

Ćwiczenia: Zaawansowane uprawnienia w systemie plików NTFS (**Wiersz polecenia**)

Cel Ogólny Lekcji: Naucz uczniów zaawansowanych technik zarządzania uprawnieniami plików i folderów w systemie plików NTFS w systemie Windows za pomocą wiersza poleceń. Uczniowie zdobędą praktyczną wiedzę i umiejętności w zakresie nadawania, usuwania i modyfikowania uprawnień dostępu do plików i katalogów, zarządzania atrybutami plików oraz zmiany właściciela plików i folderów.

Cele Szczegółowe:

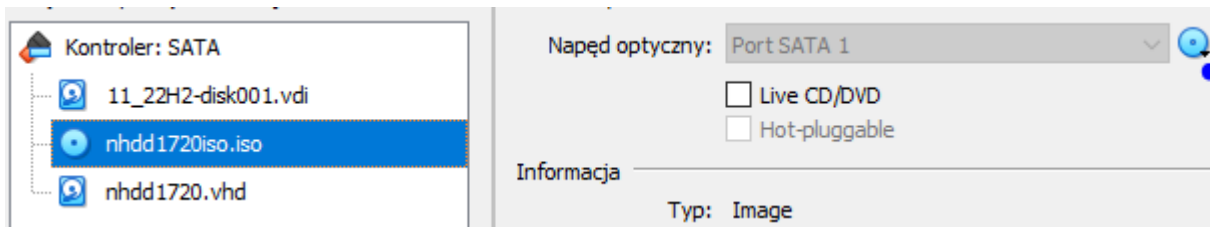
- Uczniowie nauczą się używać podstawowych poleceń systemu Windows do zarządzania plikami i katalogami za pomocą wiersza poleceń, takich jak **icacls**, **attrib**, i **takeown**.
- Uczniowie zrozumieją składnię i działanie tych poleceń oraz będą wiedzieli, jakie opcje i przełączniki można z nimi używać.
- Uczniowie dowiedzą się, jak nadawać, usuwać i modyfikować uprawnienia dostępu do plików i katalogów, zarówno dla pojedynczych użytkowników, jak i rekursywnie dla katalogów i ich zawartości.
- Uczniowie zdobędą umiejętność zmiany atrybutów plików, takich jak atrybuty ukrycia.
- Uczniowie nauczą się, jak zmieniać właściciela plików i folderów.
- Uczniowie będą mieli okazję wykonać praktyczne ćwiczenia, które pomogą im zrozumieć i zapamiętać omawiane techniki zarządzania uprawnieniami.

Dzięki tym cele szczegółowym uczniowie będą mogli skutecznie zarządzać uprawnieniami dostępu do plików i katalogów w systemie Windows, co jest istotne w kontekście zarządzania danymi i bezpieczeństwa systemu operacyjnego.

Zalecam wykonanie ćwiczenia na dysku z poprzedniego ćwiczenia, w takim przypadku **wykonuj ćwiczenie od pkt 5**. Czynności wykonuj według podanej w zadaniu kolejności, jeżeli wykonasz dowolną czynność poza kolejnością pobierz nową maszynę wirtualną (migawkę) i wykonaj ćwiczenie od początku.

Wykonaj polecenia, umieść notatkę w zeszycie dokumentującą wykonanie poleceń.

1. W folderze z materiałami znajduje się plik **nhdd1720.zip** należy go pobrać i rozpakować do przygotowanego wcześniej folderu z maszyną wirtualną a następnie **nhdd1720.vhd** podłą jako drugi dysk do maszyny wirtualnej.
2. W folderze z materiałami znajduje się plik **nhdd1720iso.zip** należy go pobrać i rozpakować do przygotowanego wcześniej folderu z maszyną wirtualną
3. Plik **nhdd1720.iso** należy podłączyć do maszyny wirtualnej jako napęd optyczny.



