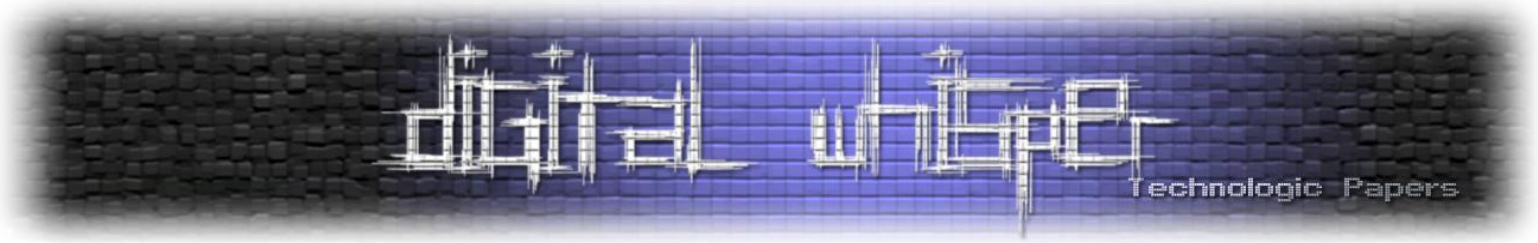


Bootable Back|Track from USB - Persistent Changes

מאת אפיק קסטיאל (cp77fk4r)

הקדמה

פרוייקט Back|Track הוא מערכת הפעלה אשר נועד לשימוש של חוקרי אבטחה, הפצת לינוקס (בגירסא הרביעית היא מבוססת על Ubuntu) המיועדת ל-Penetration Testers והאקרים. הפצה זאת מגיעה עם כמות נכבדת מאוד של כלים לביצוע שלל דברים הקשורים בנושא, כגון כלים למיפוי/פריצת רשתות מקומיות ואלחוטיות, כלים לפיענוח סיסמות, כלים לביצוע מספר רב של מתקפות שונות, כלים לביצוע ההזנות לחיבורי רשת, כלים לביצוע Reverse Engineering, כלים לסריקות חורי אבטחה במערכות שונות, כלים להרצת אקספלויטים ועוד. במאמר זה אסביר איך להתקין את המערכת על התקן Disk On Key "וקינפוגה" כך שהיא "תזכור" (Persistent Changes) את השינויים שביצענו על כל מחשב. כך בעצם ניתן יהיה לטעון אותה מכל מקום, על כל מחשב, מבלי צורך להתקין אותה כל פעם בחדש. שימוש באפשרות זאת מגביר את גמישותה של המערכת בכך שבעזרתה אפשר להפוך כל עמדת-קצה לסביבת עבודה נוחה שלא תבייש שום האקר.

קצת רקע על הפרוייקט:

פרוייקט Back|Track כמו שאנחנו מכירים אותו כיום הוא שילוב של שני הפרוייקטים הבאים: הפרוייקט הראשון-Whoppix, הפצת Penetration מבוססות על Knoppix שבגרסתה השלישית התבססה על Slax ועקב כל שמה שונה ל-Whax (אגב, ה-W מגיע מהביטוי "White-hat"). והפרוייקט השני- Auditor Security Collection (הפצת LiveCD שמבוססת על Knoppix). את הפרוייקט יצרו מתי אהרוני (Muts) - חוקר אבטחה ישראלי, ומקס מוסר (Max Moser). הגירסא הראשונה של Back|Track יצאה בשנת 2006, ונכון להיום (אוקטובר 2009) הגרסה הרביעית של ההפצה נמצאת בשלבי סיום ("Pre-final/Pre-Released").

הכנות לפני ההתקנה

במאמר אני אשתמש ב-Back|Tack 4 Beta, אך הפעולה זהה גם בגירסאות אחרות של ההפצה. במאמר גם אסביר כיצד אפשר לגרום למערכת לזכור את השינויים שביצענו גם לאחר ניתוק התקן ה-USB, ולכך נאלץ ליצור שני מחיצות על ההתקן שלנו.

המחיצה הראשונה שניצור היא מסוג FAT32 תהיה בגודל של לפחות 2GB והמחיצה השניה שניצור תשמש לשמירת השינויים שלנו - והיא תהיה מסוג Ext2 (עבור מחיצה זו מספיק אפילו חצי GB).

- רב התקני ה-USB מגיעים עם מערכת הקבצים NTFS, ולכן עלינו לפרמט אותם ל-FAT32 בשלב הראשון. הדבר לא הכי פשוט מכיוון ש-Windows אינה תומכת בפיצול התקני Removable למחיצות. נרחיב על כך בהמשך.
- בכדי ליצור את המחיצה השניה (Ext2) נשתמש בכלי Fdisk שמגיע עם (כמעט?) כל הפצת לינוקס.
- בכדי לפרוס את קובץ ה-ISO של המערכת על התקן ה-USB ולהגדירו כ-"Bootable" השתמשתי בכלי: "UNetbootin".

