

Ασφάλεια Συστημάτων Ubuntu 16.04LTS

Δημήτριος Πολίτης
Αθήνα, Ελλάδα

29 Αυγούστου 2016

Περιεχόμενα

1 Εισαγωγή στην Ασφάλεια Η/Υ	2
1.1 Η έννοια της ασφάλειας Η/Υ	2
1.2 Έλεγχοι Ασφαλείας	2
2 Συμβουλές Ασφαλούς Εγκατάστασης ΛΣ Linux	3
2.1 Ρυθμίσεις Bios	3
2.2 Διαμερισμός Δίσκου	3
2.3 Ασφάλιση του Boot Loader	5
2.4 Εφαρμογή Γενικών Ρυθμίσεων Ασφαλείας	6
2.4.1 Διατήρηση του Ελάχιστου ΛΣ	6
2.4.2 Ενεργοποίηση του AppArmor	7
2.4.3 Απεγκατάσταση Διαχειριστών Παραθύρων	7
2.4.4 Απενεργοποίηση Οδηγών και Προσαρτημάτων Πυρήνα	8
2.4.5 Απενεργοποίηση μη Χρησιμοποιούμενων Συστημάτων Αρχείων	8
2.4.6 Απενεργοποίηση εν Δυνάμει Ανασφαλών Δικτυακών Πρωτοκόλλων	8
2.4.7 Έλεγχος αν το Apport είναι Απενεργοποιημένο	9
2.4.8 Απενεργοποίηση Αποτυπωμάτων ΛΣ	9
2.4.9 Απενεργοποίηση Cronjobs για τους Χρήστες	9
2.4.10 Ρύθμιση των Ορίων Ασφαλείας των Χρηστών	10
2.4.11 Αφαίρεση suid από Συγκεκριμένα Αρχεία	10
2.4.12 Εφαρμογή Αυστηρότερων Δικαιωμάτων σε Αρχεία - Φακέλους	10
2.4.13 Καθορισμός DNS Εξυπηρετητών	10
2.4.14 Αφαίρεση Ρυθμίσεων Απομακρυσμένης Πρόσβασης	11
2.4.15 Έλεγχος Πρόσβασης με το TCP Wrappers	11
2.4.16 Ρύθμιση των Banners	11
2.4.17 Αφαίρεση μη Αναγκαιούντων Χρηστών	11
2.4.18 Δημιουργία Νέων Χρηστών με Ανενεργό shell	12
2.4.19 Ασφάλιση του NTP	12
2.4.20 Ρύθμιση του logrotate	12
2.4.21 Απενεργοποίηση του Συνδυασμού Ctrl+Alt+Delete	12
2.5 Ασφάλεια Λογαριασμών	13
2.5.1 Δημιουργία Ασφαλών Κωδικών Χρήστη	13
2.5.2 Επιβολή Ισχυρών Κωδικών ασφαλείας	13
2.5.3 Πολιτική Λήξης Λογαριασμών και Κωδικών	14
2.5.4 Κλείδωμα Λογαριασμών	14
2.5.5 Κλείδωμα Συνεδρίας – Αυτόματη Αποσύνδεση	15
2.5.6 Περιορισμός της Πρόσβασης root	15
2.6 Απειλές για τις Υπηρεσίες	16
2.6.1 Ασφαλής ρύθμιση του NFS	17
2.6.2 Ασφάλιση του Apache HTTP Διαχομιστή	20
2.6.2.1 Ασφάλεια του Apache	21
2.6.2.2 Καθορισμός Ρυθμίσεων	21
2.6.2.3 Απενεργοποίηση Αχρησιμοποίητων Αρθρωμάτων Apache2	23

2.6.2.4	Ενεργοποίηση του Αρθρώματος mod_security	24
2.6.2.5	Ενεργοποίηση του Αρθρώματος mod_evasive	24
2.6.2.6	Συνιστώμενα Πρωτόκολλα Κρυπτογράφησης	25
2.6.2.7	Χρήση του fail2ban	26
2.6.3	Ασφάλιση του SSH	26
2.6.4	Ασφαλής Ρύθμιση του SAMBA	28
2.7	Ασφαλής Ρύθμιση της Δικτυωκής Πρόσβασης	29
2.7.1	Ασφάλεια Διαφόρων Παραμέτρων του Δικτύου	29
2.7.2	Ασφάλιση του DNS με το DNSSEC	32
2.8	Εφαρμογή Επιπλέον Ρυθμίσεων Ασφαλείας	33
2.8.1	Αποστολή Αρχείων Καταγραφής σε ένα Συγκεντρωτικό Σύστημα Καταγραφής Συμβάντων	33
2.8.2	Εγκατάσταση Λογισμικού Προστασίας από Ιούς	33
2.8.3	Εξασφάλιση της Ακεραιότητας των Αρχείων	34
2.8.4	Εγκατάσταση Λογισμικού Ανίχνευσης Rootkit	34
2.8.5	Εγκατάσταση Λογισμικού Intrusion Detection	35
2.8.6	Εποπτεία Συστήματος (System Audit)	35
2.8.6.1	Εγκατάσταση των Πακέτων Audit	36
2.8.6.2	Προρυθμισμένα Αρχεία Κανόνων Audit	36
3	Εργαλεία για Ασφάλιση του Συστήματος	37
3.1	Bastille Linux	37
3.2	Αξιολόγηση του Συστήματος με το SCAP Security Guide	38
4	Bash Script για Εφαρμογή Πολιτικών Ασφαλείας	39
4.1	Αξιολόγηση Συστήματος	40
5	Συμπεράσματα	41
Παραρτήματα		42
Παράρτημα Α' Κώδικας Bash Script		43

Περίληψη

Στο σύγχρονο, συνεχώς μεταλλασσόμενο επαγγελματικό περιβάλλον, οι διαχειριστές συστημάτων αντιμετωπίζουν καθημερινά νέες προκλήσεις, καθώς προσπαθούν να ασφαλίσουν τις υποδομές τους. Το αυτό βρίσκει εφαρμογή με περισσότερη έμφαση στα διασυνδεδεμένα δίκτυα, όπου διακινούνται πολύτιμες πληροφορίες, μεταξύ μεγάλου πλήθους συσκευών. Στο παρόν, γίνεται μια προσπάθεια να σκιαγραφηθούν βασικές διαδικασίες ασφάλισης ενός εξυπηρετητή Linux. Οι παραπάνω οδηγίες αφορούν κυρίως σε λειτουργικό σύστημα Ubuntu 16.04 LTS (Desktop ή Server). Το παρόν πόνημα, καθώς και το bash script, το οποίο το συνοδεύει παρέχονται υπό τους όρους της αδείας GPLv3 και είναι διαθέσιμα στο διαδίκτυο, στην Αγγλική και στην Ελληνική γλώσσα, από την ιστοσελίδα: <https://github.com/dpolitis/Ubuntu-Xenial-Security/>.

1 Εισαγωγή στην Ασφάλεια H/Y

1.1 Η έννοια της ασφάλειας H/Y

Η ασφάλεια H/Y είναι ένας γενικότερος όρος, ο οποίος καλύπτει μια ευρεία περιοχή της επιστήμης των H/Y και της επεξεργασίας της πληροφορίας. Αρκετοί σύμβουλοι ασφαλείας Πληροφορικής, καθώς και εταιρίες του χώρου συμφωνούν στο ρομπόν αποδεκτό μοντέλο ασφαλείας H/Y, γνωστό και ως ΕΑΔ (CIA) **Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα**. Αυτό το τρίπτυχο θεωρείται ως γενικά αποδεκτό για την αξιολόγηση ασφαλείας των Πληροφοριακών Συστημάτων (ΠΣ). Παρακάτω παρατίθεται επεξήγηση του μοντέλου ΕΑΔ, με περισσότερη λεπτομέρεια [1]:

Εμπιστευτικότητα Οι ευαίσθητες πληροφορίες θα πρέπει να είναι διαθέσιμες μόνο σε ένα αυστηρά καθορισμένο σύνολο οντοτήτων. Μη εξουσιοδοτημένη εκπομπή και χρήση της πληροφορίας αυτής, θα πρέπει να περιορίζεται αυστηρά.

Ακεραιότητα Η πληροφορία δε θα πρέπει να αλλοιώνεται με οποιοδήποτε τρόπο, ο οποίος την καθιστά ελλιπή ή εσφαλμένη. Μη εξουσιοδοτημένοι χρήστες δεν θα πρέπει να έχουν τη δυνατότητα να τροποποιούν ή να καταστρέψουν ευαίσθητα δεδομένα.

Διαθεσιμότητα Οι πληροφορίες θα πρέπει να είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που αυτό είναι απαραίτητο.

1.2 Έλεγχοι Ασφαλείας

Η ασφάλεια H/Y χωρίζεται συχνά σε τρεις κύριες διακριτές κατηγορίες ή ελέγχους:

Φυσικούς Ελέγχους Περιλαμβάνει όλα τα μέτρα ασφαλείας που αφορούν τη φυσική προστασία των υποδομών.

Τεχνικούς Ελέγχους Αφορά την εγκατάσταση πολιτικών ασφαλείας στο σύνολο του εξοπλισμού (εξυπηρετητών, κατανεμητών κτλ).

Διαχειριστικούς Ελέγχους Αφορά σε πολιτικές ασφαλείας οργανισμού, έλεγχοι φυσικής πρόσβασης προσωπικού σε υποδομές κτλ.

Στο επόμενο μέρος παρουσιάζεται μια σειρά από ρυθμίσεις ασφαλείας (τεχνικοί έλεγχοι) που μπορούν να εφαρμοστούν σε μια ελαχιστοποιημένη εγκατάσταση Λειτουργικού Συστήματος (ΛΣ) Linux.

2 Συμβουλές Ασφαλούς Εγκατάστασης ΛΣ Linux

Το επόμενο μέρος αφορά στην ασφάλιση μιας τυπικής εγκατάστασης Ubuntu 16.04LTS, τύπου Desktop ή Server. Βασική γνώση της χρήσης της γραμμής εντολών και η ελάχιστη εμπειρία εγκατάστασης ΛΣ Linux θεωρείται απαραίτητη. Η διαδικασία ασφάλισης ακολουθεί μια πορεία bottom-up, ξεκινώντας από τις ρυθμίσεις του BIOS και καταλήγοντας στην εκτεταμένη επιτήρηση (auditd) και αξιολόγηση του συστήματος.

2.1 Ρυθμίσεις Bios

Οι δύο κύριοι λόγοι ασφάλισης του BIOS φαίνονται παρακάτω:

Αποτροπή των αλλαγών στις ρυθμίσεις του BIOS Αν ένας επιτιθέμενος έχει πρόσβαση στο BIOS, μπορεί να αλλάξει τη σειρά εκκίνησης και να ξεκινήσει τον Η/Υ με ένα CD-ROM ή usb αποθηκευτικό μέσο. Αυτό τον καθιστά ικανό να εισέλθει σε rescue mode ή single user mode, το οποίο με τη σειρά του, του επιτρέπει να εκτελέσει αυθαίρετα προγράμματα στο σύστημα ή να υποκλέψει ευαίσθητα δεδομένα.

Αποκλεισμός Εκκίνησης Κάποια BIOS προστατεύουν την διαδικασία εκκίνησης με κωδικό πρόσβασης. Όταν ενεργοποιείται, ο επιτιθέμενος εξαναγκάζεται στην εισαγωγή κωδικού, πριν το BIOS καλέσει το bootloader.

2.2 Διαμερισμός Δίσκου

Είναι μια καλή πρακτική να δημιουργούνται ξεχωριστά διαμερίσματα για τους φακέλους /boot/, /, /home/, /tmp/ και /var/tmp/. Ο λόγος είναι διαφορετικός για το κάθε ένα και εξετάζονται αναλυτικά παρακάτω.

/boot Αυτό είναι το πρώτο διαμέρισμα το οποίο διαβάζει το ΛΣ κατά την εκκίνηση. Ο πυρήνας και ο bootloader οι οποίοι εκκινούν το ΛΣ, αποθηκεύονται σε αυτό το διαμέρισμα. Αυτό το διαμέρισμα λοιπόν δε θα πρέπει να είναι κρυπτογραφημένο, γιατί αν για κάποιο λόγο γίνει μη διαθέσιμο (για παράδειγμα είναι στο ίδιο διαμέρισμα με το κρυπτογραφημένο / και χαθεί το passphrase), τότε το σύστημα δε θα είναι σε θέση να εκκινήσει.

Είναι επίσης καλή πρακτική το /boot να προσαρτάται ως μόνο για ανάγνωση. Αυτό προστατεύει τα κρίσιμα αρχεία του συστήματος από μη εξουσιοδοτημένη τροποποίηση. Για να το επιτύχουμε αυτό τροποποιούμε το αρχείο /etc/fstab

```
~]# vi /etc/fstab
```

ως εξής [8]:

```
/boot      /boot      ext2      defaults,ro      1  2
```

Αξίζει να σημειωθεί, ότι είναι αναγκαία η προσάρτηση του παραπάνω τόμου με δικαιώματα εγγραφής, αν χρειαστεί στο μέλλον να γίνει αναβάθμιση του πυρήνα ή αλλαγή ρυθμίσεων στο bootloader.

/home Σε περίπτωση που τα αρχεία των χρηστών (/home) βρίσκονται στο ίδιο διαμέρισμα με το /, αντί ενός ξεχωριστού τόμου, τότε αυτό μπορεί να γεμίσει με αρχεία και ως αποτέλεσμα να καταστεί το σύστημα ασταθές. Επίσης, κατά την μετάβαση σε νεότερη έκδοση του ΛΣ, είναι ευκολότερο να διατηρηθούν τα δεδομένα στο διαμέρισμα /home, καθώς δε θα διαγραφούν κατά την εγκατάσταση. Επίσης αν ο τόμος / αλλοιωθεί για κάποιο λόγο, τα αρχεία που βρίσκονται σε ξεχωριστό τόμο δε θα χαθούν. Χρησιμοποιώντας διαφορετικούς τόμους για τα δεδομένα, υπάρχει μεγαλύτερη προστασία από απώλεια δεδομένων, ενώ είναι πιο εύκολο να λαμβάνονται από αυτό, προγραμματισμένα αντίγραφα ασφαλείας.

/tmp και /var/tmp Οι φάκελοι /tmp και /var/tmp χρησιμοποιούνται για προσωρινή αποθήκευση δεδομένων. Είναι όμως δυνατό να γεμίσουν σχετικά γρήγορα και να απορροφήσουν όλο το διαθέσιμο χώρο. Αν τυγχάνει οι φάκελοι να βρίσκονται στο ίδιο τόμο με το /, τότε το σύστημα μπορεί να καταστεί ασταθές ή να καταρρεύσει. Για αυτό το λόγο είναι καλή ιδέα να βρίσκονται σε δικό τους διαμέρισμα - τόμο. Επίσης είναι καλή πρακτική η απενεργοποίηση των δικαιωμάτων εκτέλεσης στο /tmp.

/dev/shm Επίσης είναι μια πολύ καλή πρακτική η απενεργοποίηση των δικαιωμάτων εκτέλεσης στη κοινόχρηστη μνήμη (shared memory). Αυτό επιτυγχάνεται δημιουργώντας το αρχείο /etc/systemd/system/dev-shm.mount.

```
~]# cat > /etc/systemd/system/tmp.mount << EOF
# /etc/systemd/system/default.target.wants/tmp.mount -> ../../tmp.mount

[Unit]
Description=Temporary Directory
Documentation=man:hier(7)
Before=local-fs.target

[Mount]
What=tmpfs
Where=/tmp
Type=tmpfs
Options=mode=1777,strictatime,nosuid,noexec
EOF
```

και ένα symlink [6]:

```
~]# ln -s /etc/systemd/system/dev-shm.mount /etc/systemd/system/
default.target.wants/dev-shm.mount
```

και έπειτα επανεκκίνηση του systemctl:

```
~]# systemctl daemon-reload
```

Οι φάκελοι /tmp και /var/tmp ασφαλίζονται με τον ίδιο τρόπο.

2.3 Ασφάλιση του Boot Loader

Η αλλαγή των παραμέτρων GRUB_TIMEOUT=0 και GRUB_HIDDEN_TIMEOUT=0 στο αρχείο /etc/default/grub δεν είναι μια ασφαλής επιλογή και είναι καλύτερο να ασφαλίζεται ο bootloader με κωδικό πρόσβασης:

Απόκλεισμός Πρόσβασης στο Single User Mode Αν κάποιος επίδοξος εισβολέας μπορέσει να εκκινήσει το σύστημα σε αυτό το mode, τότε μπορεί να εισέλθει στο σύστημα χωρίς να εισάγει τον κωδικό του root.

Απόκλεισμός Πρόσβασης στο GRUB 2 Console Αν το σύστημα χρησιμοποιεί GRUB 2 ως bootloader, ένας εισβολέας μπορεί να χρησιμοποιήσει την κονσόλα του ώστε να αλλάξει ρυθμίσεις ή να συλλέξει πληροφορίες, χρησιμοποιώντας την εντολή cat.

Απόκλεισμός Πρόσβασης σε μη Ασφαλή ΛΣ Αν το σύστημα είναι dualboot τότε ένας κακόβουλος χρήστης μπορεί να επιλέξει να εκκινήσει ένα ΛΣ, το οποίο αγνοεί τα δικαιώματα των αρχείων και τους ελέγχους ασφαλείας του συστήματος αρχείων.

Για να ενεργοποιηθεί η χρήση κωδικού πρόσβασης κατά την εκκίνηση, πρέπει να ενεργοποιηθεί ένας υπερχρήστης, οποίος να έχει πρόσβαση στις προστατευμένες εγγραφές. Συνίσταται ο υπερχρήστης να είναι **διαφορετικός από τους χρήστες του ΛΣ**. Μπορούν να οριστούν και απλοί χρήστες που θα έχουν πρόσβαση μόνο επιλογής. Για να δημιουργηθεί ένας κωδικός για τον υπερχρήστη, δώστε τις παρακάτω εντολές:

```
~]# grub-mkpasswd-pbkdf2
```

Τώρα εισάγετε το hash, που δημιουργήθηκε στο κατάλληλο αρχείο:

```
~]# cat >> /etc/grub.d/40_custom <<EOF
set superusers="myuser"
password_pbkdf2 myuser grub.pbkdf2.sha512.10000.64A6B637605F49DF603B062
0ACAC22A1CD074E5969CFB41F7E6F633EB988DBBAB43356377F05B33CF4BFAFAEFE5163
B0FEDA48FE71FE5ADA63CCE2C6D6B29485.7E2FD8CC9A4CCD7951F7E333CB55E743E355
9A6C64DD05B6ACBD7BD4EFF2E98902A3FBC63A4E70B443902F0CFB2777533BE874957B3
9398FA850E40E260E305D
export superusers
EOF
```

Τώρα αλλάξτε την ακόλουθη γραμμή στο αρχείο /etc/default/grub:

```
GRUB_CMDLINE_DEFAULT==users myuser
```

και τέλος ενημέρωση των ρυθμίσεων:

```
~]# update-grub
```

Για να απενεργοποιήσετε την πρόσβαση χωρίς κωδικό στο Single User Mode [3]:

```
~]# vi /lib/systemd/system/emergency.service
~]# vi /lib/systemd/system/rescue.service
```

Βρείτε τη γραμμή: ExecStart και αλλάξτε το sushell σε sulogin.

2.4 Εφαρμογή Γενικών Ρυθμίσεων Ασφαλείας

Εκτός από την ασφάλιση του bootloader και των προσαρτήσεων των τόμων και άλλα μέτρα ασφαλείας μπορούν να εφαρμοστούν:

2.4.1 Διατήρηση του Ελάχιστου ΛΣ

Είναι επιθυμητό η αρχική εγκατάσταση του ΛΣ να περιέχει μόνο τα ακρως απαραίτητα πακέτα για τη λειτουργία του, να είναι απενεργοποιημένες υπηρεσίες που δεν είναι αναγκαίες και να έχει ενεργοποιημένο το τείχος προστασίας. Επίσης είναι απαραίτητο το σύστημα να ενημερώνεται συχνά, με αυτόματη εγκατάσταση των ενημερώσεων ασφαλείας.

```
~]# systemctl list-units | grep service  
~]# systemctl disable rpcbind  
  
~]# ufw enable
```

εξ' ορισμού το ufw είναι ασφαλές καθώς είναι ρυθμισμένο ώστε να αποκλείει τις εισερχόμενες συνδέσεις και να επιτρέπει τις εξερχόμενες.

Η ρύθμιση των αυτόματων εγκαταστάσεων των ενημερώσεων ασφαλείας γίνεται ως εξής:

```
~]# cat > /etc/cron.weekly/apt-security-updates << EOF  
echo "*****" >> /var/log/apt-security-updates  
date >> /var/log/apt-security-updates  
aptitude update >> /var/log/apt-security-updates  
aptitude safe-upgrade -o Aptitude::Delete-Unused=false --assume-yes \  
--target-release `lsb_release -cs`-security \  
>> /var/log/apt-security-updates  
echo "Security updates (if any) installed"  
EOF  
  
~]# chmod +x /etc/cron.weekly/apt-security-updates  
  
~]# cat > /etc/logrotate.d/apt-security-updates << EOF  
/var/log/apt-security-updates {  
    rotate 2  
    weekly  
    size 250k  
    compress  
    notifempty  
}  
EOF
```

Η παραπάνω ρύθμιση εγκαθιστά τις ενημερώσεις ασφαλείας σε εβδομαδιαία βάση και εφαρμόζει logrotation, κάθε εβδομάδα ή αν το αρχείο καταγραφής είναι μεγαλύτερο από 250kB (βλ. 2.4.20), συμπιέζοντας τα παλαιότερα (compress). Τα δύο νεότερα αρχεία καταγραφής διατηρούνται (rotate 2) και δε πραγματοποιείται logrotation αν το αρχείο είναι άδειο (notifempty).

