



ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

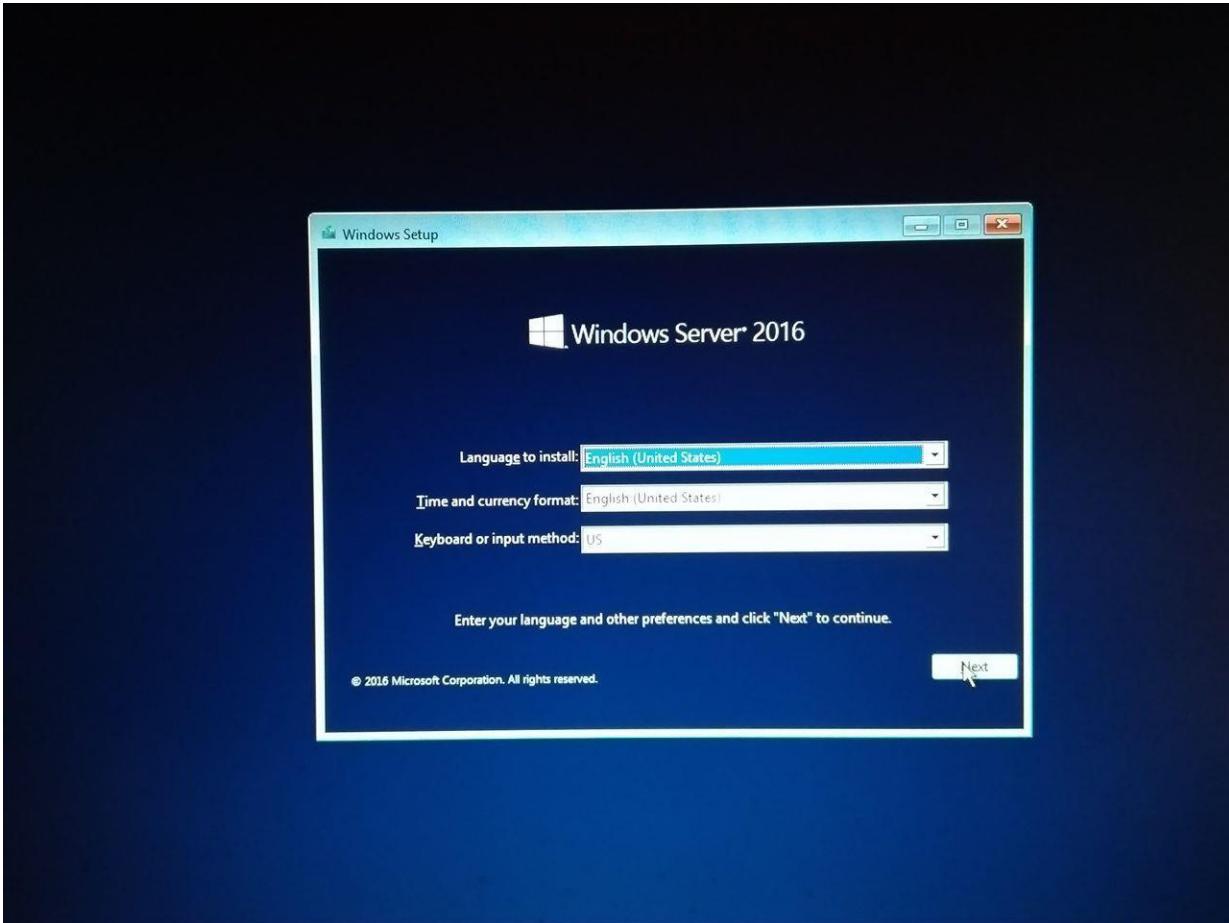
Πρώτη Εργαστηριακή Άσκηση

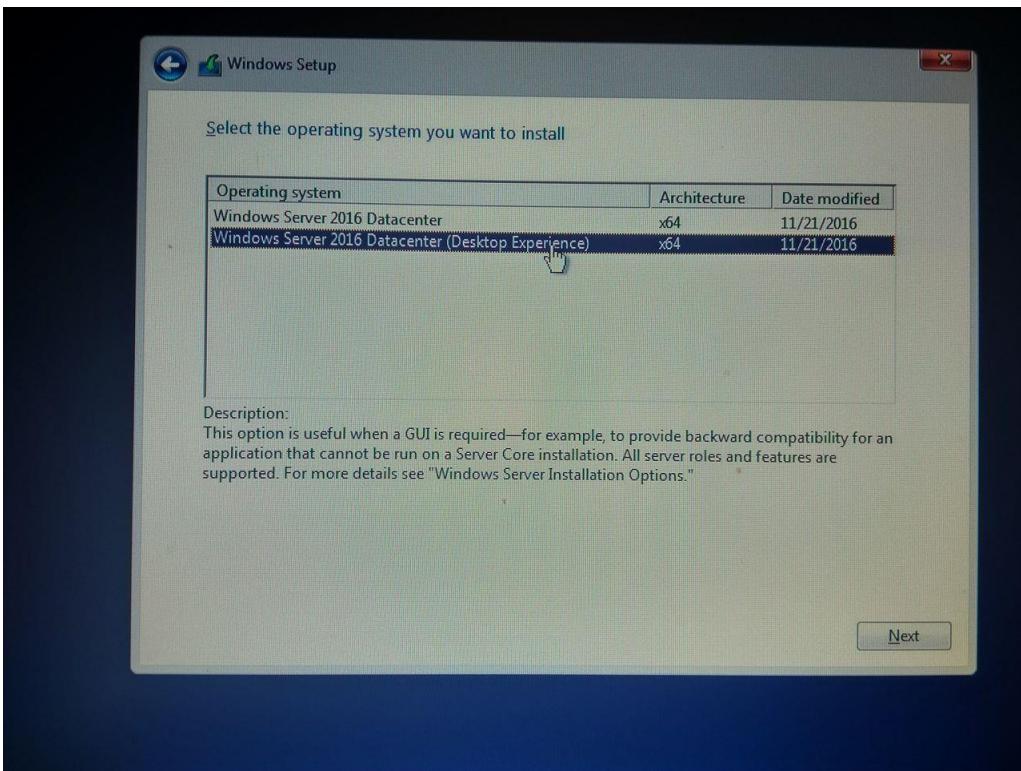
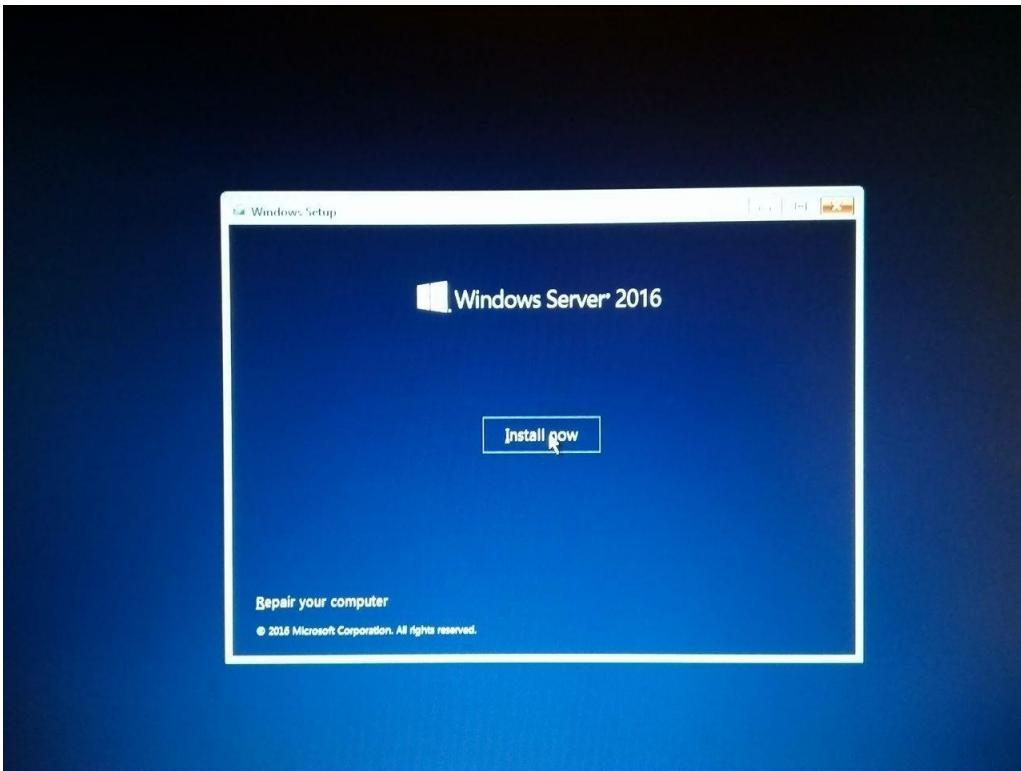
Φοιτητής:

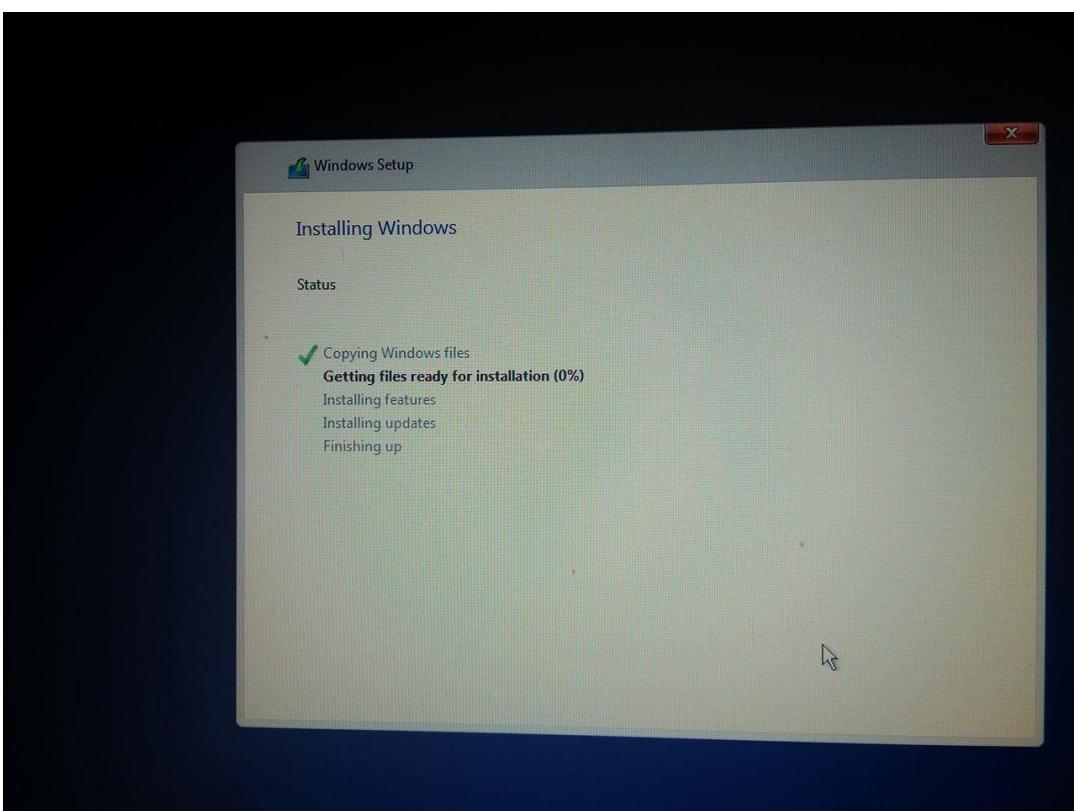
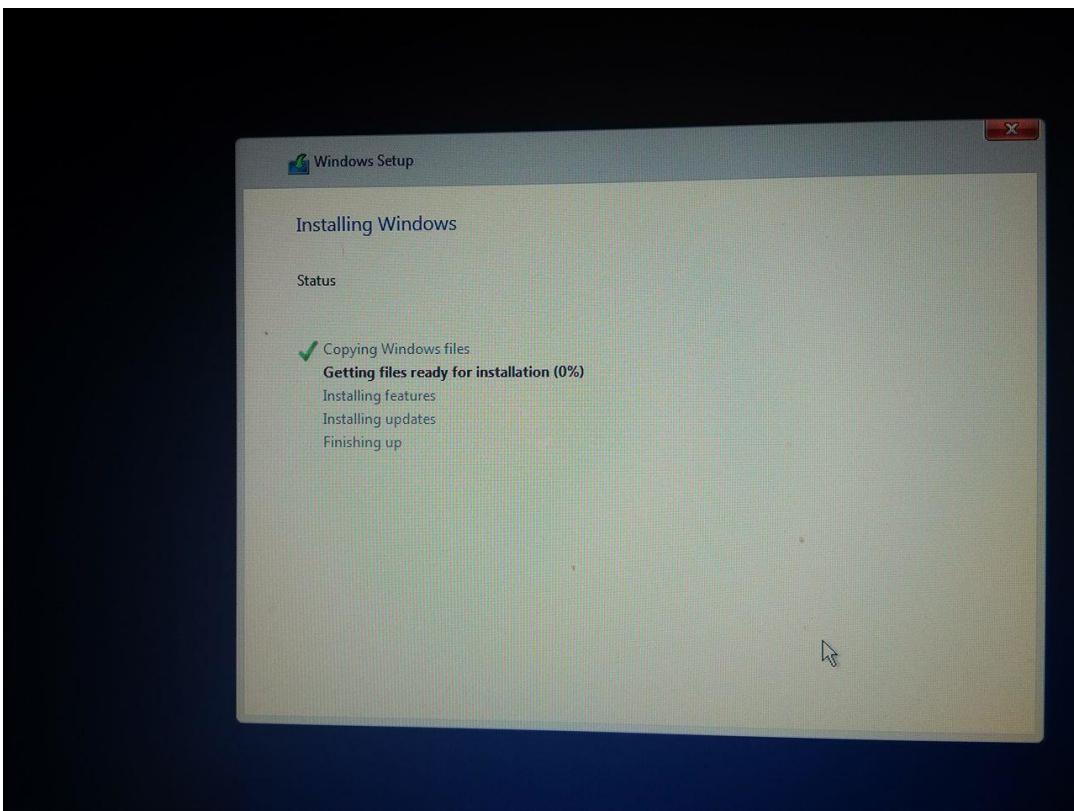
Μπινιάκου Θεοφάνης icsd13126

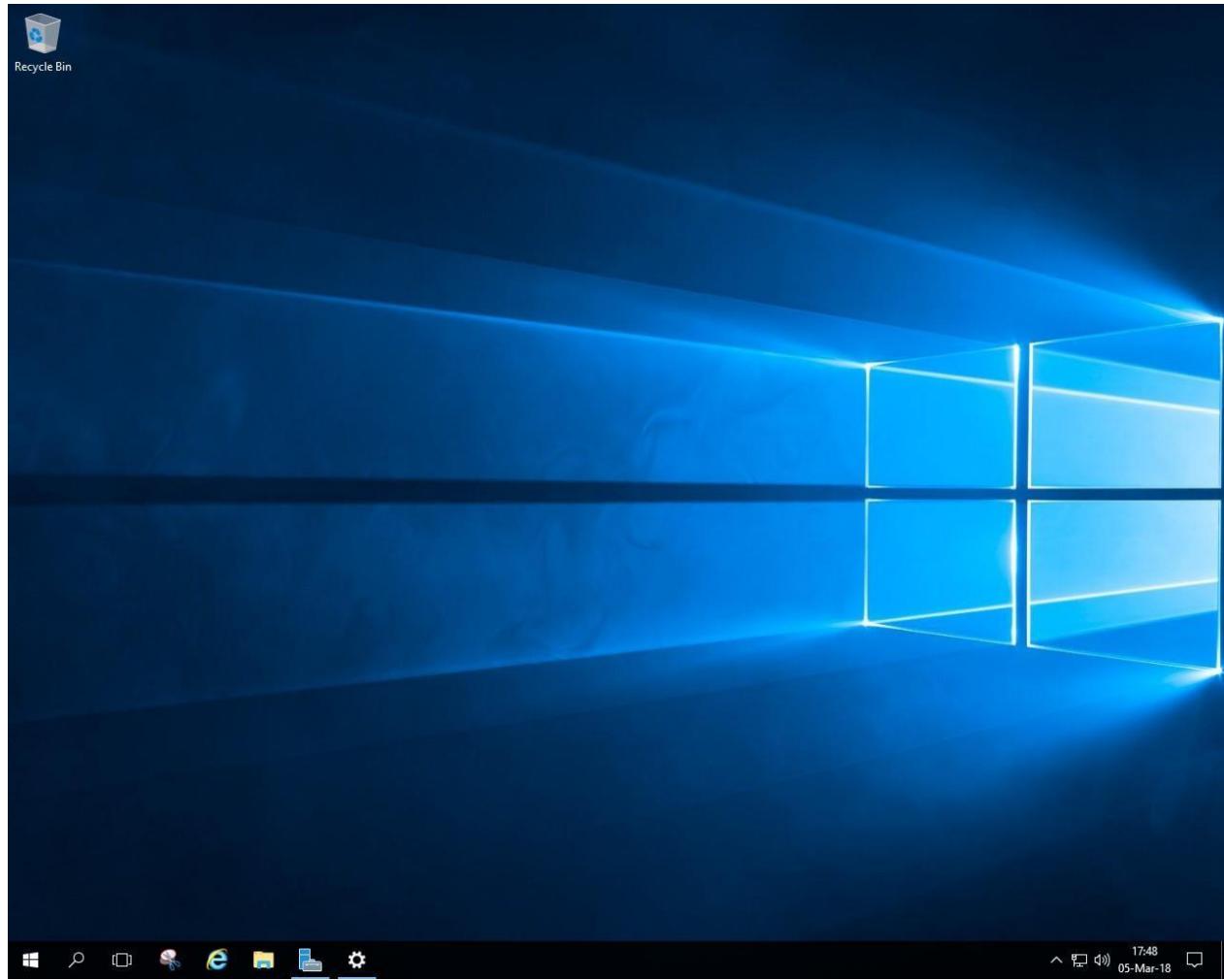
Windows Server (Περιβάλλον Εργασίας)

Η εγκατάσταση των Windows Server 2016 έγινε τοπικά σε υπολογιστή. Το λογισμικό το κατέβασα από https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_cs=1&cmi_mnuMain=dba_23cf-e05e-e011-971f-0030487d8897&ws=dd9a7e50-836f-e011-971f-0030487d8897&vsro=8 (Microsoft Imagine).







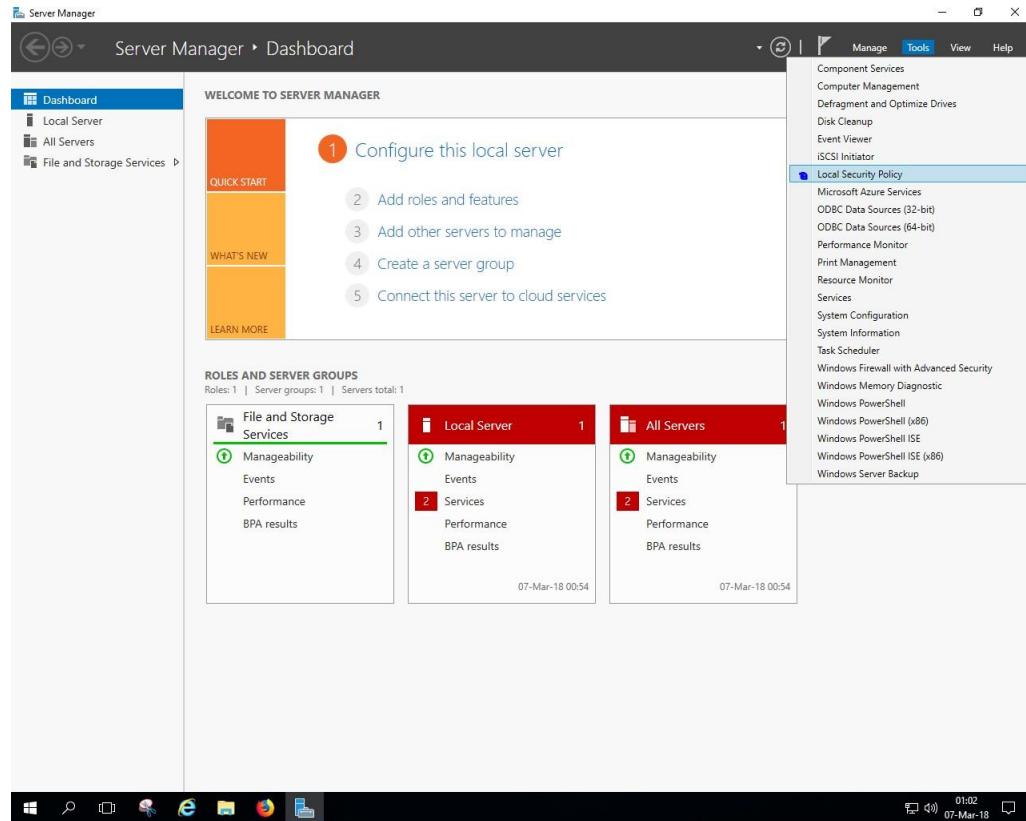


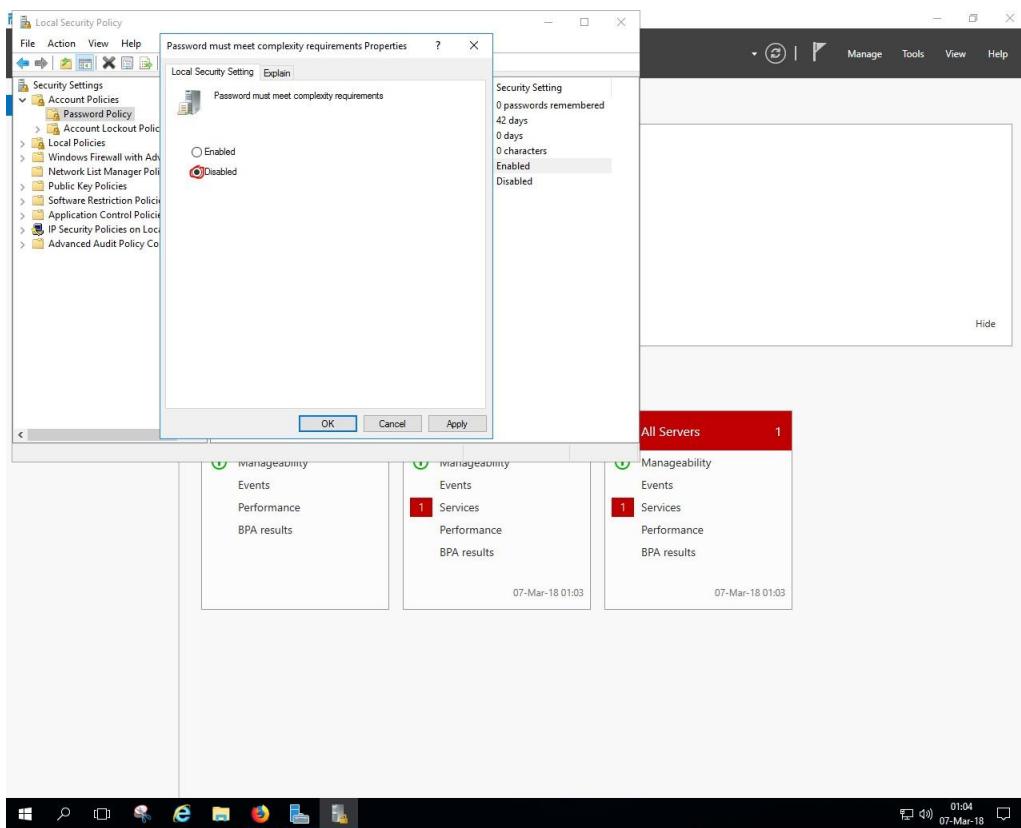
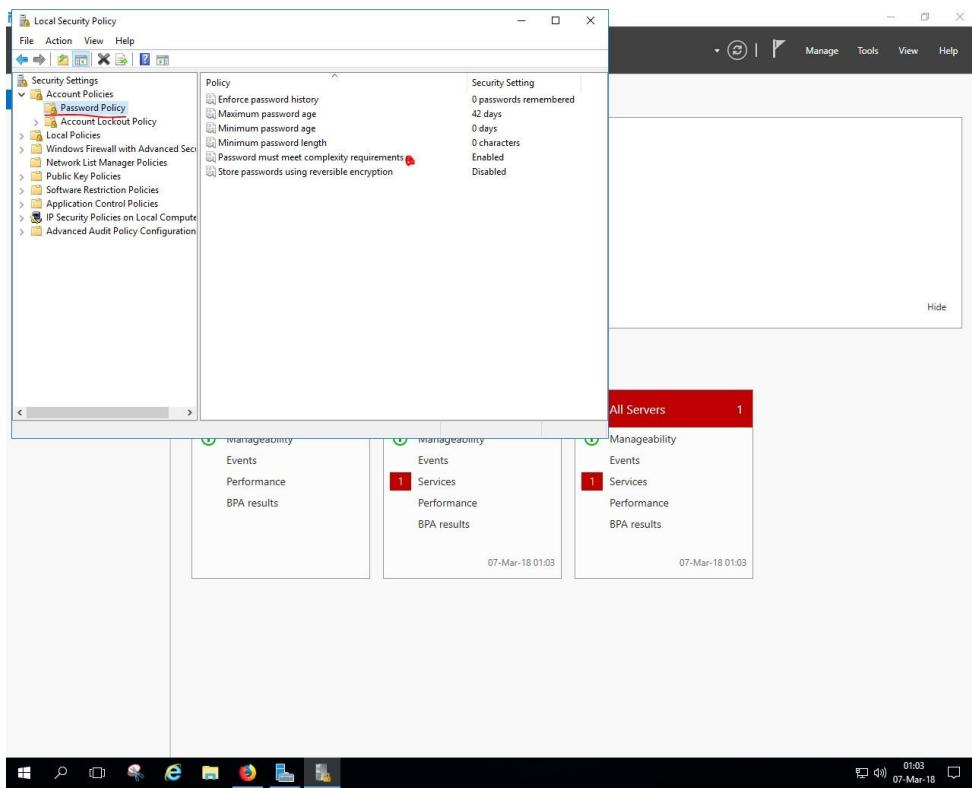
Στην συνέχεια έκανα update στο σύστημα, και ο server είναι έτοιμος για χρήση και επεξεργασία.

1. Διαχείριση Χρηστών και Αυθεντικοποίηση

1.1 Δημιουργία Χρηστών και Ομάδων

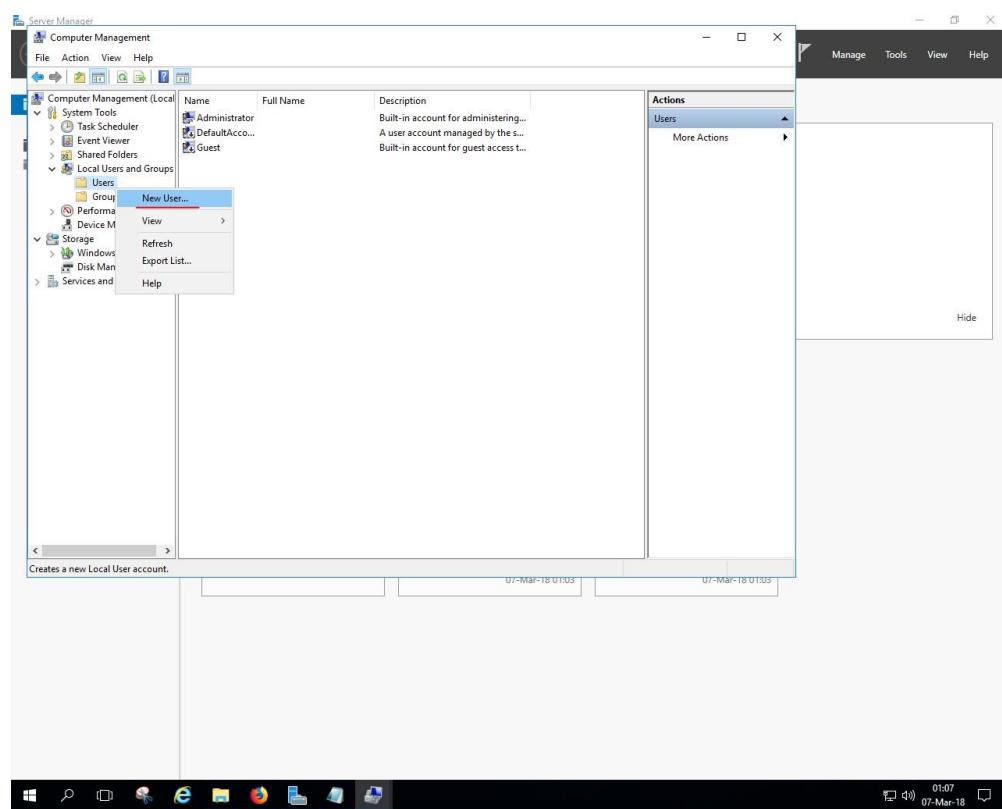
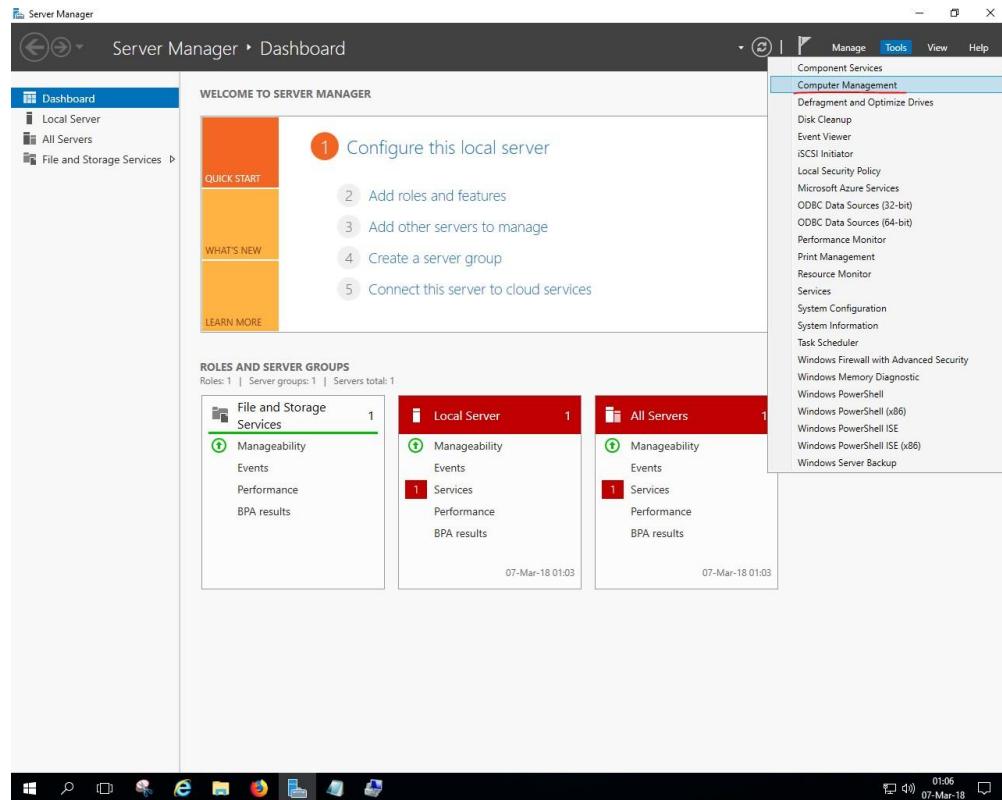
Αρχικά, για να μπορέσω να δημιουργήσω κάποιους χρήστες με πολύ απλό κωδικό, έπρεπε να αλλάξω τις πολιτικές ασφάλειας κωδικών επειδή από default ο windows server έχει ενεργοποιημένο το complexity requirements. Ο τρόπος που το έκανα φαίνεται παρακάτω :

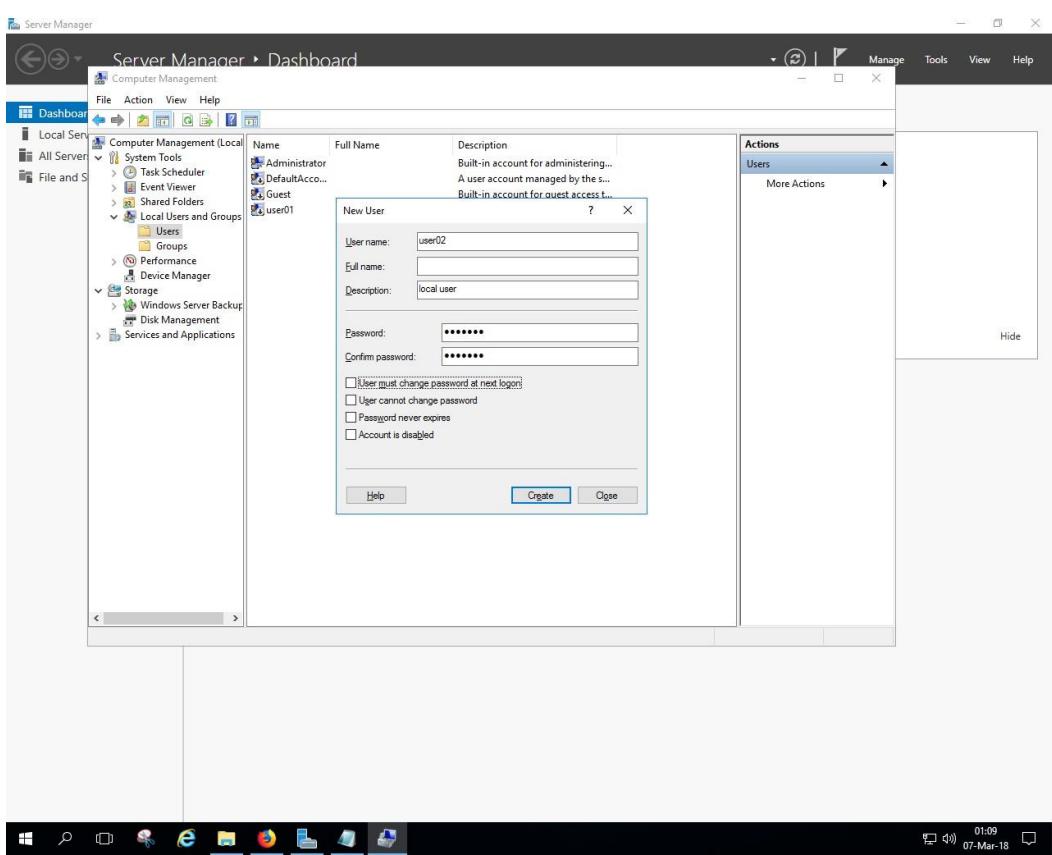
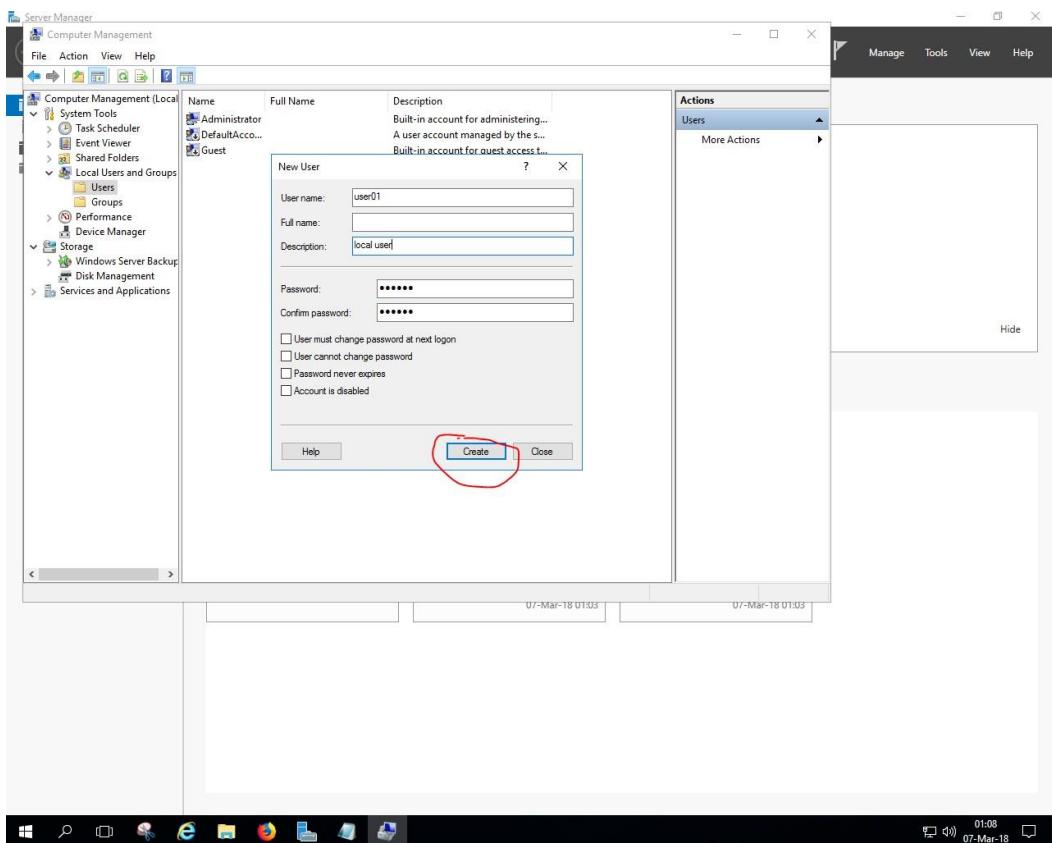


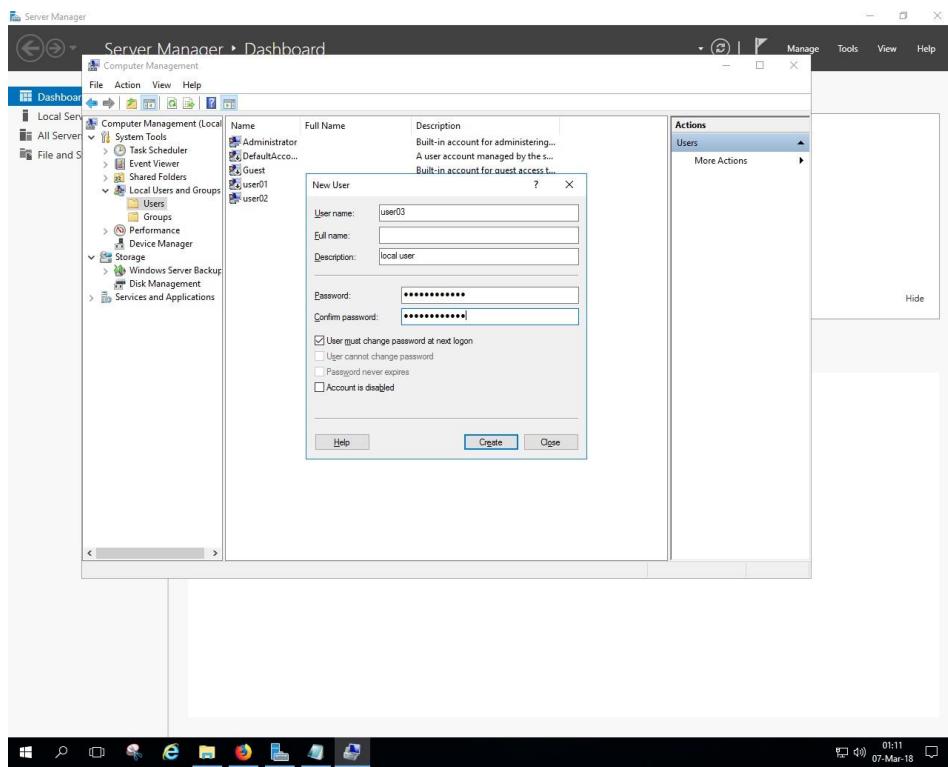


Δεν χρειάστηκε να αλλάξω κάτι άλλο για να μπορέσω να δημιουργήσω χρήστη με κωδικό 123456 όπως στο παράδειγμα της εκφώνησης.

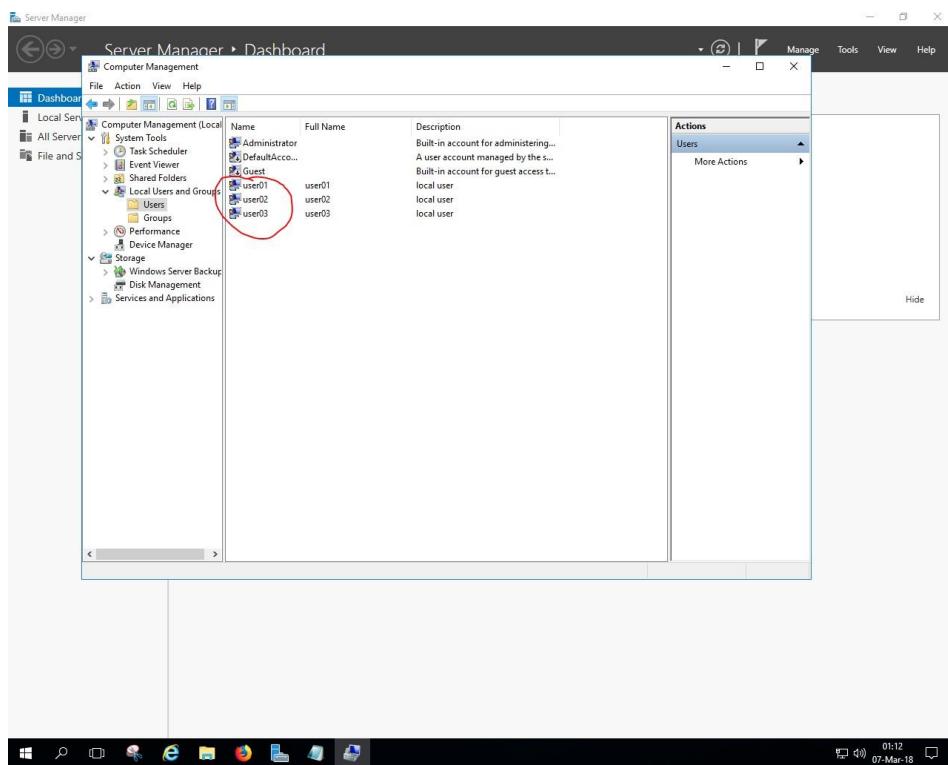
Παρακάτω φαίνεται η διαδικασία δημιουργίας των 3 τοπικών χρηστών.



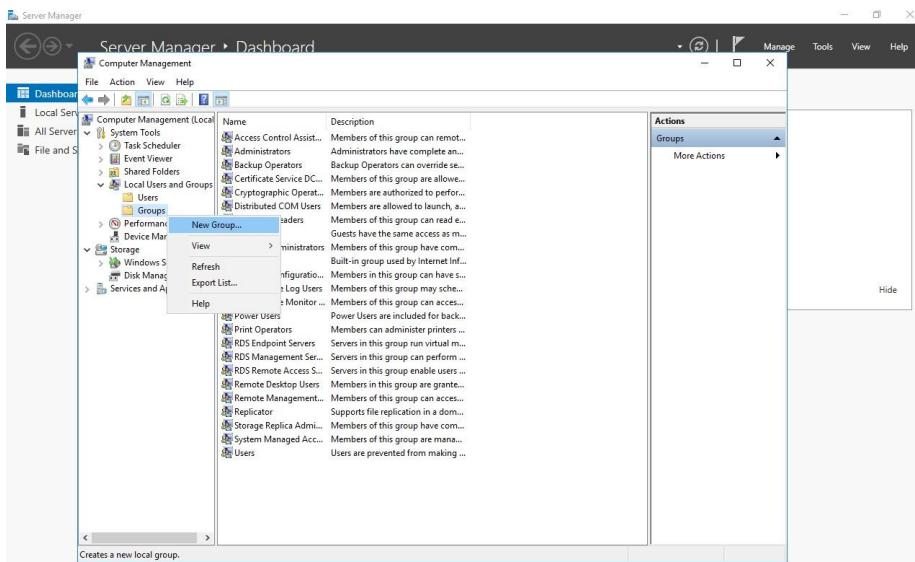




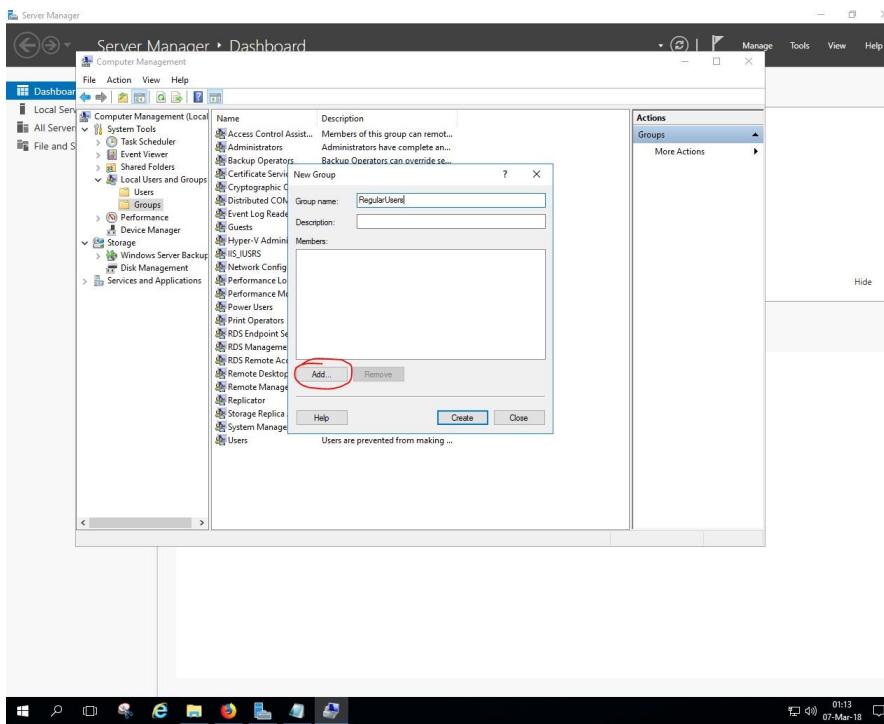
Και εδώ επιβεβαιώνετε η δημιουργία των 3 χρηστών.

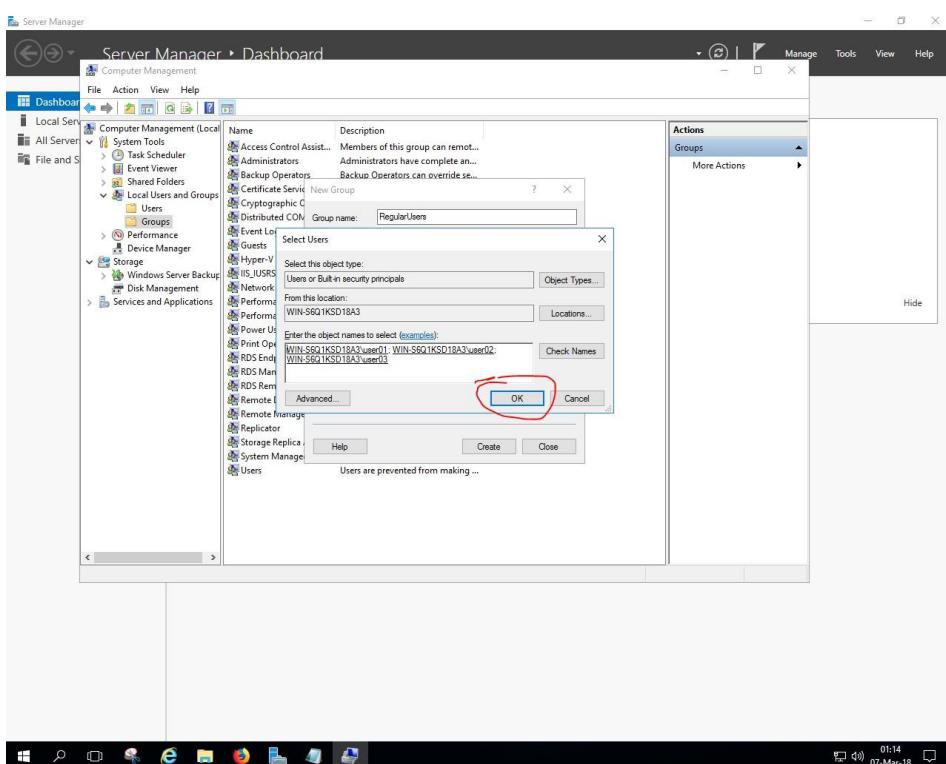
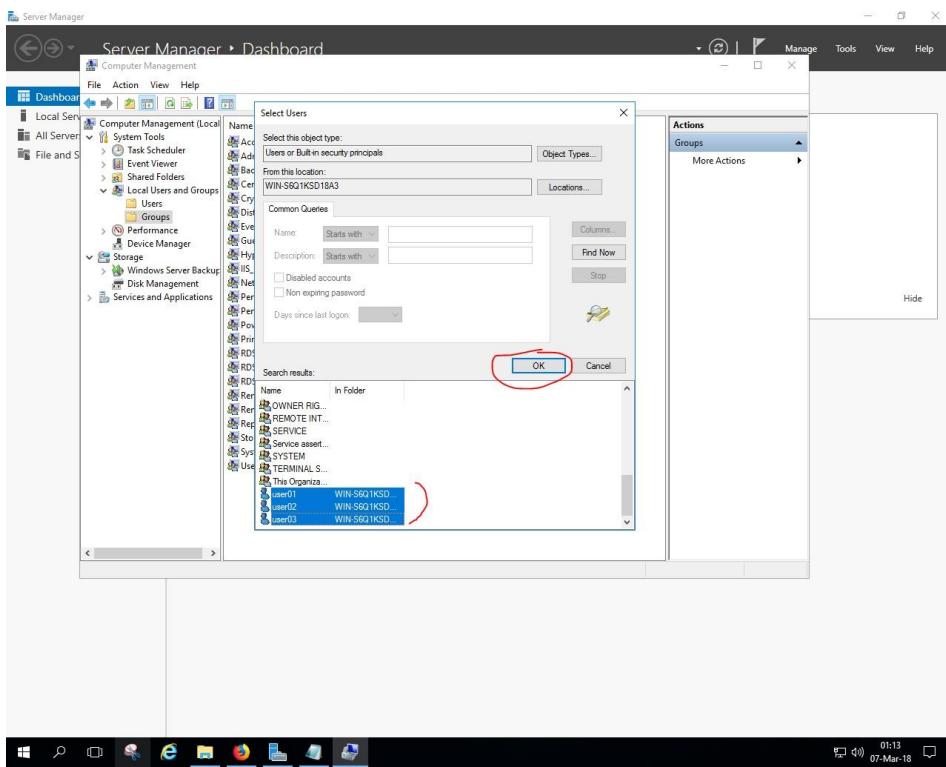


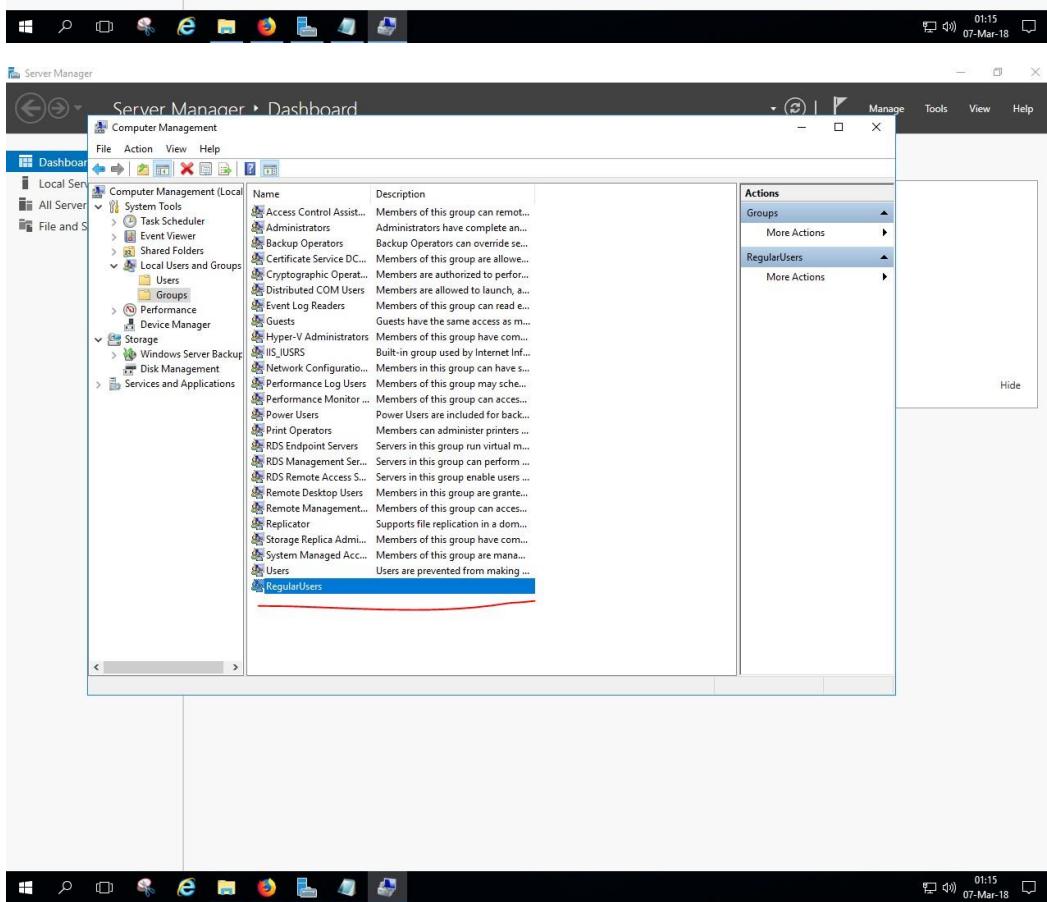
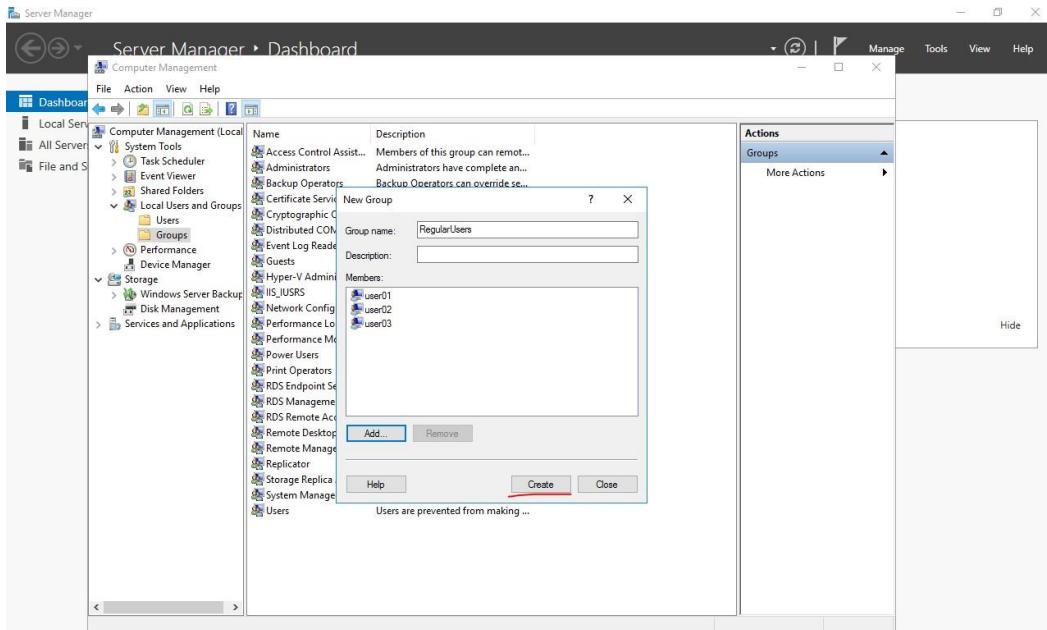
Στην συνέχεια δημιουργώ το γκρουπ “RegularUsers”



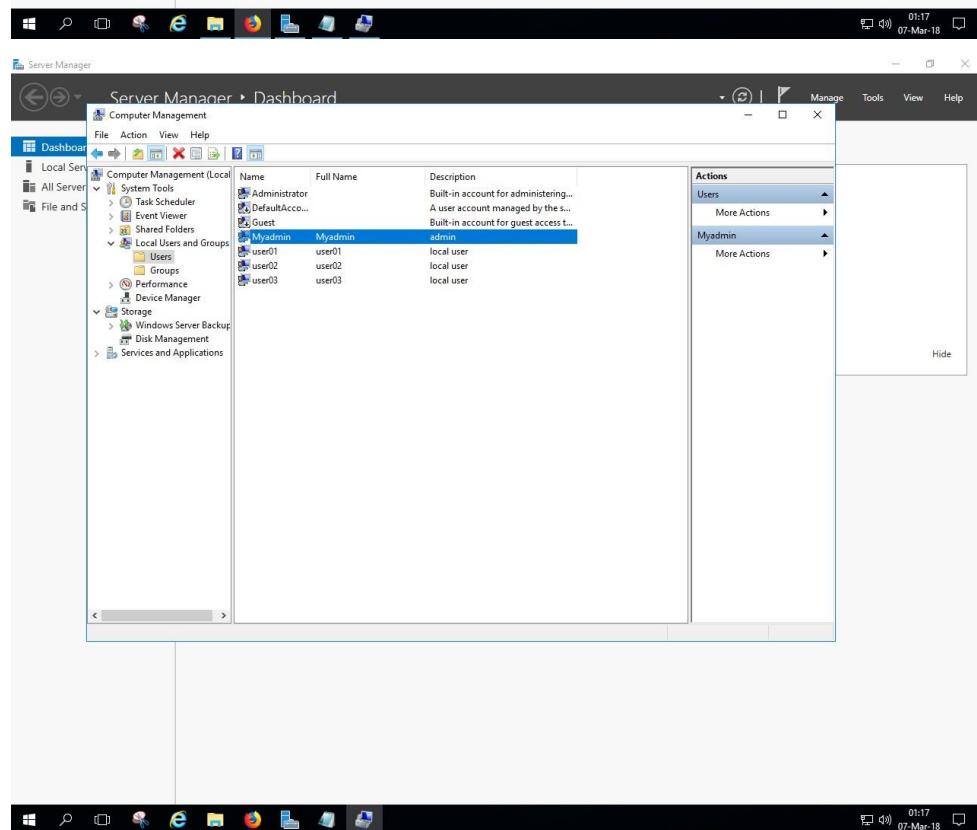
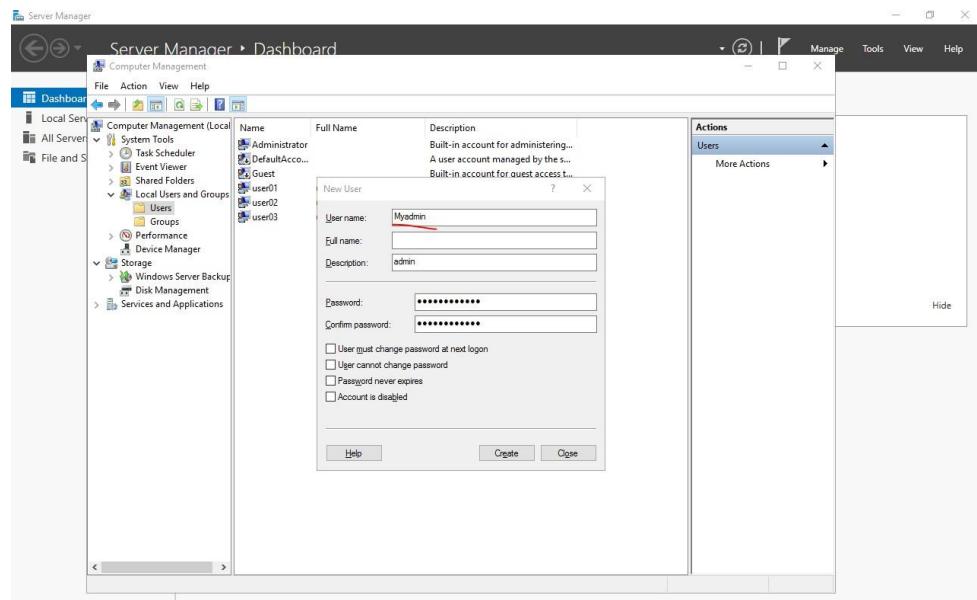
Και προσθέτω τους 3 τοπικούς χρήστες σε αυτή την ομάδα.



