Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. " Ασφάλεια Ψηφιακών Συστημάτων "

ΔΙΠΛΩΜΑΤΙΚΗ - ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ενδυνάμωση ασφάλειας σε εξυπηρετητές παγκόσμιου ιστού (CentOS Use Case)

Κωνσταντίνος Ε. Γαλανομάτης

Αρ.Μητρώου: mte1905

Μεταπτυχιακός φοιτητής του τμήματος Ψηφιακών Συστημάτων

του Πανεπιστημίου Πειραιώς

Μεταπτυχιακό πρόγραμμα: «Ασφάλεια Ψηφιακών Συστημάτων»

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, 2021

Αφιερωμένη στην,
οικογένειά μου

Dedicated to,
my family

Abstract

At today's time more and more companies and organizations are launching their products and services on the Internet in order to gain an edge over their competitors. However, this business plan carries a lot of risks and dangers if not done carefully and with the right security procedures for transitioning on the Internet. In the tech world, cyber-attacks are a daily occurrence for system administrators. Malicious users attempt to steal legitimate users' data, other sensitive system data and even disrupt their smooth operation by causing the company to lose reputation, money and at the same time reduce its customers. These attacks are called denial of service attacks and one of them will concern us in this master thesis. System administrators are required to properly configure the technologies used to provide the company's services, by respecting the three main pillars of information systems security, confidentiality, integrity and availability (CIA triad).

This master thesis aims to create an analytical step-by-step guide for enhancing the security of the CentOS operating system and the Apache web server program, and also ways to deal with the DoS Slowloris attack, which targets Apache web servers. In addition to the guide, there will be the practical part of the thesis which is the creation of a script which will execute appropriate commands to automate the process of system security hardening. The script will be executed and then various security auditing and vulnerability scanning tools will be used to check the overall security of the system. The harden system will be compared with the 'vanilla' system as provided by the official CentOS website. Finally, we will run a Slowloris attack on the system before and after activating the Apache security modules so that we can check in real scenario how our security mechanism for the attack is working.

Key-Words: CentOS, Apache, DoS, Web Server Security, Cyber-attacks

Περίληψη

Είναι γεγονός ότι, στη σημερινή εποχή όλο και περισσότερες επιχειρήσεις και οργανισμοί μεταφέρουν τα προϊόντα και τις υπηρεσίες του στο Διαδίκτυο ώστε να αποκτήσουν προβάδισμα έναντι των ανταγωνιστών τους. Ωστόσο, αυτή η κίνηση κρύβει αρκετούς κινδύνους εάν δεν γίνει με προσοχή και με την εφαρμογή σωστών διαδικασιών μετάβασης στο χώρο του Διαδικτύου. Στον τεχνολογικό κόσμο, οι κυβερνοεπιθέσεις αποτελούν καθημερινότητα για τους διαχειριστές των συστημάτων. Κακόβουλοι χρήστες επιχειρούν να υποκλέψουν στοιχεία νόμιμων χρηστών, άλλα ευαίσθητα δεδομένα των συστημάτων ακόμα και να διαταράξουν την ομαλή λειτουργία τους προκαλώντας μείωση της φήμης της εταιρείας και συνάμα μείωση των πελατών της. Οι συγκεκριμένες επιθέσεις ονομάζονται, επιθέσεις άρνησης παροχής υπηρεσιών και μία τέτοια θα μας απασχολήσει και στην συγκεκριμένη εργασία. Οι διαχειριστές καλούνται να παραμετροποιήσουν κατάλληλα τις τεχνολογίες που χρησιμοποιούνται ώστε να παρέχουν τις υπηρεσίες τους, τηρώντας τους τρεις βασικούς πυλώνες της ασφάλειας των πληροφοριακών συστημάτων, την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα.

Η παρούσα εργασία έχει ως στόχο την δημιουργία κατάλληλου οδηγού για την επαύξηση του λειτουργικού συστήματος CentOS και του προγράμματος εξυπηρετητή ιστού Apache, ενώ θα υπάρχουν και τρόποι αντιμετώπισης της επίθεσης Slowloris, μίας επίθεσης άρνησης παροχής υπηρεσιών. Επιπλέον του οδηγού, θα υπάρχει και το πρακτικό κομμάτι της εργασίας όπου είναι η δημιουργία κατάλληλου script το οποίο θα ακολουθεί κατάλληλα βήματα ώστε να αυτοματοποιήσει την διαδικασία της συνολικής επαύξησης του συστήματος. Το script θα εκτελεστεί και έπειτα θα χρησιμοποιηθούν διάφορα εργαλεία ελέγχου ασφαλείας ώστε να ελεγχθεί η τελική παρεχόμενη ασφάλεια του συστήματος. Το τελικό σύστημα θα συγκριθεί με το αρχικό σύστημα όπως παρέχεται από την επίσημη ιστοσελίδα του CentOS. Τέλος, θα διεξαχθεί μία επίθεση Slowloris κατά του συστήματος πριν και μετά την ενεργοποίηση των αρθρωμάτων ασφαλείας του Apache ώστε να δούμε και στην πράξη ότι ο μηχανισμός ασφαλείας μας για αυτή την επίθεση, όντως λειτουργεί.

Λέξεις-Κλειδιά: CentOS, Apache, DoS, Ασφάλεια εξυπηρετητή ιστού, Κυβερνοεπιθέσεις

Ευχαριστίες

Με την παράδοση αυτής της διπλωματικής εργασίας, ολοκληρώνεται με επιτυχία ο πλήρης κύκλος σπουδών μου στο Πανεπιστήμιο Πειραιώς. Υπήρξα σε αυτό το ακαδημαϊκό χώρο αρχικά ως φοιτητής στο τμήμα Ψηφιακών Συστημάτων. Έπειτα από την καθοδήγηση των καθηγητών του τμήματος αυτού, αποφάσισα να ακολουθήσω το μεταπτυχιακό πρόγραμμα της Ασφάλειας Ψηφιακών Συστημάτων. Αισθάνομαι την ανάγκη να ευχαριστήσω τα συγκεκριμένα άτομα τα οποία με βοήθησαν να ασχοληθώ με το συγκεκριμένο τομέα της επιστήμης των υπολογιστών καθώς και τα στενά μου πρόσωπα που μου συμπαραστάθηκαν, όλα αυτά τα χρόνια, όντας κύριοι αρωγοί των επιτυχιών μου.

Θα ήθελα να ευχαριστήσω, αρχικά τον κ. Κωνσταντίνο Λαμπρινουδάκη, ο οποίος υπήρξε καθηγητής μου και στα δύο προγράμματα σπουδών και αποτελεί τον κύριο λόγο που διάλεξα το συγκεκριμένο μεταπτυχιακό πρόγραμμα.

Θα ήθελα επίσης να ευχαριστήσω τον κ. Χρήστο Ξενάκη καθώς και τους υπόλοιπους καθηγητές του μεταπτυχιακού προγράμματος, οι οποίοι με βοήθησαν να αποκτήσω περαιτέρω γνώσεις γύρω από τον τομέα της ασφάλειας των υπολογιστών.

Επιπλέον, θα ήθελα να ευχαριστήσω τον κ. Γεώργιο Βάσιο, ταγματάρχη (ΕΠ) του Κέντρου Πληροφορικής Υποστήριξης Ελληνικού Στρατού που μου έδειξε εμπιστοσύνη για το παρόν θέμα της διπλωματικής, με καθοδήγησε και μου παρείχε χρήσιμο υλικό για την διεκπεραίωσή της και ήταν πάντα διαθέσιμος για οποιαδήποτε απορία ή πρόβλημα που προ έκυπτε για την διεκπεραίωσή της.

Τους φίλους μου καθώς και τους υπόλοιπους συμφοιτητές του τμήματός μου, που ήταν δίπλα μου σε όλες τις εύκολες και δύσκολες στιγμές της φοιτητικής ζωής μου, προσφέροντας μου συμπαράσταση και με ωθούσαν προς την σωστή κατεύθυνση σε κάθε επιλογή που έπρεπε να κάνω. Τους ευχαριστώ για όλα και οι αναμνήσεις μαζί τους, θα με ακολουθούν για το υπόλοιπο της ζωής μου.

Ειδικά, θα ήθελα να ευχαριστήσω την κ.Ταξιαρχούλα, καθηγήτρια μου από το Γυμνάσιο, η οποία όχι μόνο με δίδαξε, αλλά υπήρξε σημαντική ψυχολογική και ηθική στήριξη από την πρώτη ημέρα που την γνώρισα, πίστεψε πραγματικά στις δυνατότητες μου και είναι κύριος αρωγός των επιτυχιών μου.

Τέλος, θα ήθελα να ευχαριστήσω τον σημαντικότερο αρωγό των επιτυχιών μου, την οικογένεια μου. Έκανε αρκετές θυσίες για εμένα, μου παρείχε την κατάλληλη στήριξη και τα εργαλεία και με ενθάρρυνε να προσπαθώ παρά τα λάθη μου, σε όλους τους τομείς της ζωής μου. Θα τους ευγνωμονώ και θα τους αγαπάω για πάντα.

'Sic Parvis Magna'

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Κεφάλαιο 1ο – Εισαγωγή

1.1 Αντικείμενο έρευνας

Οι εξυπηρετητές ιστού και ως συνέπεια τα πληροφοριακά συστήματα είναι για μία επιχείρηση, τα σημαντικότερα τεχνολογικά αγαθά. Μέσα σε αυτά βρίσκονται ευαίσθητα προσωπικά δεδομένα τόσο των χρηστών-πελατών της αλλά και στοιχεία της ίδιας επιχείρησης. Το σύνολο αυτών των δεδομένων πρέπει να προστατεύονται από κακόβουλες επιθέσεις που διεξάγονται στον χώρο του Διαδικτύου. Οι κακόβουλοι χρήστες μπορούν να έχουν ως στόχο, όχι μόνο την υποκλοπή αυτών αλλά και την διαταραχή της ομαλής λειτουργίας του συνόλου των συστημάτων μίας επιχείρησης, μέσω επιθέσεων άρνησης παροχής υπηρεσιών.

Οι διαχειριστές των συστημάτων της επιχείρησης πρέπει να αντιμετωπίσουν ένα μεγάλο εύρος επιθέσεων για διαφορετικά σενάρια χρήσης τους. Για αυτό το λόγο, είναι αναγκαία η ύπαρξη οδηγών επαύξησης ασφάλειας τόσο του λειτουργικού συστήματος που χρησιμοποιούνται όπως και για τα υπόλοιπα λογισμικά-υπηρεσίες (όπως ο Apache, το sshd κ.α.).

Διάφοροι οργανισμοί που ασχολούνται με τον τομέα της κυβερνοάμυνας έχουν φτιάξει αναλυτικούς οδηγούς για πολλούς τρόπους χρήσης (use cases) συστημάτων ακόμα και έτοιμες ‘εικόνες’ ωστόσο δεν βρέθηκε πλήρης οδηγός για έναν εξυπηρετητή ιστού που χρησιμοποιεί λειτουργικό CentOS αλλά να περιέχει ασφάλεια για Apache καθώς και τρόπους άμυνας για επιθέσεις τύπου άρνησης παροχής υπηρεσιών, Slowloris.

Η παρούσα εργασία έχει ακριβώς αυτό τον στόχο, δηλαδή την δημιουργία ενός οδηγού για το παραπάνω σενάριο χρήσης καθώς και την δημιουργία αυτοματοποιημένου εργαλείου για την επαύξηση ασφάλειας του συστήματος. Έπειτα, θα χρησιμοποιηθούν εργαλεία για ανίχνευση ευπαθειών και αποτίμησης ασφάλειας καθώς θα διεξαχθούν επιθέσεις τύπου Slowloris προς το σύστημα. Στο τέλος, θα βγουν τα συμπεράσματα της εργασίας όπως το τελικό επίπεδο ασφάλειας που παρέχεται και το κατά πόσο εύκολη ήταν η αντιμετώπιση της επίθεσης Slowloris.

1.2 Διάρθρωση εργασίας

Η παρούσα εργασία έχει χωριστεί σε 5 κεφάλαια, επιπλέον του πίνακα περιεχομένων, του πίνακα εικόνων καθώς και της βιβλιογραφίας, τα οποία παρουσιάζονται στη συνέχεια αυτής της ενότητας.

Κεφάλαιο 1ο

Ο λόγος ύπαρξης του παρόντος κεφαλαίου είναι η εισαγωγή στις τεχνολογίες που θα χρησιμοποιήσουμε στην συγκεκριμένη εργασία. Πιο συγκεκριμένα, θα παρουσιαστούν τα πλεονεκτήματα καθώς και τα μειονεκτήματα χρήσης των τεχνολογιών CentOS και Apache και το ποσοστό χρήσης του στην αγορά. Έπειτα, θα αναφερθούμε στην επίθεση άρνησης παροχής υπηρεσιών, Slowloris, τα βασικά χαρακτηριστικά της, πώς υλοποιείται, ποια αδυναμία του εξυπηρετητή ιστου Apache εκμεταλλεύεται. Είναι το σενάριο επίθεσης που καλούμαστε να παρέχουμε τρόπο αντιμετώπισης για το σύστημά μας.

Κεφάλαιο 2ο

Σε αυτό το κεφάλαιο παρουσιάζονται οι καλύτερες πρακτικές για την επαύξηση του λειτουργικού συστήματος CentOS 7. Κάθε υποκεφάλαιο θα περιέχει και μία πρακτική, το λόγο που προτείνεται να υλοποιηθεί, τον τρόπο υλοποίησης κατά μονάς καθώς και του τρόπου ελέγχου αυτής (ότι έχει υλοποιηθεί και εφαρμοστεί σωστά στο σύστημα).

Έπειτα, παρουσιάζονται οι καλύτερες πρακτικές για επαύξηση ασφάλειας του εξυπηρετητή ιστου Apache καθώς και οι τρόποι αντιμετώπισης της επίθεσης Slowloris, μέσω αρθρωμάτων.

Κεφάλαιο 3ο

Στο 3ο κεφάλαιο βρίσκεται το πρακτικό κομμάτι της εργασίας, το Bash Script. Υπάρχει, μία λίστα με τις λειτουργίες – δυνατότητες του Script και στην συνέχεια υπάρχει σε πίνακα το περιεχόμενο (ο κώδικας) του. Ουσιαστικά, πρόκειται για τον συνδυασμό των τρόπων υλοποίησης των καλύτερων πρακτικών του κεφαλαίου 2 για την δική μας περίπτωση χρήσης καθώς και επιπλέον βήματα σε περίπτωση που το περιβάλλον μας είναι ‘εικονικό’ (Virtual Machine).

Κεφάλαιο 4ο

Στο 4ο κεφάλαιο γίνονται έλεγχοι με διάφορα προγράμματα για το επίπεδο ασφαλείας του συστήματός μας. Οι έλεγχοι γίνονται σε δύο φάσεις. Αρχικά, παρουσιάζονται οι έλεγχοι πριν την χρήση του Script, πριν γίνει η επαύξηση της ασφάλειας

του συστήματος και στην συνέχεια ακολουθούν τα αποτελέσματα μετά την επαύξηση. Τέλος, γίνονται επιθέσεις HTTP Flood και Slowloris κατά του συστήματός μας πριν και μετά την εισαγωγή ασφάλειας για αυτήν καθώς αναλύονται και σενάρια επίθεσης και τον αναμενόμενο τρόπο αντίδρασης που θα έχει το σύστημά μας.

Κεφάλαιο 5ο

Στο τελευταίο κεφάλαιο βρίσκονται τα συμπεράσματα της εργασίας καθώς και πιθανοί τρόποι βελτίωσης του παραδοτέου Script.

1.3 Το λειτουργικό σύστημα CentOS

Το CentOS (**C**ommunity **ent**erprise **O**perating **S**ystem) είναι ένα λειτουργικό σύστημα διανομής Linux - Fedora το οποίο είναι ανοιχτού κώδικα και συντηρείται από την κοινότητα που το δημιούργησε – χρησιμοποιεί. Ουσιαστικά, πρόκειται για ένα λειτουργικό σύστημα με ίδιες δυνατότητες με το RHEL με κύρια διαφορά ότι παρέχεται δωρεάν. Πρόκειται για ένα από τα πιο σταθερά λειτουργικά συστήματα και όντας ανοιχτού κώδικα και Linux είναι πλήρες παραμετροποιήσιμο. Για τους παραπάνω λόγους, προτιμάται από πολλούς διαχειριστές συστημάτων ως βάση για εξυπηρετητές ιστού.

Ωστόσο, υπάρχει καθυστέρηση στις αναβαθμίσεις σε σχέση με το πότε εκτελούνται στο RHEL και μερικά πακέτα λογισμικού δεν ανανεώνονται το ίδιο συχνά σε σχέση με άλλες διανομές. Εάν και οι χρήστες μπορούν να βασιστούν στον οδηγό χρήσης του RHEL λόγω αλληλοεπικάλυψης, υπάρχει έλλειψη αναλυτικού οδηγού για το CentOS ενώ σε περίπτωση προβλήματος δεν παρέχεται «επίσημη» υποστήριξη παρά μόνο από την κοινότητα.

Τέλος, πρόσφατα ανακοινώθηκε το τέλος υποστήριξης του λειτουργικού από την Red Hat το οποίο αποτελεί το μεγαλύτερο με προκάλεσε αντιδράσεις από την κοινότητα που το χρησιμοποιεί τόσα χρόνια. Η έκδοση 7 θα λάβει την τελευταία ενημέρωση το 2024 ενώ η έκδοση 8 τέλη του 2021. Το CentOS θα συνεχίσει να υπάρχει σε μία διαφορετική μορφή ‘rolling release’ όπου θα αναβαθμίζεται συνεχώς και πιθανώς να δημιουργηθούν προβλήματα σταθερότητας του λειτουργικού συστήματος.

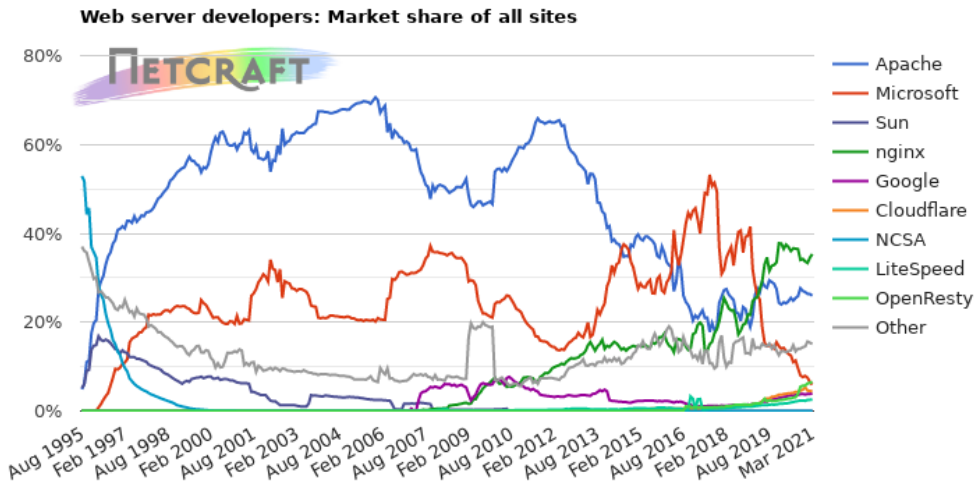
Στην παρούσα εργασία χρησιμοποιήθηκε η έκδοση CentOS 7.8.2003 64-bit. Ωστόσο, το Bash Script δοκιμάστηκε και στην έκδοση CentOS 8.2.2004 64-bit με ελάχιστες τροποποιήσεις για να είναι δυνατή η ομαλή εκτέλεσή του.

1.4 Ο εξυπηρετητής ιστού Apache

Ο εξυπηρετητής ιστού Apache είναι ένα πρόγραμμα το οποίο μπορεί να χρησιμοποιηθεί σε συνδυασμό με πολλά λειτουργικά συστήματα και χρησιμοποιείται για να φιλοξενεί ιστοσελίδες. Είναι και αυτός ανοιχτού κώδικα λογισμικό και διατίθεται δωρεάν από το 1993. Μπορεί να συνεργαστεί με συστήματα διαχείρισης βάσης δεδομένων όπως MySQL, Oracle. Το πρόγραμμα Apache περιέχει αρκετές δυνατότητες σε μορφή αρθρωμάτων (modules) με τα πιο δημοφιλή να είναι το mod_auth_digest για αυθεντικοποίηση, το mod_ssl για υποστήριξη SSL/TLS, το mod_proxy και mod_rewrite ενώ για επαύξηση ασφαλείας μπορεί να χρησιμοποιηθεί το τείχος προστασίας διαδικτυακής εφαρμογής (WAF), mod_security. Ενημερώνεται συχνά από τους δημιουργούς του ώστε να περιέχει προστασία από πρόσφατες ευπάθειες που έχουν ανακαλυφθεί. Τέλος, το μεγαλύτερο πλεονέκτημα χρήσης του Apache είναι η χρήση εικονικών «εξυπηρετητών» με αποτέλεσμα να μπορεί να φιλοξενεί πολλές ιστοσελίδες ταυτόχρονα.

Ωστόσο, είναι αργό σε σχέση με άλλα τέτοια προγράμματα όσο αφορά την εξυπηρέτηση στατικών ιστοσελίδων ενώ παράλληλα καταναλώνει σχετικά πολλούς πόρους του συστήματος. Η καμπύλη εκμάθησης για νέους χρήστες είναι αρκετά υψηλή παρόλο που υπάρχει αρκετό υλικό για την σωστή παραμετροποίησή του. Τέλος, ο Apache είναι ευάλωτος σε επιθέσεις τύπου άρνησης παροχής υπηρεσιών Slowloris λόγω του τρόπου λειτουργίας του δηλαδή της δημιουργίας καινούργιου socket για κάθε νέα σύνδεση.

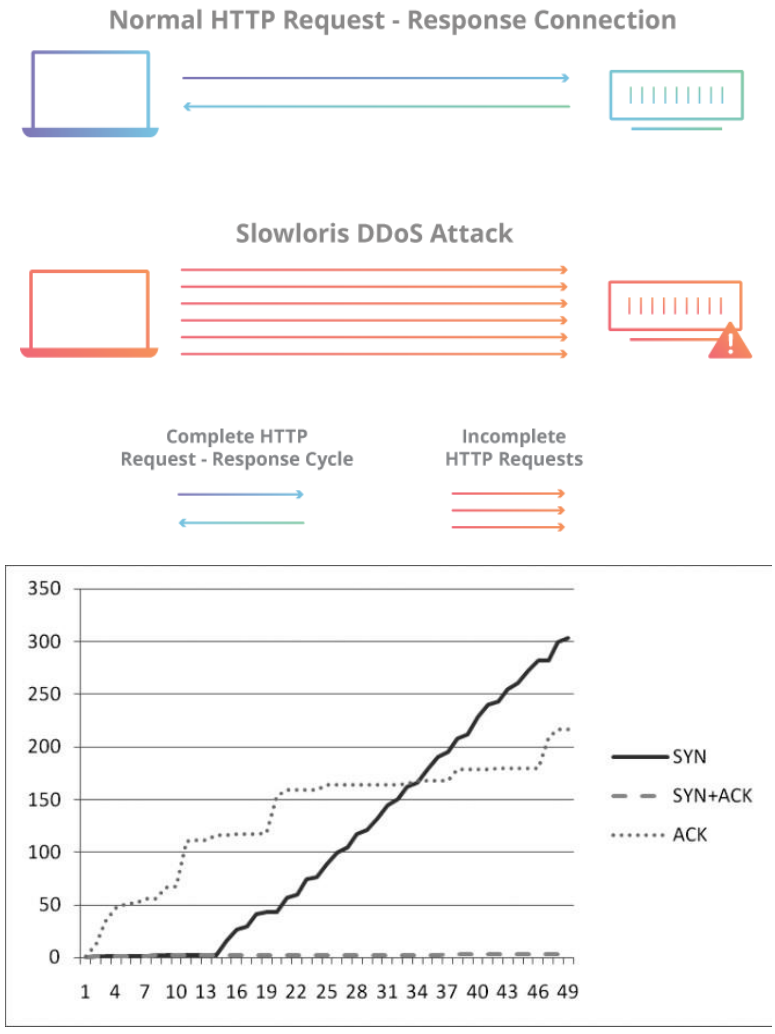
Παρόλο τα αναφερθέντα προβλήματα, μέχρι και σήμερα κατέχει το δεύτερο υψηλότερο μερίδιο χρήσης στην αγορά από το σύνολο των προγραμμάτων εξυπηρετητή ιστού.



Εικόνα 1 - Μερίδιο χρήσης Apache στην αγορά (Πηγή: Netcraft)

1.5 Η επίθεση άρνησης παροχής υπηρεσιών Slowloris

Η επίθεση άρνησης παροχής υπηρεσιών Slowloris επιτρέπει σε έναν κακόβουλο χρήστη να θέσει εκτός λειτουργίας έναν εξυπηρετητή ιστού με ελάχιστους υπολογιστικούς πόρους ακόμα έχοντας και μικρό εύρος ζώνης (bandwidth). Πιο συγκεκριμένα, εκμεταλλεύεται την προ αναφέρουσα ευπάθεια του λογισμικού Apache και δημιουργεί πολλές συνδέσεις HTTP μεταξύ του τερματικού του επιτιθέμενου και του εξυπηρετητή, χωρίς αυτές να τερματίζονται ποτέ με αποτέλεσμα να μην έχει άλλα διαθέσιμα sockets για τους νόμιμους πελάτες του συστήματος. Αυτό επιτυγχάνεται στέλνοντας πολλά μη ολοκληρωμένα αιτήματα (requests), στέλνοντας ελάχιστα δεδομένα κάθε φορά και σε τακτά χρονικά διαστήματα ώστε να μην τερματιστεί (timeout) η σύνδεση με τον εξυπηρετητή. Έτσι, ο εξυπηρετητής ανοίγει πολλά sockets, ένα για κάθε αίτημα, εκλαμβάνεται πως ένας νόμιμος χρήστης έχει απλά αργή σύνδεση με αυτόν και δεν απελευθερώνεται ποτέ κανένα από τα sockets. Ακολουθεί ένα διάγραμμα που αναπαριστά μία τέτοια επίθεση καθώς και τα πακέτα που καταγράφονται.



Εικόνα 2 - Διαγράμματα επιθέσεις τύπου Slowloris

Για την διεξαγωγή μίας τέτοιας επίθεσης υπάρχουν έτοιμα εργαλεία σε διάφορες γλώσσες προγραμματισμού με το πιο διαδεδομένο εργαλείο να είναι το pyloris, υλοποιημένο σε Python. Συνεπώς, δεν χρειάζονται ιδιαίτερες τεχνικές γνώσεις για να διεξαχθεί η επίθεση προς έναν στόχο. Αρκεί κάποιος να γνωρίζει την IP του θύματος (της ιστοσελίδας) και το λογισμικό εξυπηρετητή ιστού.

Όπως θα δούμε και στο επόμενο κεφάλαιο όπου θα βρίσκονται οι καλύτερες πρακτικές για επαύξηση ασφαλείας, υπάρχουν πολλοί τρόποι άμυνας έναντι μίας τέτοιας επίθεσης. Αρχικά, μπορεί να αυξηθεί το πλήθος των πελατών που μπορούν να συνδεθούν στον εξυπηρετητή, ωστόσο σίγουρα είναι η λύση με το μεγαλύτερο κόστος. Έπειτα, υπάρχει η δυνατότητα περιορισμού του πλήθους συνδέσεων που μπορεί να γίνει από έναν χρήστη (δηλαδή από μία IP) προς τον εξυπηρετητή. Αυτό, μπορεί να επιτευχθεί με την χρήση των iptables, με αναχώματα ασφαλείας (firewalls) καθώς και με την χρήση αρθρωμάτων του Apache. Τέλος, μπορεί να καθοριστεί ένα κατώφλι ελάχιστης ταχύτητας που μπορεί ένας χρήστης να στέλνει δεδομένα ή ένα χρονικό περιθώριο που ο χρήστης θα παραμένει συνδεδεμένος στον εξυπηρετητή. Τα δύο τελευταία δεν είναι ιδανικά καθώς μπορούν εξ’ αρχής να αποκλείουν και νόμιμους χρήστες του συστήματος. Στην παρούσα εργασία χρησιμοποιήθηκε ένας συνδυασμός αναχώματος ασφαλείας (ufw-iptables) και αρθρωμάτων Apache (mod_qos, mod_security) για την αντιμετώπιση επιθέσεων Slowloris.

1.6 Εισαγωγή στην ασφάλεια πληροφοριακών συστημάτων

Η ασφάλεια είναι ένας γενικός όρος, ο οποίος καλύπτει μια ευρεία περιοχή της επιστήμης των υπολογιστών αλλά και της επεξεργασίας και προστασίας των πληροφοριών. Αρκετοί σύμβουλοι ασφαλείας πληροφορικής, καθώς και εταιρίες του χώρου της κυβερνο-ασφάλειας συμφωνούν στο κοινώς αποδεκτό μοντέλο, γνωστό και ως η τριάδα ΕΑΔ (CIA triad) τα οποία είναι αρχικά για: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα. Αυτό το τρίπτυχο θεωρείται ως γενικά αποδεκτό για την αξιολόγηση ασφαλείας των Πληροφοριακών Συστημάτων.

1) Εμπιστευτικότητα: Όταν ένα σύστημα τηρεί τον όρο της εμπιστευτικότητας αυτό σημαίνει ότι, οι ευαίσθητες πληροφορίες που περιέχει είναι διαθέσιμες μόνο σε ένα αυστηρά καθορισμένο σύνολο οντοτήτων – χρηστών. Μη εξουσιοδοτημένη εκπομπή και χρήση της ευαίσθητης αυτής πληροφορίας, περιορίζεται αυστηρά από το σύστημα.
2) Ακεραιότητα: Όταν τηρείται ο όρος της ακεραιότητας, η πληροφορία δεν αλλοιώνεται με οποιοδήποτε τρόπο, ο οποίος την καθιστά ελλιπή ή εσφαλμένη. Έτσι, μη εξουσιοδοτημένοι χρήστες δεν έχουν τη δυνατότητα να τροποποιούν ή να καταστρέφουν ευαίσθητα δεδομένα του συστήματος.
3) Διαθεσιμότητα: Οι πληροφορίες θα πρέπει να είναι διαθέσιμες στους νόμιμους πελάτες κάθε φορά που ζητούν πρόσβαση σε αυτήν.