2.4.2 Ενεργοποίηση του AppArmor

Επιπρόσθετες ρυθμίσεις ασφαλείας για το Ubuntu. Το AppArmor είναι ένα πολύ χρήσιμο εργαλείο για τη μείωση του πλήθους του λογισμικού, που μπορεί να γίνει στόχος επίθεσης, όπως οι εξυπηρετητές ιστοσελίδων και άλλες υπηρεσίες [11]. Οι προστατευμένες διεργασίες περιορίζονται με τη χρήση προφίλ. Είναι δυνατή η χρήση επιπλέον προφίλ με την εγκατάσταση του πακέτου apparmor-profiles.

```
~]# apt-get install apparmor-profiles
```

Τα προφίλ αποθηκεύονται στο φάκελο /etc/apparmor.d

Το AppArmor έχει δυο τρόπους λειτουργίας:

- Enforce - Όλοι οι κανόνες των προφίλ επιβάλλονται και όλες οι μη επιτρεπτές ενέργειες καταγράφονται στο syslog.
- Complain – Όλες οι ενέργειες καταγράφονται χωρίς να περιορίζονται.

Μπορούμε να εμφανίζουμε τον τρόπο λειτουργίας του AppArmor ως εξής:

```
~]# apparmor_status
```

Για να αλλάξουμε τον τρόπο λειτουργίας (π.χ. mysqld):

```
~]# apt-get install apparmor-utils  
~]# aa-enforce /usr/sbin/mysqld
```

ή να ρυθμίσουμε το AppArmor ώστε να μόνο να εμφανίζει μηνύματα, χωρίς να εφαρμόζει τους περιορισμούς:

```
~]# aa-complain /usr/sbin/mysqld
```

Για να φορτώσουμε ένα προφίλ στον πυρήνα του ΛΣ:

```
~]# cat /etc/apparmor.d/profile.name | sudo apparmor_parser -a
```

Για να ενεργοποιήσουμε ένα προφίλ για μια εφαρμογή (π.χ. firefox):

```
~]# rm /etc/apparmor.d/disable/usr.bin.firefox  
~]# cat /etc/apparmor.d/usr.bin.firefox | sudo apparmor_parser -a
```

Για να απενεργοποιήσουμε το παραπάνω προφίλ, αν δημιουργεί προβλήματα:

```
~]# ln -s /etc/apparmor.d/usr.bin.firefox /etc/apparmor.d/disable/  
~]# apparmor_parser -R /etc/apparmor.d/usr.bin.firefox
```

2.4.3 Απεγκατάσταση Διαχειριστών Παραθύρων

Συνίσταται η απεγκατάσταση του συστήματος παραθύρων X, των διαχειριστών παραθύρων και του συνοδευτικού λογισμικού **σε παραγωγικούς εξυπηρετητές**, καθώς επιβαρύνουν το σύστημα με άχρηστα πακέτα και εγείρουν ζητήματα ασφαλείας.

```
~]# apt-get remove x-window-system-core  
~]# apt-get autoremove --purge
```

2.4.4 Απενεργοποίηση Οδηγών και Προσαρτημάτων Πυρήνα

Προσαρτήματα πυρήνα και οδηγοί συσκευών οι οποίες δε χρησιμοποιούνται, θα πρέπει να είναι απενεργοποιημένες [3].

```
~]# echo "install bluetooth /bin/true" > /etc/modprobe.d/disablemod.conf
~]# echo "install firewire-core /bin/true" >> /etc/modprobe.d/
disablemod.conf
~]# echo "install net-pf-31 /bin/true" >> /etc/modprobe.d/disablemod.conf
~]# echo "install soundcore /bin/true" >> /etc/modprobe.d/disablemod.conf
~]# echo "install thunderbolt /bin/true" >> /etc/modprobe.d/
disablemod.conf
~]# echo "install usb-midi /bin/true" >> /etc/modprobe.d/disablemod.conf
~]# echo "install usb-storage /bin/true" >> /etc/modprobe.d/
disablemod.conf
```

2.4.5 Απενεργοποίηση μη Χρησιμοποιούμενων Συστημάτων Αρχείων

Συστήματα αρχείων τα οποία δε χρησιμοποιούνται από το ΛΣ για τις ανάγκες λειτουργίας του, θα πρέπει να απενεργοποιούνται για λόγους ασφαλείας [3].

```
~]# echo "install cramfs /bin/true" > /etc/modprobe.d/disablemnt.conf
~]# echo "install freevxfs /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install jffs2 /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install hfs /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install hfsplus /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install squashfs /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install udf /bin/true" >> /etc/modprobe.d/disablemnt.conf
~]# echo "install vfat /bin/true" >> /etc/modprobe.d/disablemnt.conf
```

2.4.6 Απενεργοποίηση εν Δυνάμει Ανασφαλών Δικτυακών Πρωτοκόλλων

Δικτυακά πρωτόκολλα, τα οποία δεν είναι κοινώς διαδεδομένη η χρήση τους και δε χρησιμοποιούνται από το ΛΣ για την εκτέλεση των λειτουργιών του, θα πρέπει να απενεργοποιούνται [3].

```
~]# echo "install dccp /bin/true" >> /etc/modprobe.d/disablenet.conf
~]# echo "install sctp /bin/true" >> /etc/modprobe.d/disablenet.conf
~]# echo "install rds /bin/true" >> /etc/modprobe.d/disablenet.conf
~]# echo "install tipc /bin/true" >> /etc/modprobe.d/disablenet.conf
```

2.4.7 Έλεγχος αν το Appport είναι Απενεργοποιημένο

Το Appport είναι ένα σύστημα το οποίο επεμβαίνει όταν ένα λογισμικό καταρρέει και συλλέγει πολύτιμες πληροφορίες για το συμβάν και το ΛΣ, ενώ αποστέλλει στους προγραμματιστές του εγκατεστημένου λογισμικού πληροφορίες για τα πωκέτα, την έκδοση του ΛΣ κτλ. Το Appport είναι απενεργοποιημένο στις σταθερές εκδόσεις, ακόμα και αν είναι εγκατεστημένο και αυτό συμβαίνει για διάφορους λόγους:

- Το Appport συλλέγει δυνητικά ευαίσθητες πληροφορίες όπως αποτυπώσεις πυρήνα, περιεχόμενα στοίβας μνήμης συστήματος και αρχεία καταγραφών. Στις παραπάνω πληροφορίες μπορεί να περιέχονται κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, σειριακοί αριθμοί και άλλα προσωπικά δεδομένα.
- Η διαδικασία συλλογής δεδομένων από το AppPort απαιτεί αρκετούς πόρους από τον επεξεργαστή και τις Ι/Ο συσκευές, πράγμα το οποίο επιβραδύνει το ΛΣ και δεν επιτρέπει στο χρήστη να επανεκκινήσει το καταρευθέν λογισμικό για αρκετά δευτερόλεπτα.

Η απενεργοποίηση του AppPort γίνεται ως εξής:

```
~]# sed -i 's/enabled=.*/enabled=0/' /etc/default/appport  
~]# systemctl mask appport.service
```

2.4.8 Απενεργοποίηση Αποτυπωμάτων ΛΣ

Τα αποτυπώματα του ΛΣ (coredumps) είναι δυνητικά μια σοβαρή διαρροή πληροφοριών, καθώς μπορεί να περιέχουν κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα. Συνίσταται λοιπόν η απενεργοποίησή του σε παραγωγικούς εξυπηρετητές, εάν δεν είναι αναγκαίο για την αποσφαλμάτωση. Η απενεργοποίηση λήψεων αποτυπωμάτων γίνεται ως εξής:

```
~]# sed -i 's/^#Storage=.*/Storage=none/' /etc/systemd/coredump.conf  
~]# systemctl restart systemd-journald
```

2.4.9 Απενεργοποίηση Cronjobs για τους Χρήστες

Ο χρονοπρογραμματιστής Cron έχει ενσωματωμένο τρόπο ελέγχου για το ποιος επιτρέπεται και ποιος οχι, να χρονοπρογραμματίσει εργασίες στο ΛΣ. Ο έλεγχος ρυθμίζεται μέσω των αρχείων /etc/cron.allow και /etc/cron.deny. Για να αποκλειστεί ένας χρήστης από τη χρήση του cron, θα πρέπει το username του να εισαχθεί στο αρχείο cron.deny. Αντίστοιχα, για να επιτραπεί σε ένα χρήστη η χρήση του cron, θα πρέπει να γίνει η αντίστοιχη καταχώρηση στο αρχείο cron.allow. Αν επιθυμούμε να απενεργοποιήσουμε το cron για όλους τους χρήστες (πλην root), προσθέτουμε τη γραμμή 'ALL' στο αρχείο cron.deny [8].

```
~]# echo ALL > /etc/cron.deny
```

2.4.10 Ρύθμιση των Ορίων Ασφαλείας των Χρηστών

Είναι μια καλή πρακτική η ρύθμιση ορίων ασφαλείας, όσον αφορά την πρόσβαση των χρηστών στους παραγωγικούς εξυπηρετητές. Τα όρια αυτά περιλαμβάνουν μέγιστο αριθμό ταυτόχρονων συνεδριών (max-logins), μέγιστο πλήθος εκτελούμενων διεργασιών, μέγεθος αρχείου coredump κ.α. Για τη ρύθμιση των ορίων αυτών στο σύστημα, εκτελούμε:

```
~]# sed -i 's/^# End of file*/' /etc/security/limits.conf
~]# echo "* hard maxlogins 10" >> /etc/security/limits.conf
~]# echo "* hard core 0" >> /etc/security/limits.conf
~]# echo "* soft nproc 100" >> /etc/security/limits.conf
~]# echo "* hard nproc 150" >> /etc/security/limits.conf
~]# echo "# End of file" >> /etc/security/limits.conf
```

2.4.11 Αφαίρεση suid από Συγκεκριμένα Αρχεία

Συνίσταται η αφαίρεση του suid bit από συγκεκριμένα εκτελέσιμα αρχεία που βρίσκονται στους φακέλους /bin και /usr/bin, καθώς αυτά τα αρχεία εκτελούνται με δικαιώματα υπερχρήστη 'root' ή με τα δικαιώματα της υπερομάδας 'sudo' (ή ακόμα ως ένας άλλος χρήστης ή ομάδα). Αρχικά, μπορούμε να βρούμε ποια αρχεία έχουν ενεργό το SUID και έπειτα να απενεργοποιήσουμε επιλεκτικά αυτά που θεωρούμε επικίνδυνα. (παράδειγμα για το /bin/su):

```
~]# find / -perm -4000 -print
~]# chmod -s /bin/su
```

2.4.12 Εφαρμογή Αυστηρότερων Δικαιωμάτων σε Αρχεία - Φακέλους

Για να θέσετε αυστηρότερα δικαιώματα σε νέα αρχεία και φακέλους, ρυθμίστε το συνολικό umask του συστήματος σε 027. Αυτό ορίζει τα δικαιώματα σε 640 (rw-r---) σε νέα αρχεία και 750 (rwxr-x---) σε νέους φακέλους:

```
~]# sed -i 's/umask 022/umask 027/g' /etc/init.d/rc
~]# echo "umask 027" >> /etc/profile
~]# echo "umask 027" >> /etc/bash.bashrc
```

Συνίσταται ο ορισμός του umask σε 077 σε εξυπηρετητές αρχείων, καθώς λάθος δικαιώματα μπορεί να προκαλέσουν προβλήματα σε συστήματα τα οποία διαμοιράζουν αρχεία (SAMBA ή NFS).

2.4.13 Καθορισμός DNS Εξυπηρετητών

Είναι απαραίτητο οι απαντήσεις DNS να μην αλλοιώνονται με κανένα τρόπο για την αποφυγή MITM και άλλων τύπων επιθέσεων και κινδύνων ασφαλείας. Η ασφάλιση του DNS ρυθμίζεται ενημερώνοντας το αρχείο /etc/systemd/resolved.conf όπως παρακάτω:

```
[Resolve]
DNS="YOUR PRIMARY DNS"
FallbackDNS=8.8.8.8 8.8.4.4
#Domains=
#LLMNR=yes
DNSSEC=allow-downgrade
```

Είναι επίσης καλή πρακτική η ενεργοποίηση του DNSSEC στους εξηπηρετητές DNS, όπως περιγράφεται στο τμήμα [2.7.2](#).

2.4.14 Αφαίρεση Ρυθμίσεων Απομακρυσμένης Πρόσβασης

Η αφαίρεση των `.rhosts` και `hosts.equiv` τους φακέλους χρηστών, συμβάλουν στην ασφάλεια ενός συστήματος Linux. Αυτό γίνεται ως εξής:

```
~]# for dir in $(awk -F ":" '{print $6}' /etc/passwd); do
    find "$dir" \(
        -name "hosts.equiv" -o -name ".rhosts" \
    ) \
    -exec rm -f {} \; 2> /dev/null
done

~]# if [[ -f /etc/hosts.equiv ]]; then
    rm /etc/hosts.equiv
fi
```

2.4.15 Έλεγχος Πρόσβασης με το TCP Wrappers

Τα αρχεία `/etc/hosts.allow` και `/etc/hosts.deny` χρησιμοποιούνται για τον έλεγχο της πρόσβασης στις υπηρεσίες του ΛΣ. Αν χρησιμοποιείτε μια έκδοση χρήστη (desktop) και όχι εξυπηρετητή, τότε είναι καλό να προσθέσετε τη γραμμή 'ALL' στο αρχείο `/etc/hosts.deny` και τη γραμμή 'localhost' στο αρχείο `/etc/hosts.allow`. Μια εγκατάσταση εξυπηρετητή συνήθως χρειάζεται και επιπρόσθετες γραμμές στο αρχείο `/etc/hosts.allow`. Οι παραπάνω ρυθμίσεις εισάγονται ως εξής:

```
~]# echo "ALL: LOCAL, 127.0.0.1" >> /etc/hosts.allow
~]# echo "ALL: PARANOID" > /etc/hosts.deny
```

2.4.16 Ρύθμιση των Banners

Η ρύθμιση Banners (μηνυμάτων εισόδου) είναι πιο πολύ μια αισθητική παρέμβασή παρά μια ρύθμιση ασφαλείας, αλλά προειδοποιεί τους πιθανούς εισβολείς ότι το σύστημα παρακολουθείται και είναι ασφαλές. Ο καθορισμός των Banners γίνεται με τη χρήση των αρχείων: `/etc/issue`, `/etc/motd`, `/etc/issue.net`.

2.4.17 Αφαίρεση μη Αναγκαιούντων Χρηστών

Η αφαίρεση χρηστών που είναι ανενεργοί ή αντιστοιχούν σε υπηρεσίες που δεν χρησιμοποιούνται, μειώνουν τις πιθανότητες παραβίασης του συστήματος:

```
~]# userdel -r username
```

2.4.18 Δημιουργία Νέων Χρηστών με Ανενεργό shell

Συνίσταται η δημιουργία των νέων χρηστών με εξ' ορισμού shell το /bin/false, για να αποτρέψει πιθανούς εισβολείς να αποκτήσουν πρόσβαση στην γραφική εντολών με αυτοματοποιημένα εργαλεία. Οι παραπάνω ρυθμίζεις ορίζονται στα αρχεία /etc/adduser.conf και /etc/useradd.conf:

```
DSHELL=/bin/false
```

2.4.19 Ασφάλιση του NTP

Είναι απαραίτητο η ώρα του συστήματος να είναι ακριβής ανα πάσα στιγμή. Κρίσιμες υπηρεσίες, οι οποίες απαιτούν ακριβή ώρα και ημερομηνία περιλαμβάνουν την καταγραφή του ΛΣ, το μηχανισμό εισόδου χρηστών, το χρονοπρογραμματισμό εργασιών, τις υπηρεσίες χρυπτογράφησης (επαλήθευση πιστοποιητικών). Για τη διατήρηση ακριβούς ημερομηνίας και ώρας απαιτείται μια ακριβής πηγή. Σε παραγωγικούς εξυπηρετητές μπορούν να χρησιμοποιηθούν πηγές οδηγούμενες από GPS ή ακόμα και έμπιστοι διακομιστές ώρας (NTP). Η ρύθμιση του πελάτη NTP γίνεται με την ενημέρωση του αρχείου /etc/systemd/timesyncd.conf ως εξής:

```
[Time]
NTP=3.ubuntu.pool.ntp.org pool.ntp.org
FallbackNTP=0.ubuntu.pool.ntp.org 1.ubuntu.pool.ntp.org
```

2.4.20 Ρύθμιση του logrotate

Εάν έχετε ενεργοποιημένη την λειτουργία καταγραφής στο σύστημά σας, τότε τα αρχεία καταγραφής θα συνεχίζουν να αυξάνουν σε μέγεθος μέχρι του σημείου που ο φάκελος /var/log γεμίζει και το ΛΣ καθίσταται ασταθές. Στην περίπτωση που το /var δεν είναι σε ξεχωριστό τόμο, το ΛΣ μπορεί να γίνει μη αποκρίσιμο. Πιθανές λύσεις του προβλήματος είναι η αποστολή των καταγραφών του ΛΣ σε ένα κεντρικό σύστημα καταγραφής, όπως το splunk (βλ. τμ. 2.8.1) και η ενεργοποίηση της ανακύκλωσης των αρχείων καταγραφής (logrotate). Η ανακύκλωση των αρχείων καταγραφής αποτρέπει την κατάληψη όλου του διαθέσιμου χώρου, κρατώντας ιστορικό μόνο των πιο πρόσφατων συμβάντων, βάσει συγκεκριμένων κανόνων. Η ενεργοποίηση της παραπάνω λειτουργίας γίνεται μέσω του αρχείου /etc/logrotate.conf. Στο σενάριο γραφικής εντολών (bash script), το οποίο επισυνάπτεται στην παρούσα εργασία (βλ. Κεφ. 4), το ΛΣ είναι προγραμματισμένο να ανακυκλώνει τα αρχεία καταγραφής κάθε μέρα.

2.4.21 Απενεργοποίηση του Συνδυασμού Ctrl+Alt+Delete

Στις πρόσφατες εκδόσεις του ΛΣ Linux ο συνδυασμός πλήκτρων CTRL-ALT-DEL επανεκινεί το σύστημα. Αυτό δεν είναι ιδιαίτερα επιθυμητό στους παραγωγικούς διακομιστές, καθώς ο συνδυασμός είναι δυνατό να ενεργοποιηθεί κατά λάθος. Η απενεργοποίηση της παραπάνω λειτουργίας γίνεται ως εξής [11]:

```
~]# sudo systemctl mask ctrl-alt-del.target
~]# sudo systemctl daemon-reload
```

Εάν θέλουμε το ΛΣ να μη παρεμβάλει τον παραπάνω συνδυασμό πλήκτρων αλλά απλώς να καταγράψει το συμβάν, τότε ενημερώνουμε το αρχείο `/etc/init/control-alt-delete.conf` αλλάζοντας την αντίστοιχη γραμμή [3]:

```
exec /sbin/shutdown -r now "Control-Alt-Delete pressed"  
σε  
exec /usr/bin/logger -p security.info "Control-Alt-Delete pressed"
```

2.5 Ασφάλεια Λογαριασμών

2.5.1 Δημιουργία Ασφαλών Κωδικών Χρήστη

Για λόγους ασφαλείας το σύστημα είναι ρυθμισμένο να χρησιμοποιεί SHA512 και shadow passwords. Συνίσταται ιδιαίτερα να μην αλλάζουν αυτές οι ρυθμίσεις. Κατά την δημιουργία ασφαλών κωδικών, ο χρήστης θα πρέπει να έχει υπόψη του ότι οι μακροσκελείς κωδικοί είναι πιο ασφαλείς από τους κωδικούς με λίγους χαρακτήρες, ακόμα και αν αυτοί περιέχουν τους λεγόμενους ειδικούς χαρακτήρες. Δεν είναι, λοιπόν, καλή πρακτική η δημιουργία ενός κωδικού χρήστη με μόνο οκτώ χαρακτήρες, ακόμα και αν αυτός περιέχει αριθμούς, ειδικούς ή κεφαλαιούς χαρακτήρες. Εργαλεία παραβίασης κωδικών, όπως το John The Ripper είναι ρυθμισμένα ώστε να παραβιάζουν τέτοιους ακριβώς κωδικούς, ενώ παράλληλα, τέτοιοι κωδικοί είναι δύσκολο να απομνημονευτούν.