4. Zaloguj się do konta **admin** z hasłem **zaq1@WSX**
5. Z napędu optycznego lub w maszynie wirtualnej z strony z materiałami przekopiuj plik **z21.exe** na pulpit maszyny wirtualnej.
6. Uruchom **z21.exe** jako Administrator
7. Kolejno zaloguj się do kont:
 - **admin**
 - **User_adv1** bez hasła
 - **User_adv2** bez hasła
 - **User** bez hasła
8. Zaloguj się do konta **admin**
9. Z napędu optycznego lub w maszynie wirtualnej z strony z materiałami przekopiuj plik **z212.exe** na pulpit maszyny wirtualnej.
10. Uruchom **z212.exe** jako Administrator

Poniższe zadanie wykonaj stosując tylko polecenia „wiersza polecenia” korzystając z **pomocy** dostępnej po wywołaniu:

attrib /? - do zmiany atrybutów plików i folderów, takich jak ukryty, tylko do odczytu, systemowy itp...

Atrybuty określają, czy plik lub folder jest widoczny, ukryty, chroniony przed zapisem, itp. Składnia polecenia attrib jest następująca:

ATTRIB [+attrib | -attrib] [dysk:] [katalog] [plik] [/S [/D]] [/L]

Możesz użyć znaków + lub - do dodawania lub usuwania atrybutów. Dostępne atrybuty podstawowe to:

R = Tylko do odczytu (Read-only)

A = Gotowy do archiwizacji (Archive)

S = Plik systemowy (System)

H = Plik ukryty (Hidden)

I = Plik nieindeksowalny (Not content-indexed)

Możesz też użyć opcji /S, /D lub /L do zastosowania polecenia do podfolderów, folderów lub linków symbolicznych.

Przykłady użycia polecenia attrib:

Aby wyświetlić atrybuty pliku lub folderu, wpisz attrib i ścieżkę do pliku lub folderu.

Na przykład: `attrib C:\Windows\System32\cmd.exe`

Aby dodać atrybut do pliku lub folderu, wpisz attrib i znak plus (+) oraz literę reprezentującą atrybut, a następnie ścieżkę do pliku lub folderu. Na przykład: `attrib +R C:\MojeDokumenty\ważny.txt` - to doda atrybut tylko do odczytu do pliku ważny.txt.

Aby zastosować polecenie attrib do wszystkich plików i folderów w danym katalogu i jego podkatalogach, użyj przełącznika /S. Na przykład: `attrib +A C:\MojeDokumenty\* /S` - to doda atrybut archiwum do wszystkich plików i folderów w katalogu MojeDokumenty i jego podkatalogach.

Aby zastosować polecenie attrib również do samych folderów, a nie tylko do plików w nich zawartych, użyj przełącznika /D. Na przykład: `attrib +S C:\MojeDokumenty\ /S /D` - to doda atrybut systemowy do katalogu MojeDokumenty i wszystkich plików i folderów w nim zawartych.

takeown /? - do przejmowania własności plików i folderów. Aby użyć tego polecenia, musisz mieć uprawnienie Przejęcie na własność lub Przywracaj pliki i katalogi.

Składnia polecenia takeown jest następująca:

TAKEOWN [/S system [/U użytkownik [/P [hasło]]]]

/F nazwa_pliku [/A] [/R [/D {Y|N}]]

Oto znaczenie poszczególnych parametrów:

/S system - określa zdalny system, na którym chcesz zmienić własność pliku lub folderu.

/U użytkownik - określa nazwę użytkownika zdalnego systemu.

/P [hasło] - określa hasło użytkownika zdalnego systemu. Jeśli hasło nie zostanie podane, zostanie wyświetlone monit o hasło.

/F nazwa_pliku - określa nazwę pliku lub folderu, który chcesz przejąć na własność. Możesz użyć znaków wieloznacznych * i ?, aby dopasować wiele plików.

/A - nadaje prawo własności grupie Administratorzy zamiast bieżącemu użytkownikowi.

/R - zmienia własność rekursywnie wszystkich podfolderów i plików.

/D {Y|N} - określa, czy chcesz przejąć na własność plików lub folderów, do których nie masz dostępu.

Y oznacza tak, a N oznacza nie. Domyślnie jest to N.

Przykłady użycia polecenia takeown.exe:

1. `takeown /F C:\Windows\System32\calc.exe` - staje się właścicielem pliku calc.exe w folderze System32.
2. `takeown /F C:\Windows /R /D Y` - staje się właścicielem wszystkich plików i folderów w folderze Windows i podfolderach, ignorując błędy dostępu.
3. `takeown /F "C:\Moje dokumenty" /A` - nadaje prawo własności grupie Administratorzy dla folderu Moje dokumenty.

icacls /? - (Integral Controller Access Control List) jest używane w systemach Windows do wyświetlania i modyfikowania list kontroli dostępu (ACL) plików i folderów. Pozwala na zarządzanie uprawnieniami dostępu, ustawianie właściciela pliku oraz zarządzanie dziedziczeniem uprawnień.

