Nastavni predmet:	**PRAKTIČNE OSNOVE RAČUNALSTVA**
Vježba:	LV15 – NTFS dozvole u Powershell okruženju
Cilj vježbe:	Upoznati učenike s nasljeđivanjem NTFS dozvola unutar Windows operacijskog sustava kroz Powershell sučelje.

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

Preduvjeti : Računalo/Virtualni stroj sa instaliranim Windows operacijskim sustavom minimalne verzije 10.

Pomoć : Powershell naredba se zove cmdlet, i uvijek se nosi u kombinaciji Glagol-Imenica (točno tim redoslijedom). Npr. , Get-Help je naredba koja poziva pomoć za ostale cmdletove. Dio sa glagolom uglavnom govori koja će se radnja izvršiti : Get (čitaj), Set (zapiši), Remove (obriši) itd. Dio sa imenom označava na kojem dijelu sustava će se izvršiti radnja.

Više o Powershell glagolima:

https://learn.microsoft.com/en-us/powershell/scripting/developer/cmdlet/approved-verbs-for-windows-powershell-commands?view=powershell-7.4

Napomena : Riječi unutar navodnika u terminal unosite bez navodnika. Koristite naredbe Get-Help i Get-Command za snalaženje sa cmdletima u vježbi.

Zadaci:

Pretpostavka je da već postoje korisnici Korisnik1, Korisnik2 i Korisnik3 , te stvorena struktura direktorija iz prethodne vježbe.

1. Pokrenite virtualni stroj sa Windows operacijskim sustavom koji ste prethodno instalirali. Preko Start izbornika otvorite PowerShell (koristite opciju kao administrator).

2. Koristeći Powershell, u direktoriju G:\NTFS_Pristup stvori direktorije Share i ShareCLI. Stvoriti korisnike ShareUser01 i ShareUser02.

3. U Share stvori poddirektorije: Data1, Data2, Data3.

4. U ShareCLI stvori poddirektorije: Logs, Projects, Secrets.

5. U Data1 stvori 3 testne tekstualne datoteke: doc1.txt, doc2.txt, doc3.txt.

6. U Projects stvori datoteku plan.txt s tekstom po želji.

7. Proučiti naredbe u Powershellu Get-Acl i Set-Acl, čemu služe i kako se koriste.

8. Koristeći Powershell, provjeri postojeće dozvole za direktorij Share. Ponoviti naredbu, no ovaj put prikazati rezultate kao Format-List.

9. Onemogući nasljeđivanje za direktorij Share, ali zadrži postojeće dozvole.

10. Koristeći Powershell, spremiti postojeće zapise NTFS dozvola u varijablu $acl. Prikazati sadržaj varijable na zaslonu. Ponoviti naredbu, no ovaj put prikazati rezultate kao Format-List. Koja su sve polja prikazana i koja su značenja (Path, Owner...) ?

    Ponoviti naredbu, no ovaj put prikazati samo detalje Access polja ($acl.Access). Što se može uočiti? Što označava IdentityReference polje ?

11. Koristeći Powershell, dodijeli Korisnik1 dozvolu FullControl nad Data1.

    Primjer sa objašnjenjima:

    #Definicija novog pravila. Potrebno je stvoriti novi objekt u kojem se minimalno mora definirati korisnik/grupa na koga će se primijeniti pravilo, razina pravila(read,modify...) i dozvola ili zabrana (Allow ili Deny). "DOMAIN\USER" je potrebno definirati kao IME_RACUNALA\IME_KORISNIKA.

    $new_rule = New-Object \
    System.Security.AccessControl.FileSystemAccessRule("DOMAIN\USER", "Read", "Allow")

#Spremanje postojećih zapisa NTFS dozvola u varijablu

$acl = Get-Acl -Path "\FolderOrFilePath"

#Unos novog pravila u postojeći popis

$acl.SetAccessRule($new_rule)

#Primjena izmijenjenog popisa na objekt

```
Set-Acl -Path  "\FolderOrFilePath" -AclObject $acl
```

12. Koristeći Powershell, dodijeli Korisnik2 dozvolu ReadAndExecute nad Data2. Prijaviti se kao Korisnik2 i provjeriti imate li pravo stvaranja novih datoteka u direktoriju.

13. Koristeći Powershell, zabrani Korisnik3 pravo Write nad Data3. (Hint: Deny). Prijaviti se kao Korisnik3 i provjeriti imate li pravo stvaranja novih datoteka u direktoriju. Zašto je prethodno Korisnik2 imao pravo, iako je imao samo Read only ovlasti?

14. Koristeći Powershell, ukloni sve NTFS dozvole za Data3 osim onih koje pripadaju grupi Administrators. Saznati što predstavlja oznaka "$_" (bez navodnika) .