Το pwmake είναι ένα εργαλείο γραμμής εντολών το οποίο παράγει κωδικούς χρήστη, που αποτελούνται από μικρά - κεφαλαία, αριθμούς και ειδικούς χαρακτήρες.

```
~]# apt-get install libpwquality-tools  
~]# pwmake --help
```

2.5.2 Επιβολή Ισχυρών Κωδικών ασφαλείας

Το pam_cracklib χρησιμοποιείται για να ελέγξει την ισχύ ενός κωδικού πρόσβασης, σύμφωνα με προδιαγεγραμμένους κανόνες [1]. Για την ενεργοποίηση του pam_cracklib και την αποτροπή των χρηστών από τη χρήση μικρών ή απλών κωδικών πρόσβασης, προσθέτουμε την παρακάτω γραμμή στο αρχείο `/etc/pam.d/common-password`:

```
password required pam_cracklib.so retry=3 maxrepeat=3 minlen=15  
dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=8
```

Ο έλεγχος των λογαριασμών για κενούς κωδικούς, είναι επίσης μια καλή πρακτική [9]. Κάθε λογαριασμός, ο οποίος δεν έχει κωδικό πρόσβασης είναι μια απειλή ασφαλείας, καθώς εκθέτει το σύστημα σε μη εξουσιοδοτημένη πρόσβαση. Ο έλεγχος των λογαριασμών για κενούς κωδικούς ασφαλείας, γίνεται ως εξής:

```
~]# cat /etc/shadow | awk -F: '($2=="") {print $1}'
```

Ο διαχειριστής θα πρέπει επίσης να περιορίζει την επαναχρησιμοποίηση παλιών κωδικών από τους χρήστες. Ο περιορισμός τίθεται ως εξής: Τροποποιούμε το αρχείο `/etc/pam.d/common-password`:

```
~]# vi /etc/pam.d/common-password
```

Προσθέστε την παρακάτω γραμμή για να απαγορεύσετε στους χρήστες την επαναχρησιμοποίηση των 5 τελευταίων κωδικών πρόσβασης.

```
password [success=1 default=ignore] pam_unix.so obscure use_authtok  
try_first_pass sha512 remember=5
```

Με αυτό τον τρόπο, το ΛΣ αποθηκεύει τους 5 τελευταίους κωδικούς πρόσβασης. Εάν κάποιος επιχειρήσει να ξαναχρησιμοποιήσει κάποιον από αυτούς τους κωδικούς, τότε θα λάβει το παρακάτω μήνυμα:

```
Password has been already used. Choose another.
```

2.5.3 Πολιτική Λήξης Λογαριασμών και Κωδικών

Είναι απαραίτητο για τον διαχειριστή συστημάτων να εφαρμόζει την πολιτική λήξης των κωδικών και των λογαριασμών στο σύστημα. Οι ρυθμίσεις αυτές ορίζονται στο αρχείο `/etc/login.defs` όπως παρακάτω:

```
LOG_OK_LOGINS yes  
PASS_MIN_DAYS 7  
PASS_MAX_DAYS 30
```

Οι παραπάνω γραμμές καταγράφουν τις επιτυχείς εισόδους στο σύστημα, απαγορεύουν δυο διαδοχικές αλλαγές κωδικών πρόσβασης, για ένα λογαριασμό, μέσα σε 7 ημέρες και λήγουν την ισχύ των κωδικών κάθε 30 ημέρες. Για την απενεργοποίηση ενός λογαριασμού, ο οποίος δεν έχει χρησιμοποιηθεί 35 μέρες μετά από τη λήξη του κωδικού πρόσβασης, ενημερώνουμε το αρχείο `/etc/default/useradd`:

```
INACTIVE=35
```

2.5.4 Κλείδωμα Λογαριασμών

Στο Ubuntu 16.04LTS, το PAM module `pam_tally` επιτρέπει στο διαχειριστή συστήματος να κλειδώνει τους λογαριασμούς των χρηστών, μετά από ένα καθορισμένο αριθμό αποτυχημένων προσπαθειών. Ο περιορισμός των προσπαθειών εισόδου των χρηστών είναι ένα μέτρο ασφαλείας το οποίο αποτρέπει τις επιθέσεις τύπου brute force, οι οποίες στοχεύουν στην ανάκτηση του κωδικού πρόσβασης ενός χρήστη [1]. Το άρθρωμα `pam_tally`, αποθηκεύει τις αποτυχημένες προσπάθειες στο αρχείο `/var/log/faillog`.

Για να κλειδώνεται ένας χρήστης μετά από πέντε αποτυχημένες προσπάθειες και να ξεκλειδώνεται αυτόματα μετά από 15 λεπτά, προσθέστε την παρακάτω γραμμή στο αρχείο `/etc/pam.d/common-auth`:

```
auth required pam_tally.so file=/var/log/faillog deny=5 unlock_time=900
```

Και την παρακάτω γραμμή στο αρχείο `etc/pam.d/common-account`:

```
account required pam_tally.so reset
```

Για να εφαρμόσετε μια ελάχιστη αναμονή 4 δευτ. στην περίπτωση μιας αποτυχημένης προσπάθειας εισόδου στο σύστημα, προσθέστε την επόμενη γραμμή στο αρχείο `/etc/pam.d/login`:

```
auth optional pam_faildelay.so delay=4000000
```

2.5.5 Κλείδωμα Συνεδρίας – Αυτόματη Αποσύνδεση

Όταν ένας χρήστης είναι συνδεδεμένος ως root, μία μη επιτηρούμενη συνεδρία, μπορεί να αποτελέσει σημαντικό κίνδυνο ασφαλείας. Για να μειώσουμε αυτό τον κίνδυνο, μπορούμε να ρυθμίσουμε το σύστημα, ώστε να αποσυνδέει αυτόματα τους χρήστες που δεν αλληλεπιδρούν με αυτό, μετά από ένα συγκεκριμένο χρονικό διάστημα. Για να το επιτύχουμε αυτό, ενημερώνουμε το αρχείο /etc/systemd/logind.conf με τις παρακάτω γραμμές:

```
KillUserProcesses=1
KillExcludeUsers=root
IdleAction=lock
IdleActionSec=15min
RemoveIPC=yes
```

Οι παραπάνω ρυθμίσεις κλειδώνουν την συνεδρία μετά από 15 λεπτά μη αλληλεπίδρασης των χρηστών με το σύστημα και τερματίζει όλες τις τρέχουσες διεργασίες του χρήστη. Ο χρήστης root εξαιρείται από τον αυτόματο τερματισμό των διεργασιών.

Οι χρήστες μπορεί να χρειαστεί να εγκαταλείψουν το σταθμό εργασίας τους για διάφορους λόγους. Για να κλειδώσουν την κονσόλα της γραμμής εντολών, οι χρήστες μπορούν να χρησιμοποιήσουν ένα εργαλείο το οποίο ονομάζεται vlock. Για να εγκαταστήσετε το παραπάνω εργαλείο, εκτελέστε τις παρακάτω εντολές ως χρήστης root:

```
~]# apt-get install vlock
```

2.5.6 Περιορισμός της Πρόσβασης root

Αν ο διαχειριστής συστήματος δεν επιτρέπει στους χρήστες να εισέρχονται στο σύστημα, χρησιμοποιώντας τον υπερχρήστη root, τότε ο κωδικός πρόσβασης του υπερχρήστη θα πρέπει να διατηρείται κρυφός και η πρόσβαση στο runlevel one ή single user mode θα πρέπει να απαγορεύεται με τη χρήση προστασίας κωδικού πρόσβασης στον boot loader (όπως περιγράφεται στο τμήμα 2.3).

Για να αποτρέψει τους χρήστες να εισέρχονται στο σύστημα απευθείας ως υπερχρήστες, ο διαχειριστής συστήματος μπορεί να θέσει το shell του χρήστη root σε /bin/false στο αρχείο /etc/passwd. Λογισμικό το οποίο δεν απαιτεί shell, όπως FTP, mail πελάτες, και αρκετά setuid προγράμματα, δεν λαμβάνουν υπόψη τους το παραπάνω περιορισμό.

Για να περιοριστεί περαιτέρω την πρόσβαση των χρηστών στο λογαριασμό του υπερχρήστη, ο διαχειριστής συστήματος μπορεί να απενεργοποιήσει την είσοδο των χρηστών στην κονσόλα γραμμής εντολών, τροποποιώντας το αρχείο /etc/securetty. Αυτό το αρχείο περιγράφει όλες τις συσκευές μέσω των οποίων ο υπερχρήστης δύναται να εισέλθει στο σύστημα [1]. Εάν το παραπάνω αρχείο δεν υπάρχει, τότε ο υπερχρήστης μπορεί να συνδεθεί στο σύστημα μέσω οποιασδήποτε συσκευής επικοινωνίας, είτε μέσω της κονσόλας (ακόμα και σειριακής), είτε μέσω οποιασδήποτε διεπαφής δικτύου. Αυτό είναι επικίνδυνο, διότι ένας χρήστης μπορεί να συνδεθεί στην μηχανή ως υπερχρήστης μέσω του πρωτοκόλλου telnet, το οποίο διακινεί τους κωδικούς πρόσβασης ακρυπτογράφητους εντός του δικτύου:

```
~]# echo '' > /etc/securetty
```

Επίσης, συνιστάται η απενεργοποίηση του λογαριασμού του υπερχρήστη. Κατά αυτό τον τρόπο ένας πλαστογραφημένος χρήστης με UID 0 δεν μπορεί να πάρει πρόσβαση στο σύστημα.

```
~]# usermod -L root
```

2.6 Απειλές για τις Υπηρεσίες

Οι δικτυακές υπηρεσίες μπορούν να αποτελέσουν κίνδυνο ασφαλείας για τα συστήματα Linux. Παρακάτω περιγράφονται μερικά από τα πιο συχνά προβλήματα:

Επιθέσεις τύπου Denial of Service (DoS) Αυτός ο τύπος επίθεσης καθιστά το σύστημα μη απόκρισιμο βομβαρδίζοντας το με πλήθος αιτημάτων, τα οποία δεν είναι σε θέση να επεξεργαστεί.

Επιθέσεις τύπου Distributed Denial of Service (DDoS) Αυτός ο τύπος επίθεσης χρησιμοποιεί πάρα πολλούς ηλεκτρονικούς υπολογιστές (αρκετές φορές μπορεί να φτάνουν σε πλήθος αρκετές χιλιάδες), στους οποίους έχει εγκατασταθεί κακόβουλο λογισμικό, ώστε να εξαπολύσουν μια κατευθυνόμενη επίθεση εναντίον ενός εξυπηρετητή, τον οποίο και βομβαρδίζουν με πλήθος αιτημάτων, τα οποία δεν μπορεί να επεξεργαστεί.

Επιθέσεις που χρησιμοποιούν script Εάν ένας διακομιστής διαδικτύου (Web Server) χρησιμοποιεί script για να εκτελέσει διάφορες εργασίες, οπως συνήθως κάνουν οι διακομιστές διαδικτύου, ένας εισβολέας μπορεί να εκμεταλλευτεί τέτοια script τα οποία δεν έχουν γραφτεί σωστά. Η επίθεση αυτού του τύπου μπορεί να προκαλέσει buffer overflow ή να επιτρέψει σε έναν κακόβουλο χρήστη να αλλοιώσει αρχεία του συστήματος.

Επιθέσεις Buffer Overflow Υπηρεσίες οι οποίες πρέπει να καταλαμβάνουν τις πόρτες από 1 έως 1023, είτε ότι πρέπει να ξεκινούν με δικαιώματα υπερχρήστη είτε να έχει ρυθμιστεί για αυτές η δυνατότητα CAP_NET_BIND_SERVICE. Όταν μια διεργασία έχει ξεκινήσει, είτε τα δικαιώματα είτε η παραπάνω δυνατότητα καταργούνται. Εάν αυτό δε συμβεί, τότε η υπηρεσία είναι ευάλωτη σε επιθέσεις τύπου Buffer Overflow και ο επιτιθέμενος μπορεί να λάβει πρόσβαση στο σύστημα, με το χρήστη ο οποίος τρέχει την υπηρεσία. Για το λόγο ότι, υπάρχουν αρκετές αδυναμίες ασφαλείας τύπου Buffer Overflow, οι επιτιθέμενοι χρησιμοποιούν αυτοματοποιημένα εργαλεία για να ανιχνεύσουν συστήματα με αδυναμίες και μετά, εφόσον έχουν αποκτήσει πρόσβαση σε αυτά, εγκαθιστούν root-kits ώστε να διατηρούν αυτή την πρόσβαση.

Παραδείγματα υπηρεσιών οι οποίες είναι μη ασφαλείς περιλαμβάνουν τις rlogin, rsh, telnet, vsftpd. Όλα τα μη ασφαλή προγράμματα απομακρυσμένης πρόσβασης θα πρέπει να αποφεύγονται και να χρησιμοποιείται το SSH όπου είναι δυνατό. Το FTP δεν είναι τόσο επικίνδυνο, για την ασφάλεια του συστήματος, όσο τα απομακρυσμένα shells, όμως οι FTP εξυπηρετητές πρέπει να είναι προσεκτικά ρυθμισμένοι και να παρακολουθούνται αποτελεσματικά για την αποφυγή προβλημάτων ασφαλείας.

Τέλος, οι παρακάτω υπηρεσίες πρέπει να ρυθμίζονται με μεγάλη προσοχή και να προστατεύονται πάντα από τείχος προστασίας:

- auth

- nfs-server
- smb and nbm
- yppasswdd
- ypserv
- ypxfrd

2.6.1 Ασφαλής ρύθμιση του NFS

Το NFS αποτελεί την πιο κοινή επιλογή για διαμοιρασμό αρχείων μεταξύ UNIX διακομιστών. Η έκδοση NFS4 είναι η εξ' ορισμού εγκατεστημένη έκδοση στις πιο σύγχρονες διανομές Linux. Αυτή η έκδοση θεωρείται ασφαλής, αλλά οι προηγούμενες εκδόσεις παρουσιάζαν κάποια κενά ασφαλείας. Παρακάτω περιγράφουμε πως μπορούμε να ασφαλίσουμε την εν λόγω υπηρεσία.

Ασφάλιση του NFS - rpcbind με TCP Wrappers Είναι αρκετά σημαντική η χρήση του TCP Wrappers (βλ. τμ. 2.4.15) για τον καθορισμό των δικτύων και των H/Y που μπορούν να έχουν πρόσβαση στην υπηρεσία rpcbind, καθώς δεν παρέχει καμιά μορφή αυθεντικοποίησης. Η ασφαλής ρύθμιση του αφορά μόνο τις εκδόσεις v2 και v3, καθώς η v4 δεν την χρησιμοποιεί για τη λειτουργία της. Αν σκοπεύετε να χρησιμοποιήσετε κάποια από τις παλαιότερες εκδόσεις, τότε το rpcbind είναι απαραίτητο και το παρακάτω κείμενο βρίσκει εφαρμογή. Επίσης, είναι καλή πρακτική η χρήση μόνο IP διευθύνσεων κατά τη ρύθμιση του rpcbind, καθώς τα ονόματα DNS είναι δυνατό να πλαστογραφηθούν (π.χ. DNS poisoning κ.α.).

Προστασία του rpcbind και rpc.mountd με το ufw Για τον περαιτέρω περιορισμό της πρόσβασης στην υπηρεσία rpcbind είναι μια καλή ιδέα η προσθήκη κανόνων στο τείχος προστασίας του διακομιστή και ο περιορισμός της πρόσβασης για συγκεκριμένα δίκτυα. Από τους παρακάτω κανόνες του τείχους προστασίας, ο πρώτος επιτρέπει τις συνδέσεις TCP στην πόρτα 111 (η οποία χρησιμοποιείται για την υπηρεσία rpcbind) από το δίκτυο 192.168.1.0/24. Ο δεύτερος κανόνας επιτρέπει τις συνδέσεις στην ίδια πόρτα από τον localhost. Όλα τα υπόλοιπα πακέτα απαγορεύονται.

```
~]# ufw allow proto tcp from 192.168.1.0/24 to any port 111
~]# ufw allow proto tcp from 127.0.0.1 to any port 111
```

Κατά τον ίδιο τρόπο, για να περιοριστεί η κίνηση UDP χρησιμοποιήστε τους παρακάτω κανόνες:

```
~]# ufw allow proto udp from 192.168.1.0/24 to any port 111
```

Στη συνέχεια, για να περιοριστεί η πρόσβασή στην υπηρεσία rpc.mountd, προστίθενται κανόνες στο τείχος προστασίας ufw, ώστε να περιοριστεί την πρόσβαση σε συγκεκριμένα δίκτυα. Παρακάτω παρατίθενται δύο παραδείγματα τέτοιων κανόνων. Ο πρώτος περιορίζει όλες τις συνδέσεις εκτός αυτών που προέρχονται από το δίκτυο 192.168.1.0/24. Ο δεύτερος κανόνας επιτρέπει τις συνδέσεις UDP από τον localhost:

```
~]# ufw allow from 192.168.1.0/24 to any port 32767  
~]# ufw allow proto tcp from 192.168.1.0/24 to any port 32767
```

Οι παραπάνω κανόνες έχουν ισχύ μόνο όταν η υπηρεσία `rpc.mountd` δέχεται συνδέσεις στην πόρτα 32767. Αλλάζτε τους παραπάνω κανόνες αναλόγως, εάν οι εν λόγω υπηρεσία ακούσει διαφορετική πόρτα.

Χρήση της αυθεντικοποίησης Kerberos Η έκδοση v4 χρησιμοποιεί εξ' ορισμού Kerberos κωδικοποίηση ενώ οι εκδόσεις v2, v3 είναι δυνατόν να να ρυθμιστούν ώστε να την χρησιμοποιούν, πλην των υπηρεσιών κλειδώματος και προσάρτησης των απομακρυσμένων συστημάτων αρχείων. [1]. Όπου είναι δυνατό, **εξάγετε μόνο ολόκληρους τόμους**. Η εξαγωγή ενός μόνο υποφακέλου του συστήματος αρχείων, μπορεί να θέσει ζητήματα ασφαλείας. Και αυτό διότι είναι δυνατόν, για ένα πρόγραμμα πελάτη να βγει εκτός του υποφακέλου που εξάγεται από το σύστημα και να έχει πρόσβαση σε αρχεία συστήματος. Για περισσότερες πληροφορίες δείτε την `man page exports(5)`. Χρησιμοποιείστε όπου είναι δυνατόν την ρύθμιση μονό για ανάγνωση, όταν εξάγετε συστήματα αρχείων, για να περιορίσετε τη δυνατότητα των χρηστών να αλλοιώνουν τα δεδομένα. Η αυθεντικοποίηση Kerberos ενεργοποιείται ως εξής:

```
~]# apt-get install krb5-user libpam-krb5
```

Στο αρχείο `/etc/default/nfs-kernel-server` προσθέτουμε τη γραμμή:

```
NEED_SVC_GSSD=yes
```

Για την εξαγωγή του υποφακέλου `/export/users` στο υποδίκτυο 192.198.1.0/24, προσθέτουμε την επόμενη γραμμή στο αρχείο `/etc(exports`:

```
/export/users 192.168.1.0/24 (rw, sync, no_subtree_check, sec=krb5, anonuid=65534, anongid=65534)
```

Η αυθεντικοποίηση Kerberos μπορεί να λειτουργήσει με τρεις διαφορετικούς τρόπους, οι οποίοι μπορούν να ρυθμιστούν κατά την εξαγωγή ενός συστήματος αρχείων με το NFS:

- `krb5`: χρήση του Kerberos μόνο για αυθεντικοποίηση.
- `krb5i`: χρήση αυθεντικοποίησης Kerberos τη χρήση ενός hash για κάθε συναλλαγή, για την εξασφάλιση της ακεραιότητας. Η δικτυακή κίνηση μπορεί και πάλι να αλλοιωθεί αλλά οι αλλαγές θα είναι ανιχνεύσιμες.
- `krb5p`: χρήση αυθεντικοποίησης Kerberos και κρυπτογράφησης της δικτυακής κίνησης μεταξύ πελάτη και διακομιστή. Είναι η πιο ασφαλής ρύθμιση, αλλά παράγει και το μεγαλύτερο όγκο δικτυακής κίνησης.

Τέλος, στο αρχείο `/etc/krb5.keytab` θα πρέπει να έχει δυνατότητα ανάγνωσης μόνο ο υπερχρήστης.

Δεν είναι καλή πρακτική η χρήση της ρύθμισης `no_root_squash` και καλό είναι να γίνεται έλεγχος και σε υπάρχοντες διακομιστές ώστε να είναι απενεργοποιημένη. Εξ' ορισμού το NFS αλλάζει τον υπερχρήστη σε `nfsnobody`, ένα απλό λογαριασμό χρήστη, μετά την ενεργοποίηση της υπηρεσίας. Αυτό έχει σαν αποτέλεσμα την αλλαγή του ιδιοκτήτη για όλα τα αρχεία που έχουν δημιουργηθεί από τον `root` σε `nfsnobody`, το οποίο απαγορεύει

το ανέβασμα αρχείων με ενεργοποιημένο το setuid bit. Εάν το no_root_squash χρησιμοποιείται, τότε απομακρυσμένοι χρήστες είναι σε θέση να αλλάξουν κάθε αρχείο στο εξαγόμενο σύστημα αρχείων και να αφήσουν πίσω τους εφαρμογές και αρχεία τα οποία έχουν μολυνθεί με ιούς, δούρειους ή πους κ.α.

Η ρύθμιση secure χρησιμοποιείται από την πλευρά του διακομιστή κατά την εξαγωγή ενός συστήματος αρχείων, ώστε να περιορίσει τις πόρτες στις οποίες ακούει υπηρεσία, στις λεγόμενες δεσμευμένες (οι οποίες είναι αυτές που βρίσκονται κάτω από το 1024) [5]. Παλαιότερα, οι διακομιστές επέτρεπαν μόνο συνδέσεις από πελάτες σε αυτές τις πόρτες, καθόσον σε αυτές θεωρούνταν ότι εκτελούνταν έμπιστο λογισμικό. Όμως πολλές φορές δεν είναι δύσκολο για κάποιον να γίνει υπέρ χρήστης στο μηχάνημά του, οπότε είναι σπανίως ορθό για το διακομιστή να θεωρεί ότι δικτυακή κίνηση λογισμικού-πελάτη, η οποία προέρχεται από δεσμευμένη πόρτα, είναι ασφαλής. Για αυτό το λόγο ο περιορισμός της δικτυακής κίνησης, μόνο στις δεσμευμένες πόρτες, έχει πολύ μικρή χρηστική αξία και είναι καλύτερη λύση η χρήση της αυθεντικοποίησης Kerberos, των τειχών προστασίας και ο περιορισμός των εξαγωγών του συστήματος αρχείων, μόνο σε συγκεκριμένους Η/Υ πελάτες.

Είναι επίσης καλή πρακτική να μην επιτρέπεται στους χρήστες να αποκτούν πρόσβαση στο διακομιστή (μέσω γραμμής εντολών ή γραφικού περιβάλλοντος). Χρησιμοποιήστε τη ρύθμιση nosuid για να μην επιτρέψετε την εκτέλεση ενός προγράμματος setuid. Η ρύθμιση nosuid απενεργοποιεί τα set-user-identifier ή set-group-identifier bits. Αυτό απαγορεύει σε απομακρυσμένους χρήστες να αποκτήσουν υψηλότερα δικαιώματα στο σύστημα τρέχοντας ένα πρόγραμμα setuid. Χρησιμοποιήστε αυτή τη ρύθμιση τόσο στην πλευρά του διακομιστή όσο και στην πλευρά του πελάτη.