Polecenie icacls ma następującą składnię:

`icacls nazwa_pliku [opcje] [/T] [/C] [/L] [/Q]`

Gdzie:

- nazwa_pliku to nazwa pliku lub katalogu, dla którego chcemy wyświetlić lub zmienić ACL.
- opcje to parametry określające, jakie operacje chcemy wykonać na ACL, takie jak dodawanie, usuwanie, zmiana lub przywracanie uprawnień.
- /T to przełącznik, który powoduje przetwarzanie wszystkich podkatalogów i plików w podanym katalogu.
- /C to przełącznik, który powoduje kontynuowanie operacji nawet w przypadku wystąpienia błędów.
- /L to przełącznik, który powoduje operowanie na łączach symbolicznych zamiast na ich docelowych plikach.
- /Q to przełącznik, który powoduje wykonywanie operacji w trybie cichym, bez wyświetlania żadnych komunikatów.

Przykłady użycia icacls:

1. Wyświetlenie uprawnień dla pliku lub folderu: `icacls ścieżka_do_pliku`
2. Nadanie uprawnień użytkownikowi: `icacls ścieżka_do_pliku /grant użytkownik:(uprawnienia)`
3. Usunięcie uprawnień użytkownika: `icacls ścieżka_do_pliku /remove użytkownik`

4. Resetowanie uprawnień do stanu domyślnego: `icacls ścieżka_do_pliku /reset`

Pamiętaj, że zmiana uprawnień może wpłynąć na dostęp do plików i folderów, więc należy używać icacls ostrożnie.

Zadanie 1

Wykonaj polecenia, umieść notatkę w zeszycie dokumentujące wykonanie poleceń.

Wykonaj następujące wymagania:

1. Użytkownik **User** nie będzie miał dostępu do pliku test.txt który jest w folderze C:\Users\Public\Desktop\dod

```
icacls C:\Users\Public\Desktop\dod\test.txt /deny User:(F)
```

Wyjaśnienie użytej komendy:

- "icacls" to nazwa polecenia.
- "C:\Users\Public\Desktop\dod\test.txt" to ścieżka do pliku "test.txt" w katalogu "C:\Users\Public\Desktop\dod". To jest ścieżka do pliku, dla którego chcemy zmodyfikować uprawnienia.
- "/deny" oznacza, że będziemy negować (odmawiać) określone uprawnienia. W tym przypadku, zostaną odmówione uprawnienia.
- "User:(F)" to określenie, które użytkownika lub grupę użytkowników chcemy wybrać, aby nałożyć ograniczenia. "(F)" wskazuje na pełne (Full) uprawnienia, które zostaną odmówione. Oznacza to, że użytkownik lub grupa "User" zostanie zablokowana przed uzyskaniem pełnego dostępu do pliku "test.txt".

(zgłoszenie) 1

2. Na pulpicie konta **User** nie będzie widocznego pliku test.txt który jest w folderze C:\Users\Public\Desktop\dod

```
attrib +h C:\Users\Public\Desktop\dod\test.txt
```

Wyjaśnienie użytej komendy:

- "attrib" to nazwa polecenia, które służy do zarządzania atrybutami plików.
- "+h" oznacza, że chcemy dodać atrybut "h" do pliku. Atrybut "h" oznacza ukrycie pliku. Kiedy plik ma ustawiony ten atrybut, nie będzie widoczny w standardowym widoku eksploratora plików, chyba że zostaną wybrane opcje pokazywania ukrytych plików.
- "C:\Users\Public\Desktop\dod\test.txt" to pełna ścieżka do pliku, któremu chcemy nadać atrybut ukrycia. Po zastosowaniu tego polecenia, plik "test.txt" na dysku C:\Users\Public\Desktop\dod będzie ukryty.