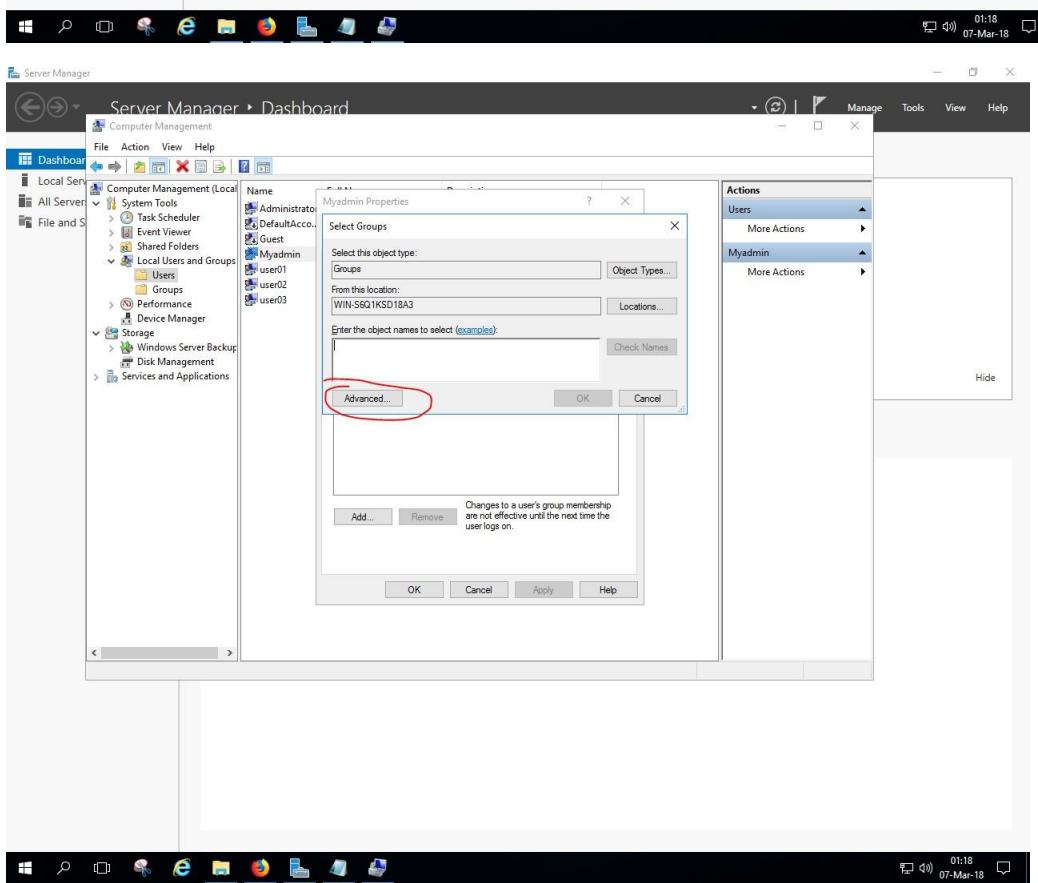
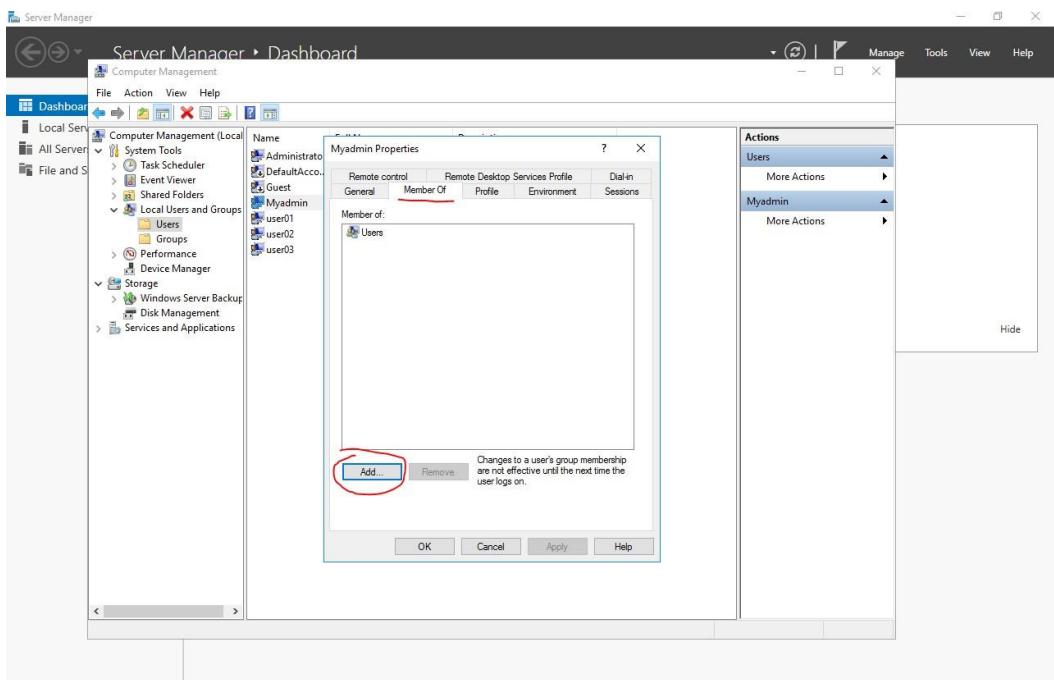


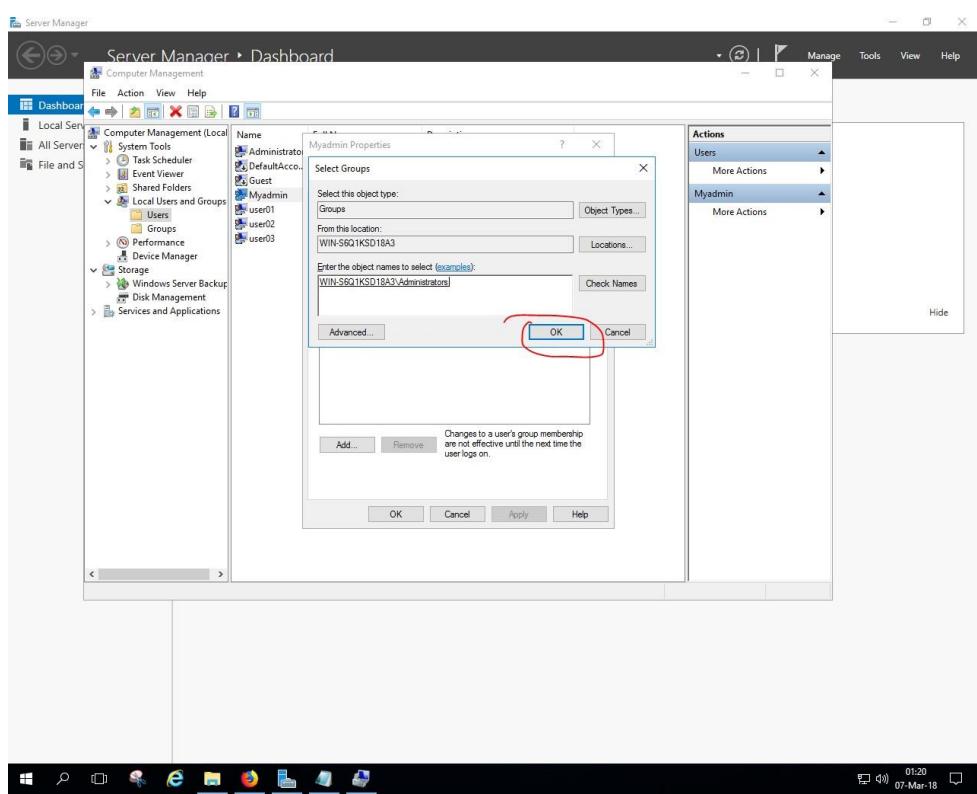
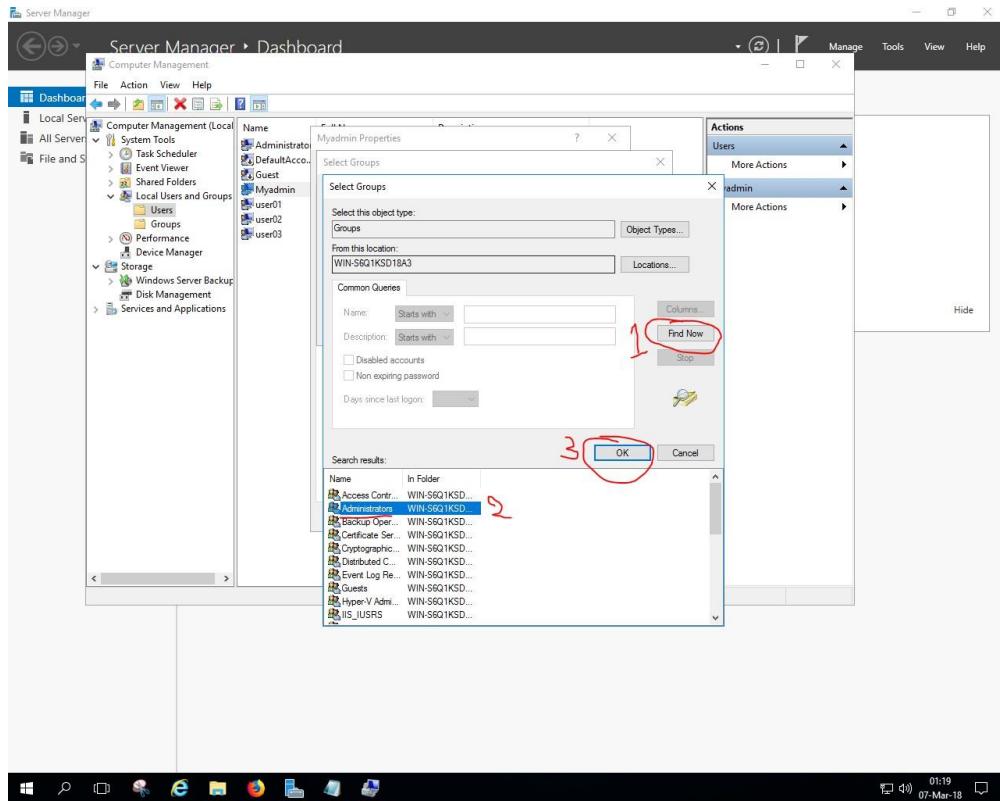


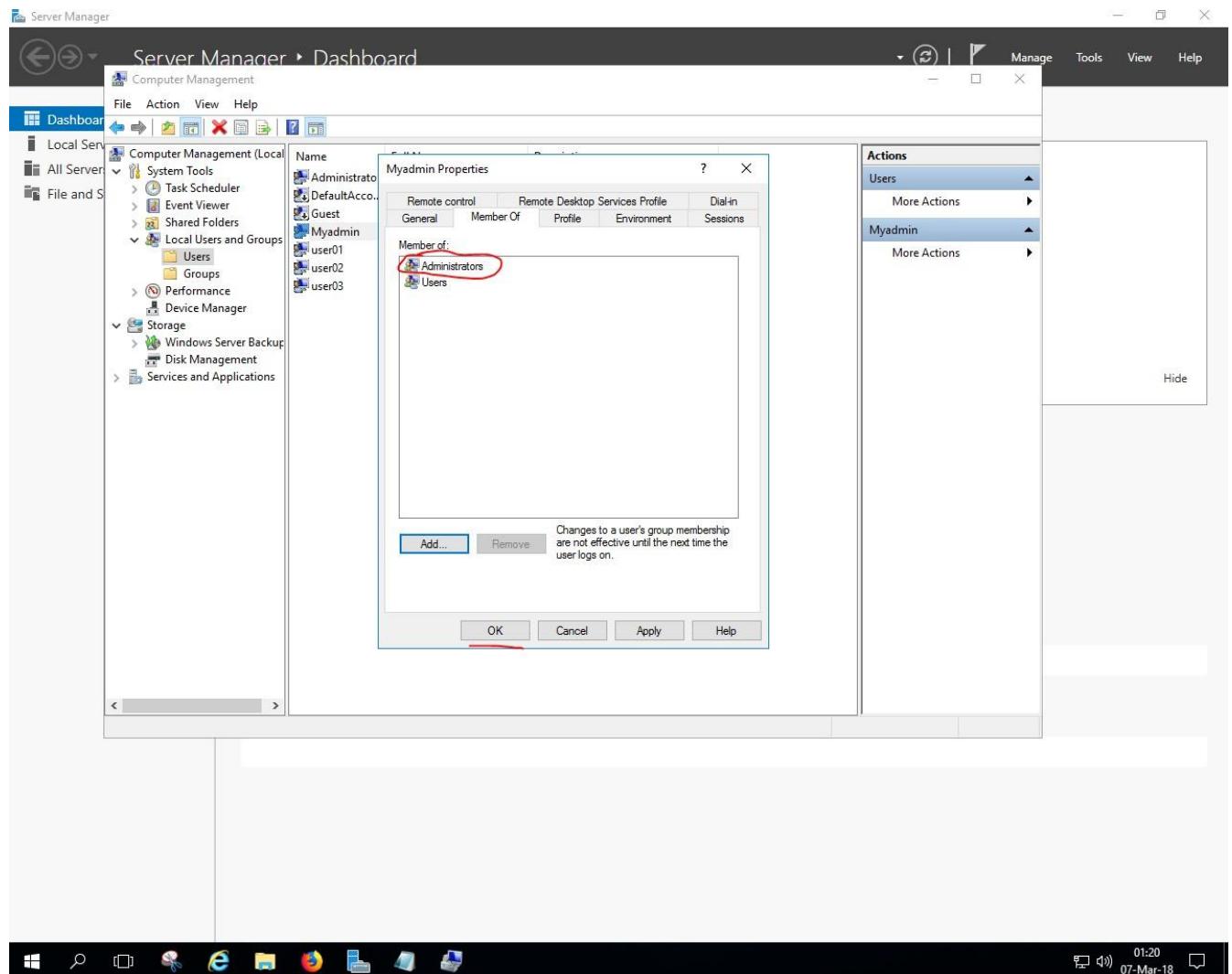
Παρακάτω φαίνεται η διαδικασία δημιουργίας του χρήστη Admin.



Και τον προσθέτω στους Administrators.







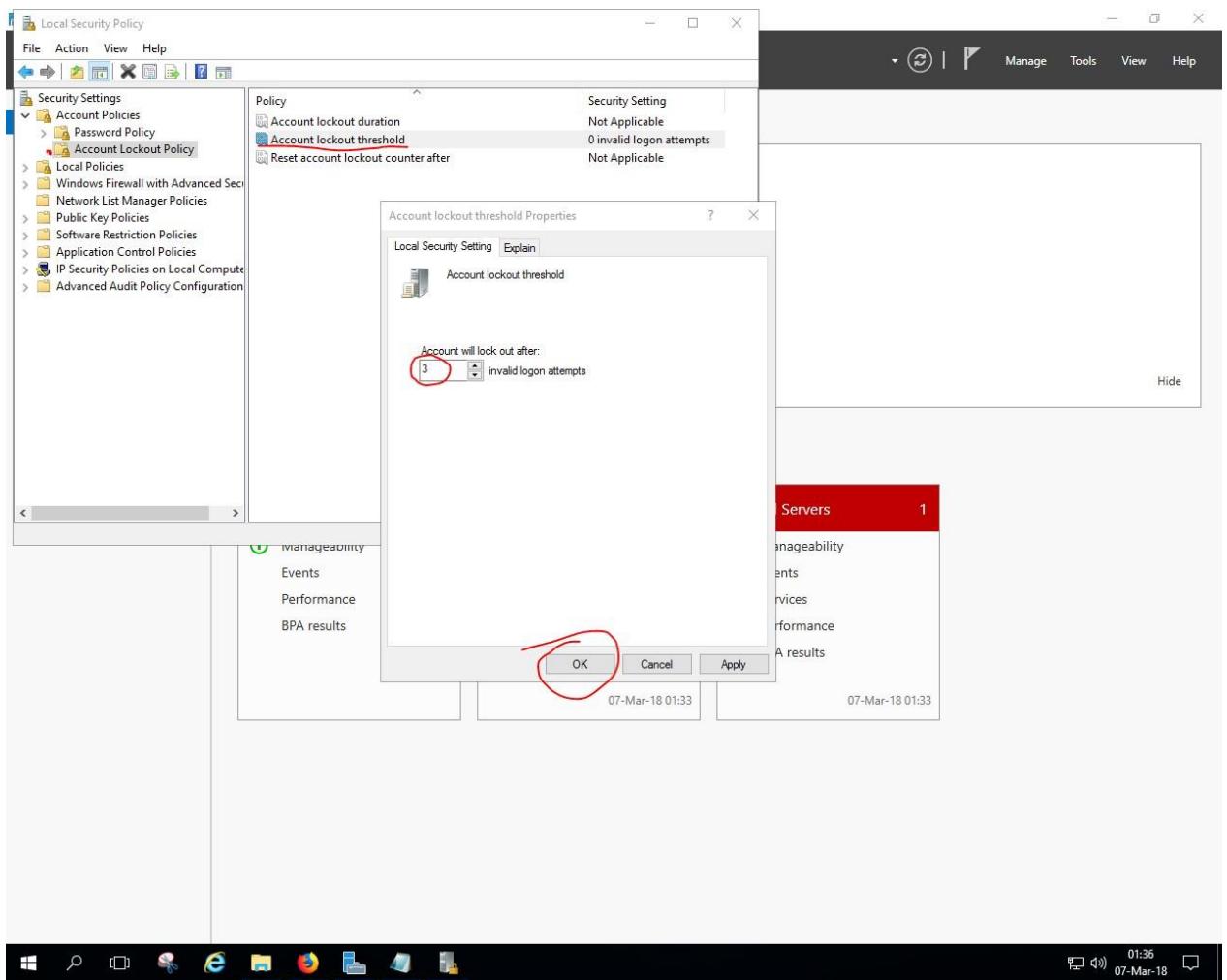
Αυτή ήταν η διαδικασία δημιουργίας τοπικών χρηστών και ενός Admin σύμφωνα με τις υποδείξεις της εκφώνησης. Οι κωδικοί των χρηστών είναι οι αντίστοιχοι από την εκφώνηση.

1.2 Πολιτικές Ασφάλειας Λογαριασμών Χρηστών

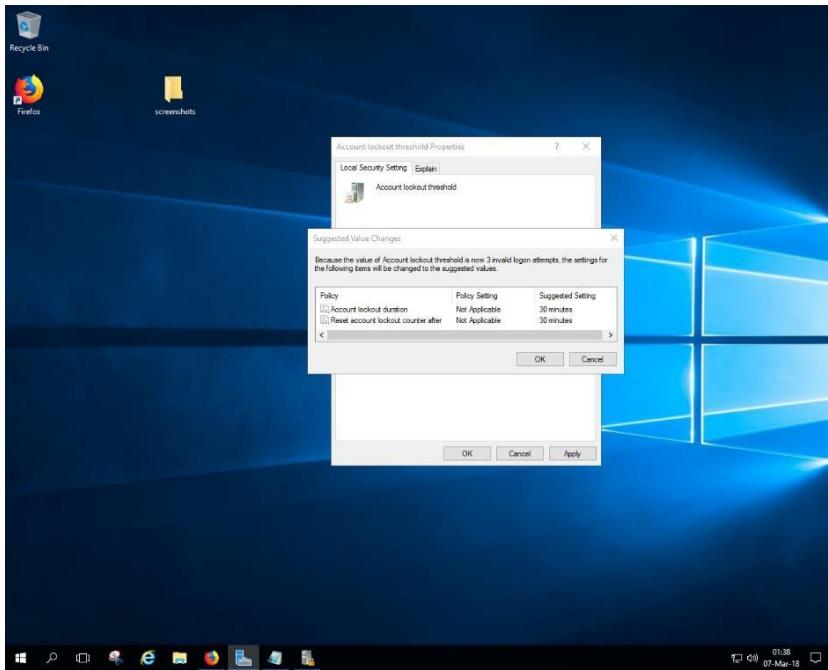
Όσον αφορά τις βασικές πολιτικές ασφάλειας που αφορούν τον λογαριασμό του χρήστη, υπάρχουν 3 βασικές :

- Account lockout duration
- Account lockout threshold
- Reset account lockout counter after

Αρχικά :



Όπου οι χρήστες μετά από 3 αποτυχημένες προσπάθειες σύνδεσης στον λογαριασμό τους, θα τους κλειδώνει ο λογαριασμός. Στην συνέχεια, μου εμφάνισε τις παρακάτω default τιμές για τις υπόλοιπες πολιτικές ασφάλειας λογαριασμού.

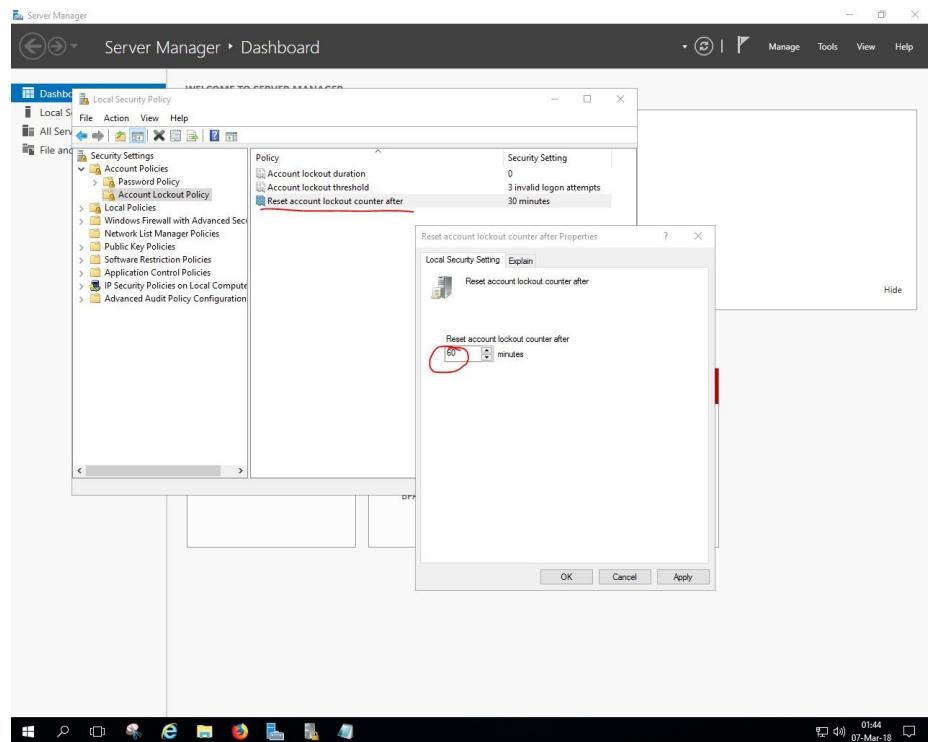


Παρακάτω φαίνονται οι αλλαγές που έκανα στις παραπάνω παραμέτρους των υπόλοιπων δύο πολιτικών ασφάλειας.

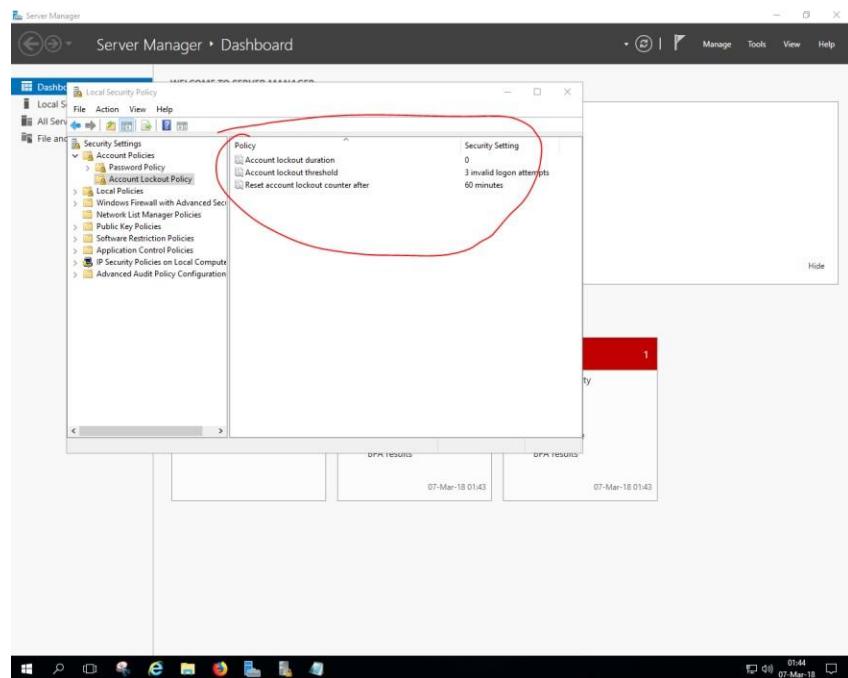
Αρχικά, μηδένισα το Account lockout duration έτσι ώστε αν κλειδώσει κάποιος λογαριασμός, να μπορεί να ξεκλειδωθεί μόνο από έναν Διαχειριστή.

The screenshot shows the Windows Server Manager interface. The left sidebar lists various security settings like Local Security Policy, IP Security Policies, and Advanced Audit Policy Configuration. The 'Local Security Policy' section is expanded, and the 'Account Lockout Policy' node is selected. In the main pane, the 'Account lockout duration' policy is being modified. The current setting is 30 minutes. A tooltip in the dialog box says: 'Account is locked out until administrator unlocks it.' The 'd' button in the minutes input field is highlighted with a red circle.

Στην συνέχεια :



Αυτό σημαίνει ότι αν ο χρήστης συμπληρώσει 2 φορές λάθος τον κωδικό του, αλλά την 3^η φορά σωστά, (ενώ το threshold = 3), ο μετρητής των αποτυχημένων προσπαθειών θα μηδενιστεί (σύμφωνα με το παραπάνω screenshot) μετά από 60 λεπτά.

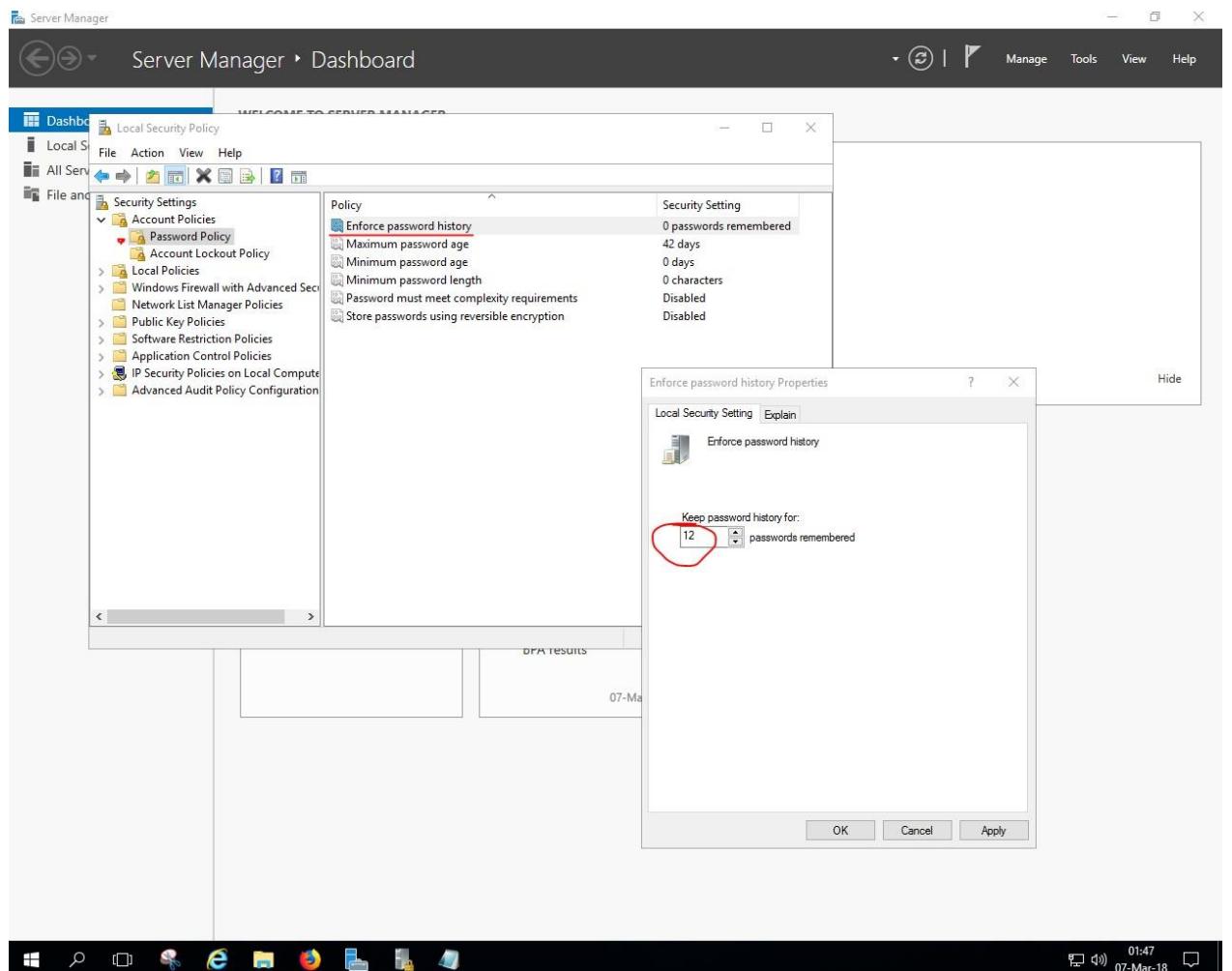


1.3 Πολιτικές Ασφάλειας Συνθηματικών

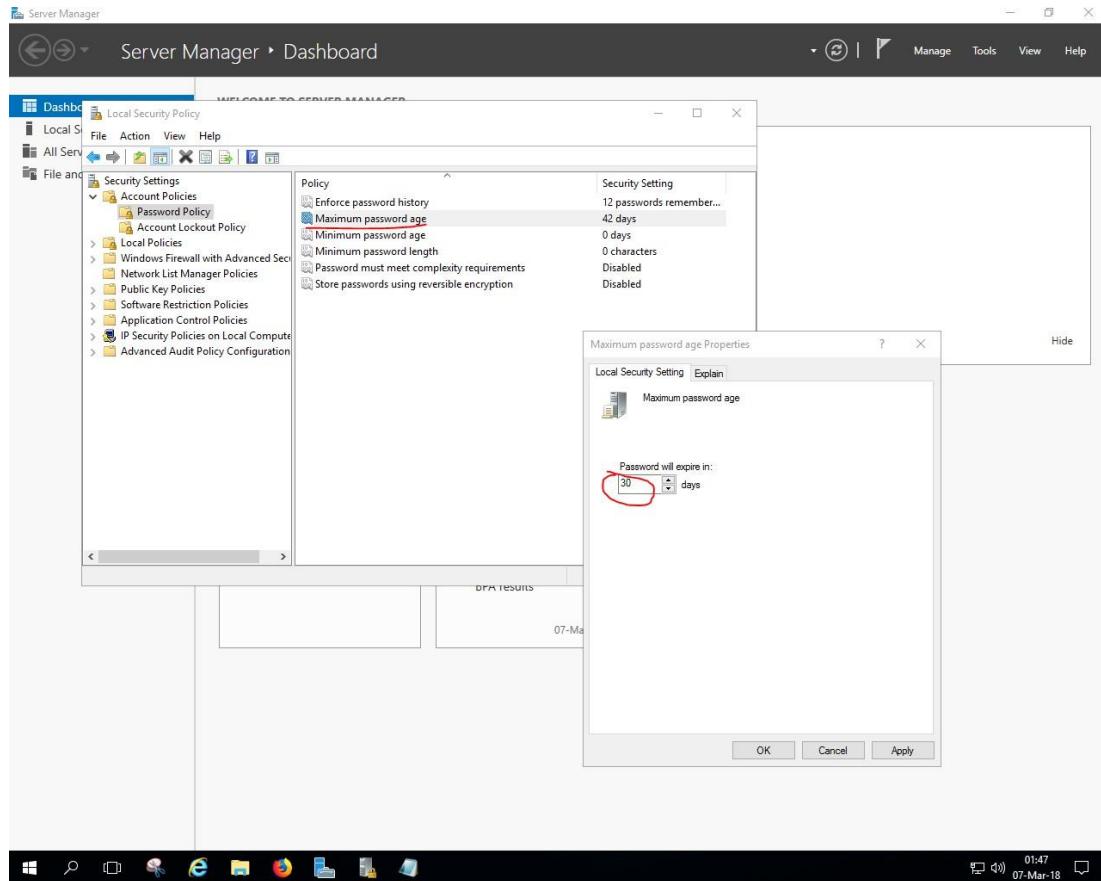
Όσον αφορά τις πολιτικές ασφάλειας συνθηματικών υπάρχουν οι παρακάτω :

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store password using reversible encryption

Παρακάτω φαίνονται οι παραμετροποιήσεις που έκανα σε κάθε μια ξεχωριστά :



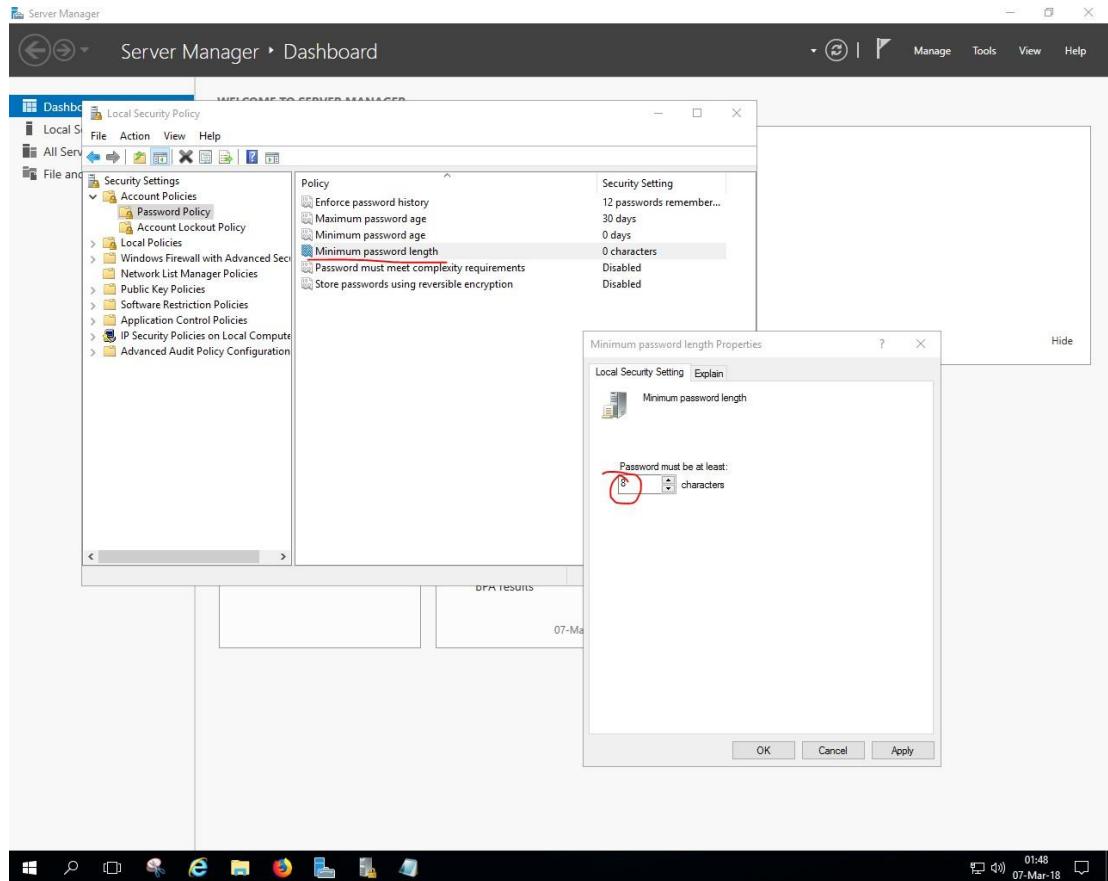
Έθεσα το enforce password history = 12. Αυτό σημαίνει ότι ο server θα «θυμάται» για κάθε χρήστη τους τελευταίους 12 κωδικούς του, με αποτέλεσμα να μην μπορεί να επαναχρησιμοποιήσει κάποιον από αυτούς. Δηλαδή όταν αλλάξει κωδικό, ο νέος κωδικός θα πρέπει να διαφέρει από τους προηγούμενους 12.



Θέτω το maximum password age = 30 μέρες. Ο χρήστης δηλαδή θα κρατάει έναν κωδικό το πολύ 30 μέρες. Μετά από αυτό το διάστημα, θα πρέπει να αλλάξει κωδικό.

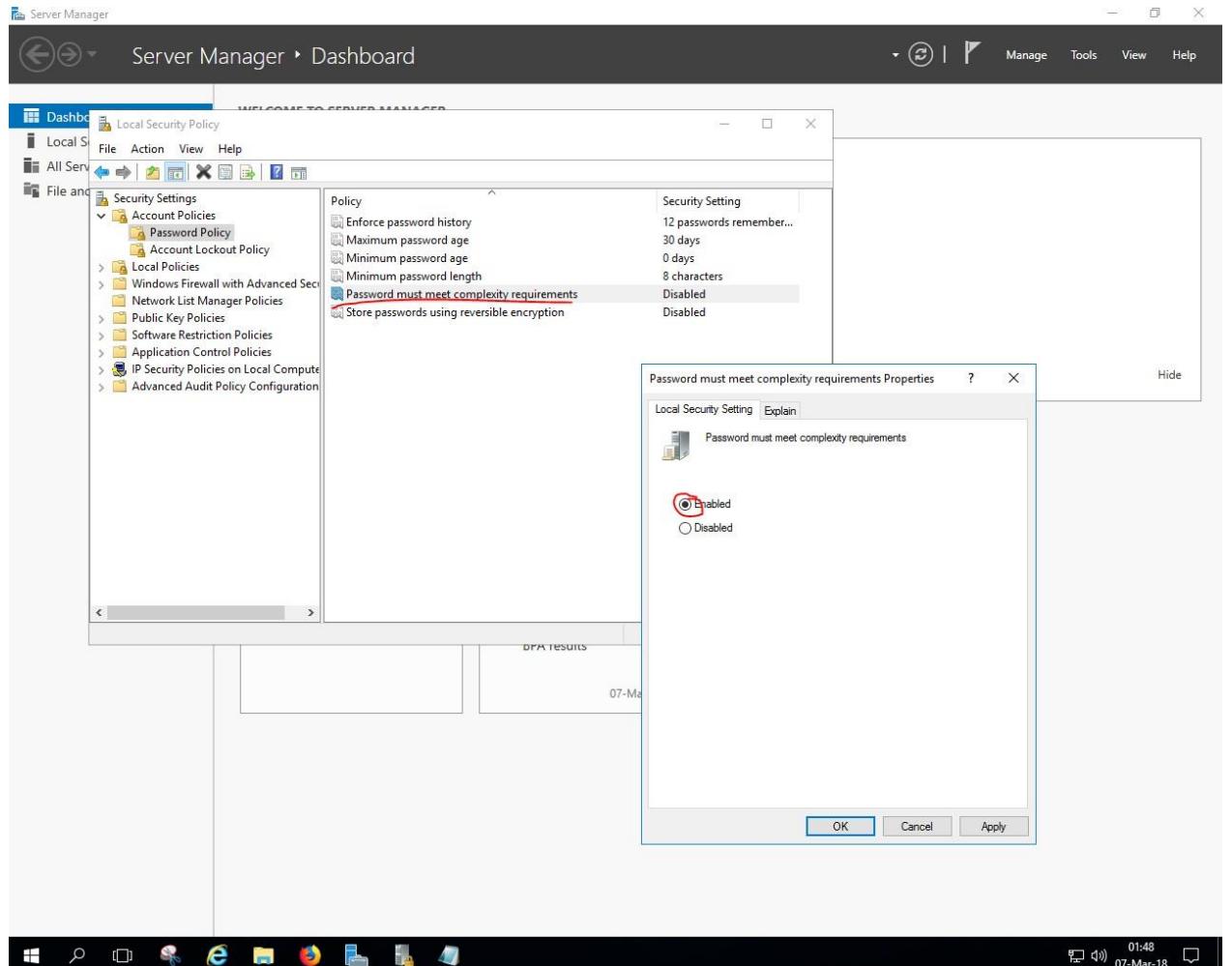
Ο συνδυασμός των δύο παραπάνω πολιτικών ασφάλειας, «αναγκάζει» τους χρήστες να αλλάζουν κωδικό πρόσβασης κάθε 30 μέρες, και σε διάστημα ενός χρόνου να μην χρησιμοποιήσει κάποιον ίδιο κωδικό.

Το minimum password age το αφήνω 0, διότι δεν υπάρχει κανένα πρόβλημα αν κάποιος χρήστης θέλει να αλλάξει τον κωδικό του κάθε μέρα.



Στην συνέχεια θέτω minimum password length = 8, υποχρεώνοντας τους χρήστες να επιλέγουν κωδικούς πρόσβασης με τουλάχιστον 8 χαρακτήρες. Οι 8 χαρακτήρες πιστεύω δεν είναι ούτε λίγοι αλλά ούτε πολλοί, βοηθώντας τους χρήστες που επιλέγουν τον ελάχιστον αριθμό χαρακτήρων για κωδικούς να τους θυμούνται πιο εύκολα.

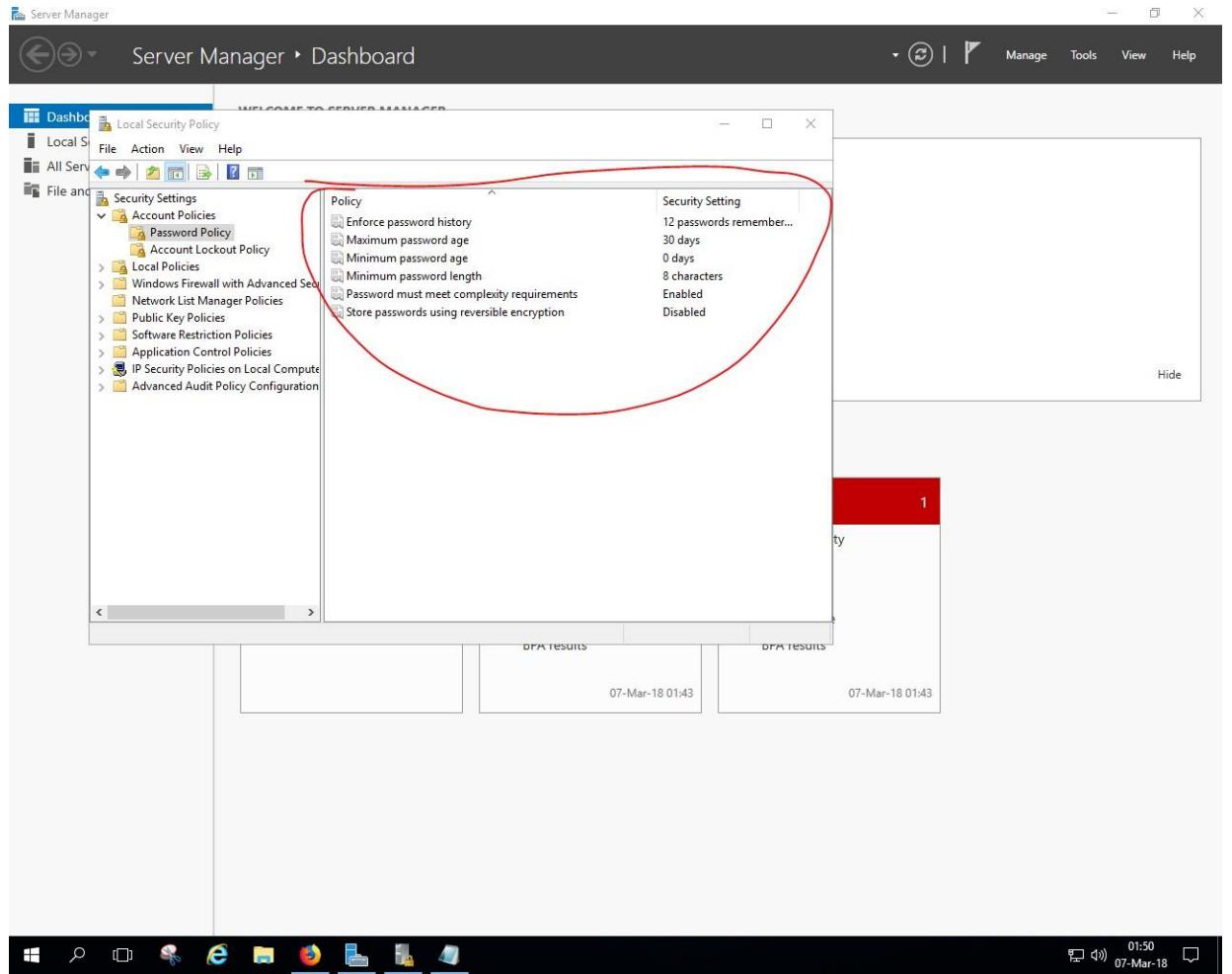
Η επόμενη πολιτική ασφάλειας συνθηματικών αποτελεί θεωρώ την πιο σημαντική σε σχέση με τις υπόλοιπες :



Η πολιτική password must meet complexity requirements από default ήταν ενεργοποιημένη (εξήγησα παραπάνω γιατί την απενεργοποίησα). Αυτή η επιλογή έχει να κάνει με την περιπλοκότητα ενός κωδικού. Είναι ευρέως γνωστό ότι όσο πιο περίπλοκος είναι ένας κωδικός τόσο πιο δύσκολο «σπάει».

Για την επόμενη πολιτική store passwords using reverse encryption δεν έκανα καμία παραμετροποίηση και την άφησα «Disabled». Η ίδια Microsoft προτείνει να αφήσουμε την επιλογή σε Disabled, παρά μόνο όταν θέλουμε να χρησιμοποιήσουμε το CHAP (Challenge-Handshake Authentication Protocol) πρωτόκολλο.

Παρακάτω φαίνονται όλες οι πολιτικές ασφάλειας συνθηματικών και οι παραμετροποιήσεις τους :

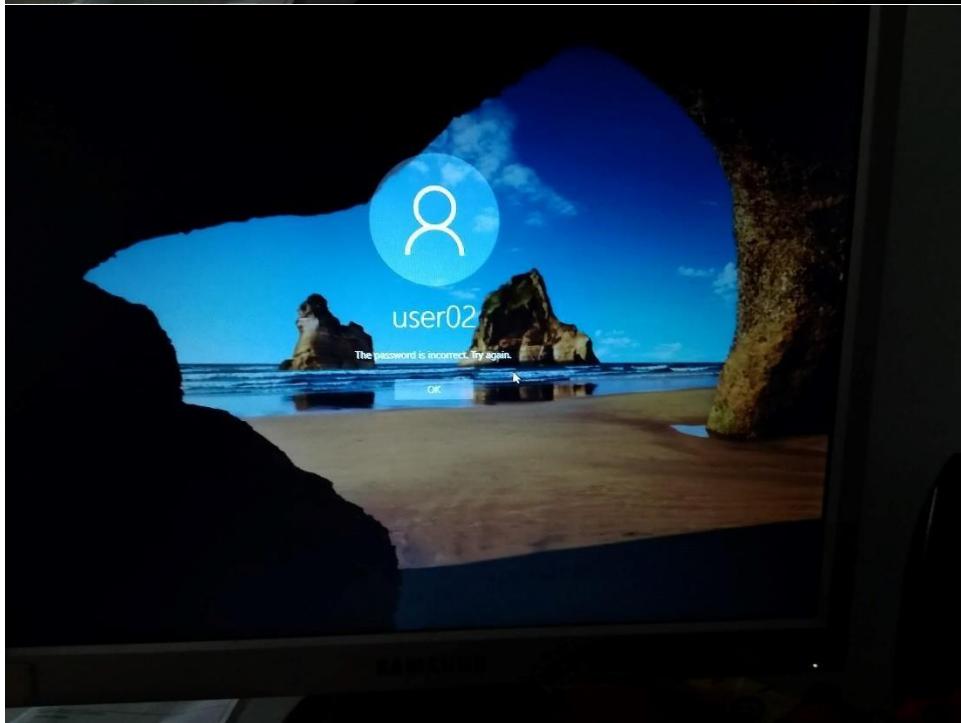
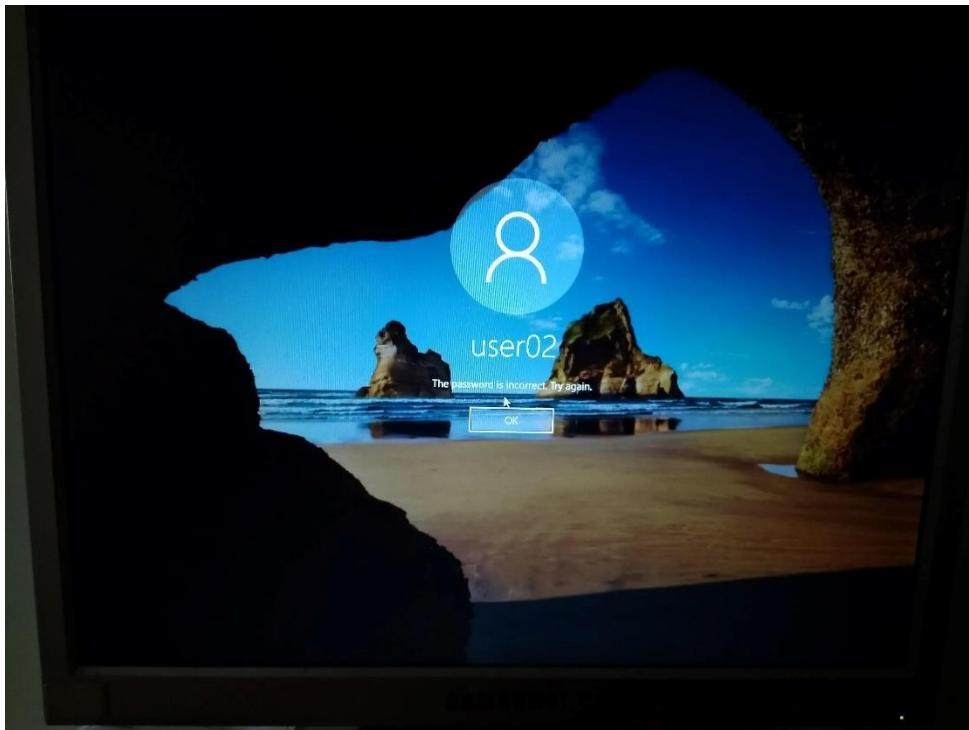


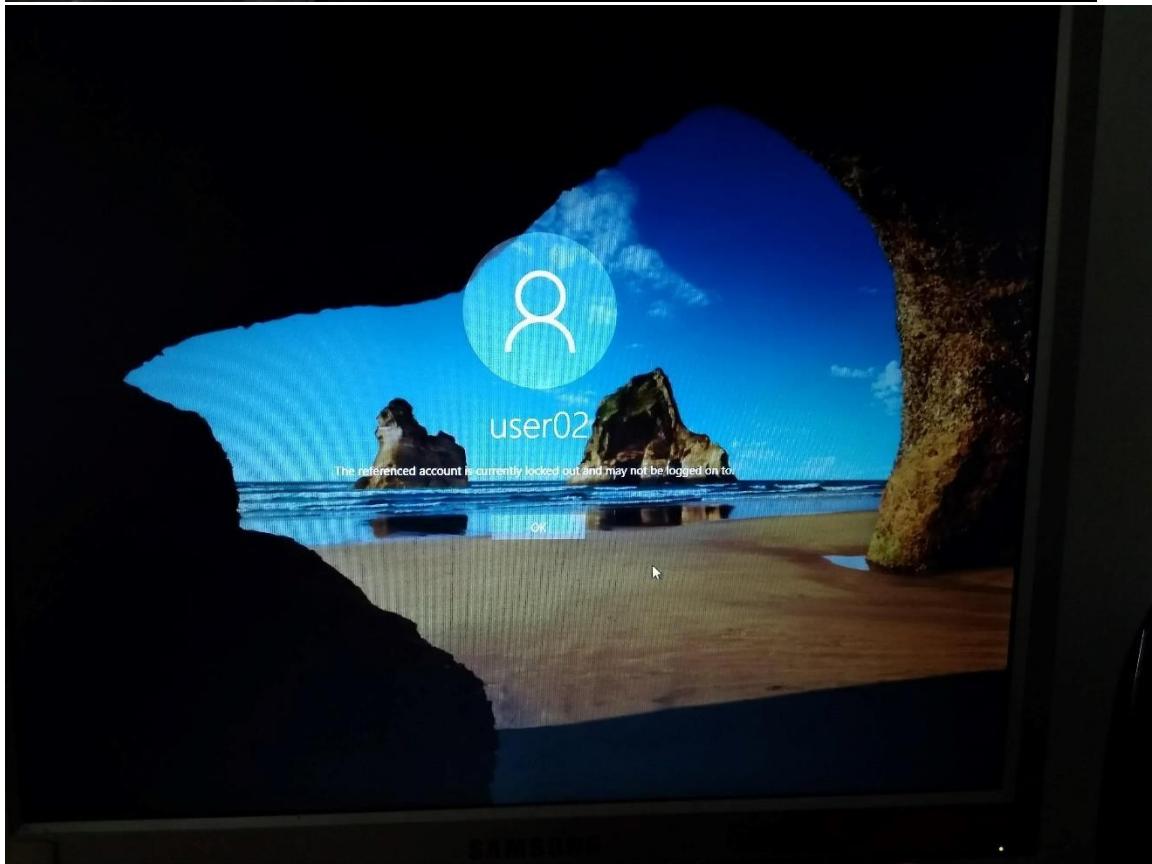
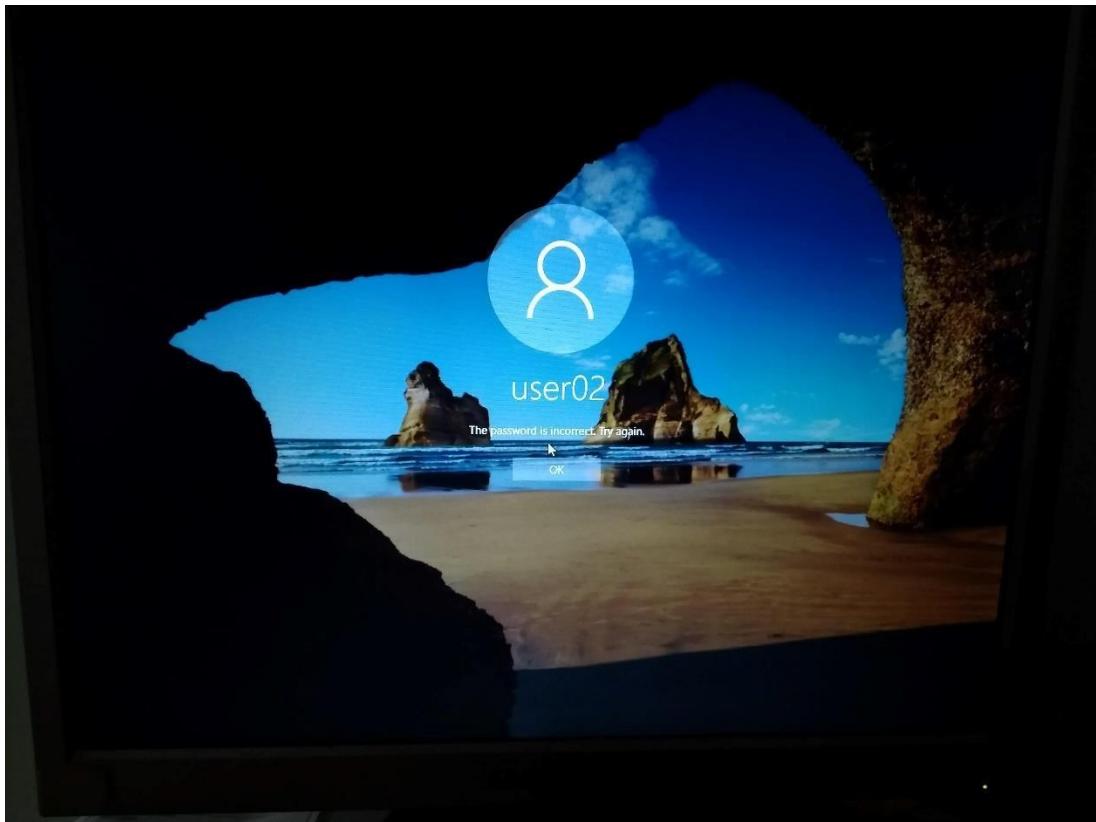
1.4 Έλεγχος κάποιων πολιτικών ασφαλείας

Αρχικά συνδέομαι στον χρήστη user01 με συνθηματικό 123456, και όλα είναι εντάξει.



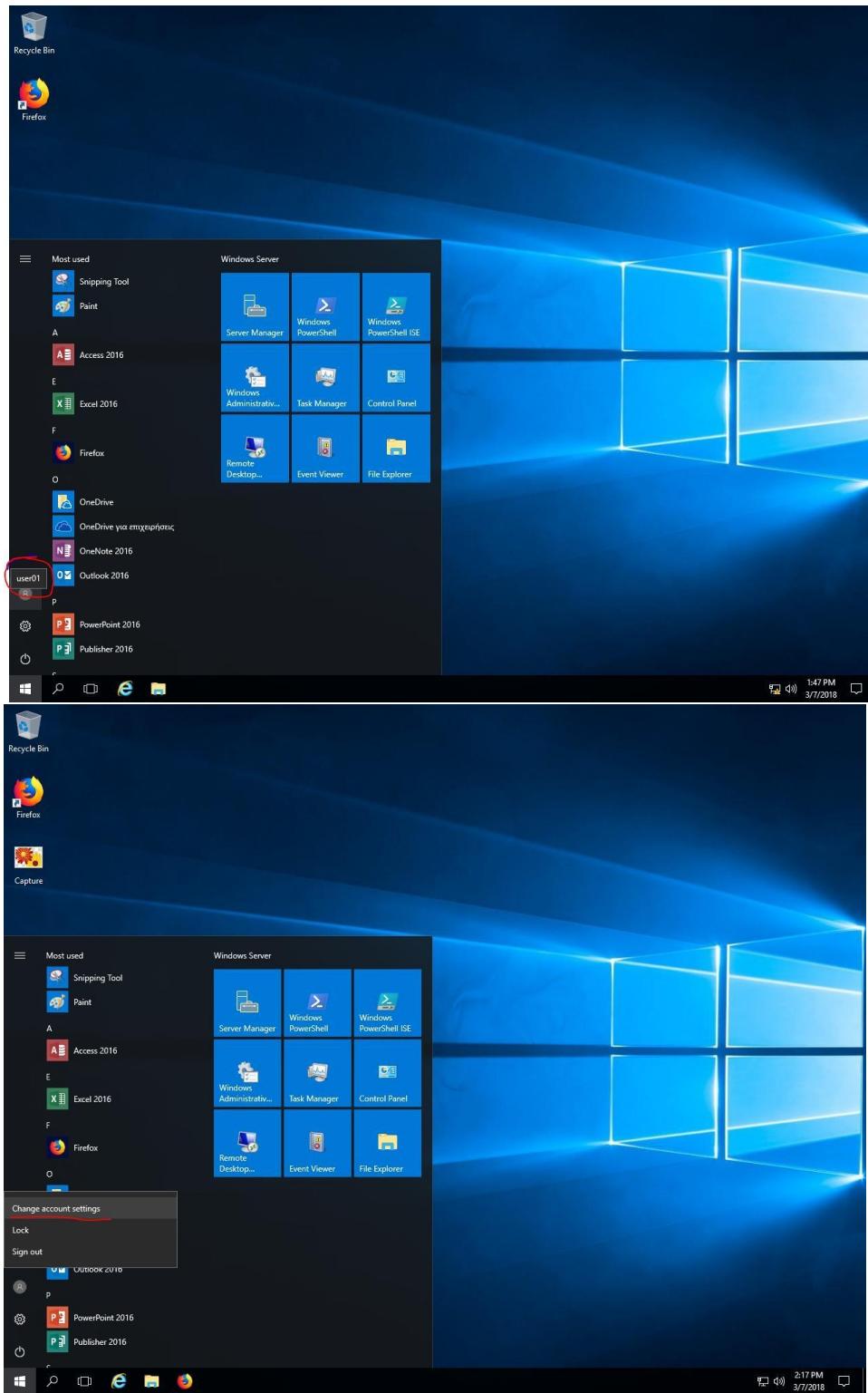
Στην συνέχεια για να ελέγξω το account lockout threshold = 3, έβαζα συνεχώς λάθος συνθηματικό στον user02

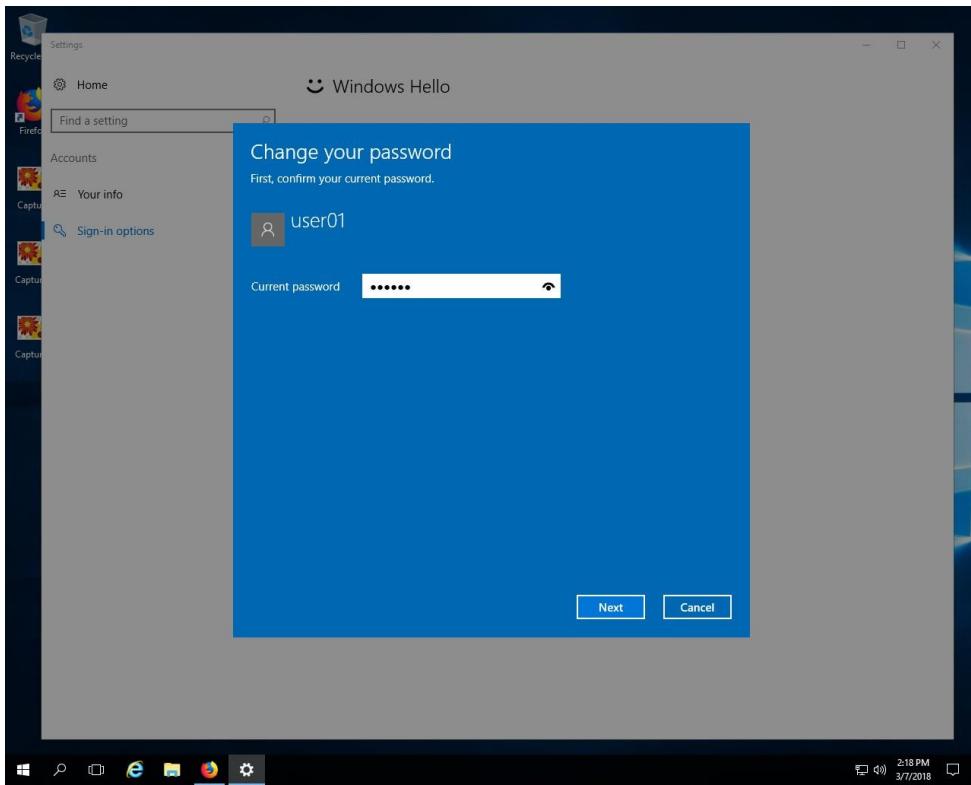
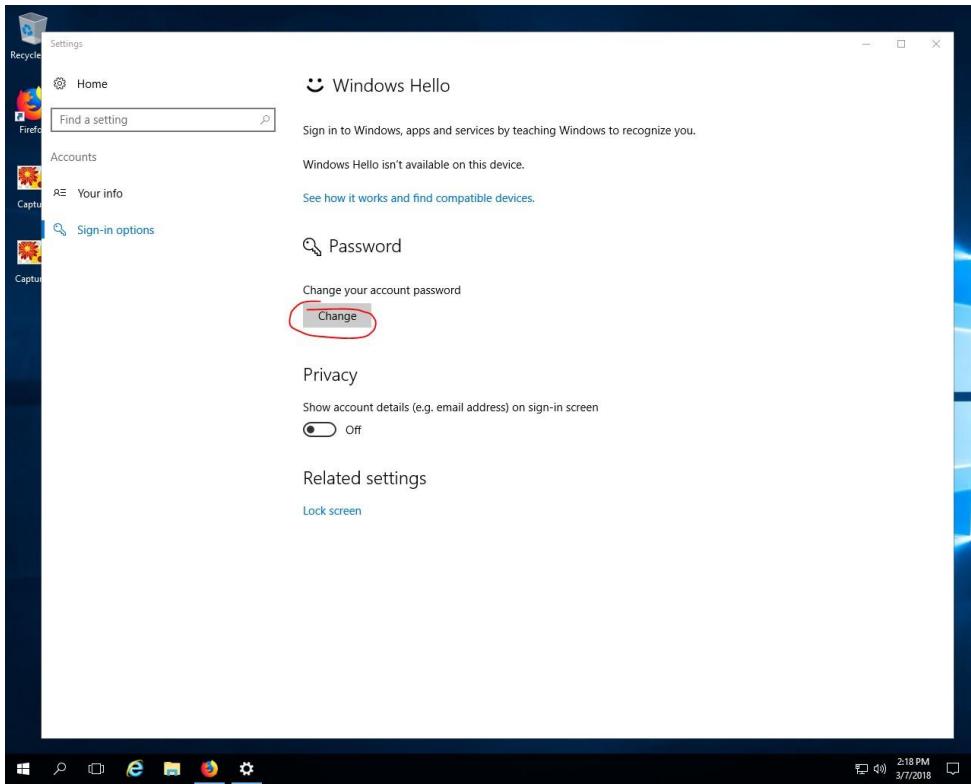


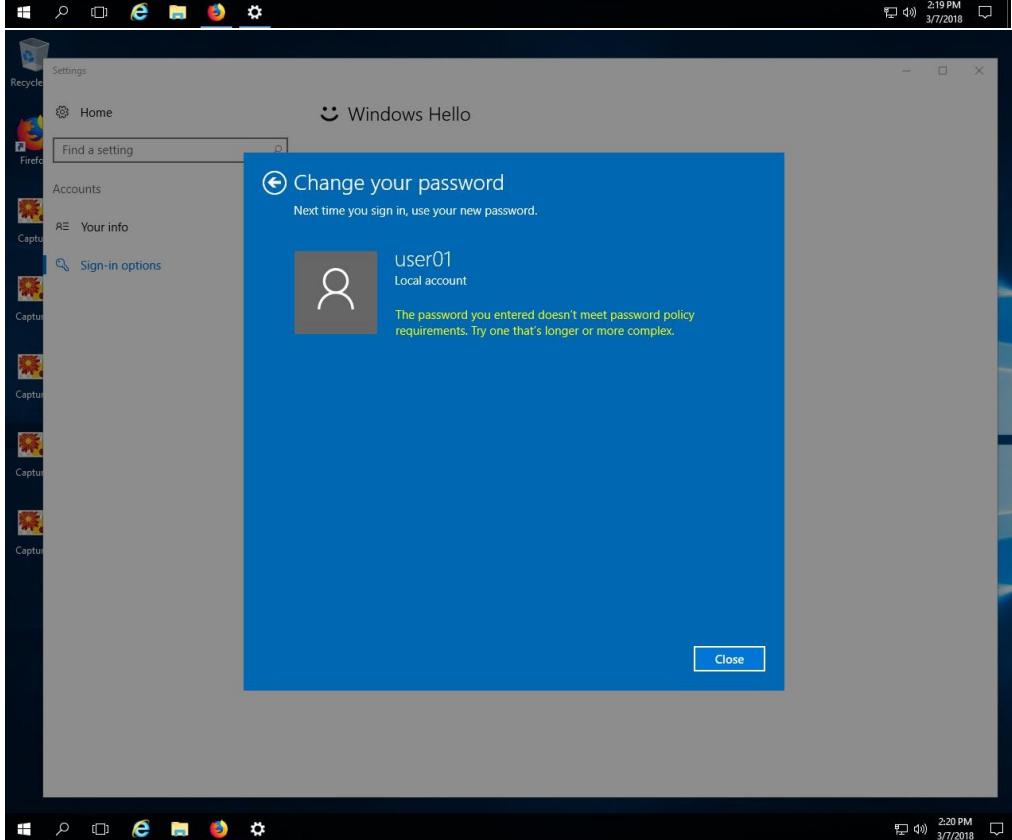
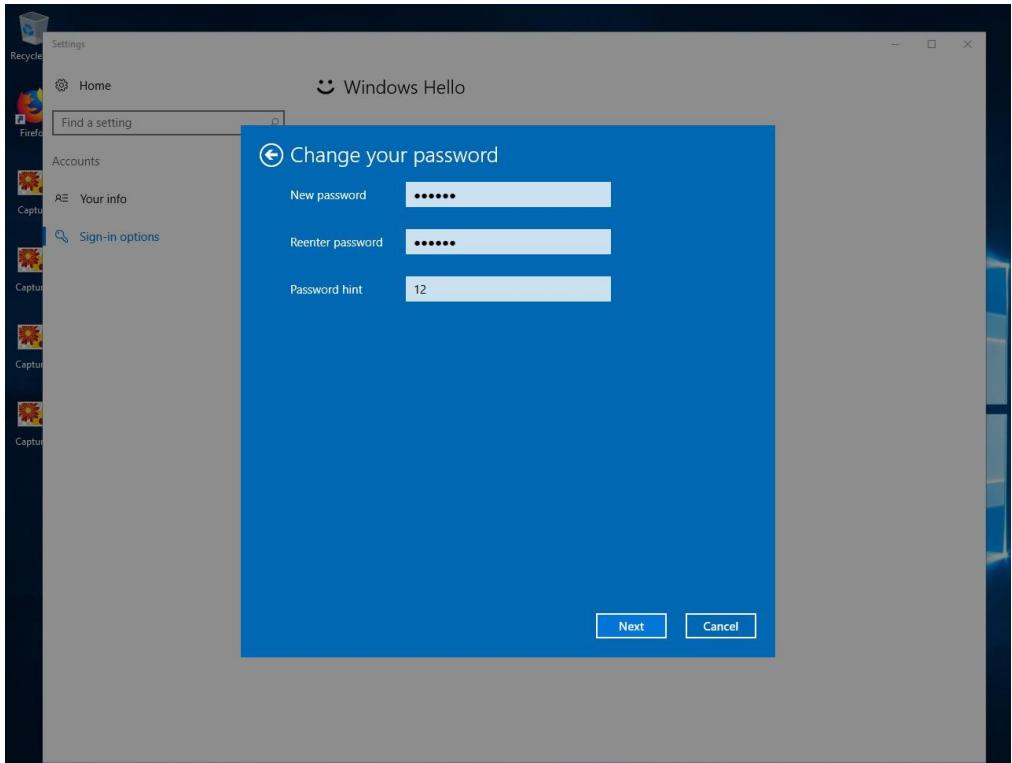


Βλέπουμε ότι οι ρυθμίσεις στο account lockout threshold δουλέψανε επιτυχώς.

Στην συνέχεια συνδέθηκα στον user01 και προσπάθησα να αλλάξω τον κωδικό πρόσβασης του σε 456123 (συνθηματικό το οποίο προφανώς εναντιώνεται στην πολιτική ασφάλειας “password must meet complexity requirements” (πολυπλοκότητα)







Βλέπουμε ότι και αυτή την φορά ενεργοποιήθηκε η πολιτική ασφάλειας και δεν επέτρεψε στον user01 να χρησιμοποιήσει ένα τόσο απλό συνθηματικό όπως το 456123.

1.5 Θεωρητικά Ερωτήματα

- Είναι αρκετά σημαντικό να γίνεται καταγραφή γεγονότων σε ένα λειτουργικό σύστημα. Με αυτό τον τρόπο οι διαχειριστές έχουν το όσον πιο δυνατό καλύτερο έλεγχο του συστήματος. Αυτό συνεπάγεται και καλύτερη οργάνωση του συστήματος. Για παράδειγμα, σε μια εταιρία που διαχειρίζεται μια βάση δεδομένων ενός πελάτη, αν χαθούν δεδομένα με την καταγραφή γεγονότων οι διαχειριστές θα ξέρουν τι έγινε, ή ποιος ευθύνεται για αυτή την κατάσταση και πιθανώς τι δεδομένα χάθηκαν.