Η ρύθμιση noexec απενεργοποιεί όλα τα εκτελέσιμα αρχεία στο εξαγόμενο σύστημα αρχείων. Χρησιμοποιήστε αυτή τη ρύθμιση για να αποτρέψετε τους χρήστες από το να τρέχουν εκτελέσιμα αρχεία, τα οποία έχουν τοποθετηθεί στο εξαγόμενο σύστημα αρχείων. Οι ρυθμίσεις nosuid και noexec είναι ενεργοποιημένες εξ' ορισμού σχεδόν για όλα τα συστήματα αρχείων. Χρησιμοποιήστε την nodev ρύθμιση, για να απαγορεύσετε την πρόσβαση σε συσκευές του διακομιστή.

Η ρύθμιση resvport ορίζεται στην πλευρά του πελάτη και περιορίζει την δικτυακή επικοινωνία μόνο σε δεσμευμένες πόρτες. Είναι η αντίστοιχη ρύθμιση secure, η οποία ορίζεται στην πλευρά του διακομιστή. Θέτοντας αυτή τη ρύθμιση, επιβάλλεται στο λογισμικό – πελάτη η χρήση μιας δεσμευμένης πόρτας για την επικοινωνία με το διακομιστή.

Όλες οι εκδόσεις του NFS υποστηρίζουν προσάρτηση τομών με αυθεντικοποίηση Kerberos. Η ρύθμιση του λογισμικού – πελάτη για την ενεργοποίηση της είναι: sec=krb5. Η έκδοση NFSv4 υποστηρίζει προσάρτηση με τη χρήση του krb5i, για την εξασφάλιση της ακεραιότητας και του krb5r για την προστασία της ιδιωτικότητας. Αυτές οι ρυθμίσεις εισάγονται από την πλευρά του λογισμικού πελάτη, αλλά πρέπει να ρυθμιστούν πρώτα στο διακομιστή με το withsec=krb5. Ανατρέξτε στο man page exports(5), για περισσότερες πληροφορίες.

Η τροποποίηση του αρχείου /etc(exports ή απέραντη) με μεγάλη προσοχή, έτσι ώστε να μη προστίθεται ο κενός χαρακτήρας, εκεί που δεν πρέπει. Για παράδειγμα οι παρακάτω γραμμή εξάγει τον υποφάκελο /tmp/nfs/ στον Η/Υ bob.example.com με δικαιώματα ανάγνωσης – εγγραφής.

```
/tmp/nfs/ bob.example.com(rw)
```

Η επόμενη γραμμή, από την άλλη πλευρά, εξάγει τον ίδιο φάκελο στον ίδιο Η/Υ με δικαιώματα μόνο-ανάγνωσης και σε όλα τα υπόλοιπα FQDN με δικαιώματα ανάγνωσης – εγγραφής, λόγω του επιπλέον κενού χαρακτήρα.

```
/tmp/nfs/ bob.example.com (rw)
```

Τέλος, είναι καλή πρακτική η εξέταση όλων των εξαγωγών NFS με τη χρήση της εντολής showmount:

```
~]# showmount -e <hostname>
```

Το NFSv4 είναι η εξ' ορισμού έκδοση για τον Ubuntu Server 16.04LTS και απαιτεί μόνο την πόρτα TCP 2049. Αν χρησιμοποιείτε την έκδοση NFSv3, τότε τέσσερις επιπλέον πόρτες είναι απαραίτητες, όπως εξηγείται παρακάτω.

Ρύθμιση του NFSv3 Οι πόρτες που χρησιμοποιούνται για το NFS, ορίζονται δυναμικά από το rpcbind, πρόγραμμα το οποίο μπορεί να δημιουργήσει προβλήματα κατά τον ορισμό κανόνων στο τείχος προστασίας. Για την απλοποίηση αυτής διαδικασίας, χρησιμοποιήστε τα αρχεία /etc/default/nfs-common και /etc/default/nfs-kernel-server, για να ορίσετε με στατικό τρόπο τις πόρτες των υπηρεσιών:

- Στο αρχείο /etc/default/nfs-kernel-server εισάγετε την επόμενη γραμμή για να καθορίσετε την πόρτα του rpc.mountd:

```
RPCMOUNTDOPTS="-p 32767"
```

- Στο αρχείο /etc/default/nfs-common εισάγετε την επόμενη γραμμή για να καθορίσετε την πόρτα του rpc.statd:

```
STATDOPTS="--port 32765 --outgoing-port 32766"
```

- Η πόρτα για το rpc.lockd μπορεί να ρυθμιστεί στο αρχείο /etc/modprobe.d/nfs_local.conf:

```
options lockd nlm_udpport=32768 nlm_tcpport=32768  
options nfs callback_tcpport=32764
```

Οι παραπάνω γραμμές θέτουν το rpc.lockd στην πόρτα 32768 TCP/UDP και την πόρτα του rpc.nfs-cb σε 32764.

- Τέλος, για τη ρύθμιση της πόρτας του rpc.quotad, δημιουργήστε το αρχείο /etc/default/quota και προσθέστε την ακόλουθη γραμμή:

```
RPCRQUOTADOPTS="-p 32769"
```

Οι παραπάνω πόρτες δε θα πρέπει να χρησιμοποιούνται από άλλες υπηρεσίες στο σύστημα, όπως και οι TCP/UDP πόρτα 2049 (NFS).

2.6.2 Ασφάλιση του Apache HTTP Διακομιστή

Ο διακομιστής ιστοσελίδων Apache είναι μια από τις πιο σταθερές και ασφαλείς υπηρεσίες, που διατίθενται για το Ubuntu Server 16.04LTS. Ένα μεγάλο πλήθος ρυθμίσεων και τεχνικών είναι διαθέσιμο για την ασφαλή εγκατάσταση του — αρκετά μεγάλο για να αναφερθεί εκτενώς εδώ. Παρακάτω παρατίθενται μερικές καλές πρακτικές για την ασφαλή ρύθμιση του διακομιστή Apache HTTP.

2.6.2.1 Ασφάλεια του Apache

Ολόκληρα βιβλία μπορούν να αφιερωθούν στην ασφαλή ρύθμιση του Apache. Περισσότερες πληροφορίες μπορεί να βρει κάποιος στην ιστοσελίδα <http://httpd.apache.org/>. Αρχικά, επιβεβαιώστε ότι οι υποφάκελοι των ρυθμίσεων του έχουν ως ιδιοκτήτη το χρήστη root και έχουν δικαιώματα 755:

```
~]# ls -lah /etc/apache2
total 88K
drwxr-xr-x  8 root root 4.0K Aug  5 18:26 .
drwxr-xr-x 102 root root 4.0K Aug  6 01:20 ..
-rw-r--r--  1 root root 7.0K Mar 19 11:48 apache2.conf
drwxr-xr-x  2 root root 4.0K Aug  5 18:26 conf-available
drwxr-xr-x  2 root root 4.0K Aug  5 18:26 conf-enabled
-rw-r--r--  1 root root 1.8K Mar 19 11:48 envvars
-rw-r--r--  1 root root 31K Mar 19 11:48 magic
drwxr-xr-x  2 root root 12K Aug  5 18:26 mods-available
drwxr-xr-x  2 root root 4.0K Aug  5 18:26 mods-enabled
-rw-r--r--  1 root root 320 Mar 19 11:48 ports.conf
drwxr-xr-x  2 root root 4.0K Aug  5 18:26 sites-available
drwxr-xr-x  2 root root 4.0K Aug  5 18:26 sites-enabled

~]# ls -lah /usr/sbin/*apache*
-rwxr-xr-x 1 root root 631K Jul 15 18:33 /usr/sbin/apache2
-rwxr-xr-x 1 root root 6.3K Mar 19 11:48 /usr/sbin/apache2ctl
lrwxrwxrwx 1 root root    10 Jul 15 18:33 /usr/sbin/apachectl ->
apache2ctl
```

Κατά τον ίδιο τρόπο το εκτελέσιμο αρχείο apache2 θα πρέπει να έχει ιδιοκτήτη το χρήστη root και να έχει δικαιώματα 511.

2.6.2.2 Καθορισμός Ρυθμίσεων

Πρέπει πάντα να επιβεβαιώνετε ότι μόνο ο χρήστης root έχει δικαιώματα εγγραφής τους υποφακέλους, οι οποίοι περιέχουν scripts - CGIs. Για να το επιτύχετε αυτό εκτελέστε τις εξής εντολές:

```
~]# chown root <directory_name>
~]# chmod 755 <directory_name>
```

Καλό είναι να ρυθμίσετε την υπηρεσία, ώστε να εκτελείται σε διαφορετική πόρτα από την συνήθη. Τροποποιείστε το αρχείο /etc/apache2/apache2.conf ως root. Ορίστε τη ρύθμιση 'Listen' σε μια άλλη πόρτα εκτός των 80 και 443. Σε αυτό το παράδειγμα, ο apache είναι ρυθμισμένος να δέχεται συνδέσεις στην πόρτα 12345:

```
Listen 127.0.0.1:12345
```

Ο διαχειριστής συστήματος θα πρέπει να είναι προσεκτικός, όταν ορίζει τις παρακάτω ρυθμίσεις στο αρχείο /etc/apache2/apache2.conf:

FollowSymLinks Αυτή η ρύθμιση είναι ενεργοποιημένη εξ' ορισμού, για αυτό το λόγο να είστε προσεκτικοί όταν δημιουργείτε symbolic links στο document root του διαχομιστή. Για παράδειγμα είναι κακή ιδέα η δημιουργία ενός συμβολικού δείκτη στο /.

Indexes Αυτή η ρύθμιση είναι ενεργοποιημένη εξ' ορισμού, αλλά μπορεί να μην είναι επιθυμητή. Για να αποτρέψετε τους επισκέπτες από το να βλέπουν τα αρχεία εντός στο διαχομιστή, απενεργοποιήστε αυτή τη ρύθμιση.

UserDir Αυτή η ρύθμιση είναι απενεργοποιημένη εξ' ορισμού, καθώς μπορεί να επιβεβαιώσει την παρουσία ενός λογαριασμού στο σύστημα. Παρόλα αυτά, εάν επιθυμείτε να ενεργοποιήσετε αυτή την ρύθμιση, παραμετροποιήστε τις παρακάτω επιλογές:

```
UserDir enabled  
UserDir disabled root
```

Οι παραπάνω παράμετροι ενεργοποιούν την πρόσβαση στο φάκελο χρήστη για όλους τους χρήστες πλην του /root/. Για να προσθέσετε χρήστες στη λίστα των απενεργοποιημένων λογαριασμών, προσθέστε μια λίστα, χωρισμένη με κενούς χαρακτήρες, στη γραμμή UserDir disabled.

ServerTokens Η ρύθμιση αυτή καθορίζει την απάντηση που στέλνει ο διαχομιστής στους πελάτες [9]. Περιλαμβάνει διάφορες πληροφορίες, οι οποίες μπορούν να ρυθμιστούν με τη χρήση των παρακάτω επιλογών:

- ServerTokens Full (εξ' ορισμού επιλογή) — επιστρέφει όλες τις διαθέσιμες πληροφορίες (πληροφορίες για το ΛΣ και τα ενεργοποιημένα αριθμάτα), για παράδειγμα:

Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2

- ServerTokens Prod ή ServerTokens ProductOnly — επιστρέφει μόνο τις ακόλουθες πληροφορίες:

Apache

- ServerTokens Major — επιστρέφει τις ακόλουθες πληροφορίες:

Apache/2

- ServerTokens Minor — επιστρέφει τις ακόλουθες πληροφορίες:

Apache/2.0

- ServerTokens Min ή ServerTokens Minimal — επιστρέφει τις ακόλουθες πληροφορίες:

Apache/2.0.41

- ServerTokens OS — επιστρέφει τις ακόλουθες πληροφορίες:

Apache/2.0.41 (Unix)

Συνίσταται η χρήση της επιλογής ServerTokens Prod, έτσι ώστε ο επιτιθέμενος να μην είναι σε θέση να συγκεντρώσει πολύτιμες πληροφορίες για το σύστημα.

htaccess Για να αποτρέψετε τους χρήστες από το να δημιουργήσουν αρχεία .htaccess, τα οποία παρακάμπτουν τις ρυθμίσεις ασφαλείας του διαχομιστή, προσθέστε την παρακάτω ρύθμιση στο αρχείο ρυθμίσεων του apache:

```
<Directory />
AllowOverride None
</Directory>
```

Για να αποτρέψετε τους χρήστες από το να έχουν πρόσβαση στο σύστημα αρχείων του διαχομιστή (ακόμα και στο root directory), προσθέστε τις παρακάτω γραμμές στο αρχείο ρυθμίσεων του apache:

```
<Directory />
    Order Deny,Allow
    Deny from all
</Directory>
```

Για να επιτρέψετε την πρόσβαση σε συγκεκριμένους φακέλους:

```
<Directory /usr/users/*/public\_html>
    Order Deny,Allow
    Allow from all
</Directory>
<Directory /usr/local/httpd>
    Order Deny,Allow
    Allow from all
</Directory>
```

IncludesNoExec Είναι καλό να μην αφαιρείται η επιλογή IncludesNoExec. Είναι ενεργοποιημένη εξ' ορισμού, ώστε το άρθρωμα Server-Side Includes (SSI) να μη μπορεί να εκτελέσει εντολές. Συνιστάται να μην αλλάζετε αυτή τη ρύθμιση, εκτός αν είναι απολύτως απαραίτητο, καθώς θα μπορούσε δυνητικά να επιστρέψει σε ένα επιτιθέμενο να εκτελέσει εντολές στο σύστημα. Τα Server-Side Includes (SSI) θέτουν ζητήματα ασφαλείας, καθώς δίνουν τη δυνατότητα εκτέλεσης CGI script και προγραμμάτων στο σύστημα, με τα δικαιώματα του χρήστη που εκτελείται η υπηρεσία apache2. Για να απενεργοποιήσετε την δυνατότητα των SSI σελίδων να εκτελούν προγράμματα, βεβαιωθείτε ότι η ρύθμιση IncludesNOEXEC και όχι η Includes είναι ενεργοποιημένη. Μπορεί να χρησιμοποιηθεί η επιλογή <--#include virtual="..."--> για να εκτελούνται CGI scripts εφόσον αυτά βρίσκονται σε φακέλους, που έχουν οριστεί με την επιλογή ScriptAlias. Ο περιορισμός της εκτέλεσης CGI scripts που βρίσκονται μόνο σε συγκεκριμένους φακέλους, δίνει περισσότερο έλεγχο πάνω στο ποια CGI scripts μπορούν να εκτελεστούν.

2.6.2.3 Απενεργοποίηση Αχρησιμοποίητων Αρθρωμάτων Apache2

Σε ορισμένες περιπτώσεις είναι καλό να απενεργοποιούνται αρθρώματα (modules) του apache, τα οποία δε χρησιμοποιούνται. Για να οριστεί η παραπάνω ρύθμιση, τοποθετήστε ένα σημείο σχολίου (#) μπροστά από την αντίστοιχη γραμμή στο αρχείο /etc/apache2/apache2.conf. Για παράδειγμα, για να απενεργοποιήσουμε το mod_proxy:

```
#LoadModule proxy_module modules/mod_proxy.so
```

Ας σημειωθεί ότι στον υποφάκελο /etc/apache2/conf-available υπάρχουν αρχεία ρυθμίσεων, τα οποία μπορούν να ενεργοποιήσουν αρθρώματα.

2.6.2.4 Ενεργοποίηση του Αρθρώματος mod_security

Το άρθρωμα mod_security είναι διαθέσιμο σε όλες τις εκδόσεις του apache και ενισχύει την ασφάλεια με την παροχή επιπλέον επιλογών στο αρχείο apache2.conf. Οι επιλογές αυτές επιτρέπουν το φιλτράρισμα / έλεγχο της δικτυακής κίνησης, που προέρχεται είτε από στατικές είτε από δυναμικές σελίδες. Μπορεί να ρυθμιστεί μια απάντηση για κάθε ανάκτηση δεδομένων από τον πελάτη, η οποία εμπίπτει σε κάποιον κανόνα ελέγχου. Μπορούν επίσης να ρυθμιστούν επιτρεπόμενοι χαρακτήρες ASCII η τύποι αρχείων που ανεβαίνουν στο διαχομιστή από τους πελάτες. Το άρθρωμα mod_security παρέχει επίσης εκτεταμένες δυνατότητες καταγραφής συμβάντων. Για περισσότερες πληροφορίες ανατρέξτε στο <http://www.modsecurity.org>.

Για να ενεργοποιηθεί το άρθρωμα:

```
~]# apt-get install libapache2-mod-security2  
~]# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/  
modsecurity.conf
```

Είναι αναγκαίο να εγκατασταθεί το τελευταίο σύνολο κανόνων ModSecurity OWASP από την αντίστοιχη ιστοσελίδα και να ενεργοποιήθει το εξ' ορισμού αρχείο ρυθμίσεων modsecurity_crs_10_setup.conf.example.

```
~]# wget -O SpiderLabs-owasp-modsecurity-crs.tar.gz \  
https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master  
~]# mv /etc/modsecurity/modsecurity_crs_10_setup.conf.example \  
/etc/modsecurity/modsecurity_crs_10_setup.conf  
~]# cp -R SpiderLabs-owasp-modsecurity-crs-*/* /etc/modsecurity/  
  
~]# cd /etc/modsecurity/base_rules  
~]# for f in * ; do sudo ln -s /etc/modsecurity/base_rules/$f /etc/  
modsecurity/activated_rules/$f ; done  
~]# cd /etc/modsecurity/optional_rules  
~]# for f in * ; do sudo ln -s /etc/modsecurity/optional_rules/$f /etc  
/modsecurity/activated_rules/$f ; done
```

Ενεργοποιούμε το άρθρωμα και επανεκκινούμε την υπηρεσία Apache.

```
~]# a2enmod security2  
~]# service apache2 restart
```

2.6.2.5 Ενεργοποίηση του Αρθρώματος mod_evasive

Το άρθρωμα mod_evasive προσφέρει δυνατότητες αντίδρασης και διαφυγής από μια διεξαγώμενη επίθεση HTTP DoS ή brute force. Είναι επίσης σχεδιασμένο να ανιχνεύει την ύποπτη κίνηση και να επικοινωνεί με τείχη προστασίας, δρομολογητές και άλλες δικτυακές συσκευές. Το άρθρωμα mod_evasive είναι σε θέση να ενημερώνει τόσο μέσω email, όσο και μέσω υποδομής syslog. Για την εγκατάστασή του πληκτρολογούμε:

```
~]# apt-get install libapache2-mod-evasive  
~]# mkdir /var/log/mod_evasive  
~]# chown www-data:www-data /var/log/mod_evasive/
```

Έπειτα, ρυθμίζουμε το άρθρωμα

```
~]# cat > /etc/apache2/mods-available/mod-evasive.conf << EOF
<ifmodule mod_evasive20.c>
    DOSHashTableSize 3097
    DOSPageCount 2
    DOSSiteCount 50
    DOSPageInterval 1
    DOSSiteInterval 1
    DOSBlockingPeriod 10
    DOSLogDir /var/log/mod_evasive
    DOSEmailNotify root@localhost
    DOSWhitelist 127.0.0.1
</ifmodule>
EOF
```

Τέλος, ενεργοποιούμε και επανεκκινούμε την υπηρεσία Apache

```
~]# a2enmod evasive
~]# service apache2 restart
```

2.6.2.6 Συνιστώμενα Πρωτόκολλα Κρυπτογράφησης

Θα πρέπει να χρησιμοποιείτε το HTTPS αντί για το παλαιότερο HTTP, όταν είναι απαραίτητο να διαχινηθεί διαβαθμισμένη πληροφορία μεταξύ πελάτη - διακομιστή, όπως κωδικοί πρόσβασης. Παρατίθενται στη συνέχεια, ορισμένες συμβουλές για την επιλογή των πρωτοκόλλων κρυπτογράφησης.

- SSL v2 Να μη χρησιμοποιείται, έχει σοβαρά κενά ασφαλείας.
- SSL v3 Να μη χρησιμοποιείται, έχει σοβαρά κενά ασφαλείας.
- TLS v1.0 Χρησιμοποιήστε μόνο για λόγους διαλειτουργικότητας. Έχει γνωστά κενά ασφαλείας, τα οποία δεν μπορούν να αντιμετωπιστούν με τρόπο ο οποίος να εξασφαλίζει τη διαλειτουργικότητα και έτσι είναι εξ' ορισμού ευάλωτο. Δεν υποστηρίζει τα σύγχρονα πακέτα κρυπτογράφησης (cipher suites).
- TLS v1.1 Χρησιμοποιήστε μόνο για λόγους διαλειτουργικότητας. Έχει γνωστά κενά ασφαλείας, τα οποία δεν μπορούν να αντιμετωπιστούν με τρόπο ο οποίος να εξασφαλίζει τη διαλειτουργικότητα και έτσι είναι εξ' ορισμού ευάλωτο. Δεν υποστηρίζει τα σύγχρονα πακέτα κρυπτογράφησης (cipher suites).
- TLS v1.2 Συνιστώμενη έκδοση, υποστηρίζει όλα τα σύγχρονα πακέτα κρυπτογράφησης (cipher suites).

Ο Apache μπορεί να χρησιμοποιήσει είτε OpenSSL είτε NSS βιβλιοθήκες για την κρυπτογράφηση TLS. Ανάλογα με την επιλογή βιβλιοθήκης, τα αρθρώματα mod_ssl ή mod_nss πρέπει να εγκατασταθούν. Για παράδειγμα, για την εγκατάσταση του OpenSSL αρθρώματος mod_nss πληκτρολογήστε τα παρακάτω ως υπερχρήστης:

```
~]# apt-get install libapache2-mod-nss
```

Το πακέτο mod_ssl εγκαθιστά το αρχείο ρυθμίσεων /etc/apache2/mods-available/ssl.conf, το οποίο είναι δυνατό να χρησιμοποιηθεί για να καθορίσει τις TLS ρυθμίσεις του Apache. Κατά τον ίδιο τρόπο, το πακέτο mod_nss εγκαθιστά το /etc/apache2/mods-available/nss.conf αρχείο ρυθμίσεων.