Όταν ένα σύστημα πληροί το τρίπτυχο ΕΑΔ τότε θεωρείται ότι είναι ασφαλές (Secure).

Εικόνα 3 - Η τριάδα ΕΑΔ (CIA)

1.7 Κατηγορίες ελέγχων ασφάλειας συστήματος

Μπορούμε να χωρίσουμε τους ελέγχους που μπορούν να γίνουν σε ένα πληροφοριακό σύστημα σε τρεις κατηγορίες:

1) Φυσικοί έλεγχοι στους οποίους περιλαμβάνονται όλα τα μέτρα ασφαλείας που αφορούν τη φυσική προστασία των υποδομών και των συστημάτων μίας εταιρείας. Φυσικός έλεγχος μπορεί να θεωρηθεί η εξουσιοδότηση προσωπικού στο δωμάτιο των εξυπηρετητών.
2) Τεχνικοί έλεγχοι οι οποίοι αφορούν την εγκατάσταση και την παραμετροποίηση πολιτικών ασφαλείας σε ένα υποσύστημα ή εάν είναι δυνατόν, στο σύνολο του εξοπλισμού της επιχείρησης.
3) Διαχειριστικοί έλεγχοι οι οποίοι αφορούν τον πλήρη έλεγχο της σωστής εφαρμογής όλων των πολιτικών ασφαλείας για κάθε υποσύστημα που υπόκειται στον οργανισμό. Συμπεριλαμβάνονται και οι φυσικοί έλεγχοι.

Στο επόμενο κεφάλαιο παρουσιάζονται οι καλύτερες πρακτικές - ρυθμίσεις ασφαλείας που μπορούν να εφαρμοστούν σε ένα σύστημα λειτουργικού CentOS 7 ο οποίος χρησιμοποιείται ως εξυπηρετητής ιστού από τον οργανισμό.

Κεφάλαιο 2ο – Καλύτερες πρακτικές

2.1 Εισαγωγή στις καλύτερες πρακτικές

Αναφερόμενοι στον όρο «καλύτερη πρακτική» εννοούμε μία μέθοδο η οποία έχει αποδεχθεί αντικειμενικά ότι παράγει το καλύτερο δυνατό αποτέλεσμα από άλλες εναλλακτικές επιλογές. Αυτή η μέθοδο μπορεί να έχει γίνει και επίσημο στάνταρ από κάποιον οργανισμό όπως είναι ο Διεθνής Οργανισμός Τυποποίησης (ISO) ή να προτείνονται από μη-κερδοσκοπικές κοινότητες που ενασχολούνται με τον τομέα της κυβερνο-ασφάλειας όπως είναι το Κέντρο Ασφάλειας Διαδικτύου (Center For Internet Security – CIS) ως μέσα θωράκισης των συστημάτων.

Όταν ακολουθούνται οι καλύτερες πρακτικές τότε μία επιχείρηση μπορεί να λάβει πιστοποιήσεις όπως την ISO-27001 για τα πληροφοριακά της συστήματα και έτσι έχει έναν τρόπο απόδειξης προς τους πελάτες της ότι τα δεδομένα τους είναι ασφαλή. Για να ληφθεί αυτή η πιστοποίηση πρέπει ο οργανισμός να αξιολογηθεί από ειδικό σωματείο πιστοποιήσεων. Ωστόσο, η τήρηση των περισσότερων καλύτερων πρακτικών από μία λίστα ελέγχου (checklist), δίνει μεγαλύτερες πιθανότητες επιτυχούς λήψης της πιστοποίησης.

2.2 Καλύτερες πρακτικές – Επαύξηση ασφάλειας CentOS

Σε αυτό το κεφάλαιο θα παρουσιαστούν οι καλύτερες πρακτικές για την επαύξηση ασφάλειας του λειτουργικού συστήματος CentOS. Αξίζει να σημειωθεί ότι αυτές οι καλύτερες πρακτικές μπορούν να εφαρμοστούν και σε άλλα λειτουργικά συστήματα τύπου Linux με σχετικές τροποποιήσεις στις εντολές που εκτελούνται καθώς και στην διαδρομή όπου βρίσκονται τα αρχεία παραμετροποίησης.

2.2.1 Ρυθμίσεις ασφάλειας κατά την εκκίνηση

Είναι μία καλή πρακτική στο να ασφαλίζονται τα παρακάτω με κωδικούς πρόσβασης: το BIOS, ο GRUB Bootloader καθώς και να κρυπτογραφείται όλος ο σκληρός δίσκος μέσω του LUKS (**L**inux **U**nified **K**ey **S**etup).

2.2.1.1 Κωδικός πρόσβασης στα BIOS

Η ύπαρξη ενός κωδικού για την είσοδο στο BIOS (**B**asic **I**nput **O**utput **S**ystem) αποτρέπει έναν κακόβουλο χρήστη που έχει φυσική πρόσβαση στο σύστημα να αλλάξει την σειρά εκκίνησης και να διαλέξει ένα λειτουργικό από κάποιο αποθηκευτικό μέσο όπως ένα CD-ROM η USB.

Τρόπος Ενεργοποίησης:

Ο κωδικός πρόσβασης ρυθμίζεται από την καρτέλα Security μέσα από το BIOS. Επιλέγουμε και την επιλογή 'Password on Boot'. Έπειτα, αποθηκεύουμε τις αλλαγές και γίνεται επανεκκίνηση του συστήματος.

Τρόπος Ελέγχου:

΄ Ανεξαρτήτως εάν θέλουμε να μπούμε στο BIOS πρέπει το σύστημα να μας ζητήσει κωδικό. Αυτό είναι καλή πρακτική διότι διαπιστώθηκε πως υπάρχει η δυνατότητα αλλαγής του μέσου εκκίνησης χωρίς την είσοδο μας στο BIOS, μπαίνοντας απλά στο Boot Menu. Για αυτό και επιλέξαμε την παραπάνω επιλογή.

Εικόνα 4 - Είσοδος κωδικού πρόσβασης στο BIOS

2.2.1.2 Κωδικός πρόσβασης στον GRUB Bootloader

Έπειτα από το BIOS ενεργοποιείται ο GRUB Bootloader ώστε να εισέλθουμε στο λειτουργικό σύστημα, ακόμα και να επιλέξουμε την έκδοση του Kernel που θα χρησιμοποιήσουμε. Ωστόσο, εάν δεν υπάρχει κωδικός πρόσβασης δίνεται η δυνατότητα σε έναν κακόβουλο χρήστη να εισάγει παραμέτρους μέσω της γραμμής εντολών (πατώντας e στην οθόνη του GRUB) και να μειώσει την ασφάλεια του συστήματος (λ.χ. Να απενεργοποιήσει το SELinux κατά την εκκίνηση) ακόμα και να αλλάξει από εκεί το διαμέρισμα εκκίνησης.

Τρόπος Ενεργοποίησης:

Δημιουργούμε έναν κρυπτογραφημένο κωδικό χρησιμοποιώντας την εντολή:

```
grub2-mkpasswd-pbkdf2
```

Εισάγουμε δύο φορές τον κωδικό και έπειτα το πρόγραμμα τον εκτυπώνει σαν hash output. Αντιγράφουμε τον κωδικό μετά την λέξη 'is' και έπειτα είτε τροποποιούμε το αρχείο στην διαδρομή: /etc/grub.d/01_users ή δημιουργούμε ένα νέο αρχείο παραμετροποίησης στην διαδρομή: /etc/grub.d (Επιλέξαμε την δεύτερη επιλογή).

```
cat << EOF
set superusers=myuser
password_pbkdf2 myuser
grub.pbkdf2.sha512.10000.2DADF8924FEAD25BCAB767126BD4F614A1D796B330BCD090A97025
B7A6E46F888DA80D62F632CF0012162858523880A04C4255535CDA50AD05669E59C54B98A1.EC
9A26BEEE3FF4B6B41B5ADAA614B4E6CBB0488938ED5851A78E252908ED02CDBDEE410CDF7
4B672EBFFF9073E8A7770B15F3DBCA26DF61FF2A2E464E940F43F
```

Έπειτα εκτελούμε την παρακάτω εντολή για την ενημέρωση του αρχείου παραμετροποίησης του Bootloader.

```
grub2-mkconfig > /boot/grub2/grub.cfg
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και επιβεβαιώνουμε ότι έχουμε το αναμενόμενο αποτέλεσμα.

```
grep "^set superusers" /boot/grub2/grub.cfg
grep "^password" /boot/grub2/grub.cfg
```

```
[admin@centos7 ~]$ sudo grep "^set superusers" /boot/grub2/grub.cfg
set superusers=myuser
[admin@centos7 ~]$ sudo grep "^password" /boot/grub2/grub.cfg
password_pbkdf2 myuser grub.pbkdf2.sha512.10000.2DADF8924FEAD25BCAB767126BD4F614
A1D796B330BCD090A97025B7A6E46F888DA80D62F632CF0012162858523880A04C4255535CDA50AD
05669E59C54B98A1.EC9A26BEEE3FF4B6B41B5ADAA614B4E6CBB0488938ED5851A78E252908ED02C
DBDEE410CDF74B672EBFFF9073E8A7770B15F3DBCA26DF61FF2A2E464E940F43F
```

Εικόνα 5 - Έλεγχος σωστής παραμετροποίησης κωδικού GRUB Bootloader

Κάνουμε και τον παρακάτω έλεγχο. Εισερχόμαστε στο σύστημα και κατά την επιλογή του Kernel του λειτουργικού μας πατάμε e για να μπούμε στην γραμμή εντολών – τροποποίησης εκκίνησης. Έχοντας κάνει σωστή παραμετροποίηση το σύστημα πρέπει να μας ζητήσει να εισάγουμε τον κωδικό.

```
CentOS Linux (3.10.0-1160.11.1.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-1127.el7.x86_64) 7 (Core)
CentOS Linux (0-rescue-60177cfa44424c639879e50d1c19e03e) 7 (Core)
```

Εικόνα 6 - Εισαγωγή κωδικού πρόσβασης GRUB Bootloader

2.2.1.3 Κρυπτογράφηση σκληρού δίσκου με χρήση LUKS

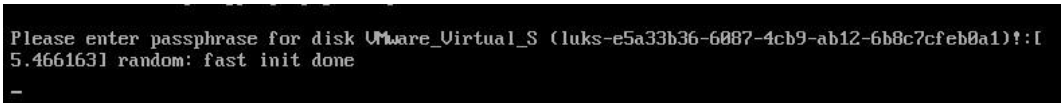
Σαν επιπλέον βήμα ασφάλειας των δεδομένων που υπάρχουν στον σκληρό δίσκο, αποτελεί η κρυπτογράφηση αυτού με κάποιο εργαλείο όπως το LUKS. Έτσι ακόμα και εάν κάποιος που έχει φυσική πρόσβαση αποκτήσει τον σκληρό δίσκο παράνομα, δεν θα μπορεί να αποκτήσει τα δεδομένα που περιέχει χωρίς αυτόν τον κωδικό.

Τρόπος Ενεργοποίησης:

Κατά την αρχική εγκατάσταση και τον διαμερισμό του δίσκου, έχουμε μία τέτοια επιλογή από το λειτουργικό CentOS. Δεν προτείνεται η κρυπτογράφηση των τόμων μετά την εγκατάσταση διότι ενδέχεται να προκαλέσει προβλήματα στην ομαλή λειτουργία του συστήματος.

Τρόπος Ελέγχου:

Αφού επιλέξουμε την έκδοση Kernel που θα χρησιμοποιήσουμε από τον GRUB Bootloader τότε θα μας ζητήσει ένα επιπλέον κωδικό για την αποκρυπτογράφησή του πριν φορτώσει τα υπόλοιπα δεδομένα.



Εικόνα 7 - Εισαγωγή κωδικού πρόσβασης για αποκρυπτογράφηση του δίσκου (LUKS)

2.2.2 Παραμετροποίηση μερών (partitions) συστήματος

Διαδρομές οι οποίες χρησιμοποιούνται από συναρτήσεις του συστήματος μπορούν να προστατευτούν καλύτερα εάν τοποθετηθούν σε ξεχωριστά μέρη (partition) του δίσκου. Αυτή η πρακτική επιτρέπει στους διαχειριστές να ενεργοποιήσουν διαφορετικές επιλογές μονταρίσματος (mount options) ανά μέρος ανάλογα την ενδεδειγμένη χρήση του καθώς

επίσης αποτρέπει το σύστημα να ξεμείνει από πόρους. Για παράδειγμα, τα δεδομένα των χρηστών μπορούν να αποθηκευτούν σε ξεχωριστό μέρος το οποίο να έχει πιο αυστηρές επιλογές μονταρίσματος. Σε εκείνο το μέρος δεν πρέπει να βρίσκεται λογισμικό το οποίο είναι απαραίτητο για την λειτουργία του συστήματος.

Χρήσιμες επιλογές μονταρίσματος είναι οι παρακάτω:

1) noexec η οποία αποτρέπει έναν επιτιθέμενο από το να εισάγει κακόβουλο κώδικα προς εκτέλεση.
2) nodev η οποία δεν επιτρέπει στο μέρος να έχει αρχεία ειδικών συσκευών.
3) nosuid η οποία αποτρέπει τους χρήστες να δημιουργήσουν setuid αρχεία.

Οι καλύτερες πρακτικές που βρίσκονται σε αυτό το κεφάλαιο είναι καλύτερα να τεθούν σε εφαρμογή κατά την αρχική εγκατάσταση του CentOS καθώς ο διαμερισμός του δίσκου σε μεταγενέστερο στάδιο είναι πιο δύσκολος και μπορεί να οδηγήσει σε απώλεια των δεδομένων. Σε τέτοια περίπτωση, προτείνεται η χρήση backup του δίσκου.

2.2.2.1 Δημιουργία ξεχωριστού μέρους /tmp και επιλογές μονταρίσματος

Η διαδρομή /tmp χρησιμοποιείται για την προσωρινή αποθήκευση δεδομένων από όλους τους χρήστες καθώς και για κάποιες εφαρμογές. Εάν χρησιμοποιήσουμε ένα ξεχωριστό μέρος για το /tmp μπορούμε να εισάγουμε τις επιλογές nodev, noexec, nosuid ώστε να ασφαλίσουμε το σύστημα από επίδοξους επιτιθέμενους.

Τρόπος Ενεργοποίησης:

Για νέες εγκαταστάσεις του λειτουργικού, δημιουργούμε ένα μέρος για το /tmp και έπειτα τροποποιούμε το αρχείο που βρίσκεται στην διαδρομή /etc/fstab για να βάλουμε τις κατάλληλες επιλογές μονταρίσματος και έπειτα ξεμοντάρουμε και ξανά μοντάρουμε το συγκεκριμένο μέρος στο σύστημά μας.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /tmp είναι μονταρισμένο και πως έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep /tmp
[admin@centos7 ~]$ mount | grep /tmp
/dev/mapper/centos_centos7-tmp on /tmp type ext4 (rw,nosuid,nodev,noexec,relatime,seclabel,data=ordered)
```

Εικόνα 8 - Μέρος /tmp και επιλογές μονταρίσματος

2.2.2.2 Δημιουργία ξεχωριστού μέρους /var/tmp και επιλογές μονταρίσματος

Όπως και η διαδρομή /tmp έτσι και η /var/tmp χρησιμοποιείται για προσωρινή αποθήκευση δεδομένων εφαρμογών καθώς και χρηστών του συστήματος. Συνεπώς, θέλουμε να εισάγουμε τις ίδιες επιλογές μονταρίσματος όπως με το μέρος /tmp.

Τρόπος Ενεργοποίησης:

Για νέες εγκαταστάσεις του λειτουργικού, δημιουργούμε ένα μέρος για το /var/tmp και έπειτα τροποποιούμε το αρχείο που βρίσκεται στην διαδρομή /etc/fstab για να βάλουμε τις κατάλληλες επιλογές μονταρίσματος και έπειτα ξεμοντάρουμε και ξανά μοντάρουμε το συγκεκριμένο μέρος στο σύστημά μας.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /var/tmp είναι μονταρισμένο και πως έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep var/tmp
```

```
[admin@centos7 ~]$ mount | grep var/tmp
/dev/mapper/centos_centos7-var_tmp on /var/tmp type ext4 (rw,nosuid,nodev,noexec,relatime,seclabel,data=ordered)
```

Εικόνα 9 - Μέρος /var/tmp και επιλογές μονταρίσματος

2.2.2.3 Δημιουργία ξεχωριστού μέρους /var/log και επιλογές μονταρίσματος

Είναι καλή πρακτική η δημιουργία ξεχωριστού μέρους για το /var/log το οποίο χρησιμοποιείται για την αποθήκευση αρχείων καταγραφής του συστήματος. Έτσι, το σύστημά μας δεν θα μείνει πότε από αποθηκευτικό χώρο καθώς αυτά τα αρχεία μπορεί να αποκτήσουν μεγάλο όγκο. Θα περιορίζονται στο διαθέσιμο χώρο του συγκεκριμένου μέρους. Παράλληλα, προστατεύουμε το περιεχόμενό τους από τροποποίηση από μη-εξουσιοδοτημένους χρήστες.

Τρόπος Ενεργοποίησης:

Για νέες εγκαταστάσεις του λειτουργικού, δημιουργούμε ένα μέρος για το /var/log και έπειτα τροποποιούμε το αρχείο που βρίσκεται στην διαδρομή /etc/fstab για να βάλουμε τις κατάλληλες επιλογές μονταρίσματος και έπειτα ξεμοντάρουμε και ξανά μοντάρουμε το συγκεκριμένο μέρος στο σύστημά μας.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /var/log είναι μονταρισμένο και πως έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep var/log
```

```
[admin@centos7 ~]$ mount | grep var/log
/dev/mapper/centos_centos7-var_log on /var/log type ext4 (rw,relatime,seclabel,data=ordered)
```

Εικόνα 10 - Μέρος /var/log και επιλογές μονταρίσματος

2.2.2.4 Δημιουργία ξεχωριστού μέρους /var/log/audit και επιλογές μονταρίσματος

Είναι καλή πρακτική η δημιουργία ξεχωριστού μέρους για το /var/log/audit το οποίο χρησιμοποιείται από το πρόγραμμα auditd για την αποθήκευση αρχείων καταγραφής συμβάντων του συστήματος. Έτσι, το σύστημά μας δεν θα μείνει πότε από αποθηκευτικό χώρο καθώς αυτά τα αρχεία μπορεί να αποκτήσουν μεγάλο όγκο. Θα περιορίζονται στο διαθέσιμο χώρο του συγκεκριμένου μέρους ενώ επιπλέον το πρόγραμμα auditd κάνει ενέργειες ανάλογα του διαθέσιμου χώρου. Παράλληλα, προστατεύουμε το περιεχόμενό τους από τροποποίηση από μη-εξουσιοδοτημένους χρήστες.

Τρόπος Ενεργοποίησης:

Για νέες εγκαταστάσεις του λειτουργικού, δημιουργούμε ένα μέρος για το /var/log/audit και έπειτα τροποποιούμε το αρχείο που βρίσκεται στην διαδρομή /etc/fstab για να βάλουμε τις κατάλληλες επιλογές μονταρίσματος και έπειτα ξεμοντάρουμε και ξανά μοντάρουμε το συγκεκριμένο μέρος στο σύστημά μας.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /var/log/audit είναι μονταρισμένο και πως έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep var/log/audit
```

```
[admin@centos7 ~]$ mount | grep var/log/audit
/dev/mapper/centos_centos7-var_log_audit on /var/log/audit type ext4 (rw,relatime,seclabel,data=ordered)
```

Εικόνα 11 - Μέρος /var/log/audit και επιλογές μονταρίσματος

2.2.2.5 Δημιουργία ξεχωριστού μέρους /home και επιλογές μονταρίσματος

Είναι καλή πρακτική η δημιουργία ξεχωριστού μέρους για το /home το οποίο χρησιμοποιείται για την αποθήκευση δεδομένων των τοπικών χρηστών. Με αυτό τον τρόπο μπορούμε να προστατεύσουμε το σύστημα από το να ξεμείνει από διαθέσιμο χώρο καθώς και να επιλέξουμε nodev στις επιλογές μονταρίσματος για να περιορίσουμε τον τύπο των αρχείων που θα μπορούν να αποθηκεύσουν οι χρήστες στο /home.

Τρόπος Ενεργοποίησης:

Για νέες εγκαταστάσεις του λειτουργικού, δημιουργούμε ένα μέρος για το /home και έπειτα τροποποιούμε το αρχείο που βρίσκεται στην διαδρομή /etc/fstab για να βάλουμε τις κατάλληλες επιλογές μονταρίσματος και έπειτα ξεμοντάρουμε και ξανά μοντάρουμε το συγκεκριμένο μέρος στο σύστημά μας.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /home είναι μονταρισμένο και πως έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep /home
[admin@centos7 ~]$ mount | grep /home
/dev/mapper/centos_centos7-home on /home type ext4 (rw,nodev,relatime,seclabel,data=ordered)
```

Εικόνα 12 - Μέρος /home και επιλογές μονταρίσματος

2.2.2.6 Μέρος /dev/shm και επιλογές μονταρίσματος

Είναι καλή πρακτική η ενεργοποίηση των επιλογών μονταρίσματος nosuid, nodev στην κοινόχρηστη μνήμη (shared memory). Στο λειτουργικό CentOS 7 είναι έτσι εξαρχής.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να ελέγξουμε εάν το μέρος /dev/shm έχει τις σωστές επιλογές μονταρίσματος.

```
mount | grep /dev/shm
[admin@centos7 ~]$ mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel)
```

Εικόνα 13 - Μέρος /dev/shm και επιλογές μονταρίσματος

2.2.3 Απενεργοποίηση μη-χρησιμοποιούμενων filesystems

Τα λειτουργικά συστήματα Linux και κατά επέκταση το CentOS, υποστηρίζουν ένα μεγάλο εύρος από filesystem. Είναι καλή πρακτική η απενεργοποίηση αυτών που δεν πρόκειται να χρησιμοποιηθούν στο σύστημά μας ώστε να μειωθεί το εύρος των διαθέσιμων επιθέσεων από κακόβουλους χρήστες. Μάλιστα κάποια από αυτά χρησιμοποιούνται για συγκεκριμένες υπηρεσίες ή είναι τόσο απαρχαιωμένα και δεν συντηρούνται και έτσι σίγουρα ενδείκνυται η απενεργοποίησή τους.

Παρακάτω ακολουθεί μία λίστα από αυτά που πρέπει να απενεργοποιηθούν:

Filesystems προς απενεργοποίηση	
cramfs	hfsplus
cifs	nfs
fat	nfsv3
freevxfs	nfsv4
gfs2	squashfs
jffs2	udf
hfs	vfat

Εικόνα 14 - Πίνακας filesystems προς απενεργοποίηση

Τρόπος Ενεργοποίησης:

Δημιουργούμε ένα καινούργιο αρχείο παραμετροποίησης (.conf) στην διαδρομή /etc/modprobe.d/ με οποιοδήποτε όνομα της επιλογής μας και μέσα σε αυτό γράφουμε για κάθε ένα από τα παραπάνω filesystems την ίδια γραμμή.

```
install όνομα_filesystem /bin/true
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και βλέπουμε εάν έχουμε το ίδιο αποτέλεσμα στο σύστημά μας. Όπου fat βάζουμε ένα-ένα τα παραπάνω filesystems.

```
modprobe -n -v fat
lsmod | grep fat
```

```
[admin@centos7 ~]$ modprobe -n -v fat
install /bin/true
[admin@centos7 ~]$ lsmod | grep fat
[admin@centos7 ~]$
```

Εικόνα 15 - Έλεγχος απενεργοποιημένων Filesystems

```
install cramfs /bin/true
install cifs /bin/true
install fat /bin/true
install freevxfs /bin/true
install gfs2 /bin/true
install jffs2 /bin/true
install hfs /bin/true
install hfsplus /bin/true
install nfs /bin/true
install nfsv3 /bin/true
install nfsv4 /bin/true
install squashfs /bin/true
install udf /bin/true
install vfat /bin/true
```

Εικόνα 16 - Τελικό αρχείο μέσα στο modprobe.d

2.2.4 Ρύθμιση ενημερώσεων λογισμικού

Είναι σημαντικό να έχουμε τις τελευταίες ενημερώσεις για τα προγράμματα που χρησιμοποιούμε καθώς σε αυτές εμπεριέχονται αλλαγές που διορθώνουν λάθη ή ευπάθειες που δημοσιεύθηκαν με κάποιο CVE. Το λειτουργικό CentOS 7 χρησιμοποιεί το yum για την διαχείριση, την ενημέρωση και την εγκατάσταση των πακέτων.

2.2.4.1 Έλεγχος σωστής παραμετροποίησης του YUM και των repositories

Ένα σύστημα πρέπει να έχει ενεργοποιημένο και σωστά ρυθμισμένο το λογισμικό διαχείρισης πακέτων ώστε να έχει πρόσβαση στις τελευταίες ενημερώσεις των προγραμμάτων από τα repositories.

Τρόπος Ενεργοποίησης:

Ανάλογα το σύστημα, μπορεί να γίνει επιλογή ξεχωριστού λογισμικού διαχείρισης πακέτων ή ακόμα και εισαγωγή ειδικών repositories.

Τρόπος Ελέγχου:

Δεδομένου χρήσης του λογισμικού διαχείρισης πακέτων YUM εκτελούμε την εντολή.

```
yum repolist
```

```
[admin@centos7 ~]$ yum repolist
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.ntua.gr
 * epel: ftp.cc.uoc.gr
 * extras: ftp.ntua.gr
 * updates: ftp.ntua.gr
repo id               repo name                                        status
base/7/x86_64         CentOS-7 - Base                                  10,072
epel/x86_64           Extra Packages for Enterprise Linux 7 - x86_64   13,592
extras/7/x86_64       CentOS-7 - Extras                                   476
updates/7/x86_64      CentOS-7 - Updates                                2,189
repolist: 26,329
```

Εικόνα 17 - Έλεγχος YUM Repositories

2.2.4.2 Έλεγχος κλειδιών GPG των πακέτων προγραμμάτων

Το RPM (και κατά επέκταση το YUM) χρησιμοποιεί υπογραφή μέσω GPG κλειδιού για επιβεβαίωση της ακεραιότητας των πακέτων προγραμμάτων. Με αυτό το τρόπο, ο χρήστης είναι σίγουρος πως εγκαθιστά πακέτα από έγκυρη πηγή και όχι κάποιο ‘rogue’ ή κακόβουλα τροποποιημένο πακέτο.

Τρόπος Ενεργοποίησης:

Ανάλογα το σύστημα, μπορεί να γίνει ενημέρωση των GPG κλειδιών για κάθε περίσταση.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή και ελέγχουμε το αποτέλεσμα.

```
rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
[admin@centos7 ~]$ rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
gpg-pubkey-f4a80eb5-53a7ff4b --> gpg(CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>)
gpg-pubkey-352c64e5-52ae6884 --> gpg(Fedora EPEL (7) <epel@fedoraproject.org>)
```

Εικόνα 18 - Έλεγχος κλειδιών GPG για την ακεραιότητα των πακέτων

2.2.4.3 Αλλαγή παραμέτρου gpgcheck

Για να εκτελείται όντως ο έλεγχος πριν την εγκατάσταση των πακέτων προγραμμάτων, πρέπει στο αρχείο στην διαδρομή /etc/yum.conf καθώς και στα ξεχωριστά αρχεία στην διαδρομή /etc/yum/repos.d/* να έχουν παράμετρο gpgcheck=1.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/yum.conf και στο σημείο main στο gpgcheck βάζουμε 1. Επιπλέον, για κάθε πακέτο που αποτυγχάνει τον παρακάτω έλεγχο πηγαίνουμε στην διαδρομή /etc/yum.repos.d/* και βάζουμε και εκεί gpgcheck, 1.

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και ελέγχουμε το αποτέλεσμα.

```
grep ^gpgcheck /etc/yum.conf
grep ^gpgcheck /etc/yum.repos.d/*
```

```
[admin@centos7 ~]$ grep ^gpgcheck /etc/yum.conf
gpgcheck=1
[admin@centos7 ~]$ grep ^gpgcheck /etc/yum.repos.d/*
/etc/yum.repos.d/CentOS-Base.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Base.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Base.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Base.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-CR.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Debuginfo.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-fasttrack.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Media.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Sources.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Sources.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Sources.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Sources.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
/etc/yum.repos.d/CentOS-Vault.repo:gpgcheck=1
```

Εικόνα 19 - gpgcheck στα repositories

2.2.5 Έλεγχος ακεραιότητας αρχείων

Είναι καλή πρακτική η ύπαρξη λογισμικού το οποίο ελέγχει τα αρχεία παραμετροποίησης (.conf) για αλλαγές και να ειδοποιεί τον διαχειριστή του συστήματος. Τέτοια λογισμικά είναι το Tripwire και το AIDE. Επιλέξαμε το δεύτερο καθώς αποτελεί την βέλτιστη λύση.

2.2.5.1 Εγκατάσταση και ρύθμιση του AIDE

Το AIDE (**A**dvanced **I**ntrustion **D**etection **E**nvironment) χρησιμοποιεί ένα σύστημα με snapshots ώστε να ελέγχει την κατάσταση των αρχείων, το χρονικό σημείο που τροποποιήθηκαν, τα δικαιώματα καθώς και το hash output τους σε σχέση με την τωρινή κατάσταση του συστήματος. Σε περίπτωση αλλαγών ειδοποιεί τον διαχειριστή. Τέλος, για την ομαλή λειτουργία του AIDE πρέπει να απενεργοποιηθεί η δυνατότητα του prelink χρησιμοποιώντας τις παρακάτω εντολές.