Επίσης, τα πάντα θα πρέπει να καταγράφονται σε περισσότερα από ένα αρχείο καταγραφής έτσι ώστε να είναι δύσκολα προσβάσιμα από κάποιον τρίτο(πχ hacking). Αν υπήρχε ένα αρχείο καταγραφής και το σύστημα έπεφτε θύμα hacking, με την εύρεση μόλις ενός αρχείου ο χακερ θα ήξερε τι γινόταν σε όλο το σύστημα.

- Η λειτουργία κλειδώματος λογαριασμού μετά από συγκεκριμένο αριθμό προσπαθειών σύνδεσης είναι αρκετά σημαντική. Αν για παράδειγμα κάποιος χακερ προσπαθεί να υποκλέψει ένα συνθηματικό είναι αρκετά σημαντικό αυτές οι προσπάθειες που έχει, να είναι λίγες (πχ 3, όπως όρισα και εγώ παραπάνω στον server).

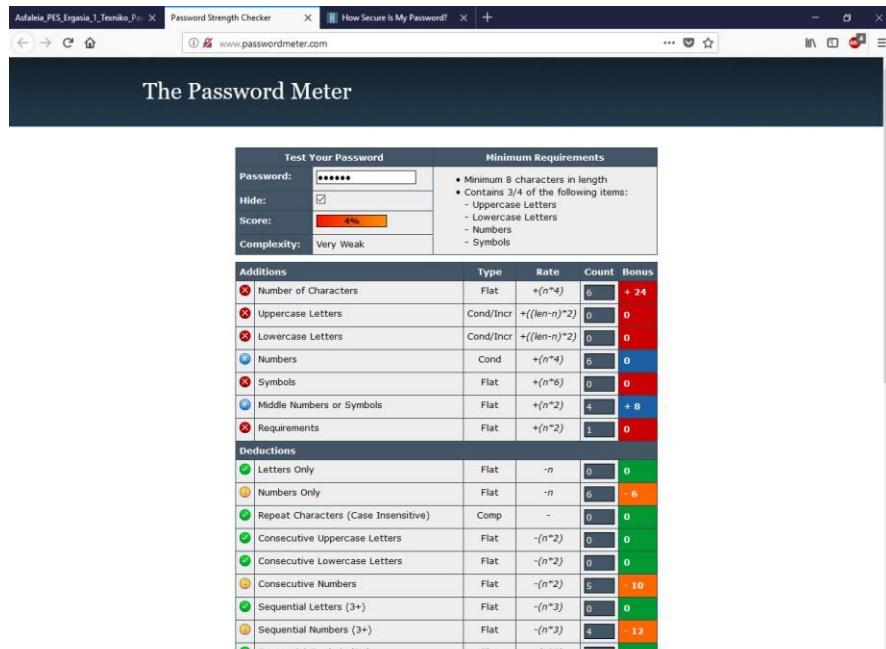
Η διάρκεια κλειδώματος είναι και αυτή σημαντική. Αν για παράδειγμα θέταμε την διάρκεια κλειδώματος με 1 ώρα, τότε ο οποιοσδήποτε χακερ θα μπορούσε να ξαναπροσπαθήσει να υποκλέψει τον κωδικό και να δοκιμάσει νέους συνδυασμούς μετά από μια ώρα. Στην περίπτωση του server μας, αν κλειδώσει κάποιος λογαριασμός πρέπει αναγκαστικά να επέμβει κάποιος διαχειριστής του συστήματος και να ξεκλειδώσει τον λογαριασμό.

- Η δυνατότητα του Λειτουργικού Συστήματος με το να διατηρεί ιστορικό συνθηματικών, «αναγκάζει» τον χρήστη να μην χρησιμοποιεί ίδιους κωδικούς σε σύγκριση με το διάστημα για το οποίο έχει διατηρηθεί ιστορικό συνθηματικών. Αυτή είναι μια αρκετά σημαντική πολιτική ασφάλειας που βοηθάει αρκετά στην ασφάλεια ενός λογαριασμού.
- Η προεπιλεγμένη ρύθμιση στο λειτουργικό των Windows επιτρέπει στον χρήστη να διατηρήσει μόνιμα το ίδιο συνθηματικό. Τα windows ωστόσο έχουν την δυνατότητα να διατηρήσουν έως 24 συνθηματικά για κάθε χρήστη.

2. Διαχείριση των συνθηματικών – Μελέτη επιθέσεων

2.1 Έλεγχος συνθηματικών

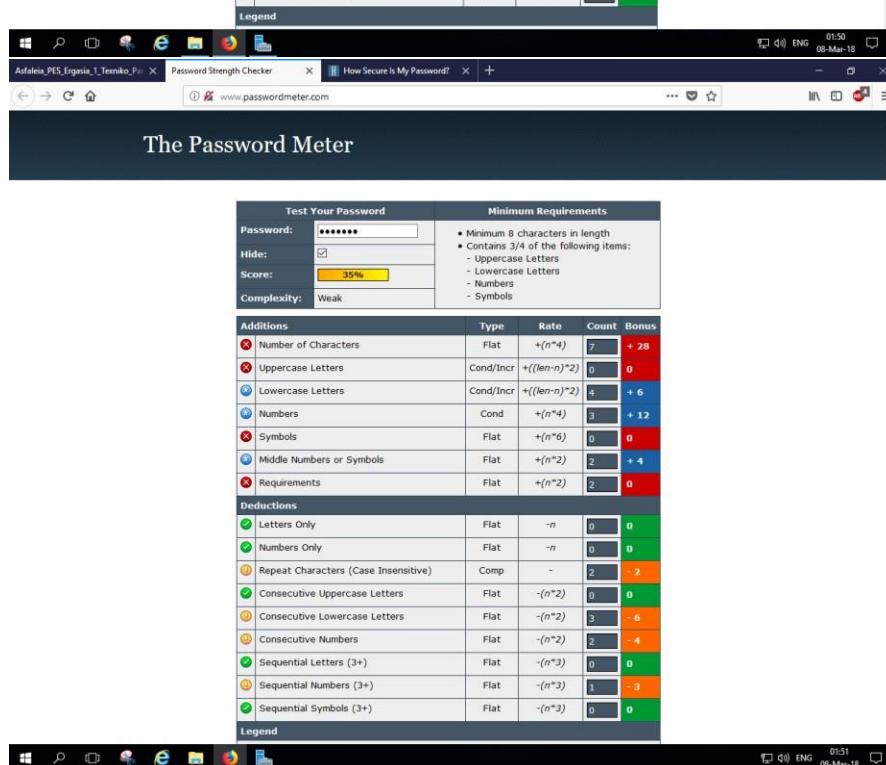
- Στην σελίδα <http://www.passwordmeter.com/> έβαλα τα συνθηματικά που δόθηκαν από το 1ο ερώτημα με την σειρά :



The screenshot shows the 'Test Your Password' section with a password of '*****'. The 'Score:' is 4%, labeled 'Very Weak'. The 'Minimum Requirements' section lists:

- Minimum 5 characters in length
- Contains 3/4 of the following items:
 - Uppercase Letters
 - Lowercase Letters
 - Numbers
 - Symbols

The 'Additions' table shows the password meets requirements for uppercase letters (0), lowercase letters (0), numbers (0), and symbols (0). The 'Deductions' table shows it fails requirements for letters only (0), numbers only (0), and repeat characters (0).



The screenshot shows the 'Test Your Password' section with a password of '*****'. The 'Score:' is 35%, labeled 'Weak'. The 'Minimum Requirements' section lists:

- Minimum 8 characters in length
- Contains 3/4 of the following items:
 - Uppercase Letters
 - Lowercase Letters
 - Numbers
 - Symbols

The 'Additions' table shows the password meets requirements for uppercase letters (0), lowercase letters (4), numbers (0), and symbols (0). The 'Deductions' table shows it fails requirements for letters only (0), numbers only (0), and repeat characters (0).

The Password Meter

Test Your Password		Minimum Requirements				
Password:	*****	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols 				
Hide:	<input checked="" type="checkbox"/>	Score:	100%			
Complexity:	Very Strong					
Additions						
<input checked="" type="radio"/>	Number of Characters	Flat	+ (n^4)	12	+ 48	
<input checked="" type="radio"/>	Uppercase Letters	Cond/Incr	+ $((len-n)^2)$	3	+ 18	
<input checked="" type="radio"/>	Lowercase Letters	Cond/Incr	+ $((len-n)^2)$	6	+ 12	
<input checked="" type="radio"/>	Numbers	Cond	+ (n^4)	0	0	
<input checked="" type="radio"/>	Symbols	Flat	+ (n^6)	3	+ 18	
<input checked="" type="radio"/>	Middle Numbers or Symbols	Flat	+ (n^2)	2	+ 4	
<input checked="" type="radio"/>	Requirements	Flat	+ (n^2)	4	+ 8	
Deductions						
<input checked="" type="radio"/>	Letters Only	Flat	- n	0	0	
<input checked="" type="radio"/>	Numbers Only	Flat	- n	0	0	
<input checked="" type="radio"/>	Repeat Characters (Case Insensitive)	Comp	-	2	- 2	
<input checked="" type="radio"/>	Consecutive Uppercase Letters	Flat	- (n^2)	0	0	
<input checked="" type="radio"/>	Consecutive Lowercase Letters	Flat	- (n^2)	3	- 6	
<input checked="" type="radio"/>	Consecutive Numbers	Flat	- (n^2)	0	0	
<input checked="" type="radio"/>	Sequential Letters (3+)	Flat	- (n^3)	0	0	
<input checked="" type="radio"/>	Sequential Numbers (3+)	Flat	- (n^3)	0	0	
<input checked="" type="radio"/>	Sequential Symbols (3+)	Flat	- (n^3)	0	0	
Legend						
<input checked="" type="radio"/>	Requirement	Flat	+ (n^2)	4	+ 8	
<input checked="" type="radio"/>	Reduction	Flat	- n	0	0	
<input checked="" type="radio"/>	Neutral	Flat	0	0	0	

The Password Meter

Τα αντίστοιχα συνθηματικά με την ίδια σειρά

The screenshot shows a browser window with the URL <https://howsecureismypassword.net>. The main heading is "HOW SECURE IS MY PASSWORD?". A large red box displays the result: "Your password would be cracked **INSTANTLY**". Below this, a tip suggests using Dashlane. The page then lists several common password patterns as weaknesses:

- TIP: USE A PASSWORD MANAGER TO SECURE AND EASILY REMEMBER YOUR PASSWORDS**
- COMMON PASSWORD: IN THE TOP 5 MOST USED PASSWORDS**
- LENGTH: VERY SHORT**
- CHARACTER VARIETY: JUST NUMBERS**
- POSSIBLY A TELEPHONE NUMBER / DATE**

The screenshot shows a browser window with the URL <https://howsecureismypassword.net>. The main heading is "HOW SECURE IS MY PASSWORD?". A large red box displays the result: "Your password would be cracked **INSTANTLY**". Below this, a tip suggests using Dashlane. The page then lists several common password patterns as weaknesses:

- TIP: USE A PASSWORD MANAGER TO SECURE AND EASILY REMEMBER YOUR PASSWORDS**
- COMMON PASSWORD: IN THE TOP 2775 MOST USED PASSWORDS**
- POSSIBLY A WORD AND A NUMBER**
- LENGTH: SHORT**
- CHARACTER VARIETY: NO SYMBOLS**

The image displays two nearly identical screenshots of the [How Secure Is My Password?](https://howsecureismypassword.net/) website, captured at different times. Both screenshots show a password strength of 12 characters, represented by 12 black dots in a horizontal bar.

Top Screenshot (Captured 08-Mar-18 15:12):

- Header:** HOW SECURE IS MY PASSWORD?
- Strength Bar:** 12 dots (representing 12 characters).
- Text Box:** It would take a computer about **1 QUINTILLION YEARS** to crack your password. Dashlane can help you remember all of your secure passwords - and it's free! [Tweet Your Result](#)
- TIP:** USE A PASSWORD MANAGER TO SECURE AND EASILY REMEMBER YOUR PASSWORDS
- Text Box:** "Dashlane is life changingly great. Get it." - David Pogue (The New York Times) [Get Dashlane - It's Free!](#)

Bottom Screenshot (Captured 08-Mar-18 15:12):

- Header:** HOW SECURE IS MY PASSWORD?
- Strength Bar:** 12 dots (representing 12 characters).
- Text Box:** It would take a computer about **1 QUINTILLION YEARS** to crack your password. Dashlane can help you remember all of your secure passwords - and it's free! [Tweet Your Result](#)
- TIP:** USE A PASSWORD MANAGER TO SECURE AND EASILY REMEMBER YOUR PASSWORDS
- Text Box:** "Dashlane is life changingly great. Get it." - David Pogue (The New York Times) [Get Dashlane - It's Free!](#)

Στην συνέχεια χρησιμοποίησα και στα 2 παραπάνω site ένα τυχαίο συνθηματικό «sU3k!g6#Wm0» και βγήκαν τα παρακάτω αποτελέσματα :

The Password Meter

Test Your Password		Minimum Requirements			
Password:	<input type="password" value="*****"/>	<ul style="list-style-type: none"> • Minimum 8 characters in length • Contains 3/4 of the following items: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers - Symbols 			
Hide:	<input checked="" type="checkbox"/>				
Score:	<div style="width: 100%;">100%</div>				
Complexity:	Very Strong				
Additions					
<input checked="" type="radio"/> Number of Characters	Type	Flat	Rate	+ (n^4)	Count 11 + 44
<input checked="" type="radio"/> Uppercase Letters	Type	Cond/Incr	Rate	+ $((len-n)^2)$	Count 2 + 18
<input checked="" type="radio"/> Lowercase Letters	Type	Cond/Incr	Rate	+ $((len-n)^2)$	Count 4 + 14
<input checked="" type="radio"/> Numbers	Type	Cond	Rate	+ (n^4)	Count 3 + 12
<input checked="" type="radio"/> Symbols	Type	Flat	Rate	+ (n^6)	Count 2 + 12
<input checked="" type="radio"/> Middle Numbers or Symbols	Type	Flat	Rate	+ (n^2)	Count 4 + 8
<input checked="" type="radio"/> Requirements	Type	Flat	Rate	+ (n^2)	Count 5 + 10
Deductions					
<input checked="" type="checkbox"/> Letters Only	Type	Flat	Rate	- n	Count 0 0
<input checked="" type="checkbox"/> Numbers Only	Type	Flat	Rate	- n	Count 0 0
<input checked="" type="checkbox"/> Repeat Characters (Case Insensitive)	Type	Comp	Rate	-	Count 0 0
<input checked="" type="checkbox"/> Consecutive Uppercase Letters	Type	Flat	Rate	- (n^2)	Count 0 0
<input checked="" type="checkbox"/> Consecutive Lowercase Letters	Type	Flat	Rate	- (n^2)	Count 0 0
<input checked="" type="checkbox"/> Consecutive Numbers	Type	Flat	Rate	- (n^2)	Count 0 0
<input checked="" type="checkbox"/> Sequential Letters (3+)	Type	Flat	Rate	- (n^3)	Count 0 0
<input checked="" type="checkbox"/> Sequential Numbers (3+)	Type	Flat	Rate	- (n^3)	Count 0 0
<input checked="" type="checkbox"/> Sequential Symbols (3+)	Type	Flat	Rate	- (n^3)	Count 0 0

HOW SECURE IS MY PASSWORD?

It would take a computer about
4 HUNDRED YEARS
 to crack your password

Why not create even stronger passwords with Dashlane? It's free!

Sponsored by Dashlane, never forget another password

Like 12K

Sponsored by Dashlane Password Manager
 Top 10 000 passwords by Mark Burnett / Typefaces by The League of Movable Type
 The source code for this site and the official HSMP jQuery plugin can be found on GitHub
 © Small Hadron Collider 2016 / Version 8.0

This site is for educational use. Due to limitations of the technology involved, the results cannot always be accurate. Your password will not be sent over the internet.

Δεδομένου και τον παραπάνω αποτελεσμάτων, τα κύρια χαρακτηριστικά ενός ασφαλούς συνθηματικού είναι ο συνδυασμός τυχαίων χαρακτήρων(κεφαλαία και μη), αριθμών και συμβόλων. Πιο ασφαλές ακόμα γίνεται αν ο τυχαίος αυτός συνδυασμός δεν έχει δύο ίδιου τύπου χαρακτήρες κολλητά (π.χ. δύο κεφαλαία γράμματα στην σειρά). Οπότε γενικά, όσο πιο τυχαίο είναι ένα συνθηματικό και δεν αποτελείτε από κάποια λέξη που βρίσκεται σε οποιοδήποτε λεξικό τόσο πιο ασφαλές είναι!

2.2 Φύλαξη λογαριασμών χρηστών στα Windows

Οι λογαριασμοί των χρηστών στο Λ.Σ. των windows φυλάσσονται στο εξής μονοπάτι : C:\Windows\System32\config. Εκεί βρίσκεται ένα αρχείο με όνομα «SAM». Για να υποκλέψει κάποιος ένα συνθηματικό πρέπει πρώτα να βρει τα hash τα οποία βρίσκονται αποθηκευμένα στο αρχείο SAM. Τα hash των συνθηματικών βρίσκονται επίσης στο αρχείο HKEY_LOCAL_MACHINE\SAM. Και στις δύο περιπτώσεις όμως, τα αρχεία αυτά δεν είναι προσβάσιμα όσο το λειτουργικό σύστημα είναι ενεργό. Για να υποκλέψει όμως ο οποιοδήποτε συνθηματικά υπάρχουν διάφοροι τρόποι οι οποίοι εξαρτώνται από το είδος της πρόσβασης που έχει στο σύστημα.

Τέλος, ένα λειτουργικό σύστημα για να ελέγχει την εγκυρότητα ενός χρήστη, «παίρνει» το hash που δημιουργείτε από την hash function όταν εισάγει συνθηματικό ο χρήστης και το ελέγχει με το hash που είναι αποθηκευμένο σε έναν πίνακα στο σύστημα, και αν είναι τα ίδια, ο χρήστης εισέρχεται στο Λ.Σ. Το σημαντικό σε αυτή την τεχνική είναι ότι οι hash functions δεν κάνουν την αντίστροφη διαδικασία, δεν μπορούν δηλαδή να πάρουν ένα hash και να το μετατρέψουν στον αντίστοιχο κωδικό.

2.3 Τεχνικές αποκάλυψης συνθηματικών

❖ Χρήση Λεξικού (Dictionary Attack)

Η χρήση λεξικού (Dictionary Attack) είναι μια μέθοδος με την οποία μπορείς να υποκλέψεις συνθηματικά σε ένα λειτουργικό σύστημα δοκιμάζοντας κάθε λέξη από ένα λεξικό σαν κωδικό πρόσβασης. Η επιτυχία της συγκεκριμένης μεθόδου βασίζεται στο ότι πολλοί χρήστες ανά τον κόσμο χρησιμοποιούν πολύ απλούς κωδικούς.

❖ Τεχνική Εξαντλητικής Αναζήτησης (Brute Force Attack)

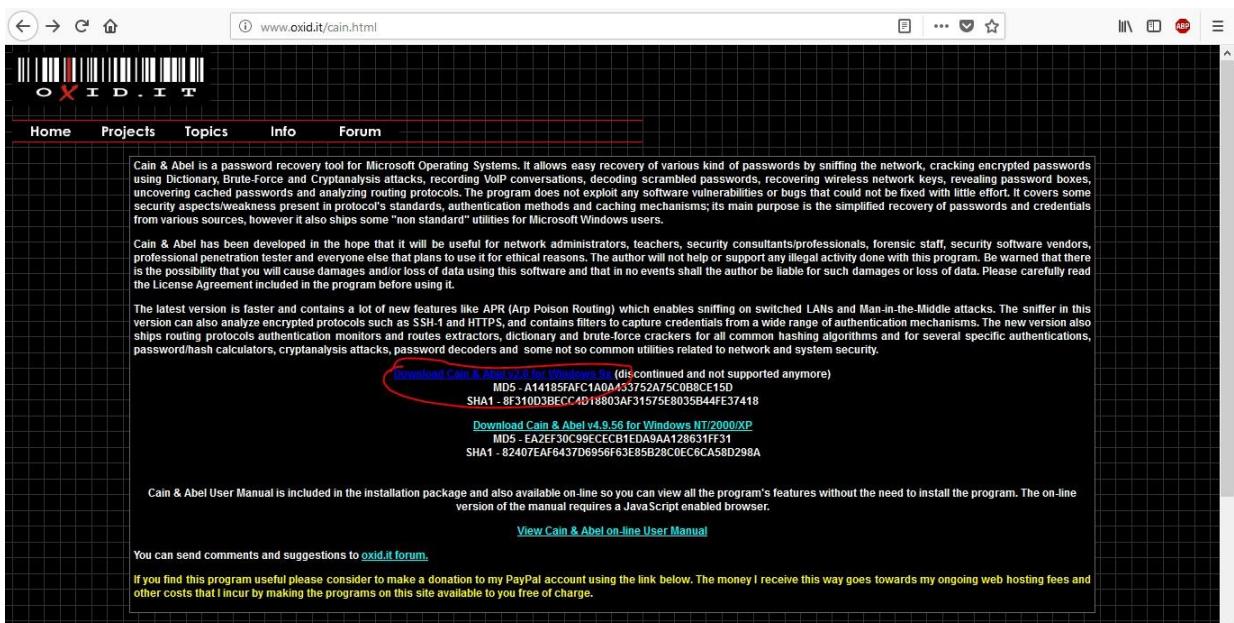
Στην τεχνική εξαντλητικής αναζήτησης (Brute Force Attack), χρησιμοποιείτε ένα αυτοματοποιημένο λογισμικό το οποίο συνεχώς προσπαθεί να μαντέψει σωστά το συνθηματικό του χρήστη που θέλει να υποκλέψει.

❖ Κρυπτανάλυση με χρήση πινάκων Rainbow

Οι πίνακες Rainbow είναι ουσιαστικά ένα λεξικό. Η λογική του όμως, διαφέρει αρκετά από τις προηγούμενες δύο τεχνικές. Γενικά, στους πίνακες Rainbow υπάρχουν ήδη προκαθορισμένα hashes και τα αντίστοιχα συνθηματικά τους. Οι πίνακες αυτοί, επιτρέπουν εν μέρη στους χάκερς να αντιστρέψουν την λειτουργία των hash function, βρίσκοντας το συνθηματικό από το hash. Υπάρχει περίπτωση δύο συνθηματικά να έχουν ίδιο hash, αλλά από την στιγμή που έχει βρεθεί ένα hash που αντιστοιχεί με ένα συνθηματικό στο λειτουργικό σύστημα, δεν έχει καμία σημασία ποιο είναι το συνθηματικό του χρήστη.

2.4 Αναλυτής Συνθηματικών (Password Cracker)

Αρχικά, κατέβασα το Cain & Abel.

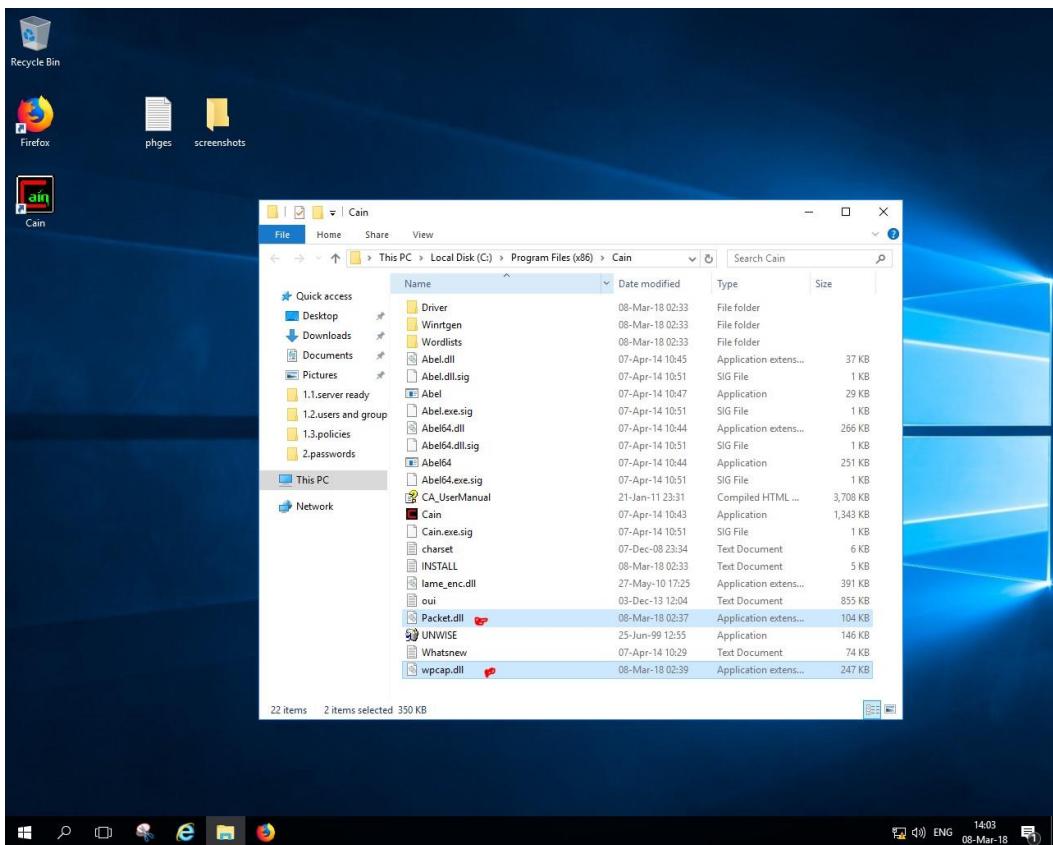




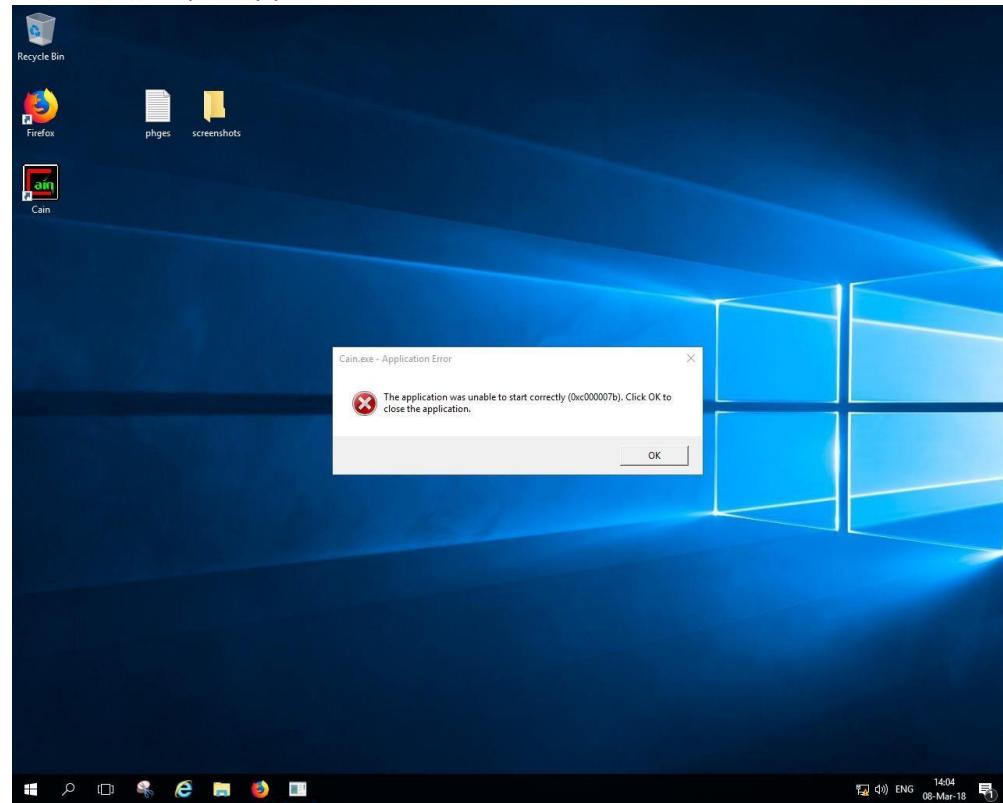
Οπότε κατέβασα την άλλη έκδοση.

A screenshot of a website page for Cain & Abel. The page features a barcode at the top left. A navigation menu includes Home, Projects, Topics, Info, and Forum. The main content area contains a brief description of the tool, its features, and its purpose. It lists two download links: "Download Cain & Abel v2.0 for Windows 3x" and "Download Cain & Abel v4.5.0 for Windows NT/2000/XP". The "Windows NT/2000/XP" link is circled in red. Below the downloads, there's information about the user manual and a donation link.

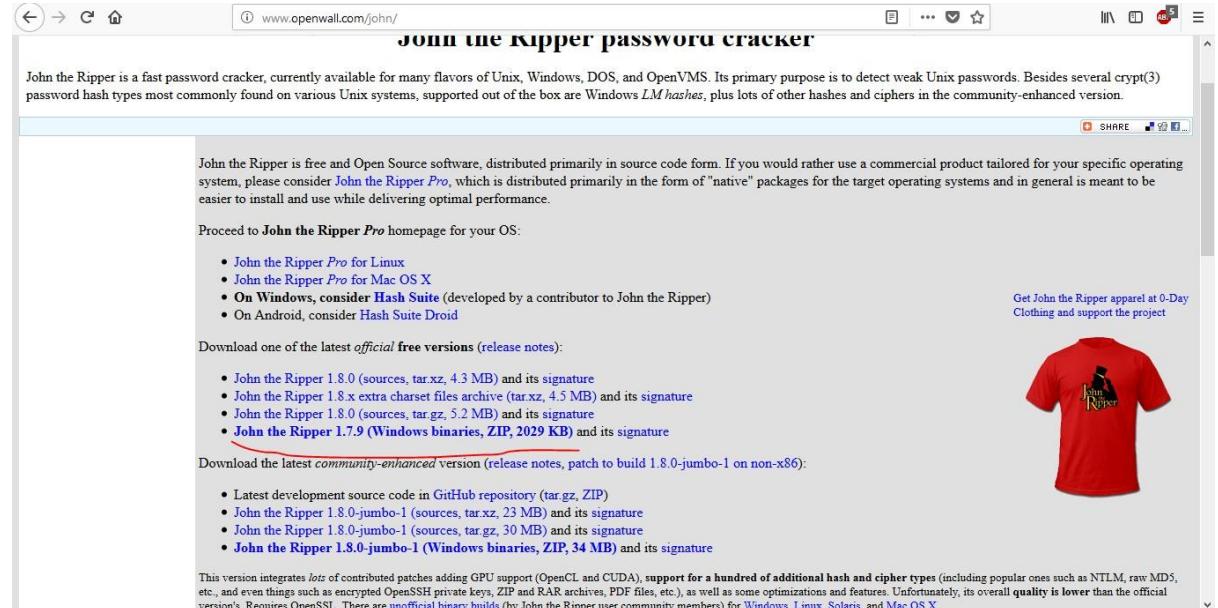
Μετά την εγκατάσταση όμως, όταν πήγα να το «τρέξω» μου εμφάνισε κάποια error που είχαν να κάνουμε με κάποια αρχεία .dll που έλλειπαν. Τα κατέβασα και τα έκανα εγκατάσταση.



Στην συνέχεια μου έβγαλε και άλλο error.

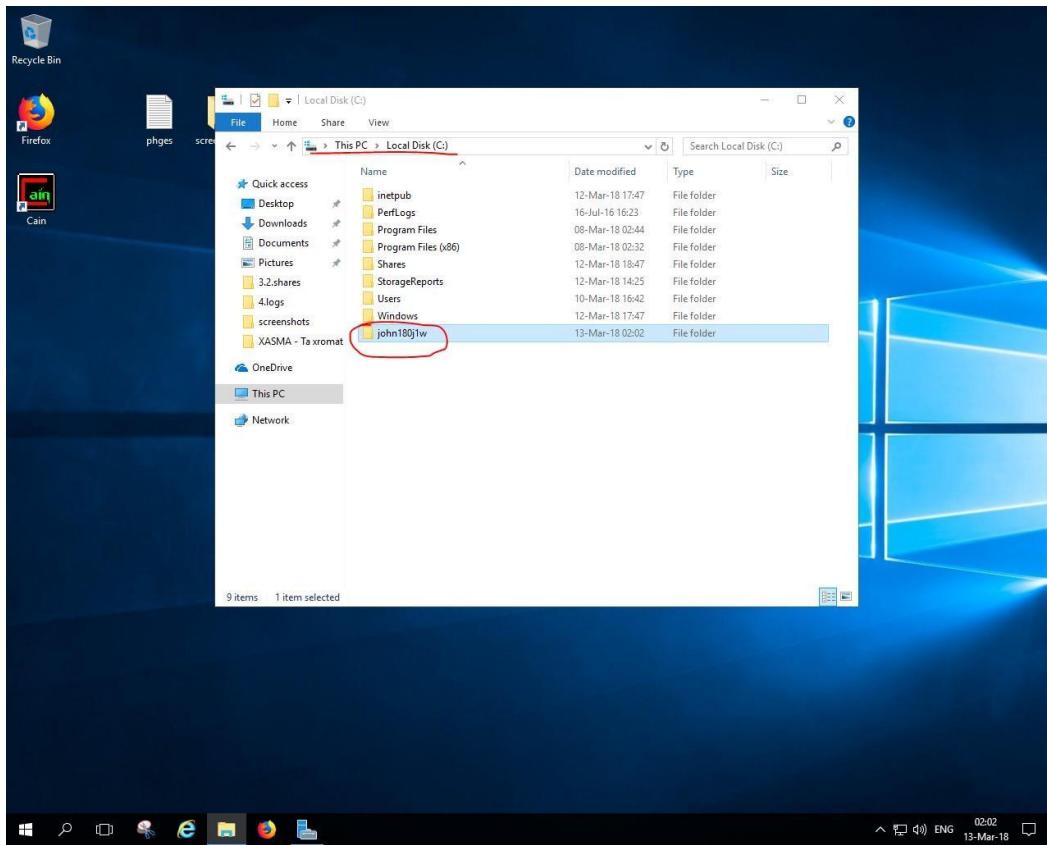
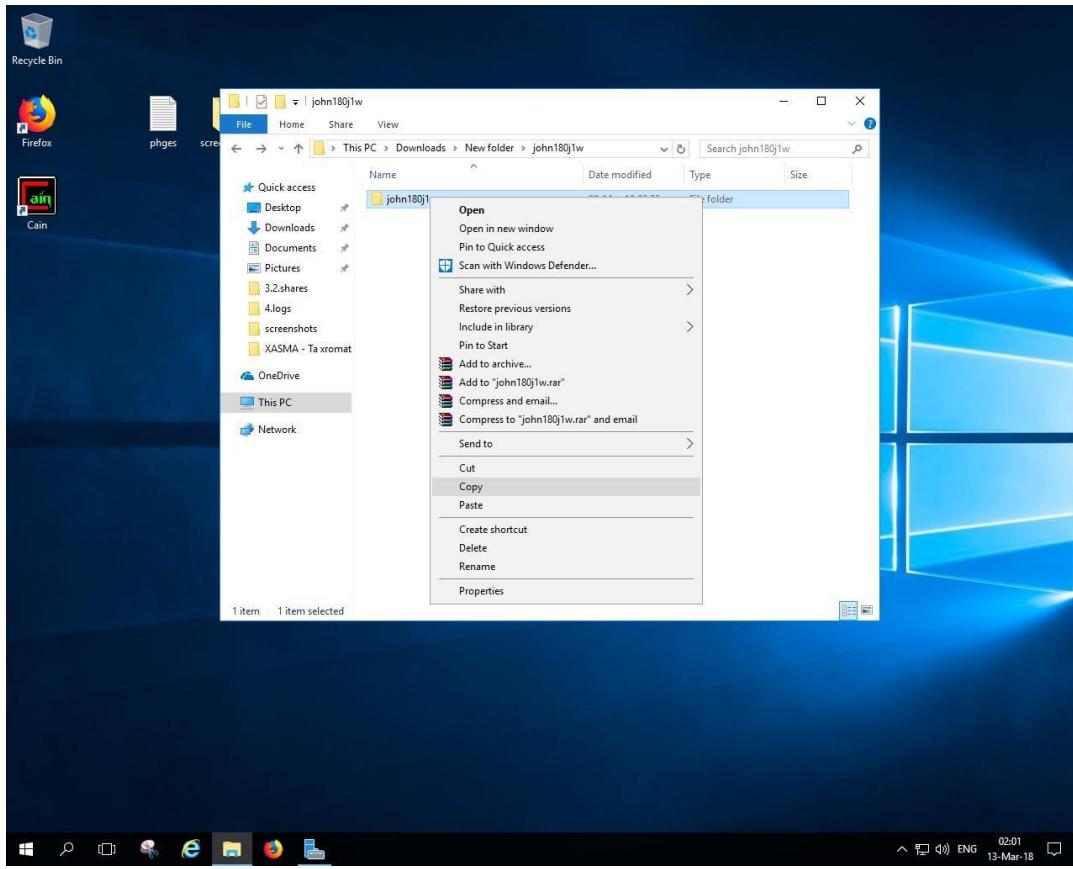


Δοκίμασα διάφορες τεχνικές, μήπως δουλέψει αλλά δεν κατάφερα τίποτα. Είτε έκανα reinstall το πρόγραμμα, είτε επανεκκίνηση στον υπολογιστή, είτε ενημερώσεις στον υπολογιστή, είτε έτρεχα το πρόγραμμα με δικαιώματα διαχειριστή, το αποτέλεσμα ήταν το ίδιο. Οπότε έψαξα διάφορα παρόμοια προγράμματα και τελικά χρησιμοποίησα το «john the reaper».

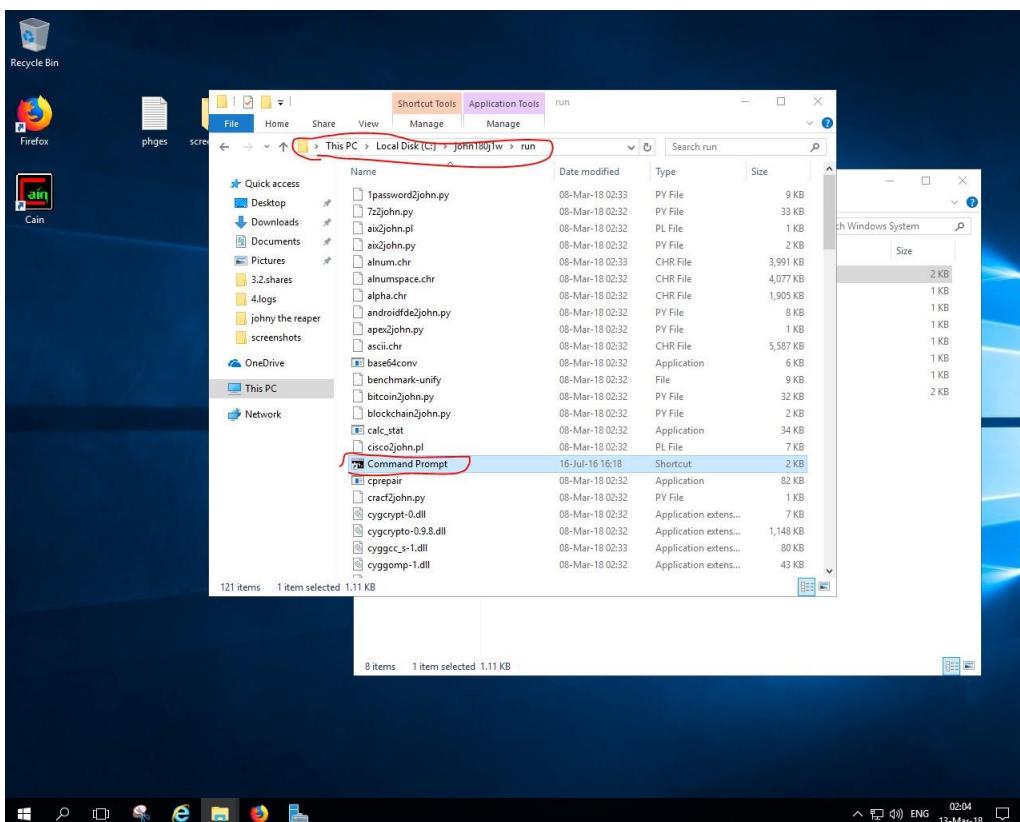
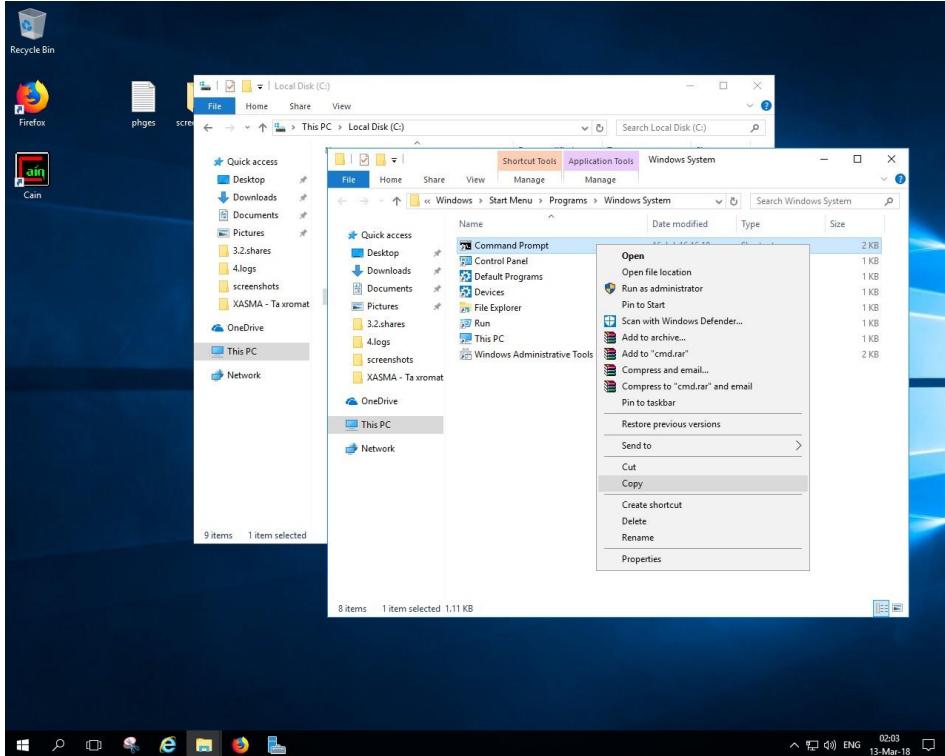


The screenshot shows the official homepage for John the Ripper. At the top, it says "JOHN THE RIPPER PASSWORD CRACKER". Below that, a paragraph explains the software's purpose: "John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version." A "SHARE" button is visible at the top right. In the center, there's a list of download links for different platforms: "Proceed to John the Ripper Pro homepage for your OS:" followed by a bulleted list: "• John the Ripper Pro for Linux", "• John the Ripper Pro for Mac OS X", "• On Windows, consider Hash Suite (developed by a contributor to John the Ripper)", and "• On Android, consider Hash Suite Droid". To the right, a small text link says "Get John the Ripper apparel at 0-Day Clothing and support the project". Below this, another section titled "Download one of the latest official free versions (release notes):" lists four options: "• John the Ripper 1.8.0 (sources, tar.xz, 4.3 MB) and its signature", "• John the Ripper 1.8.x extra charset files archive (tar.xz, 4.5 MB) and its signature", "• John the Ripper 1.8.0 (sources, tar.gz, 5.2 MB) and its signature", and "• John the Ripper 1.7.9 (Windows binaries, ZIP, 2029 KB) and its signature". A red t-shirt with the John the Ripper logo is shown on the right. Further down, a section titled "Download the latest community-enhanced version (release notes, patch to build 1.8.0-jumbo-1 on non-x86):" lists three options: "• Latest development source code in GitHub repository (tar.gz, ZIP)", "• John the Ripper 1.8.0-jumbo-1 (sources, tar.xz, 23 MB) and its signature", and "• John the Ripper 1.8.0-jumbo-1 (sources, tar.gz, 30 MB) and its signature". A note below states: "This version integrates lots of contributed patches adding GPU support (OpenCL and CUDA), support for a hundred of additional hash and cipher types (including popular ones such as NTLM, raw MD5, etc., and even things such as encrypted OpenSSH private keys, ZIP and RAR archives, PDF files, etc.), as well as some optimizations and features. Unfortunately, its overall quality is lower than the official version's. Requires OpenSSL. There are unofficial binary builds (by John the Ripper user community members) for Windows, Linux, Solaris, and Mac OS X."

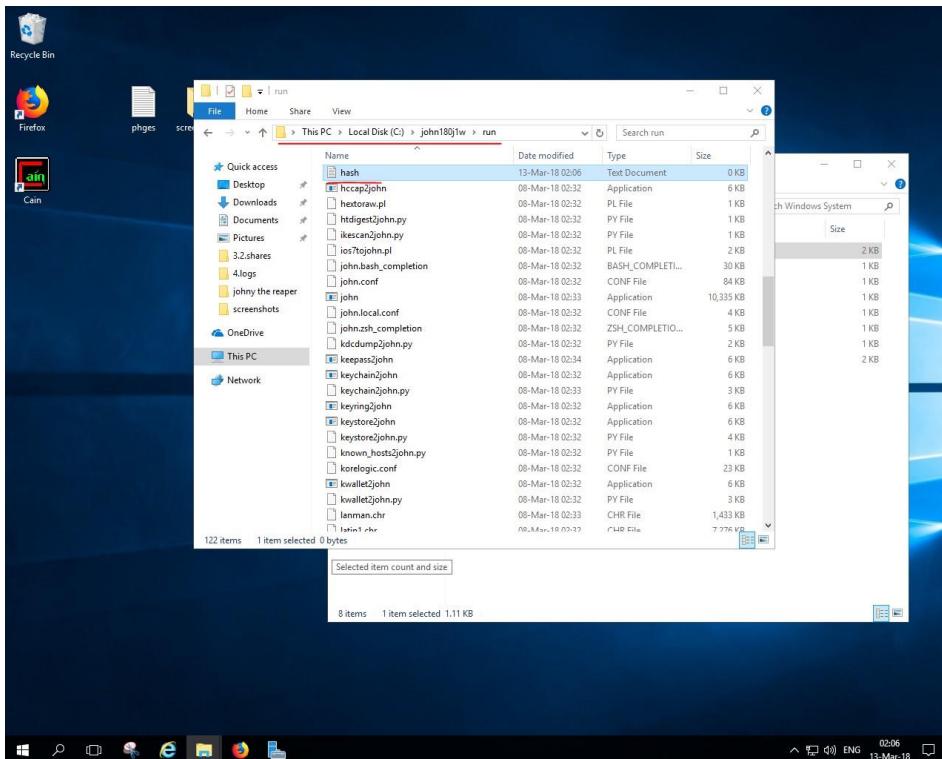
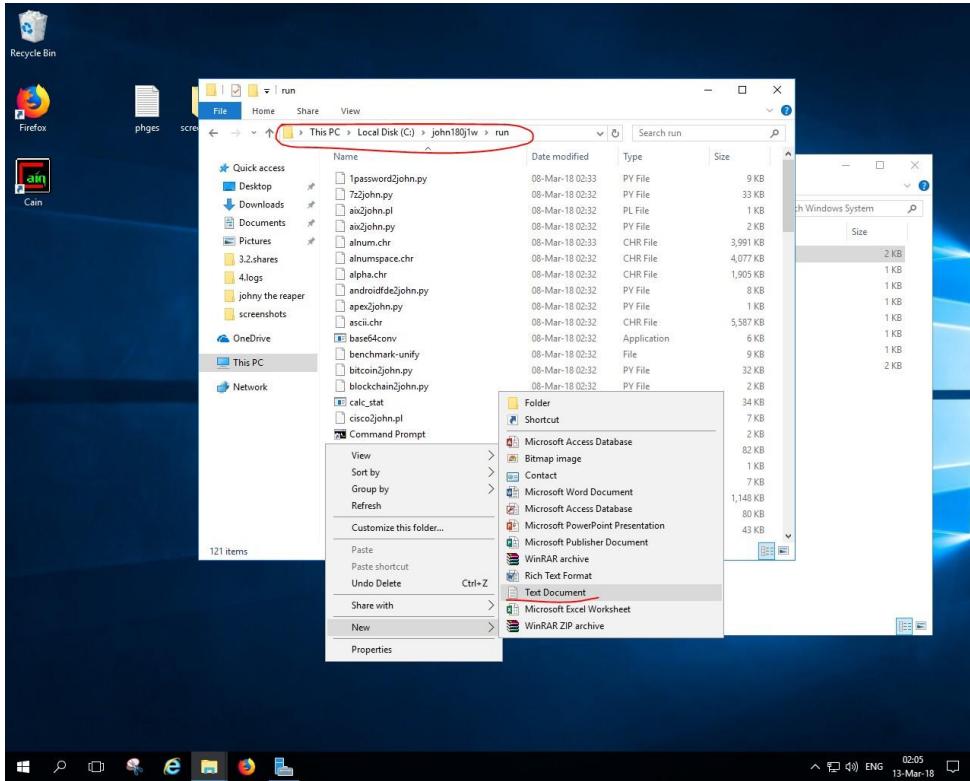
Μόλις το κατέβασα, μετέφερα τον φάκελο με το πρόγραμμα στον φάκελο C:/ . Το συγκεκριμένο πρόγραμμα δεν θέλει εγκατάσταση.



Επειδή το πρόγραμμα αυτό «τρέχει» μέσω του cmd, παίρνω την συντόμευση του cmd και την μεταφέρω στον φάκελο με τον cracker.



Στην συνέχεια δημιουργώ ύνα txt αρχείο στο οποίο θα βάζω το hash που δημιουργείτε για κάθε χρήστη από τον αλγόριθμο md5. Την μετατροπή αυτή την κάνω στο site : sherycanter.com/encrypted.php

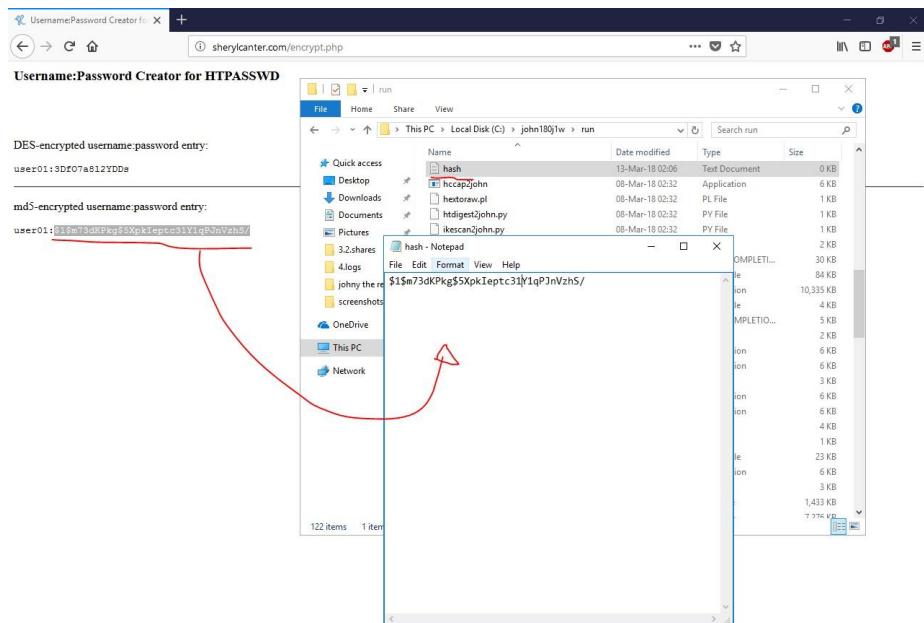


Αρχικά, θα πειραματιστούμε με τον user01 και κωδικό = 123456.

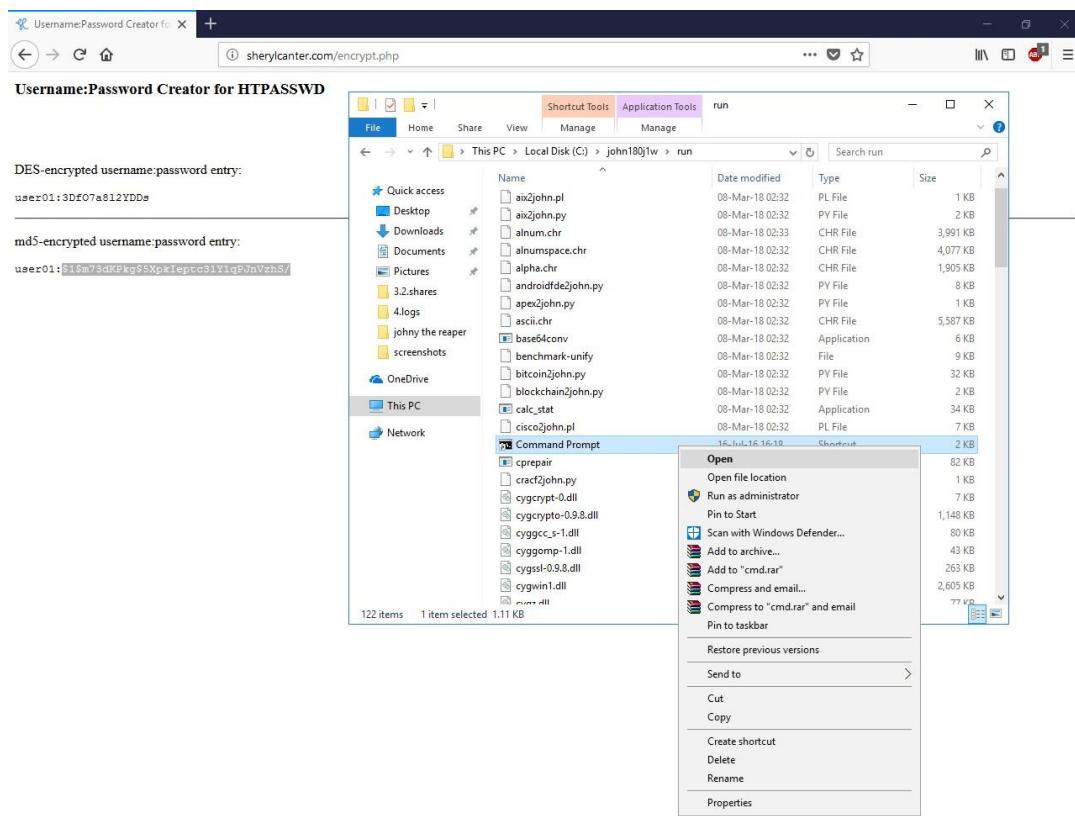
The screenshot shows a web-based form titled "Username:Password Creator for HTPASSWD". The form is used to create a username:password entry for an .htpasswd file. It has three input fields: "Username" (set to "user01"), "Password" (set to "123456"), and "DES Salt" (set to "3DF07a812YDDs"). Below the fields are three bullet points explaining salt requirements. A note states that the salt is always at the beginning of the password portion. A red circle highlights the "Create" button, which is also circled in the original image. At the bottom, there are links for "Create another entry", "Home", "Blog", and "Close".

The screenshot shows the same web-based form after the "Create" button was clicked. It displays two sections of encrypted text. The first section, "DES-encrypted username:password entry:", contains the string "user01:3DF07a812YDDs". The second section, "md5-encrypted username:password entry:", contains the string "user01:\$1\$w73dKPkgsXpkIeptc31YiqPjNvzhS/". Both sections are circled in red. At the bottom, there are links for "Create another entry", "Home", "Blog", and "Close".

Μεταφέρω το hash στο αρχείο hash.txt που δημιούργησα πριν.



Στην συνέχεια ανοίγω την συντόμευση του cmd που μετέφερα στον φάκελο του cracker.



Με την παρακάτω εντολή, βλέπουμε τις επιλογές που προσφέρει ο cracker, john the reaper.

The screenshot shows a Windows desktop environment. In the center, there is a Command Prompt window titled "Administrator: Command Prompt" with the path "C:\john1801\crunx\john". The window displays the usage information for the "john" command-line tool. At the top of the window, it says:

```
C:\john1801\crunx\john
      1 [main] John 4320 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
```

Below that, it shows the tool's version and copyright information:

```
John the Ripper password cracker, version 1.8.0-jumbo-1_omp [cygwin 32-bit SSSE3-autoconf]
Copyright (c) 1996-2014 by Solar Designer and others
Homepage: http://www.openwall.com/john/
```

The usage information for "john" is extensive and includes many options like --single, --wordlist, --rules, etc. The desktop taskbar at the bottom shows various icons for programs like File Explorer, Task View, and the Start button. The system tray in the bottom right corner shows the date (13-Mar-18), time (02:13), battery status, and network connection.

Τρέχω την εντολή «john hash.txt», όπου john το αρχείο εκτέλεσης του cracker και το hash.txt, το txt αρχείο που περιέχει το hash από τον κωδικό του χρήστη που θέλουμε να υποκλέψουμε.

The screenshot shows a Windows desktop environment. In the center, there is a Command Prompt window titled "Administrator: Command Prompt" with the following output:

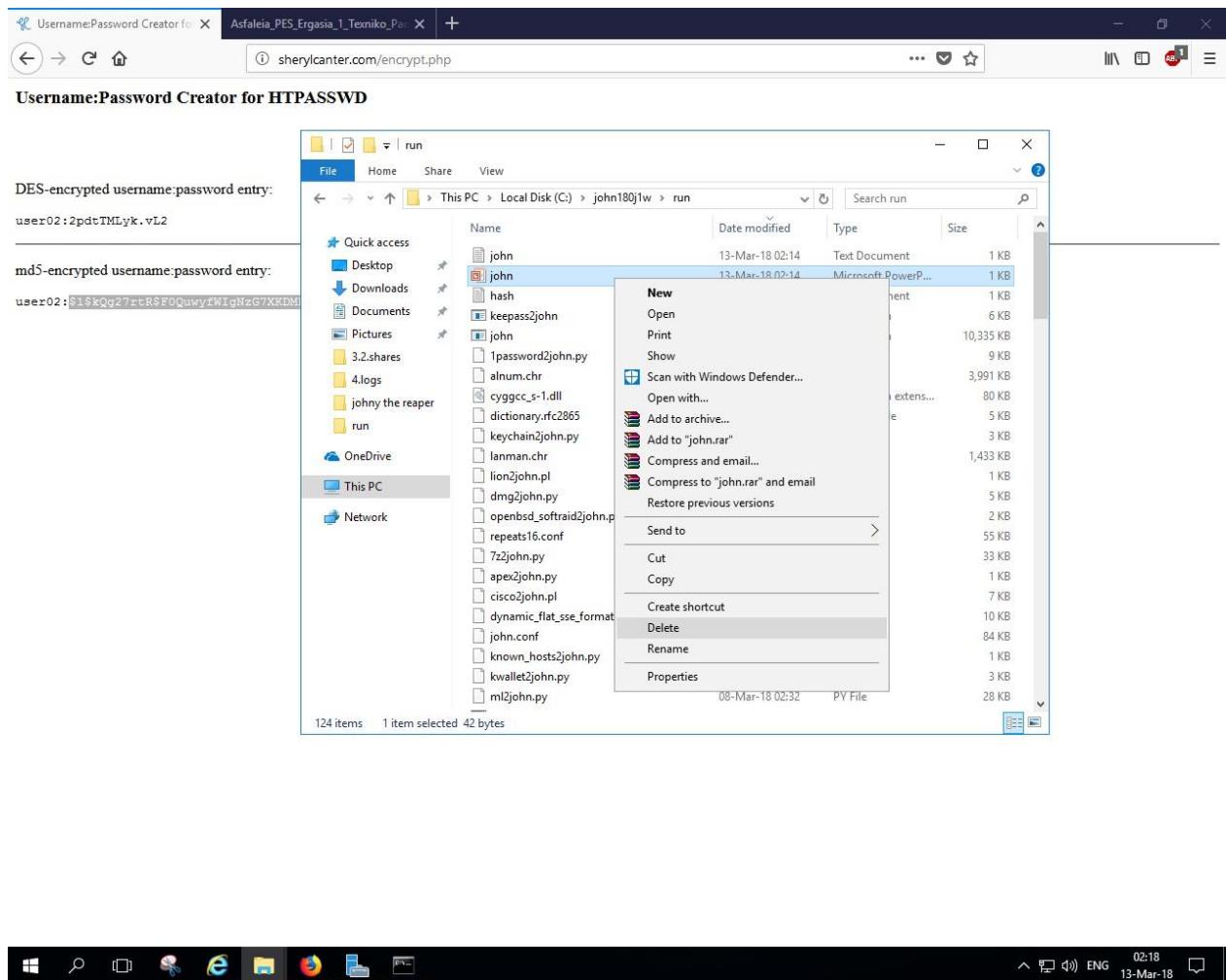
```
C:\john180j1w\run>john hash.txt
      2 [main] john 368 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-sm5"
md5-encrypted username Use the "--format=aix-sm5" option to force loading these as that type instead
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 SSSE3 12x])
user01:$1$sm73dKFkgs$Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (?)  
ig 0:00:00:00 DONE 2/3 (2018-03-13 02:14) 15.87g/s 3047p/s 3047c/s 123456..knight
Use the --show" option to display all of the cracked passwords reliably
Session completed
```

At the top, there is a browser window titled "Username:Password Creator for HTPASSWD" with the URL "sherylcanter.com/encrypt.php". Above the browser is a file explorer window showing a folder structure.



Στην 1^η κόκκινη γραμμή βλέπουμε τον κωδικό που βρήκε ο cracker (και σωστά!), και στην 2^η γραμμή ο χρόνος που πέρασε μέχρι να βρεθεί ο κωδικός.

Για να επαναλάβουμε την διαδικασία για τον επόμενο χρήστη (user02, κωδικός = pass123) διαγράφουμε το παρακάτω αρχείο



Και επαναλαμβάνουμε με ακριβώς ίδιο τρόπο την προηγούμενη διαδικασία

Username:Password Creator for HTPASSWD

Use this form to create a username:password entry for an .htpasswd file.

Username:	<input type="text" value="user02"/>
Password:	<input type="password" value="*****"/>
DES Salt:	<input type="text"/>
MD5 Salt:	<input type="text"/>

(optional, see below)

- Valid salt characters are a-z, A-Z, 0-9, the period '.', and the forward slash '/'.
- For DES, the salt is 2 random characters from the set of valid characters.
- The MD5 salt is 12 characters, only 8 of which are random. The MD5 salt always starts with '\$1\$' and ends with '\$'.

The salt is always at the beginning of the password portion of the username:password entry. If you use the same salt, you'll get the same result. This is how passwords are validated since the hashes can't be reversed.

[Create](#)

[Create another entry](#) [Home](#) [Blog](#) [Close](#)

Username:Password Creator for HTPASSWD

DES-encrypted username:password entry:
user02:2pdTMLyK.vL2

md5-encrypted username:password entry:
user02:\$1\$Qg27rtR\$FOQuwyfWIgNzG7XKDMFvX/

File Home Share View

This PC > Local Disk (C) > john18j1w > run

Name	Date modified	Type	Size
john	13-Mar-18 02:14	Text Document	1 KB
hash	13-Mar-18 02:18	Text Document	1 KB
keepass2john	08-Mar-18 02:34	Application	6 KB
john	08-Mar-18 02:33	Application	10,335 KB

hash - Notepad

```
$1$Qg27rtR$FOQuwyfWIgNzG7XKDMFvX/
```

File Edit Format View Help

123 items 1 item selected



Username:Password Creator for HTPASSWD

DES-encrypted username:password entry:

```

user02:2pdःTMLyK.vL2
md5-encrypted username:password
user02:$1$kQg27rtR$FOQuwyF
C:\john180j1w\run>john hash.txt
      2 [main] john 4768 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 SSSE3 12x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pass123      (?)
1g 0:00:02:24 DONE 3/3 (2018-03-13 02:23) 0.006903g/s 37832p/s 37832c/s 37832C/s passe08..pass0xs
Use the "--show" option to display all of the cracked passwords reliably
Session completed

C:\john180j1w\run>

```

File Home Share View

Administrator: Command Prompt

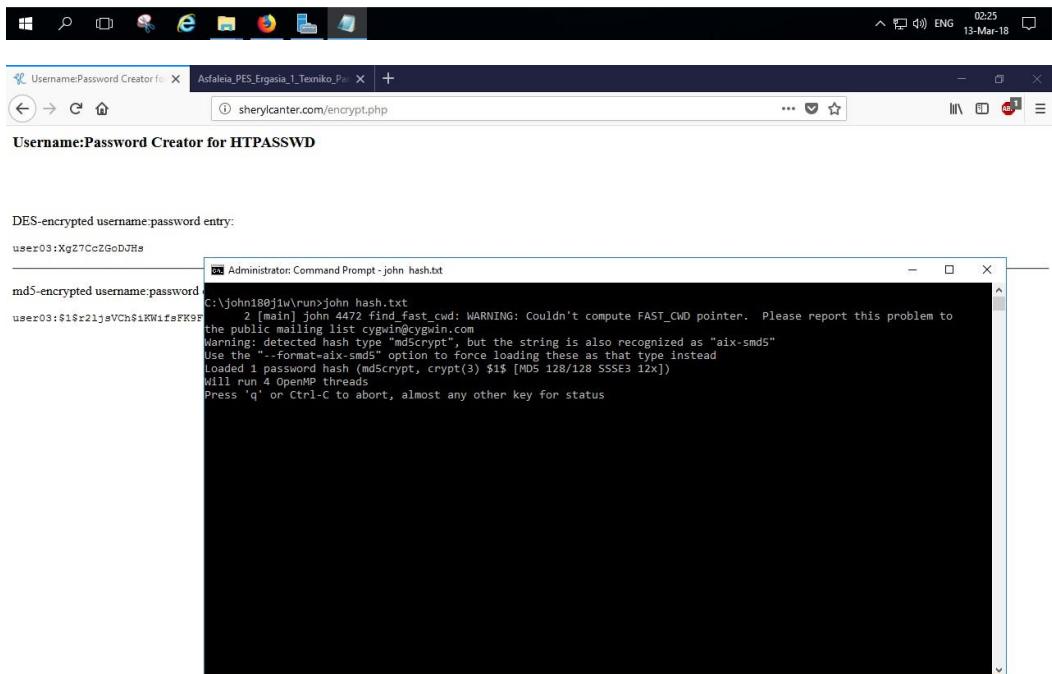
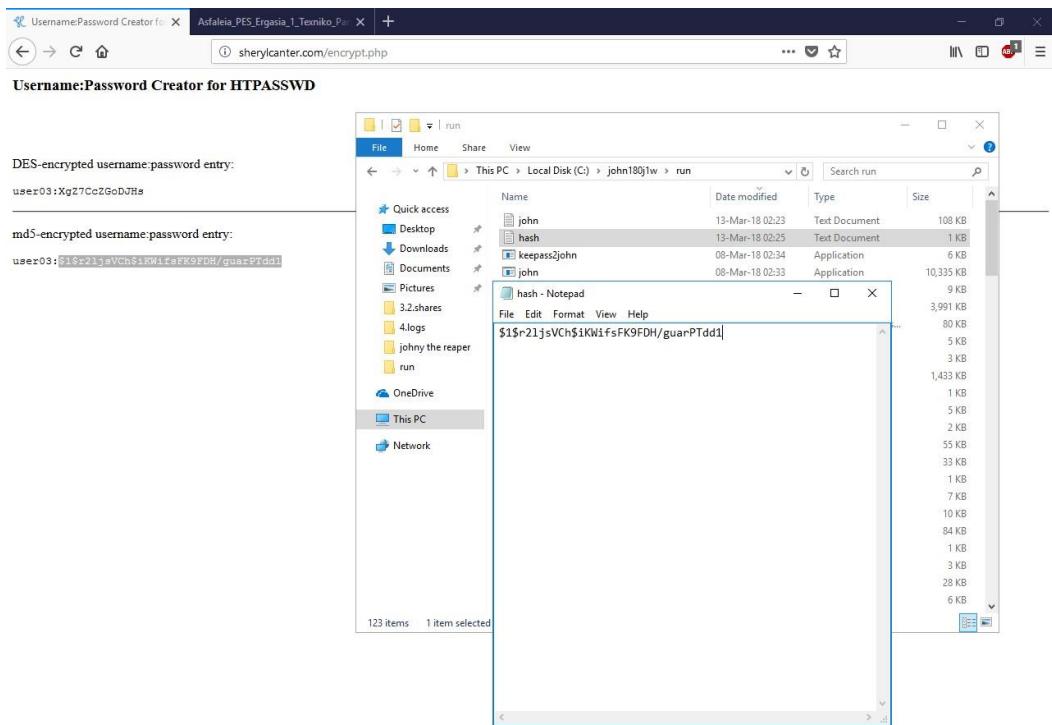
C:\john180j1w\run

124 items 1 item selected 34 bytes 08-Mar-18 02:32 CONF File 4 KB



Αυτή την φορά επειδή ο κωδικός ήταν πιο περίπλοκος σε σχέση με αυτόν του user01, ο cracker ήθελε σχεδόν 2,5 λεπτά για να βρει τον κωδικό του χρήστη user02.

