנים

קבצים:

- x – כדי להריץ
- w – כדי לכתוב בפנים
- r – כדי לראות את התוכן

ההרשאות נאכפות משמאל לימין, קודם כל הרשאות owner. אם אין לי הרשאה ב-owner ואני בעל הקובץ אז לא אקבל גישה וזה לא משנה אם אני חבר בקבוצה שיש לה הרשאות לקובץ או אם לכל שאר המשתמשים יש הרשאה.

לאחר מכן מסתכלים על ה- group אם אין לי הרשאות group ואני בקבוצה הרלוונטית לא תיהיה לי הרשאה לקובץ גם אם לכל שאר המשתמשים במערכת יש הרשאה.

מצב שלישי ואחרון הינו מצב שבו אני לא הבעלים של הקובץ ואני לא בקבוצה של הקובץ אז ההרשאות שיחולו עלי הינם הרשאות ה-others.

שינוי ההרשאות מתבצע בצורה הבאה:

- u – זה user
- g – זה group
- o – זה other
- + לתת הרשאה
- - לקחת הרשאה
- x – execute
- r – read
- w – write

מה שיראה כך:

```
chmod ugo-x file
chmod ugo+x-r file
chmod u+x,g-r,o+rwx file
chmod u=rw,g=x,o= file
chmod +x file
```

תרגיל

1. תצרו את המשתמשים **user1**,**user2**,**user3**.
2. צרפו את המשתמש **user2** לקבוצה **user1**
3. התחברו למשתמש **user1** ותצרו את התיקייה **/tmp/user_folder** שנו את ההרשאות כך שרק **user1** יוכל להיכנס לתיקייה.
4. כעת הריצו את הפקודה

```
chmod g=rw,o=x
```

האם המשתמש user2 יכול ליצור קבצים ולקרוא את התוכן שלהם בתיקייה **user_folder**?

האם המשתמש user3 יכול ליצור קבצים ולקרוא את התוכן שלהם בתיקייה **user_folder**?

האם המשתמשים user2 או user3 יכולים להיכנס לתיקיה ולצפות בתוכן שלה?

5. שנו את ההרשאות לתיקייה **user_folder** כך ש-**user2** ו-**user3** יוכלו לקרוא, ליצור ולהיכנס לתיקייה ו-**user1** לא יוכל לא להיכנס לתייקה, לא לצפות בתוכן שלה ולא ליצור קבצים.

הרשאות בייצוג מספרי:

קיימת שיטה נוספת לייצוג הרשאות, בשיטה זו אנו מגדירים את ההרשאות באמצעות מספר בצורה הבאה:

```
7 = 4+2+1 (read/write/execute)
6 = 4+2 (read/write)
5 = 4+1 (read/execute)
4 = 4 (read)
3 = 2+1 (write/execute)
2 = 2 (write)
1 = 1 (execute)
```

הגדרת הרשאות כללית בשיטת הייצוג המספרי:

```
chmod xxx [file name]
chmod --reference 1.txt 2.txt
```

כמו כן, ברירת המחדל של כל קובץ שאתם יוצרים הינה 755 והיא מוגדרת באמצעות המשתנה הסביבתי **umask** בצורה הפוכה. כך שאם נגדיר את ב-**umask** את הערך 0022 נקבל 755.

לאחר מכן מערכת ההפעלה מורידה את הרשאת הריצה אוטומטית x ולכן נקבל בפועל את ההרשאה 644 כברירת מחדל.

כדי לשנות הגדרה זו אנו מבצעים את הפקודה

```
umask [permission]
umask 0077
```

ובפועל הקובץ שניצור יהיה בעל ההרשאות 600

שינוי בעל הקובץ:

```
chown [username] [filename]
```

לשנות את הקבוצה של הקובץ

```
chgrp [groupname] [filename]
```

אם נרצה לבצע את הפעולות על מספר קבצים ותיקיות נוסיף לפני שם המשתמש את הדגל R–.