```
prelink -ua
yum remove prelink
```

Το prelink αλλάζει αρχεία binaries και έτσι το AIDE θα ανιχνεύει αλλαγές δημιουργώντας καταστάσεις ειδοποιήσεων false positive.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις παρακάτω εντολές για εγκατάσταση και αρχική εκκίνηση του AIDE.

```
yum install aide
aide --init
aide --init # mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και ελέγχουμε εάν έχουμε εγκατεστημένο το AIDE βλέποντας και την έκδοσή του.

```
rpm -q aide
[admin@centos7 ~]$ rpm -q aide
aide-0.15.1-13.el7.x86_64
```

Εικόνα 20 - Έλεγχος εγκατάστασης AIDE

2.2.5.2 Έλεγχος ακεραιότητας σε τακτά χρονικά διαστήματα

Ενδείκνυται η χρήση του AIDE με cronjobs ώστε να ελέγχεται η ακεραιότητα των αρχείων του συστήματος αυτόματα και ανά τακτά χρονικά διαστήματα.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις παρακάτω εντολές για ρύθμιση ενός cronjob για το AIDE.

```
crontab -u root -e
0 5 * * * /usr/sbin/aide --check
```

Σημείωση:

Με τις παραπάνω εντολές θα δημιουργηθεί ένα cronjob το οποίο θα ενεργοποιεί το AIDE κάθε μέρα στης 05:00. Η δεύτερη εντολή καθορίζει το χρονικό διάστημα που θα εκτελείται το AIDE. Τροποποιήστε την κατάλληλα ώστε να ταιριάζει με την δική σας πολιτική του συστήματος.

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και ελέγχουμε εάν υπάρχει cronjob για το AIDE. Αποτέλεσμα μπορεί να δώσει μία από τις δύο εντολές.

```
crontab -u root -l | grep aide
grep -r aide /etc/cron.* /etc/crontab
```

```
[admin@centos7 ~]$ sudo crontab -u root -l | grep aide
no crontab for root
[admin@centos7 ~]$ sudo grep -r aide /etc/cron.* /etc/crontab
/etc/crontab:05 4 * * * root /usr/sbin/aide --check
```

Εικόνα 21 - Έλεγχος cronjob για το AIDE

2.2.6 Ασφάλεια αρχείων εκκίνησης (GRUB Bootloader)

Σε προηγούμενο κεφάλαιο (2.2.1.2) ενεργοποιήσαμε κωδικό πρόσβασης για τον GRUB Bootloader. Πρέπει επίσης να σιγουρευτούμε πως τα αρχεία του έχουν τα κατάλληλα δικαιώματα (πρόσβαση μόνο από root).

2.2.6.1 Δικαιώματα αρχείου /boot/grub2/grub.conf

Θέτοντας τα δικαιώματα σε ανάγνωση και εγγραφή μόνο για τον χρήστη/γκρουπ root για το αρχείο /boot/grub2/grub.conf. δεν δίνεται η δυνατότητα να τροποποιηθεί ή να διαβαστεί από κάποιον άλλον χρήστη και να εντοπίσει και ενδεχομένως να εκμεταλλευτεί κάποια αδυναμία που υπάρχει κατά την εκκίνηση του συστήματος.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις παρακάτω εντολές για ρύθμιση σωστών δικαιωμάτων στο αρχείο.

```
chown root:root /boot/grub2/grub.cfg
chmod og-rwx /boot/grub2/grub.cfg
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή. Το Access πρέπει να είναι 0600 ενώ για Uid και Gid πρέπει να είναι μόνο ο χρήστης root.

```
stat /boot/grub2/grub.cfg
```

```
[admin@centos7 ~]$ sudo stat /boot/grub2/grub.cfg
  File: '/boot/grub2/grub.cfg'
  Size: 5594            Blocks: 16         IO Block: 4096   regular file
Device: 801h/2049d      Inode: 16694       Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Εικόνα 22 - Δικαιώματα αρχείου /boot/grub2/grub.conf

2.2.7 Επιπλέον ασφάλεια διεργασιών

Σε αυτό το κεφάλαιο βρίσκονται επιπλέον ρυθμίσεις που μπορούν να γίνουν για την επαύξηση ασφάλειας των διεργασιών του συστήματος.

2.2.7.1 Περιορισμός των core dumps

Το Core Dump είναι ουσιαστικά το αποτύπωμα μνήμης ενός προγράμματος. Συνήθως, χρησιμοποιείται για την εύρεση του σφάλματος που οδήγησε το πρόγραμμα στο να σταματήσει να αποκρίνεται. Ωστόσο, μπορεί να περιέχει και εμπιστευτικά δεδομένα. Το λειτουργικό σύστημα CentOS επιτρέπει τον καθορισμό soft και hard ορίου για τα core dumps. Το soft όριο μπορεί να παρακαμφθεί από τον χρήστη ενώ το hard όχι. Συνεπώς, είναι μια καλή πρακτική ο καθορισμός ενός hard ορίου για τα core dumps.

Τρόπος Ενεργοποίησης:

Πρέπει να τροποποιηθεί το αρχείο /etc/security/limits.conf ή να δημιουργηθεί ένα αρχείο στην διαδρομή /etc/security/limits.d/* με την επόμενη γραμμή.

```
* hard core 0
```

Επιπλέον πρέπει να τροποποιηθεί η παρακάτω γραμμή στο αρχείο /etc/sysctl.conf σε 0 (false).

```
fs.suid_dumpable = 0
```

Για να ενεργοποιηθεί απευθείας στον kernel σαν παράμετρο πρέπει να γράψουμε την παρακάτω εντολή αλλιώς θα ενεργοποιηθεί έπειτα από επανεκκίνηση του συστήματος (αφού τότε γίνεται η φόρτωση των παραμέτρων του αρχείου /etc/sysctl.conf).

```
sysctl -w fs.suid_dumpable=0
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές για τον έλεγχο του αρχείου Limits καθώς και της ενεργού kernel παραμέτρου. Πρέπει και στα δύο να εκτυπώσει 0 (false).

```
grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*
sysctl fs.suid_dumpable
```

```
[admin@centos7 ~]$ grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*
/etc/security/limits.conf:* hard core 0
[admin@centos7 ~]$ sysctl fs.suid_dumpable
fs.suid_dumpable = 0
```

Εικόνα 23 - Έλεγχος παραμέτρων για Core Dumps

2.2.7.2 Ενεργοποίηση της λειτουργίας ASLR

Είναι καλή πρακτική η ενεργοποίηση της λειτουργίας ASLR (**A**ddress **S**pace **L**ayout **R**andomization). Η συγκεκριμένη λειτουργία αλλάζει με τυχαίο τρόπο το εύρος διευθύνσεων της μνήμης που χρησιμοποιεί μια διεργασία. Έτσι, είναι αδύνατον να εγγραφούν κακόβουλα δεδομένα σε σημαντικές μεταβλητές που χρησιμοποιούνται από το πρόγραμμα.

Τρόπος Ενεργοποίησης:

Πρέπει να τροποποιηθεί η παρακάτω γραμμή στο αρχείο /etc/sysctl.conf σε 2.

```
kernel.randomize_va_space = 2
```

Για να ενεργοποιηθεί απευθείας στον kernel σαν παράμετρο πρέπει να γράψουμε την παρακάτω εντολή αλλιώς θα ενεργοποιηθεί έπειτα από επανεκκίνηση του συστήματος (αφού τότε γίνεται η φόρτωση των παραμέτρων του αρχείου /etc/sysctl.conf).

```
sysctl -w kernel.randomize_va_space=2
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή και ελέγχουμε ότι εκτυπώνει 2.

```
sysctl kernel.randomize_va_space
```

```
[admin@centos7 ~]$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

Εικόνα 24 - Έλεγχος λειτουργίας ASLR

2.2.8 SELinux (Security Enhanced Linux)

Είναι καλή πρακτική η χρήση του SELinux ως MAC (**M**andatory **A**ccess **C**ontrol) διότι αποδίδει καλύτερα από το προκαθορισμένο DAC (**D**iscretionary **A**ccess **C**ontrol). Σε αυτό το κεφάλαιο ακολουθούν οι παραμετροποιήσεις και ο έλεγχος ορθής λειτουργίας του SELinux σύμφωνα με τις καλύτερες πρακτικές.

2.2.8.1 Εγκατάσταση του SELinux

Βεβαιωνόμαστε ότι είναι εγκατεστημένο το SELinux πριν κάνουμε οποιαδήποτε από τις ενέργειες αυτού του κεφαλαίου.

Τρόπος Ενεργοποίησης:

Εκτελούμε την παρακάτω εντολή από το τερματικό.

```
yum install libselinux
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή και περιμένουμε ανταπόκριση της έκδοσης του SELinux.

```
rpm -q libselinux
```

```
[admin@centos7 ~]$ rpm -q libselinux
libselinux-2.5-15.el7.x86_64
```

Εικόνα 25 - Έλεγχος εγκατάστασης του SELinux

2.2.8.2 Έλεγχος ότι το SELinux δεν είναι απενεργοποιημένο

Πρέπει να γίνει έλεγχος ότι το SELinux δεν είναι απενεργοποιημένο στα αρχεία του GRUB Bootloader.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/default/grub και αφαιρούμε γραμμές όπως selinux=0 και enforcing=0. Έπειτα χρησιμοποιούμε την παρακάτω εντολή για την ανανέωση του αρχείου παραμετροποίησης του GRUB Bootloader.

```
grub2-mkconfig > /boot/grub2/grub.cfg
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή και ελέγχουμε ότι δεν υπάρχουν παράμετροι όπως selinux=0 η enforcing=0.

```
grep "^\s*linux" /boot/grub2/grub.cfg
```

```
[admin@centos7 ~]$ sudo grep "^\s*linux" /boot/grub2/grub.cfg
        linux16 /vmlinuz-3.10.0-1160.11.1.el7.x86_64 root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
        linux16 /vmlinuz-3.10.0-1127.el7.x86_64 root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
        linux16 /vmlinuz-0-rescue-60177cfa44424c639879e50d1c19e03e root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
```

Εικόνα 26 - Έλεγχος εκκίνησης SELinux

2.2.8.3 Παραμετροποίηση κατάστασης του SELinux σε enforcing

Πρέπει το SELinux να είναι ενεργοποιημένο κατά την εκκίνηση του συστήματος ώστε οι έλεγχοί του να ξεκινούν από την αρχή της εκκίνησης.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/selinux/config και αλλάζουμε την παράμετρο SELINUX σε enforcing.

```
SELINUX=enforcing
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και βεβαιωνόμαστε ότι εκτυπώνουν κατάσταση Enforcing.

```
grep SELINUX=enforcing /etc/selinux/config

sestatus
```

```
[admin@centos7 ~]$ grep SELINUX=enforcing /etc/selinux/config
SELINUX=enforcing
[admin@centos7 ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

Εικόνα 27 - Έλεγχος κατάστασης SELinux (enforcing)

2.2.8.4 Παραμετροποίηση πολιτικής του SELinux σε targeted

Είναι καλή πρακτική η ρύθμιση της πολιτικής του SELinux σε targeted. Για πιο αυστηρή πολιτική μπορεί να ακολουθήσουμε την ρύθμιση πολιτικής mls ωστόσο, ενδέχεται να δημιουργήσει προβλήματα στην ομαλή λειτουργία μερικών υπηρεσιών. Στη δική μας περίπτωση, δημιούργησε πρόβλημα στον Apache εξυπηρετητή ιστού.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/selinux/config και αλλάζουμε την παράμετρο SELINUXTYPE σε targeted.

```
SELINUXTYPE=targeted
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και βεβαιωνόμαστε ότι εκτυπώνουν κατάσταση targeted.

```
grep SELINUXTYPE=targeted /etc/selinux/config

sestatus
```

```
[admin@centos7 ~]$ grep SELINUXTYPE=targeted /etc/selinux/config
SELINUXTYPE=targeted
[admin@centos7 ~]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

Εικόνα 28 - Έλεγχος πολιτικής του SELinux (targeted)

2.2.9 Μπάνερ προειδοποιήσεων εισόδου στο σύστημα

Είναι καλή πρακτική η χρήση μπάνερ προειδοποιήσεων εισόδου στο σύστημα. Αυτό το μήνυμα θα είναι φανερό στον χρήστη πριν την είσοδό του και θα αναφέρει τις πολιτικές χρήσης του συστήματος. Παράλληλα, πρέπει να δοθεί προσοχή ώστε αυτό το μήνυμα να μην διαρρέει πληροφορίες συστήματος όπως το λειτουργικό που χρησιμοποιείται ή η έκδοσή του. Τέλος, αυτά τα μηνύματα δεν αφορούν μόνο τοπικούς χρήστες αλλά και απομακρυσμένους (λ.χ. χρήση SSH για είσοδο). Τα συγκεκριμένα αρχεία βρίσκονται στις παρακάτω διαδρομές: /etc/motd, /etc/issue, /etc/issue.net

2.2.9.1 Τροποποίηση των μπάνερ

Τρόπος Ενεργοποίησης:

Για καθένα από τα παραπάνω αρχεία προσθέτουμε το κείμενο-μήνυμα που θέλουμε να εκτυπώνετε στον χρήστη. Βεβαιωνόμαστε ότι δεν υπάρχουν στο μήνυμα τα παρακάτω καθώς εκτυπώνουν πληροφορίες του συστήματος: \m \r \s \v.

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή ώστε να εκτυπώσει το μήνυμα. Η δεύτερη εντολή μας δείχνει εάν όντως περιέχονται οι απαγορευμένοι χαρακτήρες. Δεν πρέπει να εκτυπώσει τίποτα ώστε να θεωρηθεί σωστό το μήνυμά μας.

Ακολουθούμε την ίδια διαδικασία για κάθε μία από τις διαδρομές. Το παράδειγμα αφορά το αρχείο που βρίσκεται στην τοποθεσία /etc/motd.

```
cat /etc/motd

egrep '(\\v|\\r|\\m|\\s)' /etc/motd
```

```
[admin@centos7 ~]$ cat /etc/motd

    /------------------------------------------------------------------------/
    |                       *** NOTICE TO USERS ***                          |
    |                                                                        |
    | This computer system is the private property of company_name...        |
    | It is for authorized use only.                                         |
    |                                                                        |
    | Users (authorized or unauthorized) have no explicit or implicit        |
    | expectation of privacy.                                                |
    |                                                                        |
    | Any or all uses of this system and all files on this system may be     |
    | intercepted, monitored, recorded, copied, audited, inspected, and      |
    | disclosed to your employer, to authorized site, government, and law    |
    | enforcement personnel, as well as authorized officials of government   |
    | agencies, both domestic and foreign.                                   |
    |                                                                        |
    | By using this system, the user consents to such interception,          |
    | monitoring, recording, copying, auditing, inspection, and disclosure   |
    | at the discretion of such personnel or officials.  Unauthorized or     |
    | improper use of this system may result in civil and criminal penalties |
    | and administrative or disciplinary action, as appropriate. By          |
    | continuing to use this system you indicate your awareness of and       |
    | consent to these terms and conditions of use. LOG OFF IMMEDIATELY if   |
    | you do not agree to the conditions stated in this warning.             |
    /------------------------------------------------------------------------/
[admin@centos7 ~]$ egrep '(\\v|\\r|\\m|\\s)' /etc/motd
[admin@centos7 ~]$
```

Εικόνα 29 - Έλεγχος περιεχομένου μπάνερ

2.2.9.2 Δικαιώματα των αρχείων μπάνερ

Τα παραπάνω αρχεία μπάνερ πρέπει να έχουν δικαιώματα εγγραφής μόνο από τον χρήστη root ενώ δικαιώματα ανάγνωσης για τους υπόλοιπους χρήστες ώστε να «εκτυπώνονται». Με αυτό το τρόπο διασφαλίζεται η μη-εξουσιοδοτημένη τροποποίησή τους.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις παρακάτω εντολές για όλες τις διαδρομές. Στο παρακάτω παράδειγμα επιλέξαμε την διαδρομή /etc/motd.

```
chown root:root /etc/motd
chmod 644 /etc/motd
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή για όλες τις διαδρομές. Το Access πρέπει να είναι 0644 ενώ για Uid και Gid πρέπει να είναι μόνο ο χρήστης root.

```
stat /etc/motd
```

```
[admin@centos7 ~]$ stat /etc/motd
  File: '/etc/motd'
  Size: 1897            Blocks: 8          IO Block: 4096   regular file
Device: fd01h/64769d    Inode: 786484      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:etc_t:s0
Access: 2021-05-19 11:16:17.614821828 +0300
Modify: 2020-12-30 00:58:00.965746442 +0200
Change: 2020-12-30 00:58:00.965746442 +0200
 Birth: -
```

Εικόνα 30 - Έλεγχος δικαιωμάτων μπάνερ

2.2.10 Εγκατάσταση υπηρεσίας συγχρονισμού ρολογιού

Είναι καλή πρακτική η χρήση κάποιας υπηρεσίας συγχρονισμού όπως ntp ή το chrony ώστε το σύστημα να έχει ίδιο 'χρόνο' με κάποιο κεντρικό εξυπηρετητή. Έτσι, αρχεία καταγραφής που μπορεί να συγκεντρώνονται από πολλά συστήματα θα έχουν σωστή χρονοσφραγίδα.

2.2.10.1 Εγκατάσταση και παραμετροποίηση chronyd

Τρόπος Ενεργοποίησης:

Εκτελούμε την παρακάτω εντολή για την εγκατάσταση του chrony.

```
yum install chrony
```

Επιπλέον τροποποιούμε το αρχείο /etc/chrony.conf ώστε να περιλαμβάνει κάποιους εξυπηρετητές συγχρονισμού διαθέσιμους στο διαδίκτυο ή και δικούς μας.

Τέλος στο αρχείο /etc/sysconfig/chronyd και στα OPTIONS συμπεριλαμβάνουμε το '-u chrony'.

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές ώστε να διαπιστώσουμε ότι έχουμε εγκατεστημένο το chrony και με σωστή ρύθμιση.

```
rpm -q chrony

grep "^server" /etc/chrony.conf
grep ^OPTIONS /etc/sysconfig/chronyd
```

```
[admin@centos7 ~]$ rpm -q chrony
chrony-3.4-1.el7.x86_64
[admin@centos7 ~]$ grep "^server" /etc/chrony.conf
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
[admin@centos7 ~]$ grep ^OPTIONS /etc/sysconfig/chronyd
OPTIONS="-u chrony"
```

Εικόνα 31 - Έλεγχος παραμετροποίησης chrony

2.2.11 Απενεργοποίηση μη-χρησιμοποιούμενων υπηρεσιών

Όπως εκτελέσαμε την διαδικασία για τα filesystems είναι επίσης καλή πρακτική η απενεργοποίηση ή/και η αφαίρεση υπηρεσιών που δεν χρησιμοποιούνται από το σύστημα. Έτσι μειώνεται, το εύρος των επιθέσεων προς το σύστημά μας.

Παρακάτω ακολουθεί μία λίστα από αυτά που πρέπει να απενεργοποιηθούν:

Υπηρεσίες προς απενεργοποίηση	
avahi-daemon	dovecot
cups	smb
slapd	squid
nfs	snmpd
rpcbind	ypserv
named	telnet.socket
vsftpd	tftp.socket
rsyncd	ntalk
kdump	mdmonitor
smartd	rhsmcertd

Εικόνα 32 - Πίνακας υπηρεσιών προς απενεργοποίηση

Τρόπος Ενεργοποίησης:

Για κάθε μία από τις παραπάνω υπηρεσίες εκτελούμε την παρακάτω εντολή.

```
systemctl disable όνομα υπηρεσίας
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή για κάθε μία από τις παραπάνω υπηρεσίες.

```
systemctl is-enabled όνομα υπηρεσίας
```

```
[admin@centos7 ~]$ systemctl is-enabled cups
disabled
```

Εικόνα 33 - Έλεγχος απενεργοποιημένων υπηρεσιών

2.2.12 Επαύξηση ασφάλειας δικτύου

Σε αυτό το κεφάλαιο υπάρχουν διάφορες ρυθμίσεις που μπορούν να γίνουν στο σύστημα και αφορούν την ασφάλεια των δικτυακών παραμέτρων.

2.2.12.1 Παράμετροι kernel στο αρχείο /etc/sysctl.conf

Το αρχείο /etc/sysctl.conf έχει παραμέτρους οι οποίες αφορούν την δικτυακή κίνηση. Είναι εύκολο να τις ξεχωρίσουμε αφού εκκινούν με net. Παρακάτω παρουσιάζονται σύμφωνα με τις καλύτερες πρακτικές οι σωστές ρυθμίσεις αυτών των παραμέτρων.

```
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
```

Εικόνα 34 - Δικτυακοί κανόνες αρχείου /etc/sysctl.conf

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/sysctl.conf σύμφωνα με τα παραπάνω. Εάν θέλουμε απευθείας ενεργοποίηση στον kernel τότε εκτελούμε την παρακάτω εντολή για κάθε μία από τις παραμέτρους. Σε κάθε περίπτωση ενδείκνυται η τροποποίηση του αρχείου /etc/sysctl.conf ώστε να υπάρχει σταθερότητα στις ρυθμίσεις έπειτα και από επανεκκίνηση.

```
sysctl -w όνομα παραμέτρου = ρύθμιση
sysctl -w net.ipv4.route.flush=1
```

Προσοχή! Πάντα μετά από κάθε ρύθμιση χρησιμοποιούμε το route.flush αναλόγως εάν είναι IPv4 ή IPv6.

Τρόπος Ελέγχου:

Για κάθε μία από τις παραμέτρους εκτελούμε την ακόλουθη εντολή. Ελέγχουμε ότι ταιριάζει σύμφωνα με τον πίνακα.

```
sysctl όνομα παραμέτρου
[admin@centos7 ~]$ sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1
```

Εικόνα 35 - Έλεγχος παραμέτρων δικτύου στο /etc/sysctl.conf

2.2.12.2 Απενεργοποίηση πρωτοκόλλου IPv6

Σε περίπτωση που δεν χρησιμοποιείται το πρωτόκολλο IPv6 από τον οργανισμό τότε είναι καλή πρακτική η απενεργοποίησή του για την μείωση του εύρους των επιθέσεων καθώς και για αντιμετώπιση συγκρούσεων με το IPv4 πρωτόκολλο. Αυτό μπορεί να επιτευχθεί τροποποιώντας της παραμέτρους στο /etc/sysctl.conf, γράφοντας ένα αρχείο στον φάκελο /etc/modprobe.d όπως κάναμε με τα filesystems ή τροποποιώντας το αρχείο /etc/sysconfig/network.

Για να διατηρηθεί μία σταθερότητα στο σύστημα, είναι καλή πρακτική η εφαρμογή και των τριών αυτών μέτρων.

Τρόπος Ενεργοποίησης:

Δημιουργούμε ένα αρχείο .conf στην διαδρομή /etc/modprobe.d όπως κάναμε και στο κεφάλαιο (2.2.3) το οποίο να περιλαμβάνει την παρακάτω γραμμή.

```
options ipv6 disable = 1
```

Στο αρχείο /etc/sysconfig προσθέτουμε/τροποποιούμε τις παρακάτω γραμμές κώδικα.

```
NETWORKING_IPV6=no

IPV6INIT=no
```

Τρόπος Ελέγχου:

Γράφουμε την παρακάτω εντολή και βλέπουμε εάν δίνει το αναμενόμενο αποτέλεσμα.

```
modprobe -c | grep ipv6
```

```
[admin@centos7 ~]$ modprobe -c | grep ipv6
blacklist dccp_ipv6
options ipv6 disable=1
options ipv6 disable=1
```

Εικόνα 36 - Έλεγχος απενεργοποιημένου IPv6

2.2.12.3 Εγκατάσταση TCP Wrappers

Τρόπος Ενεργοποίησης:

Εκτελούμε την ακόλουθη εντολή από το τερματικό.

```
yum install tcp_wrappers
```

Τρόπος Ελέγχου:

Εκτελούμε τις ακόλουθες εντολές ώστε να δούμε ποια έκδοση των TCP Wrappers εχουμε εγκατεστημένη.

```
rpm -q tcp_wrappers

rpm -q tcp_wrappers-libs
```

```
[admin@centos7 ~]$ rpm -q tcp_wrappers
tcp_wrappers-7.6-77.el7.x86_64
[admin@centos7 ~]$ rpm -q tcp_wrappers-libs
tcp_wrappers-libs-7.6-77.el7.x86_64
```

Εικόνα 37 - Έλεγχος εγκατάστασης TCP Wrappers

2.2.12.4 Δικαιώματα αρχείων hosts.allow και hosts.deny

Τα αρχεία στις διαδρομές /etc/hosts.allow και /etc/hosts.deny περιέχουν πληροφορίες που χρησιμοποιούνται από διάφορες εφαρμογές και συνεπώς πρέπει να είναι αναγνώσιμες από αυτές.

Ωστόσο δικαιώματα εγγραφής πρέπει να έχει μόνο ο χρήστης/γκρουπ root. Συνεπώς, θέλουμε ένα chmod 0644.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις ακόλουθες εντολές για κάθε διαδρομή.

```
chown root:root διαδρομή

chmod 0644 διαδρομή
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή για κάθε διαδρομή. Το Access πρέπει να είναι 0644 ενώ για Uid και Gid πρέπει να είναι μόνο ο χρήστης root.

```
stat διαδρομή
```

```
[admin@centos7 ~]$ stat /etc/hosts.allow
  File: '/etc/hosts.allow'
  Size: 41              Blocks: 8          IO Block: 4096   regular file
Device: fd01h/64769d    Inode: 786481      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:net_conf_t:s0
Access: 2021-05-19 17:19:13.127557177 +0300
Modify: 2020-12-30 00:57:52.138321970 +0200
Change: 2020-12-30 00:57:52.139241015 +0200
 Birth: -
```

Εικόνα 38 - Έλεγχος δικαιωμάτων αρχείων hosts

2.2.12.5 Απενεργοποίηση δικτυακών πρωτοκόλλων

Τα παρακάτω πρωτόκολλα εάν δεν χρησιμοποιούνται, είναι καλή πρακτική η απενεργοποίησή τους.

dccp
sctp
rds
tipc

Εικόνα 39 - Πίνακας δικτυακών πρωτοκόλλων προς απενεργοποίηση

Τρόπος Ενεργοποίησης:

Δημιουργούμε ένα καινούργιο αρχείο παραμετροποίησης (.conf) στην διαδρομή /etc/modprobe.d/ με οποιοδήποτε όνομα της επιλογής μας και μέσα σε αυτό γράφουμε για κάθε ένα από τα παραπάνω πρωτόκολλα την ίδια γραμμή.

```
install όνομα_πρωτοκόλλου /bin/true
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές για καθένα από τα παραπάνω πρωτόκολλα και βλέπουμε εάν έχουμε το ίδιο αποτέλεσμα στο σύστημά μας.

```
modprobe -n -v πρωτόκολλο

lsmod | grep πρωτόκολλο
```

```
[admin@centos7 ~]$ modprobe -n -v tipc
install /bin/true
[admin@centos7 ~]$ lsmod | grep tipc
[admin@centos7 ~]$
```

Εικόνα 40 - Έλεγχος απενεργοποιημένων διαδικτυακών πρωτοκόλλων

2.2.12.6 Παραμετροποίηση αναχώματος ασφαλείας (UFW-IPTables)

Είναι καλή πρακτική η ύπαρξη ενός αναχώματος ασφαλείας στο σύστημά μας. Από default το λειτουργικό CentOS έχει ενεργοποιημένο το firewalld ένα αρκετά εύχρηστο και κατανοητό εργαλείο. Ωστόσο, για καλύτερη παραμετροποίηση στις ανάγκες μας προτείνεται η χρήση των iptables καθώς και του ufw (uncomplicated firewall). Το ufw αποτελεί ουσιαστικά ένα front-end για τους κανόνες που θα περαστούν στα iptables. Στα iptables μπορούμε να καθορίσουμε διάφορους κανόνες, τα πρωτόκολλα που θα δεχόμαστε και τις ανάλογες πόρτες ακόμα και με απλούς κανόνες να προσθέσουμε προστασία για επιθέσεις όπως η Slowloris. Αυτό επιτυγχάνεται περιορίζοντας τις συνδέσεις που μπορεί να δημιουργήσει ένας χρήστης από μία IP ή ένα εύρος IP (συνήθως οι επιτιθέμενοι έχουν στην διάθεσή τους ένα εύρος από συνεχόμενες IP) συναρτήσει του χρονικού διαστήματος που αυτές μένουν ανοιχτές.

Τρόπος Ενεργοποίησης:

Αρχικά πρέπει να έχουμε εγκατεστημένα τα iptables και το ufw καθώς και να βεβαιωθούμε πως το ufw είναι το προκαθορισμένο τείχος προστασίας.

```
systemctl stop firewalld.service
systemctl disable firewalld.service
systemctl mask firewalld.service
yum install iptables
```

```
yum install ufw
systemctl enable ufw
systemctl start ufw
```

Έπειτα τροποποιούμε το αρχείο /etc/default/ufw ώστε να φορτώνει το αρχείο /etc/sysctl.conf καθώς και να μην χρησιμοποιεί το πρωτόκολλο IPv6. Τέλος, εισάγουμε τους επιθυμητούς κανόνες στο αρχείο /etc/ufw/before.rules για την δική μας περίπτωση χρήσης του εξυπηρετητή ιστού.

Παρακάτω ακολουθούν οι κανόνες που επιλέξαμε για να μπουν στο ufw.

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
:ufw-http - [0:0]
:ufw-http-logdrop - [0:0]
# End required lines


# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
```

```
# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT

#
# ufw-not-local
#
-A ufw-before-input -j ufw-not-local

# if LOCAL, RETURN
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

# if MULTICAST, RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

# if BROADCAST, RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

# all other non-local packets are dropped
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP

### Start HTTP ###

# Enter rule
-A ufw-before-input -p tcp --dport 80   -j ufw-http
-A ufw-before-input -p tcp --dport 443  -j ufw-http

# Limit connections per Class C
-A ufw-http -p tcp --syn -m connlimit --connlimit-above 40 --connlimit-mask 24 -j ufw-http-logdrop

# Limit connections per IP
-A ufw-http -m state --state NEW -m recent --name conn_per_ip --set
-A ufw-http -m state --state NEW -m recent --name conn_per_ip --update --seconds 10 --hitcount 20 -j
ufw-http-logdrop

# Limit packets per IP
-A ufw-http -m recent --name pack_per_ip --set
-A ufw-http -m recent --name pack_per_ip --update --seconds 1  --hitcount 20  -j ufw-http-logdrop

# Finally accept
-A ufw-http -j ACCEPT

# Log-A ufw-http-logdrop -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW HTTP
DROP] "
```

```
-A ufw-http-logdrop -j DROP

### End HTTP ###


# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

Εικόνα 41 - Τελικοί κανόνες UFW

Τέλος, κάνουμε επανεκκίνηση του ufw με χρήση της εντολής reload.

Τρόπος Ελέγχου:

Ελέγχουμε εάν είναι εγκατεστημένα τα iptables, το ufw και την κατάστασή του. Με χρήση της εντολής cat /etc/ufw/before.rules μπορούμε να επιβεβαιώσουμε και το περιεχόμενο των κανόνων.

