**ქვიზი 3 ინფ უსაფრთ საფუძვლები 19 04 2013**

**1**. **რომელი ბრძანებით შეიძლება რეესტრში შესვლა:**

 ა) secpol.msc ბ) cmd

გ) dpedit.msc დ) regedit.exe

**2.კიდევ რომელი ბრძანებით შეიძლება რეესტრში შესვლა:**

 ა) secpol32.msc ბ) regedt32.exe

გ) dpedit32.msc დ) cmd32

**3. რეესტრში, HKEY\_USER საქაღალდე შეიცავს:**

ა) ყველა ლოკალური მომხმარებლის უნიკალურ SID იდენტიფიკატორს ბ) მხოლოდ ადმინისტრატორის უნიკალურ SID იდენტიფიკატორს

გ) მხოლოდ სტუმრის უნიკალურ SID იდენტიფიკატორს

დ) ყველა ადმინისტრატორის უნიკალურ SID იდენტიფიკატორს

**4. SID იდენტიფიკატორის დროითი ხანგრძლივობა**

ა) SID იდენტიფიკატორი იშლება კომპიუტერის ყოველ გამორთვისას

ბ) SID იდენტიფიკატორი იქმნება კომპიუტერის ყოველი ჩართვისას და იშლება კომპიუტერის ყოველ გამორთვისას

გ) SID იდენტიფიკატორი იქმნება მომხმარებლის ახალი აღრიცხვის ჩანაწერის შექმნისთანავე და არსებობს მისი წაშლის მომენტამდე

 დ) SID იდენტიფიკატორი იქმნება მომხმარებლის ახალი აღრიცხვის ჩანაწერის შექმნისთანავე და აკომპიუტერის ყოველ გამორთვამდე

**5. რამდენი სახის უსაფრთხოების ჯგუფი არსებობენ Windows-ში**

 ა) 5 ბ) 7

 გ) 9 დ) 11

**6. დამატებით რამდენი სახის უსაფრთხოების ჯგუფები შექმნა შეიძლება Windows-ში**

 ა) არ შეიძლება ბ) ერთის

 გ) სამი დ) ნებისმიერი

**7. Administrators (ადმინისტრატორები),**

ა) აქვს მრავალი პრივილეგია

ბ) ესაა მძლავრი ჯგუფი, რომელსაც აქვს უფლება სრულად აკონტროლოს სისტემა

გ) უზრუნველყოფს რეპლიკაციების მართვას დომენურ ქსელში

დ) ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლება განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის

**8.Users (მომხმარებლები)**:

 ა) აქვს მრავალი პრივილეგია

ბ) ესაა მძლავრი ჯგუფი, რომელსაც აქვს უფლება სრულად აკონტროლოს სისტემა

გ) ესაა შეზღუდული უფლებების ნაკრები ისეთი მომხმარებლებისათვის, რომელთაც არ ეძლევათ სისტემის ადმინისტრირების უფლება

დ) ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლება განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის

**9. Guests** :

ა) აქვს მრავალი პრივილეგია

ბ)ესაა მძლავრი ჯგუფი, რომელსაც აქვს უფლება სრულად აკონტროლოს სისტემა

გ) უზრუნველყოფს რეპლიკაციების მართვას დომენურ ქსელში

დ) ამ ჯგუფის წევრებს აქვთ შეზღუდული უფლება განკუთვნილი სტუმრებისა და შემთხვევითი მომხმარებლებისათვის

**10. როგორ შევქმნათ ახალი მომხმარებლის აღრიცხვის ჩანაწერები**

 ა) start →control panel→user accounts→manage Accounts→Create a password for your Accounts

 ბ) start → control panel → user accounts → next

 გ) start → control panel → user accounts → Create New Accounts→სახელის შეყვანა→next

დ) start → control panel → user accounts →manage Accounts → Change your Accounts

**11. რამდენი ტიპის აღრიცხვის ჩანაწერების შექმნის საშუალებას იძლევაWindows XP**

ა) მხოლოდ კომპიუტერის ადმინისტრატორის ბ) მხოლოდ შეზღუდული

გ) კომპიუტერის ადმინისტრატორის და შეზღუდული დ) არცეთი ამათგანის

**12. როგორ შევცვალოთ მომხმარებლის აღრიცხვის ჩანაწერებში მონაცემები**:

ა) start → control panel → user accounts → change an account→ შესაბამის პიქტოგრამაზე დაწკაპუნებით