ניתן לשבל את 2 הפקודות האחרונות לפקודה אחת שתשנה גם את בעלות הקובץ וגם את הקבוצה:

```
chown root:my_group
chown :my_group
chown my_owner:
```

אם אני רוצה לשנות קבוצה עם chown נבצע זאת בעזרת

```
chown :my_group
```

הרשאות מיוחדות נושא של LPI 101

suid – נותן לקובץ הרשאות של ה-owner וכל מי שיריץ את הקובץ ירוץ עם ההרשאות של ה-owner, פקודה מאוד מסוכנת.

ping זו פקודה שרק root יכול לבצע ואם נוסיף לקובץ suid כל אחד יוכל להריץ אותה עם הרשאות של root.

guid – מי שמריץ את הקובץ מקבל את ההרשאות של הקבוצה, וכאשר מפעילים זאת על תיקייה אז כל קובץ בתוך התיקייה הוא בבעלות הקבוצה אוטומטית.

sticky Bit – הפקודה פעם הייתה משאירה את הקובץ בram גם לאחר שהינו סוגרים אותו והיום הפקודה יעילה על תיקיות וכך כל קובץ בתוך התיקייה ניתן למחיקה רק ליוצר הקובץ.

<u>טבלת ההרשאות:</u>

4- suid [u+s]

2- sgid [g+s]

1- sticky [o+t]

אם קודם לקובץ הייתה הרשאת x אז האות תיהיה קטנה אחרת האות תיהיה גדולה S T.

```
chmod u+s /bin/ls
ls /root/
```

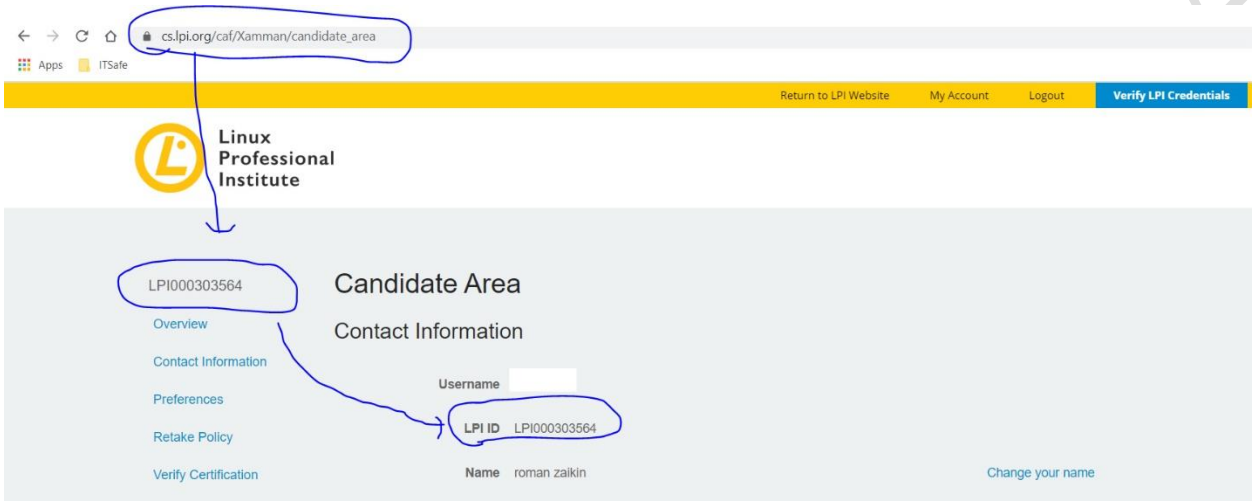
בדרך כלל זה מה שעושים על הפקודה ping.