```
rpm -q iptables

rpm -q ufw

systemctl status ufw.service
```

```
[admin@centos7 ~]$ rpm -q iptables
iptables-1.4.21-35.el7.x86_64
[admin@centos7 ~]$ rpm -q ufw
ufw-0.35-9.el7.noarch
[admin@centos7 ~]$ sudo systemctl status ufw.service
● ufw.service - Uncomplicated firewall
   Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; vendor preset: disabled)
   Active: active (exited) since Wed 2021-05-19 21:40:41 EEST; 2s ago
     Docs: man:ufw(8)
           man:ufw-framework(8)
           file:///usr/share/doc/ufw/README
  Process: 1008 ExecStart=/usr/libexec/ufw/ufw-init start (code=exited, status=0/SUCCESS)
 Main PID: 1008 (code=exited, status=0/SUCCESS)
    Tasks: 0
   CGroup: /system.slice/ufw.service
```

Εικόνα 42 - Έλεγχος UFW

2.2.13 Απενεργοποίηση επιπλέον αρθρωμάτων και θυρών USB

Είναι καλή πρακτική η απενεργοποίηση των θυρών USB εφόσον δεν χρησιμοποιούνται καθώς και άλλων αρθρωμάτων συνδεσιμότητας.

Παρακάτω ακολουθεί σχετικός πίνακας με τα αρθρώματα που πρέπει να απενεργοποιηθούν:

Αρθρώματα προς απενεργοποίηση	
appletalk	bnep
bluetooth	btusb
net-pf-31	soundcore
thunderbolt	usb-midi
usb-storage	firewire-core

Εικόνα 43 - Πίνακας επιπλέον αρθρωμάτων προς απενεργοποίηση

Τρόπος Ενεργοποίησης:

Δημιουργούμε ένα καινούργιο αρχείο παραμετροποίησης (.conf) στην διαδρομή /etc/modprobe.d/ με οποιοδήποτε όνομα της επιλογής μας και μέσα σε αυτό γράφουμε για κάθε ένα από τα παραπάνω αρθρώματα την ίδια γραμμή.

```
install όνομα_αρθρώματος /bin/true
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές για καθένα από τα παραπάνω αρθρώματα και βλέπουμε εάν έχουμε το ίδιο αποτέλεσμα στο σύστημά μας.

```
modprobe -n -v αρθρώματος

lsmod | grep πρωτόκολλο
```

```
[admin@centos7 ~]$ modprobe -n -v usb-storage
install /bin/true
[admin@centos7 ~]$ lsmod | grep usb-storage
[admin@centos7 ~]$
```

Εικόνα 44 - Έλεγχος απενεργοποιημένων αρθρωμάτων

2.2.14 Παραμετροποίηση auditd και rsyslog

Το λογισμικό auditd μπορεί να χρησιμοποιηθεί από τους διαχειριστές για την επίβλεψη διάφορων μετατροπών και γεγονότων που συμβαίνουν σε ένα σύστημα. Τα αρχεία αποθηκεύονται στην διαδρομή /var/log/audit/audit.log και ανάλογα τις ρυθμίσεις μπορεί να καταλαμβάνουν αρκετό αποθηκευτικό χώρο.

Σε αυτό το κεφάλαιο θα δούμε τις καλύτερες πρακτικές για την παραμετροποίηση του λογισμικού auditd καθώς και το σύνολο των κανόνων που θα χρησιμοποιήσουμε για την δική μας περίπτωση χρήσης.

2.2.14.1 Παραμετροποίηση μεγέθους αρχείου καταγραφής auditd

Ενδείκνυται ο καθορισμός του μεγέθους καταγραφής το οποίο θα καταλαμβάνει στον σκληρό δίσκο.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/audit/auditd.conf και την παρακάτω παράμετρο.

```
max_log_file = <MB>
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή στο τερματικό.

```
grep max_log_file /etc/audit/auditd.conf
```

```
[admin@centos7 ~]$ sudo grep max_log_file /etc/audit/auditd.conf
[sudo] password for admin:
max_log_file = 30
```

Εικόνα 45 - Έλεγχος μεγέθους αρχείο καταγραφής auditd

2.2.14.2 Παραμετροποίηση συμπεριφοράς όταν γεμίσει το αρχείο καταγραφής

Το σύστημα πρέπει να σταματήσει να λειτουργεί σε περίπτωση που γεμίσει το αρχείο καταγραφής εάν η ασφάλεια του είναι ύψιστης σημασίας.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/audit/auditd.conf και τις παρακάτω παραμέτρους.

```
space_left_action = email
action_mail_acct = root
admin_space_left_action = halt
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές στο τερματικό.

```
grep space_left_action /etc/audit/auditd.conf

grep action_mail_acct /etc/audit/auditd.conf

grep admin_space_left_action /etc/audit/auditd.conf
```

```
[admin@centos7 ~]$ sudo grep space_left_action /etc/audit/auditd.conf
space_left_action = email
admin_space_left_action = halt
[admin@centos7 ~]$ sudo grep action_mail_acct /etc/audit/auditd.conf
action_mail_acct = root
[admin@centos7 ~]$ sudo grep admin_space_left_action /etc/audit/auditd.conf
admin_space_left_action = halt
```

Εικόνα 46 - Έλεγχος συμπεριφοράς auditd σε περίπτωση μεγάλου αρχείου καταγραφής

2.2.14.3 Μη αυτόματη διαγραφή των αρχείων καταγραφής

Το σύστημα πρέπει να κάνει «περιστροφή» των αρχείων καταγραφής χωρίς όμως να διαγράφει τα προηγούμενα.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/audit/auditd.conf και την παρακάτω παράμετρο.

```
max_log_file_action = keep_logs
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή στο τερματικό.

```
grep max_log_file_action /etc/audit/auditd.conf
```

```
[admin@centos7 ~]$ sudo grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

Εικόνα 47 - Έλεγχος παραμέτρου διαγραφής αρχείων καταγραφής

2.2.14.4 Ενεργοποίηση auditd αυτόματα

Το λογισμικό auditd πρέπει να ενεργοποιείται έπειτα από την επανεκκίνηση ώστε να καταγράφει τα γεγονότα του συστήματος από την αρχή.

Τρόπος Ενεργοποίησης:

Εκτελούμε την παρακάτω εντολή από το τερματικό.

```
systemctl enable auditd
```

Τρόπος Ελέγχου:

Ελέγχουμε με την παρακάτω εντολή εάν είναι ενεργοποιημένο το auditd.

```
systemctl is-enabled auditd
```

```
[admin@centos7 ~]$ systemctl is-enabled auditd
enabled
```

Εικόνα 48 - Ενεργοποίηση auditd

2.2.14.5 Καταγραφή συμβάντων και κατά την εκκίνηση του συστήματος

Είναι καλή πρακτική η ρύθμιση του auditd ώστε να καταγράφει και συμβάντα των υπηρεσιών **και** κατά την εκκίνηση του συστήματος. Αυτό, μπορεί να επιτευχθεί με την παρακάτω επιλογή στον GRUB Bootloader.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/default/grub και προσθέτουμε την παρακάτω παράμετρο.

```
GRUB_CMDLINE_LINUX="audit=1"
```

Σημαντικό!!! Έπειτα από κάθε τροποποίηση πρέπει να ανανεώσουμε την παραμετροποίηση του GRUB Bootloader με την παρακάτω εντολή.

```
grub2-mkconfig > /boot/grub2/grub.cfg
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή στο τερματικό.

```
grep "^\s*linux" /boot/grub2/grub.cfg
```

```
[admin@centos7 ~]$ sudo grep "^\s*linux" /boot/grub2/grub.cfg
        linux16 /vmlinuz-3.10.0-1160.25.1.el7.x86_64 root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1 LANG=en_US.UTF-8
        linux16 /vmlinuz-3.10.0-1160.11.1.el7.x86_64 root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
        linux16 /vmlinuz-3.10.0-1127.el7.x86_64 root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
        linux16 /vmlinuz-0-rescue-60177cfa44424c639879e50d1c19e03e root=/dev/mapper/centos_centos7-root ro --users myuser ipv6.disable=1 audit=1
```

Εικόνα 49 - Έλεγχος εκκίνησης auditd με τον GRUB Bootloader

2.2.14.6 Παραμετροποίηση κανόνων auditd

Οι κανόνες του λογισμικού auditd αποσαφηνίζουν για το ποια συμβάντα που γίνονται στο σύστημα θεωρούνται άξια καταγραφής. Τροποποιούνται ανάλογα με την περίπτωση χρήσης και το επίπεδο ασφάλειας που θέλουμε να έχει το σύστημά μας.

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/audit/audit.rules

Παρακάτω ακολουθούν οι κανόνες που επιλέξαμε για να ενεργοποιηθούν στο auditd. Σημαντική η τελευταία επιλογή που δεν επιτρέπει αλλαγές στους κανόνες χωρίς επανεκκίνηση του συστήματος.

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## Set failure mode to syslog
-f 2

# audit_time_rules - Record attempts to alter time through adjtime
-a always,exit -F arch=b64 -S adjtimex -k audit_time_rules

# audit_time_rules - Record attempts to alter time through settimeofday
-a always,exit -F arch=b64 -S settimeofday -k audit_time_rules

# audit_time_rules - Record Attempts to Alter Time Through stime
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime -k audit_time_rules

# audit_time_rules - Record Attempts to Alter Time Through clock_settime
-a always,exit -F arch=b64 -S clock_settime -k audit_time_rules

# Record Attempts to Alter the localtime File
-w /etc/localtime -p wa -k audit_time_rules

# Record Events that Modify User/Group Information
# audit_account_changes
-w /etc/group -p wa -k audit_account_changes
-w /etc/passwd -p wa -k audit_account_changes
-w /etc/gshadow -p wa -k audit_account_changes
-w /etc/shadow -p wa -k audit_account_changes
-w /etc/security/opasswd -p wa -k audit_account_changes

# Record Events that Modify the System's Network Environment
# audit_network_modifications
```

```
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k audit_network_modifications
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k audit_network_modifications
-w /etc/issue -p wa -k audit_network_modifications
-w /etc/issue.net -p wa -k audit_network_modifications
-w /etc/hosts -p wa -k audit_network_modifications
-w /etc/sysconfig/network -p wa -k audit_network_modifications

#Record Events that Modify the System's Mandatory Access Controls
-w /etc/selinux/ -p wa -k MAC-policy

#Record Events that Modify the System's Discretionary Access Controls - chmod
-a always,exit -F arch=b32 -S chmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chmod  -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - chown
-a always,exit -F arch=b32 -S chown -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchmod
-a always,exit -F arch=b32 -S fchmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchmodat
-a always,exit -F arch=b32 -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchown
-a always,exit -F arch=b32 -S fchown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fsetxattr
-a always,exit -F arch=b32 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - lchown
-a always,exit -F arch=b32 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - lremovexattr
-a always,exit -F arch=b32 -S lremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fremovexattr
-a always,exit -F arch=b32 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fsetxattr
-a always,exit -F arch=b32 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - removexattr
-a always,exit -F arch=b32 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
```

```
#Record Events that Modify the System's Discretionary Access Controls - setxattr
-a always,exit -F arch=b32 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Attempts to Alter Logon and Logout Events
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins

#Record Attempts to Alter Process and Session Initiation Information
-w /var/run/utmp -p wa -k session
-w /var/log/btmp -p wa -k session
-w /var/log/wtmp -p wa -k session

#Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F
exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F
exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F
exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F
exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

#Ensure auditd Collects Information on the Use of Privileged Commands
#
#  Find setuid / setgid programs then modify and uncomment the line below.
#
##  sudo find / -xdev -type f -perm -4000 -o -perm -2000 2>/dev/null
#
# -a always,exit -F path=SETUID_PROG_PATH -F perm=x -F auid>=500 -F auid!=4294967295 -k
privileged

#Ensure auditd Collects Information on Exporting to Media (successful)
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k export
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k export

#Ensure auditd Collects File Deletion Events by User
-a always,exit -F arch=b32 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F
auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F
auid!=4294967295 -k delete

#Ensure auditd Collects System Administrator Actions
-w /etc/sudoers -p wa -k actions

#Ensure auditd Collects Information on Kernel Module Loading and Unloading
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

```
-a always,exit -F arch=b32 -S init_module,finit_module,delete_module -F key=modules
-a always,exit -F arch=b64 -S init_module,finit_module,delete_module -F key=modules
-w /var/run/faillock -p wa -k logins
-a always,exit -F arch=b32 -S stime -F key=audit_time_rules
# -a always,exit -F arch=b32 -S settimeofday -F key=audit_time_rules
# -a always,exit -F arch=b64 -S settimeofday -F key=audit_time_rules
# -a always,exit -F arch=b32 -S adjtimex -F key=audit_time_rules
# -a always,exit -F arch=b64 -S adjtimex -F key=audit_time_rules
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -F key=export
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -F key=export
-a always,exit -F arch=b32 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
```

```
-a always,exit -F arch=b32 -S open -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F
key=access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F
key=access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F
key=access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F
key=access
-a always,exit -F arch=b32 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S rename -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S renameat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S renameat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=unset -F key=delete



#Make the auditd Configuration Immutable
-e 2
```

Εικόνα 50 - Τελικοί κανόνες auditd

2.2.15 Ρυθμίσεις πρόσβασης, αυθεντικοποίησης και εξουσιοδότησης

Σε αυτό το κεφάλαιο βρίσκονται οι καλύτερες πρακτικές που αφορούν παραμετροποιήσεις του συστήματος για πρόσβαση σε αρχεία, αυθεντικοποίηση και εξουσιοδότηση.

2.2.15.1 Ενεργοποίηση λογισμικού cron

Το λογισμικό cron χρησιμοποιείται για την εκτέλεση πολλών διεργασιών στο σύστημα με χρήση χρονοπρογράμματος. Για παράδειγμα, η αναβάθμιση των πακέτων του λογισμικού του λειτουργικού CentOS μπορεί να οριστεί να γίνεται σε συγκεκριμένες χρονικές στιγμές μέσα στην βδομάδα όταν το σύστημα δεν χρησιμοποιείται.

Τρόπος Ενεργοποίησης:

Εκτελούμε την παρακάτω εντολή στο τερματικό για την ενεργοποίηση του cron κατά την εκκίνηση του συστήματος.

```
systemctl enable crond
```

Τρόπος Ελέγχου:

Εκτελούμε την παρακάτω εντολή για επιβεβαίωση.

```
systemctl is-enabled crond
```

```
[admin@centos7 ~]$ systemctl is-enabled crond
enabled
```

Εικόνα 51 - Έλεγχος χρήσης του cron

2.2.15.2 Δικαιώματα στα αρχεία που χρησιμοποιεί ο cron

Ο cron χρησιμοποιεί τα παρακάτω αρχεία για να εκτελέσει τις προγραμματισμένες διεργασίες σύμφωνα με το χρονοπρόγραμμα που έχει ορίσει ο διαχειριστής του συστήματος. Τα αρχεία πρέπει να μην μπορούν να τροποποιηθούν από κάποιον χρήστη παρά μόνο από τον root. Συνεπώς, θέλουμε ένα chmod 600/700 στα παρακάτω αρχεία.

Αρχεία cron προς παραμετροποίηση
/etc/crontab
/etc/cron.hourly
/etc/cron.daily
/etc/cron.weekly
/etc/cron.monthly
/etc/cron.d

Εικόνα 52 - Πίνακας αρχείων cron για κατάλληλα δικαιώματα

Τρόπος Ενεργοποίησης:

Για κάθε μία από τις παραπάνω διαδρομές εκτελούμε τις παρακάτω εντολές.

```
chown root:root διαδρομή
chmod og-rwx διαδρομή
```

Τρόπος Ελέγχου:

Για κάθε μία από τις παραπάνω διαδρομές εκτελούμε την παρακάτω εντολή και βλέπουμε τα δικαιώματα πρόσβασης. Η εκτύπωση πρέπει να δηλώνει 0600 ωστόσο και το 0700 είναι αποδεκτό.

stat διαδρομή

```
[admin@centos7 ~]$ stat /etc/cron.d
  File: '/etc/cron.d'
  Size: 4096            Blocks: 8          IO Block: 4096   directory
Device: fd01h/64769d    Inode: 787594      Links: 2
Access: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:system_cron_spool_t:s0
Access: 2021-05-24 07:55:51.494103472 +0300
Modify: 2021-05-19 12:48:54.115313995 +0300
Change: 2021-05-19 12:48:54.115313995 +0300
 Birth: -
```

Εικόνα 53 - Έλεγχος σωστών δικαιωμάτων αρχείων cron

2.2.15.3 Διαγραφή, δημιουργία και δικαιώματα σε άλλα αρχεία του cron

Τα παρακάτω αρχεία δηλώνουν για το ποιοι χρήστες έχουν δικαίωμα να χρησιμοποιήσουν τις υπηρεσίες του cron. Στην δική μας παραμετροποίηση θα αφαιρέσουμε τα αρχεία /etc/cron.deny και /etc/at.deny και θα δημιουργήσουμε τα αρχεία /etc/cron.allow και /etc/at.allow με σωστά δικαιώματα (chmod 600). ;Έτσι, μόνο οι χρήστες που υπάρχουν σε αυτά τα δύο αρχεία θα μπορούν να χρησιμοποιήσουν τις υπηρεσίες.

Τρόπος Ενεργοποίησης:

Εκτελούμε τις παρακάτω εντολές για την αφαίρεση των δύο αρχείων, την δημιουργία των .allow και τον ορισμό των κατάλληλων δικαιωμάτων σε αυτά.

```
rm /etc/cron.deny
rm /etc/at.deny
touch /etc/cron.allow
touch /etc/at.allow
chmod og-rwx /etc/cron.allow
chmod og-rwx /etc/at.allow
chown root:root /etc/cron.allow
chown root:root /etc/at.allow
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές. Για τις δύο πρώτες πρέπει να δούμε το μήνυμα: «No such file or directory» ενώ για τα άλλα δύο βλέπουμε τα δικαιώματα να είναι chmod 0600.

```
stat /etc/cron.deny
stat /etc/at.deny
stat /etc/cron.allow
stat /etc/at.allow
```

```
[admin@centos7 ~]$ stat /etc/cron.deny
stat: cannot stat '/etc/cron.deny': No such file or directory
[admin@centos7 ~]$ stat /etc/at.deny
stat: cannot stat '/etc/at.deny': No such file or directory
[admin@centos7 ~]$ stat /etc/cron.allow
  File: '/etc/cron.allow'
  Size: 0               Blocks: 0          IO Block: 4096   regular empty file
Device: fd01h/64769d    Inode: 787101      Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: unconfined_u:object_r:etc_t:s0
Access: 2021-05-24 08:38:05.868500174 +0300
Modify: 2020-12-30 00:57:46.496306475 +0200
Change: 2020-12-30 00:57:46.497225519 +0200
 Birth: -
[admin@centos7 ~]$ stat /etc/at.allow
  File: '/etc/at.allow'
  Size: 0               Blocks: 0          IO Block: 4096   regular empty file
Device: fd01h/64769d    Inode: 787102      Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: unconfined_u:object_r:etc_t:s0
Access: 2020-12-30 00:57:46.501820743 +0200
Modify: 2020-12-30 00:57:46.501820743 +0200
Change: 2020-12-30 00:57:46.501820743 +0200
 Birth: -
```

Εικόνα 54 - Έλεγχος αρχείων allow, deny, at

2.2.16 Παραμετροποίηση του PAM

Η PAM (**P**luggable **A**uthentication **M**odules) είναι μία υπηρεσία η οποία χρησιμοποιείται για την παραμετροποίηση αυθεντικοποίησης πάνω στο λειτουργικό CentOS. Τα αρχεία που αφορούν την PAM, βρίσκονται στην διαδρομή /etc/pam.d και πρέπει να ρυθμιστούν με προσοχή από τον διαχειριστή του συστήματος.

2.2.16.1 Ποιότητα – Απαιτήσεις κωδικού πρόσβασης

Μέσω του αρχείου /etc/security/pwquality.conf μπορούμε να ρυθμίσουμε τους ελέγχους που θα γίνονται στον κωδικό πρόσβασης κατά την δημιουργία του. Πιο συγκεκριμένα μπορούμε να ελέγξουμε εάν ο κωδικός ανήκει σε κάποιο λεξικό, ότι είναι συγκεκριμένου μήκους και ότι περιέχει έναν συνδυασμό από μεικτούς χαρακτήρες (πεζά – κεφαλαία – αριθμητικά – σύμβολα). Μπορούμε ακόμα να ορίσουμε το πλήθος των ελάχιστων χαρακτήρων από τα παραπάνω που θα περιέχει ένας ασφαλής κωδικός σύμφωνα με την πολιτική της επιχείρησης. Παρακάτω ακολουθούν οι επιλογές του αρχείου /etc/security/pwquality.conf καθώς και η λειτουργία που εκπληρώνουν.

Παράμετρος	Λειτουργία
minlen	Ελάχιστο μήκος κωδικού
dcredit	Ελάχιστα ψηφία κωδικού
ucredit	Ελάχιστοι κεφαλαίοι χαρακτήρες κωδικού
ocredit	Ελάχιστα σύμβολα κωδικού
lcredit	Ελάχιστοι πεζοί χαρακτήρες κωδικού

Εικόνα 55 - Πίνακας επιλογών αρχείου pwquality.conf

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/security/pwquality.conf και τις παραπάνω μεταβλητές σύμφωνα με την πολιτική της επιχείρησης.

```
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

Τρόπος Ελέγχου:

Εκτελούμε τις παρακάτω εντολές και ελέγχουμε εάν οι μεταβλητές έχουν την σωστή τιμή.

```
grep ^minlen /etc/security/pwquality.conf
grep ^dcredit /etc/security/pwquality.conf
grep ^lcredit /etc/security/pwquality.conf
grep ^ocredit /etc/security/pwquality.conf
grep ^ucredit /etc/security/pwquality.conf
```

```
[admin@centos7 ~]$ grep ^minlen /etc/security/pwquality.conf
minlen = 14
[admin@centos7 ~]$ grep ^dcredit /etc/security/pwquality.conf
dcredit = -1
[admin@centos7 ~]$ grep ^lcredit /etc/security/pwquality.conf
lcredit = -1
[admin@centos7 ~]$ grep ^ocredit /etc/security/pwquality.conf
ocredit = -1
[admin@centos7 ~]$ grep ^ucredit /etc/security/pwquality.conf
ucredit = -1
```

Εικόνα 56 - Έλεγχος πολιτικής κωδικού πρόσβασης

2.2.16.2 Παραμετροποίηση αρχείων password-auth και system-auth

Έπειτα από μελέτη των καλύτερων πρακτικών καθώς και της δικιά μας περίπτωσης χρήσης του συστήματος, δημιουργήθηκαν τα παρακάτω αρχεία στις διαδρομές /etc/pam.d/password-auth και /etc/pam.d/system-auth. Στο τέλος κάνουμε τα αρχεία αμετάβλητα (immutable).

```
auth        required                    pam_env.so
auth        required                    pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]    pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]    pam_localuser.so
auth            required
pam_faillock.so preauth silent deny=3 unlock_time=900 fail_interval=900
auth        sufficient                  pam_unix.so try_first_pass
auth            [default=die]
pam_faillock.so authfail deny=3 unlock_time=900 fail_interval=900
auth        requisite                   pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient                  pam_sss.so forward_pass
auth        required                    pam_deny.so
```

```
account  required
pam_faillock.so
account     required                      pam_unix.so
account     sufficient                    pam_localuser.so
account     sufficient                    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                      pam_permit.so

password    requisite                     pam_pwquality.so try_first_pass local_users_only retry=3
password    sufficient                          pam_unix.so sha512 shadow try_first_pass use_authtok
remember=5
password    sufficient                    pam_sss.so use_authtok
password    required                      pam_deny.so

session     optional                      pam_keyinit.so revoke
session     required                      pam_limits.so
-session    optional                      pam_systemd.so
session     [success=1 default=ignore]          pam_succeed_if.so service in crond quiet use_uid
session     required                      pam_unix.so
session     optional                      pam_sss.so
```

Εικόνα 57 - Τελικά αρχεία system-auth και password-auth

2.2.17 Μεταβλητές αρχείου /etc/login.defs

Στο συγκεκριμένο αρχείο μπορούμε να ρυθμίσουμε πότε θα λήγει ένας κωδικός πρόσβασης, την συχνότητα αλλαγής κωδικού, το χρονικό διάστημα που θα ενημερώνεται ο χρήστης για την λήξη του κωδικού του και την λήξη του έπειτα από περίοδο αδράνειας του χρήστη (μη-σύνδεση στο σύστημα για μεγάλο χρονικό διάστημα).

2.2.17.1 Λήξη κωδικού έπειτα από χρονικό διάστημα

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/login.defs και την παράμετρο PASS_MAX_DAYS. Έπειτα για κάθε χρήστη που δεν πληροί την ρύθμιση που κάναμε, εκτελούμε την παρακάτω εντολή.

```
chage --maxdays αριθμός_ημερών_λήξης χρήστης
```

Τρόπος Ελέγχου:

Ελέγχουμε με την παρακάτω εντολή εάν έχει ρυθμιστεί σωστά το αρχείο /etc/login.defs.

```
grep PASS_MAX_DAYS /etc/login.defs
```

```
[admin@centos7 ~]$ grep PASS_MAX_DAYS /etc/login.defs
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
PASS_MAX_DAYS 60
```

Εικόνα 58 - Παραμετροποίηση MAX_DAYS

2.2.17.2 Αποτροπή αλλαγής κωδικού πρόσβασης συνέχεια

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/login.defs και την παράμετρο PASS_MIN_DAYS. Έπειτα για κάθε χρήστη που δεν πληροί την ρύθμιση που κάναμε, εκτελούμε την παρακάτω εντολή.

```
chage --mindays αριθμός_ημερών χρήστης
```

Τρόπος Ελέγχου:

Ελέγχουμε με την παρακάτω εντολή εάν έχει ρυθμιστεί σωστά το αρχείο /etc/login.defs.

```
grep PASS_MIN_DAYS /etc/login.defs
[admin@centos7 ~]$ grep PASS_MIN_DAYS /etc/login.defs
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
PASS_MIN_DAYS 7
```

Εικόνα 59 - Παραμετροποίηση MIN_DAYS

2.2.17.3 Προειδοποίηση λήξης κωδικού πρόσβασης στον χρήστη

Τρόπος Ενεργοποίησης:

Τροποποιούμε το αρχείο /etc/login.defs και την παράμετρο PASS_WARN_AGE. Έπειτα για κάθε χρήστη που δεν πληροί την ρύθμιση που κάναμε, εκτελούμε την παρακάτω εντολή.

```
chage --warndays αριθμός_ημερών χρήστης
```

Τρόπος Ελέγχου:

Ελέγχουμε με την παρακάτω εντολή εάν έχει ρυθμιστεί σωστά το αρχείο /etc/login.defs.

```
grep PASS_WARN_AGE /etc/login.defs
[admin@centos7 ~]$ grep PASS_WARN_AGE /etc/login.defs
#       PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_WARN_AGE 14
```

Εικόνα 60 - Παραμετροποίηση WARN_AGE

Σημείωση!!! Για όλους τους χρήστες του συστήματος εκτελούμε την παρακάτω εντολή και βλέπουμε τις μεταβλητές. Εάν δεν συμβαδίζουν με αυτά που ρυθμίσαμε τότε πρέπει να εκτελέσουμε το βήμα της ενεργοποίησης (την εντολή του πλαισίου) από τα προηγούμενα κεφάλαια 2.2.17.1-2.2.17.3.

Για παράδειγμα ο χρήστης μας δεν πληροί τις προϋποθέσεις σύμφωνα με τα παρακάτω στοιχεία.

chage –list χρήστης

```
[admin@centos7 ~]$ chage --list admin
Last password change                                    : never
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

Εικόνα 61 - Έλεγχος χρήστη

2.2.18 UMASK 027 σε συγκεκριμένα αρχεία

Τα αρχεία των παρακάτω διαδρομών πρέπει να τροποποιηθούν ώστε να έχουν στο εσωτερικό τους umask 027 ή πιο αυστηρό.

