



L I N U X S E R V E R H A R D E N I N G

I N T E R A C T I V E W O R K S H O P 2 1 - 0 3 - 2 0 2 3

FIREWALLS

- Τα firewalls είναι ένα προστατευτικό τείχος που φιλτράρει την κίνηση (εισερχόμενη και εξερχόμενη) σε έναν υπολογιστή
- Είναι υπεύθυνα για τις ανοιχτές θύρες, καθώς και τα πακέτα τα οποία επιτρέπουν να φτάσουν σε ένα μηχάνημα.
- Το UFW, είναι μία πολύ απλή διεπαφή διαχείρισης firewall, η οποία αφαιρεί πολλά από τα πολύπλοκα βήματα που θα είχαμε με άλλα χαμηλού-επιπέδου εργαλεία (βλ. Nftables).



IDENTITY ACCESS MANAGEMENT

- Κάθε χρήστης (ή ομάδα χρηστών) πρέπει να έχει πρόσβαση σε πόρους για να μπορεί να κάνει τη δουλειά του. Δεν πρέπει όμως να έχει περισσότερη πρόσβαση από αυτή που είναι απολύτως απαραίτητη.
- Οι χρήστες γίνονται authorize με διαφορετικά επίπεδα πρόσβασης ανάλογα με τον ρόλο τους, ώστε να αποφευχθούν προβλήματα ασφαλείας από άπειρους ή κακόβουλους χρήστες.
- Τα linux δίνουν τη δυνατότητα να χειριζόμαστε τα permissions για κάθε αρχείο, χρήστη ή ομάδα χρηστών, δίνοντας μας μεγάλη ευελιξία στην οργάνωση και διασφάλιση των αρχείων μας.



H A S H I N G

- Αλγόριθμοι κατακερματισμού, η βασική ιδέα
- Χρήση hash για authentication με κωδικούς και έλεγχο αλλαγών σε αρχεία



SERVICES, SCHEDULING

- Η ανατομία μίας υπηρεσίας
- Προγραμματισμός διεργασιών με cron



M A L L W A R E

- Ransomware (Encrypts data until ransom is paid)
- Keyloggers (Monitors keystrokes)
- Trojans (Disguise as desirable code and executes malicious code instead)
- Rootkits (Remote control of a machine)

Η ανάγκη ύπαρξης λογισμικού ανίχνευσης των παραπάνω μας οδήγησε στα anti-virus, τους scanners κλπ.