Αυτή την φορά, θα πειραματιστώ με τον χρήστη user03 ο οποίος έχει υπερβολικά πιο περίπλοκο κωδικό από τους δύο προηγούμενους (My!P@ssw0rd#).



Περάσανε σχεδόν εικοσιπέντε λεπτά και το πρόγραμμα δεν βρήκε κάτι.

The screenshot shows a Windows desktop environment. At the top, there are two tabs: "Username:Password Creator for HTPASSWD" and "Asfaleia_PES_Ergasia_1_Tekniko_Par". Below the tabs is a browser bar with the URL "sherylcanter.com/encrypt.php". The main window contains a command prompt titled "Administrator: Command Prompt". The command entered is "C:\john180j1w\run>john hash.txt". The output of the command is displayed, showing the progress of the password cracking process. The progress bar indicates 0g 0:00:30:12 3/3 0g/s 44566p/s 44566c/s 44566C/s latielar..latiepsy Session aborted. The session was aborted after 30 minutes and 12 seconds, having processed 3 password hashes at a rate of 0g/s and 44566c/s. The command prompt ends with "C:\john180j1w\run>".



Αυτή ήταν μια αρκετά μικρή επίδειξη για το πως μπορούμε να βρούμε συνθηματικά χρηστών, αν ξέρουμε το hash των χρηστών.

2.5 Θεωρητικά Ερωτήματα

- Παραπάνω (στο 2.2) είδαμε ότι το λειτουργικό σύστημα αποθηκεύει το hash του συνθηματικού μέσω hash function. Άρα για κάθε λογαριασμό χρήστη στα λειτουργικά συστήματα αποθηκεύεται το κλειδί κρυπτογράφησης του συνθηματικού.
- Για να πετύχει μια επίθεση λεξικού χρειάζεται αρχικά ένα καλό λεξικό από αυτόν που θέλει να υποκλέψει συνθηματικά αλλά κυρίως βασίζεται στην άγνοια των χρηστών και στην επιμονή τους να βάζουν αρκετά απλά συνθηματικά, που δεν έχουν καμία πολυπλοκότητα και κανέναν τυχαίο συνδυασμό.

Για να πετύχει μια επίθεση εξαντλητικής αναζήτησης πρέπει το αυτοματοποιημένο λογισμικό να «μάθει» όσον το δυνατόν περισσότερα δεδομένα γίνεται για τον χρήστη έτσι ώστε τα συνθηματικά που προσπαθεί να μαντεύει να έχουν μεγαλύτερες πιθανότητες να είναι σωστά.

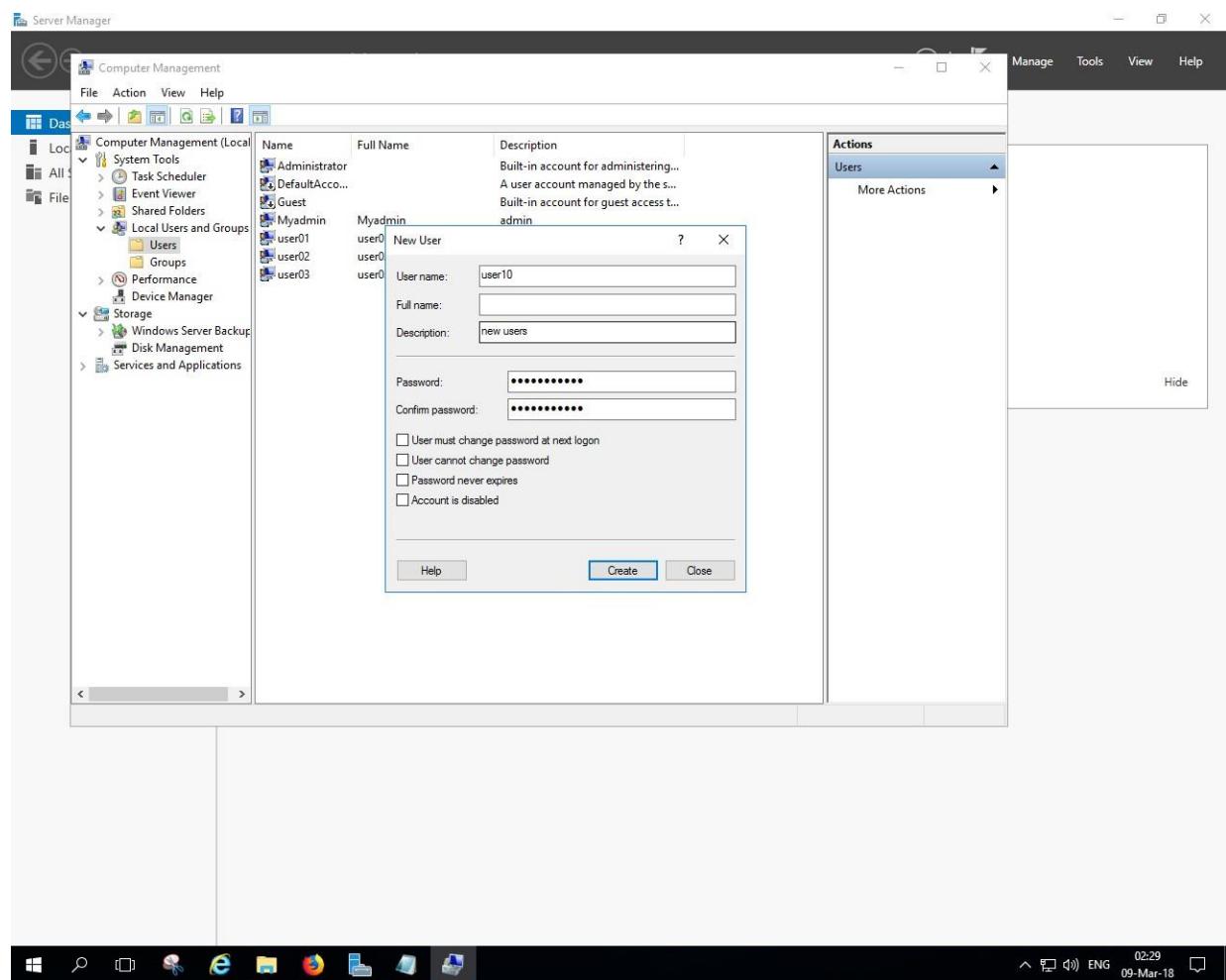
- Για την ταχύτερη αποκάλυψη ενός πολύπλοκου συνθηματικού θα διάλεγα τους πίνακες Rainbow. Δεδομένου ότι ο κωδικός είναι πολύπλοκος, η τεχνική του dictionary attack είναι σχεδόν απίθανο να δουλέψει. Χρησιμοποιώντας όμως πίνακες Rainbow, για ένα πολύπλοκο συνθηματικό ίσως είναι καλύτερα να προσπαθήσουμε να ψάξουμε με βάση το hash μέσα από ένα προκαθορισμένο σύνολο συνθηματικών και των αντίστοιχων hash. Λαμβάνοντας υπόψιν και το μικρό κόστος για αρκετά μεγάλο αποθηκευτικό χώρο, μπορούμε να δημιουργήσουμε ένα τεράστιο λεξικό με πολλές αντιστοιχίες συνθηματικών και hash.

3. Έλεγχος πρόσβασης πόρων του Λειτουργικού Συστήματος

3.1 Δημιουργία νέων χρηστών

Η διαδικασία δημιουργίας χρήστη είναι ακριβώς η ίδια με αυτή που αναλύθηκε και στην ενότητα

- Παρακάτω φαίνεται η δημιουργία των δύο καινούριων χρηστών



Server Manager

Computer Management

File Action View Help

Dashboards All Services File

Computer Management (Local)

System Tools

- Task Scheduler
- Event Viewer
- Shared Folders
- Local Users and Groups
 - Users
 - Groups
- Performance
- Device Manager
- Storage
- Windows Server Backup
- Disk Management
- Services and Applications

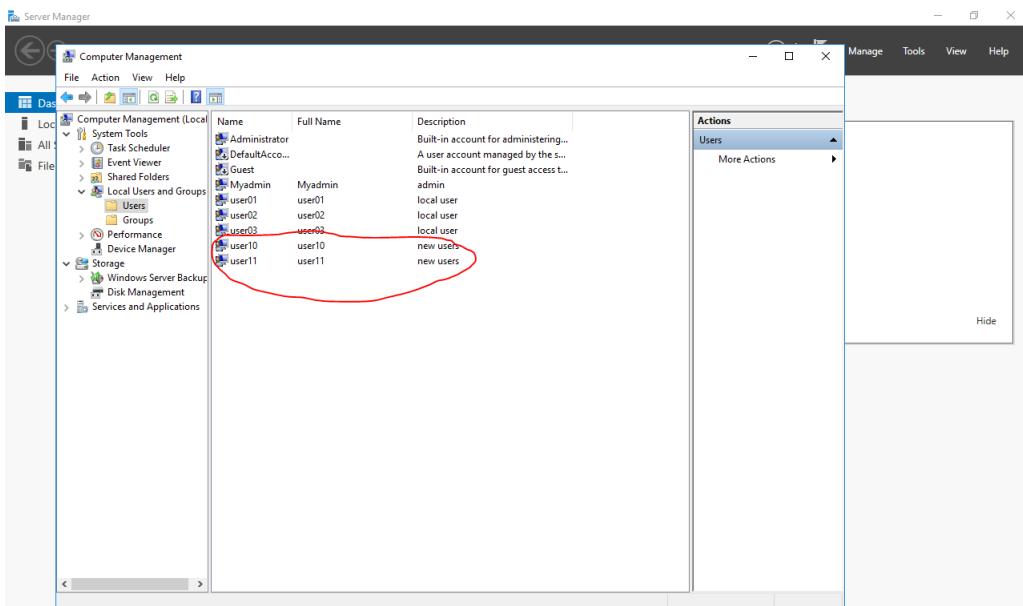
Name Full Name Description

Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
Myadmin	Myadmin	
user01	user01	local user
user02	user02	local user
user03	user03	local user
user10	user10	new users
user11	user11	new users

Actions

Users More Actions

Hide



Server Manager

Computer Management

File Action View Help

Dashboards All Services File

Computer Management (Local)

System Tools

- Task Scheduler
- Event Viewer
- Shared Folders
- Local Users and Groups
 - Users
 - Groups
- Performance
- Device Manager
- Storage
- Windows Server Backup
- Disk Management
- Services and Applications

Name Full Name Description

Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
Myadmin	Myadmin	admin
user01	New User	
user02	user02	
user03	user03	

Actions

Users More Actions

Hide

New User

User name: user11

Full name:

Description: new user

Password: *********

Confirm password: *********

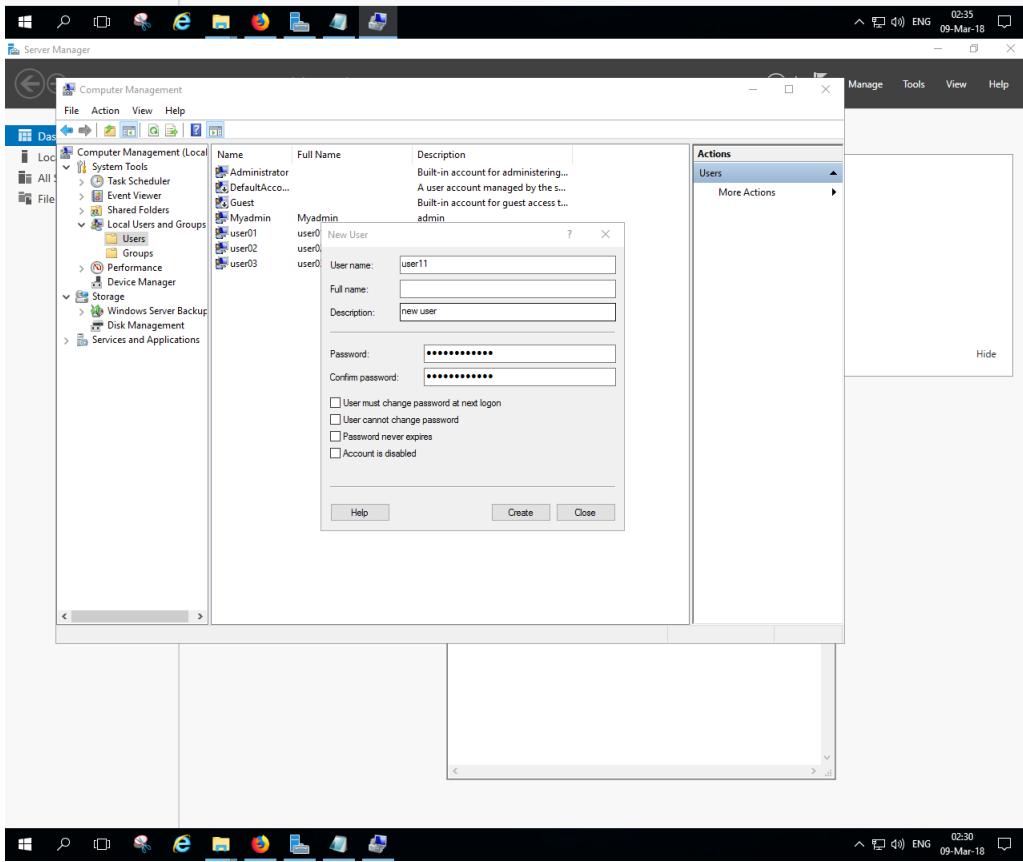
User must change password at next logon

User cannot change password

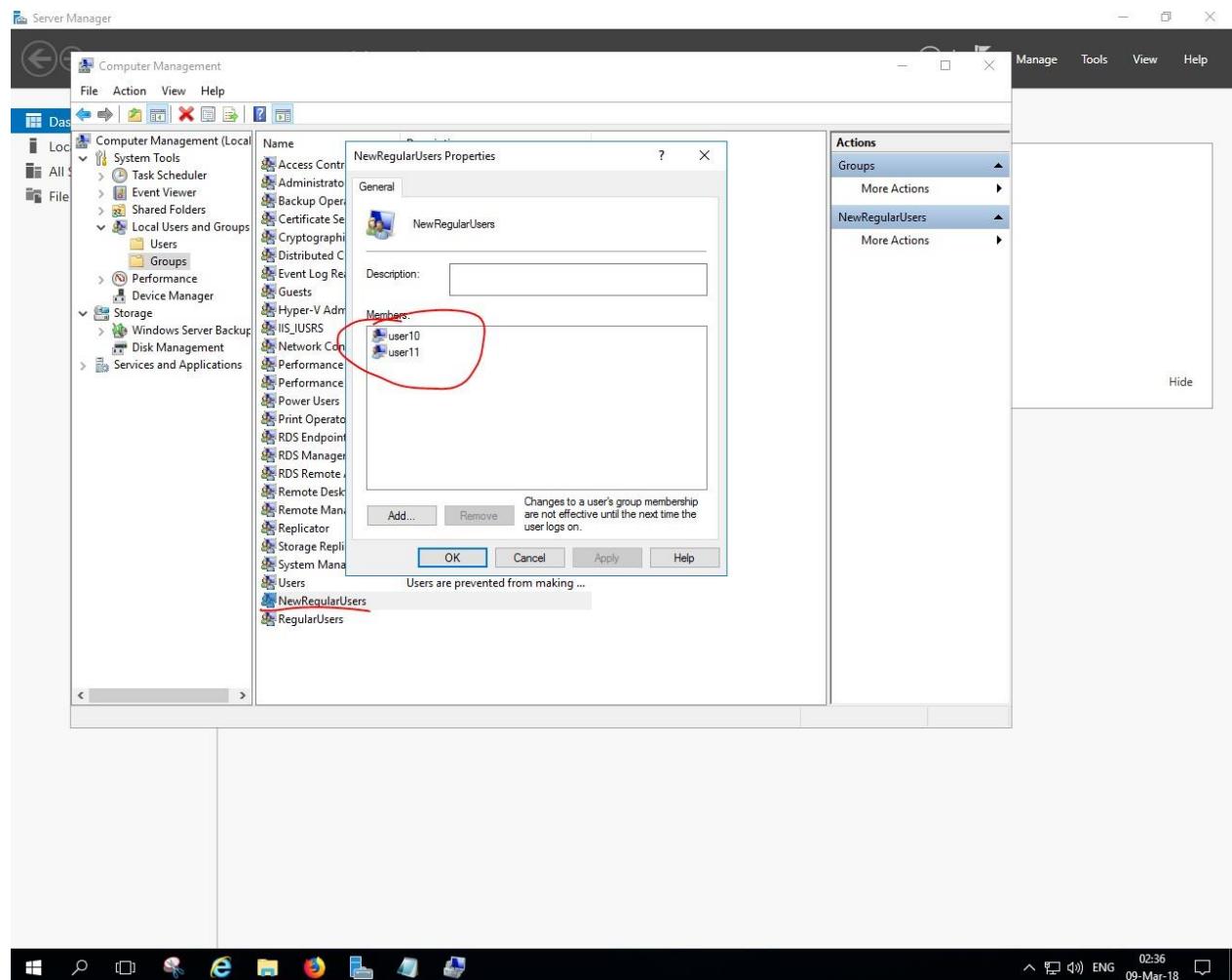
Password never expires

Account is disabled

Help Create Close

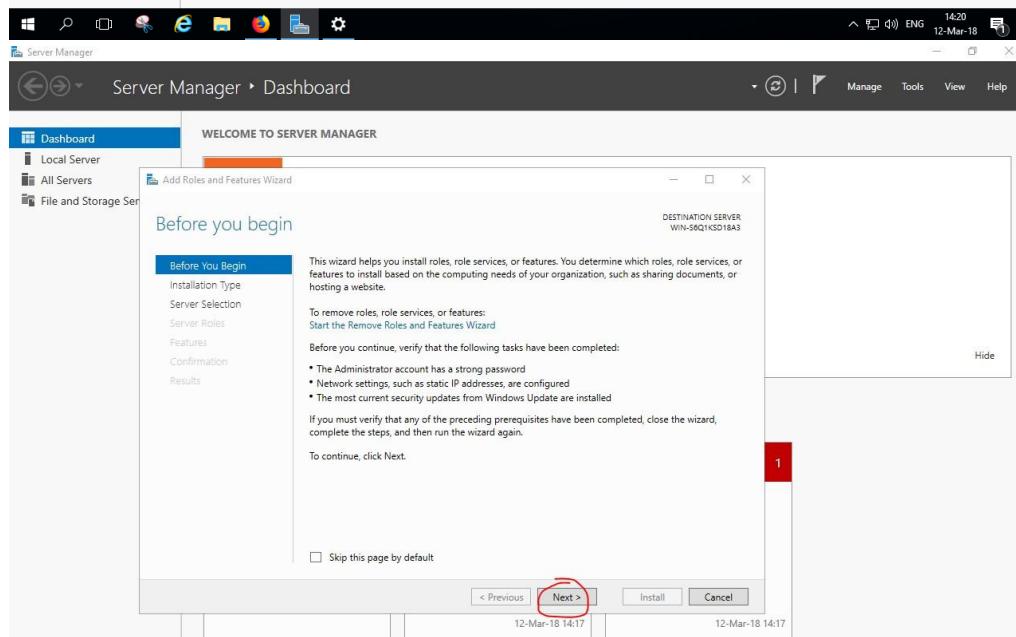
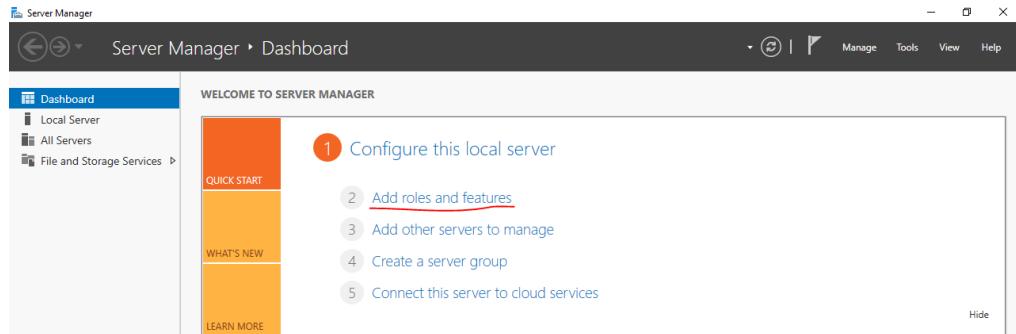


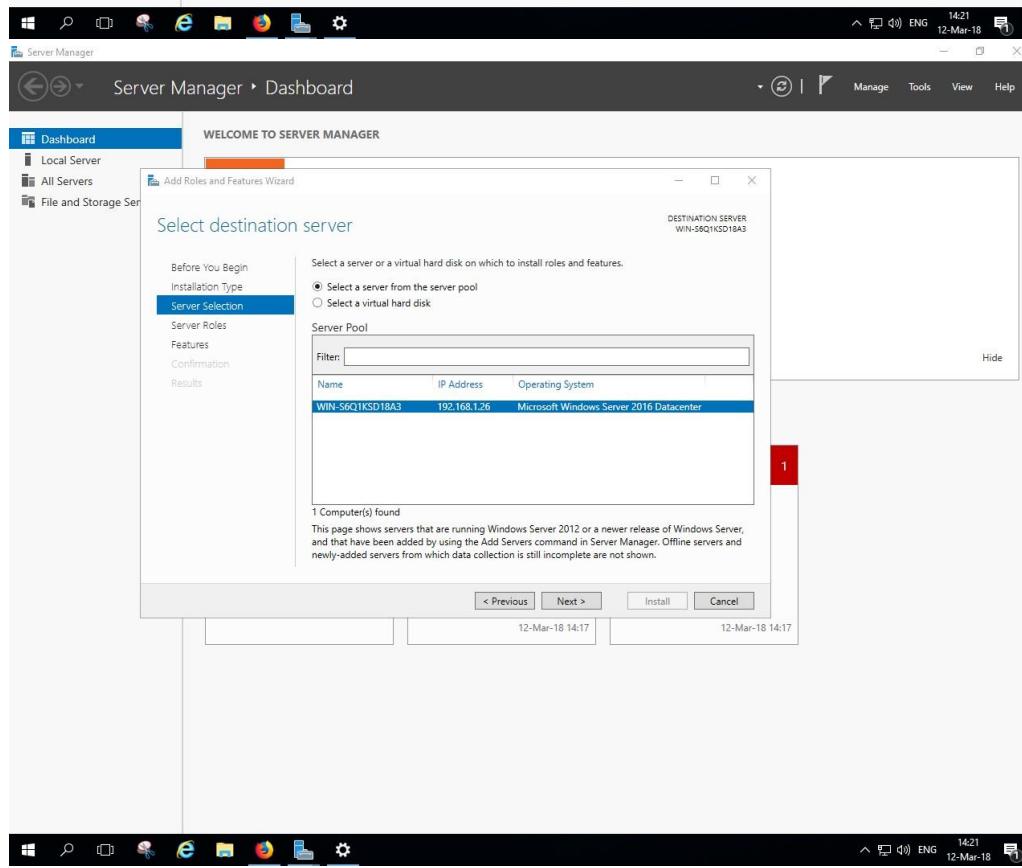
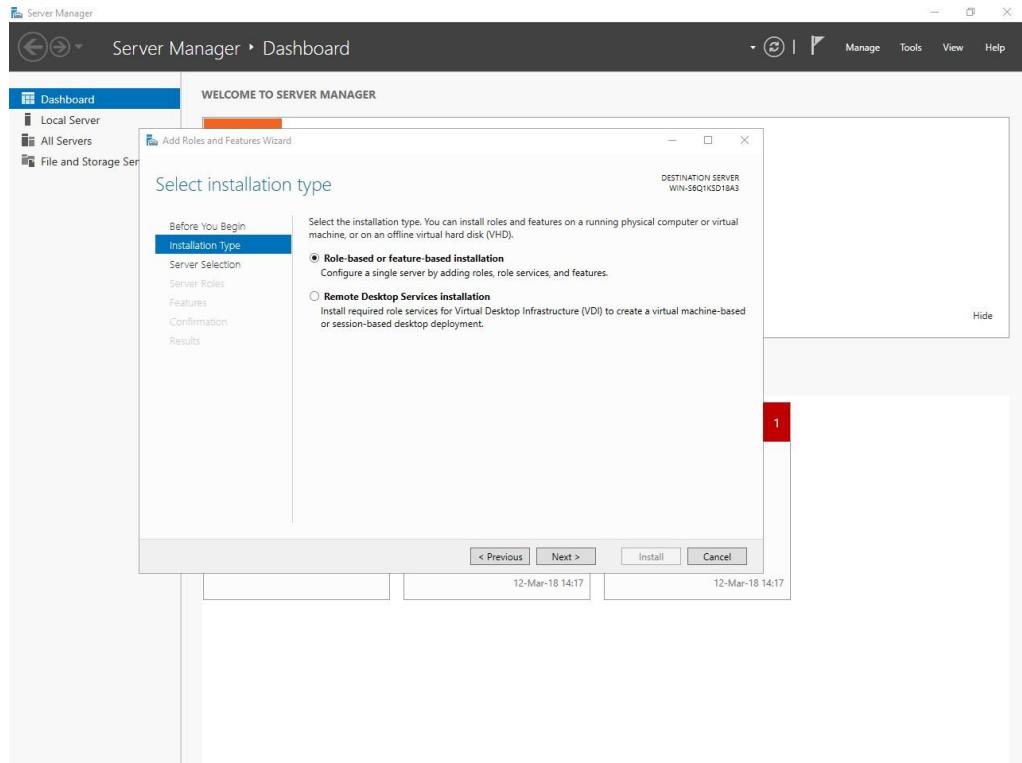
Και εδώ γίνεται η εισαγωγή τους στο γκρουπ NewRegularUsers

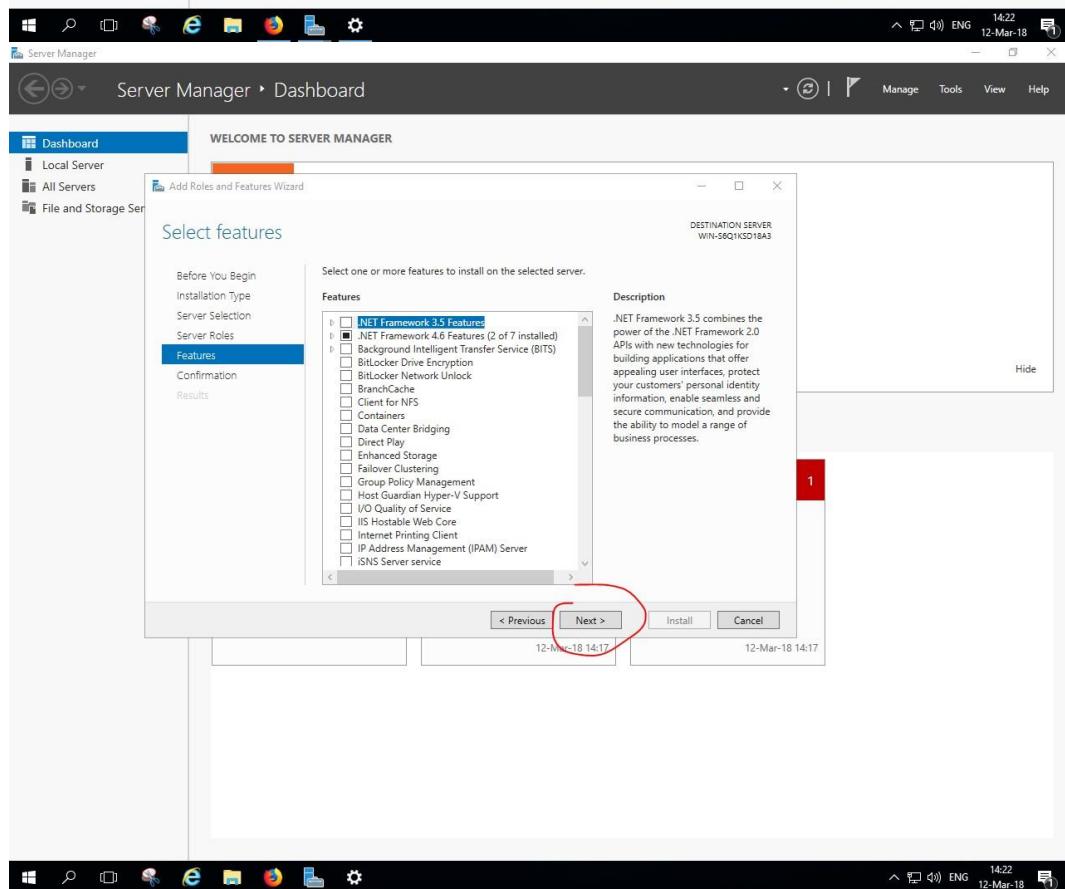
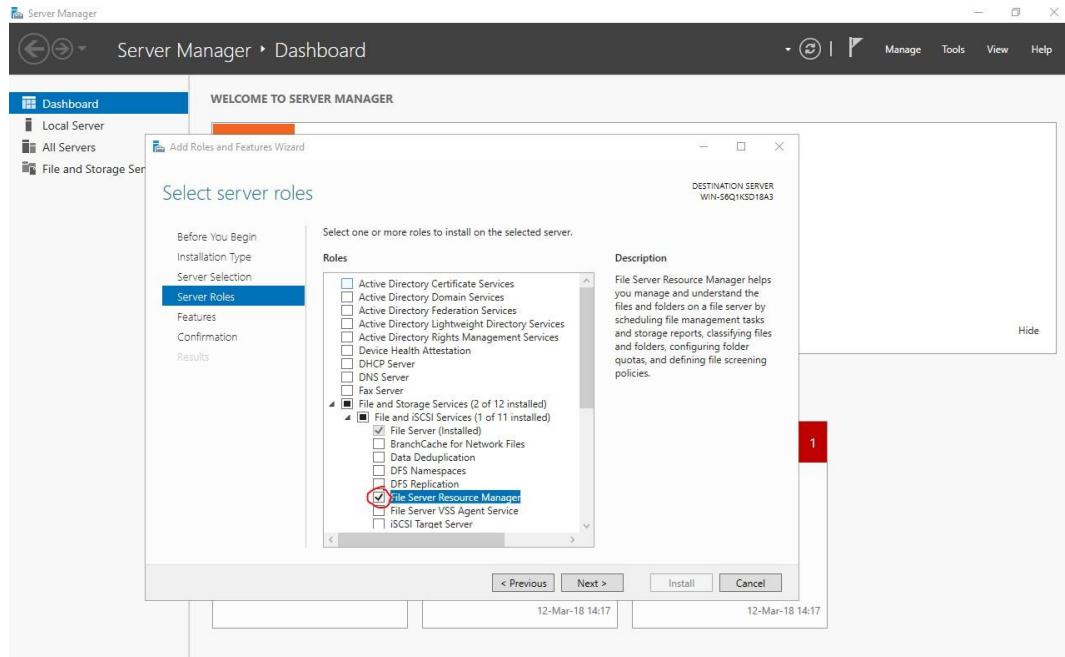


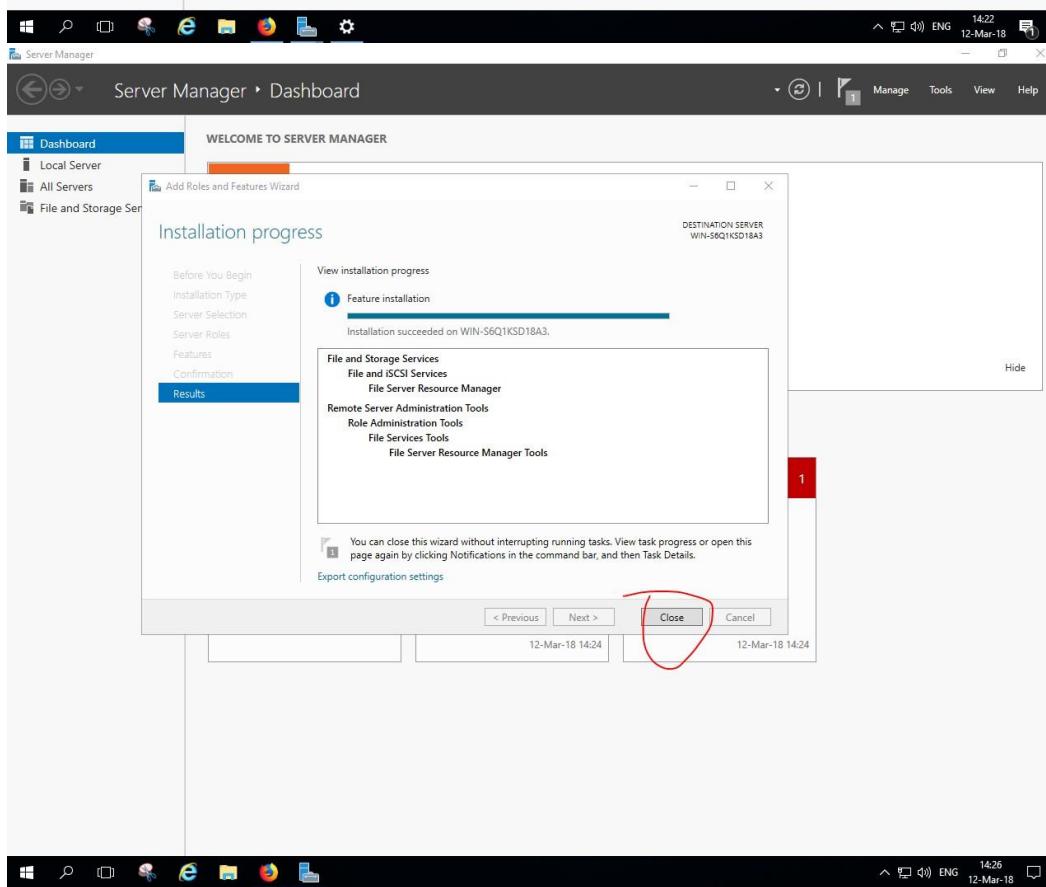
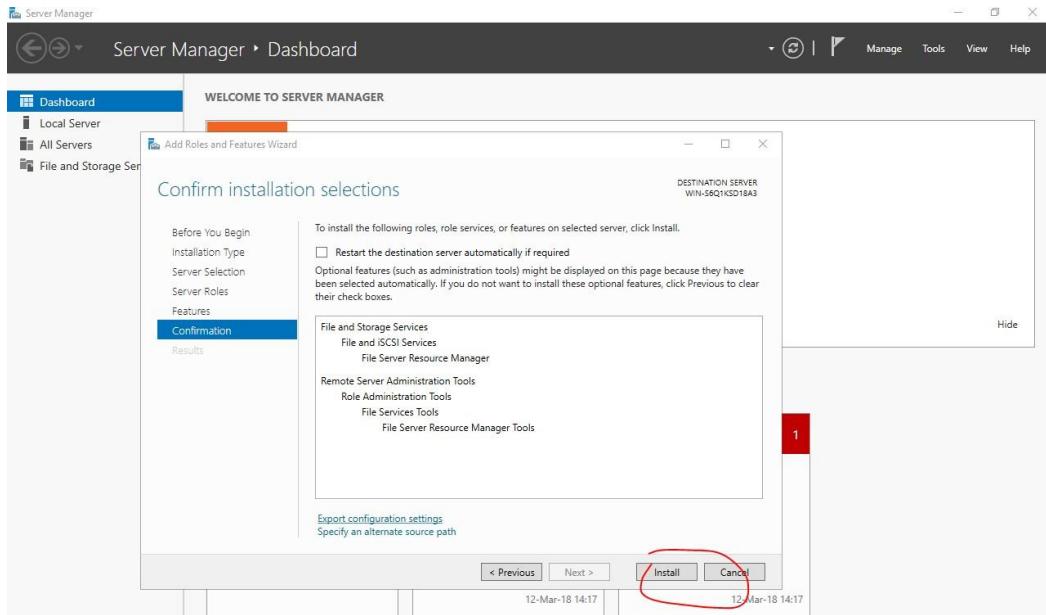
3.2 Δημιουργία φακέλων ομάδων χρηστών

Αρχικά για την καλύτερη διαχείριση των φακέλων (shares) και των δικαιωμάτων τους ακολούθησα τα παρακάτω βήματα για να κάνω εγκατάσταση το File Server Recourse Manager

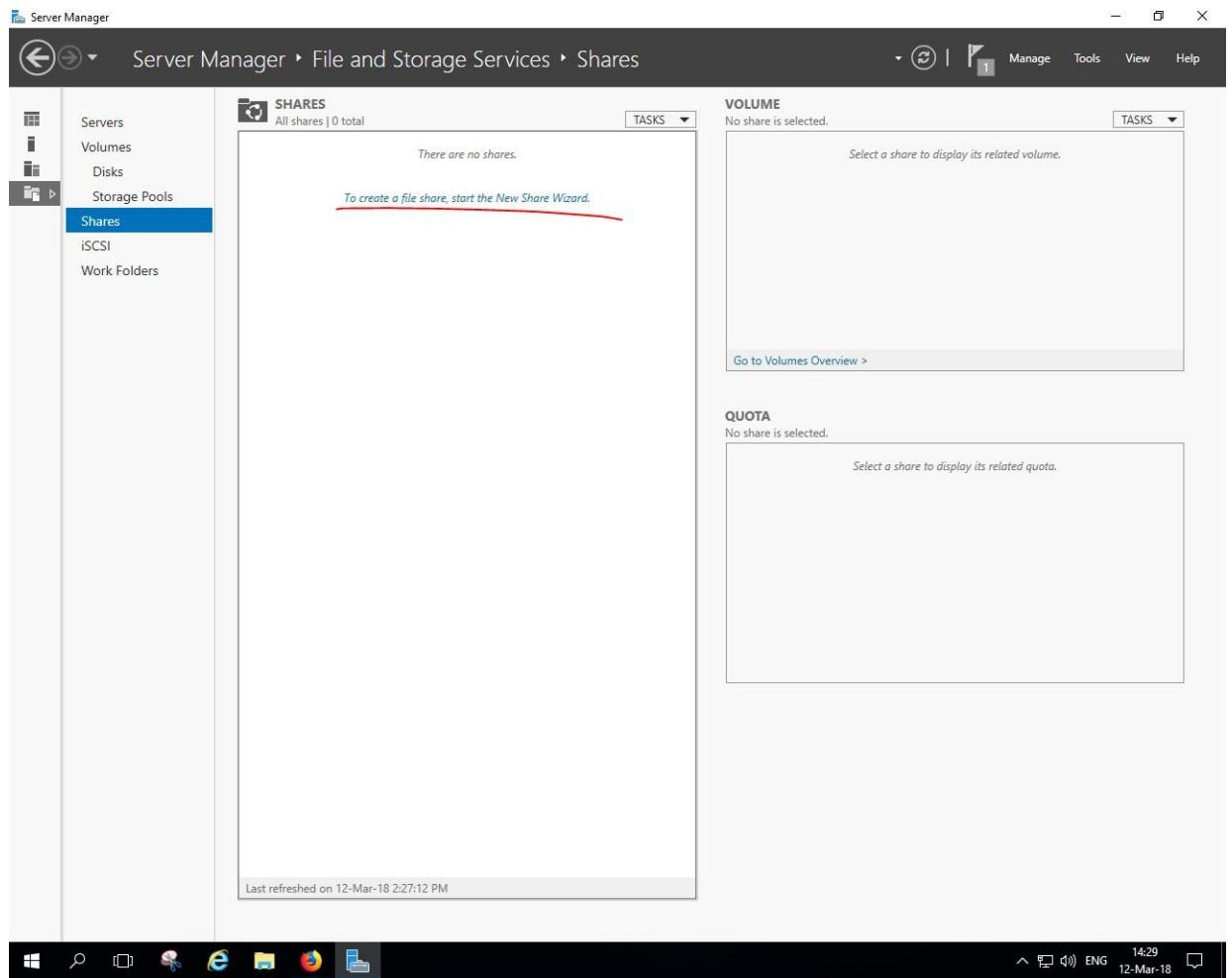


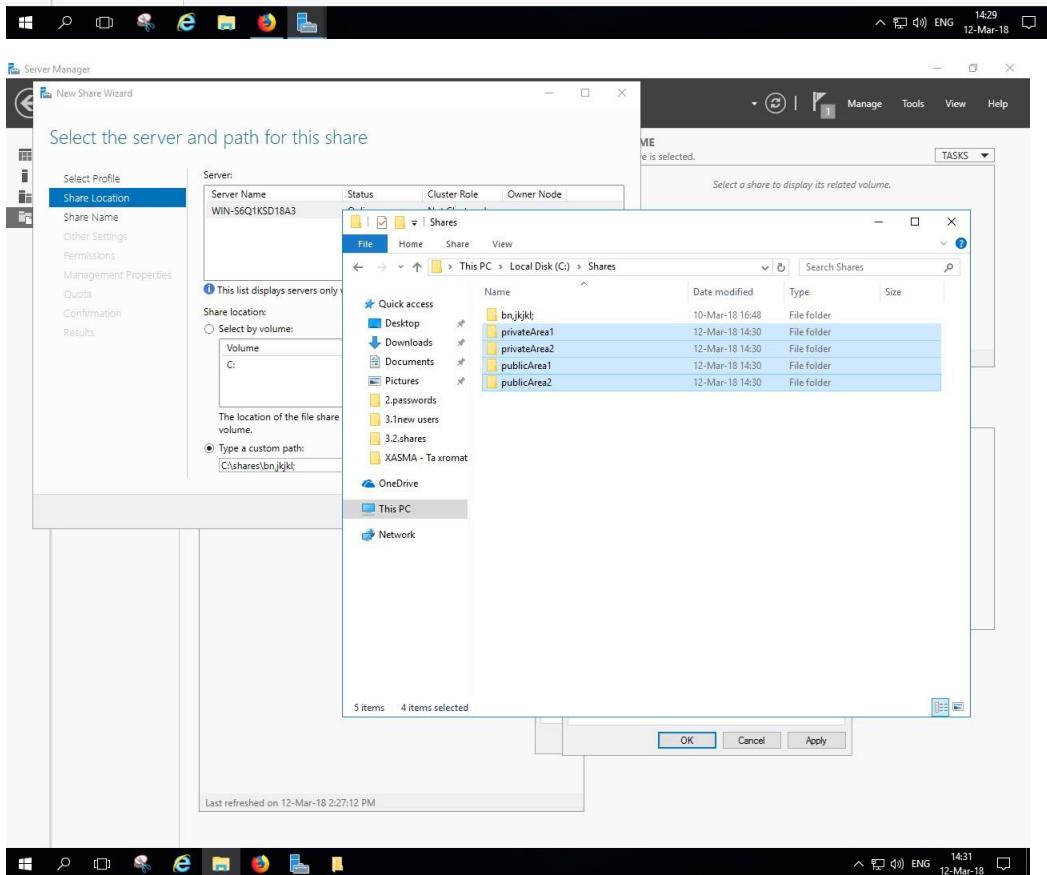
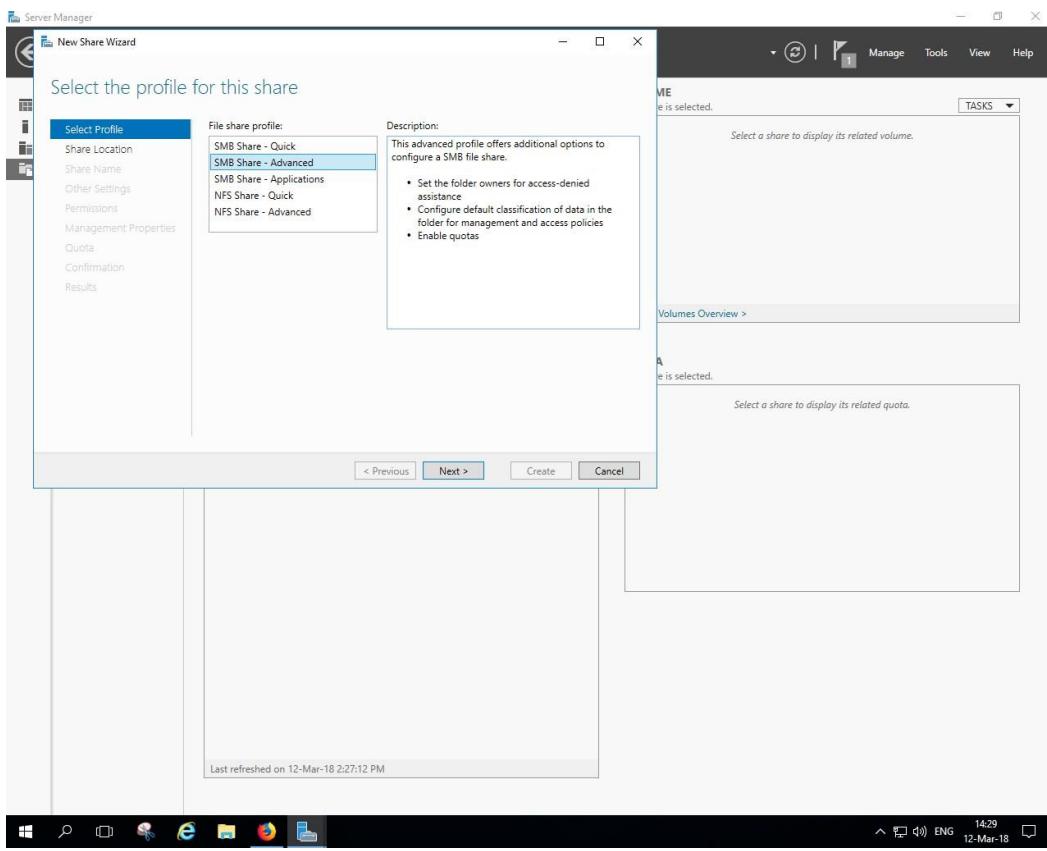


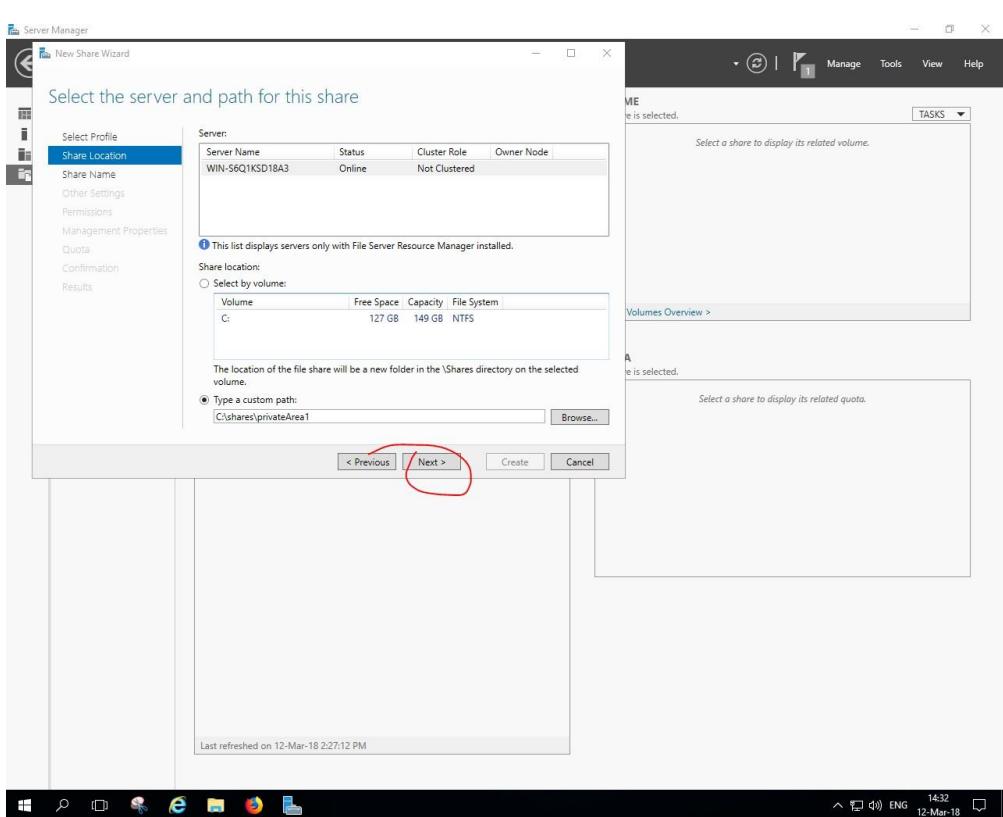
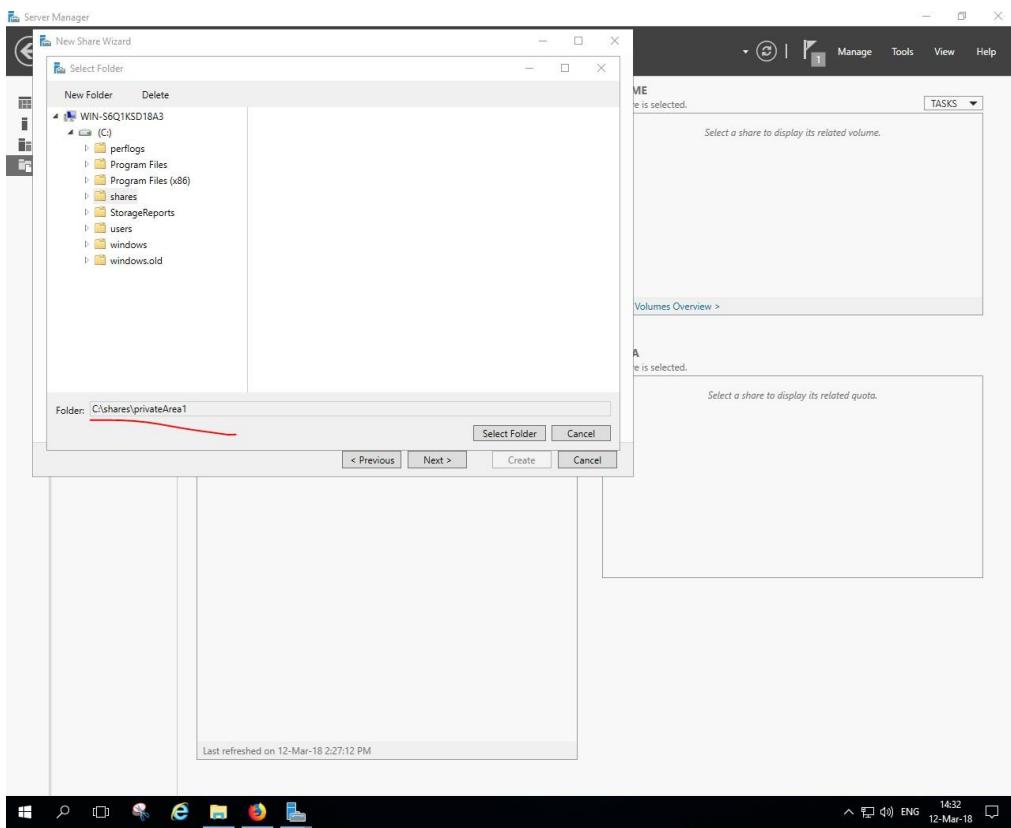


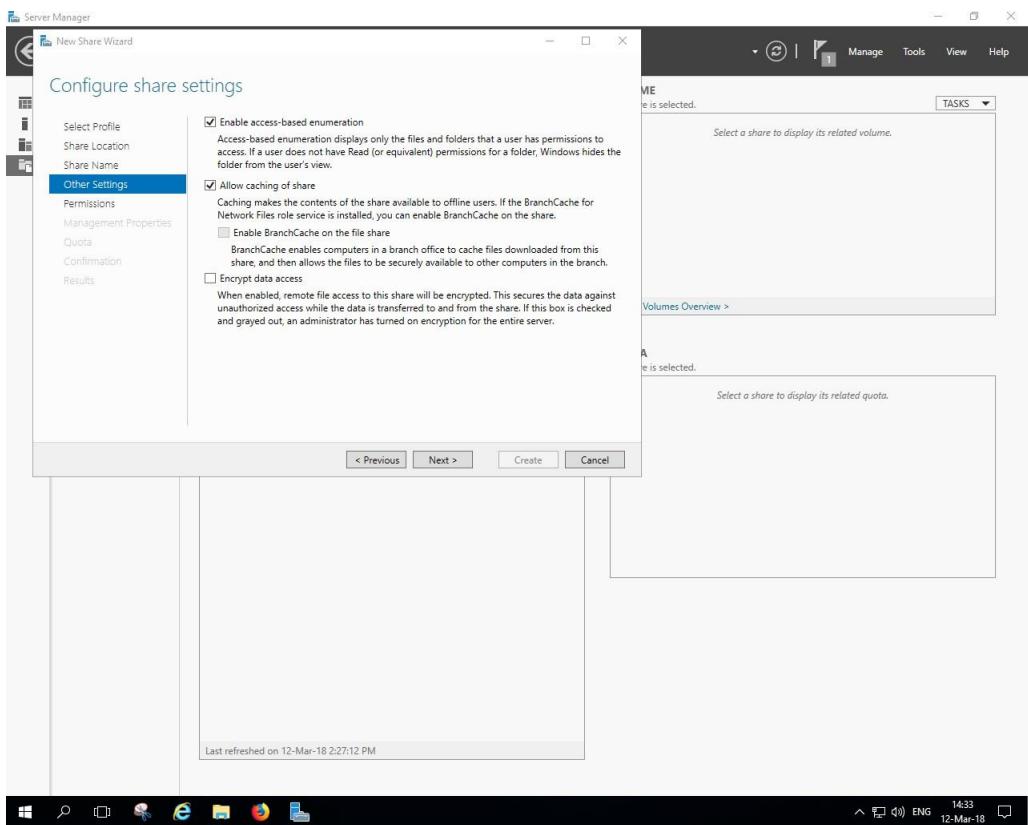
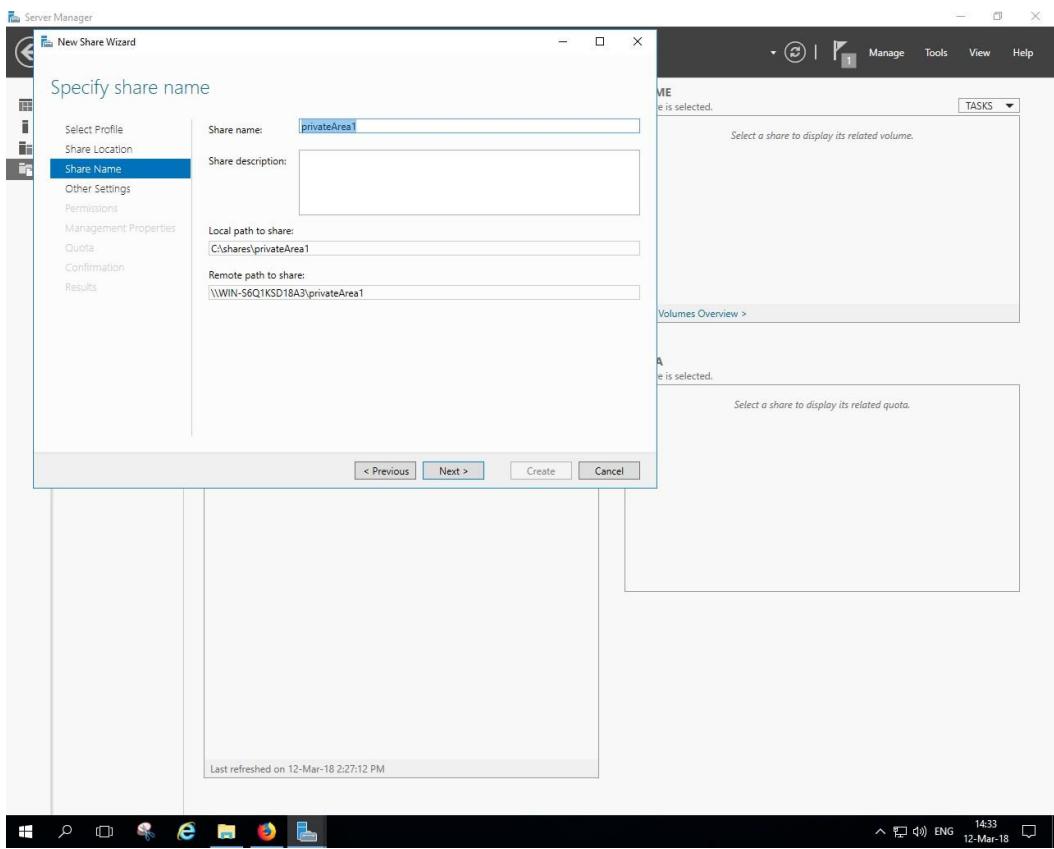


Παρακάτω φαίνεται η δημιουργία των φακέλων για κάθε ομάδα χρηστών. Επειδή ξεχάστηκα όμως στην privateArea1 έβαλα τους χρήστες από την 2^η ομάδα και στην privateArea2 αυτούς από την 1^η ομάδα. Το αντίστοιχο ισχύει και για τις privateArea1 και privateArea2.