מבחן הסמכה:

1. פותחים משתמש אישי באתר Linux Professional Institute:

https://cs.lpi.org/caf/Xamman/register?glang=en&gurl=register.html

2. לאחר ההרשמה תעתיקו את קוד המשתמש שלכם מהאתר אצלי הוא LPI000303564

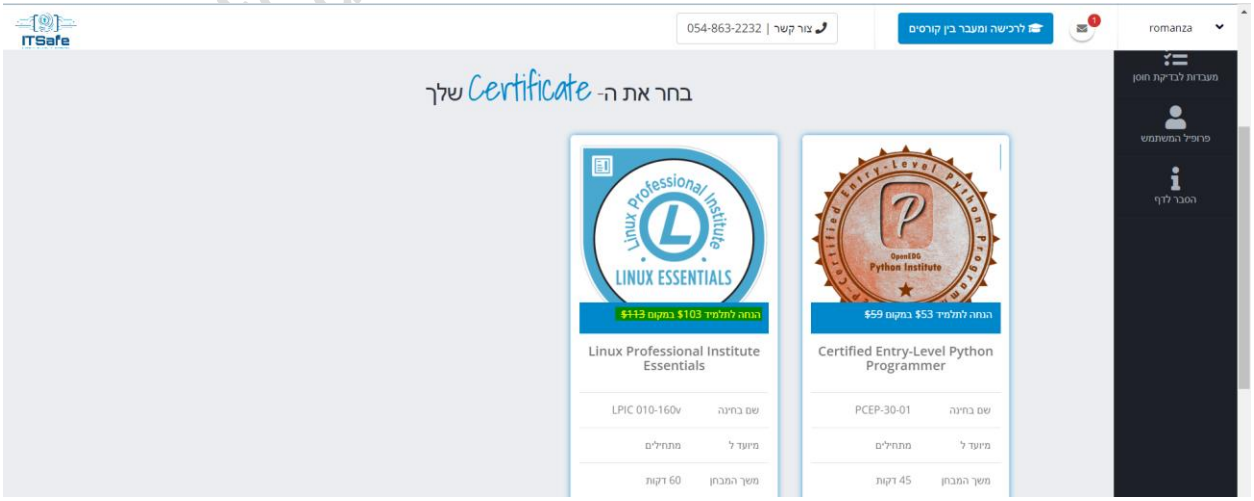


3. פתיחת משתמש ב- pearsonVUE לבחינות (Linux,Cisco,Microsoft) ומקשרים אותו לחשבון ה-LPIC שלכם באמצעות הקוד משתמש שלכם.

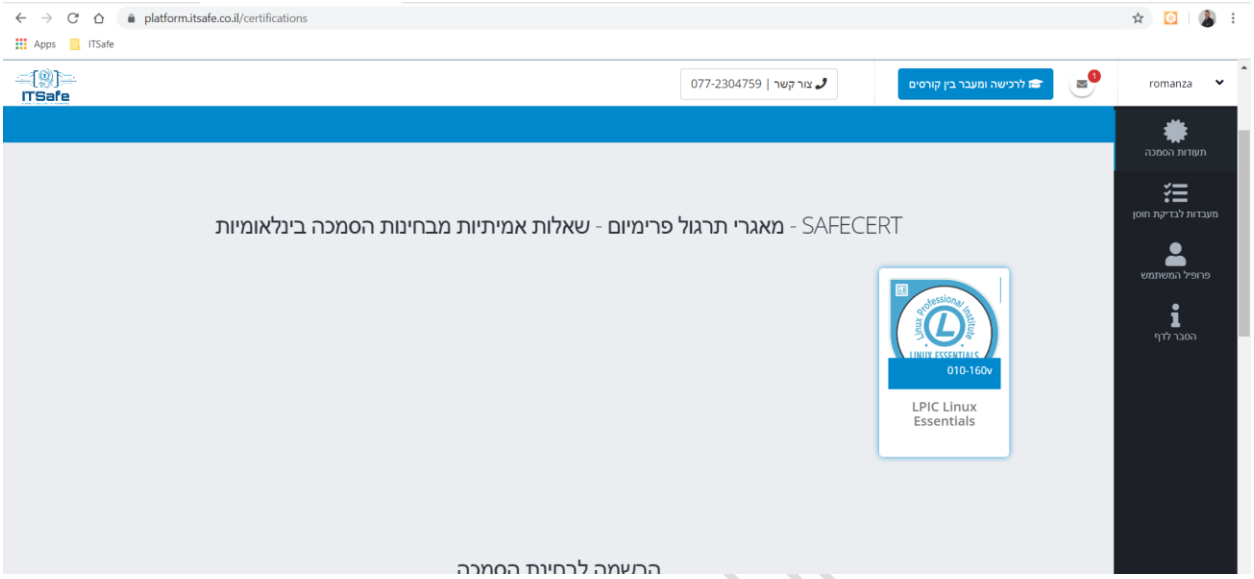
https://wsr.pearsonvue.com/testtaker/profile/create/SignUp.htm?locale=en_US&clientCode=LINUXPROFESSION

