

# הקשחת מערכת לינוקס

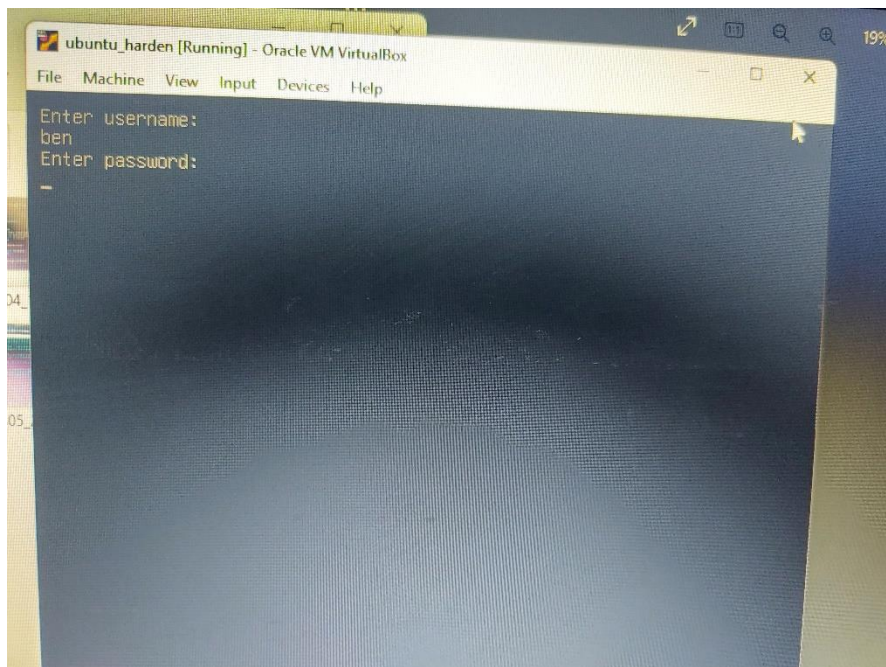
## רקע כללי:

מדובר במכונה שבה עושים שימוש מספר אגפים שונים בחברה. המכונה נמצאת בחוות השרתים הפרטית של החברה והתבקשתי לבצע הקשחה של מערכת ההפעלה על מנת למנוע אפשרות של פגיעה בחברה, שכן המכונה משמשת לחלק גדול מהעבודה השוטפת שלה. על המכונה מותקנת מערכת הפעלה לינוקס הפצת אובונטו.