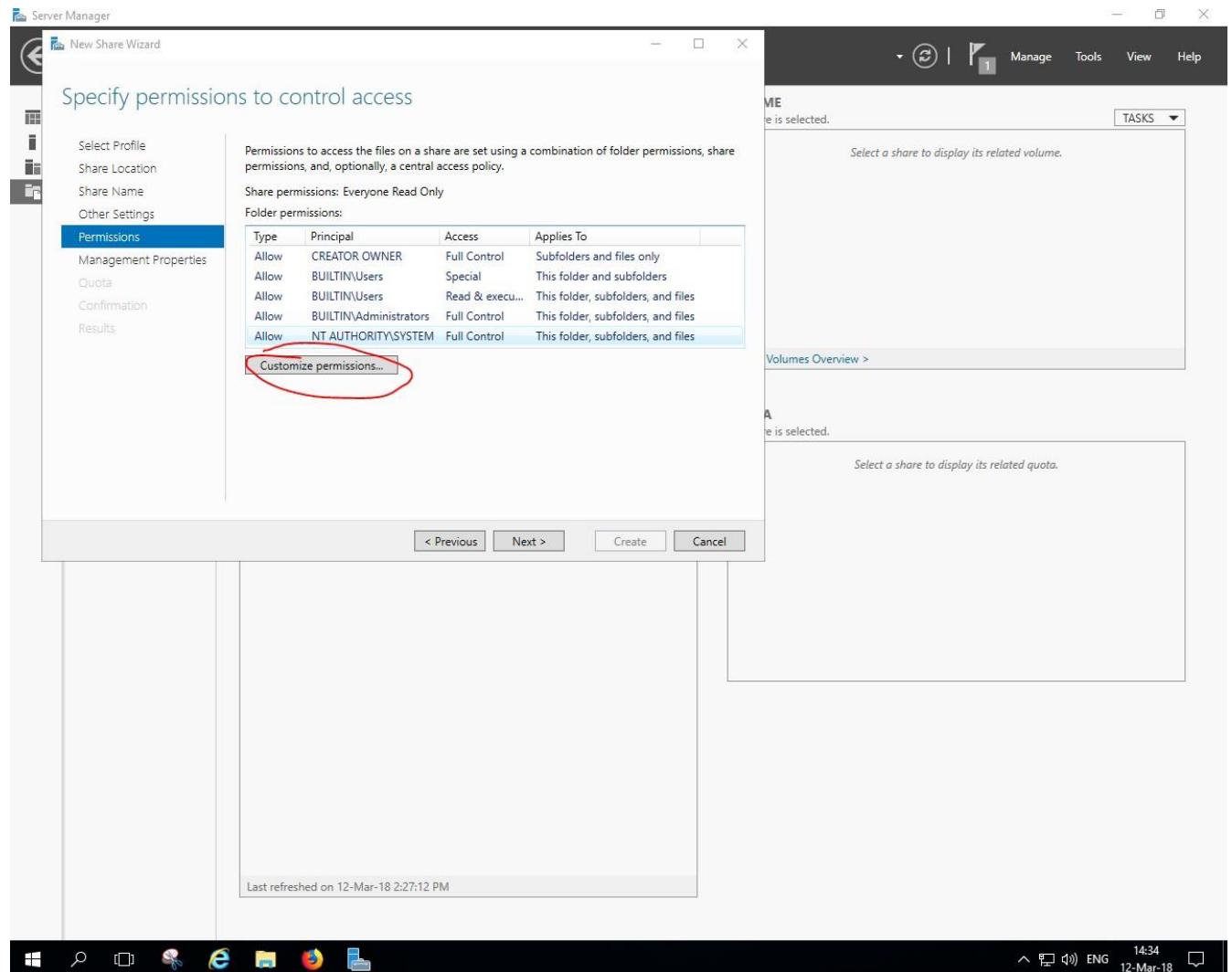






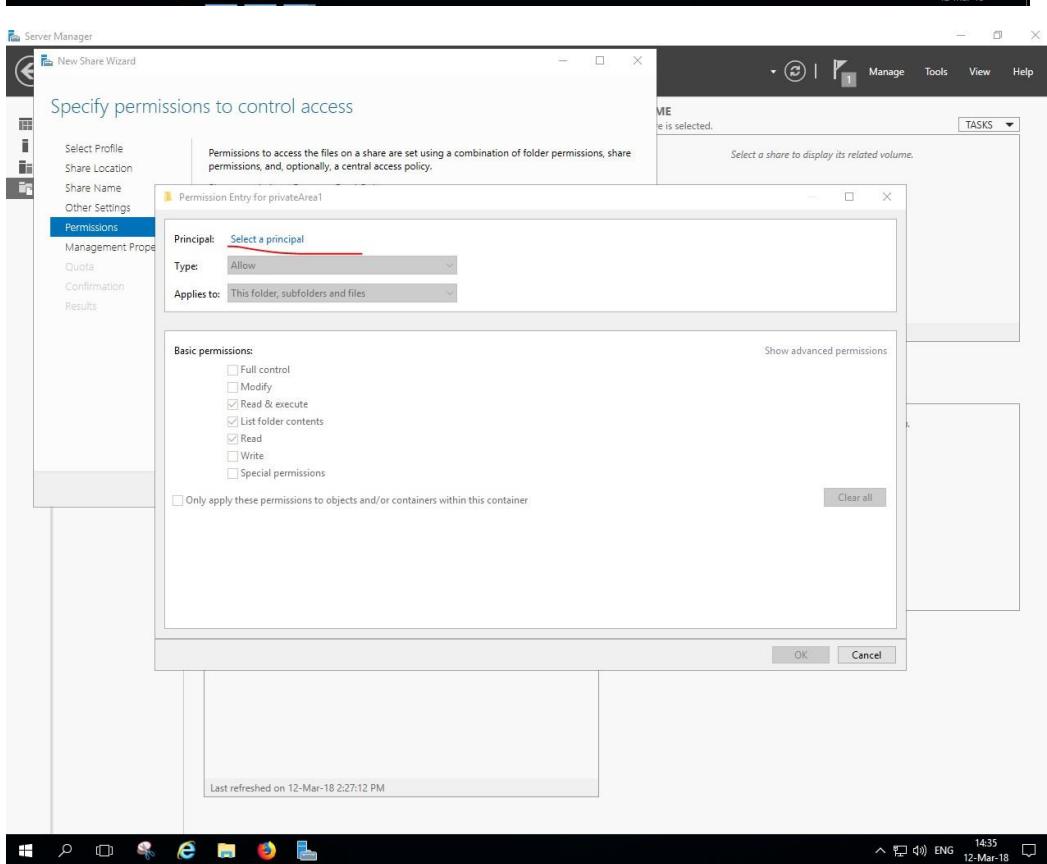
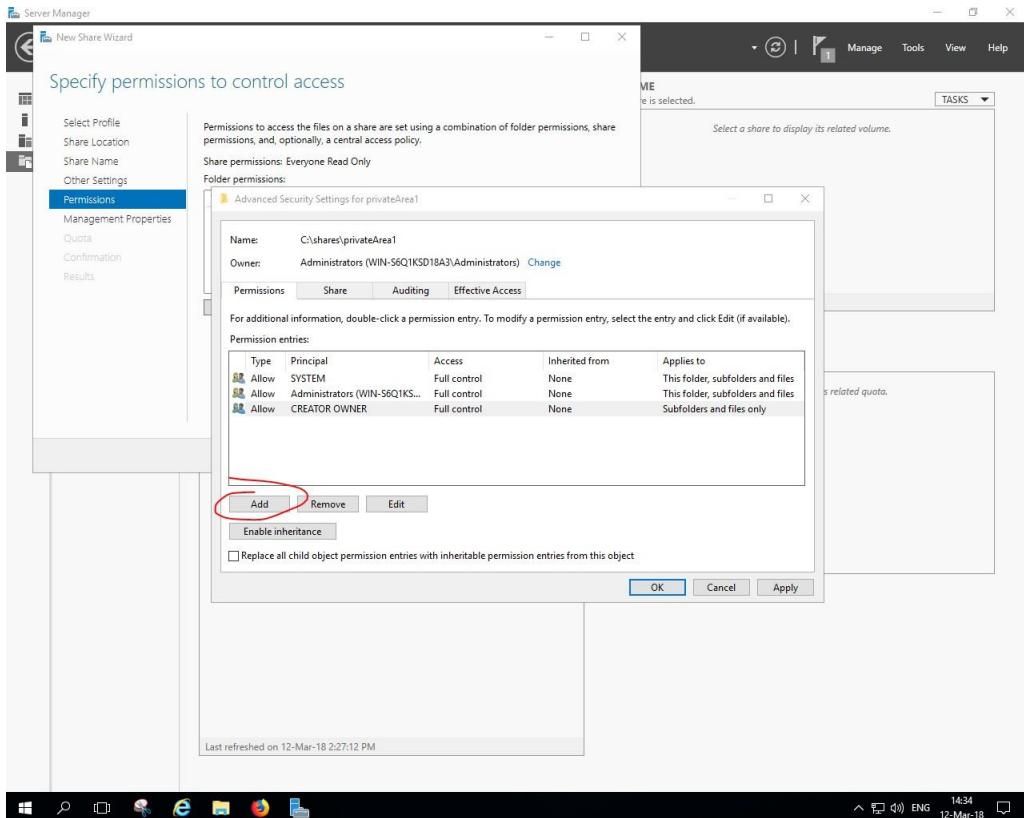


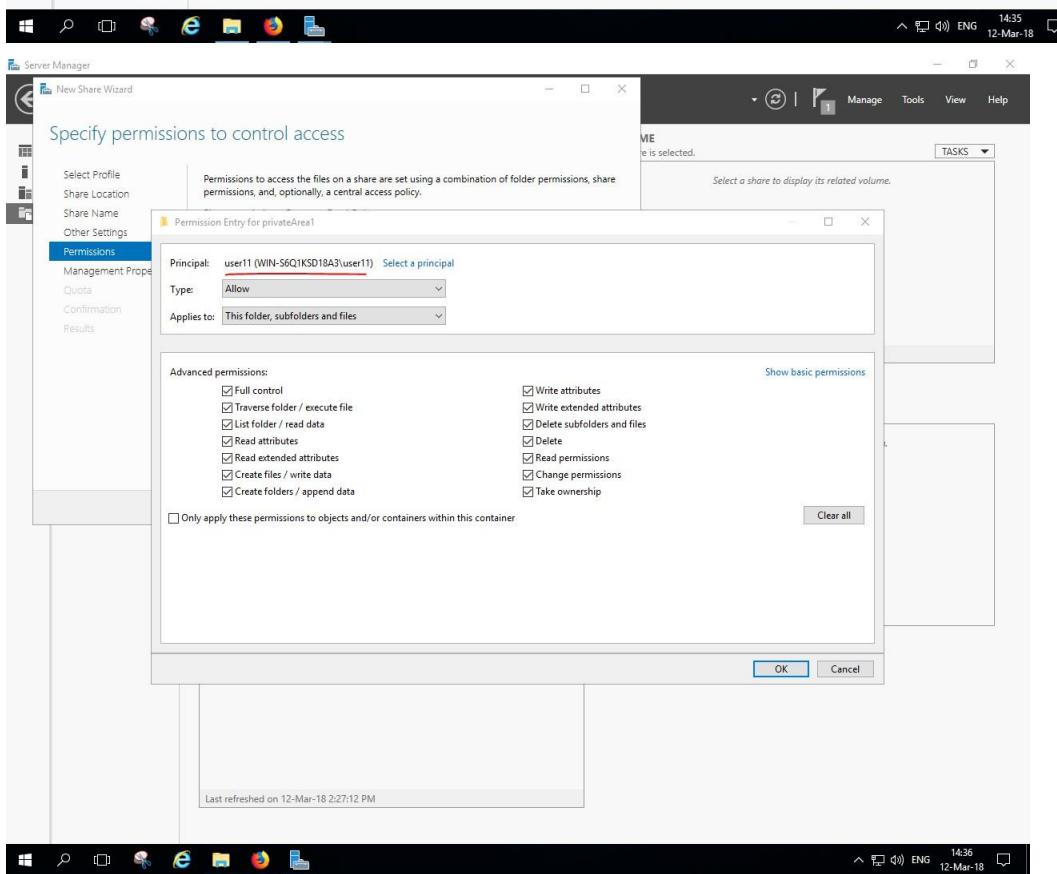
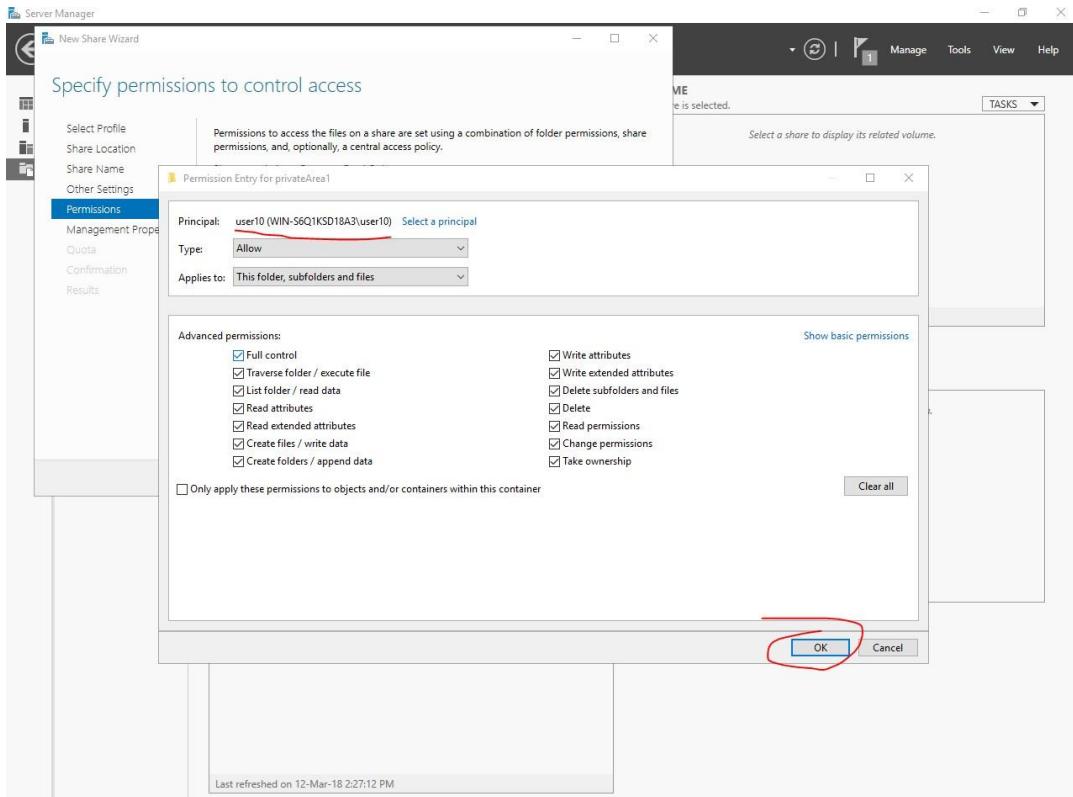
Παρακάτω φαίνεται η διαδικασία της επεξεργασίας των δικαιωμάτων που ζητά η άσκηση για κάθε ομάδα χρηστών.

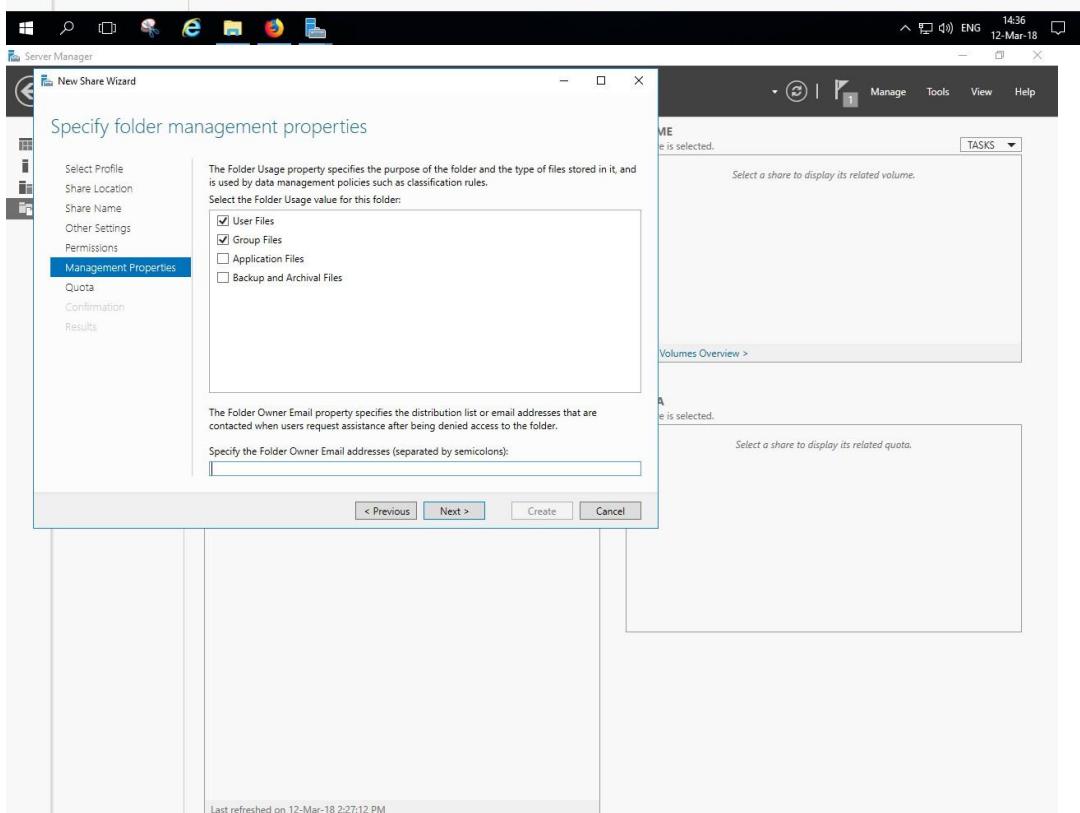
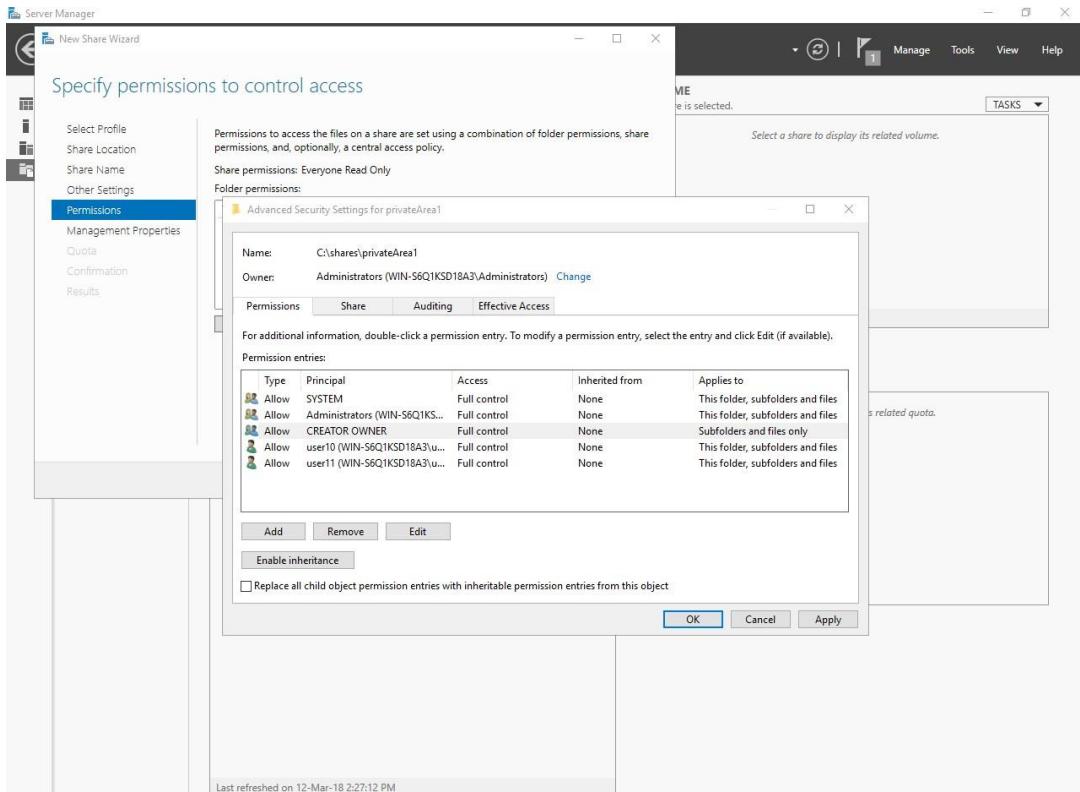


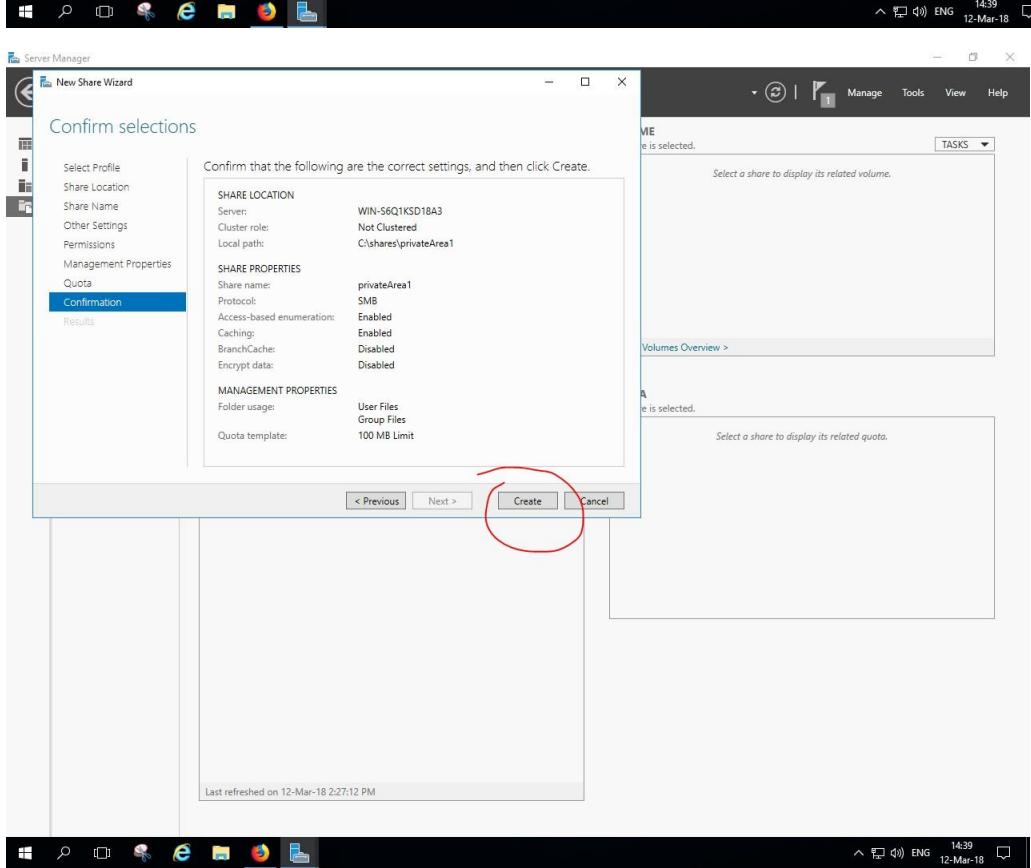
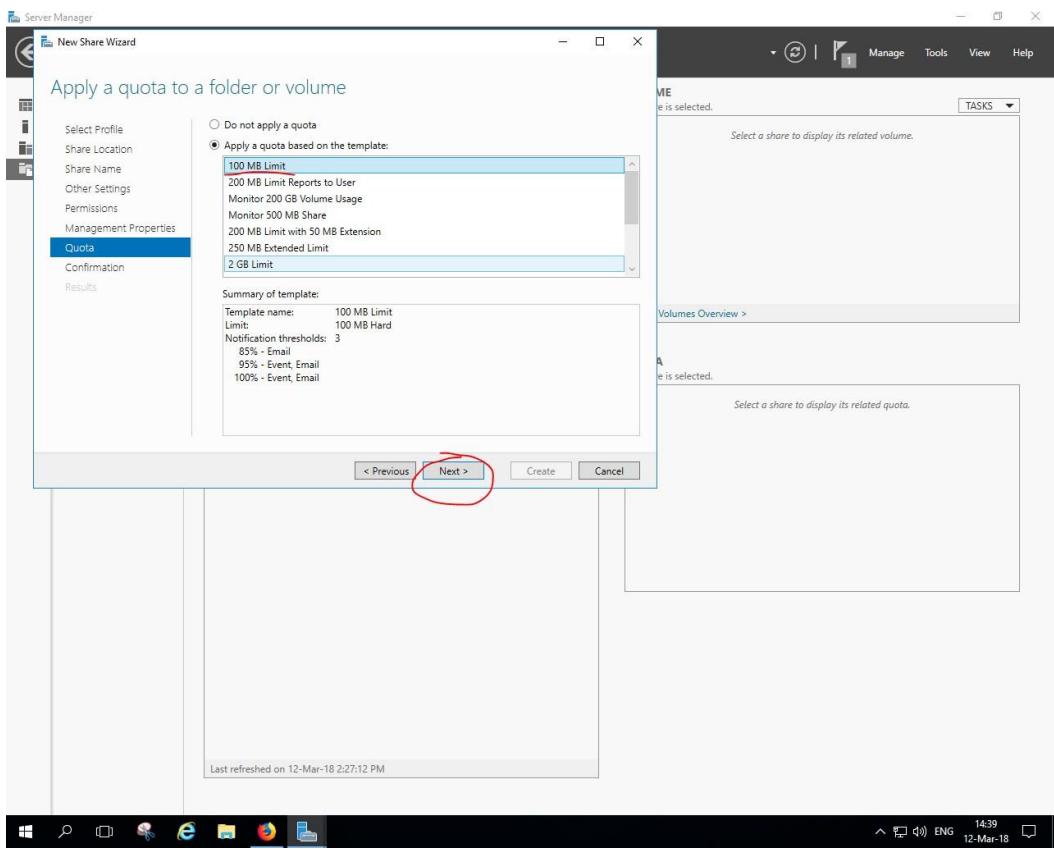
Αρχικά επεξεργάζομαι τα δικαιώματα για να μπορεί η 2^η ομάδα χρηστών να έχει **αποκλειστική** πρόσβαση. Επεξεργάζομαι και το που θα γίνει share αυτός ο φάκελος, αλλά αυτό φαίνεται παρακάτω γιατί σε αυτό το σημείο ξέχασα να το παραμετροποιήσω.

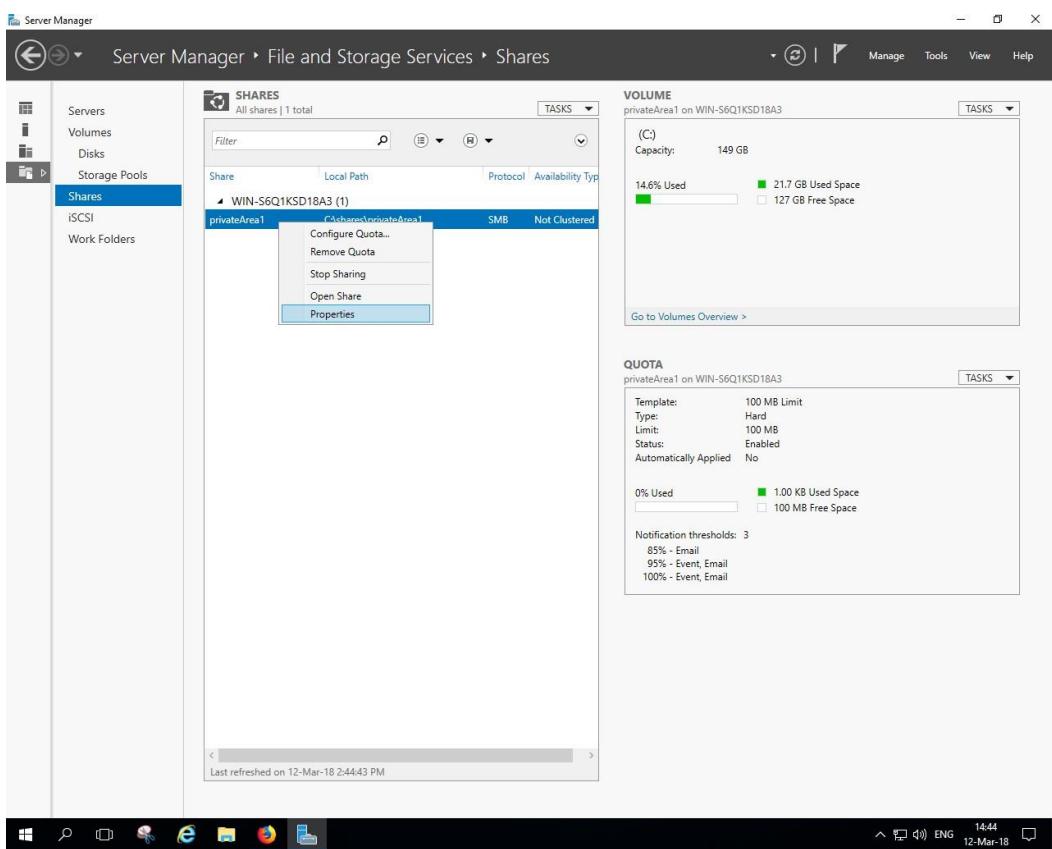
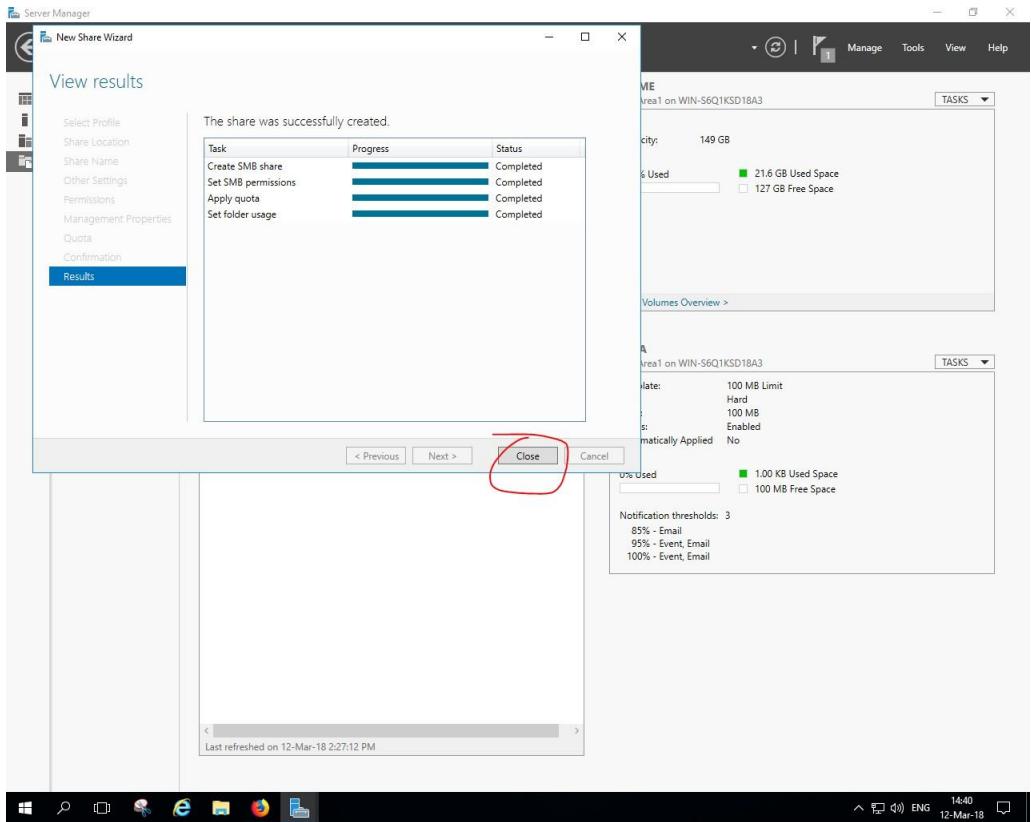
Στα permissions(όχι όμως στα share permissions) θα αφαιρέσω και τον administrator, αφού πρέπει να έχουν αποκλειστική πρόσβαση οι χρήστες. Στο αμέσως επόμενο print screen, θα επιλέξω την γραμμή του administrator και μετά θα πατήσω remove. Για να μπορέσω να έχω ευελιξία όμως στον πειραματισμό και στην παραμετροποίηση των φακέλων και των δικαιωμάτων τους, θα αφήσω τον administrator να έχει δικαιώματα.

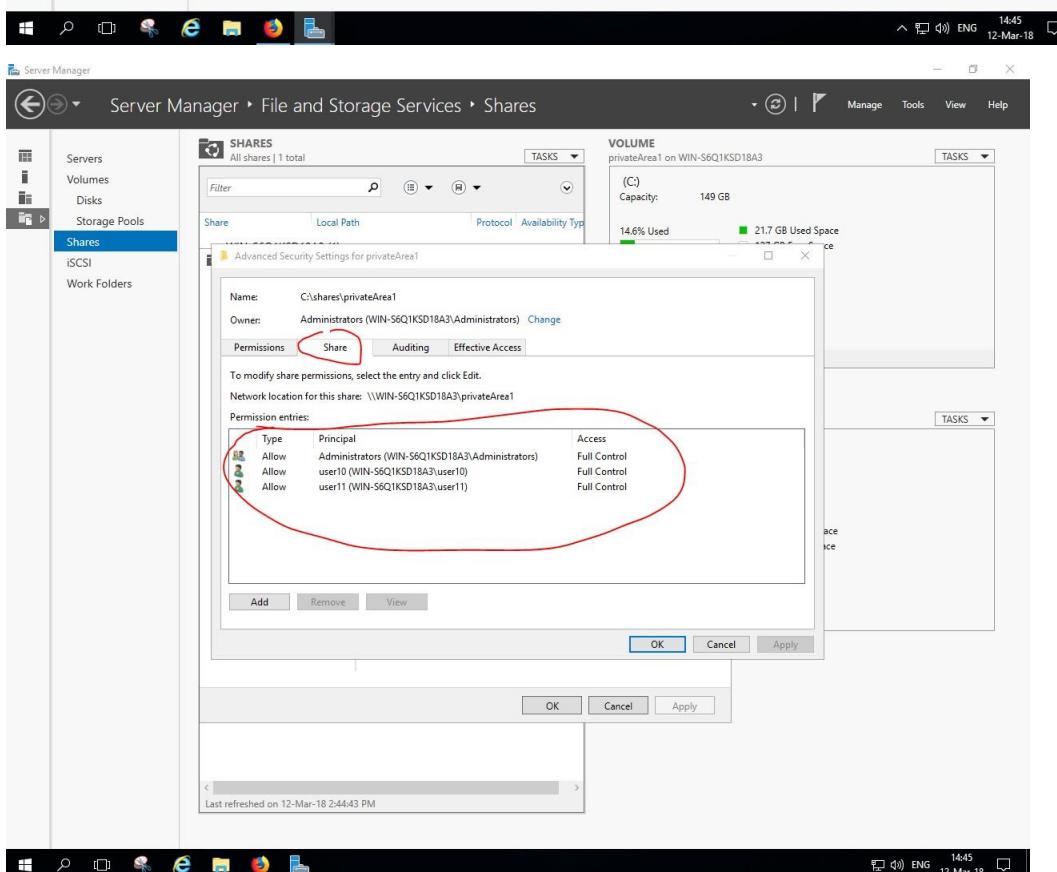
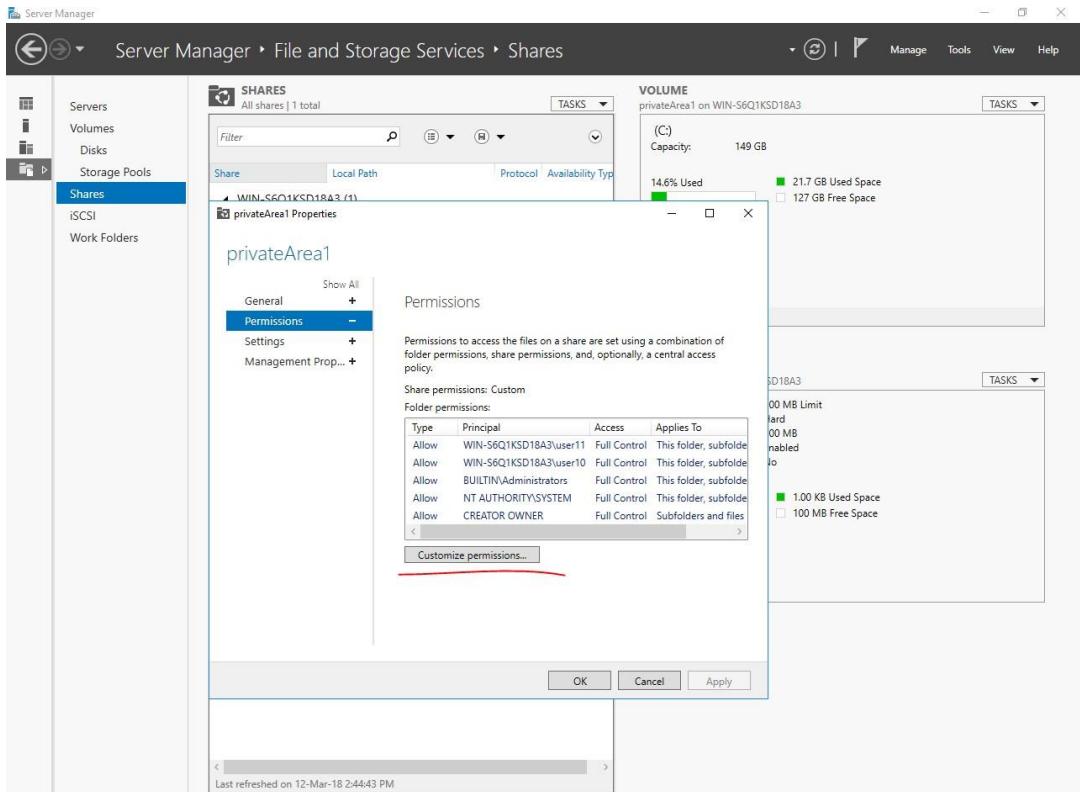




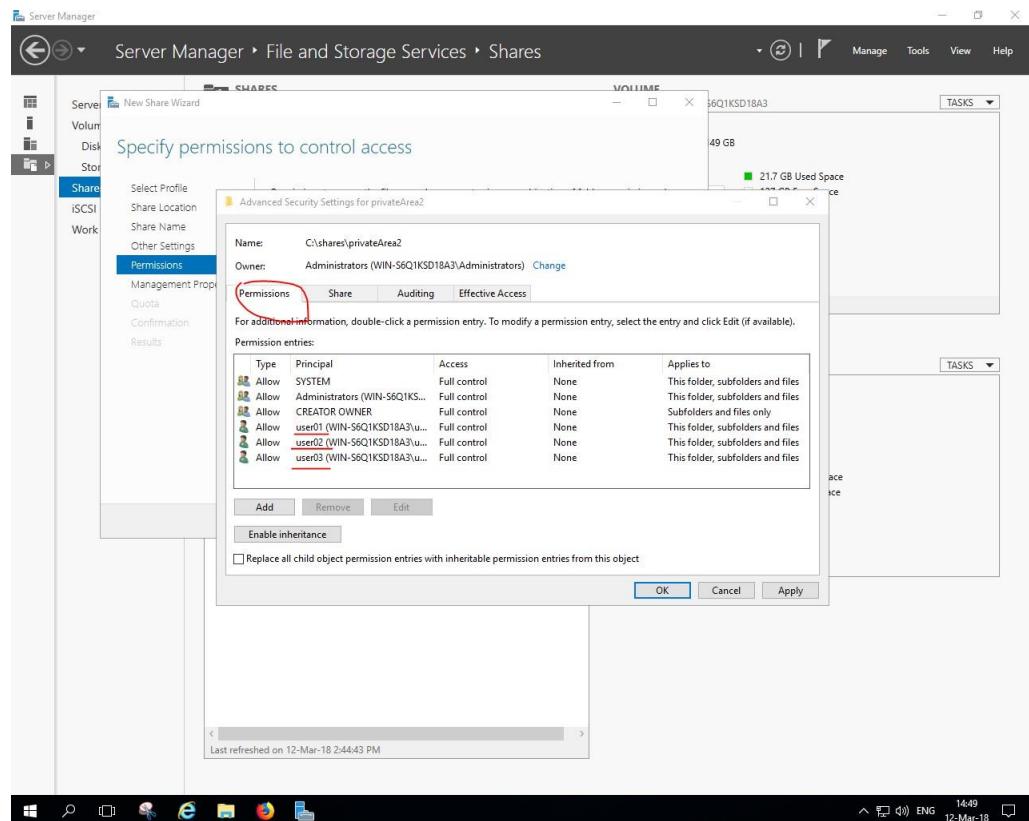


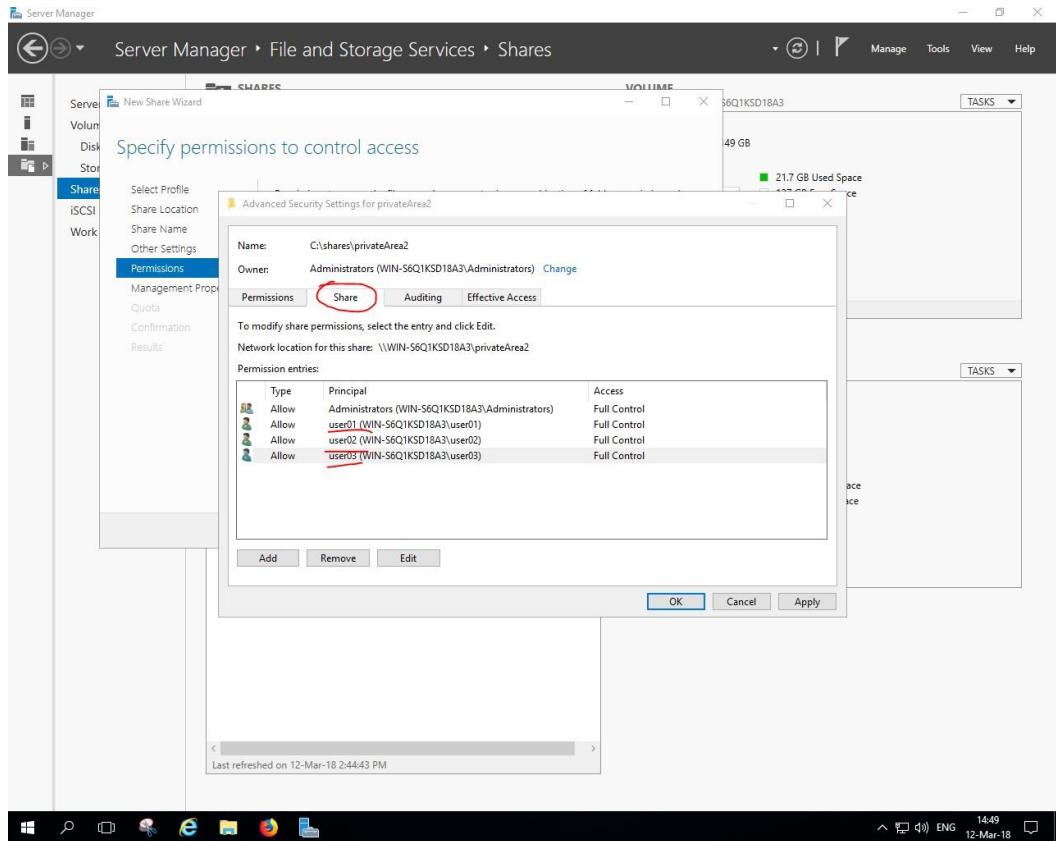




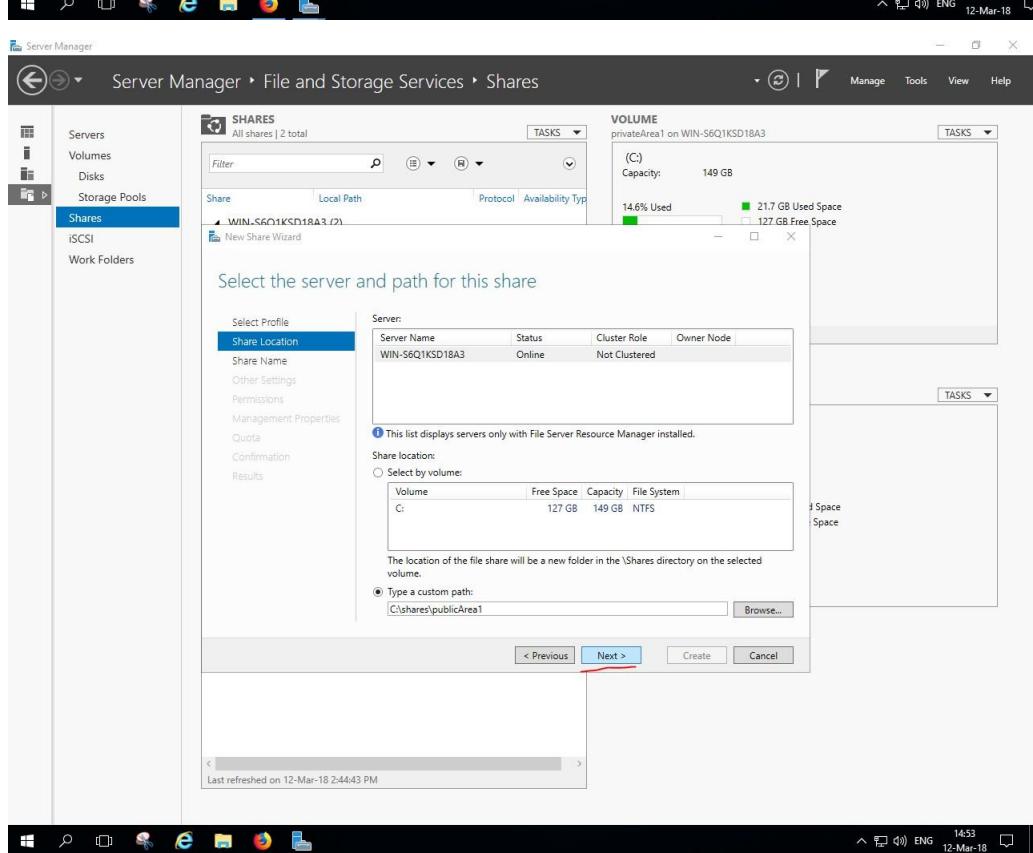
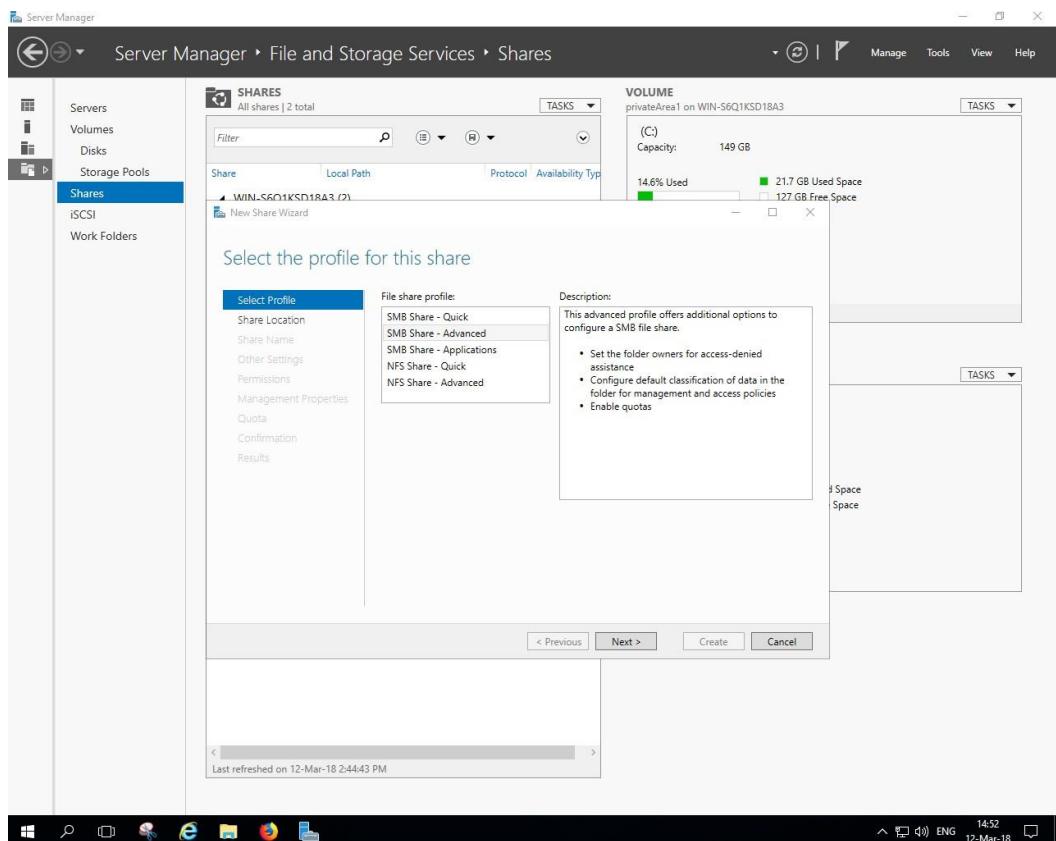


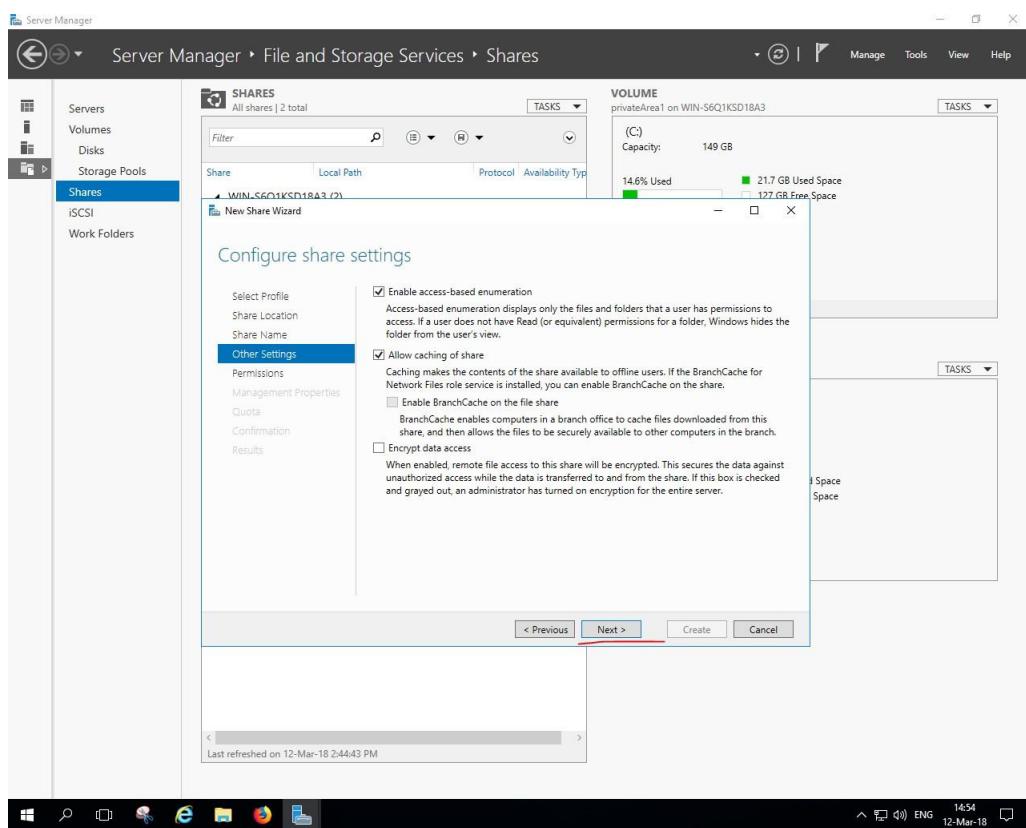
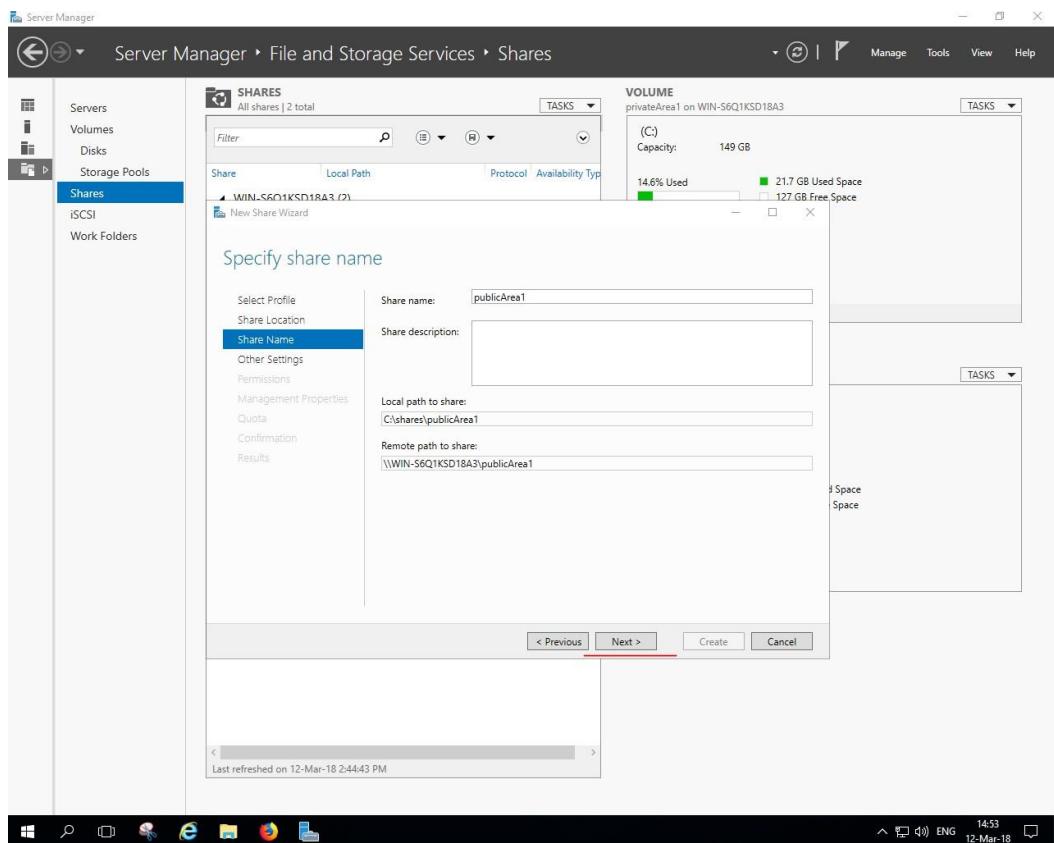
Η διαδικασία για την δημιουργία του privateArea2 είναι ακριβώς η ίδια απλά αλλάζουν οι χρήστες, όπου τώρα θα βάλω τους χρήστες της 1^η ομάδας

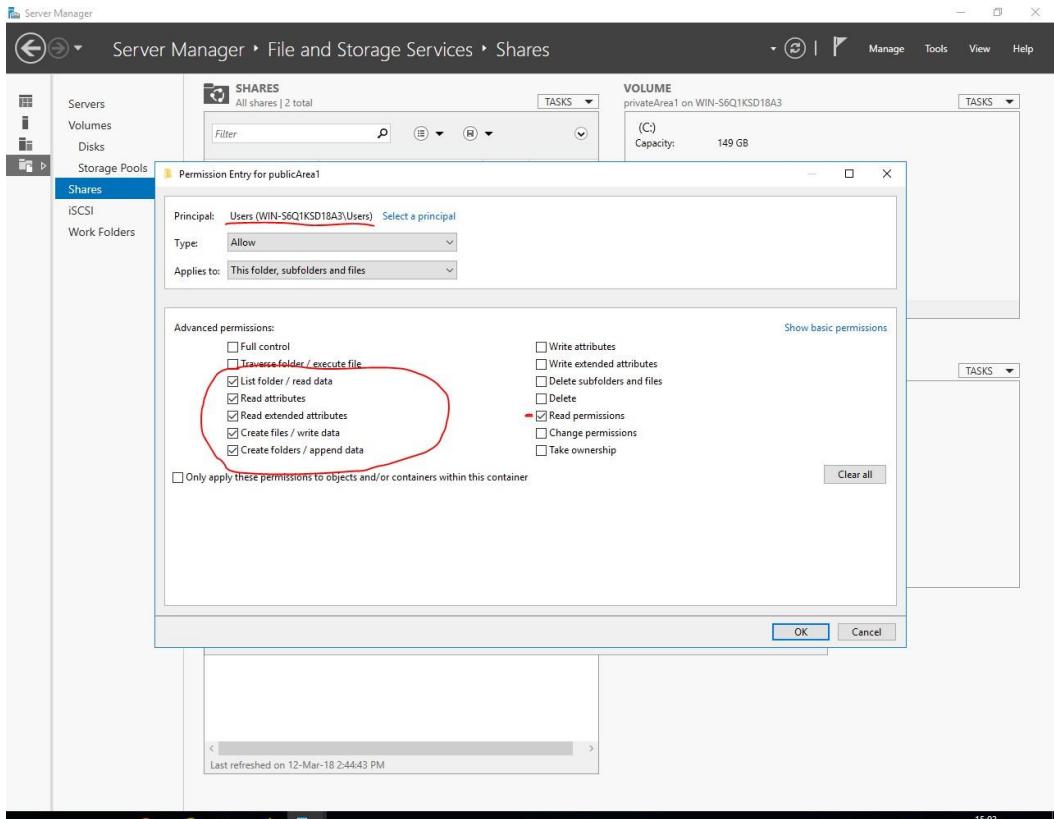
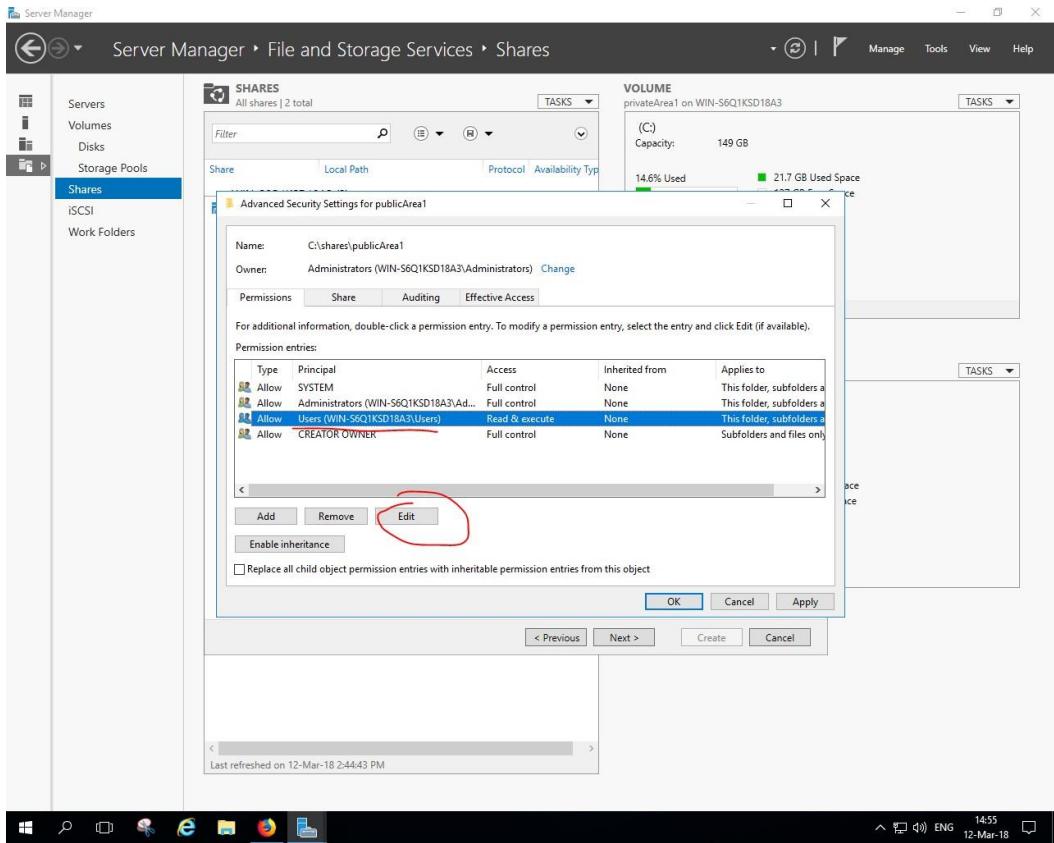


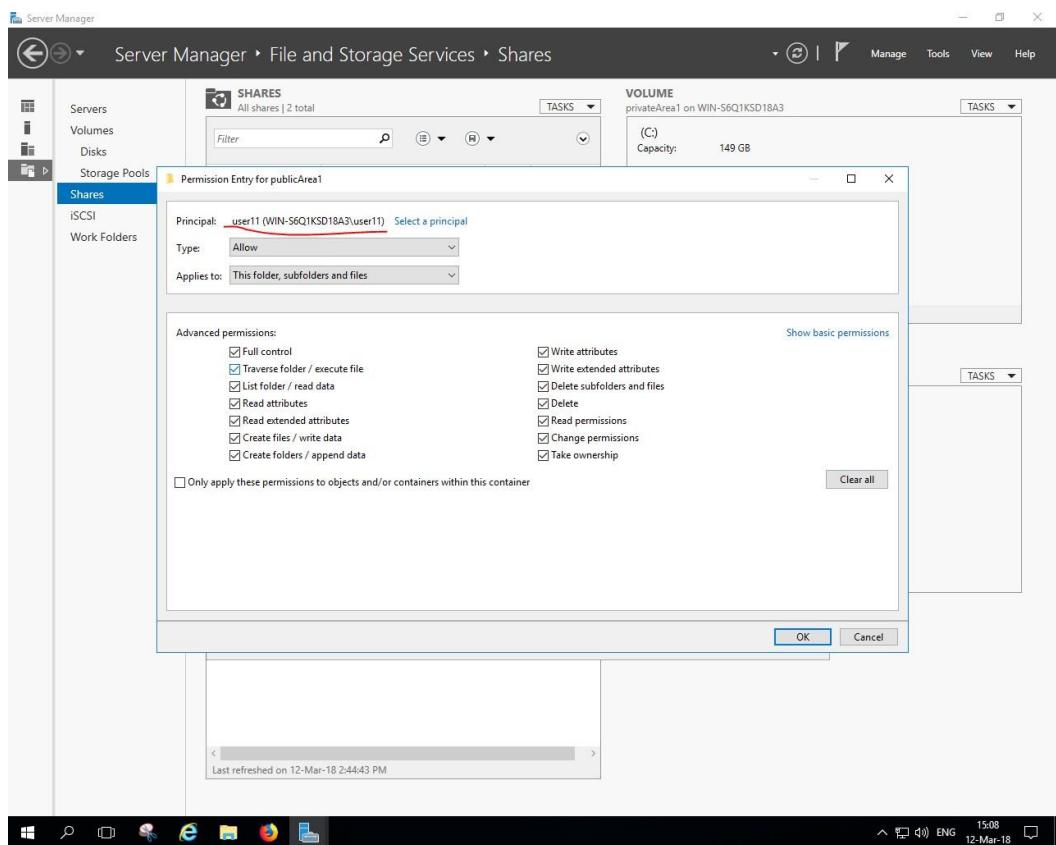
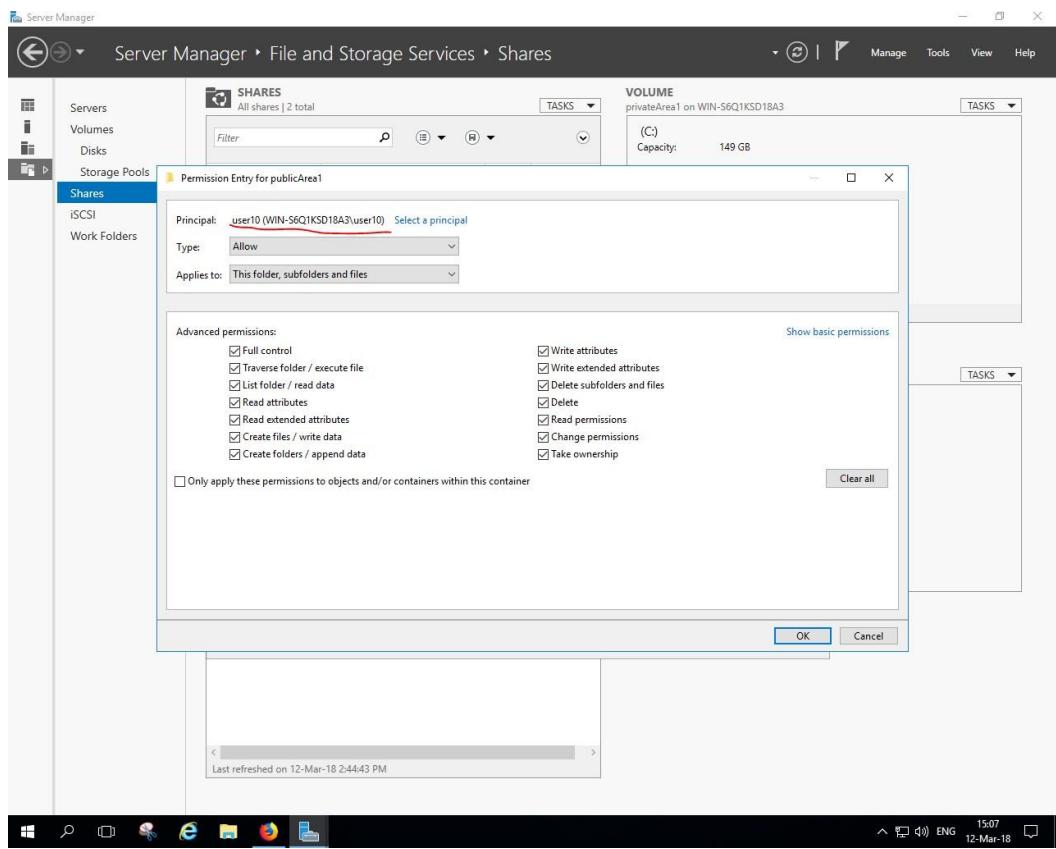


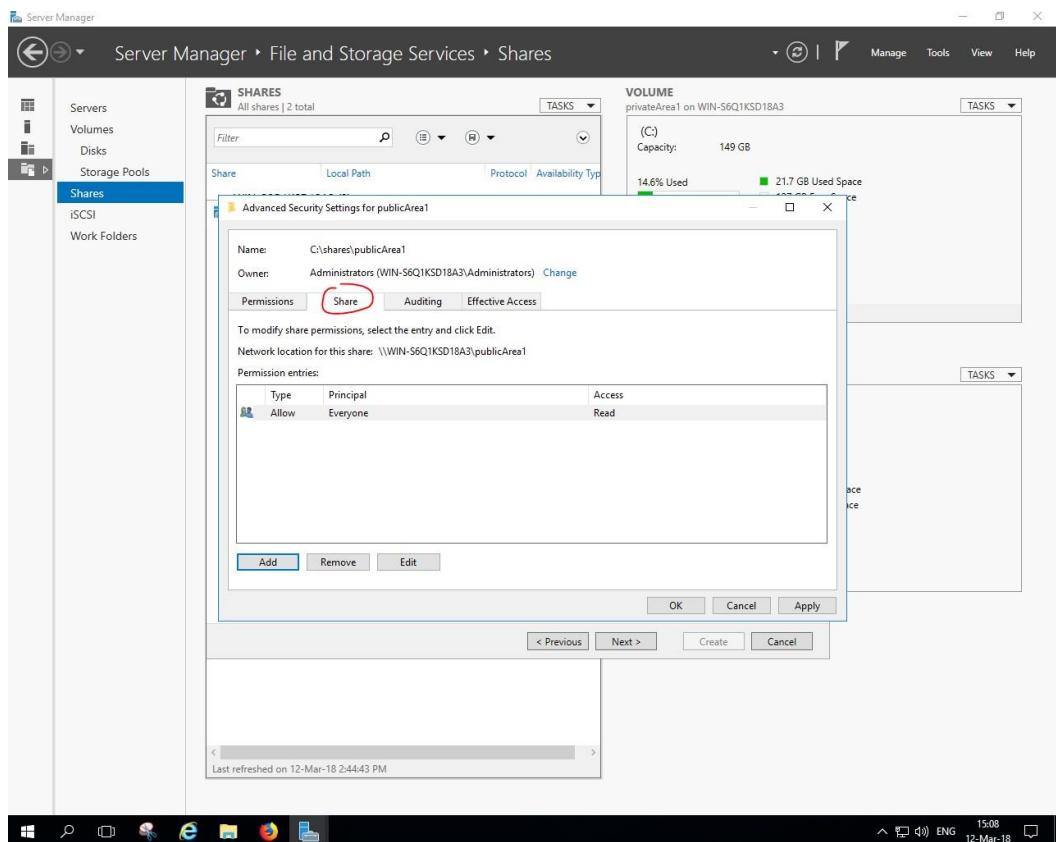
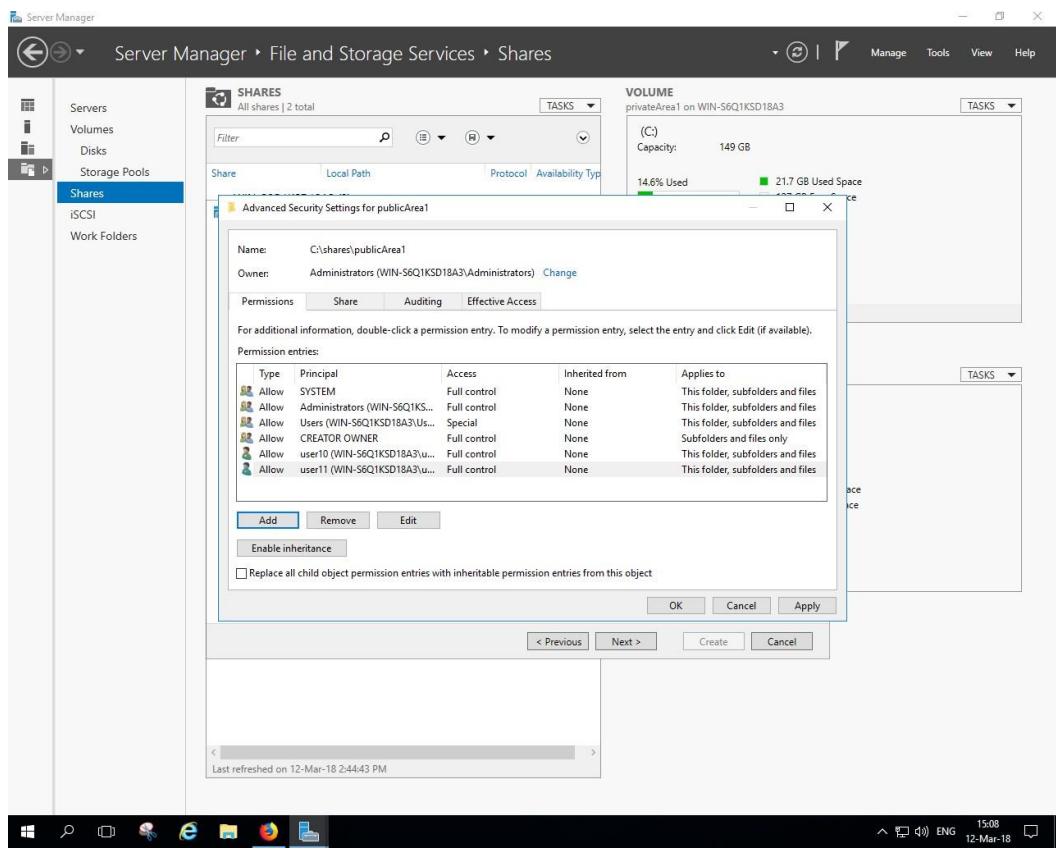
Παρακάτω φαίνεται η διαδικασία δημιουργίας των publicArea1,2. Η διαδικασία είναι ακριβώς η ίδια με αυτήν για την δημιουργία των privateArea1,2 με την μόνη διαφορά να είναι στα δικαιώματα που δίνω στους χρήστες. Οι διαφορές φαίνονται στα screenshot

