

Nastavni predmet:	PRAKTIČNE OSNOVE RAČUNALSTVA
Vježba: 18	NTFS dozvole u dijeljenim direktorijima te rad u komandnoj liniji
Cilj vježbe:	

Sve postupke, korištene naredbe i dobivene rezultate po točkama zadataka zapisivati u bilježnicu. Odgovoriti u bilježnicu na postavljena pitanja vezana uz ovu vježbu.

Zadaci:

1. Iz **HOME** particije ponovno pokrenuti računalno sa priključenim USB pogonom (prema prethodnim uputama). U **Multiboot** izborniku odabrati "**System Tools**", te zatim "**Windows 98**" operacijski sustav. Volkov Commander aplikaciju pokrenuti sa "**vc**" naredbom.
2. Pomoću aplikacije **MBRWIZD** vratiti sadržaj datoteke **H132HBKP.mbr** na **MBR** tvrdog diska, te zatim ponovno pokrenuti računalno bez USB pogona. Odabrati **Windows 7** operacijski sustav.
3. U prozoru "Network and Sharing Center", odabrati podizbornik "Advanced Sharing Settings" i za "Home or Work" mrežni profil odabrati opciju "Turn off password protected sharing". Proučiti svrhu te opcije.

KOMBINACIJA DOZVOLA MREŽNO DIJELJENIH DIREKTORIJA I NTFS DOZVOLA

4. Provjeriti jesu li stvoreni korisnici : **Korisnik1**, **Korisnik2** i **Korisnik3**. U slučaju da nisu, stvoriti ih te račune zaštititi lozinkom koja je jednaka korisničkom imenu.
U slučaju da korisnici već postoje, provjeriti da računi nisu onemogućeni te da imaju pripadajuće lozinke. Ujedno provjeriti da su članovi samo grupe **Users**.
5. Omogućiti dijeljenje direktorija **WSxy_Share_NTFS** koji se nalazi unutar direktorija **DOKUMENTI**, te grupi **Everyone** dati potpuna prava u **SHARE PERMISSIONS** prozoru (**Properties->Sharing->Advanced Sharing->Permissions**). U direktorij kopirati datoteke **read.txt** i **read and write.txt** (iz direktorija **LOKALNO**).

6. Prijaviti se kao **Korisnik1** te pokušati pristupiti dijeljenom direktoriju.

Pokušati pokrenuti **winhlp32.exe** izvršnu datoteku. Je li radnja uspješna? Zašto?

Pokušati zapisati trenutno korisničko ime u datoteku "**read and write.txt**". Je li radnja uspješna?

Zašto? Pokušati stvoriti novu datoteku i zatim je obrisati. Je li radnja uspješna? Zašto?

Pokušati preuzeti vlasništvo nad datotekom **read.txt**. Je li radnja uspješna? Zašto?

Iz prethodnog iskustva, što je moguće zaključiti o kombinaciji dozvola za dijeljenje (eng. **Share permissions**) i **NTFS** dozvola? Iz oba popisa (**NTFS** dozvole i dozvole za dijeljenje)

korisnika/grupa, koji je objekt **limitirajući** faktor u pokušaju preuzimanja vlasništva nad datotekom, te koja je dozvola potrebna kako bi radnja bila uspješna (pogledati tablicu u prilogu)?

7. Prijaviti se kao korisnik sa administratorskim pravima. Omogućiti dijeljenje direktorija **MREZNO** koji se nalazi unutar direktorija **WSxy_Share_NTFS**, te grupi **Everyone** dati samo prava za **čitanje** u **SHARE PERMISSIONS** prozoru. Za direktorij **KORISNIK1** koji se nalazi unutar direktorija **KORISNICI** postaviti slijedeće **NTFS** dozvole:

System – Full Control

Administrators – Full Control

Korisnik1 – Full Control

8. Prijaviti se kao **Korisnik1** te iz **Windows Explorer** aplikacije pristupiti direktoriju **KORISNIK1**. Unutar tog direktorija pokušati stvoriti novu tekstualnu datoteku imena **LokalniPristup.txt**. Je li radnja uspješna?

