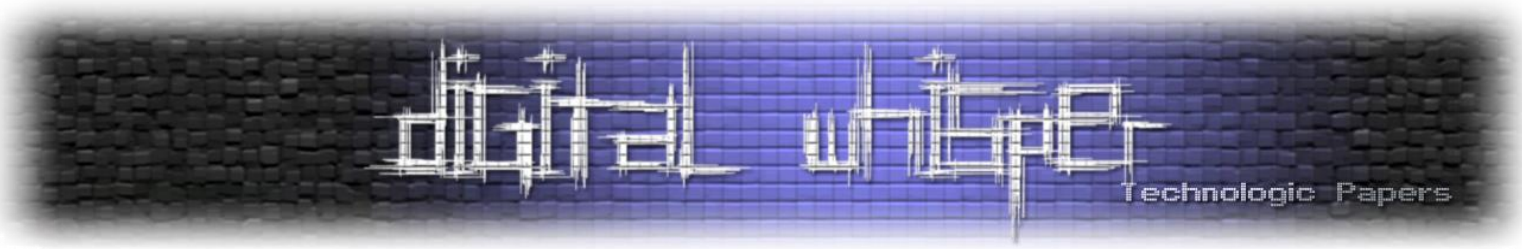


הקשחת מערכות Linux - יסודות

מאת מאור ניסן

ב-Linux זה לא היה קורה. האמנם?

ובכן, בהשוואה למערכות הפעלה אחרות, אין כל ספק כי Linux הינה מערכת הפעלה מאובטחת יותר יחסית ל-Windows, למשל. כידוע או לא, לב ליבה של ה-Linux מורכב מהגרעין (קרנל - Kernel) ואוסף כלים שמרכיבים בעצם את מערכת ההפעלה - ביחד הם מרכיבים את ה"משטח" עליו רצים תוכנות וכלים. קרנל המערכת מבוסס קוד-פתוח (כמו גם רוב כלי אבטחת המידע הקיימים כיום), מה שמאפשר לחבר'ה כמוני וכמוך לזהות חולשות, להתריע ולתקן. בנוסף, מספר גדול וגדל של תוספי אבטחה ("פיצ'רים") מוטמעים בקרנל ושינויים חיוניים בקוד הקרנל מתבצעים מדי יום. Linux מעניקה יכולת מרשימה על בקרת הגישות (מי "שולט" על מי, אילו משאבים משתמש יכול לגשת ועוד). אז, איפה הסיכונים פה?

כמו שספרה של ג'ניפר טרייג מצהיר: "השטן נמצא בפרטים הקטנים" - כאן התשובה. אבטחת המערכת תלויה באופן רוחבי בתצורת (הגדרות) אלמנטים ברובד המערכתי והאפליקטיבי. Linux והקרנל הינם רכיבים מורכבים מאוד ולעתים קרובות - קשה להגדירם באופן "ידני". אבטחת מידע ב-Linux לעולם לא סטטית. ככל שתשתמשו במערכת - כך רמת אבטחתו תרד; שינוי תפעול של פונקציות מסוימות עלול לחשוף את המערכת לאיומים מצד חולשות חדשות המתגלות מדי יום כנגד תוכנות ושירותי מערכת. אם זה לא מספיק - המון הפצות (Distribution) מגיעות עם תוכנות ותצורות מוגדרות מראש התלויות בידע של המפיץ ובמטרת ההפצה (יש הפצות שמכוונות למשתמשים ביתיים, למנהלי מערכת, חוקרי פשעי מחשב ועוד...).

התקנת הפצת המערכת

אם באבטחת מידע עסקינן, התקנת מערכת Linux (הפצה מסוימת) בברירת מחדלה - הינה צעד לא חכם במיוחד; תוכנות רבות ולעתים לא מתאימות - מותקנות, משתמשים לא נחוצים - נוצרים, ואם לא די בכך - החלטות תצורה שגויות מתקבלות.