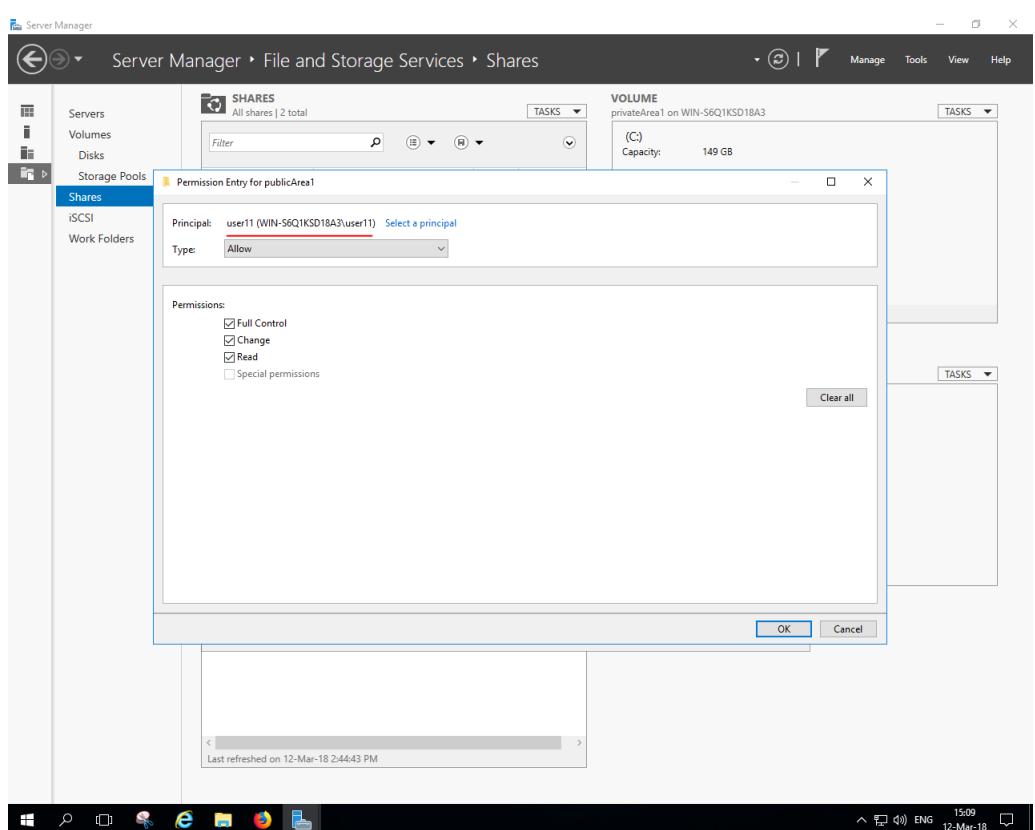
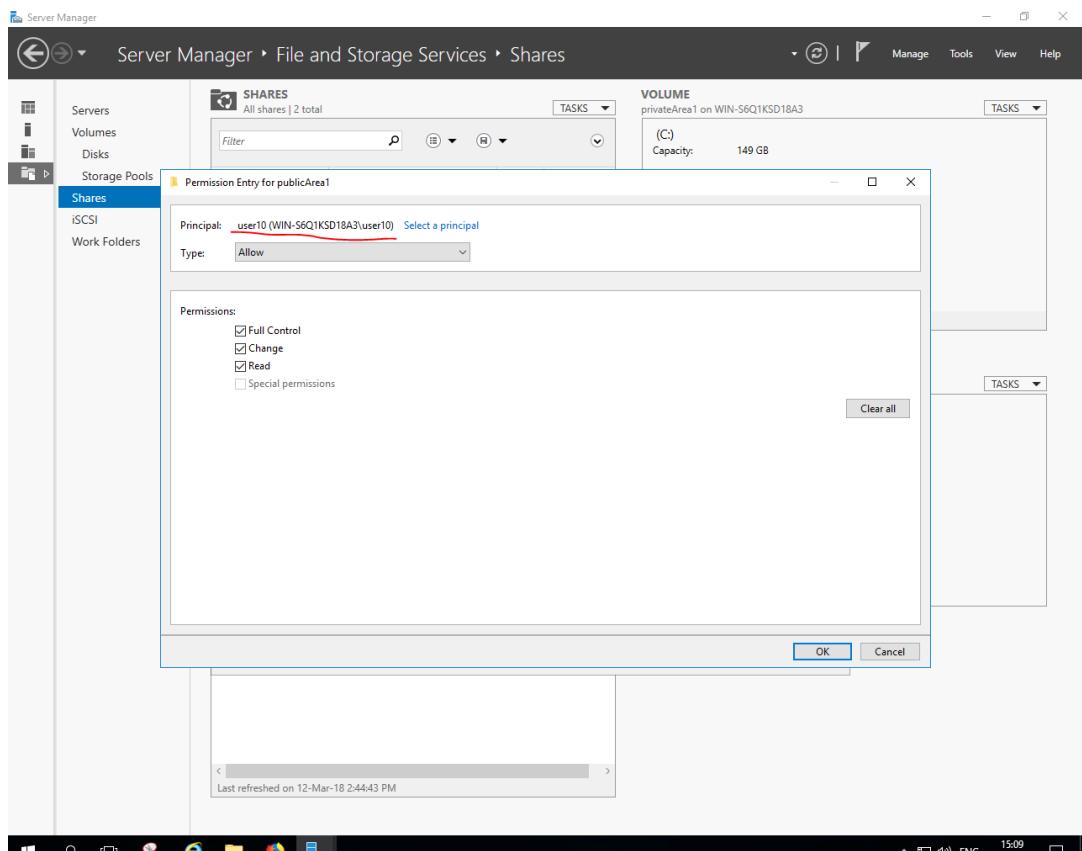


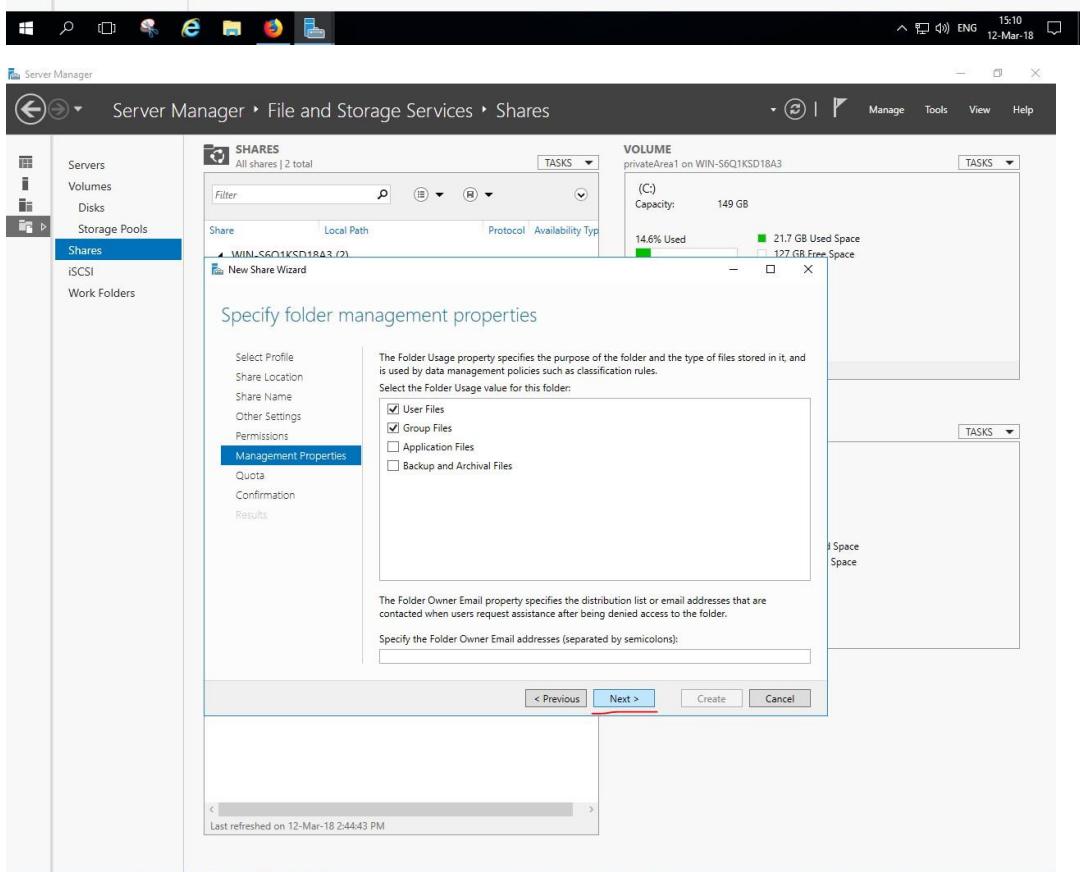
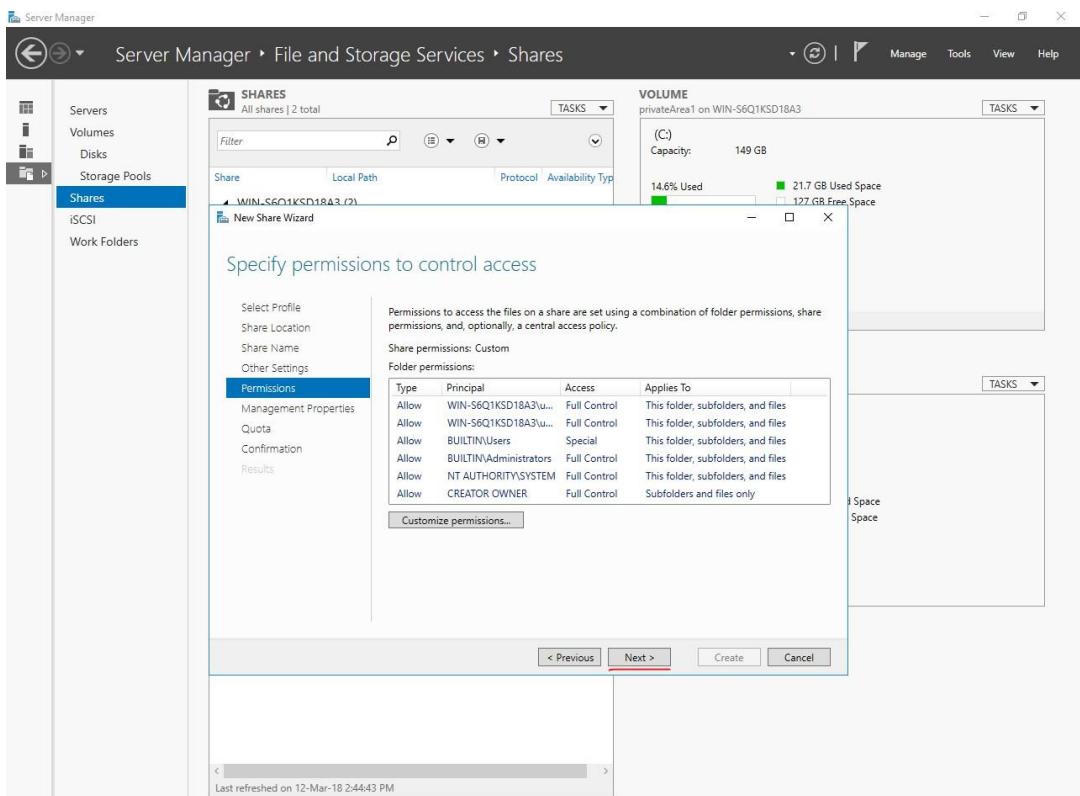


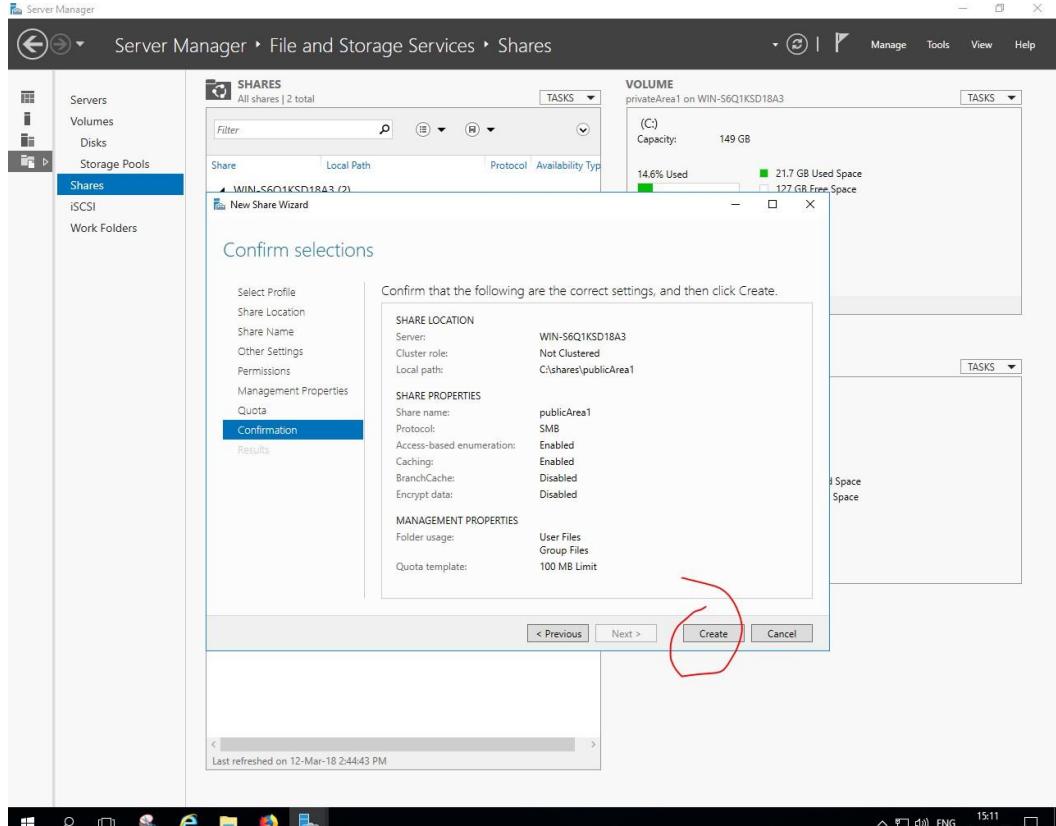
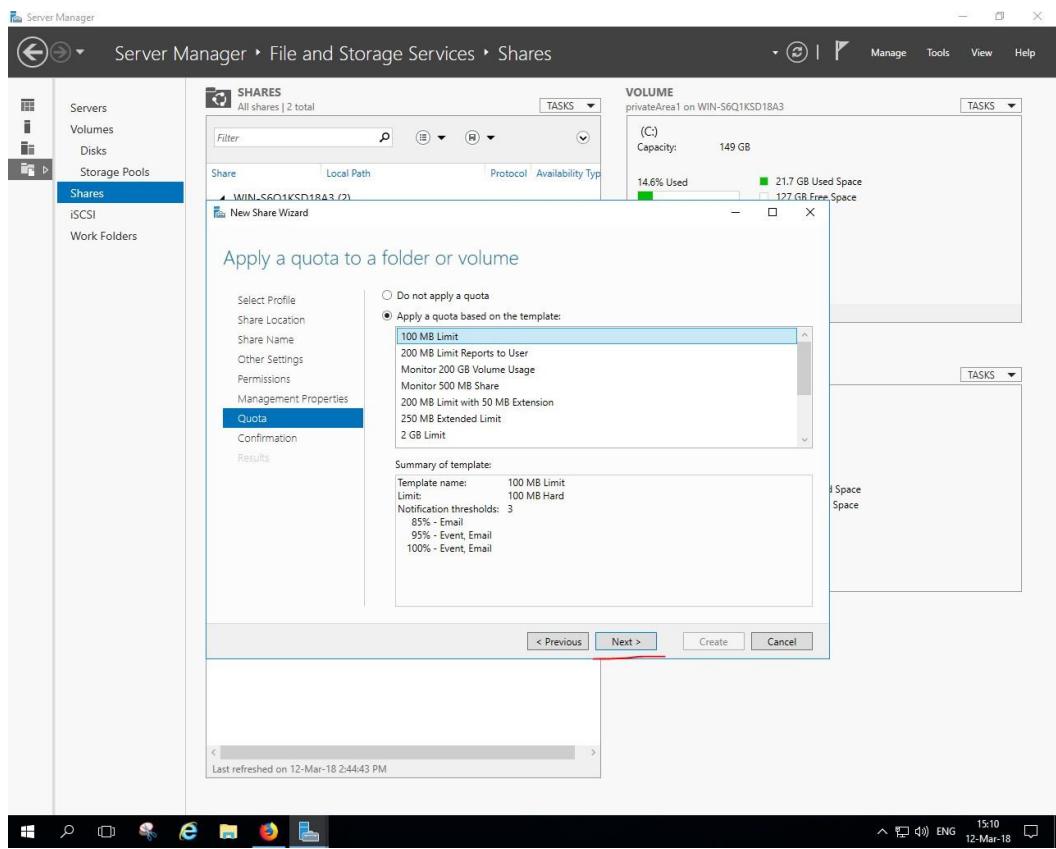


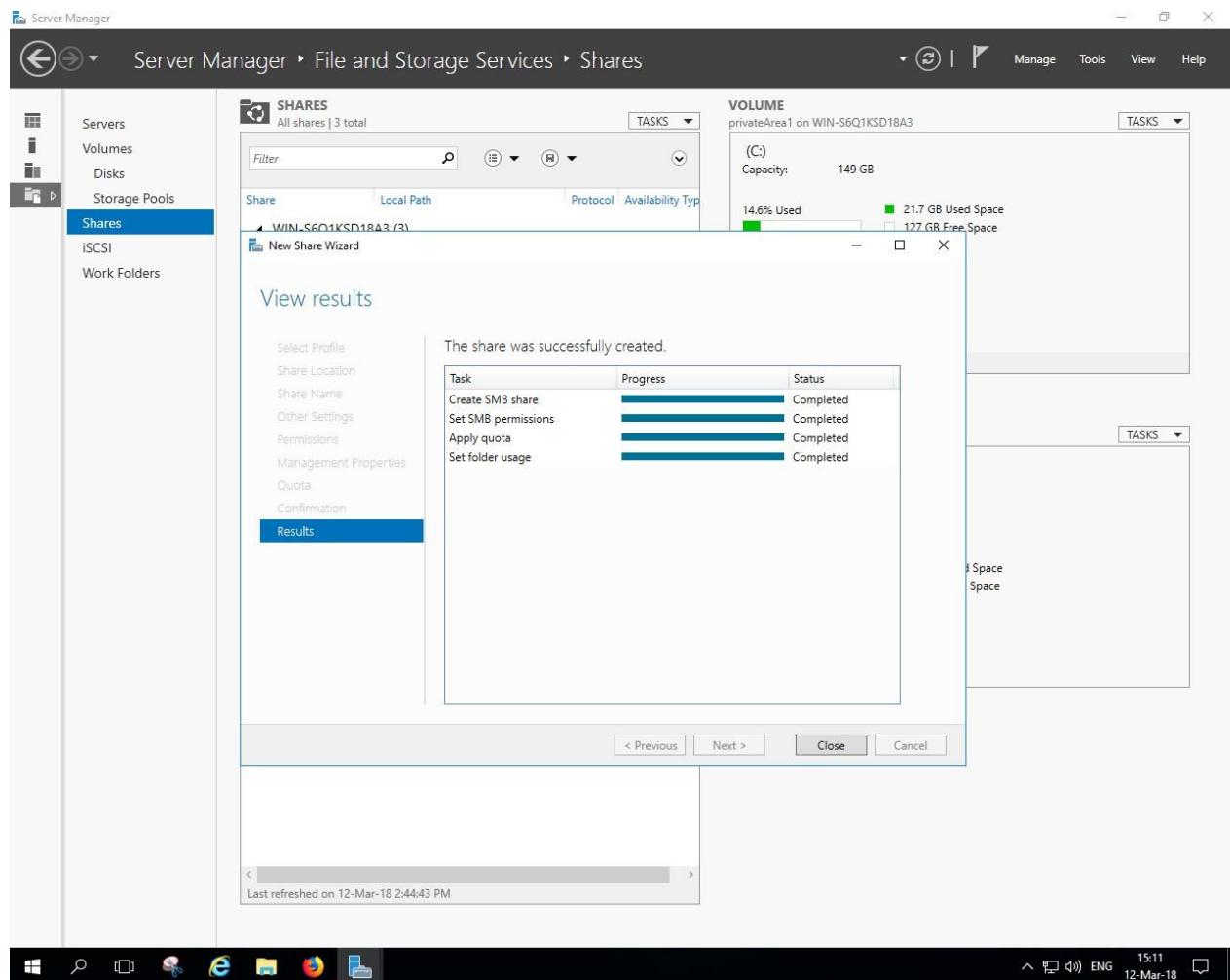






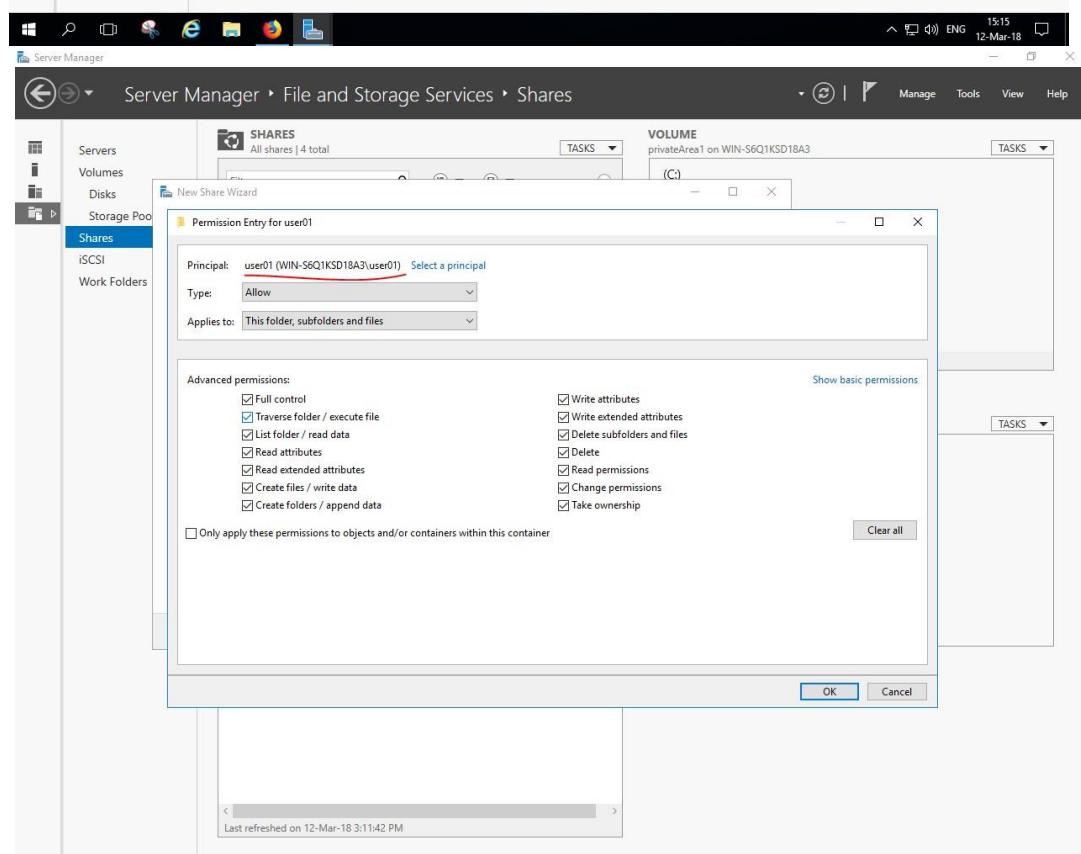
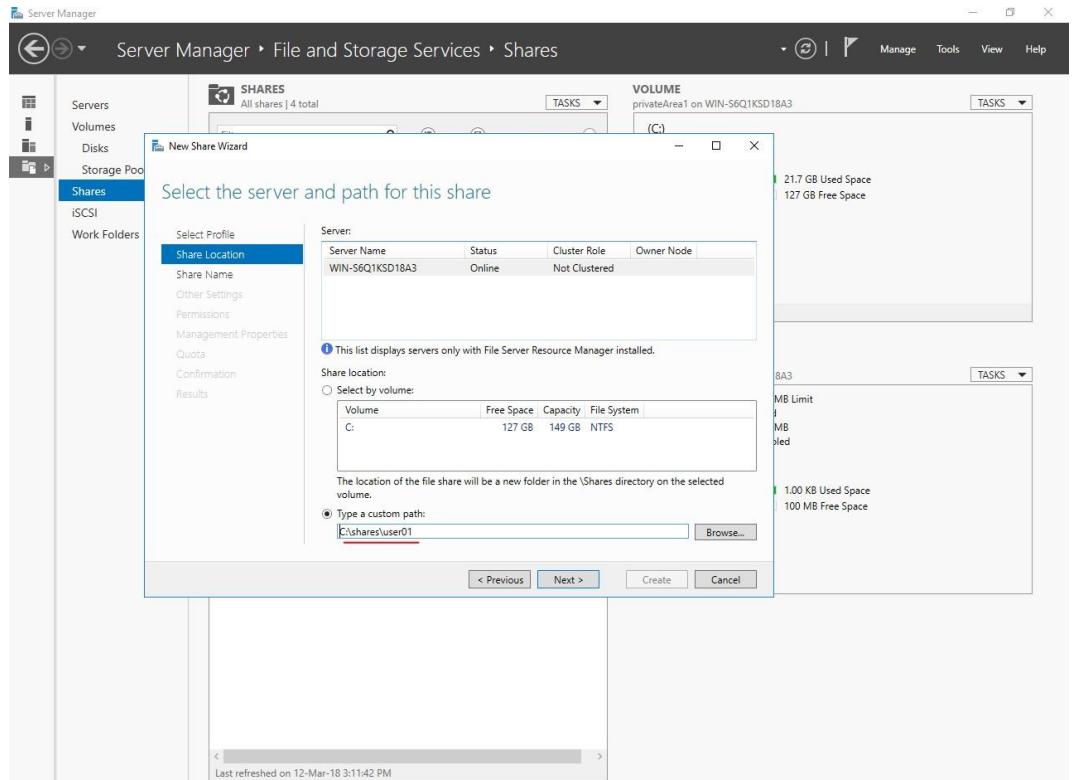


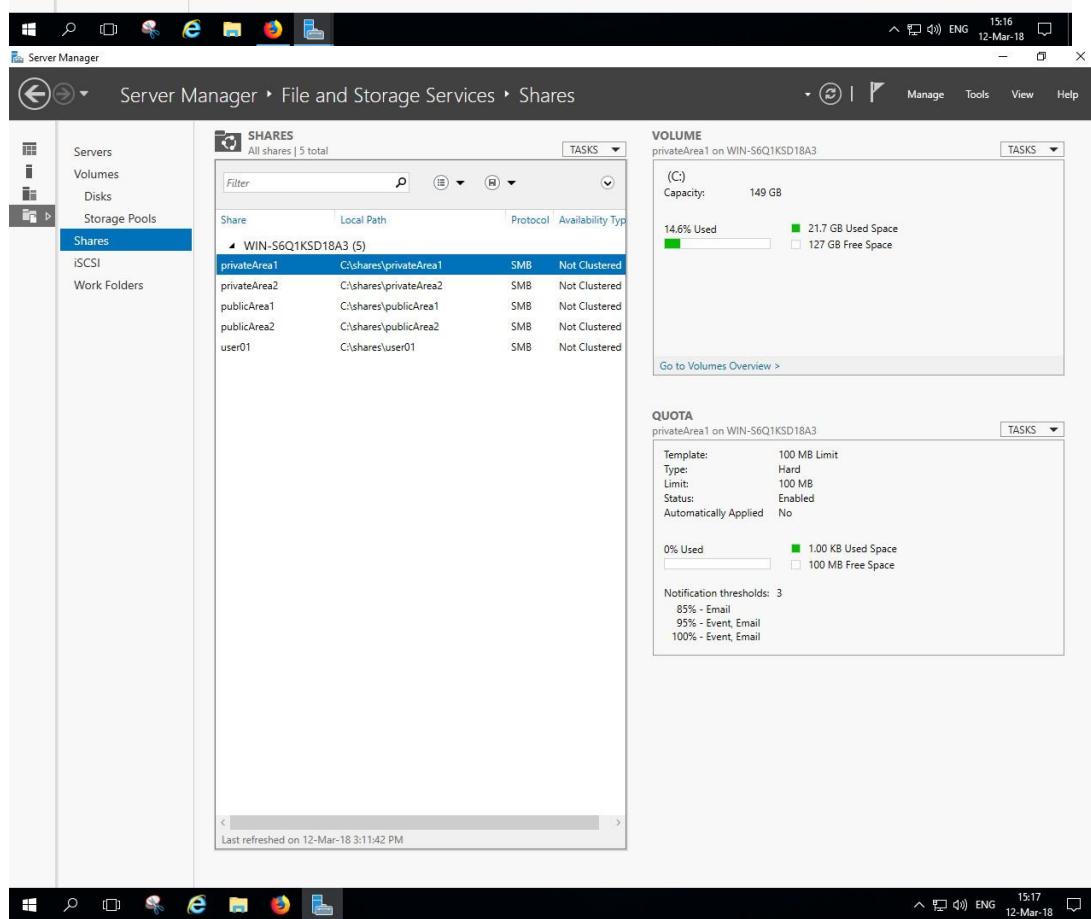
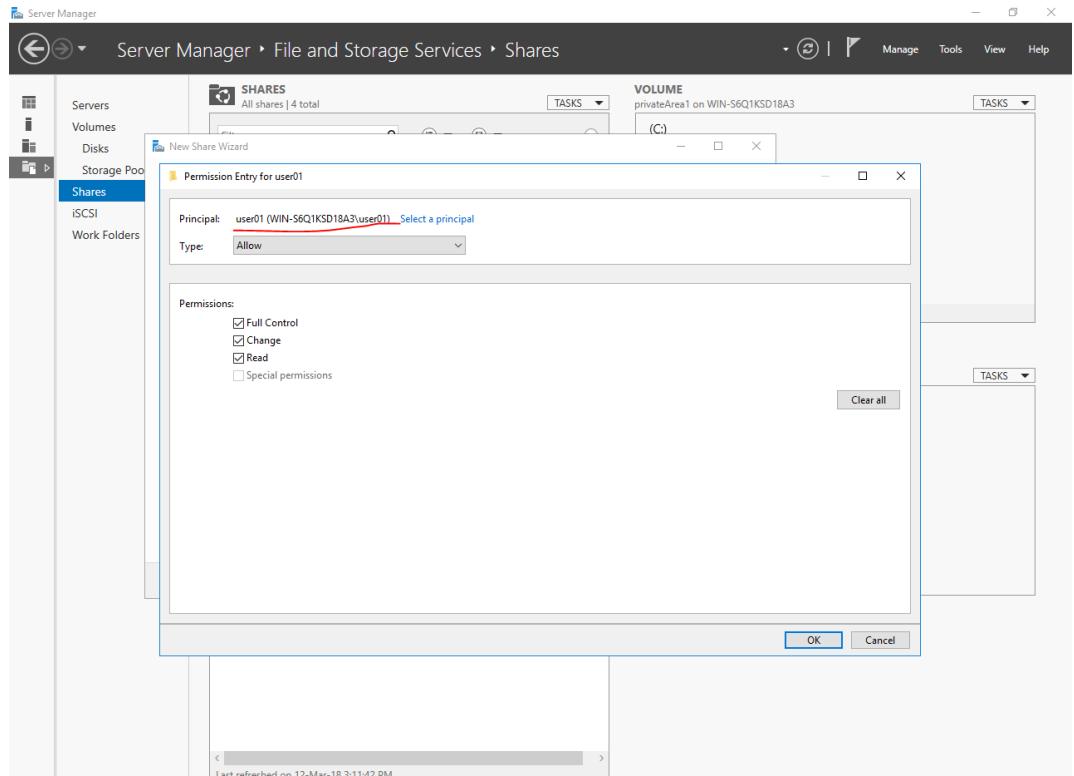




3.3 Δημιουργία φακέλων χρηστών

Παρακάτω φαίνεται η δημιουργία ενός αποθηκευτικού φακέλου για τον user01, στον οποίο έχει αποκλειστική πρόσβαση αυτός.





Η διαδικασία για όλους τους υπόλοιπους χρήστες είναι ακριβώς η ίδια.

Στην συνέχεια, θέλουμε να αποκλείσουμε προσωρινά τον χρήστη user11 από την privateArea1.

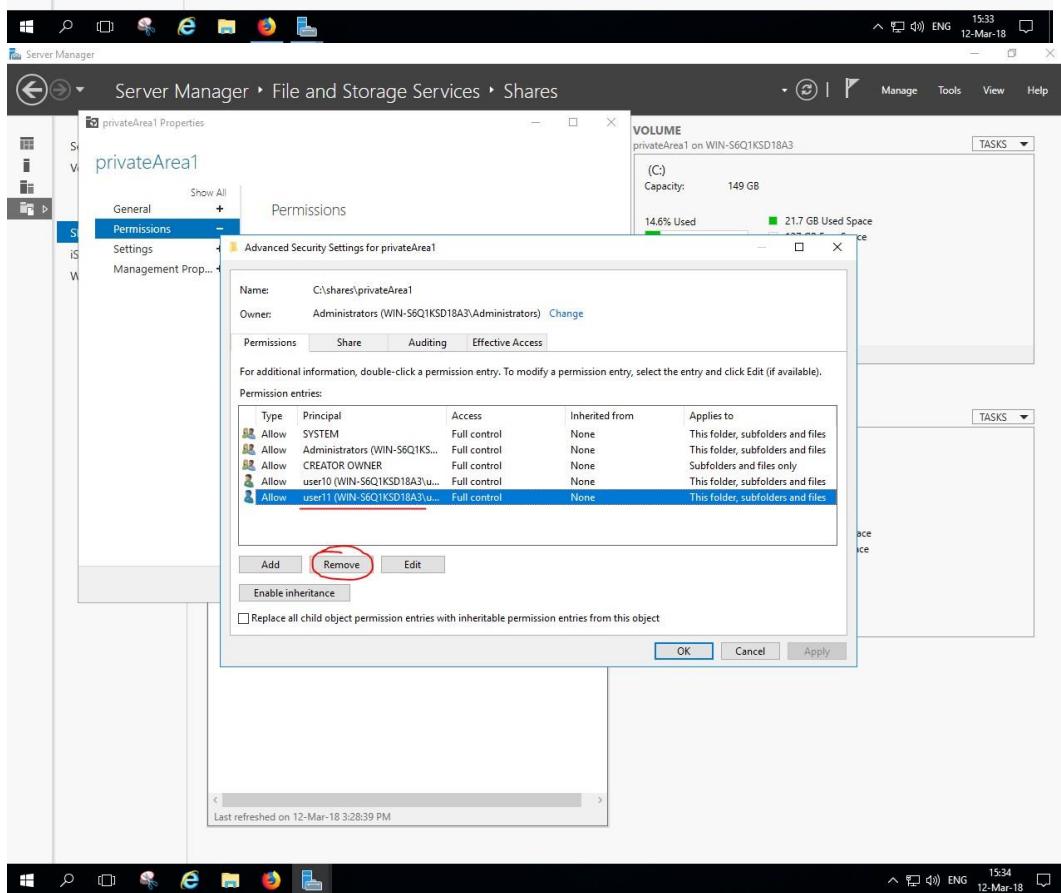
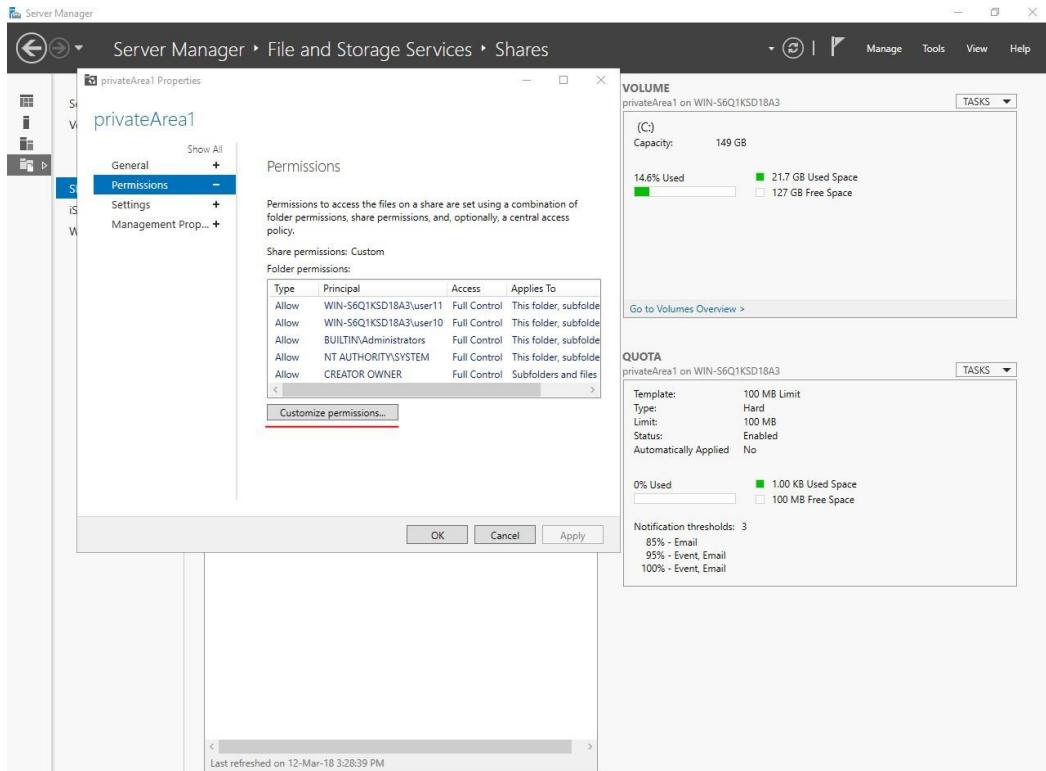
Το μόνο που θα αλλάξουμε είναι τα δικαιώματα πρόσβασης που έχει ο χρήστης. Ο φάκελος θα συνεχίσει να είναι share στον χρήστη user11 απλά δεν θα έχει δικαιώματα πρόσβασης σε αυτόν.

The screenshot shows the Windows Server Manager interface. The left navigation pane is collapsed. The main content area has two tabs: 'SHARES' and 'VOLUME'. The 'SHARES' tab is selected, displaying a list of shares under 'WIN-S6Q1KSD18A3 (5)'. One share, 'privateArea1', is selected and its properties are shown in a context menu:

- Configure Quota...
- Remove Quota
- Stop Sharing
- Open Share
- Properties

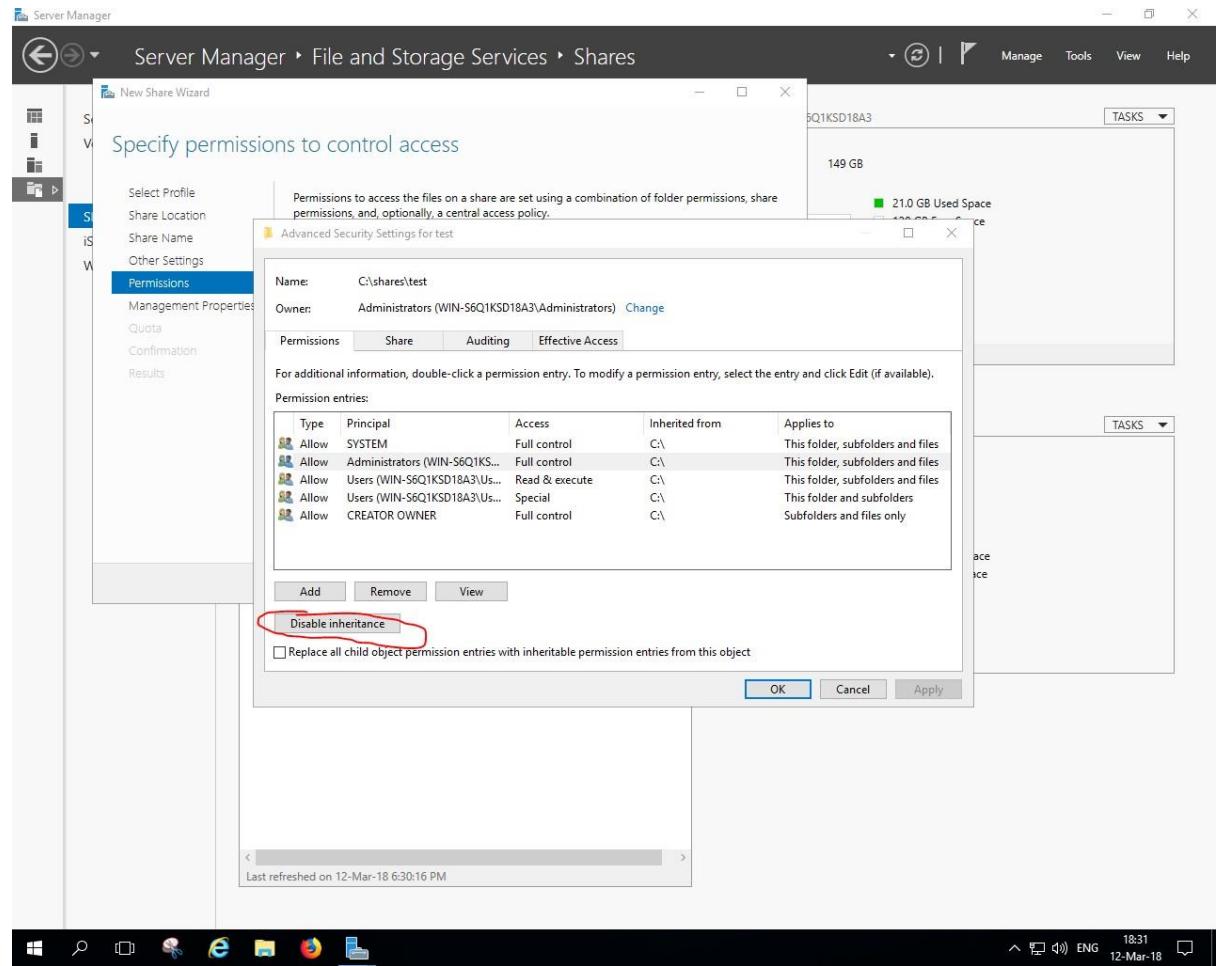
The 'VOLUME' tab is also selected, showing details for volume '(C:)'. Capacity is 149 GB, with 14.6% Used (21.7 GB Used Space, 127 GB Free Space). The 'QUOTA' tab shows a quota entry for 'privateArea1' with a limit of 100 MB.

At the bottom, the taskbar shows various icons (Windows, Search, Task View, Internet Explorer, Mail, Firefox, File Explorer) and system status (15:33, ENG, 12-Mar-18).

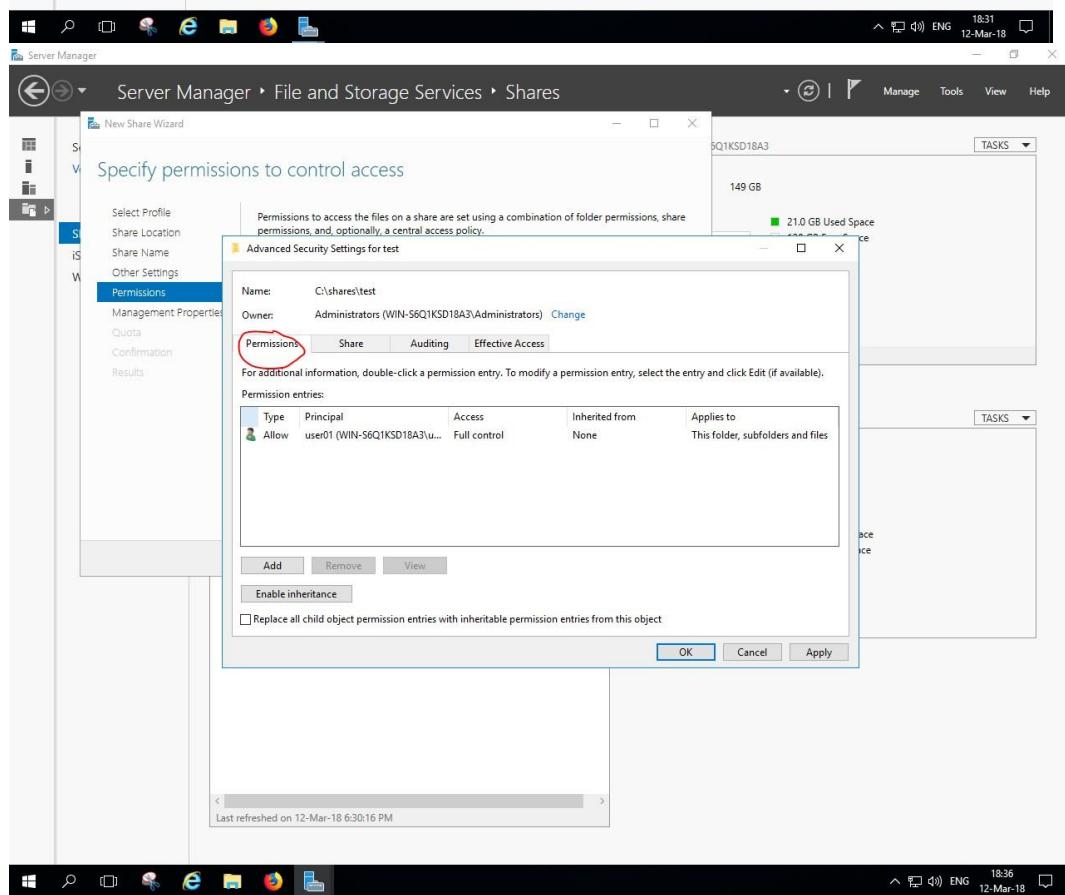
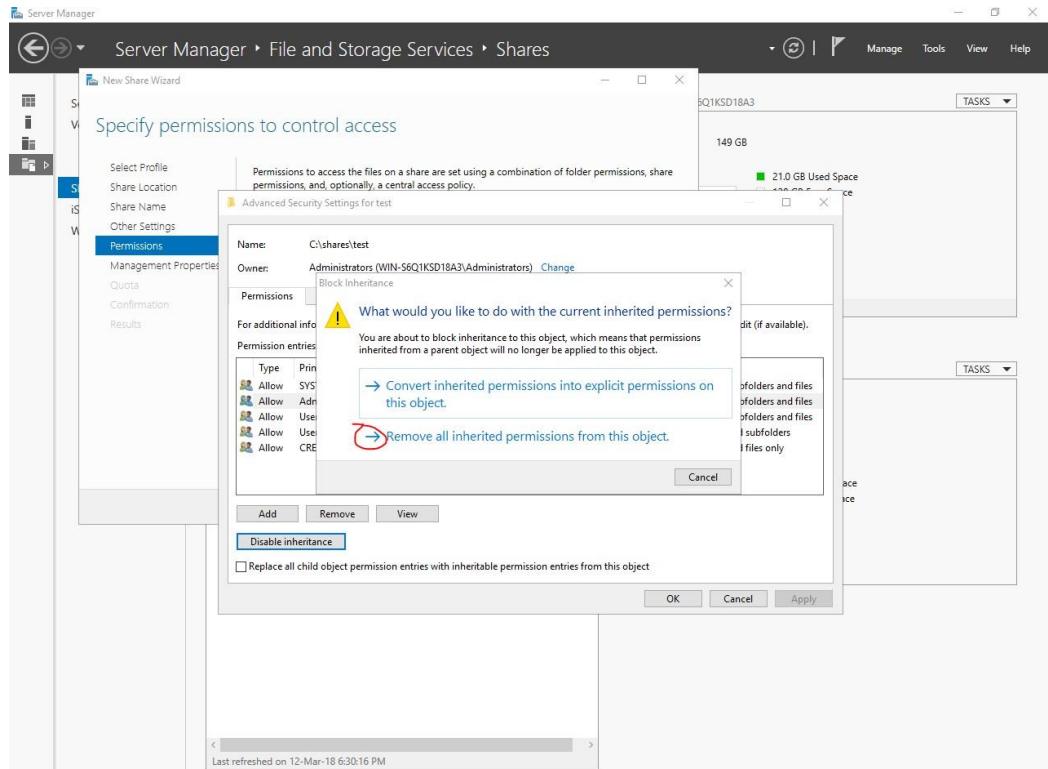


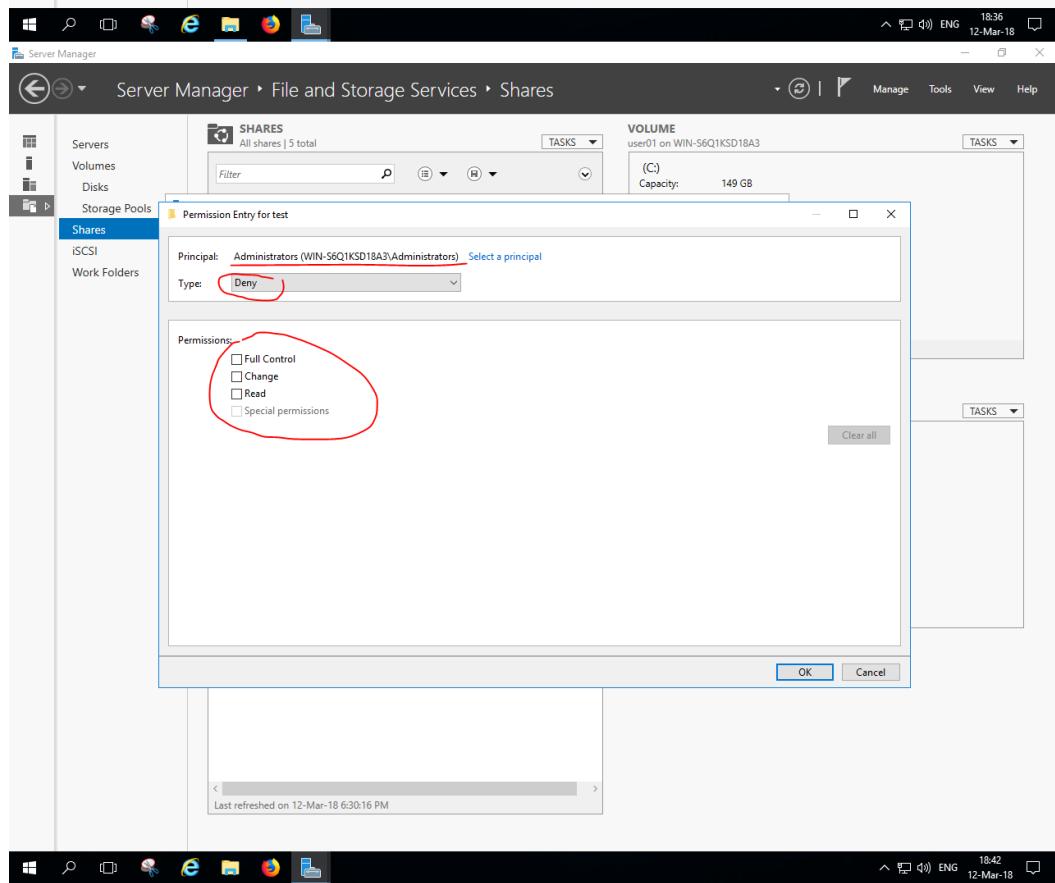
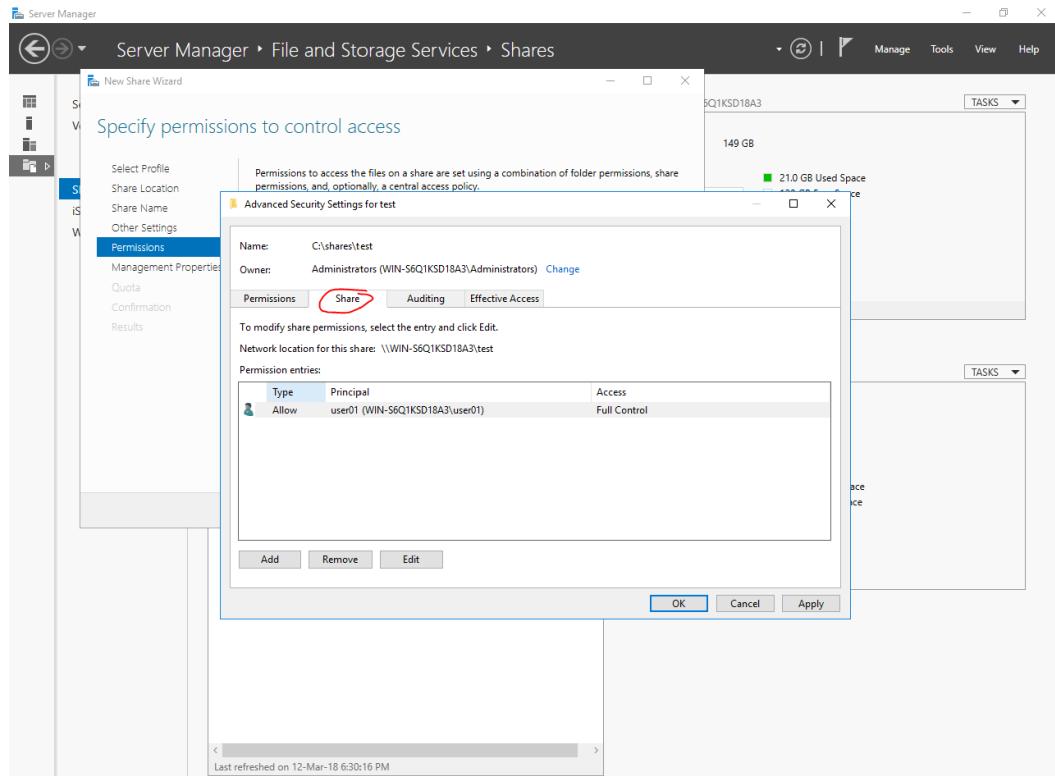
3.4 Θεωρητικά Ερωτήματα

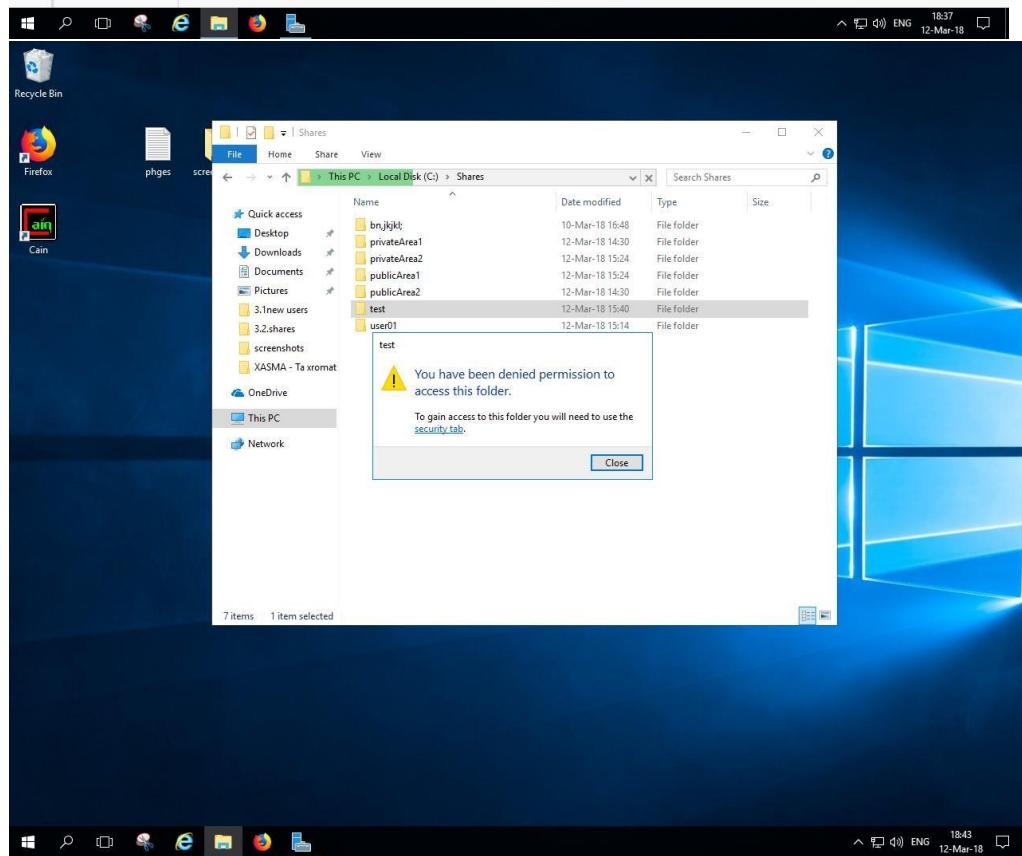
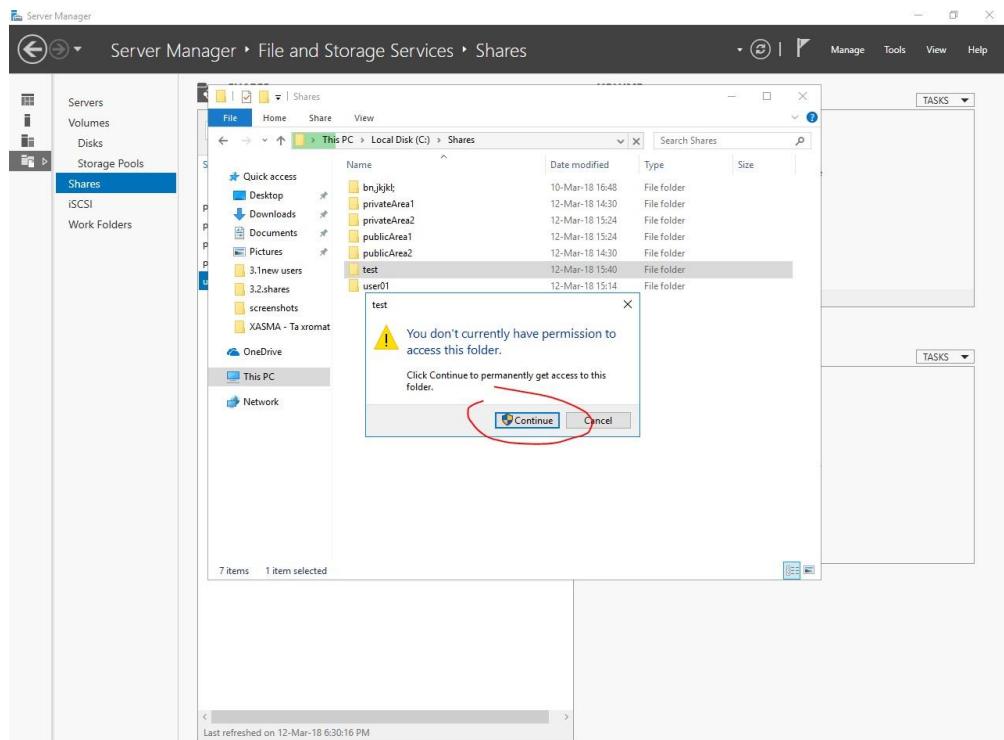
- Υπάρχει τρόπος να αποτραπεί η πρόσβαση σε μια συγκεκριμένη περιοχή από τους διαχειριστές του συστήματος, αν αφαιρέσουμε τα δικαιώματα πρόσβασης σε έναν φάκελο για τους διαχειριστές. Παρακάτω φαίνεται αναλυτικά



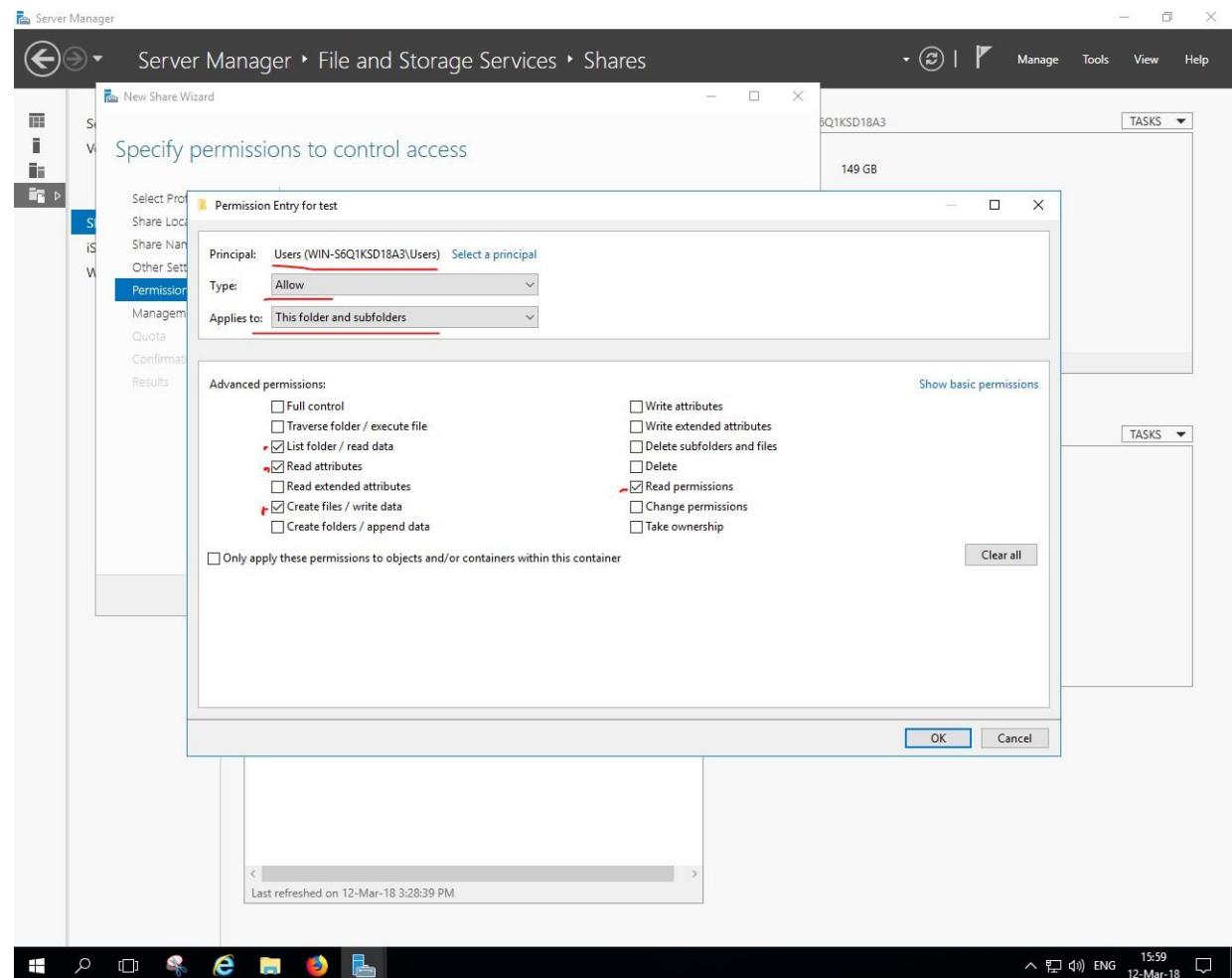
Κάνουμε disable την συγκεκριμένη επιλογή για να μπορέσουμε να αφαιρέσουμε τους διαχειριστές από τα δικαιώματα πρόσβασης



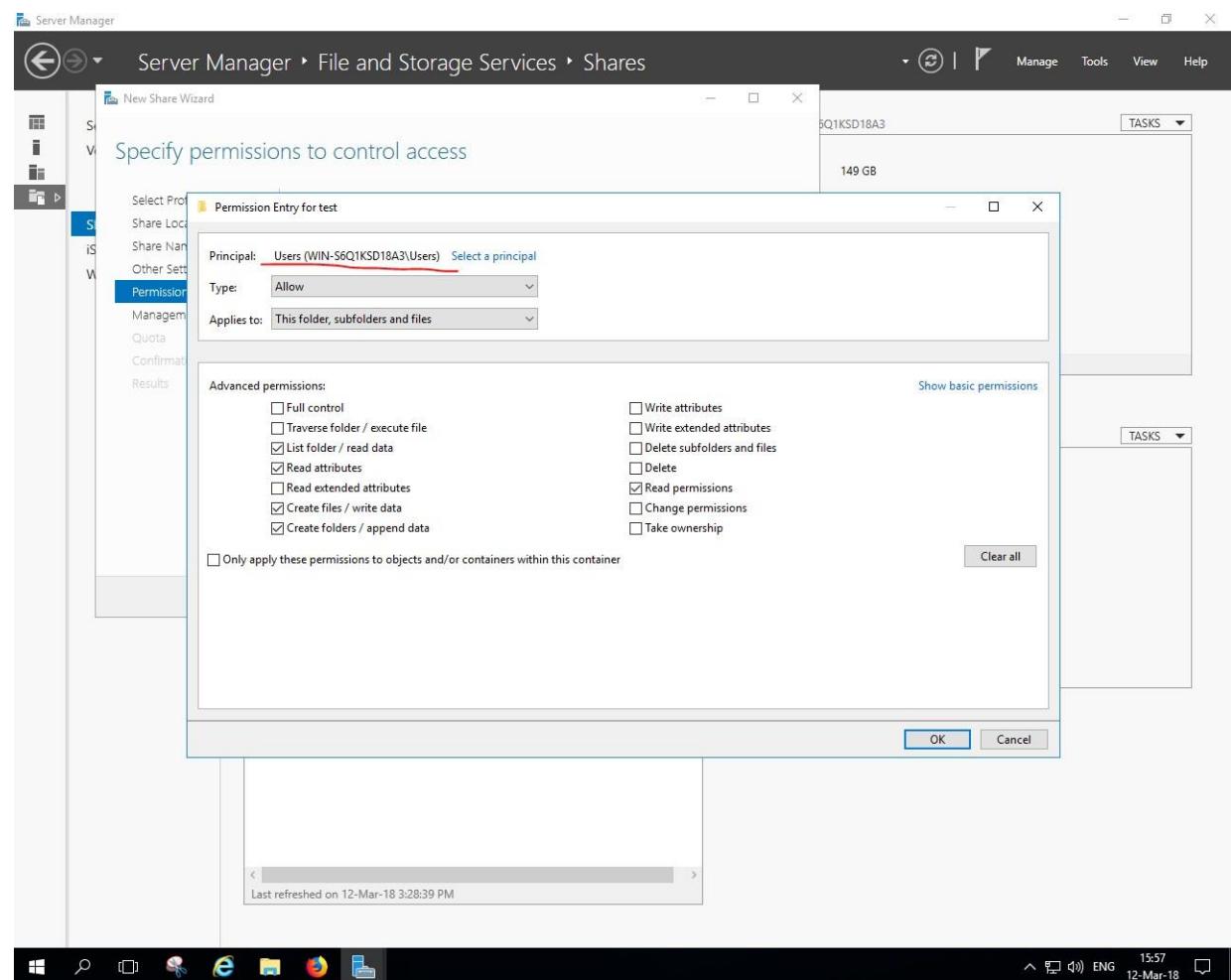




- Τα δικαιώματα που πρέπει να έχει ένας φάκελος έτσι ώστε να μην μπορεί κάποιος να δημιουργήσει νέους υποφακέλους αλλά μόνο αρχεία είναι τα εξής :



Τα δικαιώματα που πρέπει να έχει ένας φάκελος για να μην είναι ικανός κάποιος να σβήσει αρχεία ή υποφακέλους, αλλά μόνο να προσθέσει η να δημιουργεί νέα αρχεία και νέους υποφακέλους είναι τα εξής :



4. Καταγραφή και παρακολούθηση ενεργειών χρήστη

4.1 Βασικά αρχεία καταγραφής στα windows

The screenshot shows the Windows Server Manager dashboard. The left sidebar has 'Dashboard' selected. The main area displays 'WELCOME TO SERVER MANAGER' with a 'QUICK START' section containing five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a 'ROLES AND SERVER GROUPS' section showing 'File and Storage Services' (1 role), 'Local Server' (1 role), and 'All Servers' (1 role). The 'Local Server' group is highlighted with a red border. The bottom status bar shows system icons and the date/time: 12-Mar-18 19:25.

