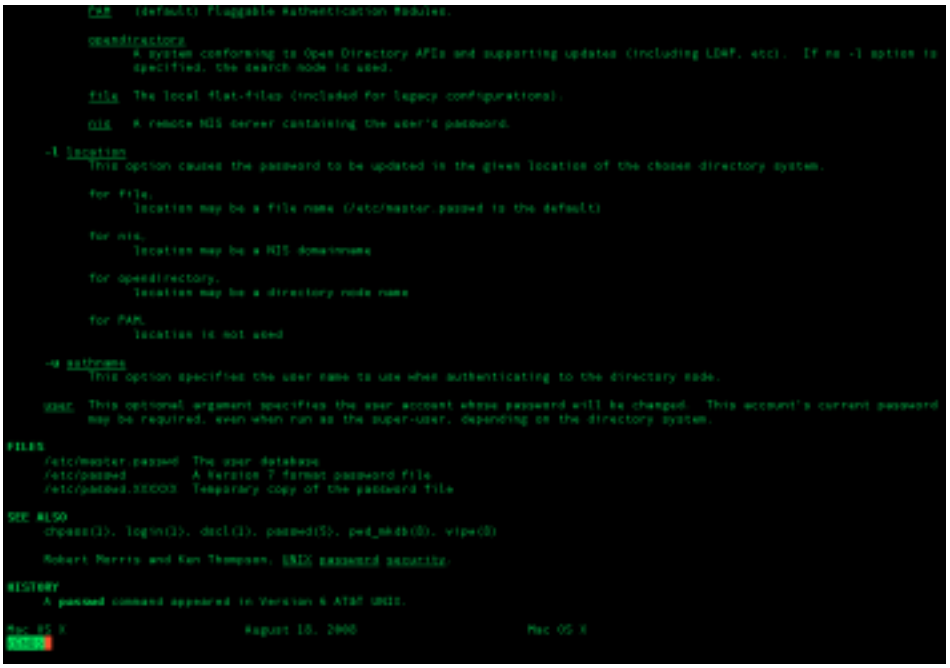
Για να θεωρηθεί ένα Λειτουργικό Σύστημα ασφαλές πρέπει να απομονωθούν όλοι οι παράγοντες παραβάσης ασφάλειας που θέτουν σε κίνδυνο την ακεραιότητα των υπολογιστών και κατ'επέκταση και των δεδομένων που βρίσκονται σε αυτά τα οποία με τη σειρά τους τίθονται σε κίνδυνο. Η ακεραιότητα των δεδομένων είναι αδιαπραγμάτευτη καθώς και η ιδιωτικότητα των χρηστών που συνδέονται άμεσα και χρησιμοποιούν το λειτουργικό σύστημα ή τις εκάστοτε εφαρμογές. Για να είναι ένα λειτουργικό σύστημα ασφαλές χρειάζονται περισσότερα από ένα απλό firewall, ένα antivirus ή οτι θεωρείται τη σήμερον ημέρα ότι προσφέρει ασφάλεια. Ασφαλή πρέπει να είναι από τα μαγνητικά μέσα αποθήκευσης μέχρι και οτι αποθηκεύεται σε αυτά, Passwords και γενικότερα τα Credentials του χρήστη είναι αναμφισβήτητα κάτι πρέπει να είναι εμπιστευτικό και μη προσβάσιμο στο ευρύ κοινό. Γι' αυτό το λόγο χρησιμοποιούνται μέθοδοι κρυπτογράφησης όπου συναρτήσεις αλλά και κωδικοποίησεις των συνθηματικών δεν επιτρέπουν στους εισβολείς να μπορέσουν να χρησιμοποιήσουν αυτά δεδομένα. Το έργο της ασφαλείας του λειτουργικού συστήματος και γενικότερα των ηλεκτρονικών υπολογιστών, φορητών συσκευών και οτιδήποτε συνδέεται με αυτά είναι διάρκειες, καθημερινό και δεν σταματάει ποτέ.

Ανίχνευση ***Σ***υνθηματικών

Σε περιβαλλον Linux

1)Με την εντολή : man –a passwd σε παράθυρο terminal λαμβάνουμε όλες τις πληροφορίες σχετικά με τα passwords, όπως για το πως μπορούμε να χειριστούμε αυτό το αρχείο για να πάρουμε επιπλέον πληροφορίες για τους χρήστες, τοποθεσία του αρχείου κλπ.