9. Ovaj puta pristupiti dijeljenom direktoriju **MREZNO** (\\Ime_Racunala\MREZNO), te unutar njega direktoriju **KORISNICI\KORISNIK1**. Ponovno pokušati stvoriti novu tekstualnu datoteku imena **Mreznipristup.txt**. Je li radnja uspješna? Zašto?

Iz prethodnog iskustva, što je moguće zaključiti o kombinaciji dozvola za dijeljenje (eng. **Share permissions**) i **NTFS** dozvola? Iz oba popisa (**NTFS** dozvole i dozvole za dijeljenje)

korisnika/grupa, koji je objekt **limitirajući** faktor u pokušaju preuzimanja vlasništva nad datotekom, te koja je **MINIMALNA** dozvola potrebna kako bi radnja bila uspješna?

10. Prijaviti se kao **Korisnik2**, pokušati pristupiti dijeljenom direktoriju **MREZNO**, te unutar njega direktoriju **KORISNICI\KORISNIK1**. Je li radnja uspješna? Zašto?

11. Ako već ne postoji, stvoriti lokalnu grupu **Korisnici** te u nju dodati korisnike : **Korisnik1**, **Korisnik2** i **Korisnik3**. Uvjeriti se kako su članovi te grupe samo navedeni korisnici.

12. Za mrežno dijeljeni direktorij **MREZNO**, u **SHARE PERMISSIONS** prozoru maknuti grupu **Everyone** iz popisa, te dodati grupu **Korisnici** te joj omogućiti potpuna prava pristupa.
13. Prijaviti se kao korisnik **SysAdmin**, te pokušati pristupiti dijeljenom direktoriju **MREZNO**. Je li radnja uspješna? Zašto? Ako se koristi **switch user** opcija, obvezno odjaviti korisnike : **Korisnik1**, **Korisnik2** i **SysAdmin**.
14. Direktoriju **KORISNICI** postaviti slijedeće **NTFS** dozvole:

System – Full Control

Administrators – Full Control

Korisnici – Read and Execute

15. Za svaki **KORISNIKx** direktorij (**x** je broj direktorija) dodati **NTFS** dozvolu koja će omogućiti pripadajućem korisničkom imenu potpuna prava, a naslijediti će **NTFS** dozvole direktorija **KORISNICI**. Primjer za **Korisnik3** direktorij:

System – Full Control

Administrators – Full Control

Korisnici – Read and Execute

Korisnik3 – Full Control

Koji će biti efekt postavljenih dozvola za korisnika **Korisnik2** dok pristupa direktoriju **Korisnik3**? Potrebno je testirati (kao **Korisnik2**) pristup direktoriju i stvaranje/brisanje datoteka, **LOKALNIM** i **MREŽNIM** pristupom.

KONFIGURACIJA NTFS DOZVOLA IZ KOMANDNE LINIJE

16. Prijaviti se kao korisnik sa administratorskim ovlastima te iz komandne linije stvoriti direktorij **LJUSKA** unutar direktorija **LOKALNO**. Unutar direktorija stvoriti slijedeću strukturu:

```
d:\DOKUMENTI\LOKALNO\LJUSKA>tree /f
Folder PATH listing for volume PrezimeRazred
Volume serial number is 5698-C300
D:
├── Ljuska.txt
├── RAZINA1
│   ├── razina1.txt
│   └── RAZINA2
│       └── razina2.txt
```

17. Proučiti upotrebu **icacls** aplikacije. Prikazati popis **NTFS** dozvola za direktorij **LJUSKA**. Proučiti i saznati što znače "**NT AUTHORITY**" i "**BUILTIN**" nazivi prije naziva korisnika i grupa u popisu.
18. Prema tablici iz **PRILOGA2** objasniti jednu **NTFS ACE** (eng. **Access Control Entry**) stavku iz popisa, npr:

BUILTIN\Administrators: (I)(OI)(CI)(F)

BUILTIN – Oznaka za ugrađene grupe u sustav, stvorene prilikom instalacije sustava

Administrators – Korisnička grupa, stvorena prilikom instalacije sustava, svi članovi grupe imaju administratorske ovlasti

(I) – NTFS stavka je naslijeđena od roditelja

(OI)(CI) – NTFS stavka tiče se postavke trenutnog direktorija, datoteka i poddirektorija

(F) – Korisnici ove grupe imaju potpune ovlasti.

Za objašnjavanje ne koristiti gornji primjer već neki drugi iz popisa!

19. U **kontrolnoj listi pristupa** (eng. **ACL, Access Control List**) maknuti stavku koja se tiče grupe **Users** (proučiti opciju **/remove**). Je li radnja bila uspješna? Zašto?
Pokušati ponoviti radnju, no ovaj puta kroz grafičko sučelje (aplikacija **Windows explorer**). Je li radnja bila uspješna? Zašto, koja se poruka pojavila? Ne micati stavku **Users**, samo pročitati poruku.
20. Proučiti kako se isključuje nasljeđivanje dozvola pomoću aplikacije **icacls**, te ih isključiti, no ostaviti već naslijeđene dozvole u listi (opcija **/inheritance:e** uključuje nasljeđivanje dozvola za

određeni objekt). Ponovno pokušati maknuti stavku koja se tiče grupe **Users**, te se uvjeriti u uspješnost te radnje.

21. U **kontrolnoj listi pristupa** (eng. **ACL, Access Control List**) ostaviti samo pristupne stavke (eng. **ACE, Access Control Entry**) koje se tiču grupe **Administrators** i korisnika **SYSTEM**, ostale stavke maknuti sa liste. Očekivani izgled **ACL** liste je prikazan na slici:

```
D:\DOKUMENTI\LOKALNO>icacls ljuska
ljuska NT AUTHORITY\SYSTEM:(OI)(CI)(F)
        BUILTIN\Administrators:(OI)(CI)(F)
Successfully processed 1 files; Failed processing 0 files
```

Kontrolnoj listi pristupa za direktorij **LJUSKA** dodati stavku za korisnika **Korisnik1** te mu pridodati dozvolu za potpune ovlasti (proučiti opciju **/grant**). Uvjeriti se u uspješnost izvršene radnje.

Primjer davanja ovlasti: **icacls FOLDER /grant User1:(F)**

22. **Korisniku1** ovog puta omogućiti dozvolu za modifikaciju sadržaja (eng. **Modify Access**). Je li radnja bila uspješna? Proučiti zadaću proširenja opcije **/grant:r** te ju upotrijebiti prilikom izmjene dozvole za korisnika **Korisnika1**. Je li ovaj put radnja bila uspješna? Je li potrebno tu opciju koristiti i prilikom povećanja ovlasti korisnika?
23. Prijaviti se kao **Korisnik1** te pokušati obrisati datoteku **Ljuska.txt**. Je li radnja uspješna? Provjeriti efektivne dozvole za direktorije **LJUSKA**, **RAZINA1** te datoteku **Ljuska.txt**. U čemu se razlikuju? Ponovno se prijaviti kao korisnik sa administratorskim ovlastima te u pristupnoj listi usporediti stavke **Korisnik1**, **SYSTEM** i **Administrators** sa tablicom objašnjenja u **Prilogu2** (na kraju ovog dokumenta). Zašto **Korisnik1** nije imao ovlasti brisanja datoteke? Ispisati pristupne liste za direktorij **LJUSKA** i sve poddirektorije, te provjeriti u kojima se nalazi stavka za korisnika **Korisnik1** (proučiti opciju **/t**).
24. Obrisati postojeću stavku, te stvoriti koju koja ima dozvolu (jednake ovlasti kao u prošlom primjeru) za korisnika **Korisnik1** tako da utječe i na poddirektorije i datoteke uz trenutni direktorij **LJUSKA** (pomoć potražiti u tablici u **Prilogu2**). Ispisati **ACL** liste za direktorij **LJUSKA** i sve poddirektorije, te provjeriti nalazi li se u svakoj od njih stavka za korisnika **Korisnik1**, te proučiti svrhu zastavice (I) u stavkama.
25. Isključiti nasljeđivanje dozvola za sve poddirektorije unutar direktorija **LJUSKA** (opcija **/t**), ali ih zadržati. Ponovno ispisati pristupne liste za direktorij **LJUSKA** i sve poddirektorije. Što se dogodilo sa zastavicom (I) u stavkama? Zašto? Za direktorij **LJUSKA** stvoriti novu stavku za korisnika **Korisnik2** sa dozvolom modifikacije sadržaja tako da utječe i na poddirektorije i datoteke, uz trenutni direktorij.