חלוקת ההתקן למחיצות:

הכניסו את התקן ה-USB לאחת היציאות המתאימות במחשב. כנסו ל-My Computer ותראו שהמחשב שלנו מזהה את ההתקן כ-Removable Media, אם ננסה לגשת ל:

```
Cntrol Panel=>Administrative Tools=>Computer Management=>Storage=>Disk
Management
```

שימו לב שההתקן אינו מופיע ככונן שאפשר לחלקו למחיצות. למה Windows לא תומך בזה? רק השטן יודע. בכל זאת, ישנה דרך מאוד מעניינת לגרום למערכת להתייחס להתקן ה-USB שלנו כ-Local Disk. על מנת לגרום ל-Windows להתייחס להתקן ה-USB כ-Local Disk אנחנו צריכים להוריד את הקובץ הבא, (הוא ישמש לנו כ-"Driver" תואם):

http://www.lancelhoff.com/downloads/USB_LocalDisk.zip

לאחר הורדת הקובץ עלינו להגדיר מספר דברים במנהל ההתקנים (Device Manager) של מערכת ההפעלה. ב-"My Computer" יש ללחוץ כפתור ימני על התקן ה-USB, ולבחור ב-"Properties". שם ניגש ללחוצץ "Hardware", תחת "All Disk Drives" נסמן את התקן ה-USB ונבחר שוב ב-"Properties". ניגש

לחוצץ האחרון-"Details" ואיפה שכתוב "Property" נבחר ב-"Device Instance Path" (למשתמשי XP יהיה כתוב "Device Instance Id") ונעתיק את התוכן שקיים ב-"Value". תוכן זה משתנה מהתקן להתקן. אצלי הוא:

```
USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER&REV_8.01\0876011D7201D615&0
```

[לכל התקן יש מחרוזת "Device Instance" שונה, המהווה את ה"מיקום" של ההתקן לגבי הקרנל.]

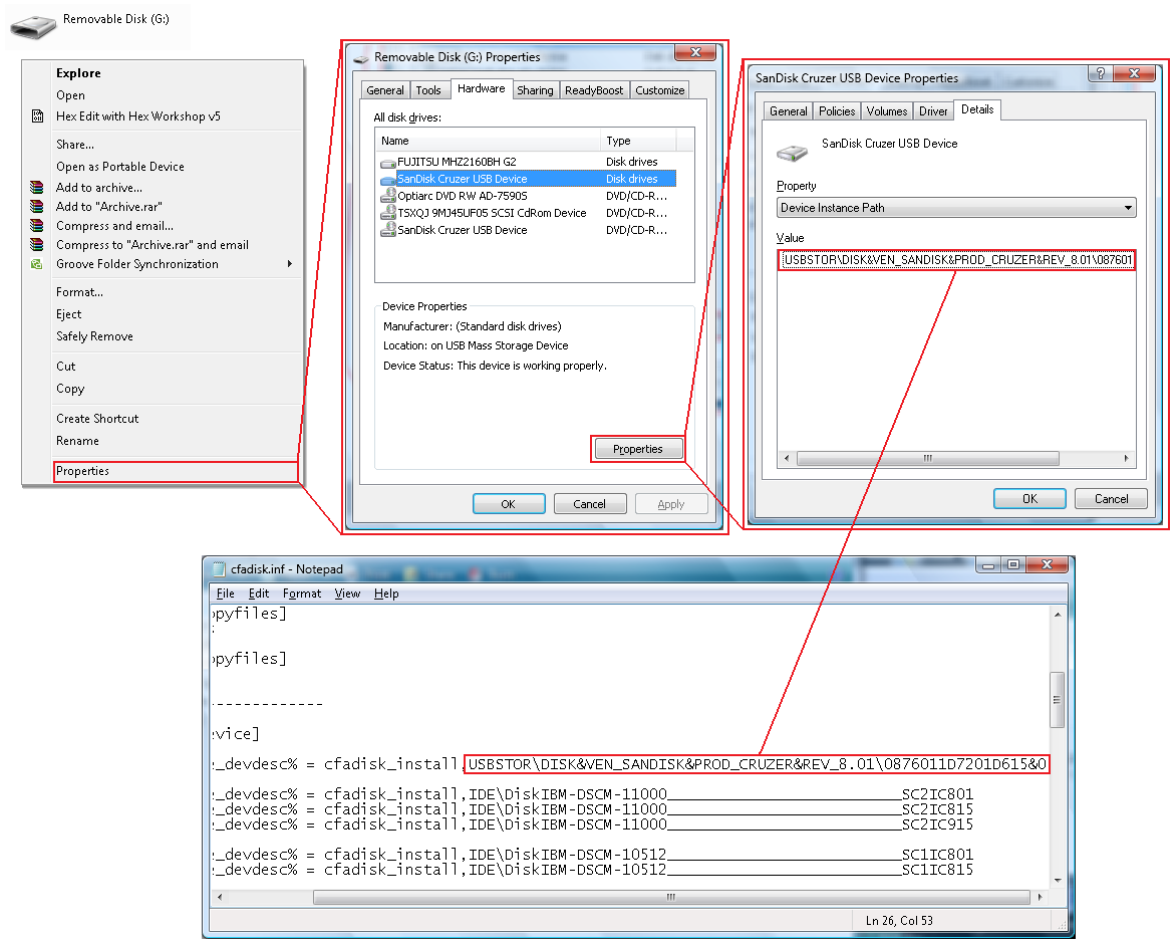
פיתחו את הקובץ שהורדנו בתחילת הפרק (USB_LockDisk) ופירסו אותו לתיקיה על מחשבכם. חפשו בתיקיה את הקובץ שאחראי על הקונפיגורציה של הדרייבר (cfadisk.inf), פיתחו אותו עם כתבן ובשורה 26 אמורה להופיע לכם המחרוזת הבאה:

```
%Microdrive_devdesc% = cfadisk_install,device_instance_id_goes_here
```