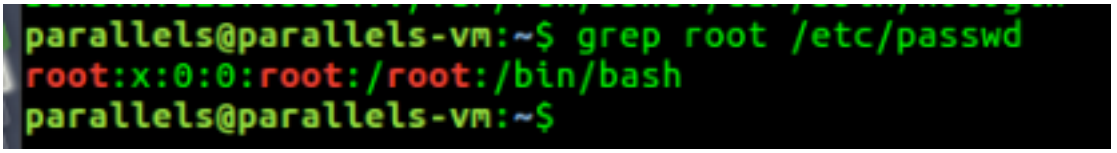
Με τα διαπιστευτήρια που μας δόθηκαν απο το εργαστήριο "Ασφάλεια στη Τεχνολογία της Πληροφορίας" θα εχουμε προσβάση στο περιβάλλον Linux που προσφέρει το SecLab. Κατ' αυτό τον τρόπο θα συνδεθούμε μέσω ασφαλους πρωτοκόλλου – κέλυφος (ssh - secure shell protocol)

ssh asf_xxx@195.130.109.116 -p 9999

Σ' αυτό το σημείο το σύστημα ζητάει από το χρήστη ένα συνθηματικό, Αν ο χρήστης πληκτρολογήσει το σωστό σημαντικό τότε εισάγετε στο σύστημα αλλιώς το σύστημα δεν επιτρέπει την πρόσβαση.

Με την εντολή : nano /etc/passwd Βλέπουμε τις εγγραφές των χρηστών όπου η πρώτη εγγραφή αντιστοιχεί στον χρήστη και ακολουθεί χωρισμένο με άνω κάτω τελείες το πεδίο passwd το οποίο στην περίπτωση της συγκεκριμένη αναπαρίσταται μέ ενα x.
Με την εντολή : ls –al /etc/passwd
Τα δικαιώματα που έχει ο root : -rw
Συγκεκριμένα ο χρήστης root έχει δικαίωμα ανάγνωσης και γραψίματος στο αρχείο.
Τα δικαιώματα που έχουμε έχει το group: --r
Η ομάδα έχει δικαιώματα μόνο ανάγνωσης.
Τα δικαιώματα που έχουν ήδη εκάστοτε χρήστες: --r
Οι χρήστες έχουν δικαίωμα μόνο ανάγνωσης.
Με την εντολή :cat /etc/passwd βλέπουμε λεπτομερώς τις εγγραφές που βρίσκονται στο αρχείο των συνθηματικών.

Με την εντολή : grep root /etc/passwd
Παίρνουμε τα εξής αποτελέσματα:



Το πρώτο πεδίο ανήκει στον χρήστη, χρησιμοποιείται όταν ο χρήστης εισάγετε στο σύστημα. Το μήκος του είναι από 1 (ένα) μέχρι 32. Το δεύτερο πεδίο είναι το πεδίο του συνθηματικού. Όπου ο χαρακτήρας x σημαίνει πως το συνθηματικό είναι κρυπτογραφημένο και φυλάσσεται στο αρχείο: shadow.
Στο τρίτο πεδίο είναι το : userid (UID) . Εδώ βλέπουμε ότι ο χρήστης: root αναπαρίσταται σε αυτό το πεδίο με το μηδέν – 0. Από τον αριθμό ένα μέχρι 99 είναι δεσμευμένα για τους προκαθορισμένους χρήστες. Τα περαιτέρω UID από το 100 μέχρι το 999 είναι δεσμευμένο από το σύστημα για διαχειριστικούς και λογαριασμός συστήματος ή ομάδες. Το τέταρτο πεδίο ονομάζεται : Group ID ή GID το πρωτότυπο GID φυλάσσεται στο αρχείο : /etc/group. Το έκτο πεδίο μας δείχνει το : /home directory στο οποίο θα βρίσκεται ο χρήστης όταν εισαχθεί στο σύστημα. Ο κατάλογος αυτός αναπαρίσταται με το απόλυτο : path του : directory. Το έβδομο πεδίο είναι τότε το απόλυτο : path που δείχνει το κέλυφος που θα χρησιμοποιεί ο χρήστης. Στην συγκεκριμένη περίπτωση ο κατάλογος είναι το: /bin/ και το κέλυφος χρησιμοποιείται είναι το : bash.

Shadow file:

Τα πεδιά στο αρχείο shadow είναι χωρισμένα με άνω κάτω(:)
Ακουλουθούν υποπεδια χωρισμένα με το σήμα του $.
Το πρώτο πεδίο είναι το πεδίο του χρήστη.
Το δεύτερο πεδίο είναι το πεδίο του : password. Το συνθηματικό πρέπει να είναι τουλάχιστον οκτώ χαρακτήρες, και μέγιστο 12 χαρακτήρες.
συνήθως το φορμάτ που χρησιμοποιεί το αρχείο shadow για το πεδίο του σημαντικού είναι ορισμένο ως εξής : idsalt$hashed Το πρώτο υποπεδίο στο πεδίο του password δείχνει τον αλγόριθμο που έχει εφαρμοστεί για την κρυπτογράφηση.