החלטות תצורה

כמעט בכל מהלך התקנה של הפצת Linux כזו או אחרת - תישאלו לגבי תצורת המערכת. בד"כ אלו שאלות חיוניות וחשובות לגבי אבטחת המערכת שלכם.

להלן כמה מהמלצותיי:

- אם תישאלו להזין סיסמה למשתמש root - תמיד תבחרו בסיסמה חזקה.
- צרו משתמש בנוסף למשתמש root - והזינו סיסמה שתהיה לכל הפחות - סבירה.
- אם תישאלו במהלך ההתקנה על התקנת חומת אש ואפשרות ל-SELinux - אשרו והתקינו.
- למרות שכיום זהו ברירת מחדל - לאפשר הצפנת סיסמאות (MD5) ו-Shadowing.

מינימליזם כדרך חיים

התקינו רק מה שאתם צריכים. אם הפצה מסוימת מציעה אפשרות להתקנה מינימלית או מוגדרת אישית - בחרו באחת האפשרויות הנ"ל. כאמור, ככל שמותקנות תוכנות (או packages ליתר דיוק), כך סביר שהמערכת תהיה חשופה לחולשות. אם כך וברצונכם להבטיח התקנת מערכת מאובטחת באופן מרבי ביותר, אני ממליץ להסיר את ה-packages הבאים:

- משחקים.
- שרתים (או שירותי רשת).
- דימונים (daemons) ושירותים נוספים.
- תוכנות וכלים סטייל "אופיס".
- כלים ותוכנות להדפסה.
- בסיסי נתונים.
- X-Windows (שרת ממשק גרפי) וסוגיו (Gnome/KDE).

מערכת Linux פרודוקטיבית אינה צריכה להכיל ממשק גרפי. X-Windows הינה חבילה ענקית המכילה מספר גדול של רכיבים ולהם היסטוריה של חולשות שהתגלו. בשונה מ-Windows, כל הגדרה במערכת יכולה להיעשות דרך ממשק שורת פקודה (command line).

הקפידו להתקין את הגרסה העדכנית ביותר של אותה הפצה, אם התקבל לידיכם גרסה ישנה - אין להתחבר לאינטרנט עד שמתקינים את כל ה-patches וה-fixes הקיימים עת ההתקנה. תקראו לי פרנואיד, אבל באבטחת מידע כמו באבטחת מידע - התזמון הוא פקטור קריטי; אם התקנתם מערכת ישנה, קיים פער של זמן עד השלמת התקנת כל העדכונים וה-patches החיוניים. בזמן זה, עת אתם מחוברים לאינטרנט והמערכת לא מעודכנת - מספיק כי תוקף "יתפוס" אתכם בעת סריקתו כדי לנצל חולשות ידועות.

בנוסף, עת סיום הורדת ההפצה, יש להבטיח את שלמותה; השוואת חתימת ה-MD5 תבטיח כי הקובץ שירד לא שונה, והוא זה שבאמת התכוונו להוריד. אמחיש בקצרה: נניח כי ברצוננו להוריד את קובץ ההתקנה של הפצת Debian, תחילה, אוודה כי אני מוריד את הגרסה העדכנית ביותר המתאימה לארכיטקטורת המעבד שלי ולנפח זיכרון ה-RAM במחשבי (64 ביט לזיכרון בנפח 4GB ומעלה). מאתר ההפצה של Debian, אגיע לכתובת הבאה:

http://cdimage.debian.org/debian-cd/current/amd64/iso-cd

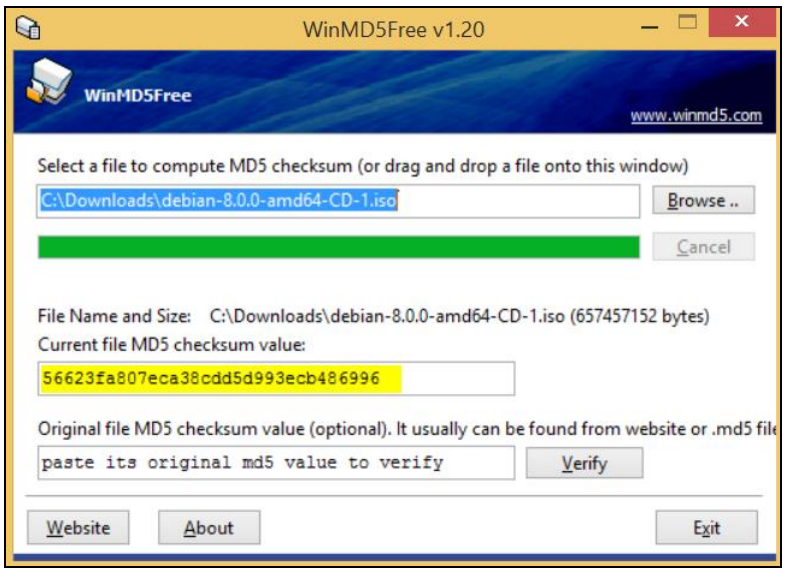
See the Debian CD FAQ for lots more information about Debian CDs and installation.

Name	Last modified	Size
Parent Directory		-
MD5SUMS	2015-04-26 01:38	5.5K
MD5SUMS.sign	2015-04-26 01:43	836
SHA1SUMS	2015-04-26 01:38	6.2K
SHA1SUMS.sign	2015-04-26 01:43	836
SHA256SUMS	2015-04-26 01:38	8.3K
SHA256SUMS.sign	2015-04-26 01:43	836
SHA512SUMS	2015-04-26 01:38	14K
SHA512SUMS.sign	2015-04-26 01:43	836
debian-8.0.0-amd64-CD-1.iso	2015-04-25 16:03	627M
debian-8.0.0-amd64-CD-2.iso	2015-04-25 16:03	645M
debian-8.0.0-amd64-CD-3.iso	2015-04-25 16:03	644M
debian-8.0.0-amd64-CD-4.iso	2015-04-25 16:03	645M
debian-8.0.0-amd64-CD-5.iso	2015-04-25 16:03	634M
debian-8.0.0-amd64-CD-6.iso	2015-04-25 16:03	638M
debian-8.0.0-amd64-CD-7.iso	2015-04-25 16:03	646M
debian-8.0.0-amd64-CD-8.iso	2015-04-25 16:03	635M
debian-8.0.0-amd64-kde-CD-1.iso	2015-04-25 14:55	628M
debian-8.0.0-amd64-lxde-CD-1.iso	2015-04-25 14:56	641M
debian-8.0.0-amd64-netinst.iso	2015-04-25 14:53	246M
debian-8.0.0-amd64-xfce-CD-1.iso	2015-04-25 14:55	636M

Apache/2.4.12 (Unix) Server at cdimage.debian.org Port 80

לאחר הורדת הקובץ, אכנס ל-MD5SUMS ואבדוק (בעזרת תוכנה כגון WinMD5) או פקודת md5sum בלינוקס אם החתימה של הקובץ תואמת לזו המוצגת ב-MD5SUMS:

```
56623fa807eca38cdd5d993ecb486996  debian-8.0.0-amd64-CD-1.iso
7deb1d91e11a6681bda866595f76f78a  debian-8.0.0-amd64-CD-10.iso
438a231a907f9443b41bdfdc4a667e43  debian-8.0.0-amd64-CD-11.iso
459014f07a38b63d0bfcce5ad25f9458  debian-8.0.0-amd64-CD-12.iso
0cb4b93bcdb1fcd769cacf0d47c117b5  debian-8.0.0-amd64-CD-13.iso
64b8822d2905a4ec72984e6623d22c78  debian-8.0.0-amd64-CD-14.iso
b51d6d445a08d1f6d267b150f5fc9b77  debian-8.0.0-amd64-CD-15.iso
54cc72182556d206efc9168d7c6550ea  debian-8.0.0-amd64-CD-16.iso
3213d804762a9b8b6d55b1ce9c060b54  debian-8.0.0-amd64-CD-17.iso
85fcde6e60cb29b4b13c1d94401a266e  debian-8.0.0-amd64-CD-18.iso
5f1beb8ed52fc60b274d19b1591ec3d1  debian-8.0.0-amd64-CD-19.iso
c159804d081f1dab44cd25ddc91ef9bf  debian-8.0.0-amd64-CD-2.iso
```