(zgłoszenie) 2

3. Na pulpicie kont **User_adv1** i **User_adv2** będzie widoczny plik test.txt który jest w folderze C:\Users\Public\Desktop\dod

```
icaccls C:\Users\Public\Desktop\dod\test.txt /grant User_adv1:(F) User_adv2:(F)
```

Wyjaśnienie użytej komendy:

- "icaccls" to nazwa polecenia.
- "C:\Users\Public\Desktop\dod\test.txt" to pełna ścieżka do pliku "test.txt" w katalogu "C:\Users\Public\Desktop\dod". To jest ścieżka do pliku, dla którego chcemy zmienić uprawnienia.
- "/grant" wskazuje, że będziemy nadawać uprawnienia użytkownikom.
- "User_adv1:(F)" oznacza, że użytkownik "User_adv1" otrzyma pełne uprawnienia ("F") do pliku "test.txt". Pełne uprawnienia pozwalają na odczytywanie, zapisywanie, modyfikowanie i usuwanie pliku.
- "User_adv2:(F)" oznacza, że użytkownik "User_adv2" również otrzyma pełne uprawnienia ("F") do pliku "test.txt".

(zgłoszenie) 3

4. W **C:** foldery **F1** i **P1** nie będą widoczne dla użytkownika konta **User**.

```
icaccls C:\F1 /deny User:(F)
```

```
icaccls C:\P1 /deny User:(F)
```

- Polecenie "**icacls**" jest używane do zarządzania kontrolą dostępu do określonych plików lub katalogów.
- **C:\F1** lub **C:\P1** to ścieżka do katalogu lub pliku, dla którego chcemy zastosować zmiany w uprawnieniach.
- **/deny** oznacza, że będziemy odmawiać (blokować) określone uprawnienia.
- **User** wskazuje na użytkownika, któremu będą blokowane uprawnienia. W tym przypadku jest to użytkownik o nazwie "User".
- **(F)** oznacza pełne (Full) uprawnienia, które zostaną zablokowane dla użytkownika "User". To oznacza, że użytkownik "User" nie będzie miał dostępu do pliku lub katalogu "C:\F1" w żadnym zakresie, w tym odczyt, zapis, modyfikacje itp.

(zgłoszenie) 4

5. Do pliku **test3.txt** który jest w folderze **F1** pełny dostęp będą mieli tylko użytkownicy kont:

- **User_adv1**
- **User_adv2**

takeown /f C:\F1\test3.txt

icacls C:\F1\test3.txt /grant User_adv1:(F) User_adv2:(F)

- Polecenie "takeown" służy do zmiany właściciela pliku lub katalogu w systemie Windows. W tym przypadku próbujemy zmienić właściciela pliku "test3.txt" znajdującego się w katalogu "C:\F1".
- **/f C:\F1\test3.txt** wskazuje, że chcemy zmienić właściciela pliku "test3.txt". To oznacza, że zostanie zmieniony właściciel pliku na użytkownika, który wykonuje to polecenie. W wyniku tego polecenia użytkownik staje się właścicielem pliku "test3.txt" i uzyskuje pewne dodatkowe uprawnienia do zarządzania tym plikiem.
- Polecenie "icacls" jest używane do zarządzania kontrolą dostępu do plików i katalogów w systemie Windows.
- **C:\F1\test3.txt** to ścieżka do pliku "test3.txt" w katalogu "C:\F1".
- **/grant** wskazuje, że będziemy nadawać uprawnienia użytkownikom.

- **User_adv1:(F)** oznacza, że użytkownik "User_adv1" otrzymuje pełne uprawnienia (Full) do pliku "test3.txt". To obejmuje prawa do odczytu, zapisu, modyfikacji i usuwania pliku.
- **User_adv2:(F)** oznacza, że użytkownik "User_adv2" również otrzymuje pełne uprawnienia (Full) do pliku "test3.txt".