26. Ispisati **ACL** liste za direktorij **LJUSKA** i sve poddirektorije, te provjeriti nalazi li se u svakoj od njih stavka za korisnika **Korisnik2**. Objasniti zašto.
27. Uključiti nasljeđivanje dozvola za direktorij **LJUSKA** i sve poddirektorije te ponovno ispisati **ACL** liste. Mogu li se uočiti duple stavke u svakoj listi? Razlikuju li se u nečemu? Prikazati i proučiti listu za direktorij **LJUSKA** i u grafičkom sučelju.
28. U ovom trenutku je najjednostavnije vratiti sve dozvole na početne vrijednosti, odnosno obrisati postojeće liste, te ih popuniti sa naslijeđenim dozvolama od direktorija više razine (u ovom slučaju, direktorij **LOKALNO**).
Pomoću opcije **/reset** vratiti sve dozvole na početnu vrijednost za direktorij **LJUSKA** i poddirektorije. Provjeriti uspješnost radnje.
29. Za direktorij **LJUSKA** (trenutni direktorij, poddirektorije i datoteke) postaviti slijedeće dozvole (što je potrebno poduzeti sa opcijom nasljeđivanja?):

System – Full Control

Administrators – Full Control

Users – Read and Execute

30. Za direktorij **LJUSKA** postaviti dozvolu modificiranja za **Korisnik1** profil, no ograničiti opseg dozvole samo na **trenutni direktorij i datoteke** (pomoć u prilogu 3). Konfiguraciju odraditi iz komandne linije, te provjeriti izgled pristupne liste. Provjeriti detalje pristupne stavke i iz grafičkog sučelja (**Properties->Security->Advanced->...**). Uočiti sadržaj opcije **"Apply to"**, te je li označena kućica opcije **"Apply these permissions to objects and/or containers within this container only"**. Što točno predstavljaju termini **"objects"** i **"containers"**?
31. Prijaviti se kao **Korisnik1** te zapisati svoje korisničko ime (proizvoljnom metodom) u sve tri datoteke : **Ljuska.txt**, **Razina1.txt** i **Razina2.txt**. Jesu li sve radnje uspješne?
32. Prijaviti se kao **Korisnik1**, te pokušati stvoriti tekstualne datoteke (pod ime postaviti svoje korisničko ime) u direktorijima **LJUSKA**, **RAZINA1** i **RAZINA2**. Koje su radnje uspješne? Pokušati stvoriti direktorije (pod ime postaviti svoje korisničko ime) u direktorijima **LJUSKA**, **RAZINA1** i **RAZINA2**. Koje su radnje uspješne?
33. Za direktorij **LJUSKA** izbrisati sve stavke za **Korisnik1** korisnika, te zatim postaviti dozvolu modificiranja za **Korisnik1** profil, no ograničiti opseg dozvole samo na **trenutni direktorij i datoteke** (pomoć u **Prilogu 3**) i obavezno uključiti opciju koja brani **propagaciju/širenje** dozvola na direktorije nižih razina (opcija **NP**, eng. **don't propagate inherit**). Konfiguraciju odraditi iz komandne linije, te provjeriti izgled pristupne liste. Provjeriti detalje pristupne stavke i iz grafičkog
- POR – LV18 – NTFS dozvole u dijeljenim direktorijima te rad u komandnoj liniji

sučelja (**Properties->Security->Advanced->...**). Uočiti sadržaj opcije "Apply to", te je li označena kućica opcije "**Apply these permissions to objects and/or containers within this container only**".