Διαδρομές
/etc/bashrc
/etc/csh.cshrc
/etc/init.d/functions
/etc/profile

Εικόνα 62 - Αρχεία για χρήση umask 027

Τρόπος Ενεργοποίησης:

Τροποποιούμε τα αρχεία των διαδρομών και την παρακάτω γραμμή τους.

umask 027

Τρόπος Ελέγχου:

Για κάθε διαδρομή εκτελούμε την παρακάτω εντολή.

grep "umask" διαδρομή

```
[admin@centos7 ~]$ grep "umask" /etc/bashrc
    # By default, we want umask to get set. This sets it for non-login shell.
       umask 027
```

Εικόνα 63 - Έλεγχος umask αρχείων

2.2.19 Παραμετροποίηση αρχείου για την υπηρεσία SSH

Έπειτα από μελέτη των καλύτερων πρακτικών καθώς και της δικιά μας περίπτωσης χρήσης του συστήματος, παρουσιάζεται το τελικό αρχείο παραμετροποίησης /etc/ssh/sshd_config.

```
# SSH port.
Port 22

# Listen on IPv4 only.
ListenAddress 0.0.0.0

# Protocol version 1 has been exposed.
Protocol 2

#
# OpenSSH cipher-related release notes.
# OpenSSH 6.2: added support for AES-GCM authenticated encryption.
# The cipher is available as aes128-gcm@openssh.com and aes256-gcm@openssh.com.
# OpenSSH 6.5: added new cipher chacha20-poly1305@openssh.com.
# OpenSSH 6.7: removed unsafe algorithms. CBC ciphers are disabled by default:
# aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, cast128-cbc.
# OpenSSH 6.9: promoted chacha20-poly1305@openssh.com to be the default cipher.
#
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc

#
# OpenSSH 6.2: added support for the UMAC-128 MAC as umac-128@openssh.com
# and umac-128-etm@openssh.com. The latter being an encrypt-then-mac mode.
# Do not use umac-64 or umac-64-etm because of a small 64 bit tag size.
# Do not use any SHA1 (e.g. hmac-sha1, hmac-sha1-etm@openssh.com) MACs
# because of a weak hashing algorithm.
# https://crypto.stackexchange.com/questions/202/should-we-mac-then-encrypt-or-encrypt-then-mac
#
MACs hmac-sha2-512,hmac-sha2-256

#
# OpenSSH 6.5: added support for ssh-ed25519. It offers better security
# than ECDSA and DSA.
# OpenSSH 7.0: disabled support for ssh-dss.
# OpenSSH 7.2: added support for rsa-sha2-512 and rsa-sha2-256.
#
HostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,ssh-rsa,ecdsa-sha2-
nistp256,ecdsa-sha2-nistp384,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-
sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-
nistp521-cert-v01@openssh.com

#
# OpenSSH 6.5: added support for key exchange using elliptic-curve
# Diffie Hellman in Daniel Bernstein's Curve25519.
# OpenSSH 7.3: added support for diffie-hellman-group14-sha256,
```

```
# diffie-hellman-group16-sha512 and diffie-hellman-group18-sha512.
#
KexAlgorithms  curve25519-sha256@libssh.org,diffie-hellman-group18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group14-sha256

# HostKeys for protocol version 2.
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Disabled because uses a small 1024 bit key.
#HostKey /etc/ssh/ssh_host_dsa_key

# Disabled because uses weak elliptic curves.
# See: https://safecurves.cr.yp.to/
#HostKey /etc/ssh/ssh_host_ecdsa_key


# INFO is a basic logging level that will capture user login/logout activity.
# DEBUG logging level is not recommended for production servers.
LogLevel INFO

# Disconnect if no successful login is made in 60 seconds.
LoginGraceTime 60

# Do not permit root logins via SSH.
PermitRootLogin no

# Check file modes and ownership of the user's files before login.
StrictModes yes

# Close TCP socket after 2 invalid login attempts.
MaxAuthTries 2

# The maximum number of sessions per network connection.
MaxSessions 3

# User/group permissions.
AllowGroups
DenyUsers root
DenyGroups root

# Password and public key authentications.
PasswordAuthentication yes
PermitEmptyPasswords no
PubkeyAuthentication no
AuthorizedKeysFile  .ssh/authorized_keys

# Disable unused authentications mechanisms.
ChallengeResponseAuthentication no
KerberosAuthentication no
GSSAPIAuthentication no
HostbasedAuthentication no
```

```
IgnoreUserKnownHosts yes

# Disable insecure access via rhosts files.
IgnoreRhosts yes

AllowAgentForwarding no
AllowTcpForwarding no

# Disable X Forwarding.
X11Forwarding no

# Disable message of the day but print last log.
PrintMotd yes
PrintLastLog yes

# Show banner.
Banner /etc/issue

# Do not send TCP keepalive messages.
TCPKeepAlive no

# Prevent users from potentially bypassing some access restrictions.
PermitUserEnvironment no

# Disable compression.
Compression no

# Disconnect the client if no activity has been detected for 900 seconds.
ClientAliveInterval 300
ClientAliveCountMax 0

# Do not look up the remote hostname.
UseDNS no

UsePAM yes
```

Εικόνα 64 - Τελικό αρχείο παραμετροποίησης SSH

Τρόπος Ελέγχου:

Στην παρακάτω φωτογραφία φαίνονται οι εντολές για τον έλεγχο της σωστής παραμετροποίησης του SSH καθώς και το τι πρέπει να εκτυπώσει. Με κόκκινο έχουν υπογραμμιστεί οι εντολές ενώ με πράσινο η σωστή ρύθμισή τους.

```
[admin@centos7 ~]$ stat /etc/ssh/sshd_config
  File: '/etc/ssh/sshd_config'
  Size: 4178            Blocks: 16         IO Block: 4096   regular file
Device: fd01h/64769d    Inode: 791756      Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:etc_t:s0
Access: 2021-05-24 10:48:50.967775936 +0300
Modify: 2021-01-07 02:38:00.962825974 +0200
Change: 2021-01-07 02:38:00.980872693 +0200
 Birth: -
[admin@centos7 ~]$ sudo grep "^Protocol" /etc/ssh/sshd_config
Protocol 2
[admin@centos7 ~]$ sudo grep "^LogLevel" /etc/ssh/sshd_config
LogLevel INFO
[admin@centos7 ~]$ sudo grep "^X11Forwarding" /etc/ssh/sshd_config
X11Forwarding no
[admin@centos7 ~]$ sudo grep "^MaxAuthTries" /etc/ssh/sshd_config
MaxAuthTries 2
[admin@centos7 ~]$ sudo grep "^IgnoreRhosts" /etc/ssh/sshd_config
IgnoreRhosts yes
[admin@centos7 ~]$ sudo grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no
[admin@centos7 ~]$ sudo grep "^PermitRootLogin" /etc/ssh/sshd_config
PermitRootLogin no
[admin@centos7 ~]$ sudo grep "^PermitEmptyPasswords" /etc/ssh/sshd_config
PermitEmptyPasswords no
[admin@centos7 ~]$ sudo grep PermitUserEnvironment /etc/ssh/sshd_config
PermitUserEnvironment no
[admin@centos7 ~]$ sudo grep "Ciphers" /etc/ssh/sshd_config
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
[admin@centos7 ~]$ sudo grep "MACs" /etc/ssh/sshd_config
# Do not use any SHA1 (e.g. hmac-sha1, hmac-sha1-etm@openssh.com) MACs
MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1,hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com
[admin@centos7 ~]$ sudo grep "^ClientAliveInterval" /etc/ssh/sshd_config
ClientAliveInterval 300
[admin@centos7 ~]$ sudo grep "^ClientAliveCountMax" /etc/ssh/sshd_config
ClientAliveCountMax 0
```

Εικόνα 65 - Έλεγχος παραμετροποίησης SSH

Σημαντικό!!! Σε περίπτωση που κάνουμε οποιαδήποτε αλλαγή στο αρχείο πρέπει να γίνει επανεκκίνηση της υπηρεσίας SSH. Αυτό επιτυγχάνεται με την παρακάτω εντολή.

```
service sshd reload
```

2.3 Καλύτερες πρακτικές – Επαύξηση ασφάλειας Apache

Σε αυτό το κεφάλαιο θα παρουσιαστούν οι καλύτερες πρακτικές για την επαύξηση ασφάλειας του προγράμματος εξυπηρετητή ιστού Apache. Θα αναλυθούν διάφορα αρθρώματα που μπορούν να χρησιμοποιηθούν τόσο για άμυνα ενάντια σε επιθέσεις τύπου DoS Slowloris αλλά και σε επιθέσεις τύπου DoS HTTP Flood. Επιπλέον, θα κάνουμε παραμετροποιήσεις ώστε να μην διαρρέουν ευαίσθητα στοιχεία του εξυπηρετητή μας στους πελάτες του συστήματος όπως το λειτουργικό ή η έκδοση του Apache. Τέλος, θα δούμε την χρήση του Mod Security, ενός Web Application Firewall (WAF) που μπορεί να προστατεύσει τυχόν ευπάθειες που έχουν οι ιστοσελίδες μας όπως SQL Injection.

2.3.1 Αρχείο παραμετροποίησης Apache

Το αρχείο παραμετροποίησης του Apache βρίσκεται στην διαδρομή /etc/httpd/conf/httpd.conf.

Σημαντικές ρυθμίσεις σε αυτό το αρχείο που επιβάλλεται να γίνουν για την επαύξηση ασφάλειας του Apache είναι οι παρακάτω.

Μεταβλητές και λειτουργία /etc/httpd/conf/httpd.conf	
ServerTokens Prod	Θα δείχνει στην απάντηση μόνο το Apache
ServerSignature Off	Θα αφαιρέσει την έκδοση του Apache από την απάντηση
FileETag None	Αποτροπή εύρεσης inode number μέσω ETag κεφαλίδας
TraceEnable off	Απενεργοποίηση της δυνατότητας Trace
Header always append X-Frame-Options SAMEORIGIN	Άμυνα εναντίον Clickjacking επιθέσεων.
Header set X-XSS-Protection "1; mode=block"	Βασική προστασία έναντι XSS
Timeout 30	Βασική προστασία έναντι Slowloris
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure	Βασική προστασία έναντι XSS

Εικόνα 66 - Απάντηση του εξυπηρετητή ιστού μας - Response Header

Επιπλέον η χρήση των παρακάτω επιλογών δεν θα επιτρέψουν σε έναν χρήστη να κάνει κάποια επίθεση τύπου Directory Listing και να έχει πρόσβαση σε άλλα ευαίσθητα δεδομένα της διαδρομής καθώς και να μην ακολουθεί τα Symbolic Links.

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

Τέλος, είναι καλή πρακτική η χρήση ενός άλλου χρήστη για την εκτέλεση του apache και να μην εκτελείται ως root εξαρχής.

2.3.2 Άρθρωμα mod_evasive

Το άρθρωμα mod_evasive μπορεί να χρησιμοποιηθεί για να αντιμετωπιστούν επιθέσεις DoS HTTP Flood και να γίνουν blacklisted οι διευθύνσεις IP των επιτιθέμενων για κάποιο χρονικό διάστημα ή να τους εκτυπώνει μήνυμα σφάλματος. Παρακάτω παρουσιάζονται οι μεταβλητές καθώς και η λειτουργία τους.

Μεταβλητές και λειτουργία mod_evasive	
DOSHashTableSize 3097	Το μέγεθος του πίνακα που θα κρατάει τις δραστηριότητες μίας IP
DOSPageCount 2	Νόμιμα Requests που μπορεί να γίνουν προς ένα URL
DOSSiteCount 50	Νόμιμα Requests που μπορεί να γίνουν προς όλη την ιστοσελίδα
DOSPageInterval 1	Χρονική διαφορά που θα θεωρηθεί DoS για ένα URL
DOSSiteInterval 1	Χρονική διαφορά που θα θεωρηθεί DoS για όλο το site
DOSBlockingPeriod 600	Δευτερόλεπτα αποκλεισμού της IP σε δευτερόλεπτα
DOSLogDir /var/log/mod_evasive	Η διαδρομή του αρχείου καταγραφής
DOSEmailNotify root@localhost	Ειδοποίηση μέσω email του διαχειριστή

Εικόνα 67 - Πίνακας παραμετροποίησης μεταβλητών mod_evasive

Στο κεφάλαιο 4ο όπου θα γίνουν επιθέσεις HTTP Flood, θα δούμε πρακτικά την προστασία που προσφέρει το συγκεκριμένο άρθρωμα στο σύστημά μας.

Το συγκεκριμένο άρθρωμα δεν έρχεται προ-εγκατεστημένο στο σύστημα του CentOS. Θα πρέπει να εγκατασταθεί με την χρήση της εντολής yum install mod_evasive και έπειτα να ενεργοποιηθεί στον Apache σε ένα αρχείο παραμετροποίησης. Το δικό μας βρίσκεται στην διαδρομή: /etc/httpd/conf.d/mod_evasive.conf.

2.3.3 Άρθρωμα mod_qos

Το άρθρωμα mod_qos μπορεί να χρησιμοποιηθεί για την διασφάλιση της ποιότητας των υπηρεσιών του συστήματος προς τους τελικούς χρήστες. Επιπλέον, μπορεί να προσφέρει προστασία έναντι επιθέσεων Slowloris σε συνδυασμό με κάποιον κανόνα ενός αναχώματος ασφαλείας. Παρακάτω παρουσιάζονται οι μεταβλητές του mod_qos.

Μεταβλητές και λειτουργία mod_qos	
QS_ClientEntries 100000	Εξυπηρέτηση μέχρι <πλήθος> IP
QS_SrvMaxConnPerIP 20	Μέγιστες συνδέσεις από μία διεύθυνση IP
QS_SrvMaxConnClose 70%	Απενεργοποίηση keep-alive συνδέσεων όταν ο εξυπηρετητής φτάσει στο % χρήσης τους
QS_SrvMinDataRate 150 1200	Ταχύτητα (bps) request-response κύκλου. Άμυνα εναντίον Slowloris

Εικόνα 68 - Πίνακας παραμετροποίησης μεταβλητών mod_qos

Στο κεφάλαιο 4ο όπου θα γίνουν επιθέσεις Slowloris, θα δούμε πρακτικά την προστασία που προσφέρει το συγκεκριμένο άρθρωμα στο σύστημά μας.

Το συγκεκριμένο άρθρωμα έρχεται πλέον προ-εγκατεστημένο στο σύστημα του CentOS. Αρκεί μόνο η ενεργοποίησή του σε ένα αρχείο παραμετροποίησης του Apache που βρίσκεται στην παρακάτω διαδρομή: /etc/httpd/conf.d/qos.conf

2.3.4 Άρθρωμα mod_security

Το άρθρωμα mod_security είναι ένα WAF (**W**eb **A**pplication **F**irewall) το οποίο αρχικά σχεδιάστηκε μόνο για χρήση με το πρόγραμμα εξυπηρετητή ιστού Apache. Είναι ανοιχτού κώδικα και το βασικό του χαρακτηριστικό είναι οι δυνατότητες φιλτραρίσματος πεδίων στις ιστοσελίδες που εφαρμόζεται ώστε σε περίπτωση που ο κώδικάς τους επιτρέπει επιθέσεις όπως SQL Injection, να αποκόπτονται. Συνεπώς, ακόμα και εάν ο κώδικας της ιστοσελίδας έχει ευπάθειες, εφαρμόζεται άμυνα μέσω του αρθρώματος.

Για να εγκατασταθεί το mod_security πρέπει να εκτελεστούν με την σειρά οι παρακάτω εντολές. Το παρακάτω απόσπασμα αντιγράφει τους βασικούς κανόνες CRS (**C**ore **R**ule **S**et) που έρχονται μαζί με το άρθρωμα ώστε να χρησιμοποιηθούν από τον Apache.

```
yum install mod_security
mkdir /etc/httpd/crs
cd /etc/httpd/crs
wget https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master
tar -xvf master
mv SpiderLabs-owasp-modsecurity-crs-* owasp-modsecurity-crs
cd /etc/httpd/crs/owasp-modsecurity-crs/
cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_setup.conf
```

Έπειτα δημιουργούμε το παρακάτω αρχείο παραμετροποίησης και εισάγουμε τους επιπλέον κανόνες SecRule για άμυνα εναντίον της Slowloris επίθεσης.

```
touch /etc/httpd/modsecurity.d/mod_security.conf
cat > /etc/httpd/modsecurity.d/mod_security.conf <<EOF
<IfModule mod_security2.c>
   SecRuleEngine On
   SecStatusEngine On
   SecRequestBodyAccess On
   SecResponseBodyAccess On
   SecResponseBodyMimeType text/plain text/html text/xml application/octet-stream
   SecDataDir /tmp
   SecRule RESPONSE_STATUS "@streq 408" "phase:5,t:none,nolog,pass,setvar:ip.slow_dos_counter=+1, expirevar:ip.slow_dos_counter=60, id:'1234123456'"
   SecRule IP:SLOW_DOS_COUNTER "@gt 5" "phase:1,t:none,log,drop,msg:'Client Connection Dropped due to high number of slow DoS alerts', id:'1234123457'"
</IfModule>
EOF
```

Μπορούμε να ελέγξουμε για τα ενεργοποιημένα αρθρώματα στον Apache χρησιμοποιώντας την παρακάτω εντολή.

```
httpd -M
```

```
qos_module (shared)
security2_module (shared)
evasive20_module (shared)
```

Εικόνα 69 - Ενεργοποιημένα αρθρώματα στον Apache

Μας ενδιαφέρει να δούμε την παραπάνω ένδειξη καθώς είναι τα τρία αρθρώματα που ενεργοποιήσαμε στον Apache.

Τέλος, φορτώνουμε μία δική μας ιστοσελίδα στην διαδρομή /var/www/html και είμαστε έτοιμοι να δοκιμάσουμε την ασφάλεια του συστήματός μας.

Κεφάλαιο 3ο – Υλοποίηση Bash Script

Για να αυτοματοποιηθεί η εφαρμογή των καλύτερων πρακτικών σε ένα σύστημα λειτουργικού CentOS δημιουργήθηκε ένα Bash Script. Σε αυτό το κεφάλαιο θα αναλυθεί το Script που δημιουργήθηκε, οι δυνατότητές του καθώς θα αναρτηθεί και ο πηγαίος κώδικας.

3.1 Λειτουργίες – Δυνατότητες του Bash Script

Το Script που δημιουργήθηκε χωρίζεται σε δύο κυρίως τμήματα, αυτού που στόχο έχει την επαύξηση της ασφάλειας του λειτουργικού συστήματος CentOS και αυτού που στόχο έχει την επαύξηση λοιπών υπηρεσιών που χρησιμοποιούνται από τους χρήστες όπως SSH καθώς και του εξυπηρετητή ιστού Apache.

Ακολουθεί η σχετική λίστα με τις λειτουργίες – δυνατότητες του Bash Script.

[0]. Έλεγχοι πριν την εκτέλεση.
   a. Εγκατάσταση βασικών πακέτων για την ορθή λειτουργία του Script.
   b. Έλεγχοι κατάλληλων δικαιωμάτων για εκτέλεση του Script (πρέπει να εκτελεστεί με δικαιώματα root).
   c. Έλεγχος περιβάλλοντος εκτέλεσης (εκτελείται μόνο σε CentOS) καθώς και εάν εκτελείται σε λογισμικό VM. Καθορισμός διαδρομών περιβάλλοντος.

[1]. Βήματα μετά της αρχικής εγκατάστασης του CentOS.
   a. Αναβάθμιση πακέτων του συστήματος (update && upgrade).
   b. Εισαγωγή κωδικού στον GRUB Bootloader.

[2]. Δικαιώματα αρχείων και μάσκες.
   a. Απενεργοποίηση μη χρησιμοποιούμενων συστημάτων αρχείων.
   b. Απενεργοποίηση οδηγών και προσαρτημάτων πυρήνα.
   c. Περιορισμός των προγραμμάτων ώστε να μην εκτελούν επικίνδυνα μοτίβα για την ασφάλεια του συστήματος (sysctl).
   d. Τροποποίηση UMASK σημαντικών αρχείων.
   e. Απενεργοποίηση αποτυπωμάτων ΛΣ.
   f. Ρύθμιση των ορίων ασφαλείας των χρηστών.
   g. Απενεργοποίηση μη χρησιμοποιούμενων υπηρεσιών.
   h. Κλείδωμα Cron.

[3]. Παραμετροποίηση δικτύου και τείχους προστασίας.
   a. Απενεργοποίηση firewalld.

b. Παραμετροποίηση uncomplicated firewall (UFW).
c. Εγκατάσταση TCP Wrappers και παραμετροποίηση.
d. Παραμετροποίηση παραμέτρων δικτύου (sysctl).
e. Απενεργοποίηση μη χρησιμοποιούμενων πρωτοκόλλων.
f. Απενεργοποίηση ZeroConf Networking.
g. Απενεργοποίηση IPv6 καθώς και ασύρματων οδηγών.

[4]. Έλεγχος Security Enhanced Linux (SELinux).
a. Έλεγχος λειτουργίας sestatus.
b. Αφαίρεση πακέτου setroubleshoot.

[5]. Έλεγχος πρόσβασης και λογαριασμών.
a. Διαγραφή μη χρησιμοποιούμενων αρχικών λογαριασμών και ομάδων.
b. Απενεργοποίηση πρόσβασης στον λογαριασμό root.
c. Καθορισμός πολιτικής κωδικών πρόσβασης χρηστών.
d. Απενεργοποίηση λογαριασμών έπειτα από την λήξη του κωδικού.
e. Καταγραφή αποτυχημένων προσπαθειών πρόσβασης.
f. Δημιουργία διαδρομής Home για όλους τους χρήστες.
g. Επιβεβαίωση ότι όλοι οι κωδικού είναι shadowed.
h. Τροποποίηση αρχείων /etc/pam.d/system-auth και /etc/pam.d/password-auth.
i. Εγκατάσταση πακέτων για κλείδωμα κονσόλας.
j. Απενεργοποίηση χρήσης Ctrl-Alt-Delete.
k. Δημιουργία μηνυμάτων – μπάνερ πρόσβασης στο σύστημα.
l. Λήξη συνεδρίας έπειτα από αδράνεια.
m. Καθορισμός μεγέθους ιστορικού.

[6]. Παραμετροποίηση αρχείων καταγραφής και σχετικών πακέτων.
a. Τροποποίηση Logrotate.
b. Παραμετροποίηση auditd μεταβλητών.
c. Εισαγωγή κανόνων auditd.
d. Εγκατάσταση Rsyslog.
e. Καταγραφή γεγονότων πριν την εκκίνηση του συστήματος.

[7]. Εφαρμογή ελέγχου ακεραιότητας αρχείων συστήματος.
a. Εγκατάσταση Advanced Intrusion Detection Environment (AIDE).
b. Εισαγωγή του στο Crontab.

[8]. Εγκατάσταση Logwatch.

[9]. Λογισμικό ασφαλείας.
a. Εγκατάσταση και παραμετροποίηση Rootkit Hunter.
b. Εγκατάσταση και παραμετροποίηση ClamAV.

[1]. Επαύξηση ασφαλείας του SSH Daemon.
   a. Αλλαγή μεταβλητών αρχείου sshd_config.

[2]. Εγκατάσταση chronyd.

[3]. Αφαίρεση ρυθμίσεων απομακρυσμένης πρόσβασης.

[4]. Εγκατάσταση και παραμετροποίηση fail2ban.

   a. Περίπτωση SSH
   b. Περίπτωση Apache

[5]. Επαύξηση ασφάλειας εξυπηρετητή ιστού Apache.
   a. Παραμετροποίηση βασικού αρχειου etc/httpd/conf/httpd.conf
   b. Προστασία από Clickjacking.
   c. Προστασία από Directory Listing.
   d. Βασική προστασία από Cross-Site Scripting.
   e. Απενεργοποίηση λεπτομερούς υπογραφής ‘εξυπηρετητή ιστου’.
   f. Εγκατάσταση και παραμετροποίηση αρθρώματος mod_evasive.
   g. Εγκατάσταση και παραμετροποίηση αρθρώματος mod_security.
   h. Παραμετροποίηση αρθρώματος mod_qos.

3.2 Παρουσίαση του Bash Script

Παρακάτω βρίσκεται ο πηγαίος κώδικας του Bash Script (.sh). Επιπλέον, ο κώδικας μπορεί να ανακτηθεί και από το GitHub, χρησιμοποιώντας το παρακάτω σύνδεσμο:

https://github.com/Kostas-Galanomatis/CentOS_7_Hardening_Script

Πηγαίος κώδικας Bash Script – CentOS_7_Hardening_Script.sh

```
#!/usr/bin/bash
################################################################################

# CONFIGURATION STARTS HERE

################################################################################

APACHE2DFILE='/etc/httpd/conf/httpd.conf'
AUDITDCONF='/etc/audit/auditd.conf'
AUDITRULES='/etc/audit/rules.d/audit.rules'
COREDUMPCONF='/etc/systemd/coredump.conf'
DEFAULTGRUB='/etc/default/grub'
DISABLEFS='/etc/modprobe.d/disablemnt.conf'
DISABLEMOD='/etc/modprobe.d/disablemod.conf'
DISABLENET='/etc/modprobe.d/disablenet.conf'
```

```
DISABLEWIRELESS='/etc/modprobe.d/disablewireless.conf'
EXPECT='/usr/bin/expect'
FW_LOCAL='127.0.0.1'
GRUB_PASSPHRASE='password'
GRUB_SUPERUSER='myuser'
GUI='Y'
HOSTSALLOW='/etc/hosts.allow'
HOSTSDENY='/etc/hosts.deny'
JOURNALDCONF='/etc/systemd/journald.conf'
LIMITSCONF='/etc/security/limits.conf'
LOGINDCONF='/etc/systemd/logind.conf'
LOGINDEFS='/etc/login.defs'
LOGROTATE='/etc/logrotate.conf'
MKPASSWD='/usr/bin/grub2-mkpasswd-pbkdf2'
MOD='appletalk bnep bluetooth btusb net-pf-31 soundcore thunderbolt usb-midi'
NPACKAGES='epel-release expect redhat-lsb-core samba ufw'
PACKAGES='httpd mod_qos tcp_wrappers'
PASSWORDAUTH='/etc/pam.d/password-auth'
PASSWORDQUALITY='/etc/security/pwquality.conf'
RKHUNTERCONF='/etc/rkhunter.conf'
SECURITYACCESS='/etc/security/access.conf'
SERVER='Y'
SSHDFILE='/etc/ssh/sshd_config'
SYSCTL='/etc/sysctl.conf'
SYSTEMAUTH='/etc/pam.d/system-auth'
SYSTEMCONF='/etc/systemd/system.conf'
SYSTEMNET='/etc/sysconfig/network'
UFWBEFORERULES='/etc/ufw/before.rules'
UFWDEFAULT='/etc/default/ufw'
UMASKFILES='/etc/bashrc /etc/csh.cshrc /etc/init.d/functions /etc/profile'
USERADD='/etc/default/useradd'
USERCONF='/etc/systemd/user.conf'
UNW_PROT='dccp sctp rds tipc'
UNW_SERVICES='avahi-daemon kdump mdmonitor rhsmcertd smartd'
UNW_FS='cramfs cifs fat freevxfs gfs2 jffs2 hfs hfsplus nfs nfsv3 nfsv4 squashfs udf vfat'
VERBOSE='Y'
VM="

################################################################################

# CONFIGURATION ENDS HERE

################################################################################

echo "---------- CentOS 7/8 Apache Web Server Hardening ----------"
################################################################################
# Check that we have bare minimum...(OK)

echo "---------- Doing some pre-execution checks ----------"

echo "Installing Needed packages so the script can be executed..."

for pack in $NPACKAGES; do
echo "Installing $pack package..."
   if [[ $VERBOSE == "Y" ]]; then
      yum install -y "$pack"
   else
      yum install -q -y "$pack"
   fi
done

if [ $EUID -ne 0 ]; then
   echo "This script must be run with root privileges..."
   echo
   exit 1
else
   echo "You run the script with root privileges. Script will continue..."
```

```
    echo
fi

if ! lsb_release -i | grep 'CentOS'; then
    echo "Unsupported Operating System. Only CentOS Supported..."
    echo
    exit 1
else
    echo "You run the script at CentOS operating system. Script will continue..."
    echo
fi

if ! [ -x "$(which systemctl)" ]; then
            echo "systemctl required. Unsupported setup..."
    echo
            exit 1
else
    echo "systemctl is OK. Script will continue..."
    echo
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

# Check that we have bare minimum end...(OK)
#################################################################################
# Set paths...(OK)

echo "Setting environment 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

echo "Setting environment paths completed..."

# Set paths end...(OK)
#################################################################################
# Set apt environment...(OK)

if [[ $VERBOSE == "Y" ]]; then
    APT_ENV='-y'
else
    APT_ENV='-q -y'
fi

APT="yum $APT_ENV"

# Set apt environment end...(OK)
```

```
################################################################################
# Check if we are running VM...(OK)

if dmidecode -q --type system | grep -i vmware; then
   VM="open-vm-tools"
   echo "The CentOS is running on VMWare VM environment..."
fi

if dmidecode -q --type system | grep -i virtualbox; then
   VM="virtualbox-guest-dkms virtualbox-guest-utils"
   echo "The CentOS is running on VirtualBox VM environment..."
fi

if [ $VM != " ]; then
   for pack in $VM; do
      $APT install "$pack"
      echo "Installing $pack package..."
   done
fi

# Check if we are running VM end...(OK)
################################################################################

echo "---------- End of pre-execution checks & tasks ----------"
echo "---------- Let's start by hardening the system settings ----------"

################################################################################
# Chapter 1...(OK)

echo "---------- Chapter 1 - Post installation ----------"

################################################################################
# Make sure system is up to date... (OK)

echo "---------- Section 1.1 - Make sure system is up to date ----------"

echo "Updating the package index files..."
$APT update
echo "Upgrading installed packages..."
$APT upgrade

# Make sure system is up to date end... (OK)
################################################################################
# Secure Bootloader... (OK)

echo "---------- Section 1.2 - Secure Bootloader ----------"

echo "Securing bootloader with Username: $GRUB_SUPERUSER and Password: $GRUB_PASSPHRASE"

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
    cp /boot/grub2/grub.cfg /boot/grub2/grub.cfg.backup
    grub2-mkconfig -o /boot/grub2/grub.cfg
fi

chown root:root /boot/grub2/grub.cfg
chmod og-rwx /boot/grub2/grub.cfg

# Secure Bootloader end... (OK)
################################################################################

echo "---------- Chapter 1 - Completed ----------"

# Chapter 1 end...(OK)
################################################################################
# Chapter 2...(OK)

echo "---------- Chapter 2 - File Permissions and Masks ----------"

################################################################################
# Restrict Dynamic Mounting and Unmounting of Filesystems... (OK)

echo "---------- Section 2.1 - Restrict Dynamic Mounting and Unmounting of Filesystems ----------"

echo "Disabling file systems..."
for disable in $UNW_FS; do
    if ! grep -q "$disable" "$DISABLEFS" 2> /dev/null; then
        echo "install $disable /bin/true" >> "$DISABLEFS"
        echo "Disabling $disable file system..."
    fi
done

echo "Configuration file for disabled file systems can be found at the directory: $DISABLEFS"

# Restrict Dynamic Mounting and Unmounting of Filesystems end... (OK)
################################################################################
# Prevent Users Mounting USB Storage... (OK)

echo "---------- Section 2.2 - Prevent Users Mounting USB Storage ----------"

echo "blacklist usb-storage" >> "$DISABLEMOD"
echo "blacklist firewire-core" >> "$DISABLEMOD"
echo "install usb-storage /bin/true" >> "$DISABLEMOD"
echo "Configuration file for prevention for mounting USB Storage can be found at the directory: $DISABLEMOD"

# Prevent Users Mounting USB Storage end... (OK)
################################################################################
# Restrict Programs from Dangerous Execution Patterns... (OK)

echo "---------- Section 2.3 - Restrict Programs from Dangerous Execution Patterns ----------"

echo "Configuring $SYSCTL file..."
echo "This will cover section 2.4 and section 3.3 at once..."

cat > $SYSCTL <<EOF
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
```

```
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).

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

# Restrict Programs from Dangerous Execution Patterns end... (OK)
################################################################################
# Set UMASK 027... (OK)

echo "---------- Section 2.4 - Set UMASK 027 ----------"

echo "UMASK 027 important files..."
for mask in $UMASKFILES; do
   echo "UMASK file $mask..."
   sed -i -e 's/umask 022/umask 027/g' -e 's/umask 002/umask 027/g' "$mask"
done

# Set UMASK 027 end... (OK)
################################################################################
# Disable Core Dumps... (OK)

echo "---------- Section 2.5 - Disable Core Dumps ----------"

echo "Disable Core Dumps at $LIMITSCONF file..."
cat > $LIMITSCONF <<EOF
* hard core 0

# 4096 is a good starting point
*      soft   nofile    4096
*      hard   nofile    65536
*      soft   nproc     4096
*      hard   nproc     4096
*      soft   locks     4096
*      hard   locks     4096
*      soft   stack     10240
*      hard   stack     32768
*      soft   memlock   64
*      hard   memlock   64
*      hard   maxlogins 10

# Soft limit 32GB, hard 64GB
*      soft   fsize     33554432
*      hard   fsize     67108864

# Limits for root
root   soft   nofile    4096
root   hard   nofile    65536
root   soft   nproc     4096
root   hard   nproc     4096
root   soft   stack     10240
root   hard   stack     32768
root   soft   fsize     33554432
# End of file
EOF

echo "Disable Core Dumps at $SYSTEMCONF and $USERCONF file..."

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=4096/' "$SYSTEMCONF"
sed -i 's/^#DefaultLimitNPROC=.*/DefaultLimitNPROC=4096/' "$SYSTEMCONF"

sed -i 's/^#DefaultLimitCORE=.*/DefaultLimitCORE=0/' "$USERCONF"
sed -i 's/^#DefaultLimitNOFILE=.*/DefaultLimitNOFILE=4096/' "$USERCONF"
sed -i 's/^#DefaultLimitNPROC=.*/DefaultLimitNPROC=4096/' "$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

# Disable Core Dumps end... (OK)
################################################################################
# Set Security Limits to Prevent DoS... (OK)

echo "---------- Section 2.6 - Set Security Limits to Prevent DoS ----------"

echo "Set Security Limits to Prevent DoS at $LIMITSCONF file..."
echo "We covered section 2.6 at previous section 2.5! $LIMITSCONF is already configured..."

# Set Security Limits to Prevent DoS end... (OK)
################################################################################
# Disable Unwanted Services... (OK)

echo "---------- Section 2.7 - Disable Unwanted Services ----------"

echo "Disabling unwanted services..."

for disable in $UNW_SERVICES; do
   echo "Disabling $disable service..."
   systemctl disable $disable
done

# Disable Unwanted Services end... (OK)
################################################################################
# Disabling RPC and CUPS...(OK)

echo "Disabling RPC..."
systemctl stop rpcbind.service
systemctl disable rpcbind.service
systemctl mask rpcbind.service
systemctl stop rpcbind.socket
systemctl disable rpcbind.socket
systemctl mask rpcbind.socket

echo "Disabling CUPS..."
systemctl stop cups.service
systemctl disable cups.service
systemctl mask cups.service
systemctl stop cups.socket
systemctl disable cups.socket
systemctl mask cups.socket

# Disabling RPC and CUPS end...(OK)
################################################################################
# Lock Down Cron... (OK)
```

```
echo "---------- Section 2.8 - Lock Down Cron ----------"

echo "Locking down Cron..."
touch /etc/cron.allow
chmod 600 /etc/cron.allow
awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/cron.deny
echo "Locking down AT..."
touch /etc/at.allow
chmod 600 /etc/at.allow
awk -F: '{print $1}' /etc/passwd | grep -v root > /etc/at.deny

for pathings in /etc/cron.hourly /etc/cron.daily /etc/cron.weekly /etc/cron.monthly /etc/cron.d /etc/crontab; do
   chmod 700 "$pathings"
done

rm /etc/cron.deny
rm /etc/at.deny

# Lock Down Cron end... (OK)
################################################################################

echo "---------- Chapter 2 - Completed ----------"

# Chapter 2 end...(OK)
################################################################################
# Chapter 3...(OK)

echo "---------- Chapter 3 - Firewall and Network Configuration ----------"

################################################################################
# Firewall... (OK)

echo "---------- Section 3.1 - Firewall ----------"

echo "Shutdown firewalld.service..."
systemctl stop firewalld.service
systemctl disable firewalld.service
systemctl mask firewalld.service
systemctl daemon-reload
echo "Configuring Uncomplicated Firewall..."

sed -i 's/IPT_SYSCTL=.*/IPT_SYSCTL=\/etc\/sysctl\.conf/' "$UFWDEFAULT"
sed -i 's/IPV6=.*/IPV6=no/' "$UFWDEFAULT"

systemctl enable ufw
systemctl start ufw

cat > $UFWBEFORERULES <<EOF
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
:ufw-http - [0:0]
:ufw-http-logdrop - [0:0]
# End required lines
```

```
# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT

#
# ufw-not-local
#
-A ufw-before-input -j ufw-not-local

# if LOCAL, RETURN
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

# if MULTICAST, RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

# if BROADCAST, RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

# all other non-local packets are dropped
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP

### Start HTTP ###

# Enter rule
-A ufw-before-input -p tcp --dport 80   -j ufw-http
-A ufw-before-input -p tcp --dport 443  -j ufw-http

# Limit connections per Class C
-A ufw-http -p tcp --syn -m connlimit --connlimit-above 20 --connlimit-mask 40 -j ufw-http-logdrop

# Limit connections per IP
-A ufw-http -m state --state NEW -m recent --name conn_per_ip --set
-A ufw-http -m state --state NEW -m recent --name conn_per_ip --update --seconds 10 --hitcount 20 -j ufw-http-
logdrop

# Limit packets per IP
-A ufw-http -m recent --name pack_per_ip --set
-A ufw-http -m recent --name pack_per_ip --update --seconds 1  --hitcount 20  -j ufw-http-logdrop
```

```
# Finally accept
-A ufw-http -j ACCEPT

# Log-A ufw-http-logdrop -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW HTTP DROP] "
-A ufw-http-logdrop -j DROP

### End HTTP ###


# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
EOF

if [[ $SERVER == "Y" ]]; then
   ufw allow http
fi

ufw logging on
ufw reload

if [[ $VERBOSE == "Y" ]]; then
   systemctl status ufw.service --no-pager
   ufw status verbose
   echo
fi

# Firewall end... (OK)
################################################################################
# TCP Wrappers... (OK)

echo "---------- Section 3.2 - TCP Wrappers ----------"

echo "Configuring TCP Wrappers..."

if [[ $SERVER == "Y" ]]; then
   echo "sshd : ALL : ALLOW" > "$HOSTSALLOW"
fi
echo "ALL: LOCAL, 127.0.0.1" >> "$HOSTSALLOW"
echo "ALL: ALL" >> "$HOSTSDENY"
chmod 644 "$HOSTSALLOW"
chmod 644 "$HOSTSDENY"

# TCP Wrappers end... (OK)
################################################################################
# Kernel Parameters Which Affect Networking... (OK)

echo "---------- Section 3.3 - Kernel Parameters Which Affect Networking ----------"

echo "We covered section 3.3 at previous section 2.4! $SYSCTL is already configured..."

# Kernel Parameters Which Affect Networking end... (OK)
################################################################################
# Kernel Modules Which Affect Networking... (OK)

echo "---------- Section 3.4 - Kernel Modules Which Affect Networking ----------"

echo "Disabling unwanted kernel modules..."

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

echo "Configuration file for unwanted kernel modules can be found at the directory: $DISABLEMOD"
```

```
echo "Disabling unwanted protocols..."
for disable in $UNW_PROT; do
   if ! grep -q "$disable" "$DISABLENET" 2> /dev/null; then
      echo "install $disable /bin/true" >> "$DISABLENET"
      echo "Disabling $disable protocol..."
   fi
done

echo "options ipv6 disable=1" >> "$DISABLENET"

echo "Configuration file for unwanted protocols can be found at the directory: $DISABLENET"

# Kernel Modules Which Affect Networking end... (OK)
################################################################################
# Disable Radios... (OK)

echo "---------- Section 3.5 - Disable Radios ----------"

echo "Disabling radios..."
nmcli radio all off

echo "Disabling Wireless Drivers..."
for i in $(find /lib/modules/$(uname -r)/kernel/drivers/net/wireless -name "*.ko" -type f);do
   echo blacklist "$i" >>"$DISABLEWIRELESS";
done

echo "Configuration file for unwanted protocols can be found at the directory: $DISABLEWIRELESS"

# Disable Radios end... (OK)
################################################################################
# Disable Zeroconf Networking... (OK)

echo "---------- Section 3.6 - Disable Zeroconf Networking ----------"

echo "Disable Zeroconf Networking at file $SYSTEMNET"
echo "NOZEROCONF=yes" >> "$SYSTEMNET"

# Disable Zeroconf Networking end... (OK)
################################################################################
# Disable Interface Usage of IPv6... (OK)

echo "---------- Section 3.7 - Disable Interface Usage of IPv6 ----------"

echo "Disable interface usage of IPv6 at file $SYSTEMNET"
echo "NETWORKING_IPV6=no" >> "$SYSTEMNET"
echo "IPV6INIT=no" >> "$SYSTEMNET"

# Disable Interface Usage of IPv6 end... (OK)
################################################################################

echo "---------- Chapter 3 - Completed ----------"

# Chapter 3 end...(OK)
################################################################################
# Chapter 4...(OK)

echo "---------- Chapter 4 - System Settings – SELinux ----------"

################################################################################
# Check sestatus and grub state enforcing... (OK)

echo "---------- Section 4.1 - Check sestatus and grub state enforcing ----------"

echo "Check sestatus below...By default should be enforcing!"

sestatus
```

```
# Check sestatus and grub state enforcing end... (OK)
################################################################################
# Delete setroubleshoot... (OK)

echo "---------- Section 4.2 - Delete setroubleshoot ----------"

echo "Removing setroubleshoot..."

$APT erase setroubleshoot
$APT erase abrt

# Delete setroubleshoot... (OK)
################################################################################

echo "---------- Chapter 4 - Completed ----------"

# Chapter 4 end...(OK)
################################################################################
# Chapter 5...(OK)

echo "---------- Chapter 5 - Account and Access Control ----------"

################################################################################
# Delete Unused Accounts and Groups... (OK)

echo "---------- Section 5.1 - Delete Unused Accounts and Groups ----------"

echo "Deleting unused accounts..."
for users in ftp games gnats irc list news uucp; do
   userdel -r "$users" 2> /dev/null
   echo "Deleting $users account..."
done

echo "Deleting unused groups..."
echo "Deleting games group..."
groupdel games

# Delete Unused Accounts and Groups end... (OK)
################################################################################
# Disable root... (OK)

echo "---------- Section 5.2 - Disable root ----------"

echo "Disabling root logins..."

sed -i 's/^#+ : root : 127.0.0.1/+ : root : 127.0.0.1/' "$SECURITYACCESS"
echo " > /etc/securetty

echo "Locking out root account..."

usermod -L root

if [[ $VERBOSE == "Y" ]]; then
   passwd -S root
   echo
fi

# Disable root end... (OK)
################################################################################
# Enable Secure (high quality) Password Policy... (OK)

echo "---------- Section 5.3 - Enable Secure (high quality) Password Policy ----------"

echo "Making a strong password policy using authconfig..."

echo "Doing changes to $PASSWORDQUALITY file..."
```

```
sed -i 's/# difok.*/difok = 8/g' "$PASSWORDQUALITY"
sed -i 's/# minlen.*/minlen = 14/g' "$PASSWORDQUALITY"
sed -i 's/# dcredit.*/dcredit = -1/g' "$PASSWORDQUALITY"
sed -i 's/# ucredit.*/ucredit = -1/g' "$PASSWORDQUALITY"
sed -i 's/# lcredit.*/lcredit = -1/g' "$PASSWORDQUALITY"
sed -i 's/# ocredit.*/ocredit = -1/g' "$PASSWORDQUALITY"
sed -i 's/# minclass.*/minclass = 1/g' "$PASSWORDQUALITY"
sed -i 's/# maxrepeat.*/maxrepeat = 2/g' "$PASSWORDQUALITY"
sed -i 's/# maxclassrepeat.*/maxclassrepeat = 2/g' "$PASSWORDQUALITY"
sed -i 's/# gecoscheck.*/gecoscheck = 1/g' "$PASSWORDQUALITY"

# Enable Secure (high quality) Password Policy end... (OK)
################################################################################
# Set Account Expiration Following Inactivity... (OK)

echo "---------- Section 5.4 - Set Account Expiration Following Inactivity ----------"

echo "Changing INACTIVE parameter at $USERADD file..."
sed -i 's/^INACTIVE.*/INACTIVE=0/' "$USERADD"

# Set Account Expiration Following Inactivity end... (OK)
################################################################################
# Secure Password Policy... (OK)

echo "---------- Section 5.5 - Secure Password Policy ----------"

echo "Making Changes to $LOGINDEFS for secure password policy..."
sed -i -e 's/^PASS_MAX_DAYS.*/PASS_MAX_DAYS 60/' \
  -e 's/^PASS_MIN_DAYS.*/PASS_MIN_DAYS 7/' \
  -e 's/^PASS_MIN_LEN.*/PASS_MIN_LEN 14/' \
  -e 's/^PASS_WARN_AGE.*/PASS_WARN_AGE 14/' "$LOGINDEFS"

# Secure Password Policy end... (OK)
################################################################################
# Log Failed Login Attempts... (OK)

echo "---------- Section 5.6 - Log Failed Login Attempts ----------"

echo "Making Changes to $LOGINDEFS to Log Failed Login Attempts..."
echo "FAILLOG_ENAB yes" >> "$LOGINDEFS"
echo "FAIL_DELAY 4" >> "$LOGINDEFS"

# Log Failed Login Attempts end... (OK)
################################################################################
# Ensure Home Directories are Created for New Users... (OK)

echo "---------- Section 5.7 - Ensure Home Directories are Created for New Users ----------"

echo "Making Changes to $LOGINDEFS to Ensure Home Directories are Created for New Users..."
sed -i 's/^CREATE_HOME.*/CREATE_HOME\t\tyes/' "$LOGINDEFS"

# Ensure Home Directories are Created for New Users end... (OK)
################################################################################
# Verify All Account Password Hashes are Shadowed... (OK)

echo "---------- Section 5.8 - Verify All Account Password Hashes are Shadowed ----------"

echo "You should see a x after this message if password hashes are shadowed..."
cut -d: -f2 /etc/passwd|uniq

# Verify All Account Password Hashes are Shadowed end... (OK)
################################################################################
# Set Deny and Lockout Time for Failed Password Attempts... (OK)

echo "---------- Section 5.9 - Set Deny and Lockout Time for Failed Password Attempts ----------"

echo "Configuring $PASSWORDAUTH and $SYSTEMAUTH files..."
```

```
cat > $PASSWORDAUTH <<EOF
# Edited by CentOS Hardening Script... passwordauth

auth        required                    pam_env.so
auth        required                    pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]    pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]    pam_localuser.so
auth            required
pam_faillock.so preauth silent deny=3 unlock_time=900 fail_interval=900
auth        sufficient                  pam_unix.so try_first_pass
auth            [default=die]
pam_faillock.so authfail deny=3 unlock_time=900 fail_interval=900
auth        requisite                   pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient                  pam_sss.so forward_pass
auth        required                    pam_deny.so

account     required                                                    pam_faillock.so
account     required                    pam_unix.so
account     sufficient                  pam_localuser.so
account     sufficient                  pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                    pam_permit.so

password    requisite                   pam_pwquality.so try_first_pass local_users_only retry=3
password    sufficient                  pam_unix.so sha512 shadow try_first_pass use_authtok remember=5
password    sufficient                  pam_sss.so use_authtok
password    required                    pam_deny.so

session     optional                    pam_keyinit.so revoke
session     required                    pam_limits.so
-session    optional                    pam_systemd.so
session     [success=1 default=ignore]          pam_succeed_if.so service in crond quiet use_uid
session     required                    pam_unix.so
session     optional                    pam_sss.so
EOF

cat > $SYSTEMAUTH <<EOF
# Edited by CentOS Hardening Script... systemauth

auth        required                    pam_env.so
auth        required                    pam_faildelay.so delay=2000000
auth        sufficient                  pam_fprintd.so
auth        [default=1 ignore=ignore success=ok]    pam_succeed_if.so uid >= 1000 quiet
auth        [default=1 ignore=ignore success=ok]    pam_localuser.so
auth            required
pam_faillock.so preauth silent deny=3 unlock_time=900 fail_interval=900
auth        sufficient                  pam_unix.so try_first_pass
auth            [default=die]
pam_faillock.so authfail deny=3 unlock_time=900 fail_interval=900
auth        requisite                   pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient                  pam_sss.so forward_pass
auth        required                    pam_deny.so

account     required                                                    pam_faillock.so
account     required                    pam_unix.so
account     sufficient                  pam_localuser.so
account     sufficient                  pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                    pam_permit.so

password    requisite                   pam_pwquality.so try_first_pass local_users_only retry=3
password    sufficient                  pam_unix.so sha512 shadow try_first_pass use_authtok remember=5
password    sufficient                  pam_sss.so use_authtok
password    required                    pam_deny.so

session     optional                    pam_keyinit.so revoke
```

```
session     required                    pam_limits.so
-session    optional                    pam_systemd.so
session     [success=1 default=ignore]          pam_succeed_if.so service in crond quiet use_uid
session     required                    pam_unix.so
session     optional                    pam_sss.so
EOF

echo "Making configurations immutable... $PASSWORDAUTH and $SYSTEMAUTH files..."
chattr +i "$PASSWORDAUTH"
chattr +i "$SYSTEMAUTH"

# Set Deny and Lockout Time for Failed Password Attempts end... (OK)
################################################################################
# Multiple Console Screens and Console Locking... (OK)

echo "---------- Section 5.10 - Multiple Console Screens and Console Locking ----------"
for pack in screen vlock; do
   echo "Installing $pack package..."
   $APT install "$pack"
done

# Multiple Console Screens and Console Locking end... (OK)
################################################################################
# Disable Ctrl-Alt-Del Reboot Activation... (OK)

echo "---------- Section 5.11 - Disable Ctrl-Alt-Del Reboot Activation ----------"

echo "Disabling Ctrl-Alt-Delete combination..."

systemctl mask ctrl-alt-del.target

if [[ $VERBOSE == "Y" ]]; then
   systemctl status ctrl-alt-del.target --no-pager
   echo
fi

# Disable Ctrl-Alt-Del Reboot Activation end... (OK)
################################################################################
# Warning Banners for System Access... (OK)

echo "---------- Section 5.12 - Warning Banners for System Access ----------"

echo "Configuring warning banners for system access..."

for f in /etc/issue /etc/issue.net /etc/motd; do
   TEXT=" *** NOTICE TO USERS ***
   This computer system is the private property of company_name...
   It is for authorized use only. "
   echo -e "$TEXT" > $f
done

# Warning Banners for System Access end... (OK)
################################################################################
# Set Interactive Session Timeout... (OK)

echo "---------- Section 5.13 - Set Interactive Session Timeout ----------"

echo "Setting interactive session timeout at etc/profile file..."

if grep --silent ^TMOUT /etc/profile ; then
      sed -i "s/^TMOUT.*/TMOUT=600/g" /etc/profile
else
      echo -e "\n# Set TMOUT to 600 per security requirements" >> /etc/profile
      echo "TMOUT=600" >> /etc/profile
fi

# Set Interactive Session Timeout end... (OK)
```

```
################################################################################
# Configure History File Size... (OK)

echo "---------- Section 5.14 - Configure History File Size ----------"

echo "Configuring history file size at etc/profile file..."
sed -i 's/HISTSIZE=.*/HISTSIZE=5000/g' /etc/profile

# Configure History File Size end... (OK)
################################################################################

echo "---------- Chapter 5 - Completed ----------"

# Chapter 5 end...(OK)
################################################################################
# Chapter 6...(OK)

echo "---------- Chapter 6 - System Accounting with auditd ----------"

################################################################################
# Set Interactive Session Timeout... (OK)

echo "---------- Section 6.1 - Configure Logrotate and JournalD ----------"

echo "Configuring logrotate..."

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

# 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/' "$JOURNALDCONF"
sed -i 's/^#SystemMaxFileSize=.*/SystemMaxFileSize=32M/' "$JOURNALDCONF"
sed -i 's/^#SystemKeepFree=.*/SystemKeepFree=512M/' "$JOURNALDCONF"
sed -i 's/^#SystemMaxUse=.*/SystemMaxUse=256M/' "$JOURNALDCONF"
sed -i 's/^#ForwardToSyslog=.*/ForwardToSyslog=yes/' "$JOURNALDCONF"
sed -i 's/^#Compress=.*/Compress=yes/' "$JOURNALDCONF"

logrotate -f /etc/logrotate.conf
systemctl restart systemd-journald

if [[ $VERBOSE == "Y" ]]; then
   systemctl status systemd-journald --no-pager
   echo
fi

################################################################################
# Auditd Configuration... (OK)

echo "---------- Section 6.2 - Auditd Configuration ----------"

echo "Installing rsyslog package..."
$APT install rsyslog

echo "Enable rsyslog service..."
systemctl enable rsyslog.service
systemctl start rsyslog.service

if [[ $VERBOSE == "Y" ]]; then
   systemctl status rsyslog.service --no-pager
   echo
fi

echo "Configuring $AUDITDCONF file..."

# Auditd num_logs
if grep -q ^num_logs "$AUDITDCONF"
then
        echo "Number of logs retained already exist..."
        sed -i 's/num_logs.*/num_logs = 10/g' "$AUDITDCONF"
        echo "Default: Replaced the count to 10..."
else
        echo "num_logs = 10" >> "$AUDITDCONF"
        echo "Number of logs retained is added & configured to 10..."
fi

# Auditd max_log_file and max_log_file_action
if grep -q ^max_log_file "$AUDITDCONF"
then
        echo "Max log file size already configured..."
        sed -i '/max_log_file_action/d' "$AUDITDCONF"
        sed -i 's/max_log_file.*/max_log_file = 30/g' "$AUDITDCONF"
        echo "Default:Replaced Max Log File Size 30MB..."
        echo "max_log_file_action = keep_logs" >> "$AUDITDCONF"
        echo "Default : max_log_file_action is set to keep_logs..."
else
        echo "max_log_file = 30" >> "$AUDITDCONF"
        echo "Max Log File Size is Added & configured to 30MB..."
fi

# Auditd space_left and admin_space_left
echo "Configure auditd to email you when space gets low..."
if grep -q ^space_left_action "$AUDITDCONF"
then
        echo "space_left is already configured..."
        sed -i '/admin_space_left_action/d' "$AUDITDCONF"
```

```
        sed -i 's/space_left_action.*/space_left_action = email/g' "$AUDITDCONF"
        echo "space_left_action is set to email..."
        echo "admin_space_left_action = halt" >> "$AUDITDCONF"
        echo "admin_space_left_action is set to halt..."
else
        echo "space_left_action = email" >> "$AUDITDCONF"
        echo "space_left_action is set to email..."
fi

# Auditd action_mail_acct
if grep -q ^action_mail_acct "$AUDITDCONF"
then
        sed -i 's/action_mail_acct.*/action_mail_acct = root/g' "$AUDITDCONF"
        echo "action_mail_acct is set to root..."
else
        echo "action_mail_acct = root" >> "$AUDITDCONF"
        echo "action_mail_acct is set to root..."
fi

# Auditd flush
if grep -q ^flush "$AUDITDCONF"
then
        echo "flush already exist..."
        sed -i 's/flush.*/flush = data/g' "$AUDITDCONF"
        echo "Default: flush = data..."
else
        echo "flush = data" >> "$AUDITDCONF"
        echo "Default: flush = data..."
fi

# Auditd Configuration end... (OK)
################################################################################
# Auditd Rules... (OK)

echo "---------- Section 6.3 - Auditd Rules ----------"

echo "Configuring $AUDITRULES file..."
echo -e "
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## Set failure mode to syslog
-f 2

# audit_time_rules - Record attempts to alter time through adjtime
-a always,exit -F arch=b64 -S adjtimex -k audit_time_rules

# audit_time_rules - Record attempts to alter time through settimeofday
-a always,exit -F arch=b64 -S settimeofday -k audit_time_rules

# audit_time_rules - Record Attempts to Alter Time Through stime
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime -k audit_time_rules

# audit_time_rules - Record Attempts to Alter Time Through clock_settime
-a always,exit -F arch=b64 -S clock_settime -k audit_time_rules

# Record Attempts to Alter the localtime File
-w /etc/localtime -p wa -k audit_time_rules

# Record Events that Modify User/Group Information
# audit_account_changes
-w /etc/group -p wa -k audit_account_changes
-w /etc/passwd -p wa -k audit_account_changes
```

```
-w /etc/gshadow -p wa -k audit_account_changes
-w /etc/shadow -p wa -k audit_account_changes
-w /etc/security/opasswd -p wa -k audit_account_changes

# Record Events that Modify the System's Network Environment
# audit_network_modifications
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k audit_network_modifications
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k audit_network_modifications
-w /etc/issue -p wa -k audit_network_modifications
-w /etc/issue.net -p wa -k audit_network_modifications
-w /etc/hosts -p wa -k audit_network_modifications
-w /etc/sysconfig/network -p wa -k audit_network_modifications

#Record Events that Modify the System's Mandatory Access Controls
-w /etc/selinux/ -p wa -k MAC-policy

#Record Events that Modify the System's Discretionary Access Controls - chmod
-a always,exit -F arch=b32 -S chmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chmod  -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - chown
-a always,exit -F arch=b32 -S chown -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchmod
-a always,exit -F arch=b32 -S fchmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchmodat
-a always,exit -F arch=b32 -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fchown
-a always,exit -F arch=b32 -S fchown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fsetxattr
-a always,exit -F arch=b32 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - lchown
-a always,exit -F arch=b32 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - lremovexattr
-a always,exit -F arch=b32 -S lremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fremovexattr
-a always,exit -F arch=b32 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - fsetxattr
-a always,exit -F arch=b32 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - removexattr
-a always,exit -F arch=b32 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Events that Modify the System's Discretionary Access Controls - setxattr
-a always,exit -F arch=b32 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod

#Record Attempts to Alter Logon and Logout Events
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
```

```
#Record Attempts to Alter Process and Session Initiation Information
-w /var/run/utmp -p wa -k session
-w /var/log/btmp -p wa -k session
-w /var/log/wtmp -p wa -k session

#Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-
EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-
EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-
EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-
EPERM -F auid>=500 -F auid!=4294967295 -k access

#Ensure auditd Collects Information on the Use of Privileged Commands
#
#  Find setuid / setgid programs then modify and uncomment the line below.
#
##  sudo find / -xdev -type f -perm -4000 -o -perm -2000 2>/dev/null
#
# -a always,exit -F path=SETUID_PROG_PATH -F perm=x -F auid>=500 -F auid!=4294967295 -k privileged

#Ensure auditd Collects Information on Exporting to Media (successful)
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k export
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k export

#Ensure auditd Collects File Deletion Events by User
-a always,exit -F arch=b32 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F
auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F
auid!=4294967295 -k delete

#Ensure auditd Collects System Administrator Actions
-w /etc/sudoers -p wa -k actions

#Ensure auditd Collects Information on Kernel Module Loading and Unloading
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

-a always,exit -F arch=b32 -S init_module,finit_module,delete_module -F key=modules
-a always,exit -F arch=b64 -S init_module,finit_module,delete_module -F key=modules
-w /var/run/faillock -p wa -k logins
-a always,exit -F arch=b32 -S stime -F key=audit_time_rules
# -a always,exit -F arch=b32 -S settimeofday -F key=audit_time_rules
# -a always,exit -F arch=b64 -S settimeofday -F key=audit_time_rules
# -a always,exit -F arch=b32 -S adjtimex -F key=audit_time_rules
# -a always,exit -F arch=b64 -S adjtimex -F key=audit_time_rules
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod
```

```
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -F key=export
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -F key=export
-a always,exit -F arch=b32 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b64 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S rename -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S renameat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S renameat -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=unset -F key=delete
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=unset -F key=delete

#Make the auditd Configuration Immutable
-e 2
" >> "$AUDITRULES"

echo "Enable auditd service..."
systemctl enable auditd.service
systemctl start auditd.service

if [[ $VERBOSE == "Y" ]]; then
   systemctl status auditd.service --no-pager
   echo
fi

# Auditd Rules end... (OK)
################################################################################
# Enable Kernel Auditing... (OK)

# echo "---------- Section 6.4 - Enable Kernel Auditing ----------"
```

```
echo "Enable Kernel auditing..."
sed -i 's/^GRUB_CMDLINE_LINUX=.*/GRUB_CMDLINE_LINUX="audit=1"/' "$DEFAULTGRUB"
grub2-mkconfig -o /boot/grub2/grub.cfg

# Enable Kernel Auditing end... (OK)
################################################################################

echo "---------- Chapter 6 - Completed ----------"

# Chapter 6 end...(OK)
################################################################################
# Chapter 7...(OK)

echo "---------- Chapter 7 - Software Integrity Checking ----------"

################################################################################
# Advanced Intrusion Detection Environment... (OK)

echo "---------- Section 7.1 - Advanced Intrusion Detection Environment ----------"

echo "Installing AIDE..."
$APT install aide && /usr/sbin/aide --init && cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz &&
/usr/sbin/aide --check && bind ^C stuff ^C
echo "AIDE is installed..."
echo "05 4 * * * root /usr/sbin/aide --check" >> /etc/crontab
echo "Configured periodic execution of AIDE, runs every morning at 04:30"

# Advanced Intrusion Detection Environment end... (OK)
################################################################################

echo "---------- Chapter 7 - Completed ----------"

# Chapter 7 end...(OK)
################################################################################
# Chapter 8...(OK)

echo "---------- Chapter 8 - Logging ----------"

################################################################################
# Logwatch...(OK)

echo "---------- Section 8.1 - Logwatch ----------"

echo "Installing logwatch package..."
$APT install logwatch

# Logwatch end...(OK)
################################################################################

echo "---------- Chapter 8 - Completed ----------"

# Chapter 8 end...(OK)
################################################################################
# Chapter 9...(OK)

echo "---------- Chapter 9 - Security Software ----------"

################################################################################
# Malware Scanners ...(OK)

echo "---------- Section 9.1 - Malware Scanners ----------"

echo "Installing malware scanners..."
for pack in rkhunter clamav clamav-update clamd; do
   echo "Installing $pack package..."
   $APT install "$pack"
done
```

```
echo "Checking and configuring rootkit hunter..."
rkhunter --update
rkhunter --propupd
sed -i 's/ALLOW_SSH_ROOT_USER=.*/ALLOW_SSH_ROOT_USER=no/g' "$RKHUNTERCONF"

echo "Checking and configuring CLAMAV..."
setsebool -P antivirus_can_scan_system 1
freshclam -v
sed -i 's/#LocalSocket \/run/LocalSocket \/run/g' /etc/clamd.d/scan.conf
sed -i 's/scanner (%i) daemon/scanner daemon/g' /usr/lib/systemd/system/clamd@.service
sed -i 's/\/etc\/clamd.d\/%i.conf/\/etc\/clamd.d\/scan.conf/g' /usr/lib/systemd/system/clamd@.service

systemctl enable clamav-freshclam.service
systemctl start clamav-freshclam.service
if [[ $VERBOSE == "Y" ]]; then
   systemctl status clamav-freshclam.service --no-pager
   echo
fi

# Malware Scanners end...(OK)
################################################################################

echo "---------- Chapter 9 - Completed ----------"

# Chapter 9 end...(OK)
################################################################################
# Chapter 10...(OK)

echo "---------- Chapter 10 - Process Accounting ----------"

################################################################################################################
#######
# Process Accounting...(OK)

echo "---------- Section 10.1 - Process Accounting ----------"

echo "Installing psacct package..."
$APT install psacct
systemctl enable psacct.service
systemctl start psacct.service
if [[ $VERBOSE == "Y" ]]; then
   systemctl status psacct.service --no-pager
   echo
fi

# Process Accounting end...(OK)
################################################################################

echo "---------- Chapter 10 - Completed ----------"

# Chapter 10 end...(OK)
################################################################################

echo "---------- Hardening the system settings - Complete ----------"
echo "---------- Let's install and harden other services... ----------"

################################################################################
# Configuring SSHD Server... (OK)

echo "Configuring SSHD server..."
echo "$SSHDFILE file location..."

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

cat > "$SSHDFILE" <<EOF
# SSH port.
```

```
Port 22

# Listen on IPv4 only.
ListenAddress 0.0.0.0

# Protocol version 1 has been exposed.
Protocol 2

#
# OpenSSH cipher-related release notes.
# OpenSSH 6.2: added support for AES-GCM authenticated encryption.
# The cipher is available as aes128-gcm@openssh.com and aes256-gcm@openssh.com.
# OpenSSH 6.5: added new cipher chacha20-poly1305@openssh.com.
# OpenSSH 6.7: removed unsafe algorithms. CBC ciphers are disabled by default:
# aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, cast128-cbc.
# OpenSSH 6.9: promoted chacha20-poly1305@openssh.com to be the default cipher.
#
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc

#
# OpenSSH 6.2: added support for the UMAC-128 MAC as umac-128@openssh.com
# and umac-128-etm@openssh.com. The latter being an encrypt-then-mac mode.
# Do not use umac-64 or umac-64-etm because of a small 64 bit tag size.
# Do not use any SHA1 (e.g. hmac-sha1, hmac-sha1-etm@openssh.com) MACs
# because of a weak hashing algorithm.
MACs hmac-sha2-512,hmac-sha2-256

#
# OpenSSH 6.5: added support for ssh-ed25519. It offers better security
# than ECDSA and DSA.
# OpenSSH 7.0: disabled support for ssh-dss.
# OpenSSH 7.2: added support for rsa-sha2-512 and rsa-sha2-256.
#
HostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-
v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com

#
# OpenSSH 6.5: added support for key exchange using elliptic-curve
# Diffie Hellman in Daniel Bernstein's Curve25519.
# OpenSSH 7.3: added support for diffie-hellman-group14-sha256,
# diffie-hellman-group16-sha512 and diffie-hellman-group18-sha512.
#
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group18-sha512,diffie-hellman-group16-
sha512,diffie-hellman-group14-sha256

# HostKeys for protocol version 2.
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Disabled because uses a small 1024 bit key.
#HostKey /etc/ssh/ssh_host_dsa_key

# Disabled because uses weak elliptic curves.
# See: https://safecurves.cr.yp.to/
#HostKey /etc/ssh/ssh_host_ecdsa_key


# INFO is a basic logging level that will capture user login/logout activity.
# DEBUG logging level is not recommended for production servers.
LogLevel INFO

# Disconnect if no successful login is made in 60 seconds.
LoginGraceTime 60

# Do not permit root logins via SSH.
PermitRootLogin no
```

```
# Check file modes and ownership of the user's files before login.
StrictModes yes

# Close TCP socket after 2 invalid login attempts.
MaxAuthTries 2

# The maximum number of sessions per network connection.
MaxSessions 3

# User/group permissions.
AllowGroups
DenyUsers root
DenyGroups root

# Password and public key authentications.
PasswordAuthentication yes
PermitEmptyPasswords no
PubkeyAuthentication no
AuthorizedKeysFile  .ssh/authorized_keys

# Disable unused authentications mechanisms.
ChallengeResponseAuthentication no
KerberosAuthentication no
GSSAPIAuthentication no
HostbasedAuthentication no
IgnoreUserKnownHosts yes

# Disable insecure access via rhosts files.
IgnoreRhosts yes

AllowAgentForwarding no
AllowTcpForwarding no

# Disable X Forwarding.
X11Forwarding no

# Disable message of the day but print last log.
PrintMotd yes
PrintLastLog yes

# Show banner.
Banner /etc/issue

# Do not send TCP keepalive messages.
TCPKeepAlive no

# Prevent users from potentially bypassing some access restrictions.
PermitUserEnvironment no

# Disable compression.
Compression no

# Disconnect the client if no activity has been detected for 900 seconds.
ClientAliveInterval 300
ClientAliveCountMax 0

# Do not look up the remote hostname.
UseDNS no

UsePAM yes
EOF

systemctl restart sshd.service

if [[ $VERBOSE == "Y" ]]; then
   systemctl status sshd.service --no-pager
```

```
    echo
fi

# Configuring SSHD Server... (OK)
################################################################################
# Network Time Protocol through chronyd.service...(OK)

cat > /etc/sysconfig/chronyd <<EOF
OPTIONS="-u chrony"
EOF

echo "Enabling chronyd.service..."
systemctl enable chronyd.service

if [[ $VERBOSE == "Y" ]]; then
    systemctl status chronyd.service --no-pager
    echo
fi

# Network Time Protocol through chronyd.service end...(OK)
################################################################################
# Disable X Windows Startup...(OK)

echo "Disabling X Windows startup..."
if [[ $GUI == "N" ]]; then
    echo "GUI is set to NO. Disabling X Windows Startup..."
    systemctl set-default multi-user.target
else
    echo "GUI is set to YES.Skipping..."
fi

# Disable X Windows Startup end...(OK)
################################################################################
# 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 [[ -f /etc/hosts.equiv ]]; then
    rm /etc/hosts.equiv
fi

# Secure user and services host files end...(OK)
################################################################################
# Fail2Ban...(OK)

echo "Enable fail2ban..."

$APT install fail2ban
systemctl enable fail2ban
systemctl start fail2ban

if [[ $VERBOSE == "Y" ]]; then
    systemctl status fail2ban --no-pager
    echo
fi

# Fail2Ban end...(OK)
################################################################################


echo "---------- Installation and hardening of other services - Complete ----------"

################################################################################
```

```
# Installing Modules and Apache for CentOS...(OK)

echo "---------- At last let's install, configure and secure Apache Web Server ----------"

for pack in $PACKAGES; do
   echo "Installing $pack package..."
   $APT install "$pack"
done

chown apache:apache -R /var/www/html
chmod -R 511 /var/www/html
restorecon -r /var/www/html

echo "Installing mod_evasive..."
$APT install mod_evasive

echo "Configuring $APACHE2DFILE ..."
cat > "$APACHE2DFILE" <<EOF
ServerRoot "/etc/httpd"

Listen 80

Include conf.modules.d/*.conf

User apache
Group apache

ServerAdmin root@localhost

<Directory />
   AllowOverride none
   Require all denied
</Directory>


DocumentRoot "/var/www/html"

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

<IfModule dir_module>
   DirectoryIndex index.html
</IfModule>

<Files ".ht*">
   Require all denied
</Files>


<IfModule mime_module>
   #
   # TypesConfig points to the file containing the list of mappings from
   # filename extension to MIME-type.
   #
   TypesConfig /etc/mime.types

   #
   # AddType allows you to add to or override the MIME configuration
   # file specified in TypesConfig for specific file types.
   #
   #AddType application/x-gzip .tgz
   #
```

```
    # AddEncoding allows you to have certain browsers uncompress
    # information on the fly. Note: Not all browsers support this.
    #
    #AddEncoding x-compress .Z
    #AddEncoding x-gzip .gz .tgz
    #
    # If the AddEncoding directives above are commented-out, then you
    # probably should define those extensions to indicate media types:
    #
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz

    #
    # AddHandler allows you to map certain file extensions to "handlers":
    # actions unrelated to filetype. These can be either built into the server
    # or added with the Action directive (see below)
    #
    # To use CGI scripts outside of ScriptAliased directories:
    # (You will also need to add "ExecCGI" to the "Options" directive.)
    #
    #AddHandler cgi-script .cgi

    # For type maps (negotiated resources):
    #AddHandler type-map var

    #
    # Filters allow you to process content before it is sent to the client.
    #
    # To parse .shtml files for server-side includes (SSI):
    # (You will also need to add "Includes" to the "Options" directive.)
    #
    AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>

AddDefaultCharset UTF-8

<IfModule mime_magic_module>
    #
    # The mod_mime_magic module allows the server to use various hints from the
    # contents of the file itself to determine its type.  The MIMEMagicFile
    # directive tells the module where the hint definitions are located.
    #
    MIMEMagicFile conf/magic
</IfModule>

<IfModule mod_headers.c>
    Header set X-XSS-Protection "1; mode=block"
    Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
</IfModule>

IncludeOptional conf.d/*.conf

ServerSignature Off
ServerTokens Prod
FileETag None
TraceEnable Off
Header always append X-Frame-Options SAMEORIGIN
Timeout 30
EOF


echo "Configuring Mod Security..."

$APT install mod_security

mkdir /etc/httpd/crs
```

```
cd /etc/httpd/crs
wget https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master
tar -xvf master
mv SpiderLabs-owasp-modsecurity-crs-* owasp-modsecurity-crs
cd /etc/httpd/crs/owasp-modsecurity-crs/
cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_setup.conf

touch /etc/httpd/modsecurity.d/mod_security.conf

cat > /etc/httpd/modsecurity.d/mod_security.conf <<EOF
<IfModule mod_security2.c>
   SecRuleEngine On
   SecStatusEngine On
   SecRequestBodyAccess On
   SecResponseBodyAccess On
   SecResponseBodyMimeType text/plain text/html text/xml application/octet-stream
   SecDataDir /tmp
   SecRule RESPONSE_STATUS "@streq 408" "phase:5,t:none,nolog,pass,setvar:ip.slow_dos_counter=+1,
expirevar:ip.slow_dos_counter=60, id:'1234123456'"
   SecRule IP:SLOW_DOS_COUNTER "@gt 5" "phase:1,t:none,log,drop,msg:'Client Connection Dropped due to
high number of slow DoS alerts', id:'1234123457'"
</IfModule>
EOF

echo "Configuring Mod Evasive..."

mkdir /var/log/mod_evasive
chown apache:apache /var/log/mod_evasive/

cat > /etc/httpd/conf.d/mod_evasive.conf <<EOF
LoadModule evasive20_module modules/mod_evasive24.so

<IfModule mod_evasive24.c>
  DOSHashTableSize 3097
  DOSPageCount  2
  DOSSiteCount  50
  DOSPageInterval 1
  DOSSiteInterval  1
  DOSBlockingPeriod  600
  DOSLogDir   /var/log/mod_evasive
  DOSEmailNotify  root@localhost
</IfModule>
EOF

echo "Configuring Welcome..."

cat > /etc/httpd/conf.d/welcome.conf <<EOF
#
# This configuration file enables the default "Welcome" page if there
# is no default index page present for the root URL.  To disable the
# Welcome page, comment out all the lines below.
#
# NOTE: if this file is removed, it will be restored on upgrades.
#
<LocationMatch "^/+$">
   Options -Indexes
   ErrorDocument 403 /noindex/index.html
</LocationMatch>

<Directory /usr/share/httpd/noindex>
   Options MultiViews
   DirectoryIndex index.html

   AddLanguage en-US .en-US
   AddLanguage es-ES .es-ES
   AddLanguage zh-CN .zh-CN
   AddLanguage zh-HK .zh-HK
```

```
    AddLanguage zh-TW .zh-TW

    LanguagePriority en
    ForceLanguagePriority Fallback

    AllowOverride None
    Require all granted
</Directory>

Alias /noindex /usr/share/httpd/noindex
EOF

semanage fcontext --add -t httpd_sys_rw_content_t "/var/log/mod_evasive(/.*)?"
restorecon -r /var/log/mod_evasive

echo "Configuring QoS Module..."
touch /etc/httpd/conf.d/qos.conf

cat > /etc/httpd/conf.d/qos.conf <<EOF
<IfModule mod_qos.c>
    # handles connections from up to 100000 different IPs
    QS_ClientEntries 100000
    # will allow only 20 connections per IP
    QS_SrvMaxConnPerIP 20
    # disables keep-alive when 70% of the TCP connections are occupied:
    QS_SrvMaxConnClose      70%
   # minimum request/response speed (deny slow clients blocking the server, ie. slowloris keeping connections open
without requesting anything):
    QS_SrvMinDataRate       150 1200
    # and limit request header and body (carefull, that limits uploads and post requests too):
    # LimitRequestFields      30
    # QS_LimitRequestBody     102400
</IfModule>
EOF

echo "Restarting Apache HTTPD..."
systemctl restart httpd
systemctl enable httpd

if [[ $VERBOSE == "Y" ]]; then
    systemctl status httpd.service --no-pager
    httpd -M
    echo
fi

# Installing Modules and Apache for CentOS end...(OK)
################################################################################
# Ensure files ownership...(OK)

echo "Ensuring files ownership (user and group)..."
find / -ignore_readdir_race -nouser -print -exec chown root {} \;
find / -ignore_readdir_race -nogroup -print -exec chgrp root {} \;

# Ensure files ownership end...(OK)
################################################################################
# Ensure permissions on all logfiles are configured...(OK)

echo "Ensuring permissions on var/log directory..."
find /var/log -type f -exec chmod g-wx,o-rwx {} +

# Ensure permissions on all logfiles are configured end...(OK)
################################################################################
# Check systemd-delta...(OK)

if [[ $VERBOSE == "Y" ]]; then
    echo "Checking systemd-delta..."
    systemd-delta --no-pager
```

```
    echo
fi

# Check systemd-delta end...(OK)
################################################################################
# End of script file...(OK)

echo "The script finished executing..."
echo "Reboot is recommended!"

# End of script file end...(OK)
################################################################################
```