Primjer sa objašnjenjima:

```
# Spremanje postojećih zapisa NTFS dozvola u varijablu
 $acl = Get-Acl .\Share\
```

Ispis samo objekata unutar Access polja, a koji ne sadržavaju "BUILTIN\Administrators" vrijednost. Ispis u obliku liste, umjesto oblika tablice

```
$acl.Access | Where-Object { $_.IdentityReference -ne "BUILTIN\Administrators" } | Format-List
```

NAPOMENA: PRIMIJETITI "IdentityReference" unutar skripte, prisjetiti se što predstavlja

#Jednaka funkcionalnost kao u prethodnom primjeru, ali ovaj put se koristi "if" funkcija, koja nam omogućava i korištenje dodatne logike, kao što će biti prikazano u slijedećem primjeru. Sve se može unijeti u jednoj liniji, ovako je prikazano radi lakšeg čitanja.

```
$acl.Access | ForEach-Object {
  if ($_.IdentityReference -ne "BUILTIN\Administrators") {
     $_ | Format-List
     }
  }
```

#Sličan primjer, no ovaj put se umjesto ispisa svih korisnika/grupa, na svakog od njih primjenjuje logika brisanja iz popisa pravila.

```
$acl.Access | ForEach-Object {
if ($_.IdentityReference -ne "BUILTIN\Administrators") {
    $acl.RemoveAccessRule($_)
   }
}
```

NAPOMENA: Proučiti https://learn.microsoft.com/en/us/dotnet/api/system.security.accesscontrol.filesystemsecurity.removeaccessrule?view=net-9.0

#Na kraju, potrebno je unijeti novi popis pravila za navedenu datoteku/direktorij.

Set-Acl -Path "\FolderOrFilePath" -AclObject $acl

15. Koristeći Powershell, dodaj grupu Users s dozvolom Read za cijeli direktorij Share.

16. Promijeni vlasništvo nad direktorijem Projects na korisnika ShareUser1. Potrebno je u zasebne varijable spremiti putanju direktorija, ispis NTFS dozvola tog direktorija (npr. $acl), i korisnika (kao posebnu vrstu objekta), te koristeći posebnu funkciju SetOwner() primijeniti na $acl varijablu (primjer $acl.SetOwner(NoviVlasnik)). Primijeniti nova pravila u $acl varijabli na direktorij. Provjeriti i potvrditi da je vlasnik promijenjen.

17. U direktoriju Secrets onemogući nasljeđivanje i izbriši sve naslijeđene dozvole. Koristi se SetAccessRuleProtection() metoda na način kao i u prethodnim primjerima.

NAPOMENA: Proučiti https://learn.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.objectsecurity.setaccessruleprotection?view=net-9.0#system-security-accesscontrol-objectsecurity-setaccessruleprotection(system-boolean-system-boolean)

18. Koristeći Powershell, dodaj ShareUser2 dozvolu Modify za direktorij Secrets.

19. Koristeći Powershell, postavi eksplicitnu zabranu pristupa za Korisnik3 na datoteku plan.txt.

20. Provjeri efektivne dozvole za Korisnik2 nad Data2 pomoću alata za analizu prava (Effective Access).

21. Postavi direktorij Logs tako da "Full Control" dozvole ima isključivo grupa Administrators.

22. Uključi opciju "Replace all child object permissions..." za direktorij ShareCLI.

23. Korištenjem grafičkog sučelja (GUI), postavi Advanced Sharing za direktorij Share. Za grupu Everyone postavi Read ovlasti. Pristupiti direktoriju preko mreže kao korisnici Korisnik01, Korisnik02 i zatim kao Korisnik03. Zapisati koje su maksimalne ovlasti za svakog korisnika.

24. Promijeniti share ovlasti za grupu Everyone na Full Control, te ponoviti proces mrežnog pristupa direktoriju za svakog od korisnika i zapisati koje sad ovlasti imaju. Zašto? Potražiti na internetu kako se računaju Share ovlasti i NTFS ovlasti prilikom mrežnog pristupa direktoriju.

25. Korištenjem PowerShell-a, stvori novi share CLISHARE za direktorij ShareCLI (New-SmbShare). Korisnici trebaju imati slijedeće Share ovlasti:

    ShareUser1 → Read

    ShareUser2 → Full

26. Provjeri sve postojeće dijeljene mape pomoću PowerShell-a (Hint: Get-SmbShare).

27. Provjeri prava pristupa za CLISHARE pomoću Powershell-a. (Hint: Get-SmbShareAccess).

28. Korištenjem Powershell-a, promijeni prava za CLISHARE tako da Korisnik1 ima pristup Change. (Hint: Grant-SmbShareAccess)

29. Ukloni ShareUser2 s liste korisnika s pristupom na CLISHARE. (Hint: Revoke-SmbShareAccess)

30. Prijavi se kao Korisnik1 i pokušaj otvoriti doc1.txt. Zabilježi rezultat.

31. Prijavi se kao Korisnik3 i pokušaj stvoriti novu datoteku u Data3. Što se dogodilo?

32. Generiraj tekstualni izvještaj svih NTFS dozvola za direktorije Share i ShareCLI i eksportaj ga u .txt datoteku.