את איפה שכתוב "device_instance_id_goes_here" שנו למחרוזת ששמרנו קודם. התוצאה הסופית:

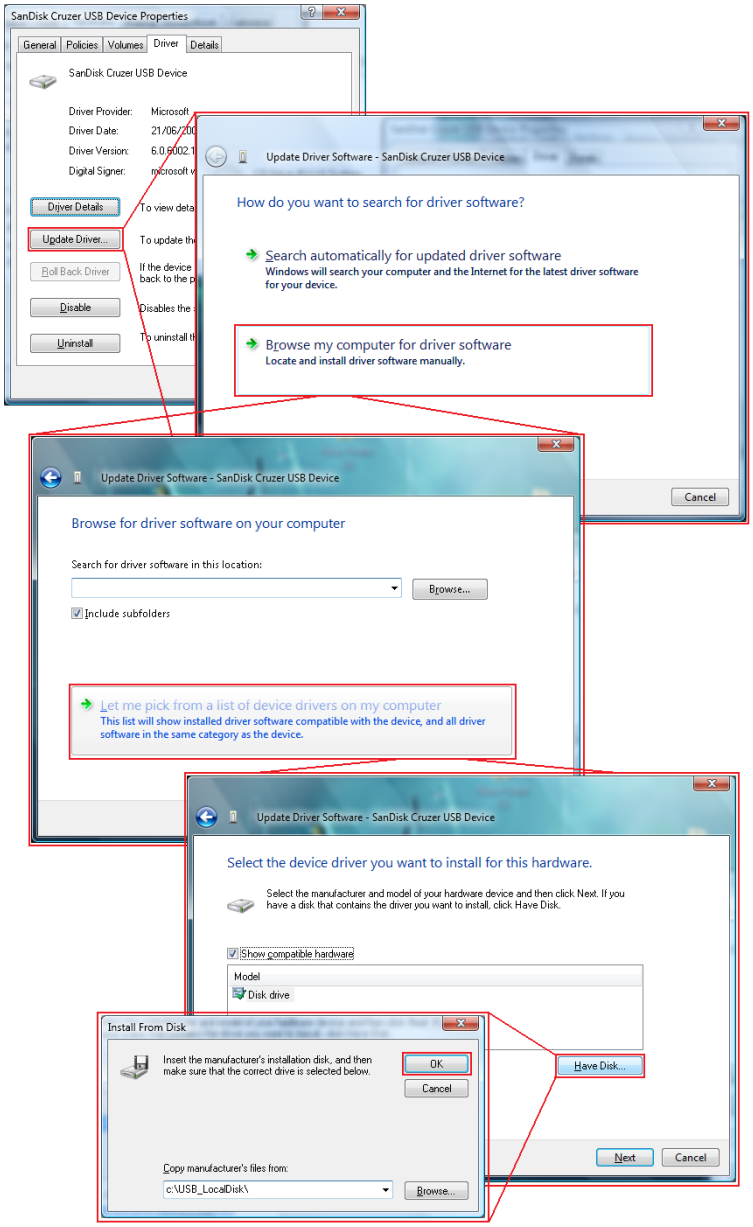
```
%Microdrive_devdesc% =
cfadisk_install,USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER&REV_8.01\0876011D7
201D615&0
```

שימרו את הקובץ וסיגרו אותו. התרשים הבא ממחיש את התהליך:



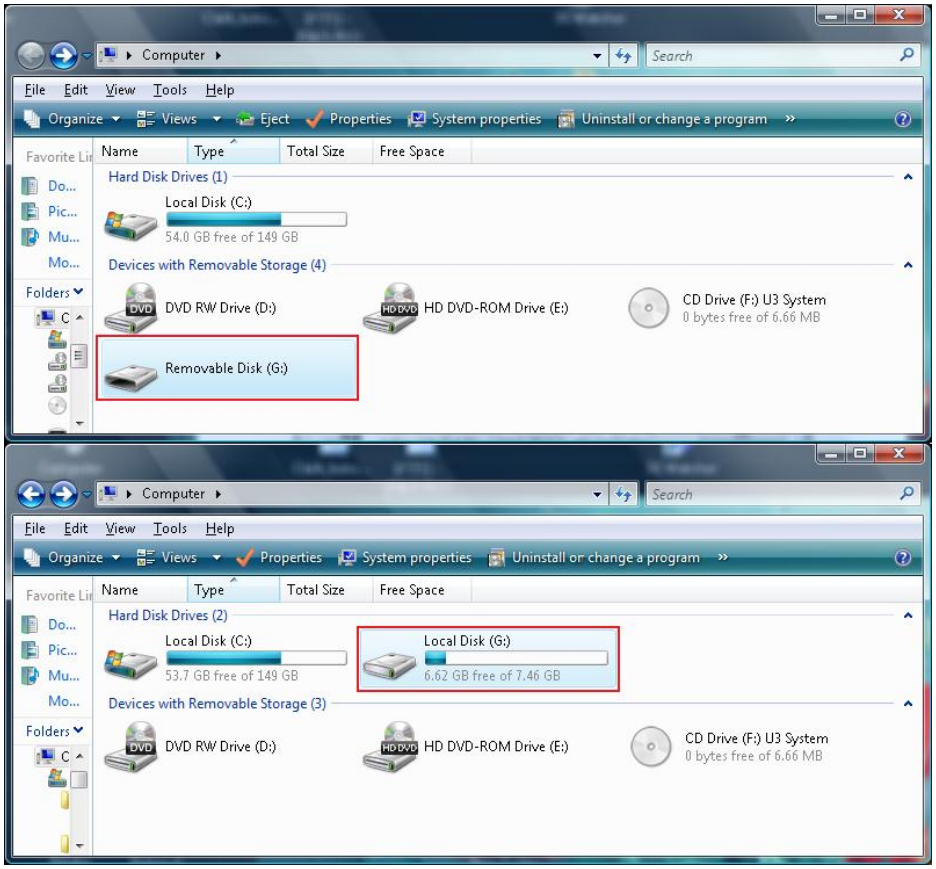
לאחר שהתאמנו את הדרייבר שלנו- אנחנו צריכים להתקין אותו להתקן הספציפי שלנו, בכדי לעשות זאת נשתמש במנהל ההתקנים של המערכת.

גשו שנית לתפריט המאפיינים של התקן ה-USB שלכם (אחרי שבחרתם תחת "All Disk Drives" ולחצתם על "Properties"), ושם במקום לבחור ב-"Hardware" ביחרו ב-"Driver". בתפריט שנפתח לכם, ביחרו ב-"Update Driver..." ושם ביחרו באפשרות השניה "Browse my computer for driver software" (האפשרות הידנית), לאחר מכן ביחרו באפשרות של " Let me pick from a lift of device drivers on my computer" ושם ליחצו על "Have Disk.."., יפתח לכם חלון שם "Browse" ושם נווטו לתיקית ה-"USB_LockDisk" שהורדתם וליחצו על אישור.



לאחר שתלחצו על "OK" - מנהל ההתקנים לבד יזהה את קובץ ה-inf וישאל אתם האם אתם בטוחים שאתם רוצים לבצע את הפעולה. לאחר שתאשרו תקפוץ לך הודעה אשר תזהיר אתכם כי הדרייבר שאתם מנסים להתקים אינו נחתם באופן תקני והדבר יכול להוות סיכון. אשרו וחכו לסוף התהליך.

בסוף התהליך תאלצו להדליק את המחשב מחדש (המלצה של מערכת ההפעלה- לא שלי) ושימו לב שמעכשיו מערכת ההפעלה תזהה את התקן ה-USB שלכם כ-"Local Disk". (תוכלו לראות את זה אם תכנסו ל-"My Computer"..):