Εικόνα 70 - Πηγαίος κώδικας Bash Script

Κεφάλαιο 4ο – Αποτίμηση ασφάλειας

Αφού έχουμε εκτελέσει το παραπάνω Bash Script για την επαύξηση ασφάλειας του συστήματός μας, πρέπει να ελέγξουμε εάν οι καλύτερες πρακτικές έχουν εφαρμοστεί επιτυχώς. Για να γίνει αυτό, μπορούμε να χρησιμοποιήσουμε έτοιμα εργαλεία όπως το Nessus το οποίο είναι ένα πρόγραμμα σάρωσης για ευπάθειες, το OpenSCAP το οποίο ελέγχει ότι το σύστημά μας ακολουθεί πολιτικές σύμφωνα με πρότυπα ασφάλειας πληροφοριακών συστημάτων που έχουν αναρτηθεί από διάφορους οργανισμούς όπως το Center For Internet Security (CIS) και το Nmap το οποίο σαρώνει το σύστημα, βρίσκει ανοιχτές πόρτες και ελέγχει για ευπάθειες μέσω της μηχανής Script που διαθέτει.

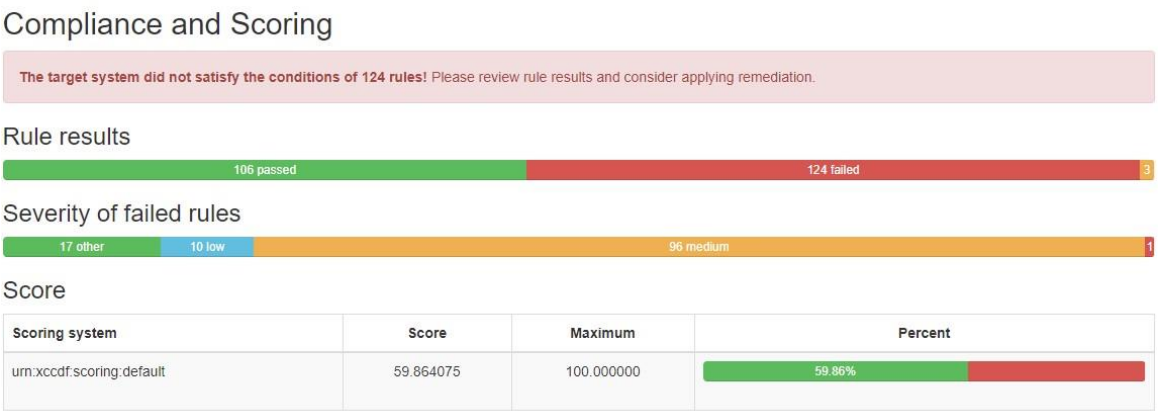
Τέλος, δεν ξεχνάμε να εκτελέσουμε επιθέσεις για τις οποίες εφαρμόσαμε αντίμετρα ώστε να διαπιστώσουμε εάν όντως λειτουργούν. Συνεπώς, θα γίνουν επιθέσεις HTTP Flood και Slowloris κατά του συστήματός μας.

4.1 OpenSCAP

Στο παρόν υποκεφάλαιο, επισυνάπτονται τα αποτελέσματα των ελέγχων που έγιναν μέσω του προγράμματος OpenSCAP με χρήση διαφορετικών προφίλ (σενάρια χρήσης του συστήματος).

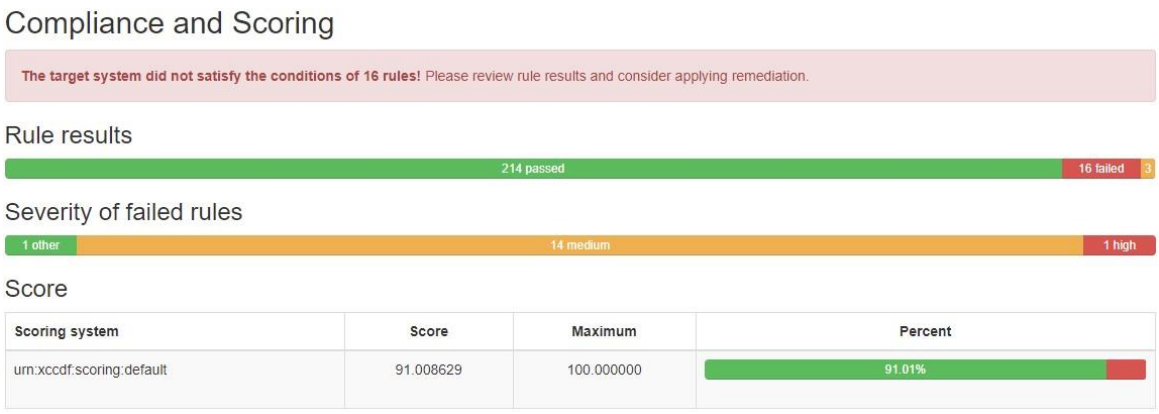
4.1.1 Προφίλ C2S (Commercial Cloud Services)

Πριν εφαρμοστεί το Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 71 - C2S Unhardened

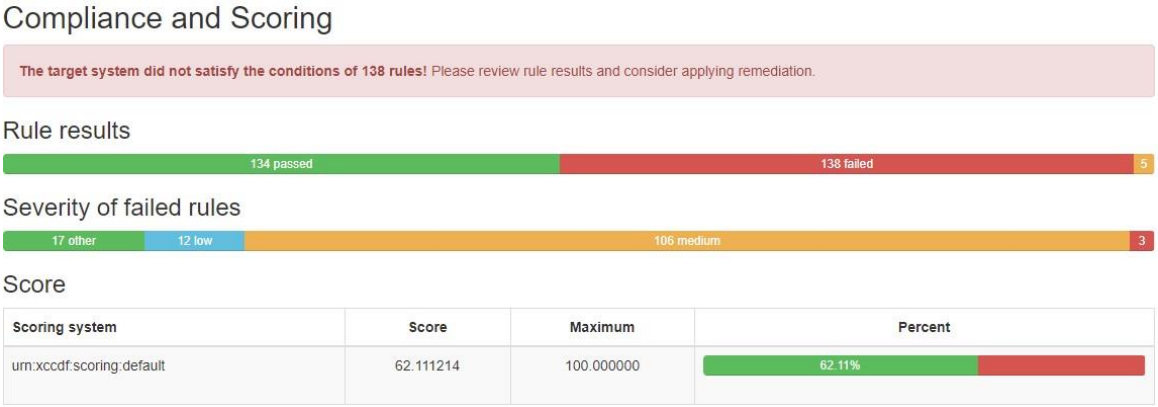
Μετά την εφαρμογή του Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 72 - C2S Hardened

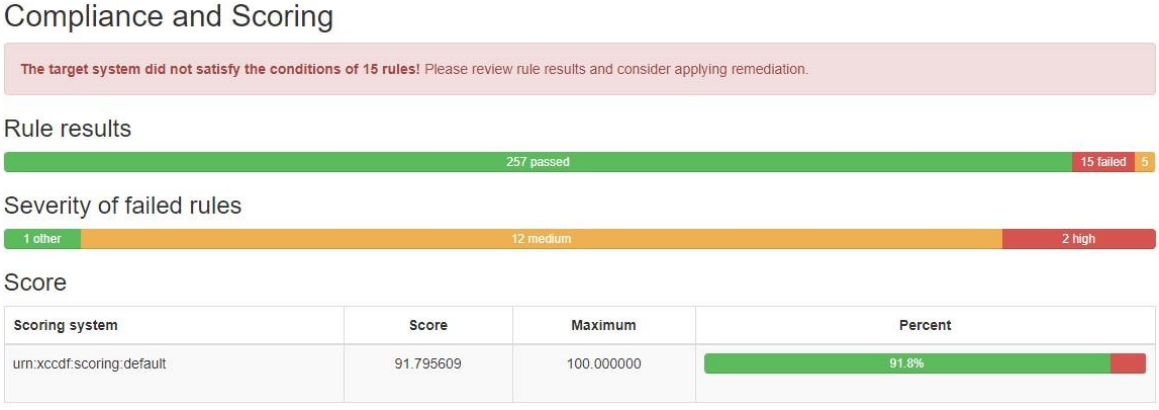
4.1.2 Προφίλ CIS (Center for Internet Security)

Πριν εφαρμοστεί το Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 73 - CIS Unhardened

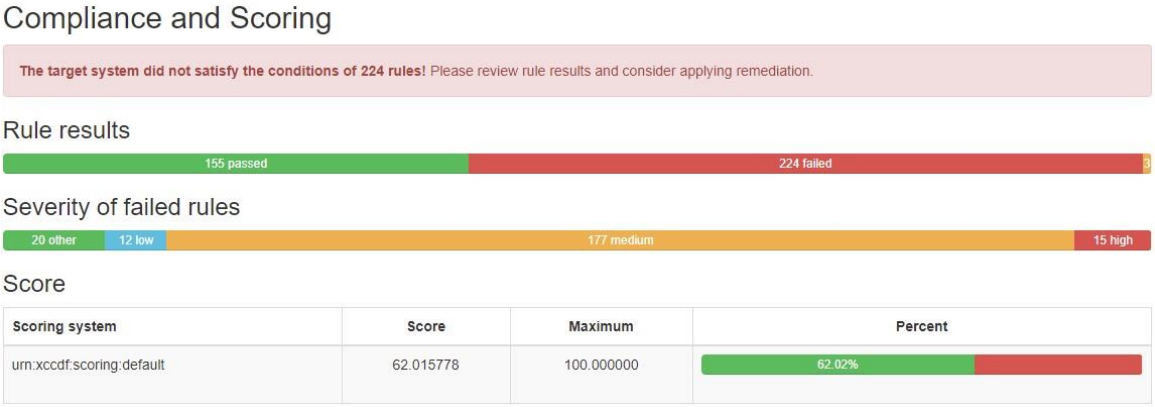
Μετά την εφαρμογή του Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 74 - CIS Hardened

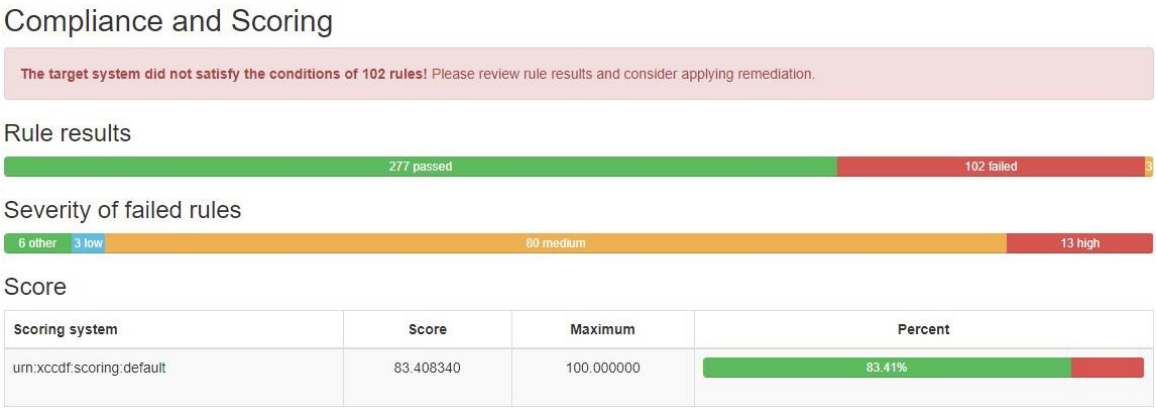
4.1.3 Προφίλ NIST (National Institute of Standards and Technology)

Πριν εφαρμοστεί το Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 75 - NIST Unhardened

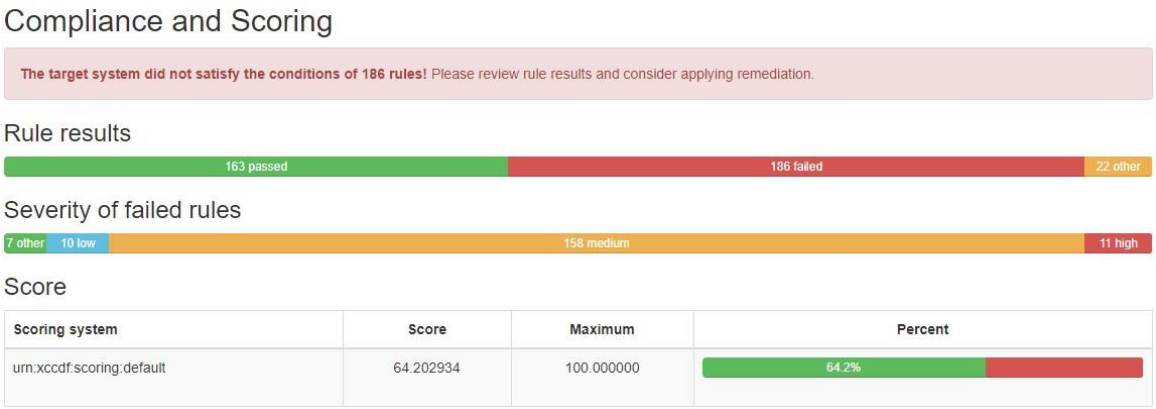
Μετά την εφαρμογή του Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 76 - NIST Hardened

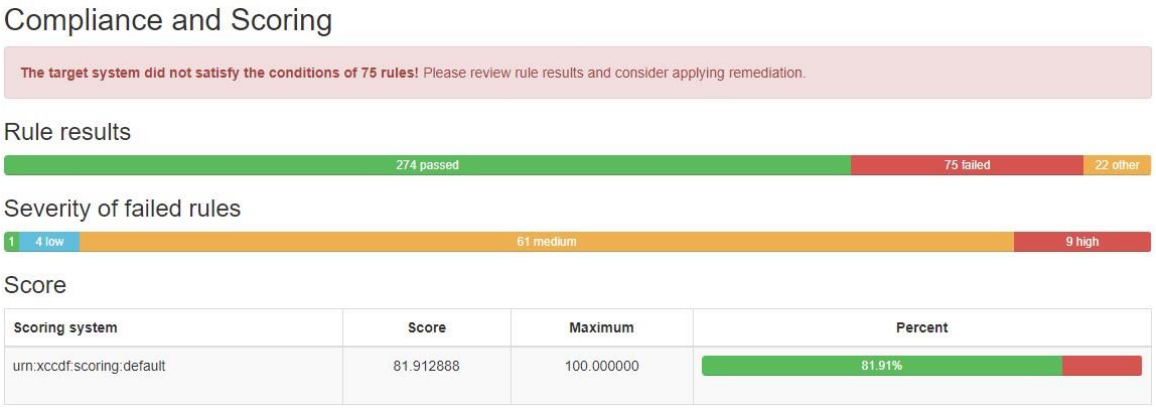
4.1.4 Προφίλ STIG (Security Technical Implementation Guides)

Πριν εφαρμοστεί το Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 77 - STIG Unhardened

Μετά την εφαρμογή του Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.