ბ) start → control panel → user accounts → or pick an account to change ნაწილში შესაბამის პიქტოგრამაზე დაწკაპუნებით

გ) ორივე შემოთ ჩამოთვლილი საშუალებით

დ) არცერთი ზემოთ ჩამოთვლილი საშუალებით

**13**. **ადმინისტრატორის რა მონაცემების შეცვლაა შესაძლებელი აღრიცხვის ჩანაწერებში**:

ა) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის. ბ) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის;

 გ) სურათის,მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება. დ) ყველა ზემოთ ჩამოთვლილის

14**. სტუმრის რა მონაცემების შეცვლაა შესაძლებელი აღრიცხვის ჩანაწერებში**:

ა) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის. ბ) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის;

 გ) სურათის,მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება. დ) ყველა ზემოთ ჩამოთვლილის

**15. არა ადმინისტრატორის და არა სტუმრის რა მონაცემების შეცვლაა შესაძლებელი აღრიცხვის ჩანაწერებში**:

ა) სახელის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის. ბ) სახელის; სურათის; პასვორდის დაყენება, გაუქმება, შეცვლა; მომხმარებლის ტიპის;

 გ) სურათის,მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება. დ) ყველა ზემოთ ჩამოთვლილის

**16. როცა ხდება მომხმარებლის აღრიცხვის ჩანაწერების გაუქმება, მაშინ მომხმარებლის მიერ შექმნილი ფაილები:**

ა) ავტომატურად ნადგურდება ბ) ავტომატურად უცვლელად რჩება

გ) გვეკითხებიან - შევინახოთ სამუშაო მაგიდა და ფაილები ”ჩემ დოკუმენტებში” , თუ გავანადგუროთ

დ) არცერთი ზემოდ ჩამოთვლილი

17. **როგორ უნდა** **მოვახდინოთ ლოკალური კომპიუტერის უსაფრთხოების პარამეტრების შერჩევა**

ა) Start → Run→ ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting

ბ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting

გ) Start → gpedit.msc → ok → Windows Setting →Security Setting

დ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting

**18. პაროლების პოლიტიკის ჩართვა**

ა) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting→ Account Policies→ Password policy

ბ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting→ Account Policies→ Password policy

გ) Start → gpedit.msc → ok → Windows Setting →Security Setting→ Account Policies→ Password policy

დ) Start → Run →ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting →Account Policies→ Password policy

19. **პაროლების პოლიტიკის ჩართვისას შესაძლებელია:**

ა) მოვითხოვოთ პაროლების განუმეორება; პაროლის მოქმედების მაქსიმალური ვადა

ბ) პაროლის მოქმედების მინიმალური ვადა; პაროლის მინიმალური სიგრძე.

გ) პაროლის სირთულე; პაროლების შენახვა უკუ გაშიფრვით

დ) ყველა ზემოთ ჩამოთვლილი

**20. პაროლების გაშიფრის (გატეხვისთვის) დაცვისთვის ირჩევენ:**

ა) Start → Run ბრძანების სტრიქონი →gpedit.msc → ok → Administrative Templates→ Windows Setting →Security Setting→ Account Policies → Account Lockout

ბ) Start → Run ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting→ Account Policies→ Account Lockout

გ) Start → Run ბრძანების სტრიქონი →gpedit.msc → ok → Windows Setting →Security Setting →Account Policies→ Account Lockout

დ)Start → gpedit.msc → ok → Windows Setting →Security Setting→ Account Policies→ Password policy → Account Lockout

**21. Account Lockout** - **პაროლების გაშიფრის (გატეხვისგან) დაცვის პოლიტიკა:**

ა) დაბლოკავს განსაზღვრული (მითითებული) დროით აღრიცხვის ჩანაწერებს სისტემაში წარუმატებული შესვლის შემდეგ - Account Lockout duration.

ბ) მიეთითება ზღვრული რაოდენობა სისტემაში წარუმატებული შესვლის, რის შემდეგაც ჩაირთვება ბლოკირების ფუნქცია - Account Lockout threshold.

გ) მიეთითება დრო რომლის განმავლობაში იქნება დაბლოკილი სისტემა, სისტემაში წარუმატებული შესვლებს მცდელობებს შორის - Account Lockout counter after.

დ) ყველა ზემოთ ჩამოთვლილ შემთხვევებში.