4. רוכשים קוד קופון למבחן ומתרגלים את השאלות לפני הגישה למבחן בסימולטור SafeCert.

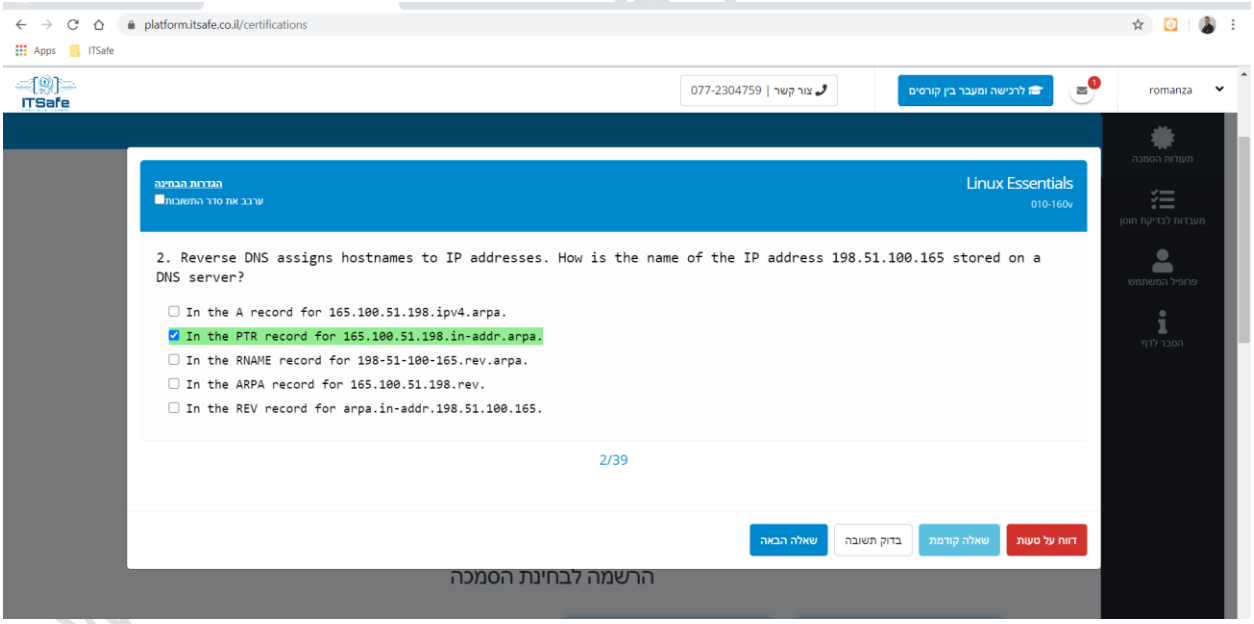
http://platform.itsafe.co.il/certifications



לאחר סיום הרכישה המערכת תצרף אתכם לרשימת התלמידים המעוניינים לגשת למבחן ובמהלך היום תקבלו מייל עם הקוד גישה שלכם, בנוסף לאחר התשלום תקבלו גם גישה לסימולטור פרימיום של ITSafe הנקרא SafeCerts שמכיל שחזורי שאלות למבחן.