Server Manager

Server Manager • Dashboard

Dashboard

Local Server

All Servers

File and Storage Services

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services	1
Manageability	1
Events	
Services	
Performance	
BPA results	

Local Server	1
Manageability	1
Events	
Services	2
Performance	
BPA results	

All Servers	1
Manageability	1
Events	
Services	2
Performance	
BPA results	

12-Mar-18 19:25

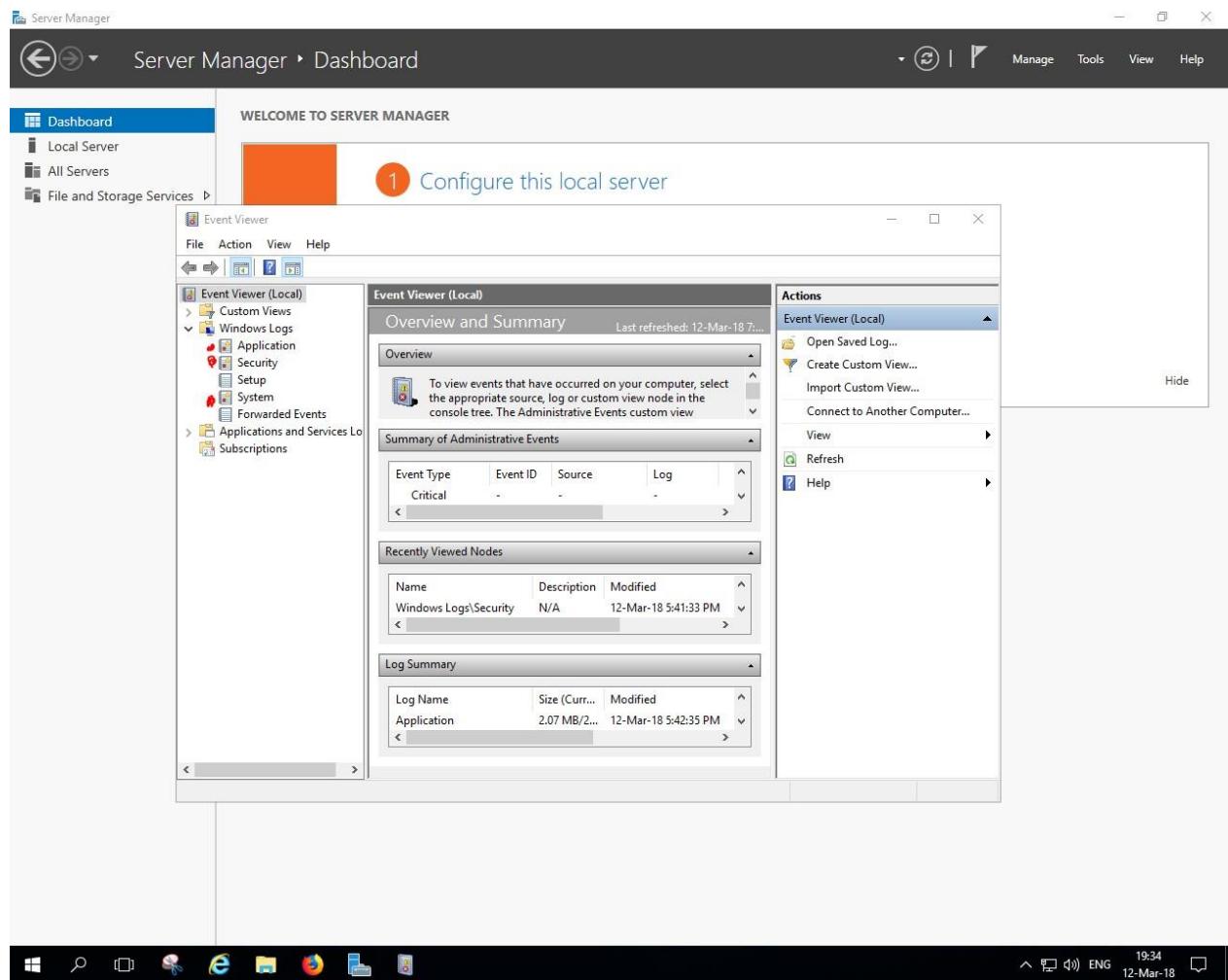
12-Mar-18 19:25

Manage Tools View Help

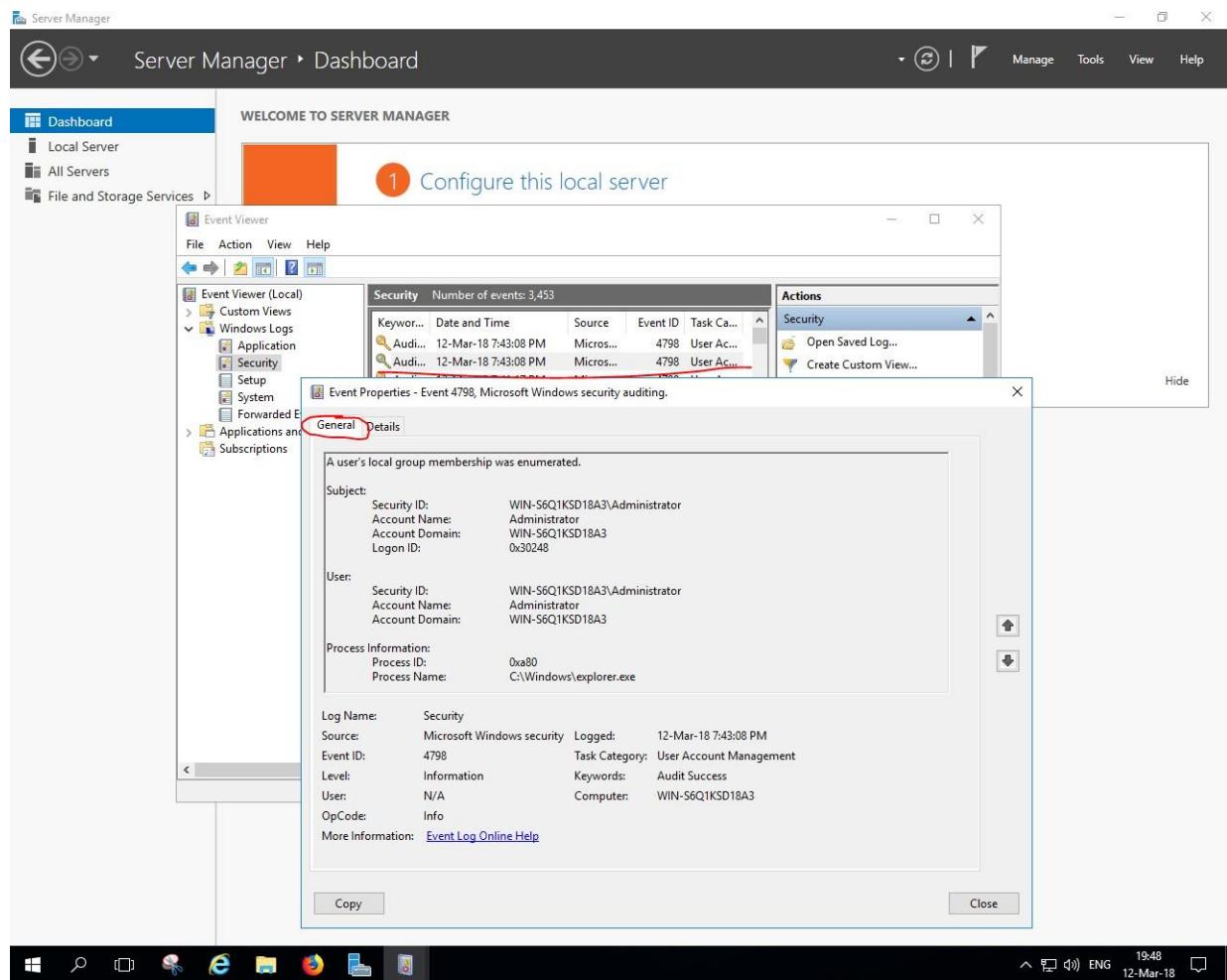
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
Event Viewer
File Server Resource Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

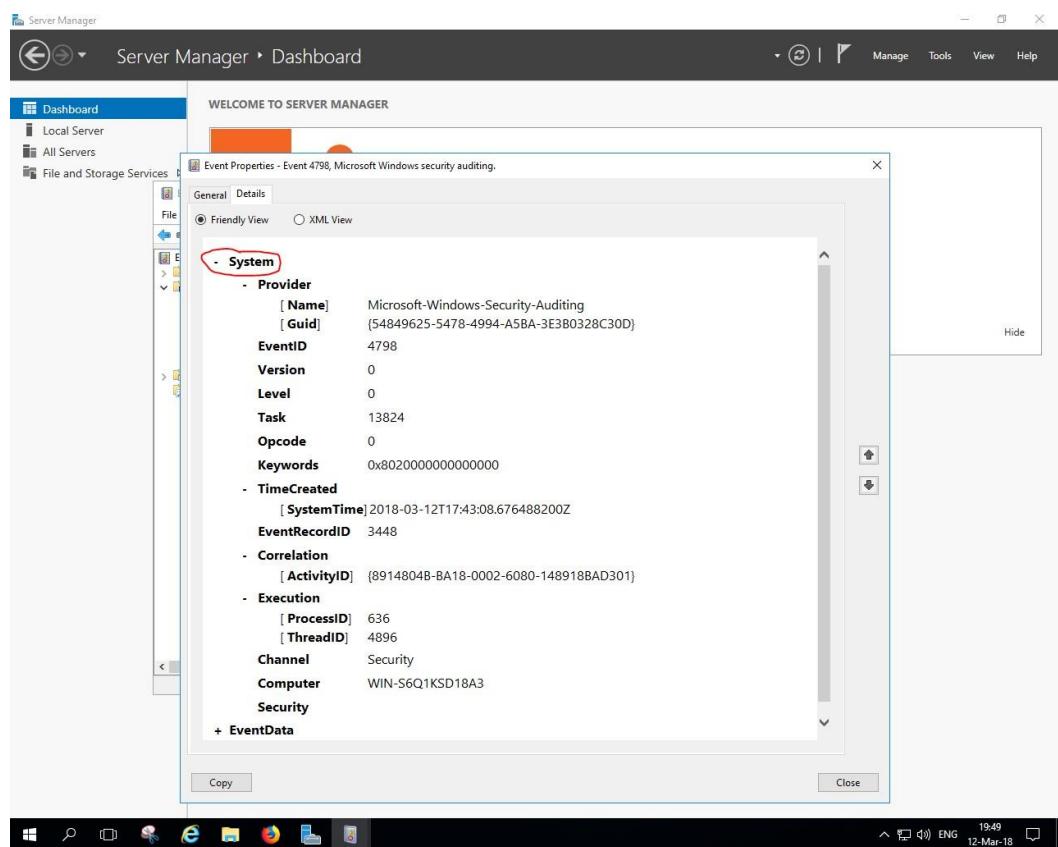
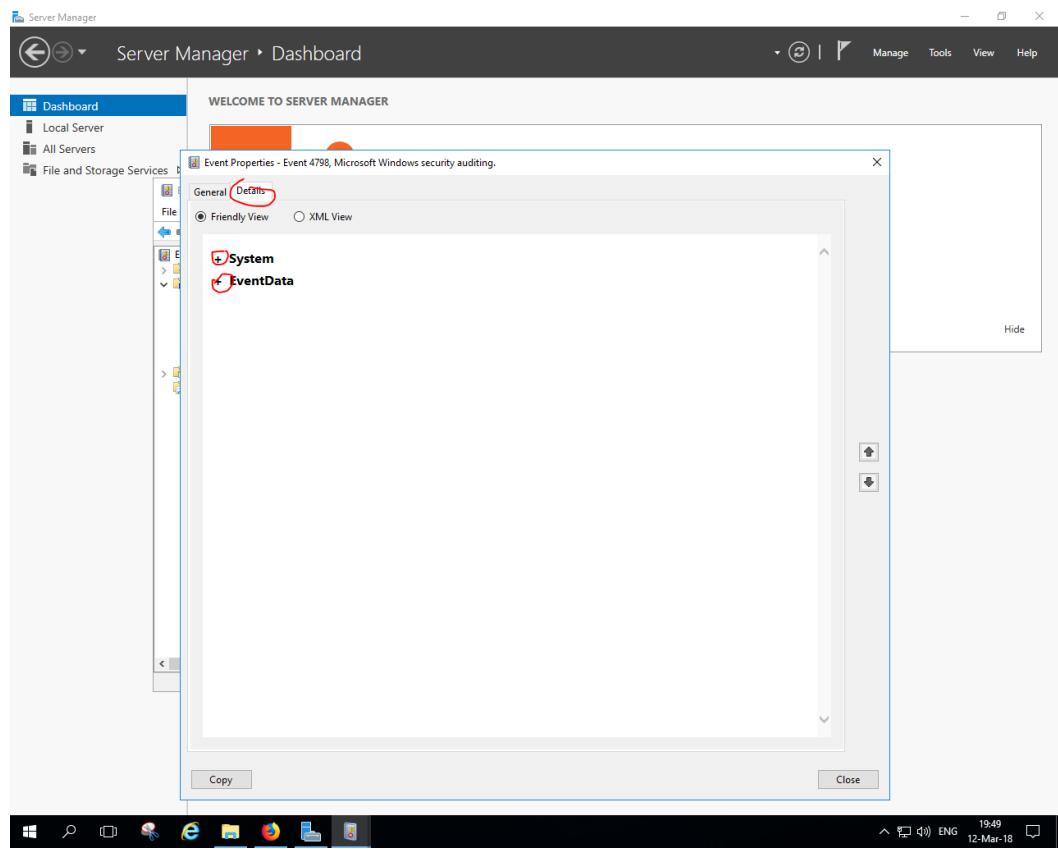
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

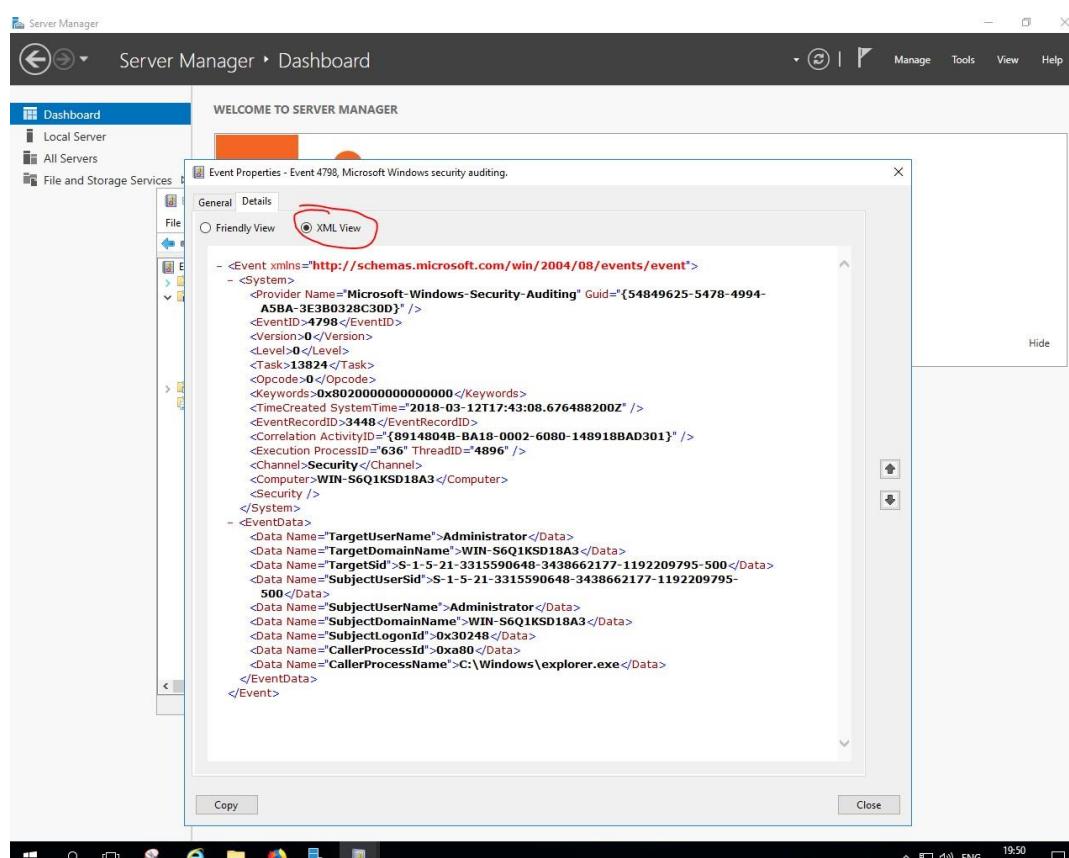
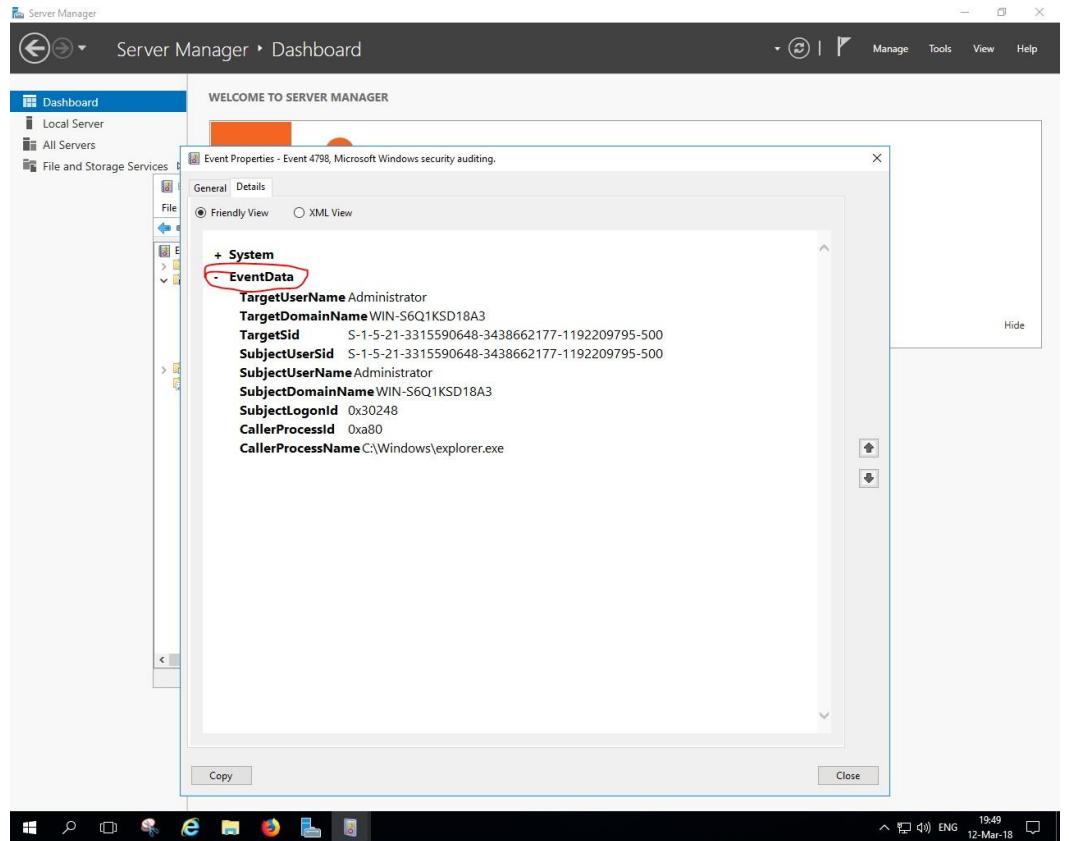
19:33 ENG 12-Mar-18



Σε ένα τυχαίο γεγονός στο Security log καταγράφονται τα παρακάτω στοιχεία :

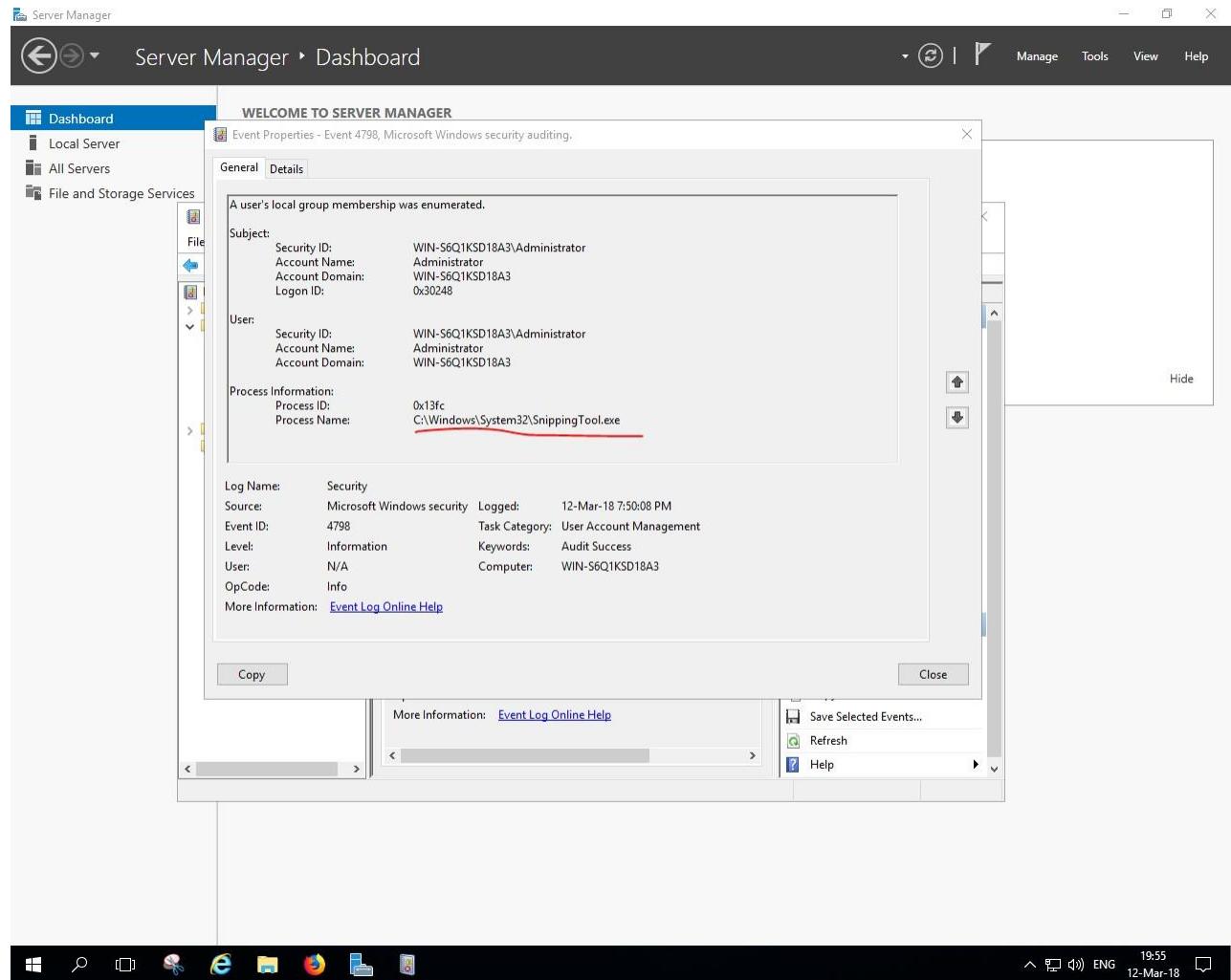




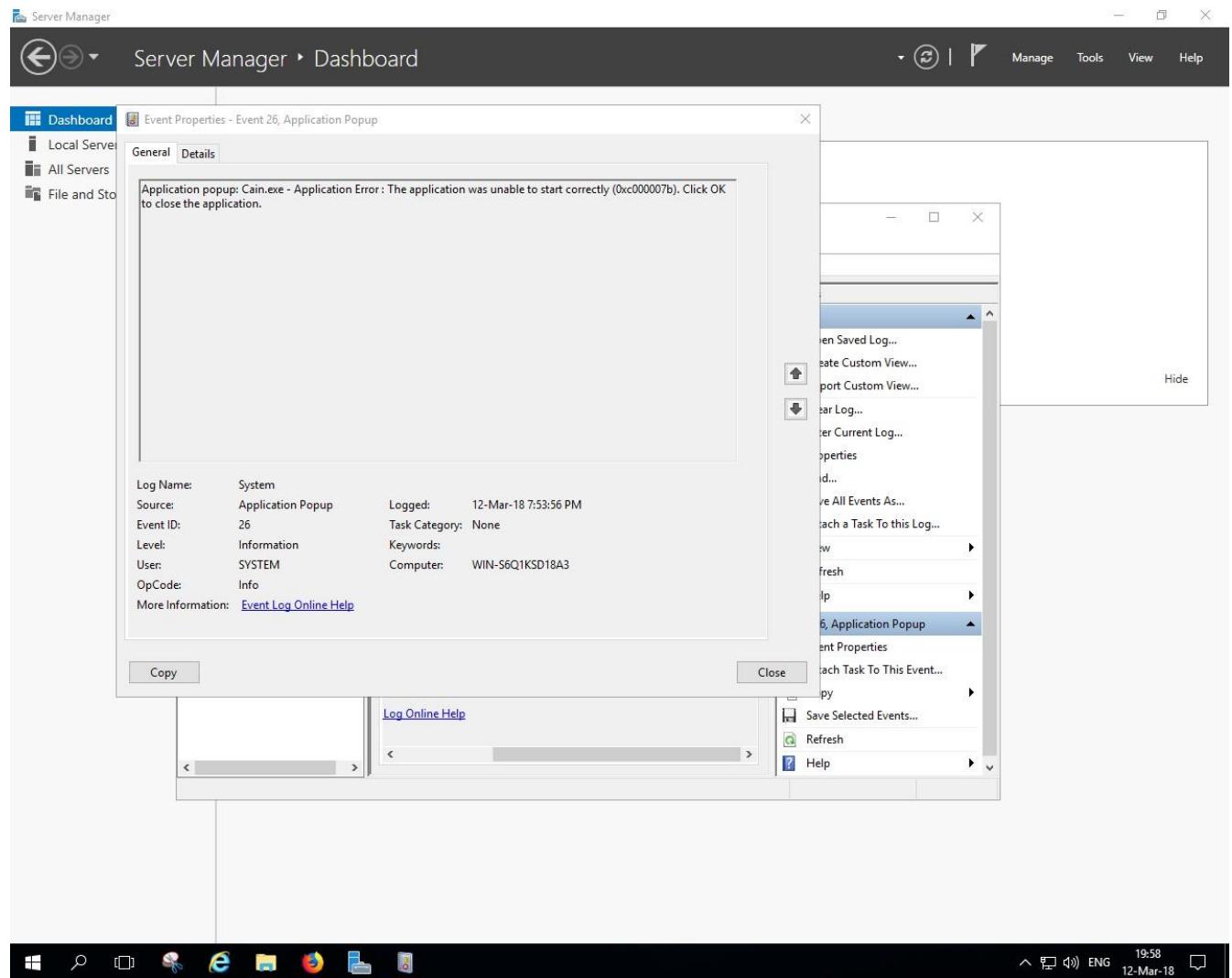


Γενικά παρατηρούμε ότι αυτά τα τρία βασικά αρχεία καταγραφής, μας δίνουν αρκετά σημαντικές πληροφορίες. Όπως το πότε έγινε το οτιδήποτε στο σύστημα και από ποιόν χρήστη. Επίσης, σε περίπτωση που υπάρξει κάποιο crush στον υπολογιστή, μπορούμε μέσα από τα logs να δούμε από που προήλθε το πρόβλημα. Η χρήση των log είναι μείζονος σημασίας για την καλή και αποδοτική λειτουργία του λειτουργικού συστήματος. Στα χέρια των διαχειριστών είναι ένα αρκετά σημαντικό εργαλείο το οποίο τους προσφέρει πλήρη έλεγχο και εικόνα του λειτουργικού.

Στην συνέχεια ανοίγω το “Snipping Tool” και πηγαίνω στα log για να δω την καταγραφή αυτού του γεγονότος :



Επίσης, ανοίγω το πρόγραμμα Cain & Abel, το οποίο όμως δεν λειτουργεί στον λειτουργικό μου σύστημα και καταγράφεται και αυτό από το σύστημα :



4.2 Δαίμονας Syslog

Syslog σημαίνει System Logging Protocol, και χρησιμοποιείτε σε ηλεκτρονικές συσκευές όπως routers, σε firewalls, σε Unix/Linux servers (στα windows server υπάρχουν τα Event Logs, τα οποία όμως μπορούν να χρησιμοποιηθούν σε σύνδεση με έναν Syslog server) και σε άλλες συσκευές που συνδέονται σε κάποιο δίκτυο. Στην πράξη, μια ηλεκτρονική συσκευή συνδεδεμένη στον server μας για παράδειγμα, μπορεί να δημιουργεί syslog/event μηνύματα και να τα στέλνει στον Syslog Server (ή στον Daemon), τα οποία βοηθάνε τους διαχειριστές να παρακολουθούν τις συσκευές που είναι συνδεδεμένες και να αντιμετωπίσουν οποιοδήποτε πρόβλημα προκύπτει από αυτές τις συσκευές.

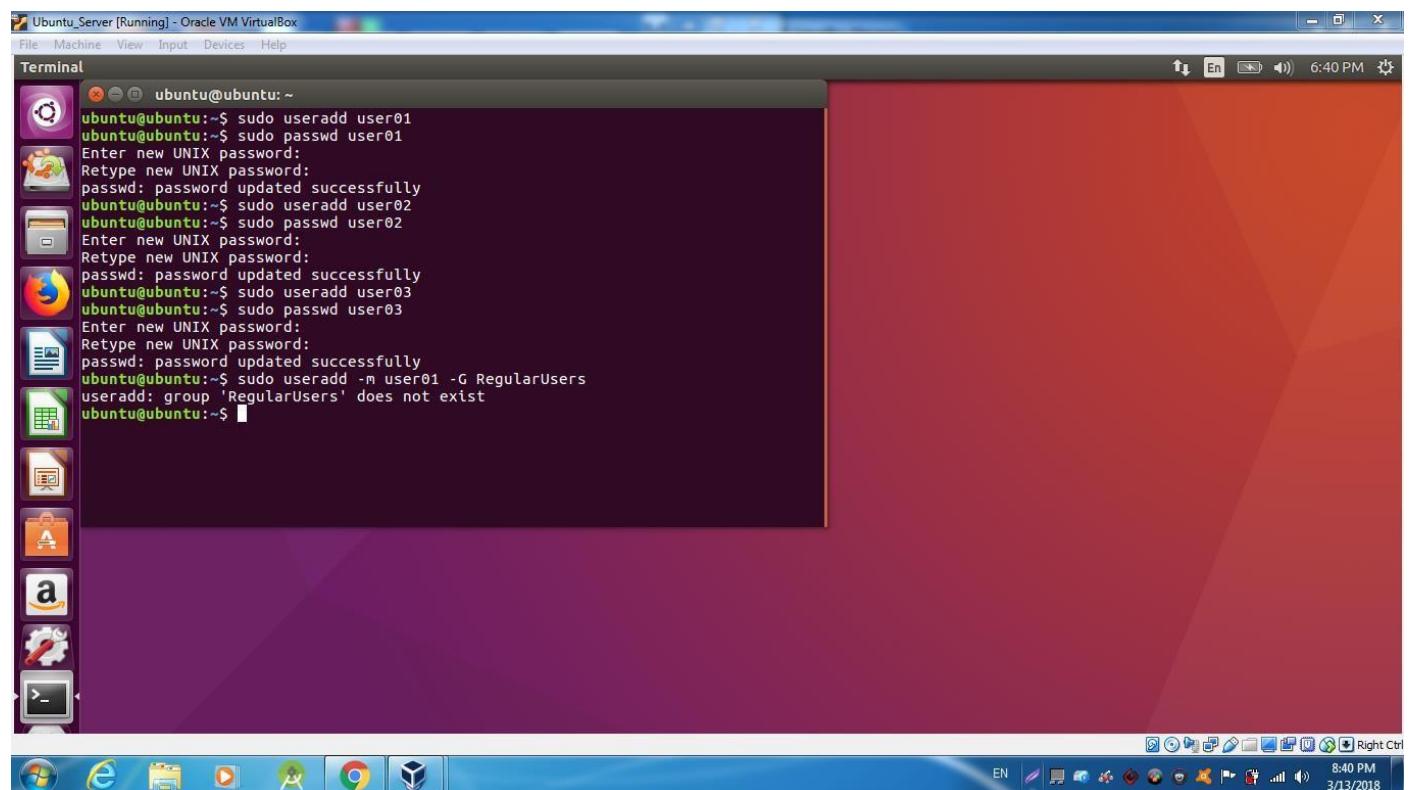
Linux Server (Περιβάλλον Εργασίας)

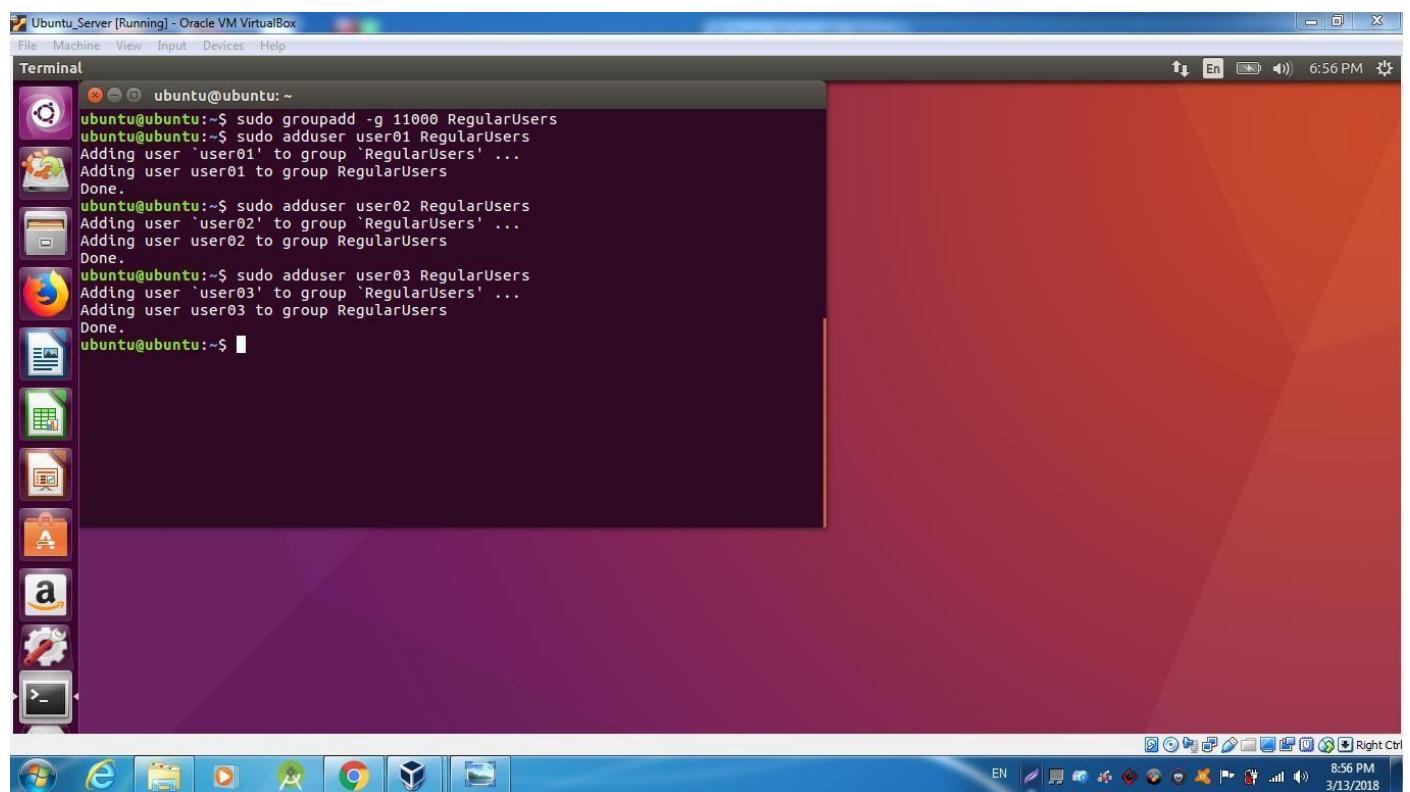
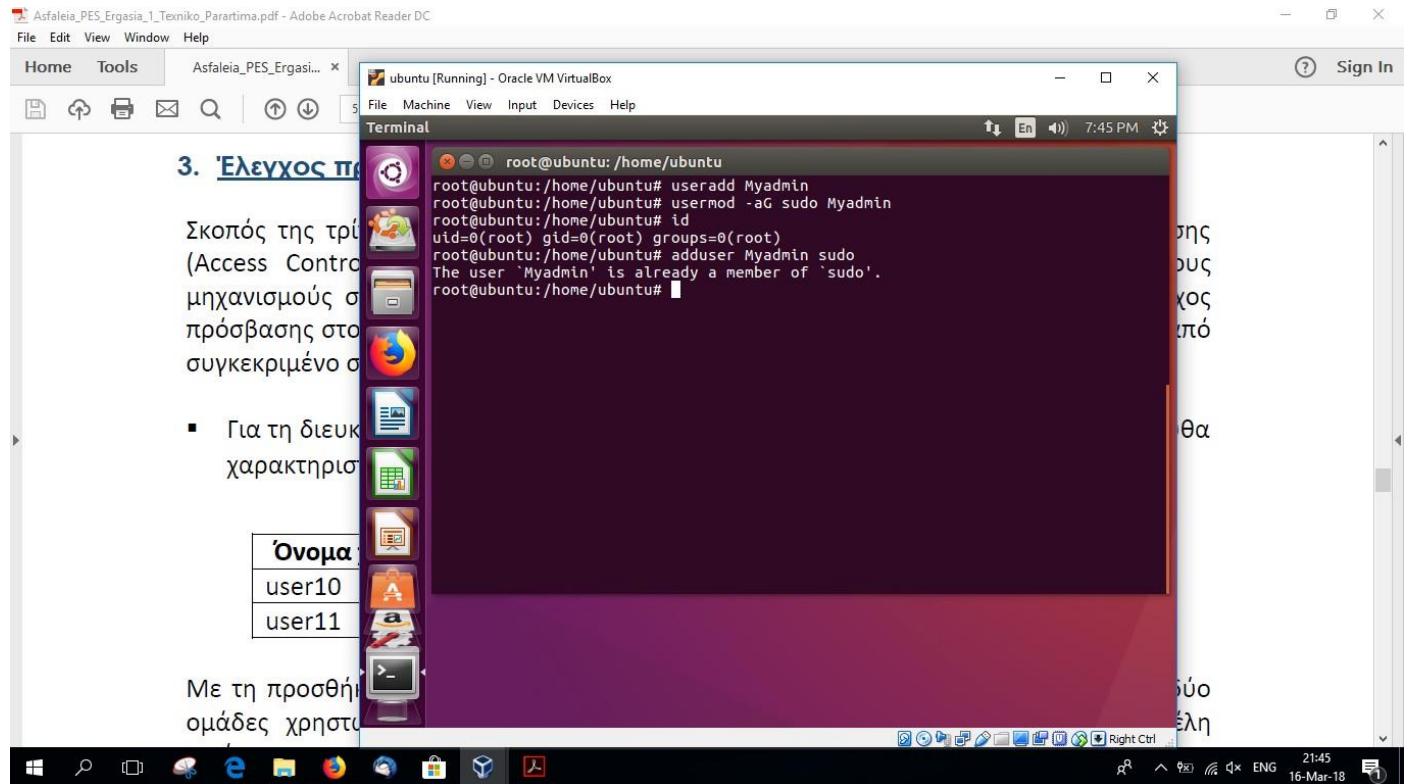
Υλοποίησα τον linux server σε ubuntu 16.04. Η εγκατάσταση έγινε μέσω του Oracle VM VirtualBox. Όσον αφορά τα θεωρητικά ερωτήματα, όλα όσα ήταν κοινά για τα δύο Λειτουργικά Συστήματα, έχουν ήδη απαντηθεί παραπάνω. Παρακάτω θα αναλυθούν μόνο αυτά που είναι αποκλειστικά για τα linux.

1. Διαχείριση Χρηστών και Αυθεντικοποίηση

1.1 Δημιουργία Χρηστών και Ομάδων

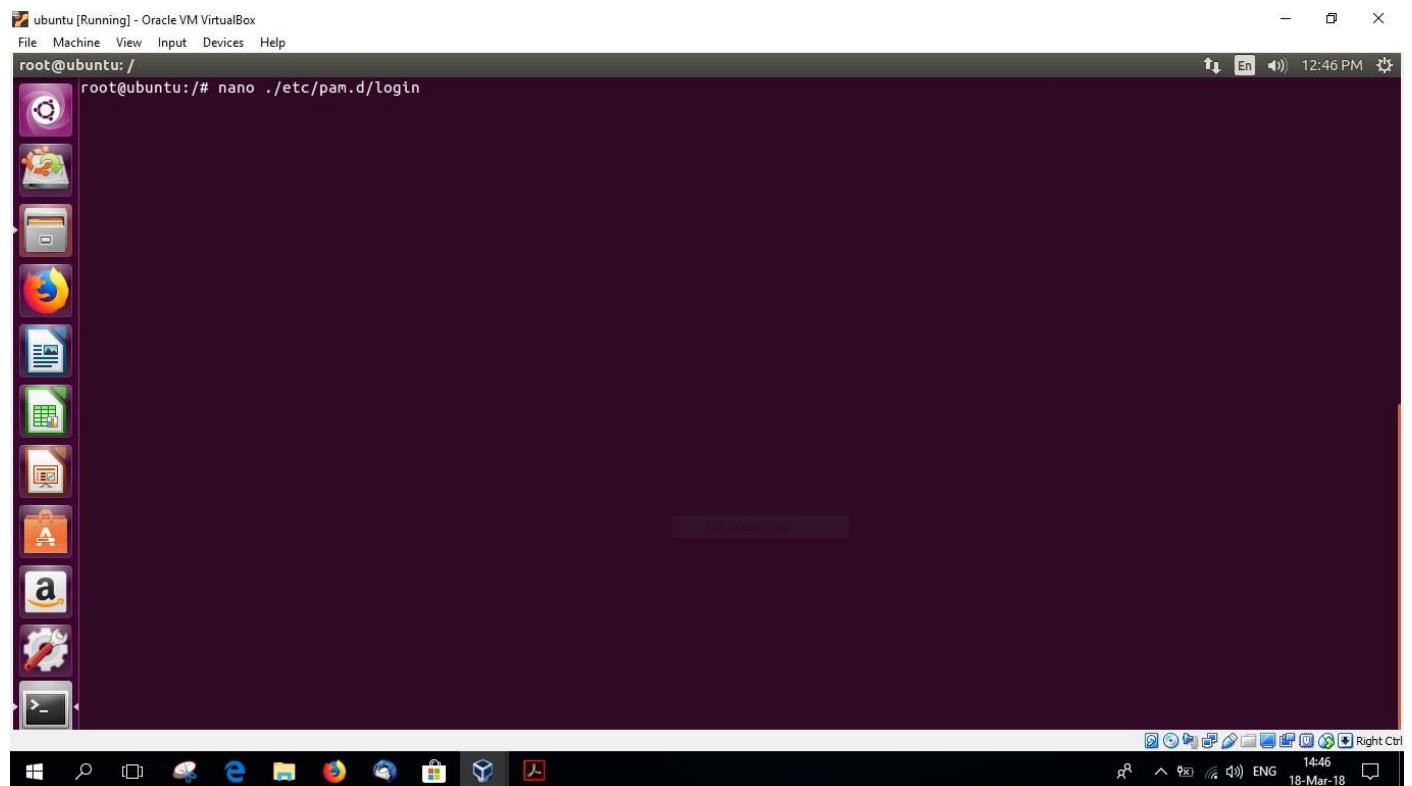
Παρακάτω φαίνονται οι εντολές που έτρεξα στο terminal για να δημιουργηθούν οι χρήστες και οι κωδικοί τους και η ομάδα που θα βάλω αυτούς τους χρήστες





1.2 Πολιτικές Ασφάλειας Λογαριασμών Χρηστών

Παρακάτω φαίνονται οι εντολές που έτρεξα για να παραμετροποιήσουμε τις πολιτικές ασφάλειας των λογαριασμών των χρηστών.



```

root@ubuntu:/etc/pam.d
GNU nano 2.5.3          File: ./etc/pam.d/login
Modified

#
# The PAM configuration file for the Shadow `login' service
#
# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth optional pam_faildelay.so delay=3000000

auth required pam_tally2.so deny=3
# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth required pam_issue.so issue=/etc/issue

# Disallows root logins except on tty's listed in /etc/securetty
# (Replaces the `CONSOLE' setting from login.defs)
#
# With the default control of this module:
# [success=ok new_authtok_reqd=ok ignore=ignore user_unknown=bad default=die]
# root will not be prompted for a password on insecure lines.
# if an invalid username is entered, a password is prompted (but login
# will eventually be rejected)
#
# You can change it to a "requisite" module if you think root may mis-type
# her login and should not be prompted for a password in that case. But
# this will leave the system as vulnerable to user enumeration attacks.
#
# You can change it to a "required" module if you think it permits to
# guess valid user names of your system (invalid user names are considered
# as possibly being root on insecure lines), but root passwords may be
# communicated over insecure lines.

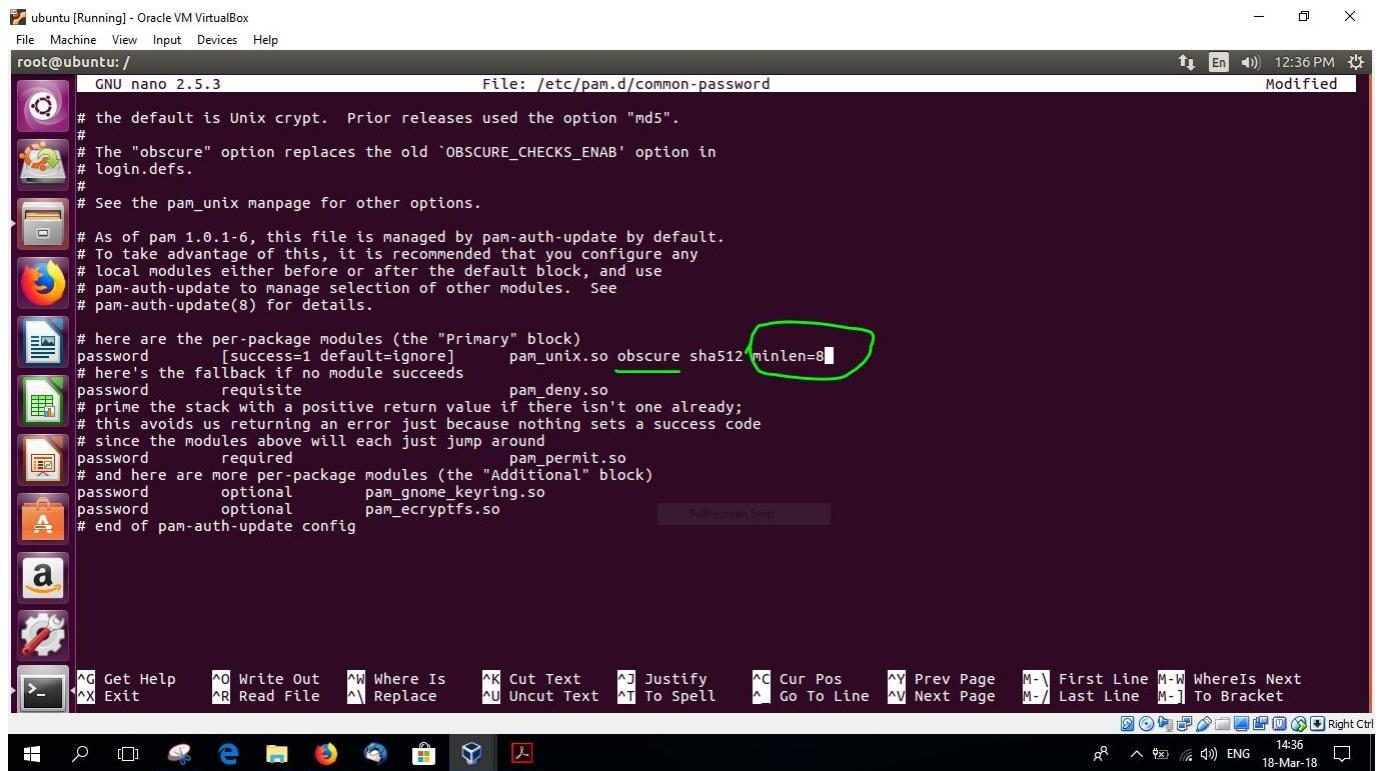
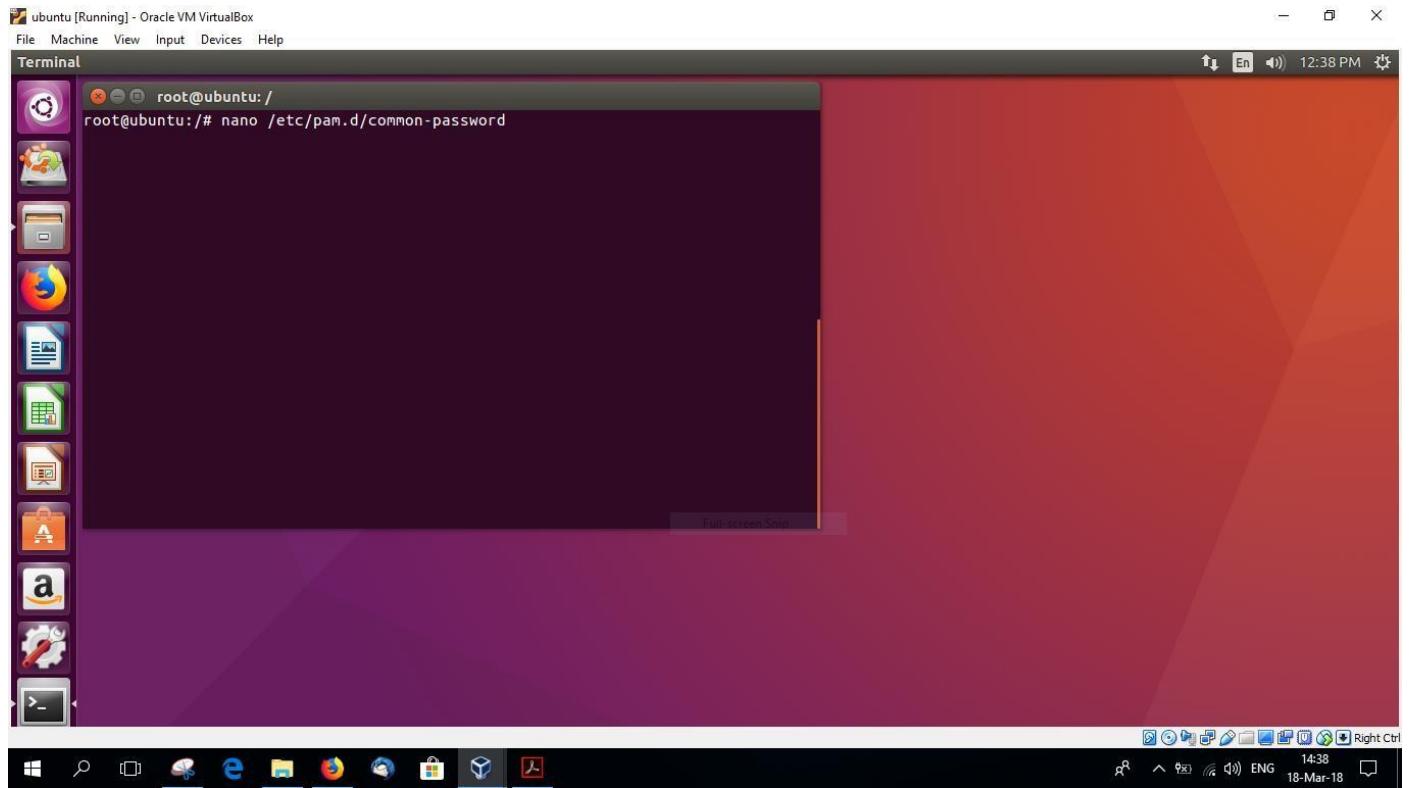
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   ^Y Prev Page   M-\ First Line M-W WhereIs Next
^X Exit       ^R Read File   ^A Replace    ^U Uncut Text  ^I To Spell   ^B Go To Line  ^V Next Page   M-/ Last Line M-] To Bracket

```

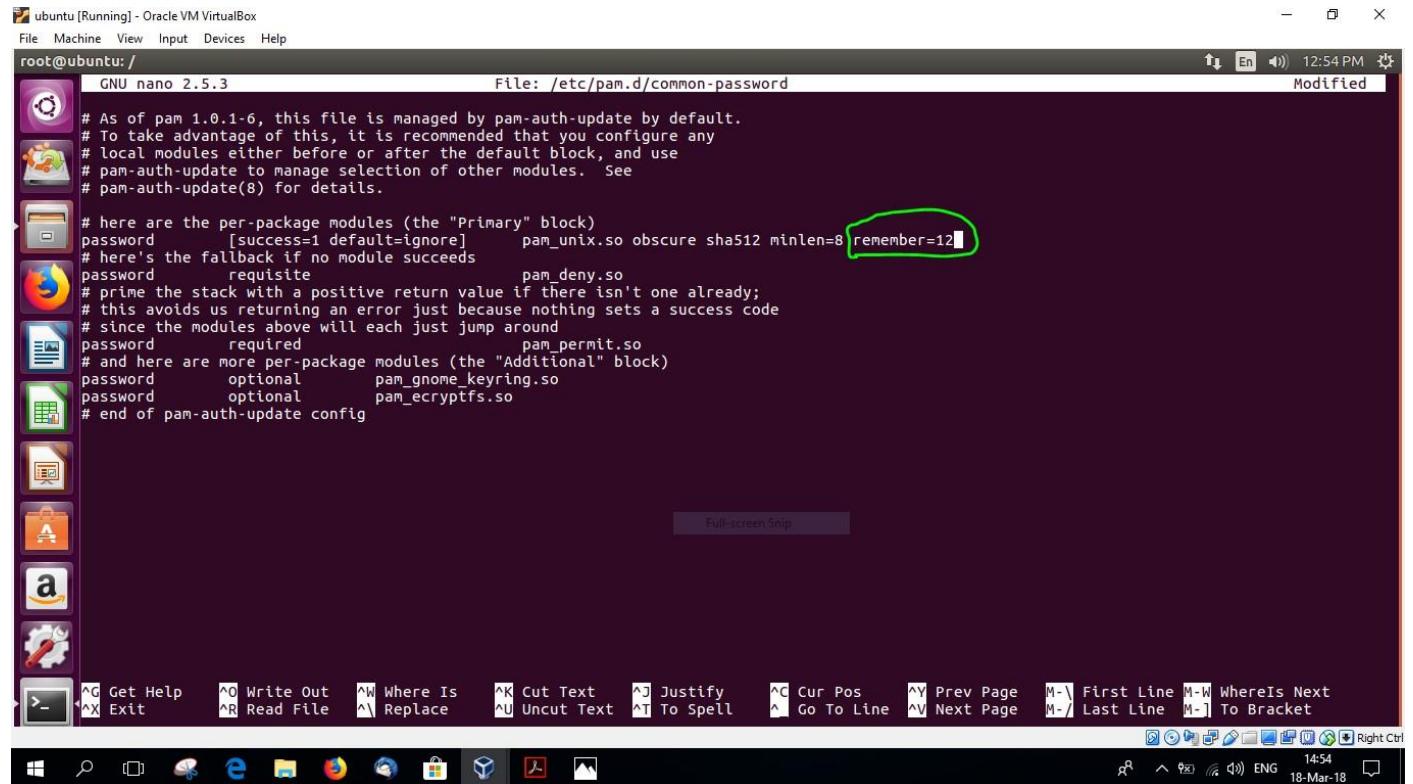
Όπως φαίνεται, μπήκα στο αρχείο `login` και πρόσθεσα την γραμμή που είναι υπογραμμισμένη με πράσινο. Το `deny=3` σημαίνει ότι ο χρήστης έχει 3 προσπάθειες για να βάλει σωστά το συνθηματικό του, αλλιώς κλειδώνει ο λογαριασμός του. Επίσης θα μπορούσα να προσθέσω στην συνέχεια του `deny=3`, το `unlock_time` όπου θα έβαζα το πόσο χρόνο μετά από το κλείδωμα του λογαριασμού θα ξεκλείδωνε ο λογαριασμός. Δεν το πρόσθεσα όμως, επειδή έθεσα σαν πολιτική ασφάλειας, το ξεκλείδωμα του λογαριασμού να γίνεται μόνο από έναν administrator.

1.3 Πολιτικές Ασφάλειας Συνθηματικών

Όπως φαίνεται και παρακάνω, επεξεργάστηκα το αρχείο `common-password`. Όταν το άνοιξα, άψαξα την γραμμή που φαίνεται και στο print screen, και πρόσθεσα αυτό που είναι κυκλωμένο με πράσινο. Αρχικά το «`obscure`» ενεργοποιεί την πολυπλοκότητα των συνθηματικών. Κανείς χρήστης δηλαδή δεν μπορεί να χρησιμοποιήσει απλά συνθηματικά (πχ 123456,password,pass123 κ.α.). Στην συνέχεια, πρόσθεσα το «`minlen=8`» όπου κάθε συνθηματικό θα πρέπει να έχει τουλάχιστον 8 χαρακτήρες.



Στην συνέχεια προσθέσαμε στην ίδια γραμμή το «remember=12» ώστε να θυμάται τα τελευταία 12 συνθηματικά για κάθε χρήστη, και σε αυτό το διάστημα να μην μπορεί να χρησιμοποιήσει ένα ίδιο συνθηματικό. Επίσης, μπορούμε να προσθέσουμε, μετά το remember=12, το enforce_for_root για να ισχύει η παρακάτω πολιτική ασφάλειας και για τον root.



```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@ubuntu: /GNU nano 2.5.3 File: /etc/pam.d/common-password Modified
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]  pam_unix.so obscure sha512 minlen=8 remember=12
# here's the fallback if no module succeeds
password      requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required           pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional           pam_gnome_keyring.so
password      optional           pam_encryptfs.so
# end of pam-auth-update config

Full-screen Snip
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page M-\ First Line M-W WhereIs Next
^X Exit      ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^A Go To Line ^V Next Page M-/ Last Line M-] To Bracket
Windows Start button, taskbar icons, system tray, and status bar showing date/time.
```

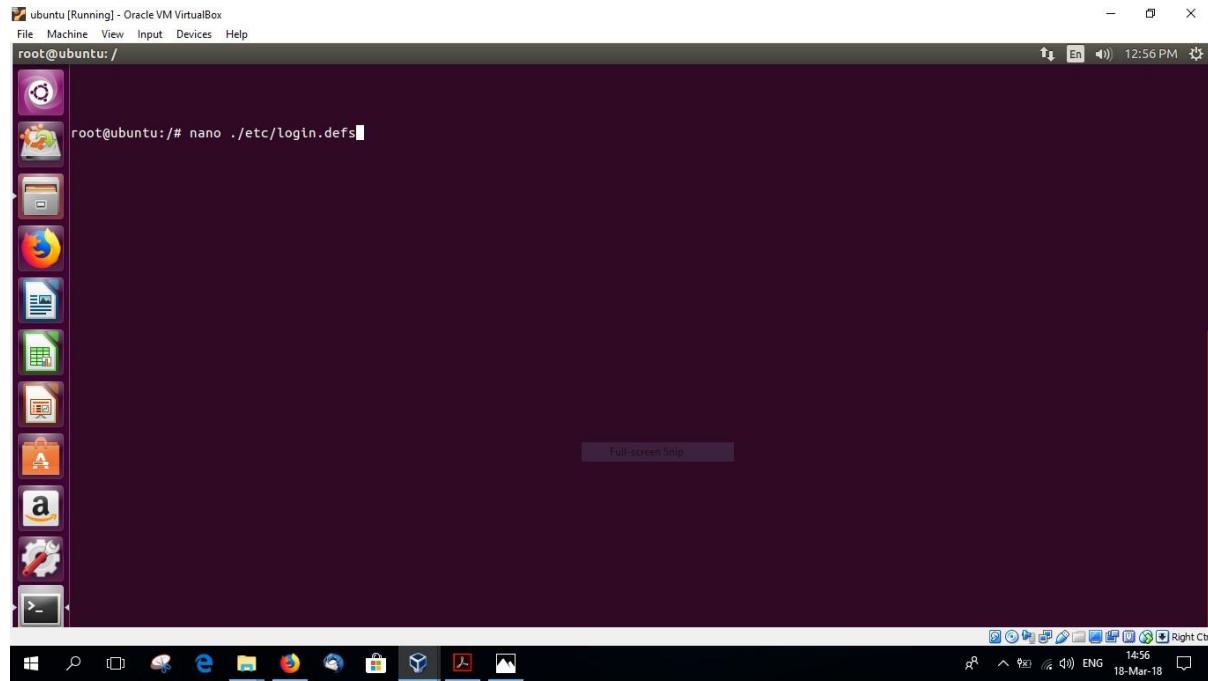
```

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@ubuntu: / File: /etc/pam.d/common-password Modified
GNU nano 2.5.3
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]    pam_unix.so obscure sha512 minlen=8 remember=12 enforce_for_root
# here's the fallback if no module succeeds
password      requisite                pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
password      required                 pam_permit.so
# and here are more per-package modules (the "Additional" block)

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   ^Y Prev Page   M-[ First Line M-W WhereIs Next
^X Exit       ^R Read File    ^A Replace    ^U Uncut Text  ^I To Spell   ^G Go To Line  ^V Next Page   M-] Last Line M-] To Bracket

```

Στην συνέχεια επεξεργάστηκα το αρχείο login.defs και έθεσα τον μέγιστο χρόνο που κάποιος χρήστης μπορεί να χρησιμοποιήσει το ίδιο συνθηματικό χωρίς να το αλλάξει. Έβαλα PASS_MAX_DAYS = 30, έτσι ώστε κάθε χρήστης να υποχρεώνεται κάθε 30 μέρες να αλλάζει συνθηματικό. Το PASS_MIN_DAYS το αφήνω 0, διότι αν κάποιος χρήστης θέλει να αλλάξει κωδικό την ίδια μέρα που το άλλαξε ήδη, να μπορεί να το κάνει. Να μην είναι υποχρεωμένος δηλαδή να κρατήσει έναν κωδικό πρόσβασης για τουλάχιστον μία μέρα. Το PASS_WARN_AGE το θέσαμε με 2. Δηλαδή 2 μέρες πριν λήξει η διορία της αλλαγής του συνθηματικού, να έρχεται ειδοποίηση στον χρήστη, με το που συνδέεται στο σύστημα, ότι σε 2 μέρες θα πρέπει να αλλάξει το συνθηματικό του. Παρακάτω φαίνεται η υλοποίηση αυτών των πολιτικών ασφάλειας.



```
root@ubuntu:/# nano ./etc/login.defs
GNU nano 2.5.3                               File: ./etc/login.defs
Modified

# 022 is the "historical" value in Debian for UMASK
# 027, or even 077, could be considered better for privacy
# There is no One True Answer here : each sysadmin must make up his/her
# mind.
#
# If USERGROUPS_ENAB is set to "yes", that will modify this UMASK default value
# for private user groups, i. e. the uid is the same as gid, and username is
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
ERASECHAR      0177
KILLCHAR       025
UMASK          022

#
# Password aging controls:
#
# PASS_MAX_DAYS   Maximum number of days a password may be used.
# PASS_MIN_DAYS   Minimum number of days allowed between password changes.
# PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS  99999
PASS_MIN_DAYS  0
PASS_WARN_AGE  7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
UID_MAX         60000

^G Get Help     ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos    ^Y Prev Page   M-\ First Line M-W WhereIs Next
^X Exit        ^R Read File   ^L Replace    ^U Uncut Text  ^T To Spell   ^V Go To Line  ^V Next Page   M-/ Last Line M-B To Bracket
^A Get Help     ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos    ^Y Prev Page   M-\ First Line M-W WhereIs Next
^X Exit        ^R Read File   ^L Replace    ^U Uncut Text  ^T To Spell   ^V Go To Line  ^V Next Page   M-/ Last Line M-B To Bracket
```

ubuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@ubuntu:/

GNU nano 2.5.3 File: ./etc/login.defs Modified

```
# 022 is the "historical" value in Debian for UMASK
# 027, or even 077, could be considered better for privacy
# There is no One true Answer here : each sysadmin must make up his/her
# mind.
#
# If USERGROUPS_ENAB is set to "yes", that will modify this UMASK default value
# for private user groups, i. e. the uid is the same as gid, and username is
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
ERASECHAR      0177
KILLCHAR        025
UMASK           022

#
# Password aging controls:
#
#          PASS_MAX_DAYS   Maximum number of days a password may be used.
#          PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#          PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS  30
PASS_MIN_DAYS  0
PASS_WARN_AGE  2

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
UID_MAX         60000

^G Get Help    ^O Write Out   ^W Where Is    ^X Cut Text     ^J Justify     ^C Cur Pos      ^Y Prev Page   M-\ First Line M-W WhereIs Next
^X Exit        ^R Read File   ^A Replace     ^U Uncut Text   ^I To Spell    ^L Go To Line   ^V Next Page   M-/ Last Line M-] To Bracket
^Q Quit        ^P Print File  ^F Find        ^B Copy         ^K Kill        ^H Home        ^N Next Line   M-` Last Line M-[ To Bracket
```

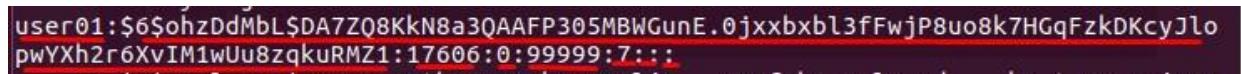
2. Διαχείριση των συνθηματικών – Μελέτη επιθέσεων

2.2 Φύλαξη λογαριασμών χρηστών στα Linux

Η φύλαξη των πληροφοριών για τα προφίλ των χρηστών γίνεται στο αρχείο /etc/passwd, στα μοντέρνα όμως συστήματα Linux στη θέση των κωδικών υπάρχει ένα και οι πραγματικοί κωδικοί βρίσκονται σε ένα γειτονικό αρχείο που το διαχειρίζεται και έχει πρόσβαση μόνο ο super user και λέγεται /etc/shadow (ή /etc/master.passwd σε συστήματα BSD).