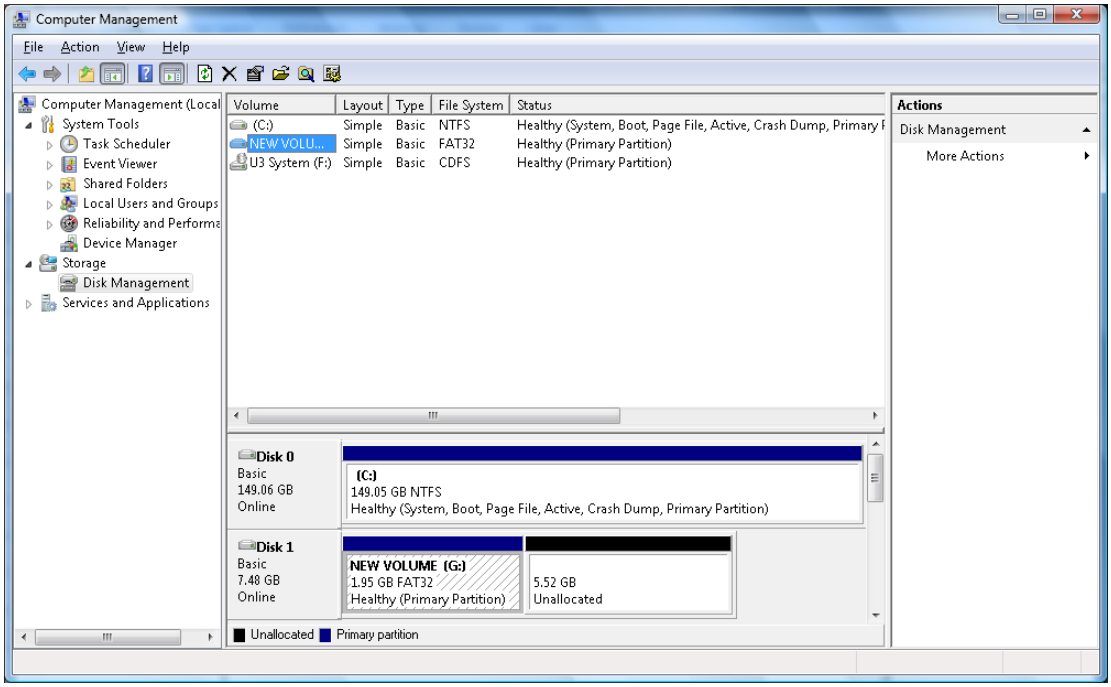


עכשיו, כל שעליכם לעשות הוא להכנס ל:

Cntrol Panel=>Administrative Tools=>Computer Management=>Storage=>Disk Management

לבחור את התקן ה-USB שלכם שמזוהה ככונן מקומי. כפתור ימני ואז-"Delete Volume", לאחר כמה שניות תראו שכל הזיכרון בהתקן נמצא כ-"Unallocate". זה הזמן לפרמט את הכונן כ-FAT32.

לחצו על הכפתור הימני וביחרו ב-"Format" המערכת BackTrack לא זקוקה ליותר מ-2GB, ואין סיבה להשתמש ביותר, פרמטו 2GB מההתקן כ-FAT32 ואת השאר תשאירו כ-"Unallocate".



לאחר התהליך הנ"ל יש לכם ביד התקן USB מפורמט עם מערכת קבצים מסוג- 32FAT בגודל של 2GB.

התקנת המערכת:

מה שנשאר לנו בכדי להתקין את המערכת הוא להוריד את קובץ התמונה שלה (ISO), ואת התוכנה שתפרוס לנו אותו על מחיצת ה-FAT32 שלנו ותהפוך אותו ל-Bootable.

קבצי ISO (ראשי תיבות של: International Standarts Format) הוא קובץ "Image", קובצי Image או קבצי תמונה של דיסק. הם מכילים את התוכניות ואת ה-DATA בדיוק כמו שהוא נראה על הדיסק, אופן שמירתם ותצורת התיקיות. (ישנם עוד סוגים של קבצי תמונה כגון-BIN, ISO, CIF, NRG)

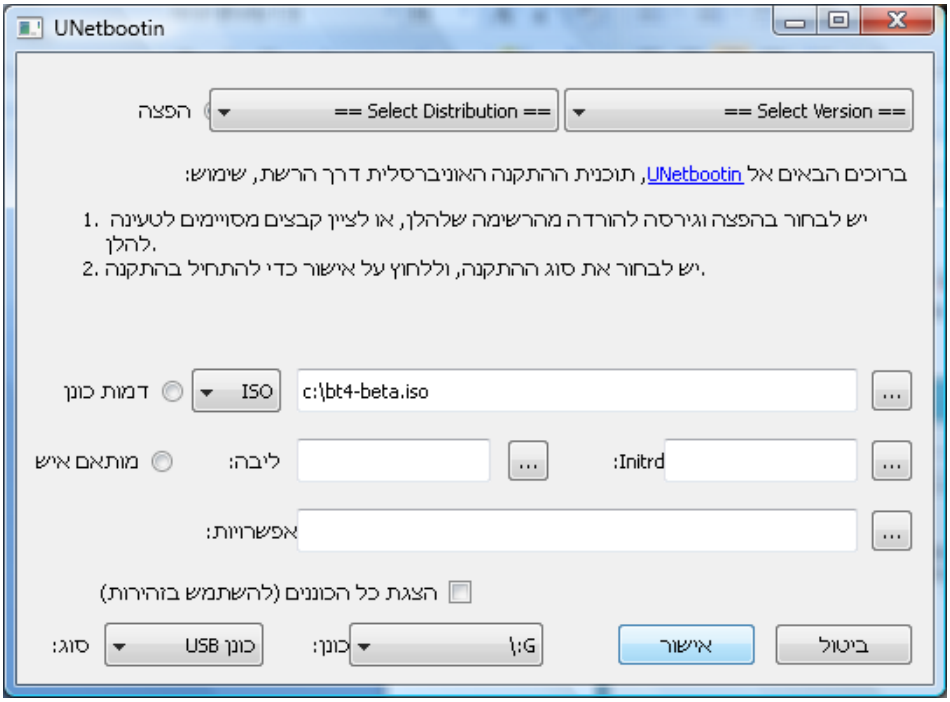
את קובץ ה-ISO המכיל את הגיסרא האחרונה של Back|Track תוכלו להוריד מכאן:

http://www.remote-exploit.org/cgi-bin/fileget?version=bt4-prefinal-iso

ואת UNetbootin, תורידו מכאן:

http://unetbootin.sourceforge.net/

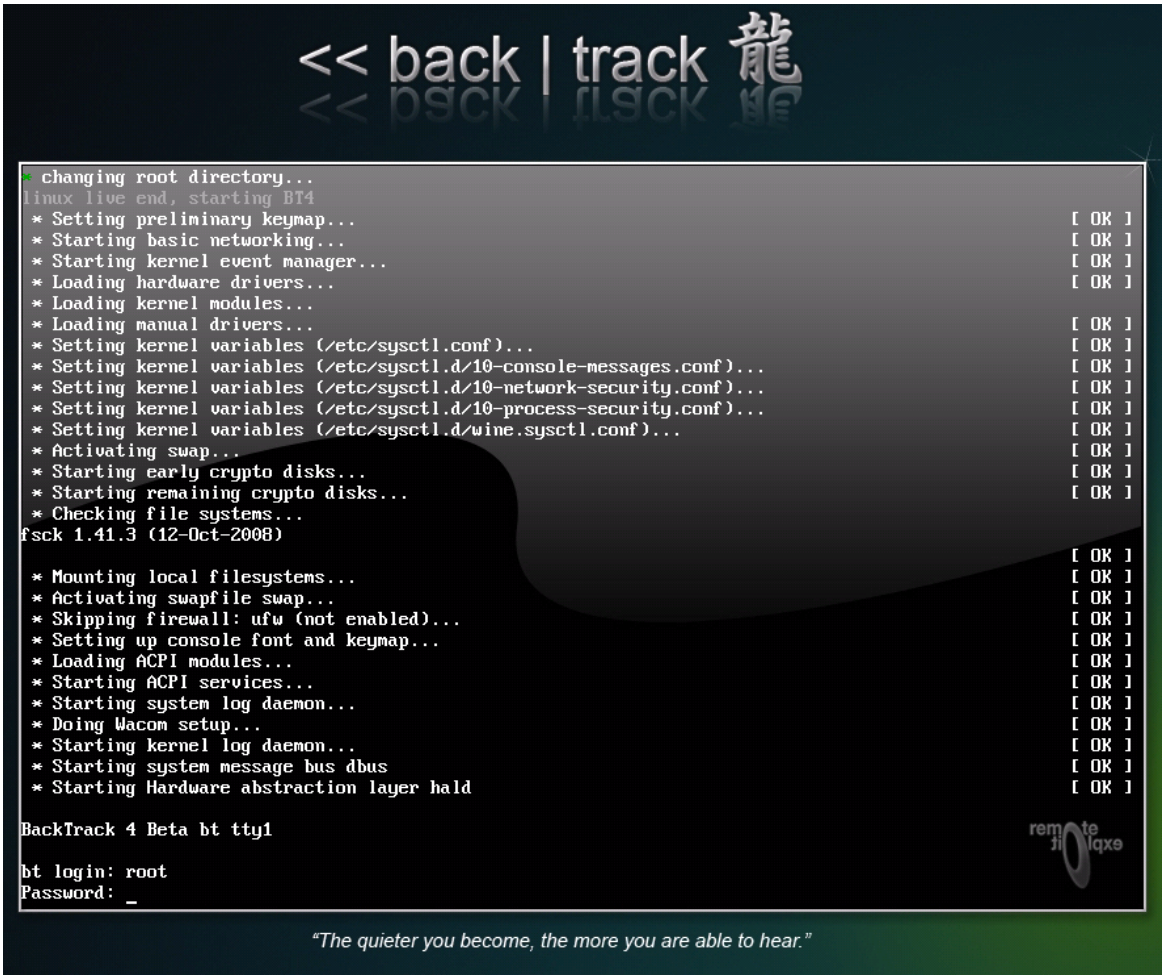
לאחר שהורדתם את שני הקבצים, פיתחו את UNetbootin וביחרו באפשרות של לבצע את הפעולה דרך קובץ ISO (וכמובן ביחרו את קובץ ה-ISO שזה הרגע סיימתם להוריד). ביחרו את התקן ה-USB שפירמטתם קודם לכן ואשרו את הפעולה:



לאחר אישור ביצוע הפעולה, התוכנה תפרוס את קובץ ה-ISO על התקן ה-USB שלכם, תדאג לאתר ולדאוג לכל מה שצריך לעדכן ב-syslinux.cfg.

אם עשיתם הכל נכון, לאחר סיום ביצוע הפעולה הנ"ל, יש לכם ביד התקן USB שעליו מותקנת מערכת Back|Track4 Pre-Released והוא מוגדר כ-Bootable. זאת אומרת שאם תכניסו את ההתקן הנ"ל לאחת מיציאות ה-USB במחשבכם ותדליקו אותו- המחשב יטען את המערכת (אם לא, תכנסו להגדרות הביוס שלכם ותדאגו שהמחשב ינסה לבצע דבר ראשון Boot מהתקן ה-USB ורק לאחר מכן מהרד-דיסק או מהרשת.