1. 1 is MD5
2. $2a$ is Blowfish
3. $2y$ is Blowfish
4. 5 is SHA-256
5. 6 is SHA-512

Το δεύτερο υποπεδίο είναι το: salt. Γενικότερα στην κρυπτογραφία το : salt είναι δεδομένα που παράγονται με τυχαία μορφή και χρησιμοποιούνται για επιπρόσθετη είσοδο σε μία : one way συνάρτηση οποία κάνει : Hash τα δεδομένα όπως ένα συστηματικό.

Το τρίτο υποπεδίο είναι το : Hashed Value το οποίο λαμβάνει το συνθηματικό που έχει εισάγει ο χρήστης και παράγει ένα αλφαριθμητικό κωδικοποιημένο με μοναδικό τρόπο πάλι μέσω της συνάρτησης η οποία λειτουργεί με μόνο μια κατεύθυνση. Κάθε φορά που εισάγεται ο χρήστης δεν συγκρίνεται το πραγματικό password αλλά το : Hashed Value αυτού μέσω συνάρτησης : Crypt.

Crypt : είναι μια συνάρτηση κρυπτογράφησης η οποία δουλεύει βασισμένη σε ένα κλειδί σαν φίλτρο και κρυπτογραφει - αποκρυπτογράφει από το stdin στο stdout.
Εστω το αρχείο: simple.txt
Το οποίο εμπεριέχει 1 απλό κείμενο στην αγγλική γλώσσα.
Με την εντολή:

```
cat simple.txt | crypt > my.cpy
Enter key :
```

Το σύστημα ζητάει ένα κλειδί για κρυπτογράφηση. Και ύστερα μέσω σωλήνωσης το αρχικό κείμενο οδηγείται στο τελικό κείμενο my.cpy όπου πλέον παράγεται ένα κρυπτογραφημένο κείμενο. Αν γνωρίζουμε το password με το οποίο κρυπτογραφiθηκε το αρχικό κείμενο τότε μπορούμε να αποκρυπτογραφήσουμε και να πάρουμε το αρχικό μας κείμενο. Με την εντολή : cat –n my.cpy βλέπουμε τα περιεχόμενα του κειμένου.

Το τρίτο πεδίο είναι η ημερομινια ποτε αλλαξε τελευταια φορα το passwd.

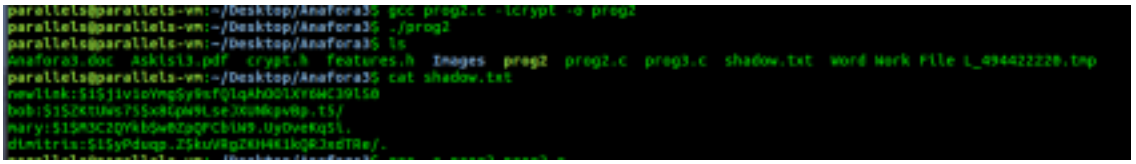
Το τέταρτο πεδίο αφορά το ελάχιστο περιθώριο που χρειάζεται για να αλλάξει το συνθηματικό.
Το πέμπτο πεδίο προσδιορίζει το μέγιστο αριθμό σε μέρες πριν αυτο ληξει. Ο χρήστης ειδοποιείται ότι το : password πρέπει να αλλάξει.

Το έβδομο πεδίο προσδιορίζει τον αριθμό των ημερών μετά τις όποιες Ο λογαριασμός θα λήξει και επομένως ο λογαριασμός γίνεται ανενεργός.

Το όγδοο πεδίο αφορά την λήξη του λογαριασμού σε μια απόλυτη ημερομηνία όπου η είσοδος δεν επιτρέπεται μετά τη συγκεκριμένη ημερομηνία.

2)

Παρατίθενται κώδικας σε γλώσσα C, και ακολουθεί screenshot που δείχνει την εκτέλεση προγράμματος.