Στη περύττωση αυτή το σύστημα δημιουργεί μία κρυπτογραφημένη δομή που ακολουθεί τοπρότυπο :

Τα διαφορετικά πεδία χωρίζονται με semicolon (:).



```
user01:$6$ohzDdMbL$DA7ZQ8KkN8a3QAAFP305MBWGunE.0jxxbxbl3fFwjP8uo8k7HGqFzkDKcyJlo
pwYXh2r6XvIM1wUu8zqkuRMZ1:17606:0:99999:7:::
```

- Username
- Password*
- Τελευταία αλλαγή κωδικού (μετρίεται σε μέρες που περάσαν από Jan 1,1970)
- Minimum , μέρες που μπορεί ο χρήστης να αλλάξει τον κωδικό απτην τελευταία φορά που ολλάχθηκε.
- Maximum , μέρες που ο κωδικός θα είναι δεκτός(θα αναγκασθεί να τον αλλάξει μετά).
- Warn , πόσες μέρες πριν θα ειδοποιηθεί ο χρήστης ότι πρέπει να αλλαχτεί ο κωδικός.
- Inactive , σε πόσες μέρες μετά την λήξη του κωδικού θα γίνει inactive το account.
- Expire , (μετρίεται σε μέρες που περάσαν από Jan 1,1970) πότε θα γίνει disabled το account.

Ο κωδικός έχει την μορφή : \$id\$salt\$hashed

Id : είναι ο αλγόριθμος που χρησιμοποιείται

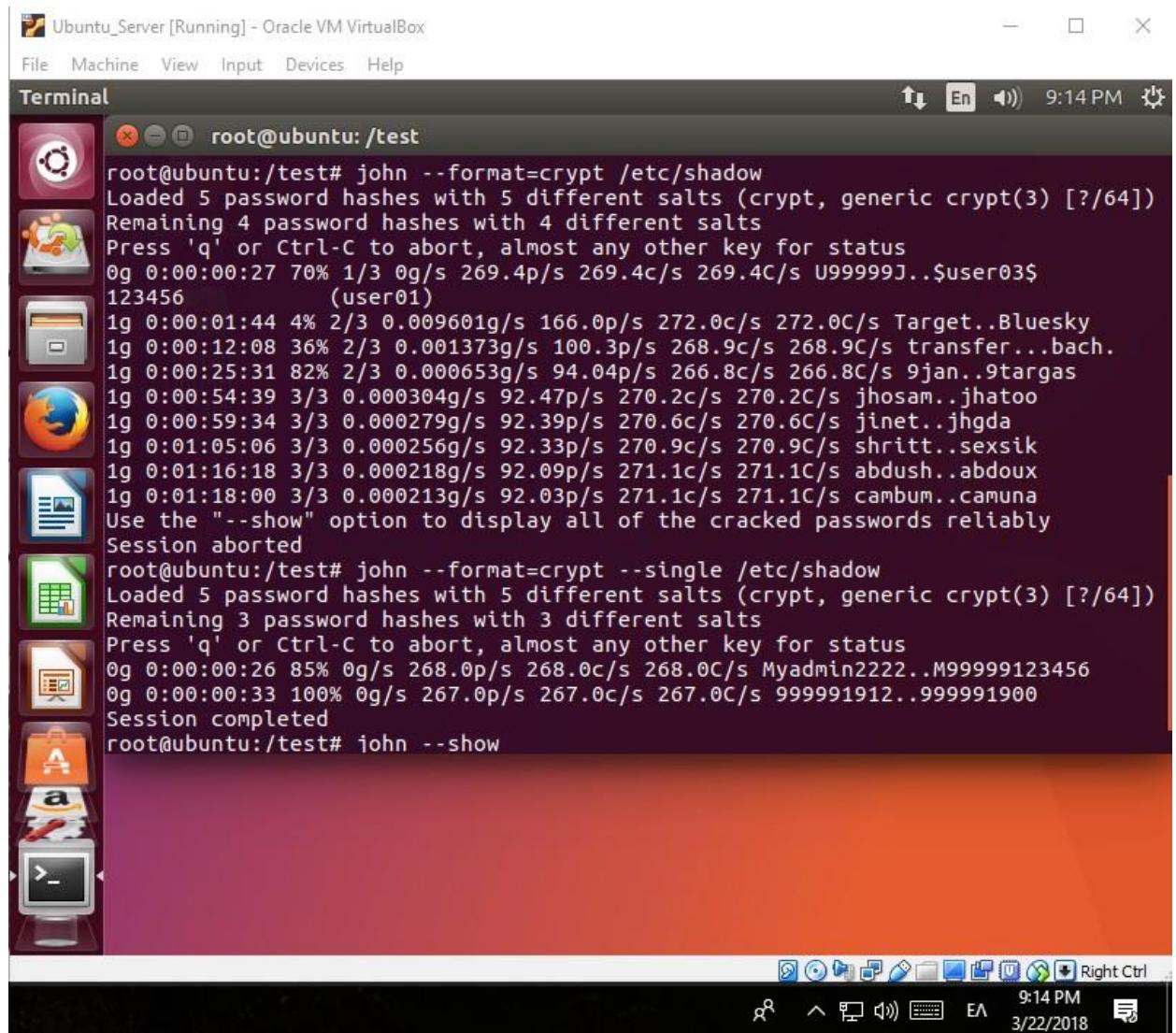
- \$1\$ για MD5
- \$2a\$ για Blowfish
- \$2y\$ για Blowfish
- \$5\$ για SHA-256
- \$6\$ για SHA-512

Salt : είναι ένα τυχαίο string το οποίο θα ανακατευτεί με το hash του κωδικού κάνοντας ακόμα πιο δύσκολη το σπάσιμο του κωδικού και αχρηστεύοντας τελείως την τεχνική αποκρυπτογράφησης με Rainbow tables.

Hashed : είναι το hash του κωδικού ανακατεμένο με το salt.

2.3 Αναλυτής Συνθηματικών (Password Cracker)

Με την βοήθεια του προγράμματος John the Ripper δοκιμάζω να κρακάρω τους κωδικούς που βρίσκονται στο /etc/shadow με τις τεχνικές dictionary και brute force attack. Τα rainbow tables δεν δουλεύουν στην προκειμένη περίπτωση λόγο του salt.



The screenshot shows a terminal window titled "root@ubuntu:/test" running on an Ubuntu Server. The user is executing the command "john --format=crypt /etc/shadow". The output indicates that 5 password hashes were loaded with 5 different salts (crypt, generic crypt(3)). The cracking process has completed, displaying several cracked passwords:

```
root@ubuntu:/test# john --format=crypt /etc/shadow
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Remaining 4 password hashes with 4 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:27 70% 1/3 0g/s 269.4p/s 269.4c/s 269.4C/s U99999J..$user03$
123456          (user01)
1g 0:00:01:44  4% 2/3 0.009601g/s 166.0p/s 272.0c/s 272.0C/s Target..Bluesky
1g 0:00:12:08  36% 2/3 0.001373g/s 100.3p/s 268.9c/s 268.9C/s transfer...bach.
1g 0:00:25:31  82% 2/3 0.000653g/s 94.04p/s 266.8c/s 266.8C/s 9jan..9targas
1g 0:00:54:39  3/3 0.000304g/s 92.47p/s 270.2c/s 270.2C/s jhosam..jhatoor
1g 0:00:59:34  3/3 0.000279g/s 92.39p/s 270.6c/s 270.6C/s jinet..jhgda
1g 0:01:05:06  3/3 0.000256g/s 92.33p/s 270.9c/s 270.9C/s shritt..sexsik
1g 0:01:16:18  3/3 0.000218g/s 92.09p/s 271.1c/s 271.1C/s abdush..abdoux
1g 0:01:18:00  3/3 0.000213g/s 92.03p/s 271.1c/s 271.1C/s cambum..camuna
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@ubuntu:/test# john --format=crypt --single /etc/shadow
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Remaining 3 password hashes with 3 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:26  85% 0g/s 268.0p/s 268.0c/s 268.0C/s Myadmin2222..M99999123456
0g 0:00:00:33  100% 0g/s 267.0p/s 267.0c/s 267.0C/s 999991912..999991900
Session completed
root@ubuntu:/test# john --show
```

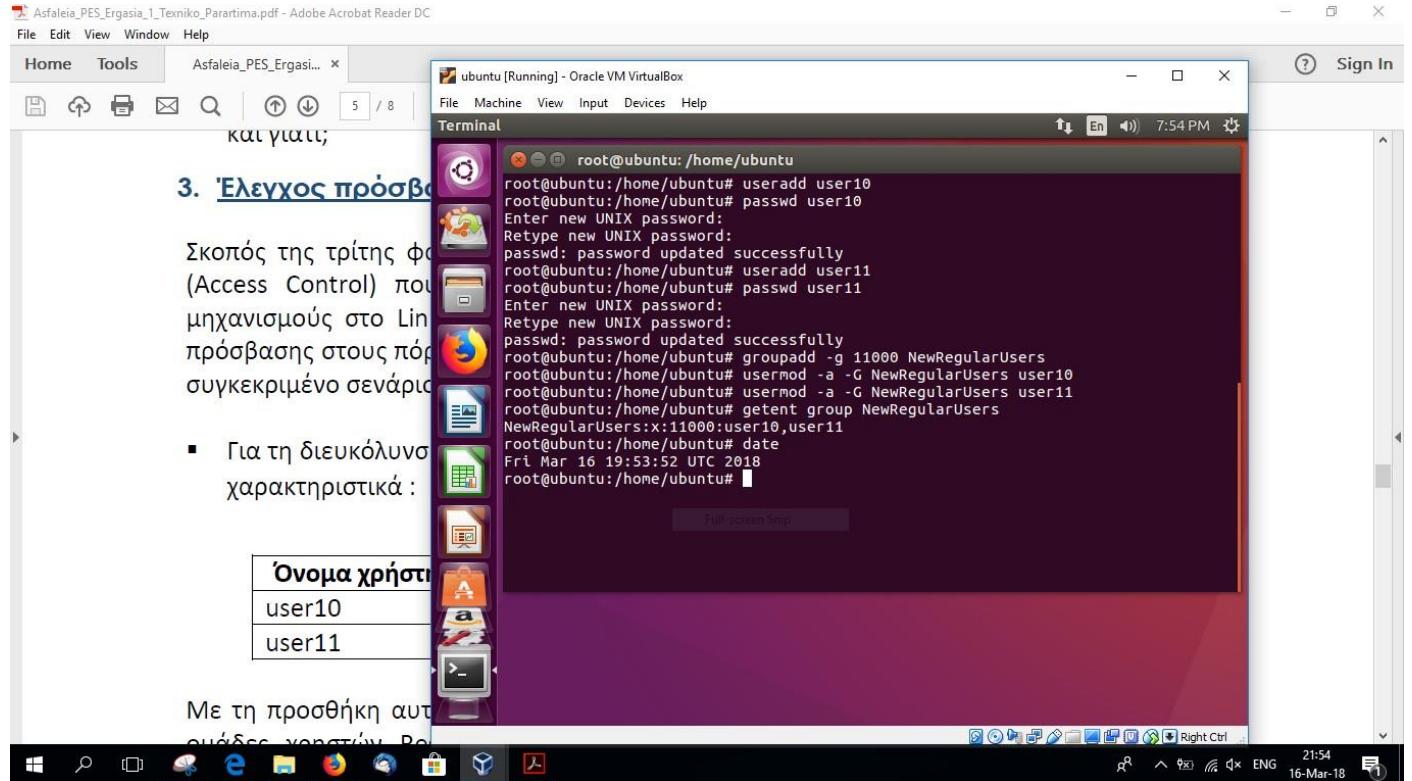
The terminal window is part of an Oracle VM VirtualBox environment, as indicated by the title bar. The desktop icons on the left include the Dash, Home, Applications, and Help. The system tray at the bottom right shows the date and time (9:14 PM, 3/22/2018), battery level (88%), and network status.

Παρατηρείτε ότι και στις δύο περιπτώσεις το john καταφέρνει να σπάσει τα δύο πρώτα προφίλ : τον ubuntu και τον user01. (Το dictionary το σταμάτησα περίπου στη 1 ώρα).

3. Έλεγχος πρόσβασης πόρων του Λειτουργικού Συστήματος

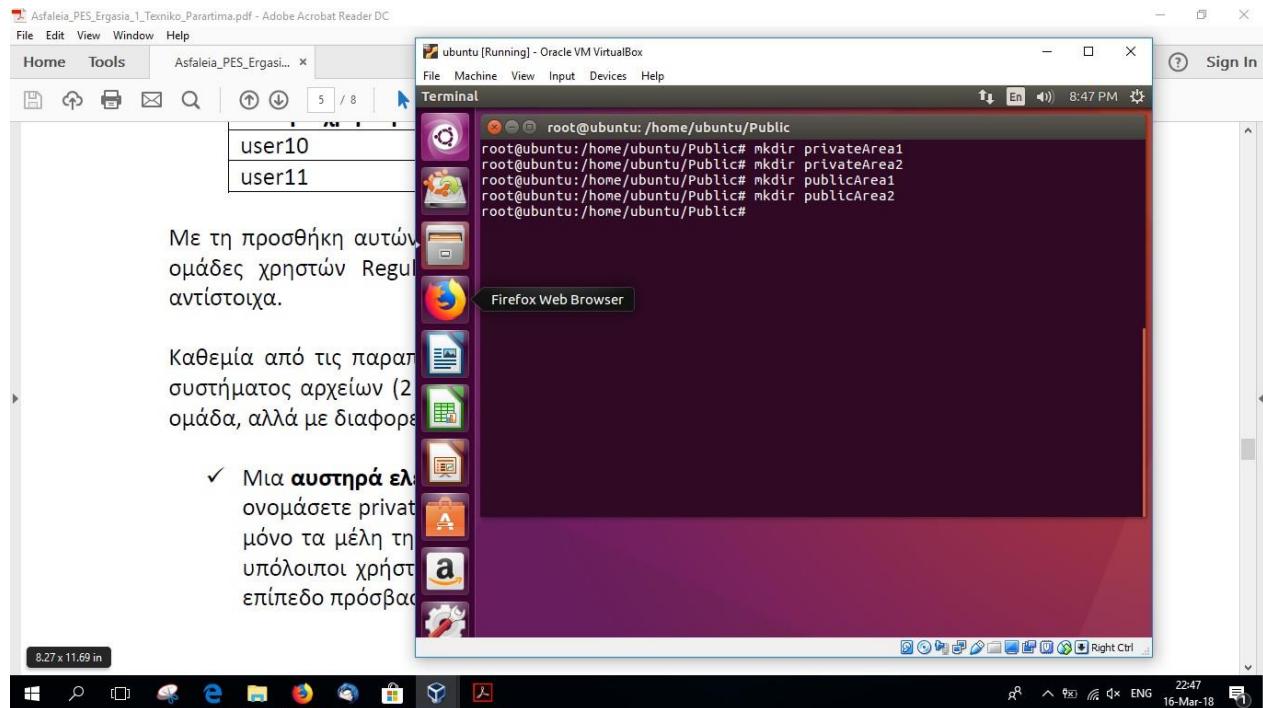
3.1 Δημιουργία νέων χρηστών

Παρακάτω φαίνεται η δημιουργία των νέων χρηστών και η εισαγωγή τους στην νέα ομάδα χρηστών

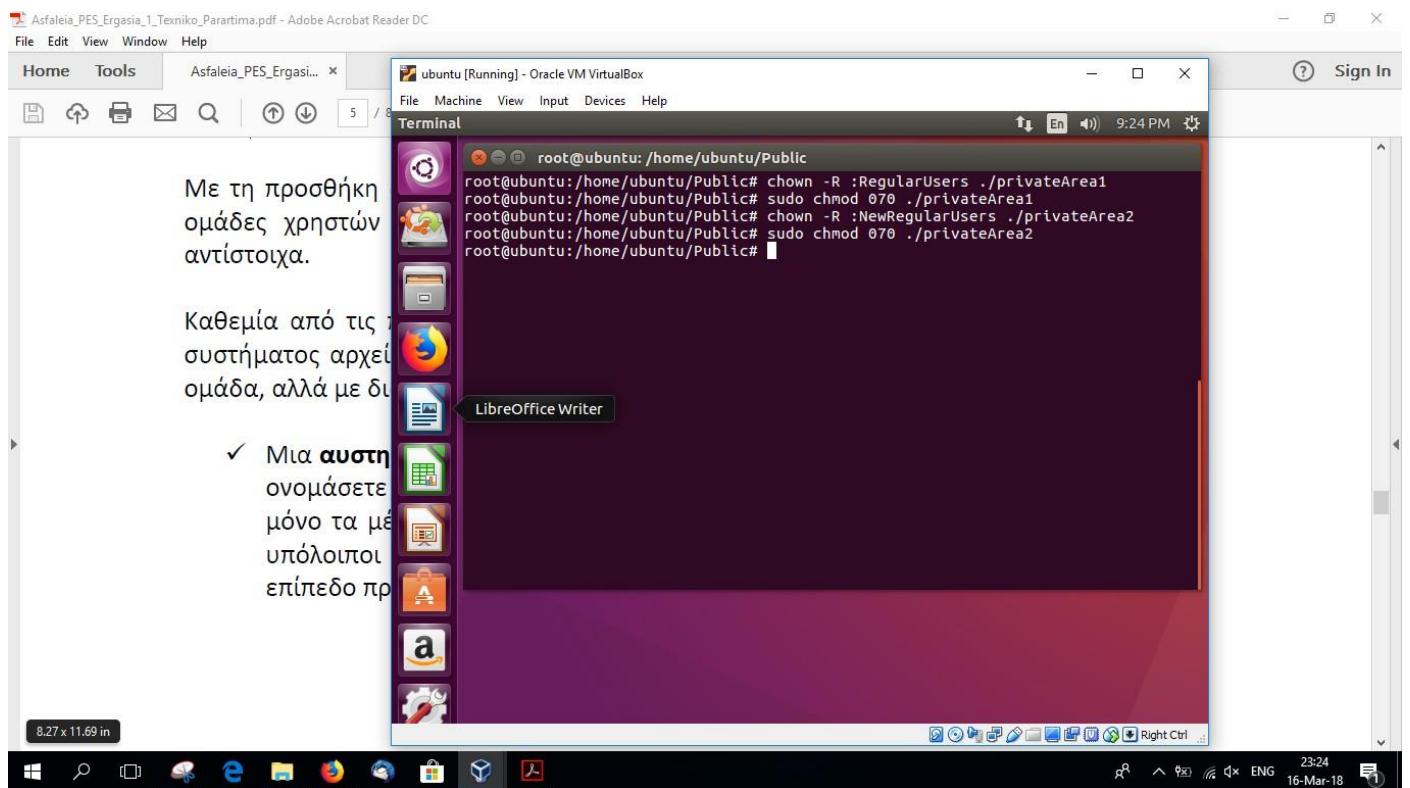


3.2 Δημιουργία φακέλων ομάδων χρηστών

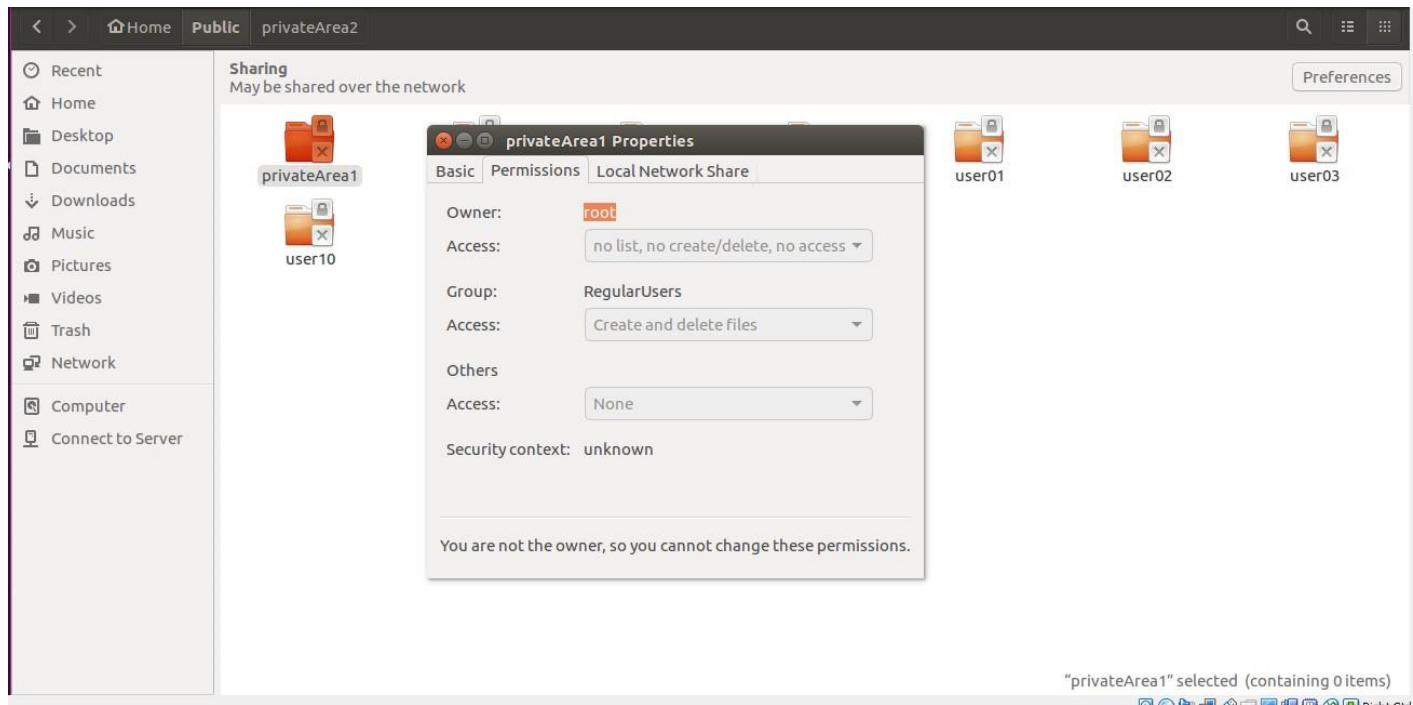
Δημιουργώ 4 φακέλους τους οποίους ονομάζω όπως ζητάει η εκφώνηση



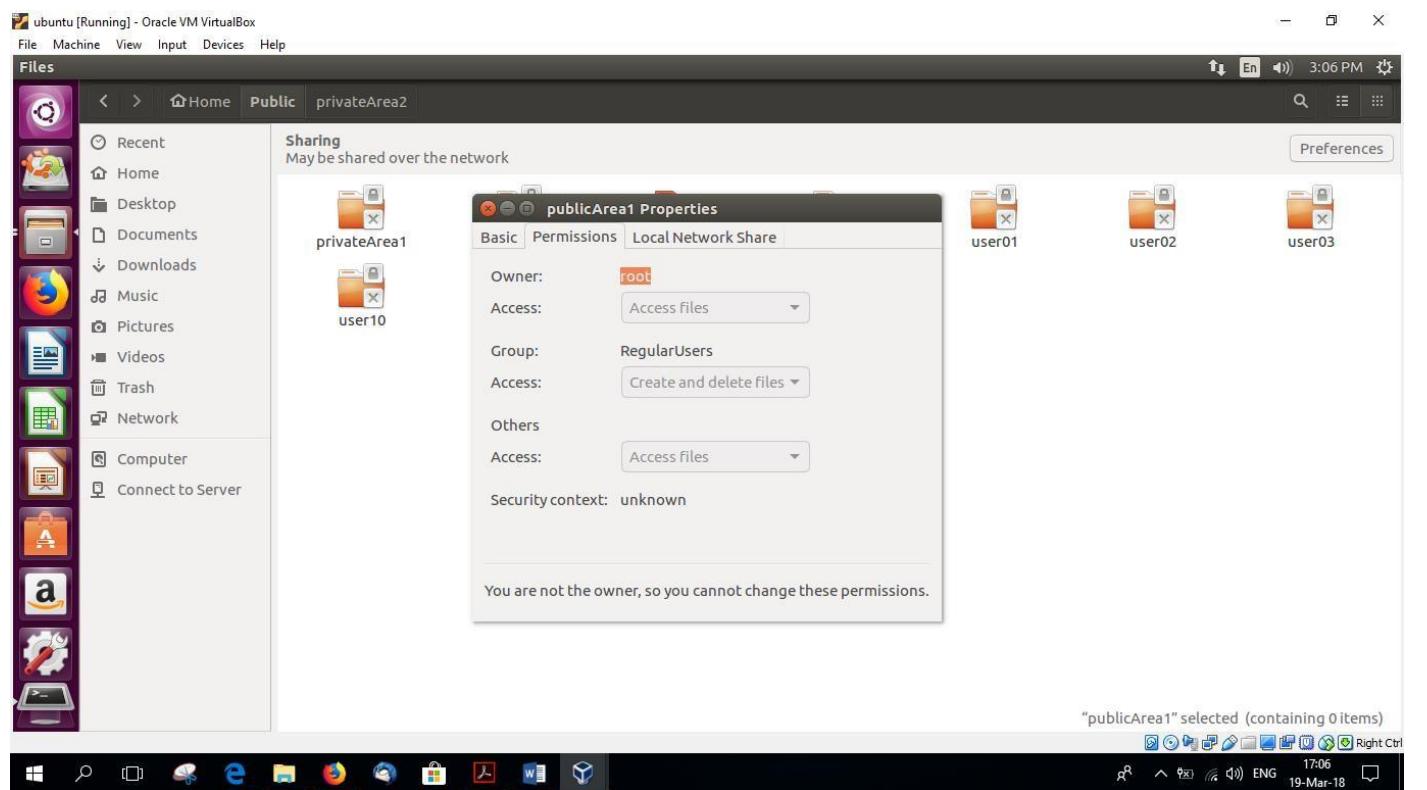
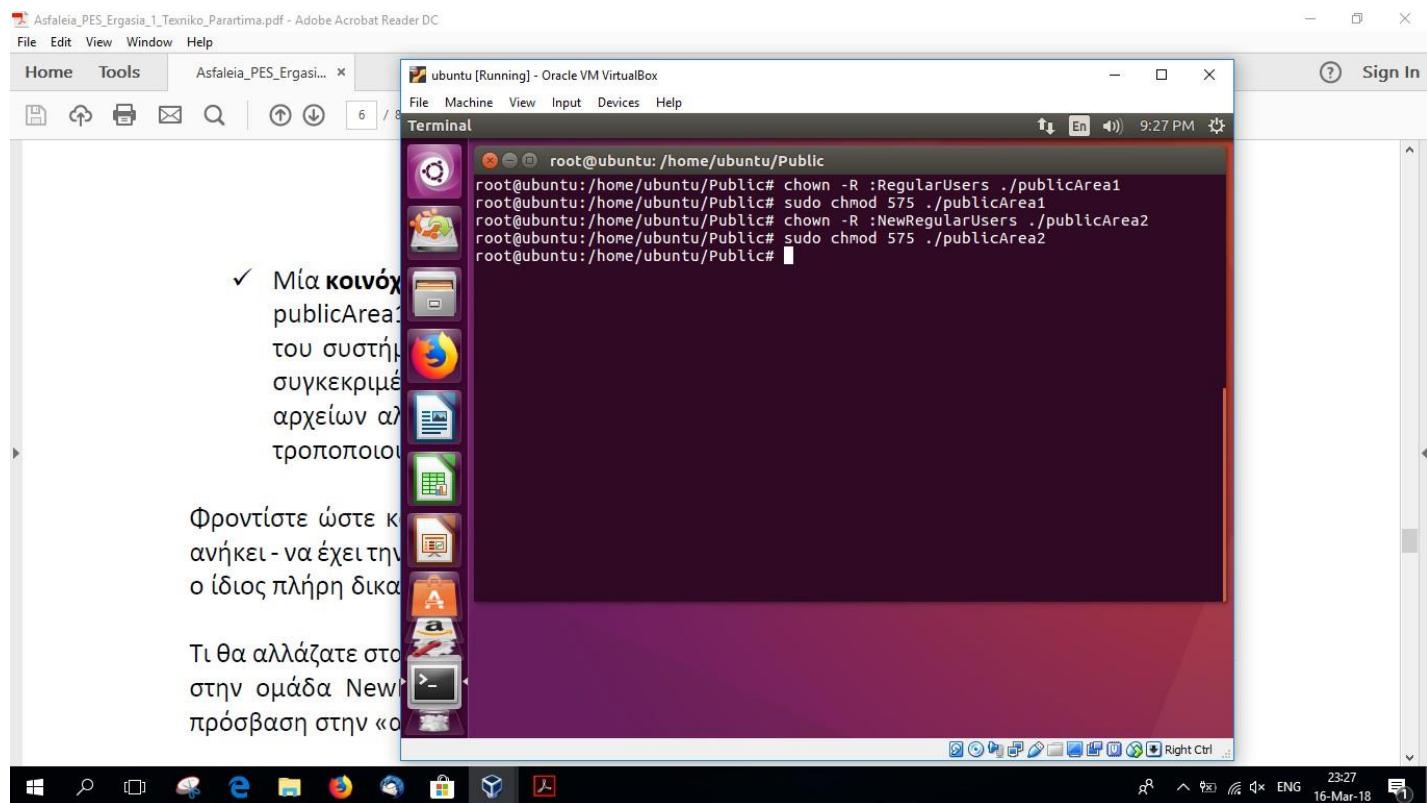
Παρακάτω φαίνονται οι εντολές που κάνουν τους 2 privateArea φακέλους να χρησιμοποιούνται αποκλειστικά από τους χρήστες της ομάδας RegularUsers



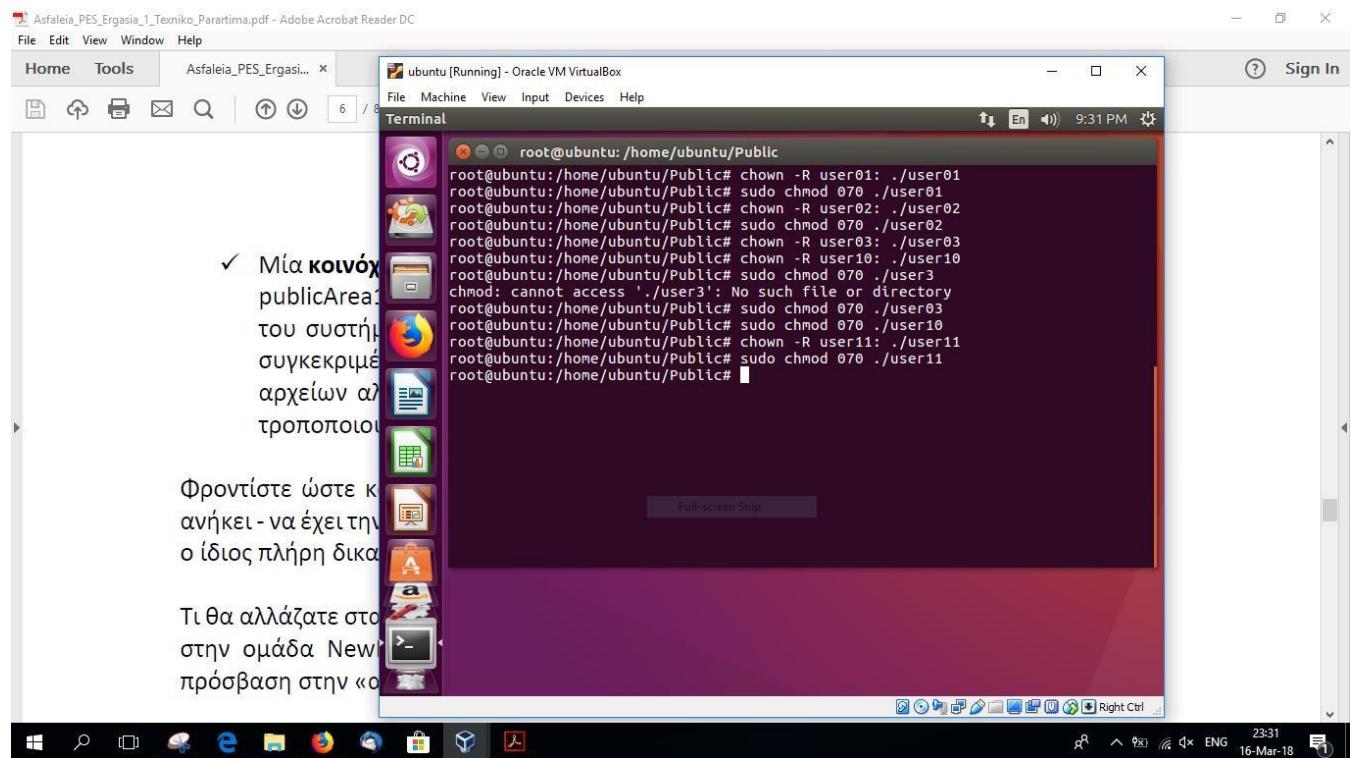
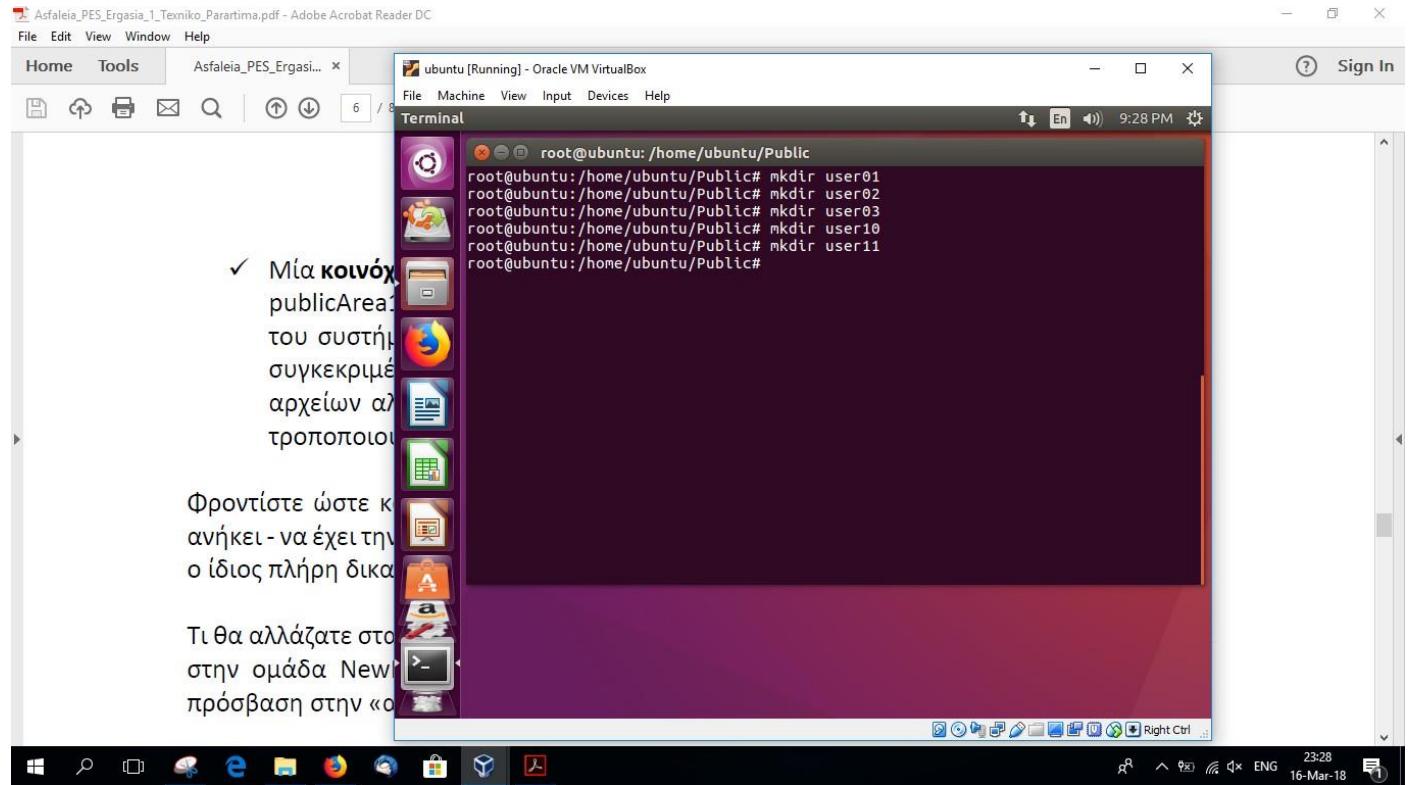
Πηγαίνω στον φάκελο privateArea1, πατάω δεξί κλικ και πληροφορίες.



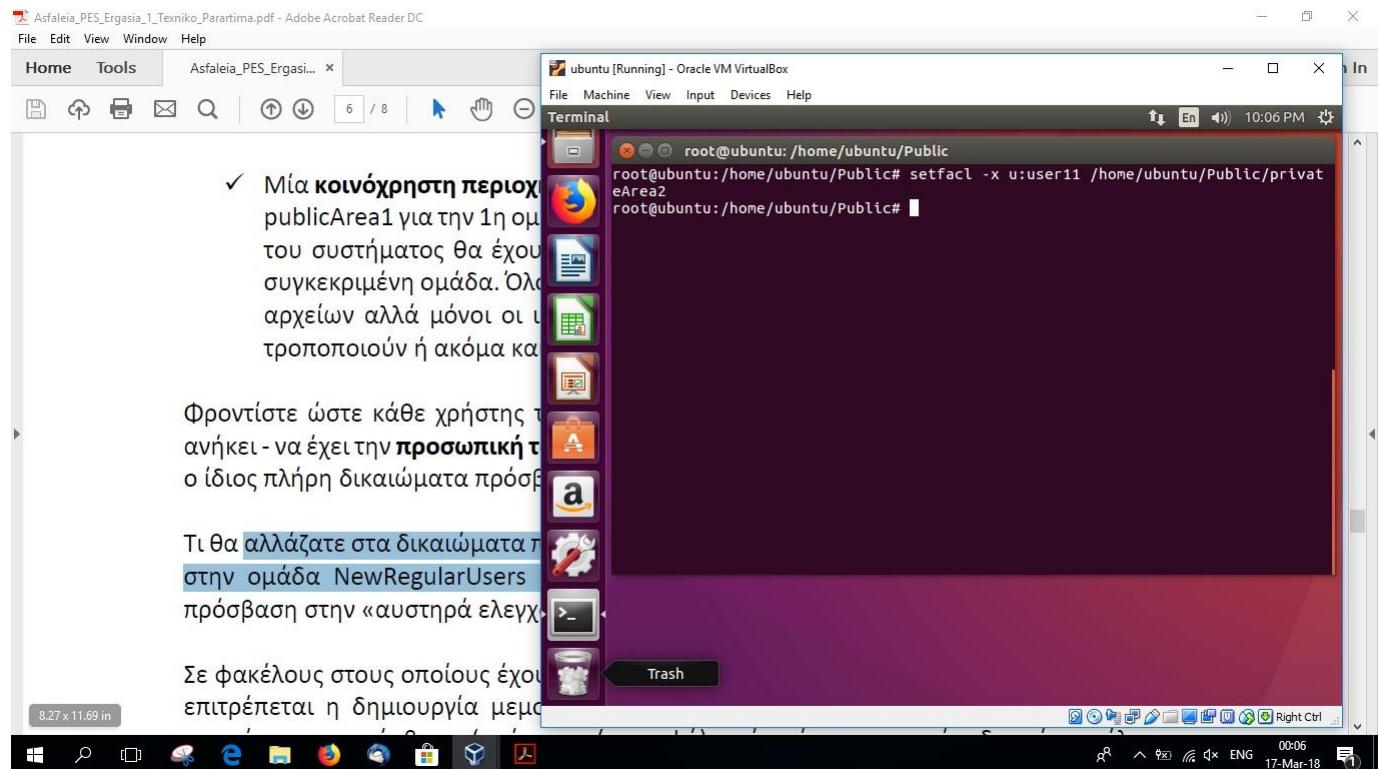
Παρακάτω φαίνεται η διαδικασία επεξεργασίας των φακέλων publicArea



Στην συνέχεια φτιάχνουμε τους φακέλους για κάθε χρήστη ξεχωριστά στους οποίους ο κάθε χρήστης θα έχει αποκλειστική πρόσβαση στον δικό του φάκελο



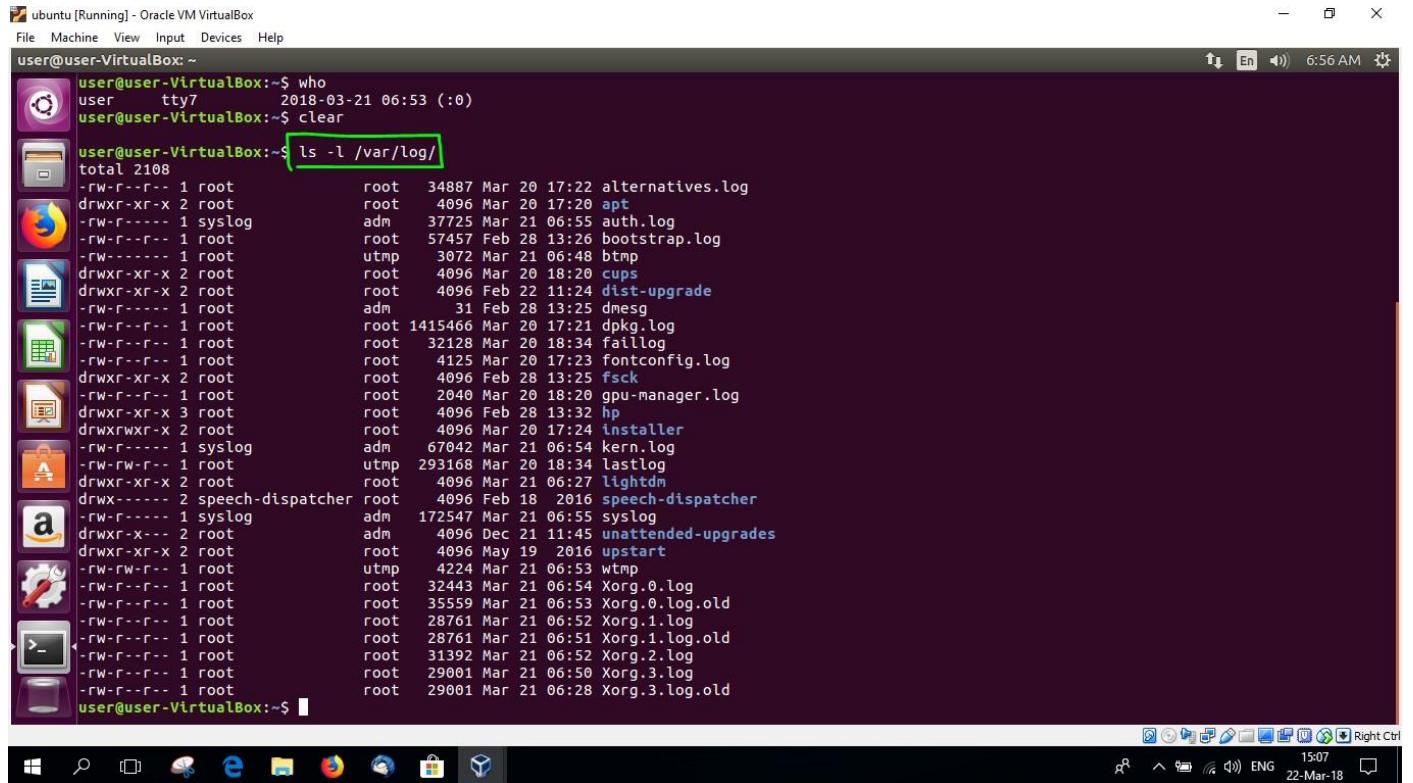
Με την παρακάτω εντολή αφαιρούμε τα δικαιώματα του χρήστη user11 να έχει πρόσβαση στον φάκελο privateArea2



4. Καταγραφή και παρακολούθηση ενεργειών χρήστη

4.1 Βασικά αρχεία καταγραφής στα linux

Στα linux τα βασικά αρχεία καταγραφής, βρίσκονται στο /var/log. Μερικά από τα αρχεία καταγραφής υπάρχουν μόνο σε κάποιες διανομές linux(πχ το dpkg.log υπάρχει στα Debian συστήματα). Παρακάτω φαίνονται όλα τα αρχεία καταγραφής που υπάρχουν στο λειτουργικό μας σύστημα :

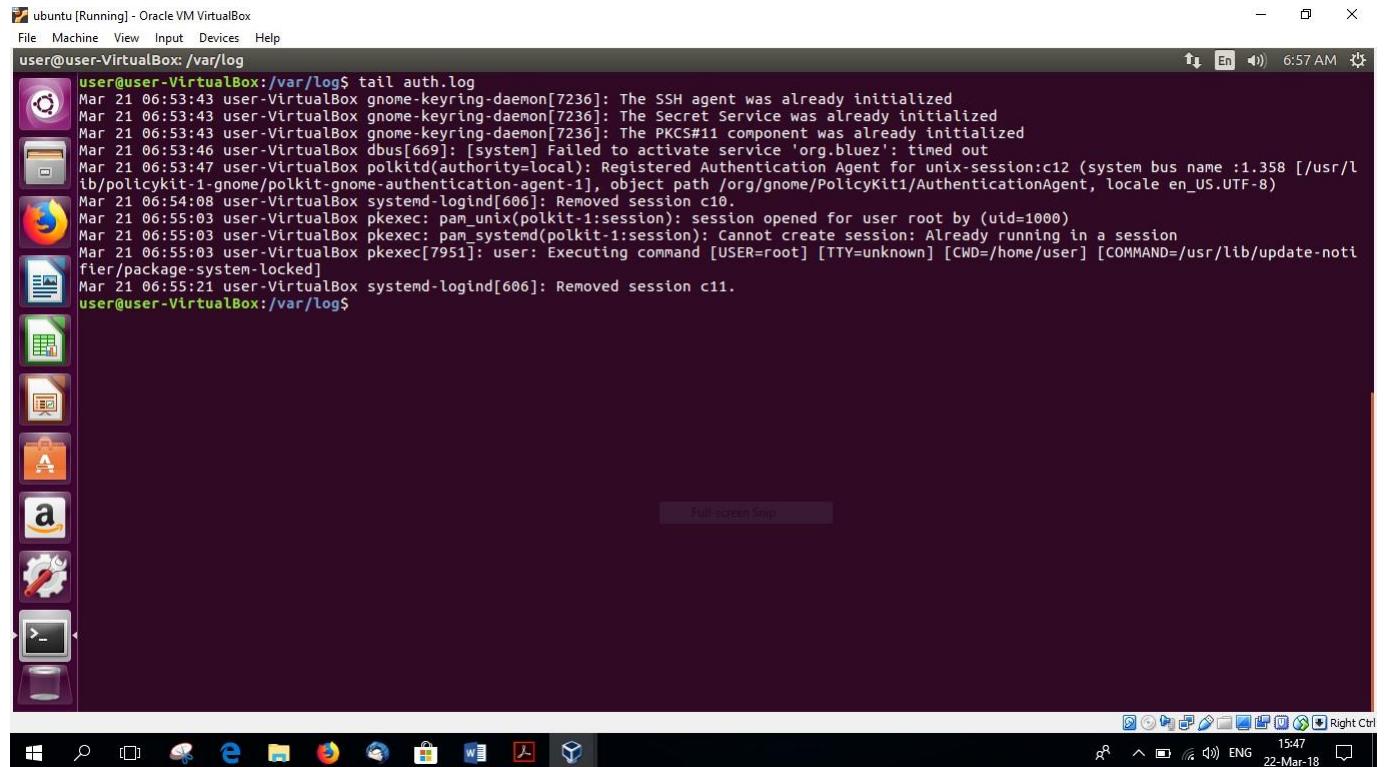


```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user@user-VirtualBox:~$ who
user    tty7     2018-03-21 06:53 (:0)
user@user-VirtualBox:~$ clear
user@user-VirtualBox:~$ ls -l /var/log/
total 2108
drwxr-xr-x 2 root      root      4096 Mar 20 17:22 alternatives.log
drwxr-xr-x 2 root      root      4096 Mar 20 17:20 apt
drwxr--r-- 1 syslog     adm       37725 Mar 21 06:55 auth.log
drwxr--r-- 1 root      root      57457 Feb 28 13:26 bootstrap.log
drwxr-xr-x 2 root      root      4096 Mar 20 18:20 cups
drwxr-xr-x 2 root      root      4096 Feb 22 11:24 dist-upgrade
drwxr--r-- 1 root      adm       31 Feb 28 13:25 dmesg
drwxr--r-- 1 root      root      1415466 Mar 20 17:21 dpkg.log
drwxr--r-- 1 root      root      32128 Mar 20 18:34 faillog
drwxr--r-- 1 root      root      4125 Mar 20 17:23 fontconfig.log
drwxr-xr-x 2 root      root      4096 Feb 28 13:25 fsck
drwxr--r-- 1 root      root      2040 Mar 20 18:20 gpu-manager.log
drwxr-xr-x 3 root      root      4096 Feb 28 13:32 hp
drwxrwxr-x 2 root      root      4096 Mar 20 17:24 installer
drwxr--r-- 1 syslog     adm       67042 Mar 21 06:54 kern.log
drwxr--r-- 1 root      utmp     293168 Mar 20 18:34 lastlog
drwxr-xr-x 2 root      root      4096 Mar 21 06:27 lightdm
drwxr----- 2 speech-dispatcher root      4096 Feb 18 2016 speech-dispatcher
drwxr--r-- 1 syslog     adm       172547 Mar 21 06:55 syslog
drwxr-xr-x 2 root      adm       4096 Dec 21 11:45 unattended-upgrades
drwxr-xr-x 2 root      root      4096 May 19 2016 upstart
drwxr--r-- 1 root      utmp     4224 Mar 21 06:53 wtmp
drwxr--r-- 1 root      root      32443 Mar 21 06:54 Xorg.0.log
drwxr--r-- 1 root      root      35559 Mar 21 06:53 Xorg.0.log.old
drwxr--r-- 1 root      root      28761 Mar 21 06:52 Xorg.1.log
drwxr--r-- 1 root      root      28761 Mar 21 06:51 Xorg.1.log.old
drwxr--r-- 1 root      root      31392 Mar 21 06:52 Xorg.2.log
drwxr--r-- 1 root      root      29001 Mar 21 06:50 Xorg.3.log
drwxr--r-- 1 root      root      29001 Mar 21 06:28 Xorg.3.log.old
user@user-VirtualBox:~$
```

Κάποια από τα βασικά αρχεία καταγραφής που βρίσκονται εκεί είναι τα εξής :

- **/var/log/auth.log**

Εδώ καταγράφονται πληροφορίες για τις εξουσιοδοτήσεις(authorization) που υπάρχουν στο σύστημα, όπως και συνδέσεις χρηστών στο σύστημα και οι μηχανισμοί αυθεντικοποίησης



```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user@user-VirtualBox: /var/log
user@user-VirtualBox: /var/log$ tail auth.log
Mar 21 06:53:43 user-VirtualBox gnome-keyring-daemon[7236]: The SSH agent was already initialized
Mar 21 06:53:43 user-VirtualBox gnome-keyring-daemon[7236]: The Secret Service was already initialized
Mar 21 06:53:43 user-VirtualBox gnome-keyring-daemon[7236]: The PKCS#11 component was already initialized
Mar 21 06:53:46 user-VirtualBox dbus[669]: [system] Failed to activate service 'org.bluez': timed out
Mar 21 06:53:47 user-VirtualBox polkitd(authority=local): Registered Authentication Agent for unix-session:c12 (system bus name :1.358 [/usr/lib/polkit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Mar 21 06:54:08 user-VirtualBox systemd-logind[606]: Removed session c10.
Mar 21 06:55:03 user-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Mar 21 06:55:03 user-VirtualBox pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Mar 21 06:55:03 user-VirtualBox pkexec[7951]: user: Executing command [USER=root] [TTY=unknown] [CWD=/home/user] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Mar 21 06:55:21 user-VirtualBox systemd-logind[606]: Removed session c11.
user@user-VirtualBox: /var/log$
```

- **/var/log/lastlog**

Εδώ καταγράφονται οι πρόσφατες πληροφορίες σύνδεσης στο λειτουργικό για όλους τους χρήστες

```

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user@user-VirtualBox: /var/log
lp                                **Never logged in**
mail                             **Never logged in**
news                            **Never logged in**
uucp                            **Never logged in**
proxy                           **Never logged in**
www-data                         **Never logged in**
backup                          **Never logged in**
list                            **Never logged in**
irc                            **Never logged in**
gnats                           **Never logged in**
nobody                           **Never logged in**
systemd-timesync                  **Never logged in**
systemd-network                   **Never logged in**
systemd-resolve                    **Never logged in**
systemd-bus-proxy                  **Never logged in**
syslog                           **Never logged in**
_apt                            **Never logged in**
messagebus                        **Never logged in**
uuid                            **Never logged in**
lightdm                          **Never logged in**
whoopsie                          **Never logged in**
avahi-autoipd                     **Never logged in**
avahi                           **Never logged in**
dnsmasq                           **Never logged in**
colord                           **Never logged in**
speech-dispatcher                  **Never logged in**
hplip                            **Never logged in**
kernoops                          **Never logged in**
pulse                            **Never logged in**
rtkit                            **Never logged in**
saned                            **Never logged in**
usbmux                           **Never logged in**
user                            **Never logged in**
user01                           **Never logged in**
user02                           **Never logged in**
user11                           **Never logged in**
user@user-VirtualBox:/var/log$ 

```

- **/var/log/faillog**

Εδώ υπάρχουν οι ανεπιτυχείς προσπάθειες των χρηστών να συνδεθούν στο σύστημα

- **/var/log/kern.log**

Αυτό το αρχείο περιέχει πληροφορίες καταγεγραμμένες από το kernel

```

ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user@user-VirtualBox: /var/log
user@user-VirtualBox: /var/log$ tail kern.log
Mar 21 06:56:52 user-VirtualBox NetworkManager[702]: <info> [1521629812.8427] dhcpc4 (enp0s3): state changed bound -> done
Mar 21 06:56:52 user-VirtualBox NetworkManager[702]: <info> [1521629812.8479] dhcpc4 (enp0s3): activation: beginning transaction (timeout in 4
5 seconds)
Mar 21 06:56:52 user-VirtualBox NetworkManager[702]: <info> [1521629812.8759] dhcpc4 (enp0s3): dhclient started with pid 8315
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0104] address 10.0.2.15
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0110] plen 24 (255.255.255.0)
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0116] gateway 10.0.2.2
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0120] server identifier 10.0.2.2
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0121] lease time 86400
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0122] nameserver '192.168.1.1'
Mar 21 06:56:54 user-VirtualBox NetworkManager[702]: <info> [1521629814.0122] dhcpc4 (enp0s3): state changed unknown -> bound
user@user-VirtualBox:/var/log$ 

```

- `/var/log/btmp`

Αυτό το αρχείο περιέχει πληροφορίες για τις ανεπιτυχείς προσπάθειες σύνδεσης στο λειτουργικό σύστημα

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@user-VirtualBox: /var/log". The command "tail bttmp" is being run, displaying a log entry from "/var/log/btmp". The log entry reads:

```
[root@user-VirtualBox ~]# tail /var/log/btmp
[1]ty7:0user:0***Z**[1]
user02***Zia***user11_**Z:,      w[1]ty023***[1]ty10:3user02:3*3*Z***[1]ty10:3user02:3*3*Z)***[1]ty10:3user:3*3*Z[1][1]user02|8*Z*kroot@user-VirtualBox
:[/var/log#]
```

The desktop interface includes a vertical dock on the left containing icons for various applications like a terminal, file manager, browser, and system tools. A "Full-screen Screenshot" button is visible in the center of the desktop. The bottom taskbar shows the system tray with icons for battery, signal, and network, along with the date and time (22-Mar-18, 15:50). The top right corner shows system status icons for battery level, signal strength, and volume.

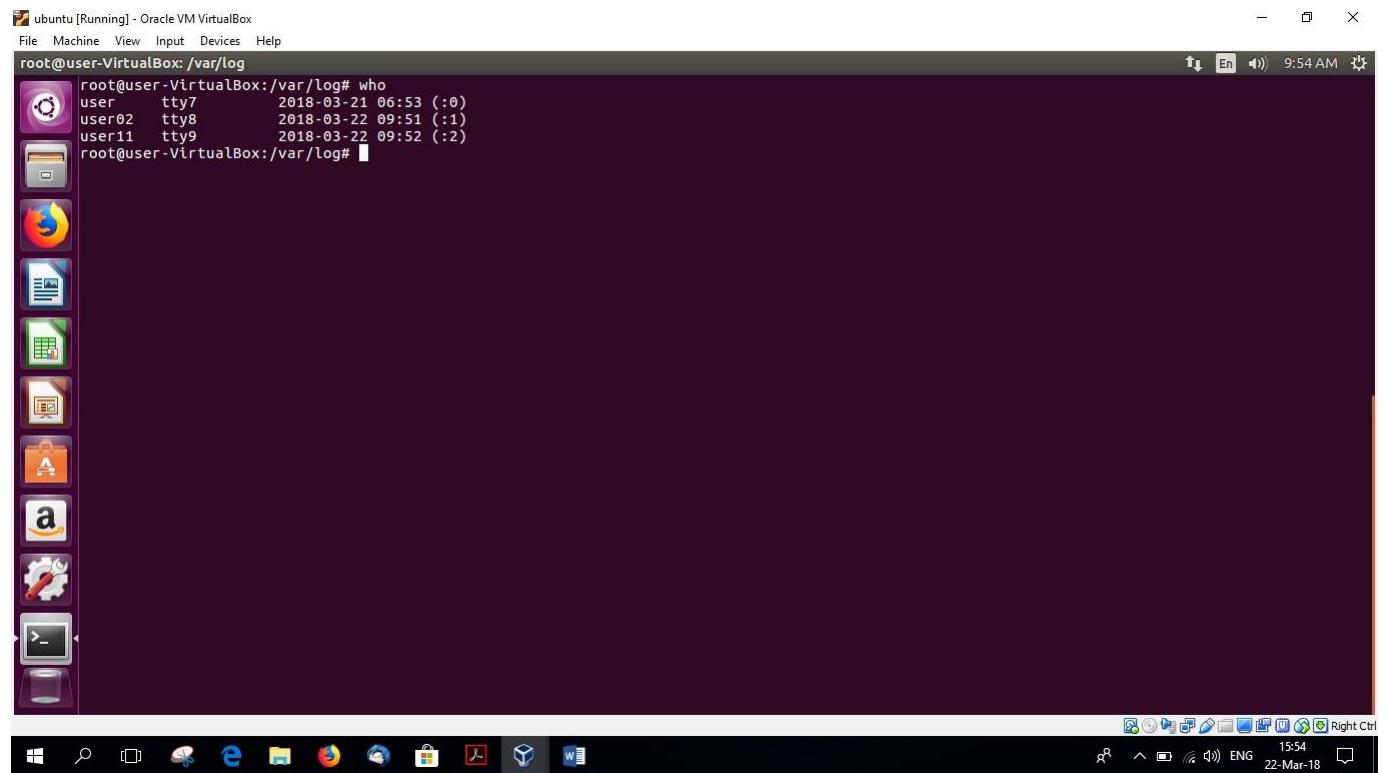
- `/var/log/boot.log`

Εδώ υπάρχουν πληροφορίες που καταγράφονται κατά την εκκίνηση του λειτουργικού συστήματος

- `/var/log/messages`

Το αρχείο αυτό καταγράφει global μηνύματα συστήματος, συμπεριλαμβανομένου και πληροφορίες κατά την εκκίνηση του λειτουργικού συστήματος

Για να δω ποιοι χρήστες είναι συνδεδεμένοι στο σύστημα, γράφω την εντολή «who»



5. Σύγκριση των δύο Λειτουργικών Συστημάτων

- Στα linux επειδή το λογισμικό διατίθεται δωρεάν, κάθε χρήστης μπορεί να τα βελτιώσει και να τα παραμετροποιήσει στα δικά του μέτρα. Με αυτές τις προϋποθέσεις το λειτουργικό των linux με το πέρασμα των χρόνων έχει βελτιωθεί αρκετά, σε πάρα πολλούς τομείς, και ειδικά σε αυτόν της ασφάλειας. Δεν τίθεται θέμα, ότι τα linux είναι πολύ πιο ασφαλές από τα windows. Ένα βασικό θέμα των windows είναι ότι «μολύνονται» από ιούς, κάτι που μειώνει το ποσοστό ασφάλειας του λειτουργικού συστήματος και χρειάζονται περεταίρω ενέργειες για την διασφάλιση της όσο δυνατόν περισσότερο γίνεται ασφάλειας του συστήματος. Επίσης, στα windows, επειδή ο κώδικας τους δεν διατίθεται, ένας διαχειριστής «συμβιβάζεται» με τις λειτουργίες που υπάρχουν ήδη στο σύστημα, σε σχέση με τα linux που λόγω του ότι ο κώδικας τους είναι ανοιχτός ο κάθε διαχειριστής μπορεί να παραμετροποιήσει και να αλλάξει ότι θέλει αυτός, σύμφωνα με τις δικές του ανάγκες.
- Η διαχείριση των μηχανισμών στα δύο λειτουργικά συστήματα διαφέρει αρκετά. Στα linux κύριος τρόπος διαχείρισης είναι το τερματικό(terminal) όπου μέσω των εντολών, ο διαχειριστής του συστήματος έχει πρόσβαση σε όλο το σύστημα και τις λειτουργίες του, και «τρέχοντας» τις απαραίτητες εντολές μπορεί να κάνει και τις ανάλογες παραμετροποιήσεις. Στα windows ο κύριος τρόπος διαχείρισης του server είναι μέσω γραφικού περιβάλλοντος. Άρα η διαχείριση ενός windows λειτουργικού είναι αρκετά πιο εύχρηστη και φυλική προς τον χρήστη από αυτή ενός linux. Επίσης στα windows server 2016, υπάρχει μια επιλογή που λέγεται «nano server» η οποία δεν έχει προεπιλεγμένο γραφικό περιβάλλον, και χρησιμοποιείτε για πολύ συγκεκριμένους σκοπούς. Αυτή η λειτουργία προσφέρει έναν αρκετά ελαφρύ server, με την διαφορά να είναι περίπου 11,5GB (500mb για έναν nano server και 12GB για έναν κανονικό με γραφικό περιβάλλον).
- Το σύστημα διαχείρισης το οποίο είναι πιο εύκολο για έναν διαχειριστή είναι τα windows. Ο κύριος λόγος που κάνει τα windows αρκετά πιο εύχρηστα (όπως εξηγήθηκε και παραπάνω) είναι το γραφικό περιβάλλον. Η παραμετροποίηση των λειτουργιών επειδή γίνεται μέσω γραφικού περιβάλλοντος, βοηθάει τον χρήστη να έχει καλύτερο έλεγχο στο τι ακριβώς κάνει στο σύστημα, αλλά και στο να βρει τι υπηρεσίες και τι επιλογές έχει σαν διαχειριστής στο λειτουργικό σύστημα.
Όσον αφορά την αποτελεσματικότητα των δύο λειτουργικών συστημάτων για τα σενάρια που μελετήσαμε, θεωρούμε ότι ένας linux server είναι πιο αποτελεσματικός. Ο κύριος λόγος είναι η ασφάλεια. Ο τρόπος κρυπτογράφησης των συνθηματικών των χρηστών, για παράδειγμα, στα linux είναι αρκετά πιο αποδοτικός από ότι στα windows, και αρκετά πιο δύσκολος για να χακαριστεί.

6. Πηγές

<https://technet.microsoft.com/en-us/library/cc956938.aspx>

<http://techgenix.com/how-cracked-windows-password-part2/>

http://download.cnet.com/L0phtCrack-Password-Auditor/3000-2653_4-10971696.html

-https://en.wikipedia.org/wiki/Dictionary_attack

-<http://searchsecurity.techtarget.com/definition/dictionary-attack>

-https://en.wikipedia.org/wiki/Brute-force_attack

-<http://searchsecurity.techtarget.com/definition/brute-force-cracking>

-<https://www.techopedia.com/definition/18091/brute-force-attack>

-https://en.wikipedia.org/wiki/Rainbow_table

-<https://www.lifewire.com/rainbow-tables-your-passwords-worst-nightmare-2487288>

<https://www.youtube.com/watch?v=6VvuSKUKFQg>

-<http://techgenix.com/configuring-syslog-agent-windows-server-2012/>

<https://unix.stackexchange.com/questions/78182/how-to-lock-users-after-5-unsuccessful-login-tries>

<https://www.thegeekstuff.com/2011/08/linux-var-log-files>

<https://www.digitalocean.com/community/tutorials/how-to-view-and-configure-linux-logs-on-ubuntu-and-centos>

- Επειδή κάποια screenshot ίσως να μην είναι τόσο καθαρά, υπάρχει οne drive link, στο οποίο υπάρχουν αριθμημένα και ταξινομημένα όλα τα screenshots της εργασίας :

<https://1drv.ms/f/s!Ar8zSXfQALTxq1pyWwzsDObOz8y>