אבטחת ה-Boot Loaders

תוקף הנגיש פיזית למערכת שלכם יכול בקלות לעקוף את מנגנוני האבטחה הפנימיים של המערכת (במיוחד בבקרות כניסה של שם משתמש וסיסמא). בנוסף, הוא יכול לבצע אתחול (אם אין הגנה על ה-BIOS) או לשנות את תצורת האתחול של המערכת ואת תהליך ה-init (המגדיר אילו שירותים, פקודות וכלים ירוצו בעת האתחול). תוקפים המסוגלים לאתחל את המערכת יוצרים שתי בעיות גדולות: האחת היא האפשרויות הרבות שמערכת Linux מעניקה לאלו המסוגלים לאתחל אותה. השנייה היא מניעת שירות ע"י אתחול לא רצוי.

רוב הפצות ה-Linux עושות שימוש באחד משני ה-Boot loaders: ה-LILO (Linux loader), פעם היה loader ברירת המחדל של Linux) ו-Grub (החליף את ה-LILO וכיום הוא ברירת המחדל ברוב הפצות ה-Linux). Boot Loaders נטענים אחרי פעולת ה-BIOS של המחשב ומעניקים שליטה על בחירת הקרנל הרצוי ובקרה על ה-Boot images. בעת עדכון קרנל, ה-Boot loader יציג את כל גרסאות הקרנל שהותקנו - כולל אלו שאינם מעודכנים. בכללי, מומלץ שלא יהיו הרבה גרסאות קרנל מותקנות - במיוחד לא גרסאות ישנות. לכן, מומלץ להסיר את אותן גרסאות מרשימת הקרנלים ב-Boot loader.

Grub מכילה פיצ'רים רבים יותר מ-LILO, מעודכנת יותר ולכן גם מאובטחת יותר. למרות זאת, ברירת המחדל של Grub היא לאפשר לכולם לאתחל את המערכת במצב Single-user mode או לשנות פרמטרי אתחול שונים. בשונה מ-LILO, Grub יכולה להתמודד עם אירועים מסוג זה ע"י בקרת גישה מבוססת סיסמה (מוצפנת SHA512).

הגנת Grub ע"י סיסמה

הזינו את הפקודה הבאה:

```
grub-mkpasswd-pbkdf2
```

הזינו סיסמא והעתיקו את הפלט המוצפן.

ערכו את הקובץ:

```
/etc/grub.d/40_custom
```

וצרו שתי שורות:

```
Setsuperuser="someUser" set password someUser PASSWORD COPIED
```

שירותי אתחול, Init וסדר האתחול

אציג בטבלה את שירותי האתחול במערכת (מתאימה ברובה ל-Debian אך גם רוב הפצות ה-Linux עושות שימוש בשירותים דומים)

שם השירות	תיאור	מומלץ להסיר?
acpid	יישום תקן ACPI להגדרת התקנים וניהול צריכת חשמל	לא
anacron	בדומה ל-cron, רק שההנחה היא כי המחשב לא פועל באופן רצוף - כלומר, משמש מחשבים שלא פועלים 24 שעות ביום ומעניק יכולת בקרה לביצוע משימות הנשלטות ע"י cron בתדירות יומית, שבועית או חודשית.	כן - במחשבים שאינם שרתים.
apmd	דור קודם של יישום ACPI ומותקן בד"כ במחשבים ישנים. אם הותקן acpid - מומלץ להסירו.	כן
auditd	The Linux Audit daemon. אחראי לכתיבת רשומות ביקורת (או הערכה) של המערכת.	לא להסיר. מומלץ להגדירו.
atd		כן
autofs	Automount	כן
crond	שירות cron	לא
cups	פונקציות מדפסת	כן
functions	פונקציות לסקריפטים מבוססי shell-script	לא
gpm	תמיכת עכבר ליישומי טקסט	כן