(zgłoszenie) 5

6. Do folderu **P1** i zawartości (poza plikiem dane.xls) **pełny dostęp** będą mieli tylko użytkownicy kont:

- **User_adv1**
- **User_adv2**

takeown /f C:\P1 /r /d y

icacls C:\P1 /grant User_adv1:(F) User_adv2:(F) /t

- Polecenie "takeown" jest używane do zmiany właściciela pliku lub katalogu w systemie Windows. W tym przypadku próbujemy zmienić właściciela katalogu "C:\P1" oraz wszystkich jego podkatalogów i plików, dlatego używamy opcji "/r" (rekursywnie).
- **/f C:\P1** wskazuje, że chcemy zmienić właściciela katalogu "C:\P1" i jego zawartości.
- **/r** oznacza, że zmiany w właścicielu mają być stosowane rekursywnie, czyli dla wszystkich plików i podkatalogów wewnątrz "C:\P1".
- **/d y** wskazuje, że należy potwierdzić pytania dotyczące zmiany właściciela "tak" (yes) automatycznie. W przeciwnym razie, system Windows może pytać użytkownika, czy chce zmienić właściciela dla każdego pliku i katalogu.
- Polecenie "icacls" jest używane do zarządzania kontrolą dostępu do plików i katalogów w systemie Windows.
- **C:\P1** to ścieżka do katalogu "C:\P1".
- **/grant** wskazuje, że będziemy nadawać uprawnienia użytkownikom.
- **User_adv1:(F)** oznacza, że użytkownik "User_adv1" otrzymuje pełne uprawnienia (Full) do katalogu "C:\P1". To obejmuje prawa do odczytu, zapisu, modyfikacji i usuwania zawartości tego katalogu.
- **User_adv2:(F)** oznacza, że użytkownik "User_adv2" również otrzymuje pełne uprawnienia (Full) do

katalogu "C:\P1".

- /t oznacza, że zmiany w uprawnieniach będą stosowane rekursywnie dla katalogu "C:\P1" i wszystkich jego podkatalogów i plików.

(zgłoszenie) 6

7. Do pliku dane.xls który jest w C:\P1 użytkownik konta **User_adv2** nie będzie miał dostępu.

```
icacls C:\P1\dane.xls /deny User_adv2:(F)
```

Wyjaśnienie tego polecenia:

- "icacls" to narzędzie w systemie Windows służące do zarządzania uprawnieniami dostępu do plików i katalogów poprzez listy kontroli dostępu (ACLs).
- "C:\P1\dane.xls" to pełna ścieżka do pliku, dla którego chcemy zmodyfikować uprawnienia. W tym przypadku jest to plik "dane.xls" w katalogu "C:\P1".
- "/deny" oznacza, że będziemy negować (blokować) określone uprawnienia. Innymi słowy, chcemy odmówić dostępu do tego pliku.
- "User_adv2" to użytkownik, któremu będziemy blokować dostęp do pliku "dane.xls". "(F)" oznacza pełne (Full) uprawnienia, które zostaną zablokowane. To oznacza, że użytkownik "User_adv2" nie będzie miał dostępu do pliku "dane.xls" w żadnym zakresie, w tym odczyt, zapis, modyfikacje i usuwanie pliku.

(zgłoszenie) 7

8. Do pliku dane.xls który jest w C:\P1 pełny dostęp będzie miał tylko użytkownik konta **User_adv1**.

```
icacls C:\P1\dane.xls /grant User_adv1:(F)
```

Wyjaśnienie tego polecenia:

- "icacls" to narzędzie w systemie Windows, które służy do zarządzania uprawnieniami dostępu do plików i katalogów poprzez listy kontroli dostępu (ACLs).
- "C:\P1\dane.xls" to pełna ścieżka do pliku, dla którego chcemy zmienić uprawnienia. W tym przypadku jest to plik "dane.xls" w katalogu "C:\P1".

- "/"grant" wskazuje, że będziemy nadawać (dodawać) określone uprawnienia użytkownikowi.
- "User_adv1" to użytkownik, któremu nadajemy uprawnienia. "(F)" oznacza pełne (Full) uprawnienia, które zostaną przydzielone użytkownikowi "User_adv1". Pełne uprawnienia obejmują prawo do odczytu, zapisu, modyfikacji i usuwania pliku.

(zgłoszenie) 8

9. Do pliku `test2.txt` który jest w folderze `C:\praca` użytkownika konta **User** będzie mógł zapisywać dane, ale nie będzie mógł ich usunąć.

```
icacls C:\praca\test2.txt /grant User:(W,WDAC)
```

Wyjaśnienie tego polecenia:

- "icacls" to narzędzie w systemie Windows, które służy do zarządzania uprawnieniami dostępu do plików i katalogów za pomocą list kontroli dostępu (ACLs).
- "C:\praca\test2.txt" to pełna ścieżka do pliku, dla którego chcemy zmienić uprawnienia.
- "/"grant" wskazuje, że będziemy nadawać nowe uprawnienia użytkownikowi.
- "User" to nazwa użytkownika, któremu nadajemy uprawnienia.
- "(W,WDAC)" to zestaw uprawnień nadawanych użytkownikowi:
 - "(W)" oznacza "Zapis" (Write), co oznacza, że użytkownik będzie miał uprawnienia do zapisywania (edytowania) pliku "test2.txt". Może modyfikować zawartość pliku.
 - "(WDAC)" oznacza "Zapis do atrybutów DAC" (Write DAC, DAC to Discretionary Access Control). To oznacza, że użytkownik będzie miał uprawnienia do modyfikowania atrybutów dostępu do pliku i kontrolowania uprawnień dostępu do tego pliku.