3)

Επίσης παραδίδεται κώδικας σε γλώσσα C και ακολουθεί screenshot που δείχνει την εκτέλεση το προγράμματος και στις δύο περιπτώσεις. Όπου στην πρώτη περίπτωση Ο χρήστης εισάγετε στο σύστημα με επιτυχία. Ενώ στην δεύτερη περίπτωση εισάγουμε το όνομα χρήστη το οποίο είναι σωστό και υπάρχει στις εγγραφές αλλά με λάθος συνθηματικό. Το σύστημα

επιστρέφει μήνυμα πως η είσοδος σε αυτό απέτυχε. Αξίζει να σημειωθεί πως στη δεύτερη περίπτωση προτείνουμε έναν αόριστο τρόπο να ειδοποιήσουμε – ενημερώσουμε τον χρήστη. Χωρίς δηλαδή να να προσφέρουμε πληροφορία για το τι ακριβώς απέτυχε - ήταν το συνθηματικό it όνομα χρήστη. Για αυτό το λόγο το σύστημα εμφανίζει γενικό μήνυμα : Invalid Access

```
parallels@parallels-vm:~/Desktop/Anafora3$ gcc prog3.c -lcrypt -o prog3
parallels@parallels-vm:~/Desktop/Anafora3$ ./prog3
Username: newlink
password: lot%sa
Login successful!
Logged user newlink
parallels@parallels-vm:~/Desktop/Anafora3$ ./prog3
Username: dimitris
password: uhu
Invalid access
parallels@parallels-vm:~/Desktop/Anafora3$
```

4) Σημείωση : επειδή το συγκεκριμένο ερώτημα απαιτούσε την συνάρτηση crypt έγινε η εγκατάσταση σε περιβάλλον Linux για αυτό η απεικόνιση και τα screenshot είναι διαφορετικα απ' τα προηγούμενα ερωτημάτα.
a)Για τον χρήστη tom με βάση τις πληροφορίες που έχουμε εκτελούμε το πρόγραμμα με τα συνθηματικά που φτιάξαμε βάσει αυτών.

```
anna
marousi
pinkfloyd
User: tom

Password: pinkfloyd
```

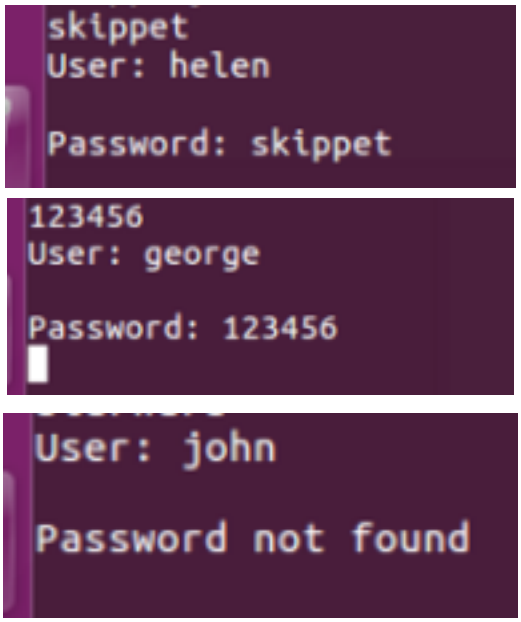
b) Εμπλουτίζουμε το : dictionary.txt και παίρνουμε τα εξής αποτελέσματα

```
starwars
User: peter

Password not found
```

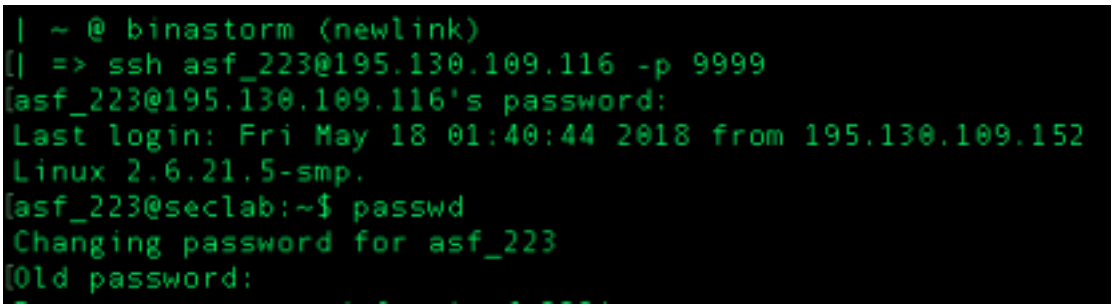
```
responsibility
User: mary

Password: responsibility
```



c) Κάνουμε :brute force attack με όλους τους πιθανούς συνδυασμούς : Για τους χρήστες : Peter ,John δεν μπορέσαμε να βρούμε τα συνθηματικά τους.

5) Με τα credentials που μας δόθηκαν μπαίνουμε στο περιβάλλον του seclab.



Πηγές που χρησιμοποιήθηκαν:

http://www.youssefkh.com/2014/01/13-free-ebooks-on-unix-and-linux.html
https://www.cyberciti.biz/faq/understanding-etcshadow-file/

Άμπελ Μπάσα
Αθήνα Μάιος 2018