Κατά την τροποποίηση των επιλογών στο αρχείο etc/apache2/mods-available/ssl.conf, βεβαιωθείτε ότι οι επόμενες επιλογές είναι ενεργοποιημένες κατ'ελάχιστο:

- SSLProtocol Καθορίζει την έκδοση του TLS (ή SSL) που επιτρέπεται.
- SSLCipherSuite Καθορίζει το επιθυμητό πακέτο κρυπτογράφησης ή απενεργοποιεί τα μη επιθυμητά.
- SSLHonorCipherOrder Επιβάλει στους πελάτες να χρησιμοποιούν τα πακέτα κρυπτογράφησης με τη σειρά προτίμησης, όπως αυτά ορίστηκαν παραπάνω. Για παράδειγμα:

```
SSLProtocol all -SSLv2 -SSLv3 SSLCipherSuite HIGH:!aNULL:!MD5
```

```
SSLHonorCipherOrder on
```

Να σημειωθεί ότι οι παραπάνω ρυθμίσεις είναι οι ελάχιστα απαραίτητες.

Για να καθορίσετε τον τρόπο λειτουργίας του mod_nss module, τροποποιήστε το ακόλουθο αρχείο ρυθμίσεων: etc/apache2/mods-available/nss.conf. Το άρθρωμα mod_nss προέρχεται από το mod_ssl και έτσι μοιράζεται πολλά κοινά στοιχεία με αυτό, όπως τις διαθέσιμες επιλογές στο αρχείο ρυθμίσεων. Η διαφορά είναι ότι στο mod_nss οι ρυθμίσεις έχουν πρόθεμα του NSS αντί για του SSL.

2.6.2.7 Χρήση του fail2ban

Η ασφάλεια του Apache μπορεί να ενισχυθεί περαιτέρω με τη χρήση του fail2ban. Για ένα παράδειγμα ρύθμισης του fail2ban για μια υπηρεσία (εν προκειμένω αυτή του SSH), δείτε το επόμενο τμήμα.

2.6.3 Ασφάλιση του SSH

Το SSH είναι ένα ισχυρό δικτυακό πρωτόκολλο, το οποίο χρησιμοποιείται για την επικοινωνία με ένα σύστημα μέσω ενός ασφαλούς καναλιού. Για να ενεργοποιηθεί η χρήση κρυπτογραφημένων κλειδιών για την αυθεντικοποίηση, πρέπει η επιλογή PubkeyAuthentication στο αρχείο /etc/ssh/sshd_config να είναι 'yes' [7]. Αυτή είναι η εξ' ορισμού ρύθμιση. Θέστε την επιλογή PasswordAuthentication σε 'no' για να απενεργοποιήσετε εντελώς τη χρήση των κωδικών για αυθεντικοποίηση. Μπορούμε να δημιουργήσουμε δημόσια κλειδιά για τη χρήση ssh, ως εξής:

```
~] $ ssh-keygen -t rsa
```

Η χρήση πολλαπλών μεθόδων αυθεντικοποίησης, ή multi-factor, αυξάνει το επίπεδο της προστασίας ενάντια σε μη εξουσιοδοτημένη πρόσβαση και θα πρέπει να εφαρμόζεται κατά την ενίσχυση της ασφαλείας ενός συστήματος, ώστε να αποτραπεί πιθανή μη εξουσιοδοτημένη πρόσβαση. Χρήστες οι οποίοι προσπαθούν να εισέλθουν στο σύστημα θα πρέπει να ολοκληρώσουν επιτυχώς όλες τις διαδικασίες αυθεντικοποίησης.

```
AuthenticationMethods publickey,gssapi-with-mic publickey,keyboard-interactive
```

Η υπηρεσία sshd η οποία έχει ρυθμιστεί με τις παραπάνω επιλογές AuthenticationMethods στο αρχείο /etc/ssh/sshd_config, επιτρέπει την είσοδο στο σύστημα μόνο όταν ο χρήστης ολοκληρώσει με επιτυχία τη διαδικασία αυθεντικοποίησης με δημόσιο κλειδί με gssapi-with-mic ή με εισαγωγή κωδικού χρήστη [1]. Οι χρήστες καλό είναι να χρησιμοποιούν το πρωτόκολλο SSH-2, καθότι παρέχει πιο ασφαλείς διαδικασίες αυθεντικοποίησης και επικοινωνίας. Επίσης, η χρήση ECDSA (Elliptic Curve Digital Signature Algorithm) προσφέρει καλύτερη απόδοση στο ίδιο μήκος συμμετρικού κλειδιού. Επίσης παράγει κλειδιά μικρότερου μήκους.

Συνίσταται, επίσης, η αλλαγή της πόρτας στην οποία δέχεται συνδέσεις η υπηρεσία, τροποποιώντας την κατάλληλη εγγραφή στο αρχείο /etc/ssh/sshd_config:

```
Listen :12345
```

Σε αυτό το σημείο πρέπει να τονιστεί ότι, η απενεργοποίηση ή κλείδωμα ενός λογαριασμού δεν αποτρέπει τον χρήστη από το να εισέλθει στο σύστημα απομακρυσμένα, εφόσον έχει ρυθμίσει αυθεντικοποίηση RSA με δημόσιο κλειδί. Για αυτό το λόγο θα πρέπει να ελέγχεται ο υποφάκελος του χρήστη για αρχεία τα οποία επιτρέπουν αυτόν τον τρόπο αυθεντικοπίησης, όπως το .ssh/authorized_keys.

Πρέπει να υφίσταται περιορισμός των χρηστών που μπορούν να λάβουν πρόσβαση SSH. Για παράδειγμα οι χρήστες που είναι αναγκαίο να έχουν πρόσβαση, είναι καλό να ανήκουν σε μια ομάδα που ονομάζεται 'sshlogin'. Η ομάδα αυτή στη συνέχεια θα πρέπει να είναι στην μεταβλητή AllowGroups στο αρχείο /etc/ssh/sshd_config. Μια άλλη λύση είναι να επιτρέπεται μόνο στους sudoers να χρησιμοποιούν απομακρυσμένη πρόσβαση.

```
AllowGroups sudo, sshlogin
```

Προσθήκη των επιτρεπόμενων χρηστών στην ομάδα 'sshlogin' και επανεκκίνηση της υπηρεσίας.

```
~]# sudo adduser username sshlogin  
~]# sudo systemctl restart sshd
```

Για την απενεργοποίηση των root logins απενεργοποιούμε την αντίστοιχη επιλογή στο αρχείο ρυθμίσεων, /etc/ssh/sshd_config:

```
PermitRootLogin no
```

Για περαιτέρω ασφάλεια, η υπηρεσία είναι δυνατό να εκτελείται σε περιβάλλον sandbox:

```
UsePrivilegeSeparation sandbox
```

Καλό είναι να απενεργοποιείται το X Forwarding για το ssh. Κατά αυτόν τον τρόπο δε μπορεί ένας κακόβουλος χρήστης να εκτελέσει προγράμματα X στο σύστημα. Αυτό έχει εφαρμογή περισσότερο σε εγκαταστάσεις desktop:

```
X11Forwarding no
```

To script το οποίο συνοδεύει το παρόν κείμενο (βλ. Κεφ. 4) ρυθμίζει πληθώρα άλλων επιλογών, όπως ενεργοποιημένα ciphers, μέγιστο πλήθος αποτυχημένων προσπαθειών αυθεντικοποίησης, ταυτόχρονων συνεδριών κ.α.

Η ασφάλεια του SSH μπορεί να ενισχυθεί περαιτέρω με τη χρήση του fail2ban. Τροποποιήστε το αρχείο ρυθμίσεων /etc/fail2ban/jail.local και ενεργοποιήστε τους απαραίτητους κανόνες:

```
~]# cat >> /etc/fail2ban/jail.local << EOF  
[ssh]
```

```
enabled  = true  
port     = ssh  
filter   = sshd  
logpath  = /var/log/auth.log  
maxretry = 3  
EOF
```

τέλος επανεκκινήστε την υπηρεσία:

```
~]# service fail2ban restart
```

2.6.4 Ασφαλής Ρύθμιση του SAMBA

To Samba είναι ένα σημαντικό εργαλείο για την ενσωμάτωση των Linux Servers - Desktops σε ένα Active Directory (AD) περιβάλλον. Η υπηρεσία αυτή μπορεί να λειτουργήσει τόσο ως domain controller (NT4-style) ή ως ένας αυτόνομος domain member (AD ή NT4-style) [2]. To Samba αποτελείται από τρεις υπηρεσίες - daemons (smbd, nmbd, and winbinddd). Αυτές οι τρεις υπηρεσίες καθορίζουν τον τρόπο λειτουργίας του SAMBA. Και οι τρεις αυτές υπηρεσίες έχουν ξεχωριστά script εκκίνησης.

Δύο είναι οι τρόποι λειτουργίας για το Samba, share-level και user-level, οι οποίοι είναι κοινώς γνωστοί ως επίπεδα ασφαλείας. To Share-level επίπεδο ασφαλείας είναι ξεπερασμένο και έχει αφαιρεθεί από τις νεότερες εκδόσεις του λογισμικού. To User-level επίπεδο ασφαλείας είναι το εξ' ορισμού ενεργοποιημένο και συνιστώμενο επίπεδο. Ακόμα και αν η παράμετρος 'security=user' δεν περιέχεται στο αρχείο ρυθμίσεων /etc/samba/smb.conf, ενεργοποιείται αυτόματα.

Σε επίπεδο ασφαλείας domain (user-level), ο διακομιστής Samba έχει ένα λογαριασμό στο επίπεδο της μηχανής (domain security trust account) και αναδρομολογεί όλες τις αιτήσεις αυθεντικοποίησης μέσα από τους domain controllers. Ο εξυπηρετητής Samba γίνεται member server του domain με τη χρήση των παρακάτω επιλογών στο αρχείο ρυθμίσεων /etc/samba/smb.conf:

```
[GLOBAL]  
security = domain  
workgroup = MARKETING
```

Αν υπάρχει έτοιμο περιβάλλον Active Directory, τότε είναι προτιμητέο να γίνει, ο εξυπηρετητής Samba, μέλος σε αυτό.

```
[GLOBAL]  
security = ADS  
realm = EXAMPLE.COM  
password server = kerberos.example.com
```

Στο επίπεδο ασφαλείας share-level, ο εξυπηρετητής δέχεται κατά τη διαδικασία της αυθεντικοποίησης, μόνο ένα κωδικό πρόσβασης από τον πελάτη, χωρίς ένα καθορισμένο όνομα χρήστη. Σε αυτή την περίπτωση, αναμένει για κάθισε εξαγόμενο σύστημα αρχείων (share) ένα κωδικό πρόσβασης, ανεξάρτητα από όνομα χρήστη. Εάν είναι αναγκαίο να χρησιμοποιήσετε αυτό το επίπεδο ασφαλείας μην ορίζετε την παράμετρο security = share αλλά τροποποιήστε το αρχείο ρυθμίσεων /etc/samba/smb.conf, όπως παρακάτω [2]:

```

[GLOBAL]
security = user
map to guest = Bad User
username map = /etc/samba/smbusers

[SHARE]
guest ok = yes

```

Πρέπει επίσης να τροποποιήσετε το αρχείο /etc/samba/smbusers όπως παρακάτω:

```

nobody = guest.

```

2.7 Ασφαλής Ρύθμιση της Δικτυακής Πρόσβασης

2.7.1 Ασφάλεια Διαφόρων Παραμέτρων του Δικτύου

Στα επόμενα τμήματα περιγράφονται με αδρές γραμμές, ζητήματα ασφαλείας που αφορούν την δικτυακή πρόσβαση.

Απενεργοποίηση Source Routing To Source routing είναι ένας μηχανισμός του διαδικτύου, ο οποίος επιτρέπει σε ένα πακέτο να μεταφέρει μια λίστα διευθύνσεων IP, η οποία ενημερώνει τον δρομολογητή για την διαδρομή που θα πρέπει να ακολουθήσει το πακέτο. Υπάρχει επίσης, η επιλογή της καταγραφής των IP (hops) που διασχίσει το πακέτο κατά τη διαδρομή του. Η λίστα των διασχισμάτων IP, το "route record", παρέχει την διεύθυνση προορισμού και πληροφορίες για τη διαδρομή επιστροφής. Αυτό επιτρέπει στην αφετηρία (source) να καθορίσει τη διαδρομή που θα ακολουθήσει το πακέτο (απόλυτα ή πιο ελεύθερα), αγνοώντας τους πίνακες δρομολόγησης των ενδιάμεσων δρομολογητών. Αυτό επιτρέπει την αναδρομολόγηση της δικτυακής κίνησης από τους κακόβουλους χρήστες. Για αυτό το λόγο θα πρέπει η παραπάνω δυνατότητα να απενεργοποιείται.

Η επιλογή accept_source_route καθορίζει τις δικτυακές διεπαφές (network interfaces) ώστε να δέχονται πακέτα με ενεργοποιημένη την παράμετρο Strict Source Route (SSR) ή Loose Source Routing (LSR). Η παραμετροποίησή της, γίνεται μέσω του sysctl. Εκτελέστε την παρακάτω εντολή ως χρήστης root, ώστε να απορίπτονται τα πακέτα που έχουν ενεργοποιημένο SSR ή LSR:

```
~]# /sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0
```

Σε συνέχεια των παραπάνω ενεργειών, θα πρέπει να απενεργοποιείται και το packet forwarding, όταν αυτό είναι εφικτό (η επέμβαση αυτή μπορεί βέβαια να έχει αντίκτυπο στο virtualization). Οι παρακάτω εντολές απενεργοποιούν το forwarding για IPv4 και IPv6 πακέτα σε όλες τις δικτυακές διεπαφές:

```
~]# /sbin/sysctl -w net.ipv4.conf.all.forwarding=0
~]# /sbin/sysctl -w net.ipv6.conf.all.forwarding=0
```

Επίσης, οι εξής εντολές απενεργοποιούν το forwarding για τα πακέτα multicast σε όλες τις δικτυακές διεπαφές:

```
~]# /sbin/sysctl -w net.ipv4.conf.all.mc_forwarding=0  
~]# /sbin/sysctl -w net.ipv6.conf.all.mc_forwarding=0
```

Η αποδοχή ICMP redirects έχει ελάχιστες χρήσιμες εφαρμογές. Γι' αυτό είναι καλό να απενεργοποιούνται, εκτός αν είναι απολύτως αναγκαίο. Οι εξής εντολές απενεργοποιούν την αποδοχή για όλα τα ICMP redirected πακέτα σε όλες τις δικτυακές διεπαφές.

```
~]# /sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0  
~]# /sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0
```

Η εξής εντολή απενεργοποιεί την αποδοχή για όλα τα secure ICMP redirected πακέτα σε όλες τις δικτυακές διεπαφές.

```
~]# /sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0
```

Η εξής εντολή απενεργοποιεί την αποστολή για όλα τα ICMP redirected πακέτα σε όλες τις δικτυακές διεπαφές.

```
~]# /sbin/sysctl -w net.ipv4.conf.all.send_redirects=0
```

Απενεργοποίηση του Reverse Path Forwarding To Reverse Path Forwarding χρησιμοποιείται για να αποτρέψει πακέτα τα οποία εισήλθαν από μια δικτυακή διεπαφή (interface) να εξέλθουν μέσω μιας άλλης. Η κατάσταση κατά την οποία οι δρομολογήσεις εισόδου / εξόδου (outgoing / incoming routes) είναι διαφορετικές, καλείται ασύμμετρη δρομολόγηση (asymmetric routing). Οι δρομολογητές συχνά χρησιμοποιούν αυτό τον τύπο δρομολόγησης, αλλά οι περισσότεροι Η/Υ συνήθως δε χρειάζεται να το κάνουν. Περιπτώσεις στις οποίες μπορεί να χρησιμοποιείται αυτός ο τρόπος δρομολόγησης είναι, σε εφαρμογές οι οποίες στέλνουν δικτυακή κίνηση από μια δικτυακή συσκευή και δέχονται κίνηση από μία άλλη, η οποία επικοινωνεί με διαφορετικό service provider. Παραδείγματα τέτοιων περιπτώσεων είναι οι συνδυασμοί DSL με leased lines ή δορυφορικές συνδέσεις με 3G. Εάν αυτό το σενάριο δεν ανταποκρίνεται στην πραγματικότητα, όσον αφορά μια υποδομή, τότε η ενεργοποίηση του reverse path forwarding στη δικτυακή διεπαφή εισόδου είναι απαραίτητη. Εν ολίγοις, εκτός εάν γνωρίζετε ότι η λειτουργία αυτή δεν είναι απαραίτητη, πρέπει να ενεργοποιείται καθώς αποτρέπει τους χρήστες να πλαστογραφούν διευθύνσεις από διάφορα υποδίκτυα (IP spoofing) και μειώνει την πιθανότητα DDoS επιθέσεων.

Το Reverse Path Forwarding ενεργοποιείται με τη χρήση της παραμέτρου rp_filter. Το sysctl μπορεί να χρησιμοποιηθεί για να αλλάξει τις ρυθμίσεις αυτές προσωρινά, ενώ η μόνιμη αλλαγή αποθηκεύεται με την εγγραφή στο αρχείο /etc/sysctl.conf. Η παραμέτρος rp_filter χρησιμοποιείται για να θέσει στον πυρήνα του ΛΣ έναν από τους παρακάτω τρόπους λειτουργίας.

```
~]# sysctl -w net.ipv4.conf.default.rp_filter=integer  
~]# sysctl -w net.ipv4.conf.all.rp_filter=integer
```

όπου integer είναι ένας από τους παρακάτω:

- 0 — No source validation.
- 1 — Strict mode / RFC 3704.
- 2 — Loose mode / RFC 3704.

Η ρύθμιση αυτή μπορεί να γίνει και κατά διεπαφή:

```
~]# sysctl -w net.ipv4.conf.interface.rp_filter=integer
```

Για να θέσετε μόνιμα αυτές τις αλλαγές, τροποποιήστε το αρχείο /etc/sysctl.conf.
Για παράδειγμα, εισάγετε στο αρχείο αυτό τη γραμμή:

```
net.ipv4.conf.all.rp_filter=1
```

Απενεργοποίηση του Zeroconf Networking Το Zeroconf καθορίζει την διεύθυνση την οποία θα λάβει ο Η/Υ, εφόσον δεν καταφέρει να λάβει μια μέσω DHCP. Σε αυτή την περίπτωση, η διεπαφή θα λάβει μια διεύθυνση στο υποδίκτυο 169.254.0.0. Για να απενεργοποιήσετε την παραπάνω λειτουργία, εκτελέστε τις εξής εντολές [3]:

```
~]# apt-get purge avahi-autoipd
```

Αγνόηση των πακέτων ICMP - Broadcast Request - Martian Packets Προσθέστε την ακόλουθη γραμμή στο αρχείο /etc/sysctl.conf για να εξαναγκάσετε το ΛΣ να αγνοεί τα ping ή τα broadcast requests:

- Αγνόηση ICMP request:

```
net.ipv4.icmp_echo_ignore_all = 1
```

- Αγνόηση Broadcast request:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

- Καταγραφή πακέτων από μη ορθές ή μη αναμενόμενες διευθύνσεις (Martian Packets / Un-routable Source Addresses):

```
net.ipv4.conf.all.log_martians = 1
```

Απενεργοποίηση πρωτοκόλλου IPv6 Εάν δεν χρησιμοποιείτε το IPv6 τότε είναι καλό να απενεργοποιείτε, καθώς οι περισσότερες υπηρεσίες εντός DMZ δεν το χρησιμοποιούν και συνήθως είναι ελλιπής ο έλεγχος του μέσω των τειχών προστασίας. Ανοίξτε το αρχείο /etc/modprobe.d/disablenet.conf και προσθέστε την επιλογή:

```
ipv6 disable=1
```

Απενεργοποιείστε το IPv6 μέσω sysctl για όλες τις διεπαφές, τροποποιώντας το αρχείο /etc/sysctl.conf [6].

```
net.ipv6.conf.all.disable_ipv6 = 1  
net.ipv6.conf.default.disable_ipv6 = 1  
net.ipv6.conf.lo.disable_ipv6 = 1
```

Τέλος, απενεργοποιείστε το IPv6 στον πυρήνα του ΛΣ. Τροποποιήστε το αρχείο /etc/default/grub και προσθέστε ipv6.disable=1 στη γραμμή που καθορίζει τις παραμέτρους φόρτωσης του πυρήνα (GRUB_CMDLINE_LINUX_DEFAULT). Τέλος ενημερώστε το grub με τις αλλαγές, όπως παρακάτω:

```
~]# update-grub
```

Απενεργοποίηση του RPC IPv6 Οι υπηρεσίες RPC, όπως το NFS, επιχειρούν να εκκινήσουν χρησιμοποιώντας το IPv6 ακόμα και αν αυτό ειναι απενεργοποιημένο στο /etc/modprobe.d [3]. Για να εμποδίσετε αυτή τη συμπεριφορά, τροποποιήστε το αρχείο /etc/netconfig και τοποθετήστε ένα σημείο σχολίου (#) μπροστά από τις εξής γραμμές:

```
#udp6      tpi_clts      v      inet6      udp      -      -
#tcp6      tpi_cots_ord  v      inet6      tcp      -      -
```

2.7.2 Ασφάλιση του DNS με το DNSSEC

Το DNSSEC είναι μια προσθήκη ασφαλείας για το DNS (Domain Name System Security Extensions, DNSSEC), η οποία δίνει τη δυνατότητα σε ένα πελάτη της υπηρεσίας DNS, να αυθεντικοποιεί και να ελέγχει την ακεραιότητα των απαντήσεων του διαχομιστή DNS, με απώτερο σκοπό να επιβεβαιώσει την προέλευσή τους και να διαπιστώσει εάν έχουν αλλοιωθεί κατά την μετάβασή τους. Η ενεργοποίηση του DNSSEC γίνεται ως εξής:

```
~]# apt-get install unbound
~]# systemctl enable unbound
~]# systemctl start unbound
```

Ο unbound daemon επιτρέπει την ρύθμιση των τοπικών δεδομένων dns cache, καθώς και των στατικών αντιστοιχίσεων dns, χρησιμοποιώντας τους εξής υποφάκελους:

- Ο /etc/unbound/conf.d χρησιμοποιείται για να προσθέσει παραμέτρους για ένα συγκεκριμένο domain name. Αυτό χρησιμοποιείται για την ανακατεύθυνση αιτήσεων DNS, που αφορούν συγκεκριμένο domain name, σε συγκεκριμένο διαχομιστή. Η ανακατεύθυνση αυτή βρίσκει εφαρμογή σε sub-domains, τα οποία βρίσκονται μόνο εντός ενός εσωτερικού δικτύου (corporate WAN).
- Ο υποφάκελος /etc/unbound/keys.d χρησιμοποιείται για την προσθήκη trust anchors σε ένα domain name. Αυτό απαιτείται όταν ένα εσωτερικό domain name είναι υπογεγραμμένο ψηφιακά από το DNSSEC, αλλά δεν υπάρχει εγγραφή στους δημόσιους DNS διακομιστές, ώστε να δημιουργηθεί το απαραίτητο μονοπάτι εμπιστοσύνης. Άλλη μια περίπτωση στην οποία χρησιμοποιείται, είναι όταν το εσωτερικό domain name είναι υπογεγραμμένο με διαφορετικό DNSKEY από το αντίστοιχο domain name, που είναι δημοσίως γνωστό εκτός του εσωτερικού δικτύου.
- Ο υποφάκελος /etc/unbound/local.d χρησιμοποιείται για να προσθέσει στατικές DNS αντιστοιχίσεις. Αυτό μπορεί να χρησιμοποιηθεί και για τη δημιουργία λιστών αποκλεισμού (blacklists). Τα δεδομένα αυτά θα επιστρέφονται στους πελάτες, αλλά δε είναι ψηφιακά υπογεγραμμένα από DNSSEC.

