Write-Up: There was an incident! (Forensics)

|  |  |
| --- | --- |
| Ομάδα: | mousiko\_gymsasio\_agriniou\_lt\_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.) |
| Μαθητές/Μαθήτριες | Πέτρος Παπαθανασίου |

# Επισκόπηση Δοκιμασίας

Η συγκεκριμένη δοκιμασία μας δίνει έναν server στον οποίο πρέπει να συνδεθούμε με κάποια credentials. Κατάλληλο προτόκολο σύνδεσης σε αυτόν αποτελείτο ssh. Με την εντολή “ssh [support@challenges.pmdk.gr](mailto:support@challenges.pmdk.gr) -p 37654” μπορούμε να συνδεθούμε στο περιβάλλον της δοκιμασίας.

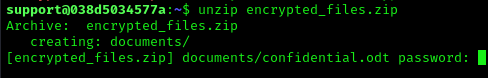
# Επίλυση

## Αρχική ανάλυση

Όταν συνδεόμαστε στον server βλέπουμε τα προσβάσιμα αρχεία με την εντολή “ls”.



Η εκφώνηση της δοκιμασίας αναφέρετε σε κρυπτογράφηση αρχείων. Αμέσως καταλαβαίνουμε ότι αναφέρεται στα αρχεία που είναι σε μορφή zip . Για αυτόν τον λόγο προσπαθούμε να τα κάνουμε unzip. Όμως παρατηρούμε ότι χρειάζεται κάποιος κωδικός.



Μία κλασική τεχνική είναι να πάρουμε το hash τους και να το κάνουμε crack με ένα εργαλείο που ονομάζεται johnthereaper.



Όμως παρατηρούμε ότι κάποιες εντολές είναι απαγορευμένες από τον server.

## Εκμετάλλευση ευπάθειας

Με αρκετό ψάξιμο φάνηκε ότι ο server είχε κρατήσει τις εντόλες που είχε τρέξει ένας χρήστης πριν αποσυνδεθεί. Με άλλα λόγια μπορούμε να μετακινηθούμε στο ιστορικό των εντολών με τα βελάκια. Αρκετό ενδιαφέρον έχει η εντολή “zip --password VmM8Yr6xgbaAh295iIFZKs53asP8b9w6 -r encrypted\_files.zip ./documents/”, στην οποία φαίνεται ο κωδικός που χρησιμοποιήθηκε για να κλειδώσει το zip αρχείο.



Έτσι, τρέχουμε την εντολή “unzip encrypted\_files.zip” με κωδικό “VmM8Yr6xgbaAh295iIFZKs53asP8b9w6” για να πάρουμε το αρχείο flag.txt.

# Σημαία

Η σημαία που βρέθηκε:

|  |
| --- |
| FLAG{c4lm\_d0wn!...I\_r3c0vered\_y0ur\_F1L35!} |