כשתפעילו את המערכת יעלו לפניכם ארבעה אפשרויות, ביחרו בראשונה, לאחר שהמערכת תטען את כל ה-Live Scripts ותסיים לזהות את כל החומרה שיש לכם במחשב היא תציג בפניכם את ממשק הקונסול, הוא יבקש ממכם שם משתמש וסיסמה, שם המשתמש בברירת המחדל הוא: root, וסיסמתו היא: toor.



אחרי שתכניסו אותם תוכלו להתחיל להשתמש במערכת הפעלה. בכדי לטעון את הממשק הגראפי KDE (הפצת ה-Back|Track מגיעה עם ממשק KDE וממשק FVWM עם Crystal) יש לכתוב את הפקודה:

```
startx
```

כדי לטעון את FVWM, יש לכתוב את הפקודה:

```
bt-crystal
```

שמירת השינויים במערכת (Persistent Changes)

הצלחנו ליצור התקן USB שממנו אנחנו יכולים להריץ על כל מחשב את Back|Track, אבל מה, נסו ליצור קובץ על שולחן העבודה ותגלו שלאחר שתסגרו את המערכת ותפעילו אותה מחדש- הקובץ יעלם. למען האמת, בכל פעם שתריצו את המערכת מחדש- היא תרוץ כאילו היא רצה בפעם הראשונה, ולא משנה כמה שינויים עשיתם בה. הדבר מעצבן מאוד ואף מציק ביותר, לדוגמא- בכל פעם שנפעיל את המערכת מחדש- נאלץ לעדכן את כל הכלים בהם אנו נרצה להשתמש. לא נוכל לשמור קונפיגורציות של כלים או מידע על סריקות קודמות שעשינו.

אז איך בכל זאת נוכל להתגבר על הצרה הזאת? ממשיכים לקרוא...

בתחילת המאמר אמרתי לכם שניצור שני מחיצות על התקן ה-USB שלנו, עד כה יצרנו רק מחיצה אחת- למערכת ההפעלה, עכשיו ניצור מחיצה שעליה נאכסן את כל המידע ה"דינאמי" שלנו. מדובר במספר פעולות די פשוטות שיקלו עלינו באופן נרחב ביותר.

הכניסו את התקן ה-USB והפעילו את הלינוקס שלכם- לא מדובר בלהפעיל את המערכת שהרגע התקנו מהכונן ה-USB, מדובר במערכת נפרדת- בכדי שנוכל לבצע שינויים בכונן ה-USB שלנו. אני מעלה את ה-Ubuntu שלי, מכניס את התקן ה-USB, ההפצה לבד מזהה את ההתקן ומצמידה לו Mount Point ("Mount Point" זאת "נקודת עגינה" - מעין הלינק לאותו התקן כדי שהמערכת תדע לזאת אותו), אני ניגש לתיקיה Media (אצלכם יש מצב שתמצאו אותו ב-mnt זה תלוי בהפצה שלכם), רואה את הנקודת עגינה- אצלי היא "/Media/NEW VOLUME", איך אני יכול לזהות אותה? פשוט מאוד- אנחנו יודעים איזה קבצים אמורים להיות על ההתקן- ואם הם נמצאים שם- אנחנו יכולים להיות בטוחים שזאת הנקודת עגינה שלנו. אחרי שזיהנו את נקודת העגינה אנחנו צריכים לנתק אותה- לעשות לה "Un-Mount" (למה? בכדי שנוכל לכתוב עליה מחיצה נוספת- לא נוכל לעשות את זה בזמן שהיא במצב "Mount"), פשוט מאוד- כפתור שמאלי ולבחור ב-"Unmount Volume".

אפשר גם לעשות את זה דרך הקונסול למי שרוצה, בעזרת הפקודה הבאה:

```
sudo umount -f [Mount-Point]
```

אצלי נקודת העגינה היא למשל /Media/NEW VOLUME אז אני אכתוב את הפקודה כך:

```
sudo umount -f /media/NEW\ VOLUME
```

כמובן שהמערכת תבקש את סיסמת האדמין.

לאחר שביטלנו את העגינה של ההתקן (אך לא ניתקנו אותו פיזית מהמחשב), כיתבו בקונסול את הפקודה הבאה:

```
fdisk /dev/sdb
```

כדי להפעיל את תוכנת ה-Fdisk ליצירת המחיצה החדשה, הקישו "p" ותקבלו את רשימת המחיצות שקיימות לכם על ההתקן- נכון לעכשיו אתם אמורים לראות שורה בסיגנון הבא:

```
Device        Boot     Start     End    Blocks      Id    System
```

ומתחתיה אמור להופיע לכם רק שורה אחת (יש לנו רק מחיצה אחת על הכונן):

```
/dev/sdb1     *         4         7155   2048000     c      W95   FAT32
```

לאחר מכן, לחצו על "n" בכדי ליצור מחיצה חדשה, התוכנה תשאל אתכם איך להתייחס למחיצה, תקישו "p" כדי לבחור "Primary Partition", ולבסוף תקישו "2" כדי לקבוע אותה כמחיצה השניה.