Για να διαπιστώσετε εάν λειτουργεί σωστά το DNSSEC, μπορείτε να χρησιμοποιήσετε το εργαλείο dig, από το πακέτο bind-utils. Άλλα χρήσιμα εργαλεία είναι το drill (πακέτο ldns) και unbound-host (πακέτο unbound). Τα παλαιότερα εργαλεία nslookup και host είναι ξεπερασμένα και δε πρέπει να χρησιμοποιούνται. Για να αποστείλετε μια αίτηση DNSSEC με dig, πρέπει να προσθέσετε την παράμετρο +dnssec:

```
~]$ dig +dnssec uom.gr
```

2.8 Εφαρμογή Επιπλέον Ρυθμίσεων Ασφαλείας

Για να εξασφαλιστεί η ακεραιότητα του συστήματος, είναι αναγκαία η εφαρμογή κάποιων επιπλέον μέτρων ασφαλείας:

2.8.1 Αποστολή Αρχείων Καταγραφής σε ένα Συγκεντρωτικό Σύστημα Καταγραφής Συμβάντων

Για την εγκατάσταση του splunk forwarder, εκτελέστε τις παρακάτω εντολές ως root:

```
~]# curl -RO https://download.splunk.com/products/universalforwarder/releases/6.4.2/linux/splunkforwarder-6.4.2-00f5bb3fa822-linux-2.6-amd64.deb  
~]# dpkg -i ./splunkforwarder-6.4.2-00f5bb3fa822-linux-2.6-amd64.deb  
  
~]# /opt/splunkforwarder/bin/splunk enable boot-start  
~]# /opt/splunkforwarder/bin/splunk add monitor /var/log/  
~]# /opt/splunkforwarder/bin/splunk add forward-server hostname.domain:9997  
~]# service splunk start
```

Όπου 'hostname.domain' είναι το FQDN ή IP του διακομιστή splunk (για παράδειγμα indexer.splunk.com). Όλα τα αρχεία καταγραφής μπορούν να αναλυθούν μέσω του splunk web interface.

2.8.2 Εγκατάσταση Λογισμικού Προστασίας από Ιούς

Δημοφιλείς επιλογές τέτοιου λογισμικού είναι: [10]:

- BitDefender (εμπορικό)
- ClamAV

Για την εγκατάσταση του clamav antivirus, εκτελέστε τις παρακάτω εντολές ως root:

```
~]# apt-get install clamav clamdscan clamav-daemon  
~]# service clamav-daemon start  
~]# freshclam  
~]# service clamav-freshclam start
```

Για να ρυθμίσετε το clamav, ώστε να ελέγχει ένα συγκεκριμένο φάκελο καθημερινά (εν προκειμένω το /home), δημιουργήστε το ακόλουθο αρχείο:

```
~]# echo > /etc/cron.daily/manual_clamscan << EOF  
#!/bin/bash  
SCAN_DIR="/home"  
LOG_FILE="/var/log/clamav/manual_clamscan.log"  
/usr/bin/clamscan -i -r $SCAN_DIR >> $LOG_FILE  
EOF  
  
~]# chmod +x /etc/cron.daily/manual_clamscan
```

2.8.3 Εξασφάλιση της Ακεραιότητας των Αρχείων

Για την εξασφάλιση της ακεραιότητας των αρχείων, μετά την εγκατάσταση όλων των απαραίτητων πακέτων για τη λειτουργία του συστήματος, εγκαταστείστε ένα από τα παρακάτω [9]:

- Tripwire (τελευταία ενημέρωση 2013)
- AIDE (Advanced Intrusion Detection Environment)
- OSSEC
- Samhain

Για την εγκατάσταση του AIDE εκτελέστε τις παρακάτω εντολές:

```
~]# apt-get install aide-common  
~]# sed -i 's/^Checksums =.*/Checksums = sha512/' /etc/aide/aide.conf  
~]# aideinit --yes
```

Κατά περιόδους είναι χρήσιμο να ελέγχεται η ακεραιότητα των εγκατεστημένων πακέτων, με τη χρήση του διαχειριστή πακέτων:

```
~]# debsums | grep -v OK
```

2.8.4 Εγκατάσταση Λογισμικού Ανίχνευσης Rootkit

Διαθέσιμες επιλογές όπως παρακάτω [10]:

- Rkhunter (τελευταία ενημέρωση 2013)
- OSSEC

για την εγκατάσταση του Rkhunter εκτελέστε τις παρακάτω εντολές:

```
~]# apt-get install rkhunter  
~]# vi /etc/default/rkhunter
```

Τροποποιήστε τις επόμενες γραμμές για να ενεργοποιήσετε το Rkhunter:

```
CRON_DAILY_RUN="yes"  
APT_AUTOGEN="yes"
```

Τέλος εκτελέστε:

```
~]# rkhunter --propupd
```

2.8.5 Εγκατάσταση Λογισμικού Intrusion Detection

Διαθέσιμες επιλογές όπως παρακάτω:

- Snort με acidbase
- OSSEC
- fail2ban

Ως μια ολοκληρωμένη λύση, το OSSEC είναι δυνατό να εγκατασταθεί ώστε να εξασφαλίσει την ακεραιότητα του συστήματος. Συνίσταται η χρησιμοποίηση του OSSEC σε συνδυασμό με ένα συγκεντρωτικό security manager, όπως το AlienVault OSSIM. Για την εγκατάσταση του OSSEC agent, εκτελέστε τις παρακάτω εντολές ως χρήστης root:

```
~]# apt-key adv --fetch-keys http://ossec.wazuh.com/repos/apt/conf/ossec-key.gpg.key  
~]# echo "deb http://ossec.wazuh.com/repos/apt/ubuntu xenial main" >> /etc/apt/sources.list  
~]# apt-get update  
~]# apt-get install ossec-hids ossec-hids-agent
```

Εξάγετε ένα κλειδί από το OSSIM και σημειώστε το, μαζί με την διεύθυνση IP του OSSIM server. Ενημερώστε στο μηχάνημα πελάτη το αρχείο /var/ossec/etc/ossec.conf με την διεύθυνση του OSSIM server. Τέλος, στο μηχάνημα πελάτη, εκτελέστε τις παρακάτω εντολές:

```
~]# /var/ossec/bin/ossec-configure
```

Ακολουθήστε τις οδηγίες και εισάγετε το προαναφερθέν κλειδί, όταν σας ζητηθεί. Τέλος, εκκινήστε την υπηρεσία.

```
~]# /var/ossec/bin/ossec-control start
```

2.8.6 Εποπτεία Συστήματος (System Audit)

Ο έλεγχος συστήματος (Linux Audit System) παρέχει έναν τρόπο καταγραφής των πληροφοριών που έχουν σχέση με την ασφάλεια στο σύστημα, σύμφωνα με καταγεγραμμένους κανόνες. Το Linux Audit παράγει αρχεία καταγραφής, ώστε να περιλάβει όσο το δυνατό περισσότερες πληροφορίες για τα συμβάντα στο σύστημα. Παραδείγματα συμβάντων που ελέγχονται, όπως παρακάτω[1]:

Παρακολούθηση πρόσβασης στα αρχεία Είναι δυνατός ο έλεγχος εάν σε ένα αρχείο ή υποφάκελο ζητήθηκε πρόσβαση, εάν αυτό αλλοιώθηκε, εκτελέσθηκε ή μεταβλήθηκαν οι ιδιότητές του (attributes). Αυτό είναι απαραίτητο για την ανίχνευση της πρόσβασης σε κρίσιμα αρχεία και εφόσον αυτά έχουν αλλοιωθεί, για την δυνατότητα διερευνησής του συμβάντος.

Παρακολούθηση κλήσεων συστήματος To Linux Audit είναι δυνατό να ρυθμίστεί ώστε να παράγει μια εγγραφή στο σύστημα καταγραφής του συστήματος, κάθε φορά που μια συγκεκριμένη κλήση συστήματος ενεργοποιείται. Αυτό για παράδειγμα, μπορεί να χρησιμοποιηθεί για την παρακολούθηση των αλλαγών στην ώρα συστήματος, ελέγχοντας τις κλήσεις συστήματος `settimeofday`, `clock_adjtime`, και άλλες που έχουν σχέση με το χρόνο.

Καταγραφή των εντολών του χρήστη Καθώς ο έλεγχος μπορεί να γίνει πάνω στο ποια αρχεία εκτελούνται, ένας αριθμός από κανόνες μπορεί να καθοριστεί, για να εποπτεύει κάθε εκτέλεση μιας συγκεκριμένης εντολής. Για παράδειγμα μπορεί να οριστεί ένας κανόνας για την παρακολούθηση της εκτέλεσης οποιουδήποτε εκτελέσιμου βρίσκεται στον υποφάκελο /bin. Οι λαμβάνουσες εγγραφές στο αρχείο καταγραφής, μπορούν να αναζητηθούν για πληροφορίες με βάση το user ID, ώστε να υπάρχει εποπτεία του τι εκτέλεσε κάθε χρήστης.

Καταγραφή συμβάντων ασφαλείας Η εποπτεία συστήματος μπορεί να παραμετροποιηθεί ώστε να καταγράφει τις αποτυχημένες προσπάθειες εισόδου στο σύστημα και να παρέχει επιπρόσθετες πληροφορίες για το χρήστη που επιχείρησε να εισέλθει.

Αναζήτηση για συμβάντα Η εποπτεία συστήματος παρέχει το εργαλείο ausearch, το οποίο μπορεί να χρησιμοποιηθεί για να φιλτράρει τις εγγραφές του αρχείου καταγραφής και να προβάλει πληροφορίες με βάση συγκεκριμένα κριτήρια.

Εξαγωγή περιληπτικών αναφορών Το εργαλείο aureport είναι δυνατό να χρησιμοποιηθεί για να παράγει, μεταξύ άλλων, ημερήσιες αναφορές για τα καταγεγραμμένα συμβάντα. Ο διαχειριστής συστήματος, είναι σε θέση να ερευνήσει περαιτέρω τυχόν ύποπτες ενέργειες, με την ανάλυση των αναφορών αυτών.

Παρακολούθηση δικτυακής πρόσβασης Τα εργαλεία iptables και ebtables μπορούν να παραμετροποιηθούν ώστε εκκινούν Audit Events, επιτρέποντας στους διαχειριστές συστήματος να παρακολουθούν την δικτυακή πρόσβαση.

2.8.6.1 Εγκατάσταση των Πακέτων Audit

Για την εγκατάσταση του Audit System, εκτελέστε τις παρακάτω εντολές ως υπερχρήστης:

```
~]# apt-get install auditd
```

2.8.6.2 Προρυθμισμένα Αρχεία Κανόνων Audit

Στον υποφάκελο /usr/share/doc/auditd/examples/, το πακέτο audit παρέχει ένα σύνολο από αρχεία με προρυθμισμένους κανόνες, σύμφωνα με συγκεκριμένα πιστοποιημένα πρότυπα. Για να χρησιμοποιήσετε τα παραπάνω αρχεία, δημιουργήστε ένα αντίγραφο ασφαλείας από το αρχικό αρχείο /etc/audit/audit.rules, αντικαταστήστε το με το αρχείο της επιλογής σας, από τον παραπάνω υποφάκελο και ενεργοποιήστε την υπηρεσία:

```
~]# cp /etc/audit/audit.rules /etc/audit/audit.rules_backup
~]# cp /usr/share/doc/auditd/examples/stig.rules.gz /etc/audit/
audit.rules.gz
~]# gunzip /etc/audit/audit.rules.gz
~]# systemctl enable auditd
```

3 Εργαλεία για Ασφάλιση του Συστήματος

Για τον έλεγχο ασφαλείας του συστήματος ή την επιπλέον ενίσχυσή του, τα επόμενα εργαλεία μπορούν να χρησιμοποιηθούν.

3.1 Bastille Linux

Το Bastille Linux είναι σε θέση να ελέγξει και να αναφέρει το επίπεδο ασφαλείας που παρέχει το σύστημα. Μπορεί επίσης να καταγράψει ζητήματα ασφαλείας, ακόμα και να επιδιορθώνει μη-ασφαλείς παραμετροποιήσεις.

Το πακέτο του Bastille Linux δεν περιλαμβάνεται σε κανένα repository από το Ubuntu 12.04LTS και μετά. Ένας τρόπος για να εγκαταστήσετε το πακέτο, είναι να εγκαταστήσετε τα προαπαιτούμενα και να κατεβάσετε το deb αρχείο από το <http://packages.ubuntu.com>.

```
~]# apt-get install libcurses-perl  
~]# curl -R0 http://gr.archive.ubuntu.com/ubuntu/pool/universe/b/  
bastille/bastille_3.0.9-13ubuntul_all.deb  
~]# dpkg -i ./bastille_3.0.9-13ubuntul_all.deb
```

Το πακέτο περιλαμβάνει μια διεπαφή χρήστη και ένα μηχανισμό ρυθμίσεων. Η πρωτεύουσα διεπαφή χρήστη είναι μέσω X - Perl/Tk, ενώ υπάρχει και μια Curses διεπαφή γραμμής εντολών. Το Bastille Linux έχει δύο τρόπους λειτουργίας:

- **Αλληλεπιδραστικός:** Το Bastille Linux θέτει στο χρήστη συγκεκριμένες ερωτήσεις με επεξηγήσεις για την αντίστοιχη ρύθμιση και ρυθμίζει ασφαλώς το σύστημα με βάση τις απαντήσεις του χρήστη.
- **Μη-Αλληλεπιδραστικός:** Ο χρήστης μπορεί να τροποποιήσει ένα αρχείο ρυθμίσεων, το οποίο καθορίζει τον τρόπο που το Bastille Linux εφαρμόζει τις πολιτικές ασφαλείας. Αυτό είναι βολικό για την αυτοματοποιημένη ρύθμιση πολλών Η/Υ.

Οι αλλαγές που κάνει το Bastille Linux μπορούν να προκαλέσουν ζητήματα ορθής λειτουργίας ή να καταστήσουν το σύστημα μη αποχρίσιμο. Ο διαχειριστής συστήματος πρέπει να έχει καλή κατανόηση των αλλαγών που συμβαίνουν στο σύστημα και πως κάθε μια μπορεί να επηρεάσει την ορθή λειτουργία του.

Εκτός από τα παραπάνω, όταν πρέπει να σημειωθεί ότι η ανάπτυξη του bastille-linux (bastille-unix από το 2007 και μετά [4]) έχει σταματήσει από το 2008. Έτσι το λογισμικό αυτό μπορεί να χρησιμοποιηθεί χυρίως ως εργαλείο παραγωγής αναφορών για την ασφάλεια του συστήματος:

```
~]# bastille --assess  
~]# bastille --assessnobrowser
```

Η δεύτερη σύνταξη της εντολής εκτελεί το Assessment mode, χωρίς να εμφανίζει την αναφορά. Το Bastille Linux δημιουργεί τρεις αναφορές, τις οποίες αποθηκεύει στο φάκελο /var/log/Bastille/Assessment:

- audit-report.html - Full HTML με javascript
- audit-report.txt - Text-only version
- audit-log.txt - Machine-parseable text version

Η παραγόμενη αναφορά περιέχει λεπτομέρεις παρατηρήσεις και μια βαθμολογία.

3.2 Αξιολόγηση του Συστήματος με το SCAP Security Guide

Το πακέτο SCAP Security Guide (SSG) περιλαμβάνει τις τελευταίες συστάσεις ασφαλείας και πληροφορίες για γνωστές ευπάθειες. Για την εγκατάσταση του SCAP Security Guide στο σύστημα, εκτελούμε τις παρακάτω εντολές ως υπερχρήστης:

```
~]# apt-get install libopenscap8
```

Για την παρατήρηση του περιεχομένου του scap-security-guide, χρησιμοποιείται ο διακόπτης info. Το Ubuntu δεν έχει διαθέσιμα openscap definitions, οπότε μπορούν να χρησιμοποιηθούν αυτά του Debian 8.

```
~]$ curl -R0 https://www.debian.org/security/oval/oval-definitions-2016.xml  
~]$ oscap info ./oval-definitions-2016.xml
```

Το εξαγόμενο αυτής της εντολής είναι μια περιγραφή των γνωστών ευπαθειών ασφαλείας. Χάριν παραδείγματος, η παραχώτω εντολή αξιολογεί το σύστημα χρησιμοποιώντας ένα SCAP προφίλ για Debian 8:

```
~]$ oscap oval eval \  
--results ssg-debian8-oval-result.xml \  
--report ssg-debian8-report.html \  
.oval-definitions-2016.xml
```

Μετά την εφαρμογή του bash script που συνοδεύει το κείμενο (βλ. Κεφ. 4) και την αξιολόγηση του συστήματος, η παραχθείσα αναφορά δεν έδειξε ευπάθειες.

4 Bash Script για Εφαρμογή Πολιτικών Ασφαλείας

Για την εφαρμογή των πολιτικών ασφαλείας, οι οποίες αναφέρθηκαν παραπάνω, αναπτύχθηκε ένα bash script, οποίο κάνει τις ακόλουθες αλλαγές στο σύστημα:

- Εγκατάσταση απαιτούμενων πακέτων
- Παραμετροποίηση αυτόματων εγκαταστάσεων ενημερώσεων ασφαλείας με cronjob
- Επιβολή του AppArmor
- Ασφαλή ρύθμιση του bootloader
- Απενεργοποίηση του AppPort
- Απενεργοποίηση μη απαραίτητων υπηρεσιών
- Απενεργοποίηση μη χρησιμοποιούμενων αριθμωμάτων πυρήνα ΛΣ
- Απενεργοποίηση μη χρησιμοποιούμενων συστημάτων αρχείων
- Ασφαλή ρύθμιση των προσαρτήσεων τόμων
- Απενεργοποίηση επικινδύνων δικτυακών πρωτοκόλλων
- Απενεργοποίηση δημιουργίας core dumps
- Ρύθμιση των sysctl παραμέτρων
- Ρύθμιση των security limits για τους χρήστες.
- Αφαίρεση του suid bit από συγκεκριμένα εκτελέσιμα
- Ρύθμιση του umask συστήματος σε 027
- Απενεργοποίηση του συνδυασμού πλήκτρων CTRL+ALT+DEL
- Απενεργοποίηση των root logins - Κλείδωμα του χρήστη root
- Απενεργοποίηση των Host overrides
- Ρύθμιση των Banners
- Ρύθμιση των TCP Wrappers
- Εφαρμογή πολιτικών σε λογαριασμούς και κωδικούς πρόσβασης
- Αφαίρεση μη αναγκαιούντων χρηστών
- Ασφαλή ρύθμιση του Apache Server
- Ασφαλή ρύθμιση του NFS Server

- Ασφαλή ρύθμιση του SSHD server
- Απαγόρευση της εκτέλεσης cronjobs για χρήστες εκτός του root
- Ρύθμιση του UFW
- Απενεργοποίηση IPV6
- Ασφαλή ρύθμιση των DNS resolvers
- Ασφαλή ρύθμιση του NTP Client
- Ρύθμιση του logrotate
- Επιβολή κανόνων auditd
- Ενεργοποίηση RKHUNTER
- Ενεργοποίηση CLAMAV
- Ρύθμιση AIDE

Όλες οι ρυθμίσεις καθορίζονται στην αρχή του bash script με τη μορφή μεταβλητών. Οι περισσότεροι χρήστες απαιτείται να αλλάξουν συνήθως μόνο τις μεταβλητές 'SERVER' και 'VERBOSE'. Η μεταβλητή 'SERVER' ελέγχεται από το bash script, ώστε να εφαρμόσει τις κατάλληλες ρυθμίσεις για μια εγκατάσταση server ή desktop. Οι λοιπές μεταβλητές πρέπει να αλλάζονται μόνο από έμπειρους χρήστες, καθώς έχουν τυπικές τιμές.