## ההקשחה בוצעה במספר מישורים

### המישור הפיזי:

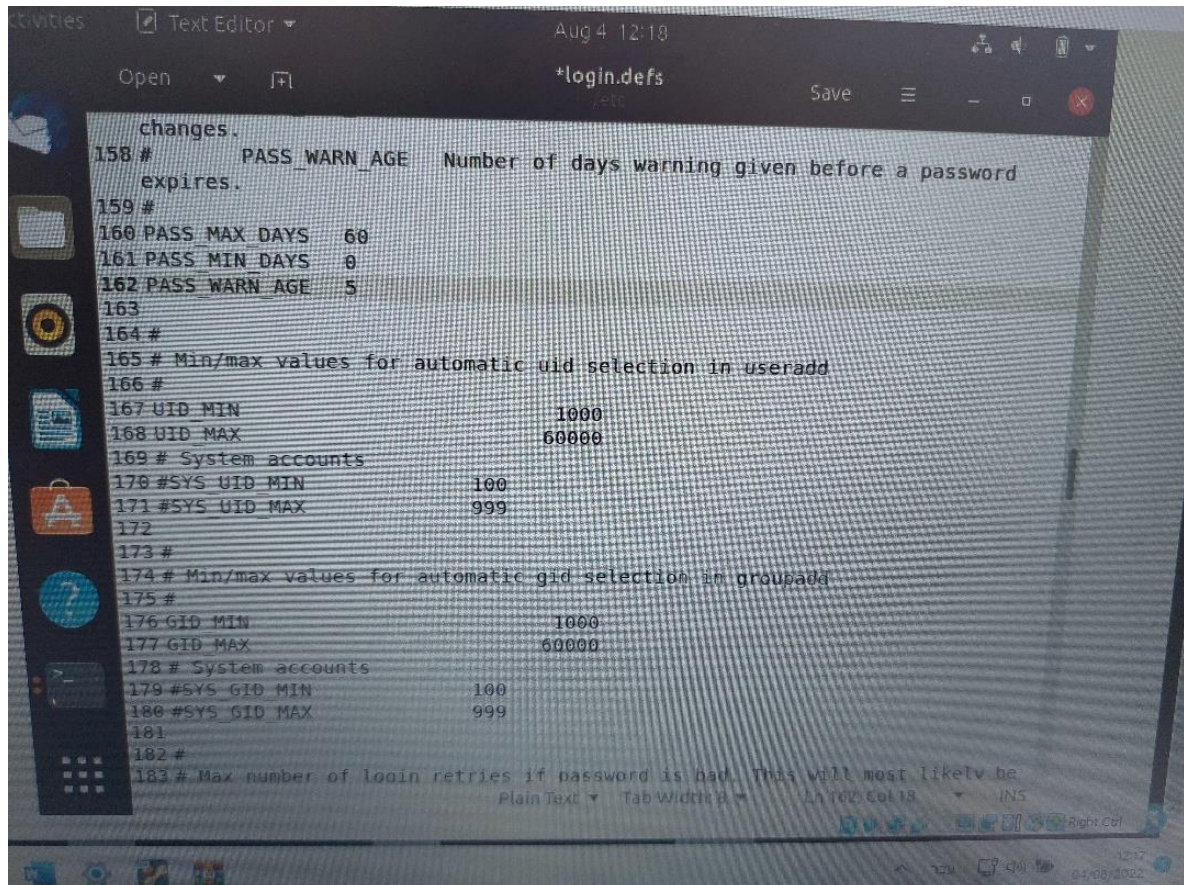
1. השרת הוכנס לארון נעול. גישה רק לבעלי תפקיד אשר זקוקים לגישה פיזית לביצוע עבודתם.
2. הוגדרה סיסמא לחשבון רוט למניעת התחברות אוטומטית במצב יוזר יחיד.
3. הוגדרה סיסמא לboot במטרה למנוע התערבות של בלתי מורשים בתהליך.



4. ישנה הצפנה של כונן קשיח אשר בו נמצא חומר שהוגדר על ידי מנהלי החברה כרגיש/קנייני.

## חשבונות ותצורת עבודה:

1. הפרדת תפקידים ושמירה על מינימום הרשאות לביצוע התפקיד על ידי חלוקה ל- 3 קבוצות משתמשים: production, networking, support. לכל קבוצה יש מנהל ותיקיית עבודה משלה. אין גישה לתיקייה למי שאיננו חבר הקבוצה.
2. למנהלי הקבוצה ישנן הרשאות נוספות לתיקייה admin בתוך התיקייה של הצוות שלו ורק הוא רשאי לקרוא ולכתוב בתיקייה זו.
3. למנהל הnetworking יש הרשאת sudo מוגבלת רק להרצת פקודות עדכון והתקנה דרך apt כדי שיוכל להתקין ולעדכן תכנות – צורך בעבודה שלו כאחראי רשתות.
4. שימוש במדיניות סיסמאות – מינימום 12 תווים, לפחות אות אחת גדולה וקטנה, לפחות מספר אחד ולפחות תו מיוחד אחד כדי לא להקשות יתר על המידה ולשמור על סביבה מאובטחת במקביל.
5. יצירת תוקף לסיסמאות: 60 יום, 5 ימים לפני תום התוקף יעודכן המשתמש. בנוסף מניעת חזרה על סיסמאות. 4 ניסיונות כושלים יובילו לחסימה, לצורך מניעת ניסיונות פיצוח סיסמא.



```
changes.
158 #      PASS_WARN_AGE    Number of days warning given before a password
    expires.
159 #
160 PASS_MAX_DAYS    60
161 PASS_MIN_DAYS    0
162 PASS_WARN_AGE    5
163
164 #
165 # Min/max values for automatic uid selection in useradd
166 #
167 UID_MIN            1000
168 UID_MAX            60000
169 # System accounts
170 #SYS_UID_MIN        100
171 #SYS_UID_MAX        999
172
173 #
174 # Min/max values for automatic gid selection in groupadd
175 #
176 GID_MIN            1000
177 GID_MAX            60000
178 # System accounts
179 #SYS_GID_MIN        100
180 #SYS_GID_MAX        999
181
182 #
183 # Max number of login retries if password is bad. This will most likely be
```