עכשיו התוכנה תבקש ממנו לקבוע את **גודלה** של המחיצה- אנחנו רוצים ששאר הכונן יהיה המחיצה שלנו, ולכן נלחץ אנטר פעמיים. (פעם ראשונה בכדי לקבוע מיקום ראשון פנוי לנקודת ההתחלה של המחיצה ופעם שניה בכדי לקבוע את המיקום האחרון האפשרי לנקודת סוף המחיצה).

אחרי שקבענו את הגודל- אנחנו רוצים לקבוע את **סוג** המחיצה, לכן נלחץ על p, ואז נלחץ על המספר 2 (בכדי לקבוע את סוגה של המחיצה שכרגע קבענו את גודלה), לאחר מכן נתבקש לקבוע את סוג המחיצה, אנו קובעים זאת ע"י סימון סוג המחיצה כמספר הקסדצימאלי, בכדי לראות את הרשימה של המחיצות והמספרים שמסתמנים אותן נלחץ על L. אנו רוצים לקבוע מחיצת לינוקס רגילה- אצלי המספר הוא "83 - Linux".

אם הכל עד עכשיו טוב, נקבל את השורה הבאה:

```
Changed system type of partition 2 to 83 (Linux)
```

נלחץ שוב p בכדי להגיע לתפריט שמראה לנו את מצב המחיצות על ההתקן- שימו לב שנוספה לנו מחיצה בשם sdb2 (במקרה שלי), אם הכל תואם למה שרצינו- נלחץ על w בכדי לכתוב את ההגדרות על ההתקן.

לאחר מכן מה שנותר לנו הוא לפרמט את המחיצה לסוג ext2, נבצע זאת ע"י שימוש בכלי mkfs שמאפשר לנו ליצור מחיצות ext2 ו-ext3, נשתמש בו כך:

```
mkfs.ext2 /dev/sdb2
```

אם הכל עבר חלק- סיימנו לקבוע את "התשתית" של המערכת שלנו, יש לנו כונן עם מערכת הפעלה שאפשר לבצע ממנו Boot ועוד כונן ext2 שבו אנו נשמור את השינויים שאנחנו נבצע, מה שנותר לנו לבצע הוא לשנות את הקונפיגורציה הנכונה במערכת בכדי שתדע איפה לשמור מה וסיימנו!

תפעילו מחדש את המחשב (Restart) וכנסו שוב למערכת עם הסיסמה והכל. כנסו לתיקיה:

```
/mnt
```

ושם תראו את שתי המחיצות שיצרנו, על אחת מהן יושבת מערכת ההפעלה שלנו, ועל השני ישבו השינויים שנבצע, כנסו למחיצה sdb2 וצרו בה את התיקיה שתכיל את השינויים, קראו לה:

```
changes
```

לאחר מכן כנסו למחיצה בה יושבת מערכת ההפעלה שלנו, כנסו לתיקית BOOT, ושם כנסו לתיקיה syslinux, בתוכו כנסו לקובץ "syslinux.cfg" , זהו הקובץ שממנו המערכת טוענת את אפשרויות והגדרות מסך ה-Boot של מערכת ההפעלה שלנו, חפשו את ה-Label של האפשרות שבה אתם משתמשים (אני משתמש לרב ב-Console) ותחתיה, חפשו את השורה של ה-APPEND.

אצלי השורה נראת כך:

```
APPEND vga=0x317 initrd=/boot/initrd.gz ramdisk_size=6666
```

עלינו להוסיף את המתג "changes" ולקבוע אותו למחיצה שיצרנו באופן הבא:

```
changes=/dev/sdb2
```

השורה המקורית תראה עכשיו כך:

```
APPEND vga=0x317 changes=/dev/sdb2 initrd=/boot/initrd.gz
ramdisk_size=6666
```

שימרו את הקובץ.

(ישנה עוד אפשרות שבמקום לשנות את השורה המקורית- תוכלו להעתיק את כל הבלוק וליצור אפשרות כניסה חדשה למערכת ואליה להוסיף את האפשרות שהמערכת תשמור את השינויים וכך לאפשר לעצמכם בעתיד לקבוע האם תירצו לשמור שינויים או לא- רק לא לשכוח לשנות את ה-Title.)

סיכום

מאוד מומלץ לעבור על סט הכלים הכלול במערכת וללמוד עליהם. המערכת מציעה מגוון רחב יחסית של כלים לביצוע מספר רב של פעולות. למי שלא התעסק עם לינוקס בחייו השימוש במערכת לא יהיה חלק ולכן מומלץ להכיר את הסביבה לפני-כן.

בנוסף, נכון לכתיבת שורות אלו עוד לא יצאה גירסת ה-Stable של הגרסא הרביעית, אבל שווה לחכות ולהתעדכן בפורומים של Remote-Exploit.