Επεμβάσεις οι οποίες απαιτησαν αλληλεπίδραση με το χρήστη, όπως η εισαγωγή κλειδιών από τον OSSIM Server ή η ρύθμιση του Splunk forwarder, παραλήφθηκαν σκοπίμως, αλλά ο αναγνώστης είναι σε θέση να εφαρμόσει αυτές τις πολιτικές ασφαλείας αντιγράφοντας τις αντίστοιχες εντολές από το κείμενο, με αλλαγές όπου απαιτείται.

4.1 Αξιολόγηση Συστήματος

Μετά την εφαρμογή του bash script, το σύστημα αξιολογήθηκε με τη χρήση openscap profiles για debian 8, όπως περιγράφηκε στο τμήμα 3.2, χωρίς να βρεθούν ευπάθειες.

Το σύστημα ελέγχθηκε επίσης με τα λογισμικά Nessus και Greenbone Security Assistant και έλαβε βαθμολογία 85-90% με ήσσονος σημασίας σχόλια. Το εν λόγω bash script βρίσκεται στο παρότημα A' του παρόντος.

5 Συμπεράσματα

Στο παρόν πόνημα, καταβλήθηκε προσπάθεια περιγραφής σε αδρές γραμμές, των πιο χρήσιμων συμβουλών ασφαλείας, για μια βασική εγκατάσταση ΛΣ Ubuntu Linux. Η λίστα δεν είναι εξαντλητική και περιλαμβάνει μια αρχική βάση. Ένα bash script αναπτύχθηκε για την εφαρμογή των ρυθμίσεων, που παρουσιάστηκαν, με αυτόματο τρόπο. Αναγκαία κρίνεται η επιβολή και άλλων μέτρων ασφαλείας που καθορίζονται από τις ιδιαιτερότητες του περιβάλλοντος και των υποδομών.

Παραρτήματα

A' Κώδικας Bash Script

```
#!/usr/bin/env bash
#####
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.

# You should have received a copy of the GNU General Public License
# along with this program. If not, see <http://www.gnu.org/licenses/>.

#####
# Script tries to harden a default setup of Ubuntu Server 16.04LTS
# All configuration parameters lie in the begining of the file,
# in terms of global variables (Capitalized). Fell free to change
# the configuration according to your needs. Only change if you know
# what you're doing..You have been warned!
#####

# CONFIGURATION STARTS HERE
#####
ADDUSER=' /etc/adduser.conf'
APACHE2DFILE=' /etc/apache2/conf-available/custom_secure.conf'
AUDITDCONF=' /etc/audit/auditd.conf'
AUDITRULES=' /etc/audit/rules.d/hardening.rules'
COMMONPASSWD=' /etc/pam.d/common-password'
COMMONACCOUNT=' /etc/pam.d/common-account'
COMMONAUTH=' /etc/pam.d/common-auth'
COREDUMPCONF=' /etc/systemd/coredump.conf'
DEBIAN_FRONTEND='noninteractive'
DEFAULTGRUB=' /etc/default/grub'
DISABLEFS=' /etc/modprobe.d/disablemnt.conf'
DISABLEMOD=' /etc/modprobe.d/disablemod.conf'
DISABLENET=' /etc/modprobe.d/disablenet.conf'
EXPECT=' /usr/bin/expect'
FW_LOCAL='127.0.0.1'
GRUB_PASSPHRASE='password'
GRUB_SUPERUSER='myuser'
JOURNALDCONF=' /etc/systemd/journald.conf'
LIMITSCONF=' /etc/security/limits.conf'
LOGINDCONF=' /etc/systemd/loginctl.conf'
LOGINDEFS=' /etc/login.defs'
LOGROTATE=' /etc/logrotate.conf'
MKPASSWD=' /usr/bin/grub-mkpasswd-pbkdf2'
MOD=' bluetooth firewire-core net-pf-31 soundcore thunderbolt usb-midi'
MODSEC=' /etc/modsecurity/modsecurity.conf'
PACKAGES="acct aide-common apache2 apparmor-profiles apparmor-utils auditd \
clamav clamdscan clamav-daemon debsums expect fail2ban git haveged \
libapache2-mod-security2 libapache2-mod-evasive libpam-cracklib \
libpam-tmpdir nfs-kernel-server openssh-server rkhunter samba $VM"
PAMLOGIN=' /etc/pam.d/login'
RESOLVEDCONF=' /etc/systemd/resolved.conf'
RKHUNTERCONF=' /etc/default/rkhunter'
SECURITYACCESS=' /etc/security/access.conf'
SERVER='Y'
SSHDFILE=' /etc/ssh/sshd_config'
SSH_GROUPS='sudo'
SYSTCL=' /etc/sysctl.conf'
SYSTEMCONF=' /etc/systemd/system.conf'
TERM='linux'
TIMESYNCD=' /etc/systemd/timesyncd.conf'
UFWDEFAULT=' /etc/default/ufw'
USERADD=' /etc/default/useradd'
```

```

USERCONF='/etc/systemd/user.conf'
UNW_PROT='dccp sctp rds tipc'
UNW_SERVICES='rpcbind'
UNW_FS='cramfs freevxfs jffs2 hfs hfsplus squashfs udf vfat'
VERBOSE='Y'
#####
# CONFIGURATION ENDS HERE
# Do not change anything below this line!
#####
# Prepare ENV (OK)
export TERM
export DEBIAN_FRONTEND
#####
# Check that we have bare minimum..(OK)
if [ $EUID -ne 0 ]; then
    echo "This script must be run with root privileges."
    echo
    exit 1
fi

if ! lsb_release -i | grep 'Ubuntu'; then
    echo "Unsupported Linux distribution. Only Ubuntu Supported"
    echo
    exit 1
fi

if ! ps -p $$ | grep -i bash; then
    echo "Please install bash to continue.."
    echo
    exit 1
fi

if ! [ -x "$(which systemctl)" ]; then
echo "systemctl required. Unsupported setup.."
    echo
exit 1
fi

if ! test -f "$UFWDEFAULT"; then
    echo "$UFWDEFAULT firewall config file not found."
    if ! dpkg -l | grep ufw 2> /dev/null 1>&2; then
        echo 'Please install ufw package to continue.'
    fi
    exit 1
fi

echo "End of Pre-Flight checks.."
# End of Pre-Flight checks..
#####
# Set paths(OK)
echo "Setting paths..."

sed -i 's/PATH=.*PATH=\/usr\/local\/bin:\/usr\/bin:\/bin/' /etc/environment

cat > /etc/profile.d/initpath.sh <<EOF
#!/bin/bash

if [[ $EUID -eq 0 ]];
then
    export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
else
    export PATH=/usr/local/bin:/usr/bin:/bin
fi
EOF

chown root:root /etc/profile.d/initpath.sh
chmod 0644 /etc/profile.d/initpath.sh
#####
# Install needed packages(OK)
if [[ $VERBOSE == "Y" ]]; then
    APT_ENV='-y'
else

```

```

        APT_ENV=' -qq -y'
fi

APT="apt-get $APT_ENV"

echo "Updating the package index files..."
$APT update

echo "Upgrading installed packages..."
$APT upgrade

echo "Installing base packages..."

# Are we running a VM?
if dmidecode -q --type system | grep -i vmware; then
    VM="open-vm-tools"
fi

if dmidecode -q --type system | grep -i virtualbox; then
    VM="virtualbox-guest-dkms virtualbox-guest-utils"
fi

for deb in $PACKAGES; do
    $APT install --no-install-recommends "$deb"
done
#####
# Install security updates via cronjob(OK)
cat > /etc/cron.weekly/apt-security-updates <<EOF
echo "*****" >> /var/log/apt-security-updates
date >> /var/log/apt-security-updates
aptitude update >> /var/log/apt-security-updates
aptitude safe-upgrade -o Aptitude::Delete-Unused=false --assume-yes --target-release \
`lsb_release -cs`-security >> /var/log/apt-security-updates
echo "Security updates (if any) installed"
EOF

chmod +x /etc/cron.weekly/apt-security-updates

cat > /etc/logrotate.d/apt-security-updates <<EOF
/var/log/apt-security-updates {
    rotate 2
    weekly
    size 250k
    compress
    notifempty
}
EOF
#####
# Enforce AppArmor(OK)
echo "Enforcing apparmor profiles..."

find /etc/apparmor.d/ -maxdepth 1 -type f -exec aa-enforce {} \;
aa-complain /etc/apparmor.d/usr.sbin.rsyslogd
#####
# Secure bootloader(OK)
echo "Securing bootloader..."

expect_script() {
    cat <<EOF
    log_user 0
    spawn ${MKPASSWD}
    sleep 0.33
    expect "Enter password: " {
        send "$GRUB_PASSPHRASE"
        send "\n"
    }
    sleep 0.33
    expect "Reenter password: " {
        send "$GRUB_PASSPHRASE"
        send "\n"
    }
    sleep 0.33
    expect eof {

```

```

        puts "\$expect_out(buffer)"
    }
    exit 0
EOF
}

if [ -n "$GRUB_PASSPHRASE" ]; then
    sed -i 's/^GRUB_CMDLINE_LINUX=.*$/GRUB_CMDLINE_LINUX="--users $GRUB_SUPERUSER"/' "$DEFAULTGRUB"
    echo "set superusers=$GRUB_SUPERUSER" >> /etc/grub.d/40_custom
    GRUB_PASS=$(expect_script "$1" | $EXPECT | sed -e "/^r$/d" -e "/^$/d" -e "s/.* \(.*/\1/")
    echo "password_pbkdf2 $GRUB_SUPERUSER $GRUB_PASS" >> /etc/grub.d/40_custom
    echo 'export superusers' >> /etc/grub.d/40_custom
fi
#####
# Disable AppPort (OK)
echo "Disabling apport"

sed -i 's/enabled=1/enabled=0/' /etc/default/apport
systemctl mask apport.service

if [[ $VERBOSE == "Y" ]]; then
    systemctl status apport.service --no-pager
    echo
fi
#####
# Disable unwanted services (OK)
echo "Disabling unwanted services"

for disable in $UNW_SERVICES; do
    systemctl disable $disable
done
#####
# Disable unneeded kernel modules(OK)
echo "Disabling unneeded kernel modules"

for disable in $MOD; do
    if ! grep -q "$disable" "$DISABLEMOD" 2> /dev/null; then
        echo "install $disable /bin/true" >> "$DISABLEMOD"
    fi
done

if [[ $SERVER == "Y" ]]; then
    echo "install usb-storage /bin/true" >> "$DISABLEMOD"
fi
#####
# Disable unneeded file systems(OK)
echo "Disabling unneeded file systems"
for disable in $UNW_FS; do
    if ! grep -q "$disable" "$DISABLEFS" 2> /dev/null; then
        echo "install $disable /bin/true" >> "$DISABLEFS"
    fi
done
#####
# Securing Mounts(OK)
echo "Securing mounts"

cat > /etc/systemd/system/tmp.mount <<EOF
# /etc/systemd/system/default.target.wants/tmp.mount -> ../tmp.mount

[Unit]
Description=Temporary Directory
Documentation=man:hier(7)
Before=local-fs.target

[Mount]
What=tmpfs
Where=/tmp
Type=tmpfs
Options=mode=1777,strictatime,nosuid,nodev
EOF

sed -i '/floppy/d' /etc/fstab

```

```

if [ -e /etc/systemd/system/tmp.mount ]; then
    sed -i '/^\/tmp/d' /etc/fstab

    for t in $(mount | grep -e "[[:space:]]/tmp[[:space:]]" -e \
    "[[:space:]]/var/tmp[[:space:]]" -e "[[:space:]]/dev/shm[[:space:]]" \ | awk '{print $3}'); do
        umount "$t"
    done

    sed -i '/[[:space:]]\tmp[[:space:]]/d' /etc/fstab

    ln -s /etc/systemd/system/tmp.mount /etc/systemd/system/default.target.wants/tmp.mount
    sed -i 's/Options=.*/Options=mode=1777,strictatime,nodev,nosuid/' /etc/systemd/system/tmp.mount

    cp /etc/systemd/system/tmp.mount /etc/systemd/system/var-tmp.mount
    sed -i 's/\tmp/\var\tmp/g' /etc/systemd/system/var-tmp.mount
    ln -s /etc/systemd/system/var-tmp.mount /etc/systemd/system/default.target.wants/var-tmp.mount

    cp /etc/systemd/system/tmp.mount /etc/systemd/system/dev-shm.mount
    sed -i 's/\tmp/\dev/shm/g' /etc/systemd/system/dev-shm.mount
    ln -s /etc/systemd/system/dev-shm.mount /etc/systemd/system/default.target.wants/dev-shm.mount
    sed -i 's/Options=.*/Options=mode=1777,strictatime,noexec,nosuid/' /etc/systemd/system/dev-shm.mount

    chmod 0644 /etc/systemd/system/tmp.mount
    chmod 0644 /etc/systemd/system/var-tmp.mount
    chmod 0644 /etc/systemd/system/dev-shm.mount

    systemctl daemon-reload
else
    echo '/etc/systemd/system/tmp.mount was not found.'
fi
#####
# Disable unwanded and potentially dangerous protocols(OK)
echo "Disabling unwanded protocols.."
for disable in $UNW_PROT; do
    if ! grep -q "$disable" "$DISABLENET" 2> /dev/null; then
        echo "install $disable /bin/true" >> "$DISABLENET"
    fi
done
#####
# Disable core dumps(OK)
echo "Disabling coredump"
sed -i 's/^#DumpCore=.*/DumpCore=no/' "$SYSTEMCONF"
sed -i 's/^#CrashShell=.*/CrashShell=no/' "$SYSTEMCONF"
sed -i 's/^#DefaultLimitCORE=.*/DefaultLimitCORE=0/' "$SYSTEMCONF"
sed -i 's/^#DefaultLimitNOFILE=.*/DefaultLimitNOFILE=100/' "$SYSTEMCONF"
sed -i 's/^#DefaultLimitNPROC=.*/DefaultLimitNPROC=100/' "$SYSTEMCONF"

sed -i 's/^#DefaultLimitCORE=.*/DefaultLimitCORE=0/' "$USERCONF"
sed -i 's/^#DefaultLimitNOFILE=.*/DefaultLimitNOFILE=100/' "$USERCONF"
sed -i 's/^#DefaultLimitNPROC=.*/DefaultLimitNPROC=100/' "$USERCONF"

systemctl daemon-reload

if test -f "$COREDUMPCONF"; then
    echo "Fixing Systemd/coredump.conf"
    sed -i 's/^#Storage=.*/Storage=none/' "$COREDUMPCONF"

    systemctl restart systemd-journald

    if [[ $VERBOSE == "Y" ]]; then
        systemctl status systemd-journald --no-pager
        echo
    fi
fi
#####
# Configure sysctl parameters(OK)
echo "Configuring sysctl parameters..."

cat > $SYSTCTL <<EOF
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.

```

```

#
# Documentation:
# "Draft Red Hat 7 STIG Version 1, Release 0.1"
# "Guide to the Secure Configuration of Red Hat Enterprise Linux 5"
# "CIS Ubuntu 12.04 LTS Server Benchmark v1.0.0"
# https://wiki.ubuntu.com/Security/Features
#

fs.protected_hardlinks = 1
fs.protected_symlinks = 1
fs.suid_dumpable = 0
kernel.core_uses_pid = 1
kernel.kptr_restrict = 2
kernel.panic = 60
kernel.panic_on_oops = 60
kernel.perf_event_paranoid = 2
kernel.randomize_va_space = 2
kernel.sysrq = 0
kernel.yama.ptrace_scope = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.ip_forward = 0
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_rfc1337 = 1
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_syn_retries = 5
net.ipv4.tcp_timestamps = 0
net.ipv4.conf.all.forwarding = 0
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_ra = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.dad_transmits = 0
net.ipv6.conf.default.max_addresses = 1
net.ipv6.conf.default.router_solicitations = 0
net.ipv6.conf.default.use_tempaddr = 2
net.ipv6.conf.eth0.accept_ra_rtr_pref = 0
net.ipv6.conf.all.forwarding = 0
net.netfilter.nf_conntrack_max = 2000000
net.netfilter.nf_conntrack_tcp_loose = 0
EOF

sed -i '/net.ipv6.conf.eth0.accept_ra_rtr_pref/d' "$SYSCTL"

for i in $(arp -n -a | awk '{print $NF}' | sort | uniq); do
    echo "net.ipv6.conf.$i.accept_ra_rtr_pref = 0" >> "$SYSCTL"
done

echo 1048576 > /sys/module/nf_conntrack/parameters/hashsize

chmod 0600 "$SYSCTL"
systemctl restart systemd-sysctl

```

```

if [[ $VERBOSE == "Y" ]]; then
    systemctl status systemd-sysctl --no-pager
    echo
fi
#####
# Configure user security limits(OK)
echo "Setting limits..."

sed -i 's/^# End of file/**' "$LIMITSCONF"
echo "* hard maxlogins 10" >> "$LIMITSCONF"
echo "* hard core 0" >> "$LIMITSCONF"
echo "* soft nproc 100" >> "$LIMITSCONF"
echo "* hard nproc 150" >> "$LIMITSCONF"
echo "# End of file" >> "$LIMITSCONF"
#####
# Remove suid bits(OK)
echo "Removing suid bits"

for p in /bin/fusermount /bin/mount /bin/ping /bin/ping6 /bin/su /bin/umount \
        /usr/bin/bsd-write /usr/bin/chage /usr/bin/chfn /usr/bin/chsh \
        /usr/bin/mlocate /usr/bin/mtr /usr/bin/newgrp /usr/bin/pkexec \
        /usr/bin/traceroute6.iputils /usr/bin/wall /usr/sbin/pppd;
do
    if [ -e "$p" ]; then
        oct=$(stat -c "%a" $p |sed 's/^4/0/')
        ug=$(stat -c "%U %G" $p)
        dpkg-statoverride --remove $p 2> /dev/null
        dpkg-statoverride --add "$ug" "$oct" $p 2> /dev/null
        chmod -s $p
    fi
done

for SHELL in $(cat /etc/shells); do
    if [ -x "$SHELL" ]; then
        chmod -s "$SHELL"
    fi
done
#####
# Set umask(OK)
echo "Setting umask..."
sed -i 's/umask 022/umask 027/g' /etc/init.d/rc

if ! grep -q -i "umask" "/etc/profile" 2> /dev/null; then
    echo "umask 027" >> /etc/profile
fi

if ! grep -q -i "umask" "/etc/bash.bashrc" 2> /dev/null; then
    echo "umask 027" >> /etc/bash.bashrc
fi
#####
# Lock up CTRL+ALT+DEL(OK)
echo "Lockup Ctrl-alt-delete"

systemctl mask ctrl-alt-del.target

if [[ $VERBOSE == "Y" ]]; then
    systemctl status ctrl-alt-del.target --no-pager
    echo
fi
#####
# Disable root logins(OK)
echo "Disabling root logins..."

sed -i 's/^#+ : root : 127.0.0.1/+ : root : 127.0.0.1/' "$SECURITYACCESS"
echo '' > /etc/securetty
#####
# Secure user and services host files(OK)
echo "Securing .rhosts and hosts.equiv"

for dir in $(awk -F ":" '{print $6}' /etc/passwd); do
    find "$dir" \( -name "hosts.equiv" -o -name ".rhosts" \) -exec rm -f {} \; 2> /dev/null
done

```



```

if [[ $VERBOSE == "Y" ]]; then
    passwd -S root
    echo
fi
#####
# Remove unneeded users(OK)
echo "Removing unwanted users"

for users in games gnats irc list news uucp; do
    userdel -r "$users" 2> /dev/null
done
#####
# Secure Apache(OK)
chmod 511 /usr/sbin/apache2
chown 0:0 /usr/sbin/apache2
chattr +i /etc/apache2/apache2.conf

a2dismod autoindex

cat > "$APACHE2DFILE" <<EOF
<Directory />
    Order Deny,Allow
    Deny from all
    Options None
    AllowOverride None
</Directory>

<Directory /var/www/>
    Order Allow,Deny
    Allow from all
    Options +FollowSymLinks -Indexes +IncludesNoExec
    AllowOverride None
    Require all granted
</Directory>

ServerSignature Off
ServerTokens Prod
TraceEnable Off
EOF

a2enconf custom_secure

# Enable mod_security
mv /etc/modsecurity/modsecurity.conf-recommended $MODSEC
sed -i 's/.*SecRuleEngine.*$/SecRuleEngine On/' "$MODSEC"
sed -i 's/.*SecRequestBodyLimit.*$/SecRequestBodyLimit 16384000/' "$MODSEC"
sed -i 's/.*SecRequestBodyInMemoryLimit.*$/SecRequestBodyInMemoryLimit 16384000/' "$MODSEC"

wget -O /tmp/SpiderLabs-owasp-modsecurity-crs.tar.gz \
https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master
cd /tmp
tar -zxf ./SpiderLabs-owasp-modsecurity-crs.tar.gz
cp -R SpiderLabs-owasp-modsecurity-crs-*/* /etc/modsecurity/
rm -R SpiderLabs-owasp-modsecurity-crs-*
mv /etc/modsecurity/modsecurity_crs_10_setup.conf.example /etc/modsecurity/modsecurity_crs_10_setup.conf

cd /etc/modsecurity/base_rules
for f in * ; do sudo ln -s /etc/modsecurity/base_rules/$f /etc/modsecurity/activated_rules/$f ; done
cd /etc/modsecurity/optional_rules
for f in * ; do sudo ln -s /etc/modsecurity/optional_rules/$f /etc/modsecurity/activated_rules/$f ; done

cat > /etc/apache2/mods-available/security2.conf <<EOF
<IfModule security2_module>
    # Default Debian dir for modsecurity's persistent data
    SecDataDir /var/cache/modsecurity

    # Include all the *.conf files in /etc/modsecurity.
    # Keeping your local configuration in that directory
    # will allow for an easy upgrade of THIS file and
    # make your life easier
    IncludeOptional /etc/modsecurity/*.conf
    IncludeOptional /etc/modsecurity/activated_rules/*.conf

