ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΕΡΓΑΣΙΑ #1

ΘΕΜΑ: Αυθεντικοποίηση και πολιτικές ασφάλειας Windows

1. Επιλέξτε δύο (2) από τα παρακάτω συνθηματικά (password) για τον χρήστη με username chatzis, ως καταλληλότερα σύμφωνα με τους κανόνες πολυπλοκότητας. Αιτιολογείστε τις επιλογές σας.
   I. `Chatz*3_1`
   II. `F%2_=87ba^`
   III. `t4(8^rt\`
   IV. `p@s$word`

2. Από ποιά συστατικά συντίθενται οι ρυθμίσεις ασφάλειας των αντικειμένων του Active Directory;

3. Πώς γίνεται η εκχώρηση αδειών σε χρήστες για αντικείμενα του Active Directory; Πώς προκύπτουν οι ισχύουσες άδειες χρήστη;

4. Χρειάζεται να υλοποιήσετε μια πολιτική που θα αποτρέπει την εύρεση των κωδικών με την μέθοδο brute force. Ποιά/ές από τις ακόλουθες πολιτικές θα ακολουθούσατε και ποιά/ές όχι; Αιτιολογείστε τις επιλογές σας.
   I. Μέγιστη διάρκεια κωδικού πρόσβασης
   II. Επιβολή ιστορικού κωδικού πρόσβασης
   III. Ελάχιστη διάρκεια κωδικού πρόσβασης
   IV. Κλείδωμα λογαριασμού για
   V. Όριο κλειδώματος λογαριασμού
   VI. Επαναφορά μετρητή κλειδώματος λογαριασμού ύστερα από…
   VII. Οι κωδικοί πρόσβασης πρέπει να τηρούν τις προϋποθέσεις πολυπλοκότητας

5. Περιγράψτε τρεις (3) μεθόδους που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να ανακαλύψει τα συνθηματικά των χρηστών ενός συστήματος Windows, καθώς και τα πλεονεκτήματα / μειονεκτήματα που παρουσιάζει η κάθε μία από αυτές.

6. Αναφερθείτε συνοπτικά στη χρησιμότητα του Local Security Policy και στις βασικές ρυθμίσεις που περιέχει.

7. Περιγράψτε τη διαδικασία και αιτιολογείστε τον ορισμό μιας πολιτικής συνθηματικού (password policy) σύμφωνα με την οποία το σύστημα
   I. να θυμάται τα τελευταία 5 χρησιμοποιημένα συνθηματικά προκειμένου να μην ξαναχρησιμοποιηθούν από τον χρήστη. Μέχρι πόσα μπορεί να θυμάται το σύστημα;
   II. να ξαναζητάει από τον χρήστη να εισάγει νέο συνθηματικό μετά από 30 μέρες

III. να μην επιτρέπει στον χρήστη να αλλάξει ένα νέο συνθηματικό πριν από 2 μέρες χρήσης του.
IV. να επιβάλλει ελάχιστο μήκος συνθηματικού στους 6 χαρακτήρες
V. να μην περιέχει ολόκληρο ή μέρος του username
VI. να περιέχει λατινικούς χαρακτήρες και αριθμητικά ψηφία και ειδικούς χαρακτήρες, όπως !, $, #, %.

8. Περιγράψτε τη διαδικασία και αιτιολογείστε τον ορισμό μιας πολιτικής κλειδώματος λογαριασμού (account lockout policy) σύμφωνα με την οποία το σύστημα να κλειδώνει τον λογαριασμό χρήστη για 10 λεπτά μετά από 4 αποτυχημένες προσπάθειες εισόδου στο σύστημα.

9. Με ποιό μηχανισμό γίνεται η καταγραφή των συμβάντων στα Windows; Ποιά είδη συμβάντων μπορούμε να καταγράφουμε; Πώς ενεργοποιείται η καταγραφή συμβάντων ασφάλειας;

10. Περιγράψτε τη διαδικασία ορισμού μιας πολιτικής επίβλεψης (audit policy) σύμφωνα με την οποία το σύστημα
    I. να καταγράφει κάθε περίπτωση αποτυχημένης εισόδου ή εξόδου χρήστη στο/από το σύστημα
    II. να καταγράφει κάθε επιτυχή ή αποτυχημένη περίπτωση διαχείρισης λογαριασμού, όπως δημιουργία χρήστη, αλλαγή λογαριασμού κ.λ.π.
    III. να καταγράφει κάθε περίπτωση εκκίνησης ή παύσης λειτουργίας του υπολογιστή.

Καλή επιτυχία!

ΟΔΗΓΙΕΣ ΥΠΟΒΟΛΗΣ:

1. Δημιουργία αρχείου σε μορφή Rich Text Format και με όνομα 'ISS20_P1_AM.rtf', όπου θα συμπεριλάβετε τα στοιχεία σας και τις απαντήσεις στα ερωτήματα της εργασίας.
2. Το αρχείο θα αναρτηθεί στον ιστότοπο του μαθήματος και συγκεκριμένα στο σύνδεσμο «Εργασίες Φοιτητών» με Τίτλο Εργασίας το παραπάνω όνομα (π.χ. 'ISS20_P1_2199').

Προθεσμία υποβολής

31 Μαρτίου 2020, ώρα 23:59