34. Ponoviti **31.** i **32.** Zadatak, te usporediti razlike. Što se točno promijenilo? Proučiti tablice iz **Priloga 3** te izvući zaključak oko korištenja zabrane propagacije dozvola.
35. Za direktorij **LJUSKA** postaviti potpune ovlasti za **Korisnik2** profil, no ograničiti opseg dozvole samo na **poddirektorije** (pomoć u **Prilogu 3**). Konfiguraciju odraditi iz komandne linije, te provjeriti izgled pristupne liste. Provjeriti detalje pristupne stavke i iz grafičkog sučelja (**Properties->Security->Advanced->...**). Uočiti sadržaj opcije "**Apply to**".
36. Prijaviti se kao **Korisnik2**, te pokušati stvoriti direktorije sa proizvoljnim imenom unutar direktorija : **LJUSKA**, **RAZINA1** i **RAZINA2**. Koje su radnje uspješne? Zašto? Obrisati stvorene direktorije.
37. Za direktorij **LJUSKA** prvo obrisati postojeću stavku za **Korisnik2** profil, te zatim stvoriti novu i postaviti potpune ovlasti za **Korisnik2** profil, no ograničiti opseg dozvole samo na **poddirektorije** (pomoć u **Prilogu 3**) i obvezno uključiti opciju koja brani propagaciju/širenje dozvola na direktorije nižih razina (opcija **NP**, eng. **don't propagate inherit**). Konfiguraciju odraditi iz komandne linije, te provjeriti izgled pristupne liste.
38. Prijaviti se kao **Korisnik2**, te pokušati stvoriti direktorije sa proizvoljnim imenom unutar direktorija : **LJUSKA**, **RAZINA1** i **RAZINA2**. Koje su radnje uspješne? Zašto?

PITANJA:

1. Koja je razlika između dozvola za dijeljenje i **NTFS** dozvola?
2. Prilikom **lokalnog** pristupa nekom direktoriju (npr. korisnik sjedi za tim računalom), koja će vrsta dozvola imati veću težinu, **NTFS** ili **SHARING**?
3. Prilikom **udaljenog** pristupa nekom direktoriju (npr. korisnik pristupa dijeljenom direktoriju), koja će vrsta dozvola imati veću težinu, **NTFS** ili **SHARING**?
4. Prilikom kombinacije dozvola za dijeljenje i **NTFS** dozvola, koju vrstu je dobra praksa maksimalno omogućiti, a na koju postavljati restrikcije?
5. Prilikom provjere efektivnih **NTFS** dozvola za korisnika/grupu, ulaze li u kalkulaciju i dozvole za dijeljenje?
6. Koji je efekt korištenja opcija zabrane propagacije/širenja dozvola?
7. Izvršena je naredba za brisanje postojećih pristupnih stavki **NTFS** dozvola nekog direktorija. Sintaksa naredbe je ispravna, te nije došlo do pogreške (npr. manjak dozvole za izmjenu), no do izmjena nije došlo. Što je vjerojatan uzrok?
8. Nakon konfiguracije različitih **NTFS** dozvola za određeni direktorij i datoteke unutar njega, rezultati konfiguracije su neočekivani, te je dijagnostika i rješavanje problema otežano. Što bi bilo dobro napraviti u ovoj situaciji?
9. Korisnici **Željki** nisu dana specifična **NTFS** prava za datoteku, no ona svejedno može pregledavati sadržaj. Koji je vjerojatan razlog za ovu situaciju?
10. Korisniku **Ivanu** su dana **potpuna prava** nad određenim direktorijem, no on ipak ne može niti stvarati ni brisati datoteke unutar njega. Koji je vjerojatan razlog (ili razlozi) za ovu situaciju?