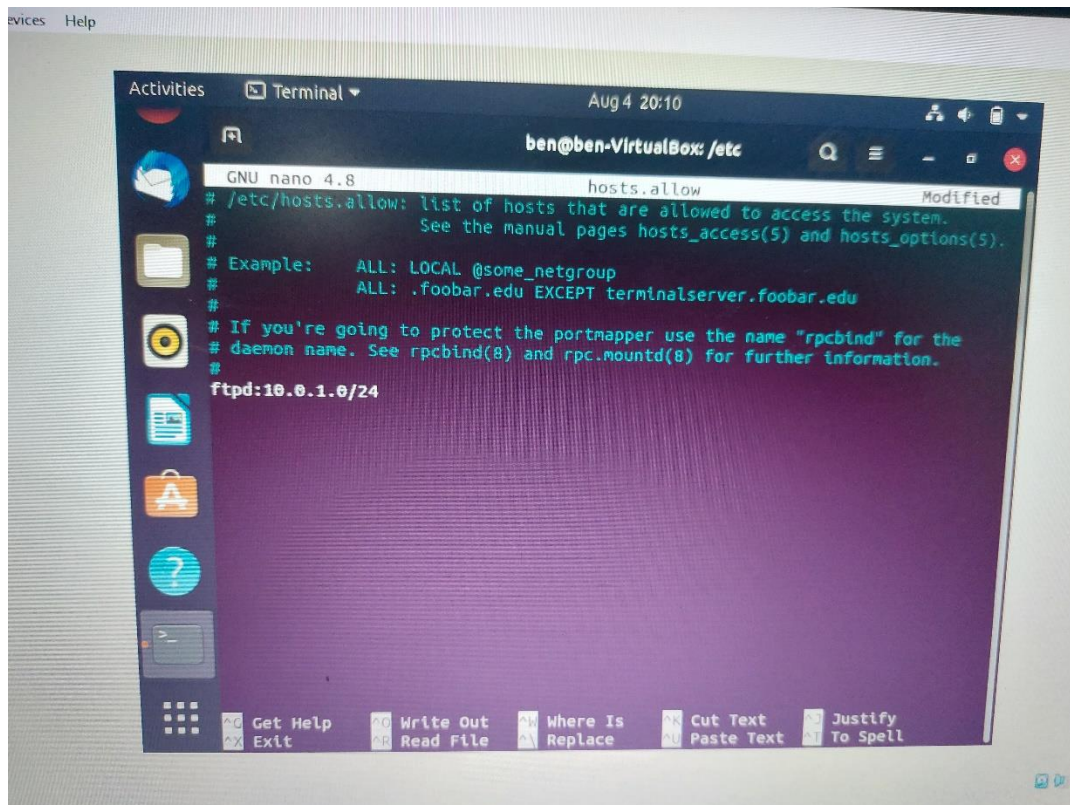


```
File Machine View Input Devices Help
Activities Terminal Aug 6 01:00
ben@ben-VirtualBox: /home
ben@ben-VirtualBox:/home$ ll
total 36
drwxr-xr-x  9 root      root      4096 Aug  4 20:11 ./
drwxr-xr-x 20 root      root      4096 Aug  3 23:10 ../
drwxr-xr-x 15 ben       ben       4096 Aug  5 23:54 ben/
drwxrwxr--  3 networking_dan networking 4096 Aug  5 20:45 Networking/
drwxr-xr-x  5 networking_dan networking_dan 4096 Aug  4 17:41 networking_dan/
drwxrwxr--  3 production_gadi production 4096 Aug  5 20:46 Production/
drwxr-xr-x  2 production_gadi production_gadi 4096 Aug  4 11:22 production_gadi/
/
drwxrwxr--  3 support_ron support support_ron 4096 Aug  5 20:46 Support/
drwxr-xr-x  2 support_ron support_ron 4096 Aug  4 11:22 support_ron/
ben@ben-VirtualBox:/home$
```