irda	תמיכה ל-IrDA	כן
isdn	תמיכה ל-ISDN	כן
keytable	מיפוי מקלדת	לא
kudzu	זיהוי חומרה	כן
lpd	שירות lpd למדפסות	כן
netfs	Mount network file systems	כן
nfslock	נעילת שירותי ה-NFS	כן
ntpd	שירות שעון מבוסס רשת	לא
pcmcia	תמיכה ל-PCMCIA	כן
portmap	תמיכה לחיבורי RPC	כן
random	לכידת אירועים אקראיים	לא
rawdevices	הקצאת התקנים	כן
rhnsd	שירות הרשת של Red hat	כן
snmpd	שירות SNMP	כן
sshd	שירות SSH	לא
winbind	תמיכה ל-Samba	כן
xfs	X font server	כן
ypbind	NIS/YP client support	כן

מסך התחברות (Login Screen)

מסך ההתחברות הינו הדבר הראשון שמשתמשי המערכת (או התוקפים) רואים עת הם מתחברים למערכת. כחלק ממדיניות אבטחת המידע שלכם, יש להציג למשתמשים מספר אזהרות והנחיות לפני התחברותם. דוגמה לכך תהיה:

- אזהרה בדבר חיבור לא מורשה למערכת.
- כחלק מעקרון "אבטחה באמצעות עמימות" (Security Through Obscurity), יש להבטיח כי גרסת מערכת ההפעלה תוסתר, סוג הפצת המערכת וכמו כן גם גרסת הקרנל. בברירת המחדל, רוב מערכות ההפעלה יציגו את הנ"ל. חשוב מאוד לתקן זאת.
- יש לוודא כי מסך ההתחברות יהיה "נקי" ויאפס טקסטים ופקודות שנכתבו לפני יציאה מהמערכת.

איך נעשה את זה? יש לערוך את הקובץ:

```
/etc/issue.net
```

ואת:

```
/etc/issue
```

הקבצים הנ"ל יוצגו בעת התחברות המשתמש לטרמינל. תחילה, יש לוודא כי מסך ההתחברות יהיה נקי. הזנת פקודת clear אל תוך קובץ ה-/etc/issue ו-/etc/issue.net - תעשה את העבודה:

```
root@maor-debian:/home/maor# clear > /etc/issue
root@maor-debian:/home/maor# clear > /etc/issue.net
```

כעת, נוסיף הודעת אזהרה לפני ההתחברות. כאמור, הטקסט מוזן לקובצי ה-issue. דוגמה להודעה:

```
**************************************************************************
* This system is for the use of authorized users only. Usage of          *
* this system may be monitored and recorded by system personnel          *
* Anyone using this system expressly consents to such monitoring         *
* and is advised that if such monitoring reveals possible                *
* evidence of criminal activity, system personnel may provide the        *
* evidence from such monitoring to law enforcement officials.            *
**************************************************************************
```

לאחר אימות המשתמש והתחברות למערכת, יוצג ה-/etc/motd (Message Of The Day) . גם הוא קובץ טקסט המאפשר להציג אזהרות, נהלים והנחיות למשתמשים שהתחברו בהצלחה למערכת.

ננעל את הקבצים הנ"ל כך שלא יהיו ניתנים לשינוי:

```
root@maor-debian:/# chown root:root /etc/issue.net /etc/issue /etc/motd
root@maor-debian:/# chmod 0600 /etc/issue.net /etc/issue /etc/motd
```

משתמשים וקבוצות

נדבך עיקרי באבטחת מערכות הינו אבטחה של נתוני התחברות (קרי שמות משתמש וסיסמאות). מטרתנו כמובן, היא להבטיח כי רק משתמשים מורשים יהיו מסוגלים להתחבר למערכת וכן למנוע מהתוקף גילוי (וניחוש) סיסמאות חלשות.