Εικόνα 78 - STIG Hardened

Η πλειοψηφία των ελέγχων που βγήκαν ως «αποτυχία» δεν χρειαζόταν να εφαρμοστούν στο σύστημά μας όπως για παράδειγμα το μπάνερ στο περιβάλλον GDM (Gnome Display Manager) καθώς δεν χρησιμοποιείται στο περιβάλλον εξυπηρετητή ιστού. Επίσης, γίνεται έλεγχος του περιεχομένου του μπάνερ ώστε να περιέχει συγκεκριμένο περιεχόμενο το οποίο δεν συμβάδιζε με το δικό μας.

4.2 Nessus

Στο παρόν υποκεφάλαιο, επισυνάπτονται τα αποτελέσματα των ελέγχων που έγιναν με το πρόγραμμα Nessus (Free έκδοση) και την εκτενή σάρωση (δείχνοντας και τα false alarms).

Πριν εφαρμοστεί το Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.

Εικόνα 79 - Nessus Extensive Unhardened

Μετά την εφαρμογή του Bash Script στο σύστημα έχουμε τα παρακάτω αποτελέσματα.

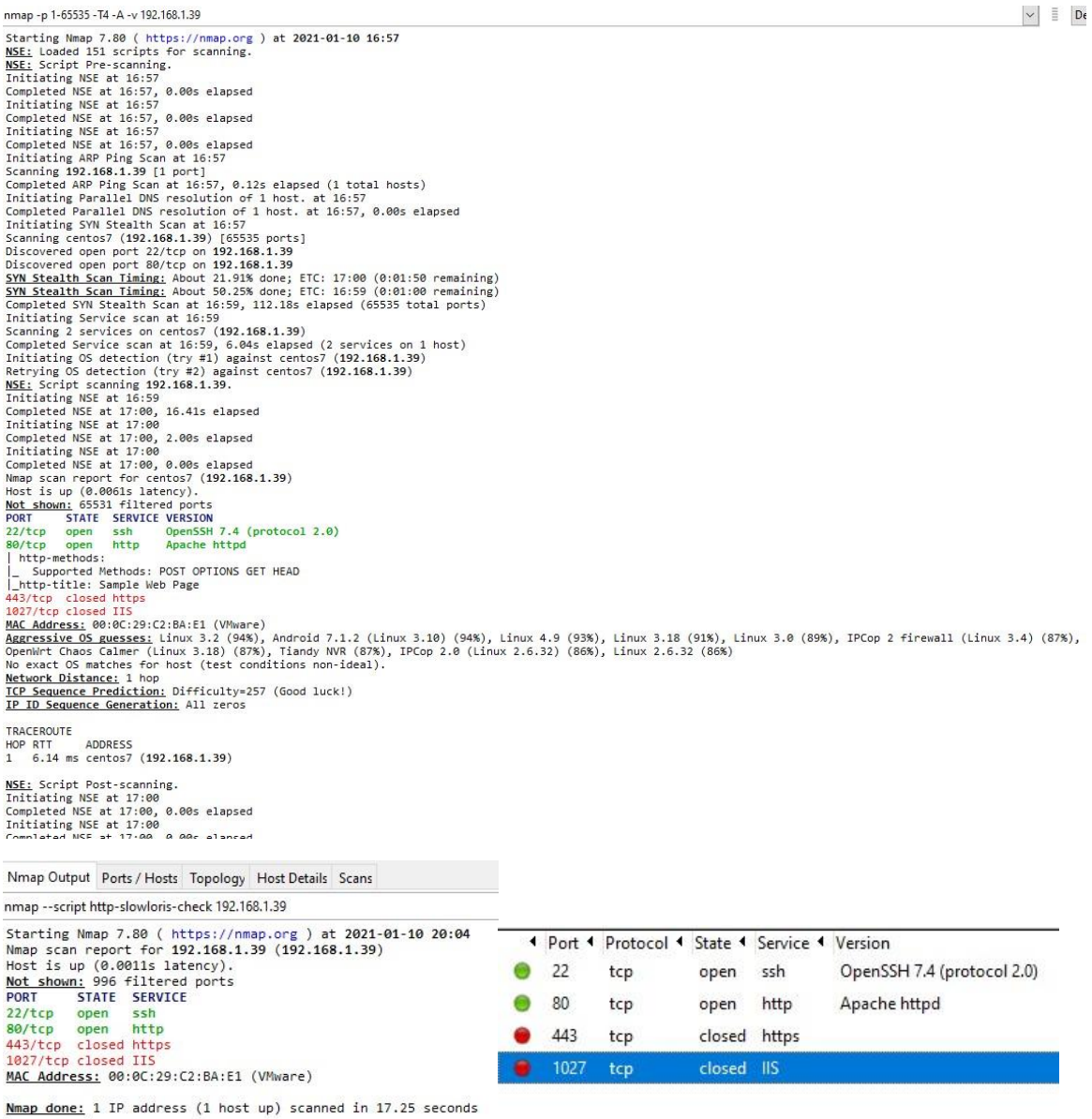
Εικόνα 80 - Nessus Extensive Hardened

Το Nessus στην σάρωση ανέφερε παλιά έκδοση του Apache (πακέτο httpd). Ωστόσο, λόγω του CentOS το πακέτο httpd γίνεται πλέον backported ώστε να εφαρμόζονται οι προστασίες έναντι καινούργιων CVEs. Συνεπώς, είναι ένα προσαρμοσμένο πακέτο και δεν αναγνωρίζεται σωστά από το Nessus. Για να βεβαιωθούμε ότι ο Apache έχει το καινούργιο μέτρο προστασίας για κάποιο CVE που μας ενδιαφέρει εκτελούμε την παρακάτω εντολή και το ψάχνουμε στην λίστα των αλλαγών (changelog).

```
sudo rpm -q –changelog httpd
```

4.3 Nmap

Στο παρόν υποκεφάλαιο, επισυνάπτονται τα αποτελέσματα των σαρώσεων που έγινε με το πρόγραμμα Nmap.



Εικόνα 81 - Nmap από Windows

Έγινε παρόμοια σάρωση με χρήση VM Kali Linux μέσω γραμμής εντολών.

```
Nmap done: 1 IP address (1 host up) scanned in 25.97 seconds
root@kali:~# nmap --script vuln 192.168.1.39
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-10 19:28 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for centos7 (192.168.1.39)
Host is up (0.00039s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
MAC Address: 00:0C:29:C2:BA:E1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 61.92 seconds
root@kali:~# nmap --script vuln 192.168.1.39
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-10 19:32 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.03% done; ETC: 19:33 (0:00:00 remaining)
Nmap scan report for centos7 (192.168.1.39)
Host is up (0.00039s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open   http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp  closed https
1027/tcp closed IIS
MAC Address: 00:0C:29:C2:BA:E1 (VMware)
```

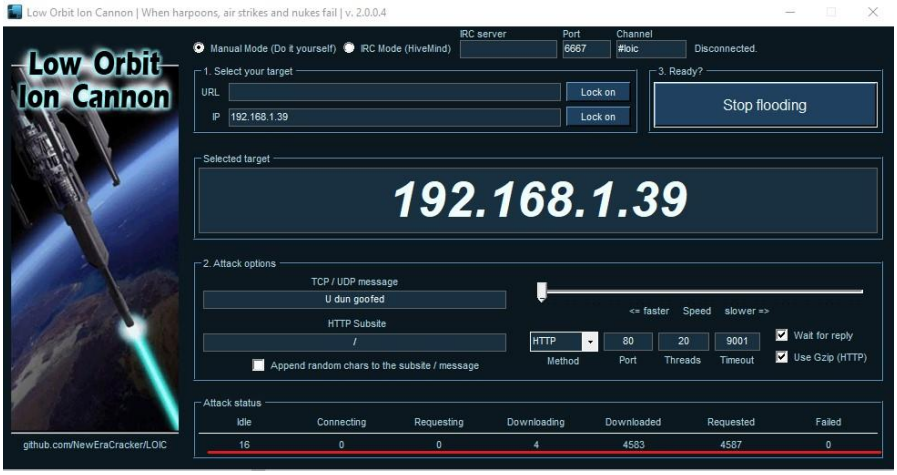
Εικόνα 82 - Nmap από Kali Linux

4.4 Επίθεση HTTP Flood

Για να διεξάγουμε μία επίθεση HTTP Flood χρησιμοποιήσαμε το πρόγραμμα LOIC (**L**ow **O**rbit **I**on **C**annon), ένα πρόγραμμα DoS επιθέσεων που έχει χρησιμοποιηθεί παλιότερα από κοινότητες όπως οι 4chan και από τους Anonymous.

Πριν περάσουμε στα αποτελέσματα, ας περιγράψουμε την αναμενόμενη συμπεριφορά του συστήματός μας έπειτα από την επαύξηση ασφάλειας. Η άμυνα που εφαρμόστηκε στο σύστημα χωρίζεται σε δύο στάδια. Το πρώτο στάδιο είναι η χρήση του ufw αναχώματος ασφάλειας που καταγράφει την κίνηση από διευθύνσεις IP και το ρυθμό αύξησης πακέτων. Εάν, αυτός ο ρυθμός είναι πολύ γρήγορος (μιλάμε πάντα για «νόμιμα» HTTP Requests και όχι την περίπτωση Slowloris) η κίνηση αποκόπτεται από το UFW. Επιπλέον, καταγράφεται και γίνεται blacklist η IP από το άρθρωμα mod_evasive. Σε περίπτωση εφαρμογής **μόνο** του Mod_evasive χωρίς την χρήση του ufw, εκτυπώνεται μήνυμα 403 Forbidden στο επιτιθέμενο (τα Requests φτάνουν στο σύστημα, αλλάζει το περιεχόμενο που επιστρέφει στον χρήστη).

Ακολουθεί η συμπεριφορά του συστήματός μας χωρίς κάποιο αντίμετρο ασφαλείας για επιθέσεις HTTP Flood με χρήση του LOIC.

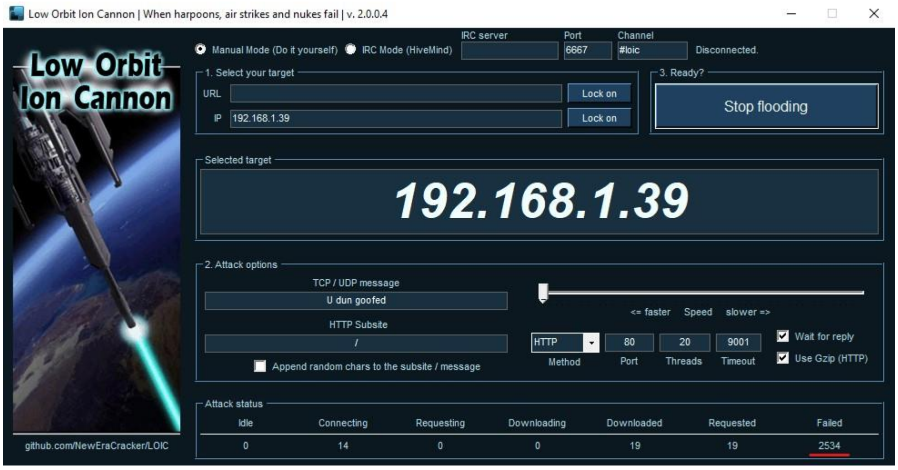


Εικόνα 83 – HTTP Flood Unhardened

Ελέγχουμε την εγκατάσταση του αρθρώματος mod_evasive.

```
[admin@centos7 Audit Scripts]$ perl modevasivetest.pl
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
```

Έπειτα διεξάγουμε ξανά επίθεση με το LOIC.




```
centos7.localdomain systemd[1]: Started The Apache HTTP Server.
centos7.localdomain mod_evasive[2078]: Blacklisting address 192.168.1.2: possible DoS attack.
```

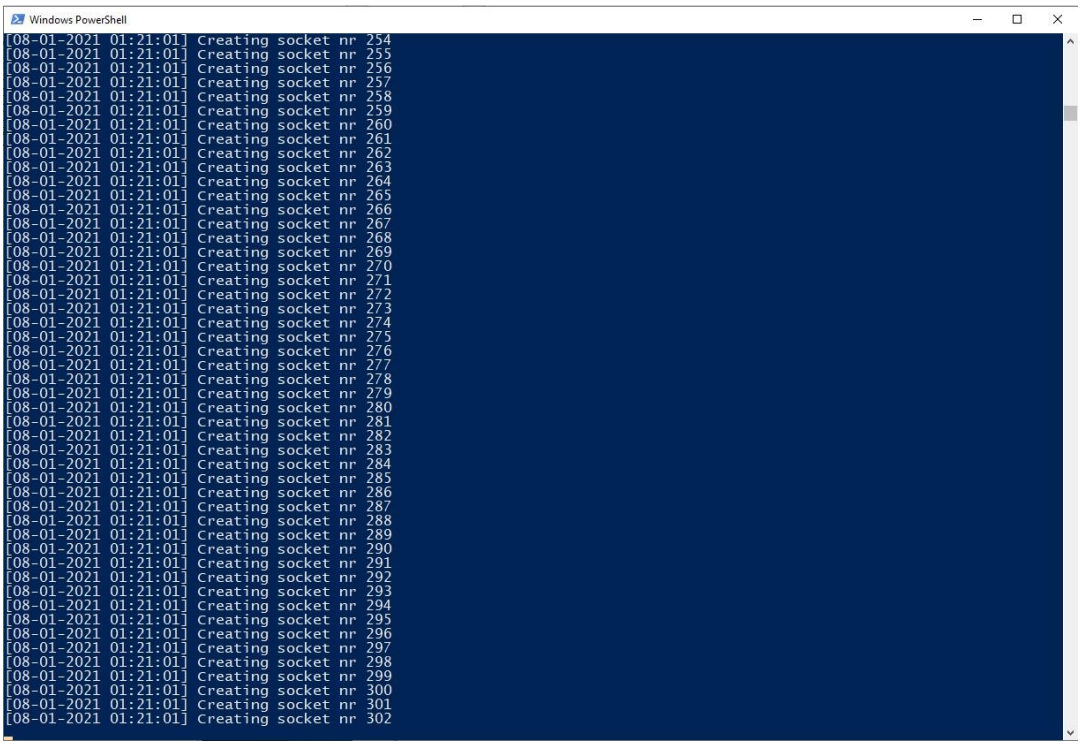
Εικόνα 84 - HTTP Hardened

4.5 Επιθέσεις Slowloris

Για την διεξαγωγή επιθέσεων Slowloris χρησιμοποιήθηκε το Pyloris (Python Slowloris) καθώς και το SlowHTTPTest μέσω λειτουργικού Kali Linux.

4.5.1 Pyloris – Slowloris επίθεση

Όταν το σύστημά μας δεν έχει κάποιο αντίμετρο για την επίθεση Slowloris, το Pyloris δημιουργεί πολλά sockets εκμεταλλευόμενο την ευπάθεια του Apache και της κρατά ενεργοποιημένες. Σε περίπτωση που κάποιο απενεργοποιηθεί, τότε το πρόγραμμα δημιουργεί ένα καινούργιο στην θέση του. Αυτό έχει ως αποτέλεσμα να μην μπορούν να δημιουργηθούν sockets για νόμιμους χρήστες του συστήματος και έτσι η ιστοσελίδα δεν φορτώνει για αυτούς.



Εικόνα 85 - Pyloris Unhardened

Με την εφαρμογή των μέτρων προστασίας δεν αφήνουμε μία διεύθυνση IP να δημιουργήσει πάνω από 20 συνδέσεις ενώ αν κάποιος επιτιθέμενος έχει ένα εύρος από διαθέσιμες IP στην σειρά τότε ελέγχεται η κλάση C των IP και έπειτα από πολλές συνδέσεις της αποκόπτει. Συνεπώς, πρώτο μέτρο προστασίας που εφαρμόζεται είναι το ufw – ανάχωμα ασφάλειας.

```
Windows PowerShell
PS C:\Users\Kostas\Desktop\Ασκήσεις\Thesis\Resources\slowloris-master> python slowloris.py 192.168.1.39 -p 80 -s 500 -v
[08-01-2021 00:36:57] Attacking 192.168.1.39 with 500 sockets.
[08-01-2021 00:36:57] Creating sockets...
[08-01-2021 00:36:57] Creating socket nr 0
[08-01-2021 00:36:57] Creating socket nr 1
[08-01-2021 00:36:57] Creating socket nr 2
[08-01-2021 00:36:57] Creating socket nr 3
[08-01-2021 00:36:57] Creating socket nr 4
[08-01-2021 00:36:57] Creating socket nr 5
[08-01-2021 00:36:57] Creating socket nr 6
[08-01-2021 00:36:57] Creating socket nr 7
[08-01-2021 00:36:57] Creating socket nr 8
[08-01-2021 00:36:57] Creating socket nr 9
[08-01-2021 00:36:57] Creating socket nr 10
[08-01-2021 00:36:57] Creating socket nr 11
[08-01-2021 00:36:57] Creating socket nr 12
[08-01-2021 00:36:57] Creating socket nr 13
[08-01-2021 00:36:57] Creating socket nr 14
[08-01-2021 00:36:57] Creating socket nr 15
[08-01-2021 00:36:57] Creating socket nr 16
[08-01-2021 00:36:57] Creating socket nr 17
[08-01-2021 00:36:57] Creating socket nr 18
[08-01-2021 00:36:57] Creating socket nr 19
[08-01-2021 00:37:01] timed out
[08-01-2021 00:37:01] Sending keep-alive headers... Socket count: 19
[08-01-2021 00:37:01] Recreating socket...
[08-01-2021 00:37:05] timed out
[08-01-2021 00:37:05] Sleeping for 10 seconds
```

Εικόνα 86 - Pyloris Hardened

Επιπλέον, δοκιμάστηκε επίθεση Slowloris χωρίς την χρήση των κανόνων ufw. Το mod_qos σταμάτησε την επίθεση με αποτέλεσμα το Pyloris απλά να προσπαθεί μάταια να δημιουργήσει ξανά τα sockets (Recreating socket…)

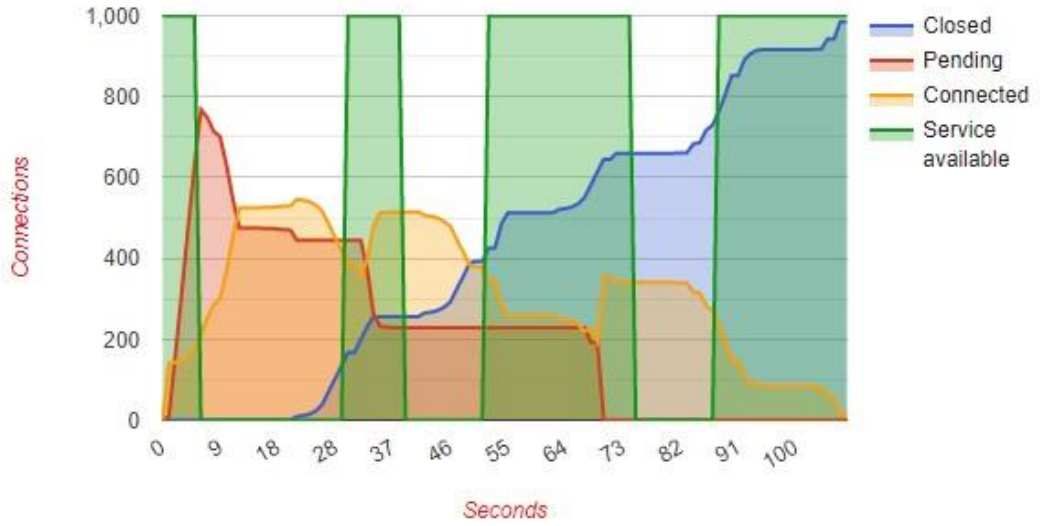
Έλεγχος στα αρχεία καταγραφής του Apache έδειχνε τα ακόλουθα μηνύματα.

```
[Thu May 27 09:54:53.762370 2021] [qos:error] [pid 3767] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.763030 2021] [qos:error] [pid 3768] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.773642 2021] [qos:error] [pid 3776] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.783922 2021] [qSos:error] [pid 3784] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21,
c=192.168.1.2
[Thu May 27 09:54:53.794259 2021] [qos:error] [pid 3762] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.804713 2021] [qos:error] [pid 3781] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.815125 2021] [qos:error] [pid 3767] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.815820 2021] [qos:error] [pid 3768] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.826200 2021] [qos:error] [pid 3776] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.836593 2021] [qos:error] [pid 3784] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.837303 2021] [qos:error] [pid 3762] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.847831 2021] [qos:error] [pid 3781] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.848356 2021] [qos:error] [pid 3767] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.859043 2021] [qos:error] [pid 3768] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.869395 2021] [qos:error] [pid 3776] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.870175 2021] [qos:error] [pid 3784] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, c=192.168.1.2
[Thu May 27 09:54:53.918675 2021] [qos:error] [pid 3781] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:53.957365 2021] [qos:error] [pid 3768] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:53.987861 2021] [qos:error] [pid 3784] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:54.037243 2021] [qos:error] [pid 3781] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:54.161202 2021] [qos:error] [pid 3768] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:54.169812 2021] [qos:error] [pid 3776] mod_qos(031): access denied, QS_SrvMaxConnPerIP rule: max=20, concurrent connections=21, message
repeated 20 times, c=192.168.1.2
[Thu May 27 09:54:54.710799 2021] [qos:error] [pid 3783] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:54.736976 2021] [qos:error] [pid 3771] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=226, this connection=37, c=192.168.1.2
[Thu May 27 09:54:54.737205 2021] [qos:error] [pid 3772] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=226, this connection=37, c=192.168.1.2
[Thu May 27 09:54:54.738746 2021] [qos:error] [pid 3770] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=226, this connection=37, c=192.168.1.2
[Thu May 27 09:54:55.433597 2021] [qos:error] [pid 1932] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:55.628353 2021] [qos:error] [pid 3753] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:55.628538 2021] [qos:error] [pid 3756] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:55.628544 2021] [qos:error] [pid 3757] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:55.640543 2021] [qos:error] [pid 3754] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=230, this connection=37, c=192.168.1.2
[Thu May 27 09:54:56.438371 2021] [qos:error] [pid 1936] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=210, this connection=37, c=192.168.1.2
[Thu May 27 09:54:56.628729 2021] [qos:error] [pid 3758] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=210, this connection=37, c=192.168.1.2
[Thu May 27 09:54:57.436853 2021] [qos:error] [pid 1933] mod_qos(034): access denied, QS_SrvMinDataRate rule (in): min=194, this connection=37, c=192.168.1.2
```

Εικόνα 87 - mod_qos Slowloris

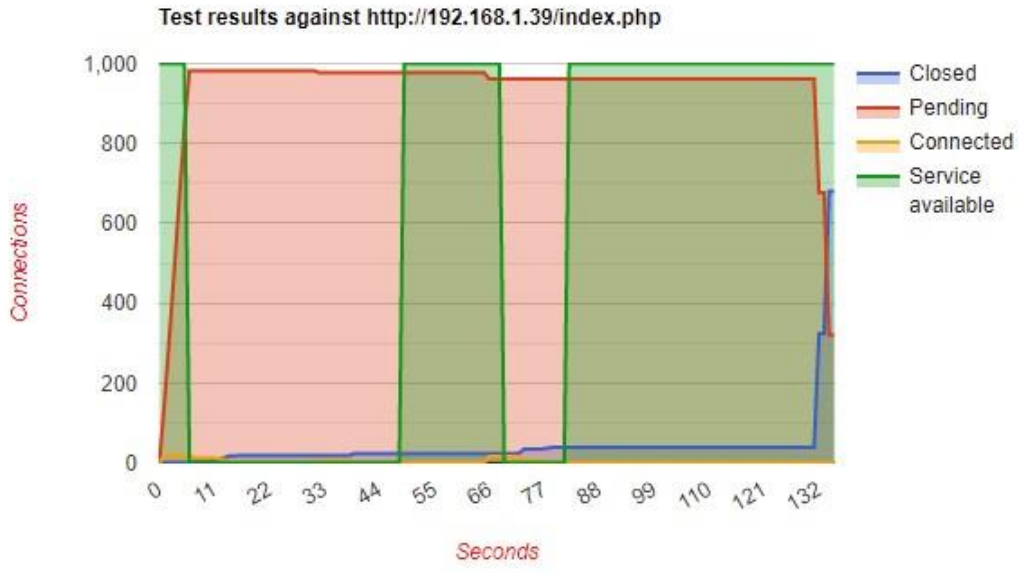
4.5.2 SlowHTTPTest – Kali Linux

Το SlowHTTPTest χρησιμοποιήθηκε κατά κύριο λόγο για την γραφική αναπαράσταση της επίθεσης Slowloris. Όπως είναι φανερό, χωρίς μέτρα προστασίας, ένας χρήστης μπορεί να δημιουργήσει πολλές συνδέσεις και να της κρατήσει ανοιχτές αποκόπτοντας τους άλλους χρήστες.



Εικόνα 88 - SlowHTTPTest Unhardened

Έπειτα από την εφαρμογή των μέτρων, βλέπουμε πως δημιουργούνται λίγες συνδέσεις και οι άλλες βρίσκονται σε αναμονή. Ο επιτιθέμενος, βλέπει ότι έχουν κοπεί οι υπηρεσίες του στόχου ωστόσο, αυτό ισχύει μόνο για την δικιά του διεύθυνση IP. Η κίνηση νόμιμων χρηστών προς το σύστημα, συνεχίζει κανονικά.



Εικόνα 89 - SlowHTTPTest Hardened

Οι αναφορές που δημιουργήθηκαν από όλα τα παραπάνω προγράμματα μπορούν να βρεθούν στο σύνδεσμο του GitHub για περαιτέρω εξέταση καθώς και στο παρακάτω σύνδεσμο Google Drive.

https://github.com/Kostas-Galanomatis/CentOS_7_Hardening_Script

https://drive.google.com/drive/folders/1cl-vm2OQHs1TN53VkRin3JZLYRoPGB1i?usp=sharing

Κεφάλαιο 5ο – Συμπεράσματα

Ακολουθώντας τον παραπάνω οδηγό των καλύτερων πρακτικών ήμασταν σε θέση να τις εφαρμόσουμε στο λειτουργικό σύστημα του CentOS ώστε να πληροί πολιτικές που απαιτούν οργανισμοί πιστοποίησης ασφάλειας των πληροφοριακών συστημάτων. Επιπλέον, εφαρμόστηκαν αντίμετρα για επιθέσεις που αφορούν το πρωτόκολλο HTTP όπως η επίθεση HTTP Flood και η DoS Slowloris.

Το παραδοτέο Script μπορεί να τροποποιηθεί ώστε να καλύψει και άλλες ανάγκες διαφορετικών σεναρίων χρήσης του συστήματος ή πιο αυστηρές πολιτικές της ίδιας χρήσης που μελετήσαμε (εξυπηρετητής ιστού). Κάποιοι παράμετροι που εφαρμόζει το Script μπαίνουν αυτούσια, συνεπώς εάν εφαρμοστεί σε ένα υπάρχον σύστημα το οποίο είναι στην «παραγωγή» μπορεί να αλλάξει σημαντικά τον τρόπο λειτουργίας του. Προτείνεται η χρήση του σε περιβάλλον Sandbox και έπειτα από έλεγχο ορθής λειτουργίας του συστήματος, η μετάβαση στο «παραγωγικό» περιβάλλον.

Βιβλιογραφία - Πηγές

1. https://github.com/dpolitis/Ubuntu-Xenial-Security
2. https://highon.coffee/blog/security-harden-centos-7/
3. https://www.lisenet.com/2017/centos-7-server-hardening-guide/
4. https://geekflare.com/apache-web-server-hardening-security/
5. https://www.tecmint.com/centos-7-hardening-and-security-guide/
6. https://secscan.acron.pl/centos7/start
7. https://www.cisecurity.org/
8. https://www.open-scap.org/
9. https://www.tecmint.com/protect-apache-using-mod_security-and-mod_evasive-on-rhel-centos-fedora/
10. http://blog.lavoie.sl/2012/09/protect-webserver-against-dos-attacks.html
11. https://www.nist.gov/
12. https://www.howtoforge.com/how-to-defend-slowloris-ddos-with-mod_qos-apache2-on-debian-lenny
13. https://www.thegeeksearch.com/how-to-use-advanced-intrusion-detection-environment-aide-to-monitor-changes-in-linux/
14. https://ep.gnt.md/index.php/how-to-configure-fail2ban-to-protect-ssh-and-apache/
15. https://www.tenable.com/products/nessus
16. https://nmap.org/book/man-port-scanning-techniques.html
17. https://github.com/shekyan/slowhttptest
18. https://ourcodeworld.com/articles/read/949/how-to-perform-a-dos-attack-slow-http-with-slowhttptest-test-your-server-slowloris-protection-in-kali-linux