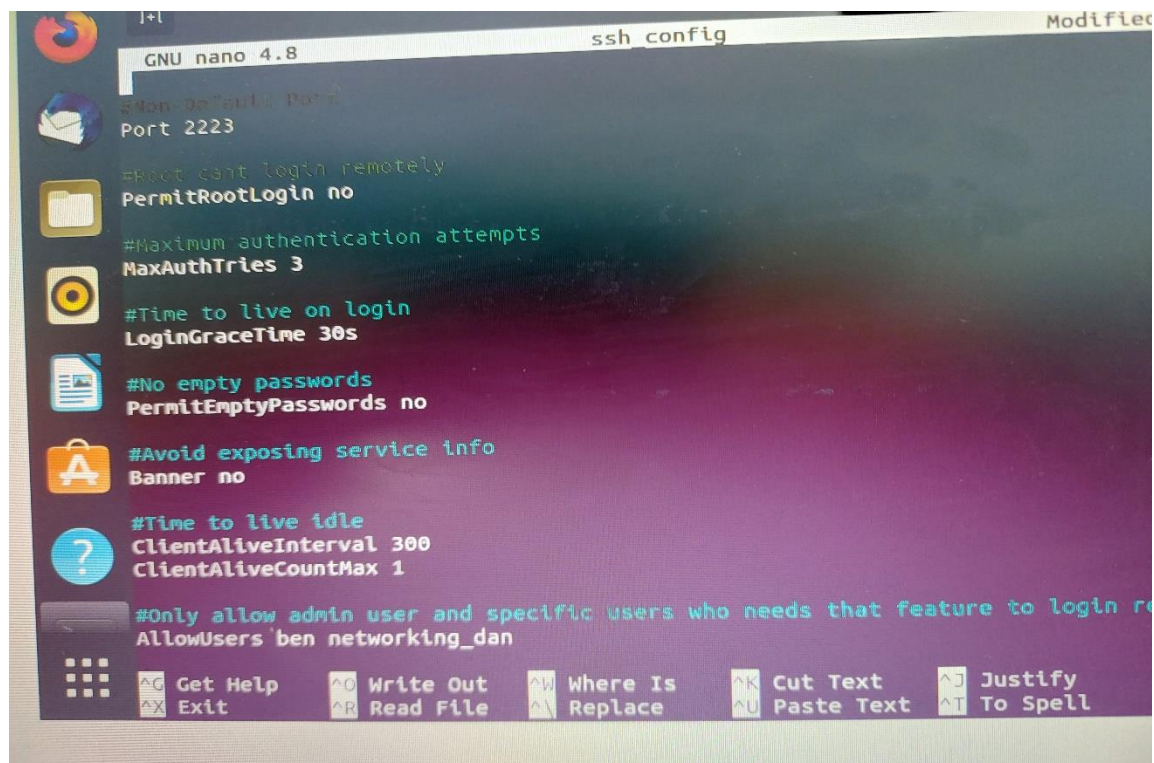
```
networking_dan@ben-VirtualBox: /etc/pam.d
BAD PASSWORD: is too simple
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: it is too simplistic/systematic
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
ben@ben-VirtualBox:/etc/pam.d$ sudo nano common-password
ben@ben-VirtualBox:/etc/pam.d$ sudo su networking_dan
networking_dan@ben-VirtualBox:/etc/pam.d$ passwd
Changing password for networking_dan.
Current password:
passwd: Authentication token manipulation error
passwd: password unchanged
networking_dan@ben-VirtualBox:/etc/pam.d$ passwd
Changing password for networking_dan.
Current password:
New password:
BAD PASSWORD: it does not contain enough DIFFERENT characters
New password:
BAD PASSWORD: it is WAY too short
New password:
```