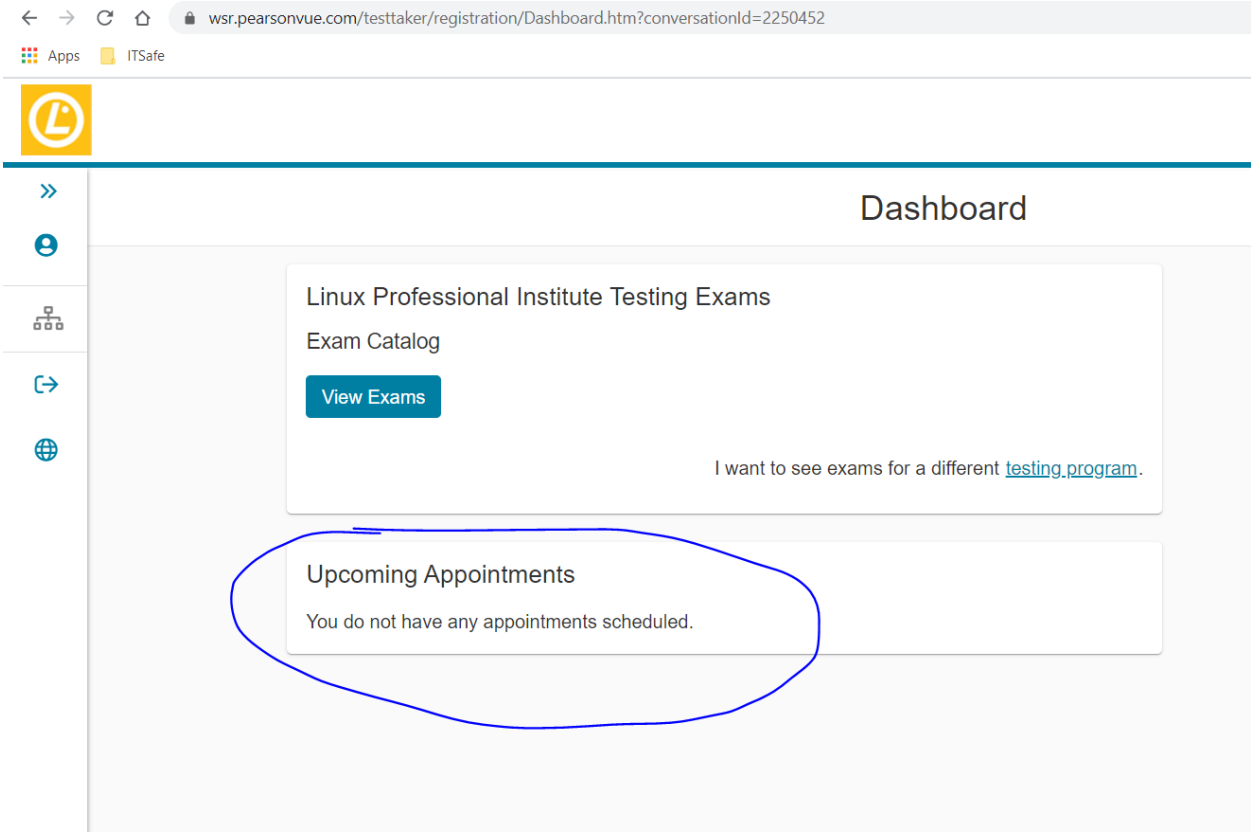
רק לאחר שתראו שאתם עונים על כל השאלות נכונה בסימולטור ומבינים את התשובות יש לגשת למבחן.



5. הרשמה לבחינה עצמה:

https://home.pearsonvue.com/lpi

6. הגישה לבחינה גם כן מהלינק הזה בחלק התחתון:



7. עברתם את המבחן בהצלחה? ייקח למערכת של LPI **כשעתיים לשלוח** לכם את התעודה למייל!
8. שלחו לנו את התעודה 😉