לינוקס שומרת נתונים אודות משתמשים וקבוצות ב-3 קבצים:

```
/etc/passwd
/etc/shadow
/etc/group
```

/etc/passwd מכיל רשימה של כל משתמשי המערכת ומאפיינם, לדוגמא:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

מבנה רשומה בנוי כדלקמן:

```
username:password:UID:GID:comments:Home Directory:Shell
```

הקשחת שירות ה-SSH

כעת, נקשיח את שרת ה-SSH הנפוץ במערכות linux. תחילה, "נכריח" את השרת להקשיב לכתובת ספציפית אחת ולא לכל הכתובות (שכנראה) מוגדרות במערכת. כמובן, נחסום גישת root ישירה כיוון שאנו רוצים שכל משתמש יתחבר דרך חשבונו בלבד (ואם הם צריכים גישת root לפעולות מסוימות - נגדיר su עבורם.

בנוסף, נבטל את האפשרות לאימות ע"י סיסמה - כלומר, הדרך היחידה להתחבר לשרת תהיה ע"פ האימות התקני של פרוטוקול ה-SSH (הווה אומר - מפתחות ציבוריים). לפרנואידים ממש - נשנה גם את פורט הגישה לפרוטוקול.

שינוי הגדרות שרת ה-SSH מתבצע ע"י עריכת קובץ ההגדרה: /etc/ssh/sshd_config:

```
# Package generated configuration file
# See the sshd(8) manpage for details
# What ports, IPs and protocols we listen for
Port 2289 #שינוי הפורט

# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress::
#ListenAddress 0.0.0.0
ListenAddress 192.168.2.10 #הגדרת כתובת ספציפית אחת
Protocol 2
```

```
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key #הגדרת מפתחות ציבוריים של קליינטים
HostKey /etc/ssh/ssh_host_dsa_key

#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
#PermitRootLogin yes
PermitRootLogin no #ביטול התחברות ישירה של חשבון מנהל
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes

# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no

# Uncomment if you don't trust ~/.ssh/known_hosts for
RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes
PasswordAuthentication no
# Kerberos options
```

```
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

# Deactivate port forwarding
AllowTcpForwarding no
#X11Forwarding yes
X11Forwarding no
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
#MaxStartups 10:30:60
#Banner /etc/issue.net
Banner /etc/issue

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
UsePAM yes
```

הגדרת sudo

sudo הינו יישום המעניק גמישות בבקרת הגישה המצויה במערכות לינוקס. היישום "מחליף" את מודל ה-root or nothing ומעניקה למנהל המערכת אפשרות להקצות הרשאת root לפקודות מסוימות במערכת ללא הצורך בסיסמת ה-root. קובץ ההגדרות של sudo נמצא ב-/etc/sudoers אבל עריכתו חייבת להיעשות באמצעות פקודת ה-visudo.

<u>גישה מלאה</u>

הפעולה הבאה מעניקה הרשאה מלאה - קרי root למשתמש maor, לכן שימו לב למי אתם מעניקים גישה שכזו.

```
root@maor-debian# visudo
# /etc/sudoers
# User privilege specification
root ALL=(ALL) ALL
maor ALL=(ALL) PASSWD: ALL #זו השורה שהוספנו
```

גישה לפקודה מסוימת

נניח כי המשתמש yosi צריך הרשאה ע"מ להריץ את tcpdump. בואו ניתן לו גישה:

```
root@maor-debian# visudo
# /etc/sudoers
# User privilege specification
root ALL=(ALL) ALL
yosi ALL=(ALL) PASSWD: /usr/sbin/tcpdump -ni eth0 #זו השורה שהוספנו
```

ביטול אתחול המערכת באמצעות צירוף המקשים CTRL+ALT+DEL

מערכות לינוקס רבות "מקבלות" אות (syscall) לאתחול המערכת עת צירוף המקשים Ctrl+Alt+Del - כן, כמו במערכות MS-DOS. כדי למנוע הפתעות לא נעימות, בואו נחסום אפשרות זו. תחילה, יש לערוך את etc/inittab/ ולשנות את השורות הבאות:

```
#What to do when CTRL-ALT-DEL is pressed.
#ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
                                                    #נוסיף את השורה הבאה במקום זאת שמעל
ca:12345:ctrlaltdel:/usr/bin/logger -s -p auth.notice -t [INIT]
"CTRL+ALT+DEL caught but ignored! This is not a Windows(r) machine".
```

ע"מ להחל את ההגדרות, נריץ את הפקודה: init q .