PRILOG 1

	Read	Write	List Folder Contents	Read & Execute	Modify	Full Control
Traverse Folder/Execute file			X	X	X	X
List Folder/Read Data	X		X	X	X	X
Read Attributes	X		X	X	X	X
Read Extended Attributes	X		X	X	X	X
Create Files/Write Data		X			X	X
Create Folders/Append Data		X			X	X
Write Attributes		X			X	X
Write Extended Attributes		X			X	X
Delete Subfolders and Files						X
Delete					X	X
Read Permissions	X		X	X	X	X
Change Permissions						X
Take Ownership						X

<http://www.sqa.org.uk/e-learning/ClientOS02CD/images/pic004.jpg>

PRILOG 2

	(I)	(OI)	(CI)	(IO)	(NP)		ZNAČENJE	DODATNA OPCIJA	KOMENTAR
1.						(F)	This folder only		Tiče se samo postavke trenutnog direktorija, no ne i datoteka/direktorija unutar njega
2.		(OI)	(CI)			(F)	This folder,subfolders and files		Tiče se postavke trenutnog direktorija, datoteka i poddirektorija
3.			(CI)			(F)	This folder and subfolders		Tiče se postavke trenutnog direktorija i poddirektorija
4.		(OI)				(F)	This folder and files		Tiče se postavke trenutnog direktorija i datoteka
5.		(OI)	(CI)	(IO)		(F)	Subfolder and files only		Tiče se postavke poddirektorija i datoteka
6.			(CI)	(IO)		(F)	Subfolders only		Tiče se postavke samo poddirektorija
7.		(OI)		(IO)		(F)	Files only		Tiče se postavke samo datoteka
8.		(OI)	(CI)		(NP)	(F)	This folder,subfolders and files	DON'T PROPAGATE	Tiče se postavke trenutnog direktorija, datoteka i poddirektorija, no samo u prvoj razini
9.		(OI)			(NP)	(F)	This folder and files	DON'T PROPAGATE	Tiče se postavke samo trenutnog direktorija i samo u prvoj razini
10.	(I)	(OI)	(CI)			(F)	This folder,subfolders and files	INHERITED	Tiče se postavke trenutnog direktorija, datoteka i poddirektorija, pravilo je naslijeđeno od roditelja

PRILOG 3

REZULTATI DOZVOLA SA UKLJUČENOM PROPAGACIJOM/ŠIRENJE (standardno uključena)	Dozvola vrijedi za trenutni direktorij	Dozvola vrijedi za trenutni direktorij i poddirektorije	Dozvola vrijedi za datoteke u trenutnom direktoriju	Dozvola vrijedi samo za poddirektorije	Dozvola vrijedi za sve datoteke u poddirektorijima
This folder only	X				
This folder,subfolders and files	X	X	X	X	X
This folder and subfolders	X	X		X	
This folder and files	X		X		X
Subfolder and files only		X	X	X	X
Subfolders only		X		X	
Files only			X		X

REZULTATI DOZVOLA SA ISKLUČENOM PROPAGACIJOM/ŠIRENJE	Dozvola vrijedi za trenutni direktorij	Dozvola vrijedi za trenutni direktorij i poddirektorije	Dozvola vrijedi za datoteke u trenutnom direktoriju	Dozvola vrijedi samo za poddirektorije	Dozvola vrijedi za sve datoteke u poddirektorijima
This folder only	X				
This folder,subfolders and files	X	X	X		
This folder and subfolders	X	X			
This folder and files	X		X		
Subfolder and files only		X	X		
Subfolders only		X			
Files only			X		