(zgłoszenie) 9

10. Użytkownicy **User_adv1**, **User_adv2** będą mogli przeglądać pliki które są w folderze `C:\praca`.

```
icacls C:\praca /grant User_adv1:(R) User_adv2:(R) /t
```

Wyjaśnienie tego polecenia:

- "icacls" to narzędzie w systemie Windows, które służy do zarządzania uprawnieniami dostępu do plików i katalogów za pomocą list kontroli dostępu (ACLs).
- "C:\praca" to ścieżka do katalogu, dla którego chcemy nadawać nowe uprawnienia.
- "/grant" wskazuje, że będziemy nadawać nowe uprawnienia użytkownikom.
- "User_adv1" i "User_adv2" to nazwy użytkowników, którym nadajemy uprawnienia.
- "(R)" oznacza "Odczyt" (Read), co oznacza, że użytkownicy "User_adv1" i "User_adv2" otrzymują uprawnienia do odczytu plików w katalogu "C:\praca". Mogą przeglądać zawartość plików, ale nie mają uprawnień do zapisu, modyfikacji lub usuwania tych plików.
- "/t" oznacza, że zmiany uprawnień zostaną zastosowane rekursywnie dla katalogu "C:\praca" i wszystkich jego podkatalogów oraz plików. To oznacza, że nadane uprawnienia do odczytu ("R") będą obowiązywać dla całej struktury katalogu "C:\praca".

(zgłoszenie) 10

Zapisz w zeszycie następujące wnioski po wykonaniu tego zadania:

Na podstawie wykonanych zadań i ćwiczeń związanych z zaawansowanymi uprawnieniami w systemie plików NTFS w systemie Windows, uczniowie mogą wyciągnąć następujące wnioski:

1. System plików NTFS oferuje zaawansowane i elastyczne mechanizmy kontroli dostępu do plików i katalogów, co umożliwia dokładne zarządzanie, które użytkownicy mają dostęp do jakich zasobów.
2. Polecenie **icacls** - można nadawać, usuwać, modyfikować i blokować uprawnienia dostępu do plików i katalogów za pomocą tego narzędzia.
3. Rekursywne stosowanie uprawnień jest istotne w przypadku katalogów zawierających wiele plików i podkatalogów. Dzięki opcji **/t** w poleceniu **icacls**, zmiany w uprawnieniach można zastosować do całej struktury katalogu.
4. Polecenie **attrib** pozwala na zmianę atrybutów plików, takich jak ukrycie. To może być przydatne do zachowania prywatności i bezpieczeństwa plików.
5. Polecenie **takeown** umożliwia zmianę właściciela plików i folderów. Uczniowie zrozumieją, że zmiana właściciela może wpływać na kontrolę nad plikami.
6. Zastosowanie polecenia **/deny** w **icacls** pozwala na blokowanie określonych uprawnień dostępu dla określonych użytkowników lub grup. To jest ważne narzędzie do implementacji polityk bezpieczeństwa.
7. Zarządzanie uprawnieniami jest kluczowym aspektem bezpieczeństwa systemu operacyjnego, a niepoprawne ustawienia uprawnień mogą prowadzić do potencjalnych zagrożeń.

8. Dobre praktyki zarządzania uprawnieniami obejmują zasady "zasad najmniejszych przywilejów" (least privilege) i dokładne monitorowanie, kto ma dostęp do jakich zasobów.

9. Wdrażanie zaawansowanych uprawnień i atrybutów plików jest istotne w środowiskach korporacyjnych i systemach, gdzie kontrola dostępu jest kluczowa.

Wnioski te pomogą zrozumieć znaczenie i praktyczne zastosowanie zarządzania uprawnieniami w systemie Windows oraz przyczynią się do zwiększenia świadomości w zakresie bezpieczeństwa danych i zasobów.

(zgłoszenie) 11

Przywróć pierwszą migawkę.

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.