## מישור הרשת:

1. על מנת לבצע את העבודה מרחוק קיים שירות SSH. בוצעה הקשחה של השירות.
  - א. מוגדר בפורט 2223.
  - ב. לא ניתן להתחבר כרוט בSSH.
  - ג. מקסימום 4 סיסמאות שגויות בהתחברות מוביל לחסימה.
  - ד. 30 שניות להזין סיסמא בהתחברות, ככל ולא הוזנה מנתק את המשתמש. בנוסף הגדרת זמן מקסימלי ללא פעולה. ניתוק של משתמש שלא מבצע שום פעולה על מנת למנוע מצב שמשתמש שכח session דולק ועזב את המחשב.
  - ה. רק יוזר אחד יכול להתחבר מרחוק – מחוץ לLAN עקב צורך עבודה. השאר רק מתוך הרשת הפנימית.
2. הגדרת פיירוול UFW. הגדרה שלו בתצורה של whitelist אישור רק להתחברות מבחוץ על פורט 2223, כל השאר חסום.
3. חסימת כתובת של משתמש שטועה בסיסמא בSSH חמש פעמים.
4. שירות FTP שניתן לגשת אליו רק מתוך הרשת הפנימית כדי לאפשר סביבת עבודה ולמנוע משיכת קבצים מרחוק.







```
GNU nano 4.8 ssh_config Modified
#Non-Default Port
Port 2223

#Root cant login remotely
PermitRootLogin no

#Maximum authentication attempts
MaxAuthTries 3

#Time to live on login
LoginGraceTime 30s

#No empty passwords
PermitEmptyPasswords no

#Avoid exposing service info
Banner no

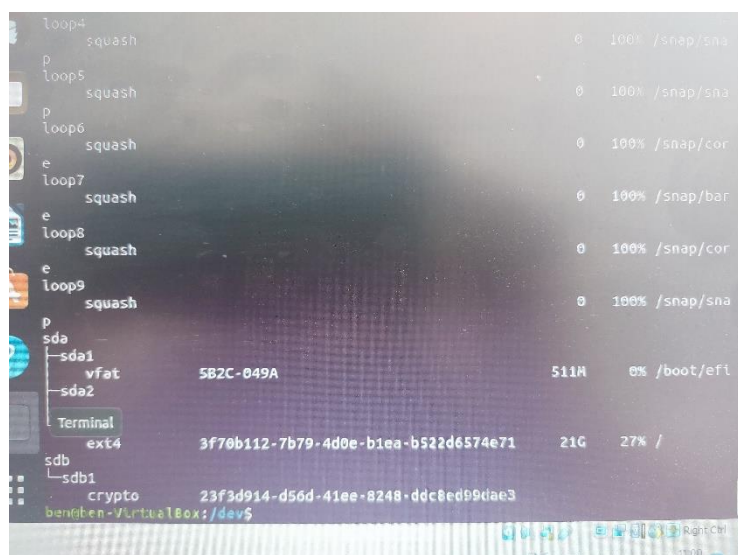
#Time to live idle
ClientAliveInterval 300
ClientAliveCountMax 1

#Only allow admin user and specific users who needs that feature to login re
AllowUsers ben networking_dan

Get Help      Write Out    Where Is     Cut Text     Justify
Exit          Read File    Replace      Paste Text   To Spell
```

### מערכת הקבצים:

1. הצפנה של כונן שעליו חומרים רגישים.
2. אנטיוירוס. מתעדכן וסורק לבד.
3. Tripwire – כחלק מסקריפט שמורץ כל שבוע על ידי אחראי האבטחה. בודק שלא נערכו שינויי קבצים רגישים.



## כללי:

1. אין חלוקת חשבונות. כל משתמש עובד עם החשבון שלו.
2. אין שימוש בחשבון רוט.
3. חינוך המשתמשים לזהירות ברשת. אין הכנסת מדיה חיצונית ואין שיתוף חשבונות.
4. סקריפט בחינת סטאטוס אבטחה שמורץ אחת לשבוע. בודק הימצאות חשבונות עם ID 0, חשבונות ללא סיסמא ובדיקת מצב קבצים רגישים מול הדאטה בייס של tripwire.

```
ben@ben-VirtualBox: ~  
-rw-rw-r-- 1 ben ben 219 Aug 4 16:50 checks.sh  
drwx----- 13 ben ben 4096 Aug 5 23:54 .config/  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Desktop/  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Documents/  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Downloads/  
drwx----- 3 ben ben 4096 Aug 4 12:20 .gnome/  
drwxr-xr-x 3 ben ben 4096 Aug 3 23:17 .local/  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Music/  
drwxr-xr-x 2 ben ben 4096 Aug 5 20:44 Pictures/  
-rw-r--r-- 1 ben ben 807 Aug 3 23:12 .profile  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Public/  
-rw-rw-r-- 1 ben ben 300 Aug 5 23:54 script.sh  
drwx----- 2 ben ben 4096 Aug 4 17:36 .ssh/  
-rw-r--r-- 1 ben ben 0 Aug 3 23:19 .sudo_as_admin_successful  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Templates/  
drwxr-xr-x 2 ben ben 4096 Aug 3 23:18 Videos/  
ben@ben-VirtualBox:~$ gedit script.sh  
ben@ben-VirtualBox:~$ sudo bash script.sh  
Users with no password:  
-----  
Users with UID 0:  
root:x:0:0:root:/root:/bin/bash  
-----  
Parsing policy file: /etc/tripwire/tw.pol  
*** Processing Unix File System ***  
Performing integrity check...
```