עדכון המערכ(ו)ת באופן אוטומטי

אוקי, נתקלתי בהרבה מנהלי מערכות שביקשו להקל על עבודתם (ועל עומס אחריותם) בהקשר של עדכון חבילות המערכת. ובכן, אני לא ממליץ על עדכון אוטומטי לחלוטין (update + upgrade) מהסיבה הפשוטה שקיימים עדכונים הדורשים קלט ממנהל המערכת. חרף זאת, נוכל לבצע אוטומטיזציה על החלקים המשעממים.

אז ככה: נחליט כי כל בוקר, בשעה 05:30, המערכת תלקט את העדכונים הקיימים (apt-get update) , תבדוק אילו מהם באמת נדרשים למערכת (apt-show-versions -u) - ותשלח אלייך דו"ח לתיבת המייל. מה שנשאר לך - מנהל המערכת לעשות הוא לקרוא את המייל, לברור אילו מהעדכונים נחוצים ולבצע את העדכון (apt-get upgrade) בהתאם למדיניות החברה או הארגון.

תחילה, נוסיף את השורה הבאה (כחשבון root) ל-crontab:

```
root@maor-debian# crontab -e
#### Update the APT database every morning (apt-get update) ####
30 5 * * * apt-get update > /dev/null 2>&1
```

ניצור סקריפט שיתחבר ב-SSH למערכת (שוב, ללא סיסמא אלא ע"י מפתח ציבורי) שיבדוק אילו עדכונים נחוצים למערכת:

```
#!/bin/bash
#
# update_check.sh
#
# Look for servers needing updates. We trust that apt-get update has already
been done.
#
# When              Who          What
# 2015-08-31        Maor         Original version
#
MAORSERVER="maor-debian maor-debian2"
for MAORSERVER in ${MAORSERVER}
do echo ===Available updates for ${MAORSERVER}===
ssh ${MAORSERVER} apt-show-versions -u 2> /dev/null
done
```

ושוב, נוסיף פעולה ל-crontab שתריץ את הסקריפט ותשלח אליך את הדו"ח:

```
#### Checking for available updates ####
0 7 * * * /bin/bash /home/sysop/update_check.sh | /usr/bin/mail -s "Linux
Updates Available on (`/bin/date -R`)" maor@domain.com
```

כיף, נכון?

לסיום, כאמור - מערכות לינוקס הינן מודולריות - הן מורכבות מהרבה יישומים המרכיבים את הפונקציונליות שלה. חשבו על מינימליזם, כמה שפחות שירותים - ככה ייטב. בנוסף, הקפידו לתעד את המערכת. תמיד. הפעולות שהצגתי הן מנדטוריות ובסיסיות למערכות "ריקות", הווה אומר כי לכל שירות (למשל apache) יש פעולות הקשחה נפרדות. אשתדל לכתוב פוסט להקשחה יותר מעמיקה לשירותים נוספים (חשבו defense-in-depth) - אבל עד אז... זכרו כי להבדיל מחלונות, לינוקס רק נותנת לכם את האפשרות ש-"זה לא יקרה".

הנספח לאבטחת מידע

המאמר פורסם במקור כפוסט בבלוג "הנספח לאבטחת מידע" של מאור ניסן, בלוג על אבטחת מידע - מחשבות, היבטים ותיאוריה. ניתן לקרוא את הפוסט הנ"ל ופוסטים נוספים בקישור:

http://blog.isec.co.il/