**22. აუდიტის პოლიტიკის ჩასართავად საჭიროა:**

ა) Start → Run→ ბრძანების სტრიქონი →gpedit.msc → ok → Computer configuration→ Windows Setting →Security Setting→ local Policies → Audit Policy

ბ) Start → control panel → Administrative Tools → local Security Policy→ local Policies→ Audit Policy

გ) Start → Run→ ბრძანების სტრიქონი →secpol.msc → local Policies→ Audit Policy

დ) ყველა ზემოთ ჩამოთვლილი შემთხვევები.

**23. აუდიტის პოლიტიკით უსაფრთხოების თვალსაზრისით დაფიქსირდება;**

ა)აღრიცხვის ჩანაწერების სისტემაში შესვლის აუდიტი; აღრიცხვის ჩანაწერების მართვის აუდიტი; კატალოგთა სამსახურის წვდომის აუდირი.

ბ) სისტემაში შესვლის მოვლენათა აუდიტი; ობიექტების წვდომის აუდიტი; პოლიტიკის შეცვლის აუდიტი.

გ) პრივილეგიების გამოყენების აუდიტი; პროცესების მიყურადების აუდიტი; სისტემური მოვლენების აუდიტი.

დ) ყველა ზემოდ ჩამოთვლილი.

**24. მომხმარებლისათვის უფლებების მინიჭებისთვის საჭიროა** Administrative Tools-იდან:

ა) local Security Policy→ local Policies→ User Right Assignment

ბ) local Security Policy→ local Policies→ Security Options → Assignment

გ) local Security Policy→ local Policies→Public key Policies

დ) ყველა ზემოდ ჩამოთვლილი

**25. მომხმარებლების ჯგუფში ჩართვისათვის, ავირჩიოთ:**

ა) Start → Control panel → Administrative Tools → Computer Management→ System Tools→ Local users and groups

ბ) Start → Control panel → Administrative Tools → Computer Management→ System Tools→Shared Folder

გ) Start → Control panel → Administrative Tools → Computer Management→ Disk management

დ) Start → Control panel → Administrative Tools → Computer Management→Storage →Disk management

**26. სტანდარტული ჯგუფების რაოდენობა არის:**

ა) 7 ბ) 8

გ) 9 დ) 10

27. **რისი უფლება აქვს არქივის ოპერატორებს** **(Backup Operators);**

ა) ნებისმიერი ოპერაციის ჩატარების

ბ) ფაილებისა და ფოლდერების დაცვითი პარამეტრების შეცვლის, როცა საქმე ეხება რეზერვულ კოპირებას და აღდგენას

გ) ქსელის პარამეტრების ცვლილების

დ) ლოკალურ სისტემასთან მიერთების, შორი წვდომის საშუალებით

**28. გამოცდილ მომხმარებელთა ჯგუფში ახალი წევრის ჩართვისას:**

ა) Computer Management→ System Tools→ Local users and groups→Users→Power User→ add→advanced→ok→ok

ბ) Computer Management→ System Tools→ Local users and groups→group→Power User→ add→advanced→ok

გ) Computer Management→ System Tools→ Storage→group→Power User→ add→advanced→ok→ok

დ) Computer Management→ System Tools→ Local users and groups→group→Power User→ add→advanced→ok→ok

**29. როგორ გამოვიტანოთ გამაფრთხილებელი შეტყობინება:**

ა) run » Secpol.msc » Security Setting » Local Policies » Security Options » Message Text For Users Attampting Top log on » ტექსტის აკრეფა » ok

ბ) run » Secpol.msc » Security Setting » Local Policies » Security Options » Message Tittle For Users Attampting to log on » ტექსტის აკრეფა » ok

გ) run » Secpol.msc » Security Setting » Local Policies » Security Options » Message Tittle For Users Attampting to log on » ტექსტის აკრეფა » ok » Message Text For Users Attampting Top log on » ტექსტის აკრეფა » ok

დ) run » Secpol.msc » Security Setting » Local Policies » Message Tittle For Users Attampting to log on » ტექსტის აკრეფა » ok » Message Text For Users Attampting to log on » ტექსტის აკრეფა » ok

**30. სად ჩაიწერება გამაფრთხილებელი შეტყობინების სათაური:**

ა) Message Text For Users Attampting to log on

ბ) Message Tittle For Users Attampting to log on

გ) ორივე შემთხვევაში

დ) არცერთი