```

```

</IfModule>
EOF

# Enable mod_evasive
mkdir /var/log/mod_evasive
chown www-data:www-data /var/log/mod_evasive/

cat > /etc/apache2/mods-available/evasive.conf <<EOF
<ifmodule mod_evasive20.c>
    DOSHashTableSize 3097
    DOSPageCount 2
    DOSSiteCount 50
    DOSPageInterval 1
    DOSSiteInterval 1
    DOSBlockingPeriod 10
    DOSLogDir /var/log/mod_evasive
    DOSEmailNotify root@localhost
    DOSWhitelist 127.0.0.1
</ifmodule>
EOF

a2enmod ssl evasive security2 headers
service apache2 restart

# Enable fail2ban
cat >> /etc/fail2ban/jail.d/defaults-debian.conf <<EOF

[apache-modsecurity]
enabled = true

[apache-shellshock]
enabled = true
EOF

service fail2ban restart
#####
# Secure NFS(OK)
echo "Enabling Kerberos Authentication for NFS4"
sed -i 's/.NEED_SVCGSSD=.NEED_SVCGSSD=yes/' /etc/default/nfs-kernel-server
#####
# Configure sshd server(OK)
echo "Configuring sshd...""

cp "$SSHDFILE" "$SSHDFILE-$(date +%s)"

sed -i '/HostKey.*ssh_host_dsa_key.*/d' "$SSHDFILE"
sed -i 's/.AuthenticationMethods.*AuthenticationMethods publickey,gssapi-with-mic \
publickey,keyboard-interactive/' "$SSHDFILE"
sed -i 's/.X11Forwarding.*X11Forwarding no/' "$SSHDFILE"
sed -i 's/.Port.*Port 1027/' "$SSHDFILE"
sed -i 's/.LoginGraceTime.*LoginGraceTime 20/' "$SSHDFILE"
sed -i 's/.PermitRootLogin.*PermitRootLogin no/' "$SSHDFILE"
sed -i 's/.KeyRegenerationInterval.*KeyRegenerationInterval 1800/' "$SSHDFILE"
sed -i 's/.UsePrivilegeSeparation.*UsePrivilegeSeparation sandbox/' "$SSHDFILE"
sed -i 's/.LogLevel.*LogLevel VERBOSE/' "$SSHDFILE"
sed -i 's/.UseLogin.*UseLogin no/' "$SSHDFILE"
sed -i 's/.Banner.*Banner \\\etc\\\issue.net/' "$SSHDFILE"
sed -i 's/.Subsystem sftp.*Subsystem sftp \\\usr\\\lib\\\ssh\\\sftp-server -f AUTHPRIV -l INFO/' "$SSHDFILE"

if ! grep -q "AllowGroups" "$SSHDFILE" 2> /dev/null; then
    echo "AllowGroups $SSH_GROUPS" >> "$SSHDFILE"
fi

if ! grep -q "MaxAuthTries" "$SSHDFILE" 2> /dev/null; then
    echo "MaxAuthTries 4" >> "$SSHDFILE"
fi

if ! grep -q "ClientAliveInterval" "$SSHDFILE" 2> /dev/null; then
    echo "ClientAliveInterval 300" >> "$SSHDFILE"
fi

if ! grep -q "ClientAliveCountMax" "$SSHDFILE" 2> /dev/null; then
    echo "ClientAliveCountMax 0" >> "$SSHDFILE"

```

```

fi

if ! grep -q "PermitUserEnvironment" "$SSHDFILE" 2> /dev/null; then
    echo "PermitUserEnvironment no" >> "$SSHDFILE"
fi

if ! grep -q "KexAlgorithms" "$SSHDFILE" 2> /dev/null; then
    echo 'KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521, \
      ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256' >> "$SSHDFILE"
fi

if ! grep -q "Ciphers" "$SSHDFILE" 2> /dev/null; then
    echo 'Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes256-ctr' >> "$SSHDFILE"
fi

if ! grep -q "Macs" "$SSHDFILE" 2> /dev/null; then
    echo 'Macs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com, \
      hmac-sha2-512,hmac-sha2-256' >> "$SSHDFILE"
fi

if ! grep -q "MaxSessions" "$SSHDFILE" 2> /dev/null; then
    echo "MaxSessions 2" >> "$SSHDFILE"
fi

if ! grep -q "UseDNS" "$SSHDFILE" 2> /dev/null; then
    echo "UseDNS yes" >> "$SSHDFILE"
fi

# Fail2Ban is already enabled by default for sshd
# Restarting Service
systemctl restart sshd.service

if [[ $VERBOSE == "Y" ]]; then
    systemctl status sshd.service --no-pager
    echo
fi
#####
# Lock up cronjobs(OK)
echo "Locking up cronjobs..."

rm /etc/cron.deny 2> /dev/null
rm /etc/at.deny 2> /dev/null

echo 'root' > /etc/cron.allow
echo 'root' > /etc/at.allow

chown root:root /etc/cron*
chmod og-rwx /etc/cron*

chown root:root /etc/at*
chmod og-rwx /etc/at*

systemctl mask atd.service
systemctl stop atd.service
systemctl daemon-reload

sed -i 's/^#cron./cron./' /etc/rsyslog.d/50-default.conf

if [[ $VERBOSE == "Y" ]]; then
    systemctl status atd.service --no-pager
    echo
fi
#####
# Configure UFW(OK)
echo "Configuring Firewall.."
sed -i 's/IPT_SYSCTL=.*/IPT_SYSCTL=/etc\sysctl\conf/' "$UFWDEFAULT"
ufw --force enable

for ip in $FW_LOCAL; do
    ufw allow log from "$ip" to any port 1027 proto tcp # SSH
done

if [[ $SERVER == "Y" ]]; then

```

```

        ufw allow proto tcp from any to any port 1027 #SSH
        ufw allow http
        ufw allow samba
        ufw allow nfs
    fi

    if [[ $VERBOSE == "Y" ]]; then
        systemctl status ufw.service --no-pager
        ufw status verbose
        echo
    fi
#####
# Disable IPV6(OK)
sed -i 's/^GRUB_CMDLINE_LINUX=.*$/GRUB_CMDLINE_LINUX="ipv6.disable=1"/' "$DEFAULTGRUB"
update-grub

sed '/udp6/d' /etc/netconfig
sed '/tcp6/d' /etc/netconfig
#####
# Configure DNS resolvers(OK)
echo "Configuring DNS..."

dnsarray=( $(grep nameserver /etc/resolv.conf | sed 's/nameserver//g') )
dnslist=${dnsarray[@]}

sed -i "s/^#DNS=.*$/DNS=$dnslist/" "$RESOLVEDCONF"
sed -i "s/^#FallbackDNS=.*$/FallbackDNS=8.8.8.8 8.8.4.4/" "$RESOLVEDCONF"
sed -i "s/^#DNSSEC=.*$/DNSSEC=allow-downgrade/" "$RESOLVEDCONF"
sed -i '/^hosts:/ s/files dns/files resolve dns/' /etc/nsswitch.conf

systemctl daemon-reload

if [[ $VERBOSE == "Y" ]]; then
    systemctl status resolvconf.service --no-pager
    echo
fi
#####
# Securing NTP(OK)
echo "Securing NTP..."

LATENCY="50"
SERVERS="4"
APPLY="YES"
CONF="$TIMESYNCNCD"
SERVERARRAY=()
FALLBACKARRAY=()
TMPCONF=$(mktemp --tmpdir ntpconf.XXXXX)

if [[ -z "$NTPSERVERPOOL" ]]; then
    NTPSERVERPOOL="0.ubuntu.pool.ntp.org 1.ubuntu.pool.ntp.org \
    2.ubuntu.pool.ntp.org 3.ubuntu.pool.ntp.org pool.ntp.org"
fi

echo "[Time]" > "$TMPCONF"

PONG="ping -c2"

for s in $(dig +noall +answer +nocomments $NTPSERVERPOOL | awk '{print $5}'); do
    if [[ $NUMSERV -ge $SERVERS ]]; then
        break
    fi

    PINGSERV=$(($PONG "s" | grep 'rtt min/avg/max/mdev' | awk -F "/" '{printf "%.0f\n", $6}')
    if [[ $PINGSERV -gt "1" && $PINGSERV -lt "$LATENCY" ]]; then
        OKSERV=$(nslookup "$s" | grep "name = " | awk '{print $4}' | sed 's/.//')
        if [[ $OKSERV && $NUMSERV -lt $SERVERS && ! (( $(grep "$OKSERV" "$TMPCONF") )) ]]; then
            echo "$OKSERV has latency < $LATENCY"
            SERVERARRAY+=("$OKSERV")
            ((NUMSERV++))
        fi
    fi
done

```

```

for l in $NTPSERVERPOOL; do
    if [[ $FALLBACKSERV -le "2" ]]; then
        FALLBACKARRAY+=("$_1")
        ((FALLBACKSERV++))
    else
        break
    fi
done

if [[ ${#SERVERARRAY[@]} -le "2" ]]; then
    for s in $(echo "$NTPSERVERPOOL" | awk '{print $(NF-1),$NF}'); do
        SERVERARRAY+=("$s")
    done
fi

echo "NTP=${SERVERARRAY[@]}" >> "$TMPCONF"
echo "FallbackNTP=${FALLBACKARRAY[@]}" >> "$TMPCONF"

if [[ $APPLY = "YES" ]]; then
    cat "$TMPCONF" > "$CONF"
    systemctl restart systemd-timesyncd
    rm "$TMPCONF"
else
    echo "Configuration saved to $TMPCONF."
fi

if [[ $VERBOSE == "Y" ]]; then
    systemctl status systemd-timesyncd --no-pager
    echo
fi
#####
# Configure logrotate(OK)
echo "Configuring logrotate..."

cat > "$LOGROTATE" <<EOF
# see "man logrotate" for details
# rotate log files daily
daily

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog

# keep 7 days worth of backlogs
rotate 7

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# compressed log files
compress

# use xz to compress
compresscmd /usr/bin/xz
uncompresscmd /usr/bin/unxz
compressext .xz

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok

```

```

monthly
create 0600 root utmp
rotate 1
}

# system-specific logs may be also be configured here.
EOF

sed -i 's/^#Storage=.*/Storage=persistent/' "$JOURNALDCONF"
sed -i 's/^#ForwardToSyslog=.*/ForwardToSyslog=yes/' "$JOURNALDCONF"
sed -i 's/^#Compress=.*/Compress=yes/' "$JOURNALDCONF"

systemctl restart systemd-journald

if [[ $VERBOSE == "Y" ]]; then
    systemctl status systemd-journald --no-pager
    echo
fi
#####
# Enforcing auditd rules
echo "Enforcing Auditd rules..."
sed -i 's/^action_mail_acct =.*/action_mail_acct = root/' "$AUDITDCONF"
sed -i 's/^admin_space_left_action = .*/admin_space_left_action = halt/' "$AUDITDCONF"
sed -i 's/^max_log_file_action = .*/max_log_file_action = keep_logs/' "$AUDITDCONF"
sed -i 's/^space_left_action = .*/space_left_action = email/' "$AUDITDCONF"
sed -i 's/^GRUB_CMDLINE_LINUX=.*$/GRUB_CMDLINE_LINUX="ipv6.disable=1 audit=1"/' "$DEFAULTGRUB"

cat > /etc/audit/audit.rules <<EOF
## Remove any existing rules
-D

## Buffer Size
-b 8192

## Failure Mode
-f 2

## Audit the audit logs
-w /var/log/audit/ -k auditlog

## Auditd configuration
-w /etc/audit/ -p wa -k auditconfig
-w /etc/libaudit.conf -p wa -k auditconfig
-w /etc/audisp/ -p wa -k audispconfig

## Monitor for use of audit management tools
-w /sbin/auditctl -p x -k audittools
-w /sbin/auditd -p x -k audittools

## Monitor AppArmor configuration changes
-w /etc/apparmor/ -p wa -k apparmor
-w /etc/apparmor.d/ -p wa -k apparmor

## Monitor usage of AppArmor tools
-w /sbin/apparmor_parser -p x -k apparmor_tools
-w /usr/sbin/aa-complain -p x -k apparmor_tools
-w /usr/sbin/aa-disable -p x -k apparmor_tools
-w /usr/sbin/aa-enforce -p x -k apparmor_tools

## Monitor Systemd configuration changes
-w /etc/systemd/ -p wa -k systemd
-w /lib/systemd/ -p wa -k systemd

## Monitor usage of systemd tools
-w /bin/systemctl -p x -k systemd_tools
-w /bin/journalctl -p x -k systemd_tools

## Special files
-a always,exit -F arch=b64 -S mknod -S mknodat -k specialfiles

## Mount operations
-a always,exit -F arch=b64 -S mount -S umount2 -k mount

```

```

## Changes to the time
-a always,exit -F arch=b64 -S adjtimex -S settim eofday -S clock_settime -k time

## Cron configuration & scheduled jobs
-w /etc/cron.allow -p wa -k cron
-w /etc/cron.deny -p wa -k cron
-w /etc/cron.d/ -p wa -k cron
-w /etc/cron.daily/ -p wa -k cron
-w /etc/cron.hourly/ -p wa -k cron
-w /etc/cron.monthly/ -p wa -k cron
-w /etc/cron.weekly/ -p wa -k cron
-w /etc/crontab -p wa -k cron
-w /var/spool/cron/crontabs/ -k cron

## User, group, password databases
-w /etc/group -p wa -k etcgrou p
-w /etc/passwd -p wa -k etcpasswd
-w /etc/gshadow -k etcgrou p
-w /etc/shadow -k etcpasswd
-w /etc/security/opasswd -k opasswd

## Monitor usage of passwd
-w /usr/bin/passwd -p x -k passwd_modification

## Monitor for use of tools to change group identifiers
-w /usr/sbin/groupadd -p x -k group_modification
-w /usr/sbin/groupmod -p x -k group_modification
-w /usr/sbin/addgroup -p x -k group_modification
-w /usr/sbin/useradd -p x -k user_modification
-w /usr/sbin/usermod -p x -k user_modification
-w /usr/sbin/adduser -p x -k user_modification

## Monitor module tools
-w /sbin/insmod -p x -k modules
-w /sbin/rmmmod -p x -k modules
-w /sbin/modprobe -p x -k modules

## Login configuration and information
-w /etc/login.defs -p wa -k login
-w /etc/securetty -p wa -k login
-w /var/log/faillog -p wa -k login
-w /var/log/lastlog -p wa -k login
-w /var/log/tallylog -p wa -k login

## Network configuration
-w /etc/hosts -p wa -k hosts
-w /etc/network/ -p wa -k network

## System startup scripts
-w /etc/inittab -p wa -k init
-w /etc/init.d/ -p wa -k init
-w /etc/init/ -p wa -k init

## Library search paths
-w /etc/ld.so.conf -p wa -k libpath

## Local time zone
-w /etc/localtime -p wa -k localtime

## Time zone configuration
-w /etc/timezone -p wa -k timezone

## Kernel parameters
-w /etc/sysctl.conf -p wa -k sysctl

## Modprobe configuration
-w /etc/modprobe.conf -p wa -k modprobe
-w /etc/modprobe.d/ -p wa -k modprobe
-w /etc/modules -p wa -k modprobe

# Module manipulations.
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

```

```

## PAM configuration
-w /etc/pam.d/ -p wa -k pam
-w /etc/security/limits.conf -p wa -k pam
-w /etc/security/pam_env.conf -p wa -k pam
-w /etc/security/namespace.conf -p wa -k pam
-w /etc/security/namespace.init -p wa -k pam

## Postfix configuration
-w /etc/aliases -p wa -k mail
-w /etc/postfix/ -p wa -k mail

## SSH configuration
-w /etc/ssh/sshd_config -k sshd

## Changes to hostname
-a exit,always -F arch=b64 -S sethostname -k hostname

## Changes to issue
-w /etc/issue -p wa -k etcissue
-w /etc/issue.net -p wa -k etcissue

## Capture all failures to access on critical elements
-a exit,always -F arch=b64 -S open -F dir=/etc -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/bin -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/sbin -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/usr/bin -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/usr/sbin -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/var -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/home -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/root -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/srv -F success=0 -k unauthedfileaccess
-a exit,always -F arch=b64 -S open -F dir=/tmp -F success=0 -k unauthedfileaccess

## Monitor for use of process ID change (switching accounts) applications
-w /bin/su -p x -k priv_esc
-w /usr/bin/sudo -p x -k priv_esc
-w /etc/sudoers -p rw -k priv_esc

## Monitor usage of commands to change power state
-w /sbin/shutdown -p x -k power
-w /sbin/poweroff -p x -k power
-w /sbin/reboot -p x -k power
-w /sbin/halt -p x -k power

## Monitor admins accessing user files.
-a always,exit -F dir=/home/ -F uid=0 -C auid!=obj_uid -k admin_user_home

## Monitor changes and executions in /tmp and /var/tmp.
-w /tmp/ -p wxa -k tmp
-w /var/tmp/ -p wxa -k tmp

## Make the configuration immutable
-e 2
EOF

sed -i "s/arch=b64/arch=$(uname -m)/g" /etc/audit/audit.rules
cp /etc/audit/audit.rules "$AUDITRULES"
update-grub 2> /dev/null

systemctl enable auditd
systemctl restart auditd.service

if [[ $VERBOSE == "Y" ]]; then
    systemctl status auditd.service --no-pager
    echo
fi
#####
# Enable RKHUNTER(OK)
echo "Enabling rkhunter..."

sed -i 's/^CRON_DAILY_RUN=.*$/CRON_DAILY_RUN="yes"/' "$RKHUNTERCONF"
sed -i 's/^APT_AUTOGEN=.*$/APT_AUTOGEN="yes"/' "$RKHUNTERCONF"

```

```

rkhunter --propupd
#####
# Enable CLAMAV(OK)
echo "Enabling CLAMAV..."
service clamav-daemon start
freshclam
service clamav-freshclam start

echo > /etc/cron.daily/user_clamscan <<EOF
#!/bin/bash
SCAN_DIR="/home"
LOG_FILE="/var/log/clamav/user_clamscan.log"
/usr/bin/clamscan -i -r $SCAN_DIR >> $LOG_FILE
EOF

chmod +x /etc/cron.daily/user_clamscan
#####
# Disable Prelinking(OK)
echo "Disabling Prelink for AIDE..."

if dpkg -l | grep prelink 1> /dev/null; then
    "$(which prelink)" -ua 2> /dev/null
    "$APT" purge prelink
fi
#####
# Secure AIDE Configuration(OK)
echo "Securing Aide...""

sed -i 's/^Checksums =.*Checksums = sha512/' /etc/aide/aide.conf
#####
# Set AIDE Postinstall(OK)
echo "Building AIDE initial db, this will take a while...""

aideinit --yes
cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db

echo "Enabling AIDE check daily..."

cat > /etc/systemd/system/aidecheck.service <<EOF
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/bin/aide.wrapper --check

[Install]
WantedBy=multi-user.target
EOF

cat > /etc/systemd/system/aidecheck.timer <<EOF
[Unit]
Description=Aide check every day at midnight

[Timer]
OnCalendar=*-*-* 00:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
EOF

chmod 0644 /etc/systemd/system/aidecheck.*

systemctl reenable aidecheck.timer
systemctl start aidecheck.timer
systemctl daemon-reload

if [[ $VERBOSE == "Y" ]]; then
    systemctl status aidecheck.timer --no-pager
    echo
fi
#####

```

```

# Remove unused packages (OK)
echo "Removing unused packages..."

$APT purge expect

if [[ $SERVER == "Y" ]]; then
    echo "Removing X-Window System"
    $APT purge x-window-system-core
    echo
fi

$APT clean
$APT autoclean
$APT autoremove
#####
# Check systemddelta(OK)
if [[ $VERBOSE == "Y" ]]; then
    echo "Checking systemd-delta..."
    systemd-delta --no-pager
    echo
fi
#####
# check if reboot is required(OK)
if [ -f /var/run/reboot-required ]; then
    cat /var/run/reboot-required
fi

echo

```

Βιβλιογραφία

- [1] al, Martin Prpić et: *Red Hat Enterprise Linux 7 Security Guide*. RedHat, US, 2013.
- [2] al, Maxim Svistunov et: *File and print servers (samba)*, 2016. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/ch-File_and_Print_Servers.html#sect-Samba, επίσκεψη την 2016-07-21.
- [3] Arr0way: *Security harden centos 7*, 2015. <https://highoncoffee.blog/security-hardening>, επίσκεψη την 2016-07-21.
- [4] Beale, Jay: *The bastille hardening program*, 2012. http://bastille-linux.sourceforge.net/news_updates.htm, επίσκεψη την 2016-07-21.
- [5] Cannon, Jason: *Linux security and hardening, the practical security guide*, 2016. <https://www.udemy.com/linux-security>, επίσκεψη την 2016-07-21.
- [6] Jethva, Hitesh: *Linux hardening and system auditing*, 2015. <https://www.maketecheasier.com/hardening-ubuntu-server>, επίσκεψη την 2016-07-21.
- [7] Orloff, Jeffrey: *Hardening the linux server*, 2014. <http://www.ibm.com/developerworks/linux/tutorials/l-harden-server>, επίσκεψη την 2016-07-21.
- [8] Saive, Ravi: *25 hardening security tips for linux servers*, 2015. <http://www.tecmint.com/linux-server-hardening-security-tips>, επίσκεψη την 2016-07-21.
- [9] Sans: *Linux security checklist*, 2014. <https://www.sans.org/media/score/checklists/linuxchecklist.pdf>, επίσκεψη την 2016-07-21.
- [10] Tom6: *Ubuntu security guides*, 2015. <https://help.ubuntu.com/community/Security>, επίσκεψη την 2016-07-21.
- [11] Tom6: *Ubuntu security server guide*, 2016. <https://help.ubuntu.com/lts/serverguide/security.html>, επίσκεψη την 2016-07-21.