

Bezpieczeństwo systemów rozproszonych

SPRAWOZDANIE Z ĆWICZENIA: Windows NTFS cz. I

Imię Nazwisko: nr albumu:

data ćwiczenia: godzina:

1. System plików NTFS

1.1 Prawa dostępu – ACL



Zadania:

1. Zaloguj się na konto Administratora.
2. Utwórz katalog C:\Public, a w nim plik Test.txt.
Sprawdź, które konta znajdują się na liście ACL tego pliku.
3. Korzystając z prostych ACL nadaj uprawnienia do *odczytu* dla użytkownika Sherlock Holmes.
Sprawdź uprawnienia rozszerzonych ACL ustawione dla tego użytkownika.
4. Uruchom Notatnik jako Sherlock Holmes i zweryfikuj, czy może on skorzystać z dostępu do Test.txt:
dostęp do odczytu: dostęp do zapisu:
5. Sprawdź efektywne uprawnienia („czynny dostęp”) użytkownika Sherlock Holmes do Test.txt.
Skąd się wzięło prawo zapisu? Wskaż podmiot i pierwotny obiekt, do którego nadano to prawo:

podmiot:

pierwotny obiekt:

6. Korzystając z prostych ACL odmów użytkownikowi Sherlock Holmes uprawnienia do *zapisu*.
– jak operacja odmowy zmieniła efektywne uprawnienia użytkownika?

- zweryfikuj dostęp z programu Notatnik:

dostęp do odczytu:

dostęp do zapisu:

7. Utwórz plik Test2.txt. Korzystając z narzędzia `icacls`, wyświetl prawa dostępu do obu plików `txt`. Zapisz odpowiednie polecenie:

8. Posługując się tym samym narzędziem, nadaj użytkownikowi Sherlock Holmes uprawnienie *odczytu* do obu plików `txt`. Zapisz odpowiednie polecenie:

- sprawdź, jakie uprawnienia są prezentowane we właściwościach pliku `Test2.txt` w Eksploratorze Windows.

9. Poleceniem `icacls` dodaj użytkownikowi Sherlock Holmes uprawnienie *modyfikacji* (nie *zapisu*) do obu plików. Co obserwujesz w oknie Właściwości/Zabezpieczenia?

10. W oknie Właściwości/Zabezpieczenia pliku `Test2.txt` usuń zezwolenie *odczyt i wykonanie*. Co zobaczysz poleceniem `icacls`?

11. Spróbuj skopiować uprawnienia (całą listę ACL) pliku `Test2.txt` do ACL pliku `Test.txt`, posługując się `icacls`. Zapisz końcowe polecenie, które spowodowało nadanie tych uprawnień do `Test.txt`.

12. Ostatecznie usuń użytkownika Sherlock Holmes z list ACL dla obu plików poleceniem:

13. Czy istnieje możliwość stworzenia pliku lub podkatalogu (i manipulacji ACL), którego właściciel katalogu nadrzędnego nie będzie mógł skasować?

plik:

podkatalog:

Jeśli masz jakiś komentarz możesz go zapisać:

1.2 Mechanizm *Bypass Traverse Checking*

14. W katalogu C:\Public utwórz nowy plik o nazwie Test3.txt. Wyłącz dla tego pliku dziedziczenie uprawnień, konwertując uprawnienia dziedziczone na jawne. Sprawdź jakie efektywne uprawnienia do pliku posiada James Bond.
15. Dla katalogu C:\Public, korzystając z prostych ACL odmów użytkownikowi James Bond wszelkich uprawnień.
16. Uruchom Notatnik jako James Bond. Spróbuj otworzyć plik Test3.txt nawigując do jego lokalizacji. Czy próba otwarcia zakończyła się powodzeniem?
17. Nadal w programie Notatnik, spróbuj otworzyć plik Test3.txt podając pełną ścieżkę dostępu do niego. Czy ta próba otwarcia zakończyła się powodzeniem?
18. Jak jest rola przywileju *Bypass Traverse Checking* (SeChangeNotifyPrivilege)?

1.3 Inspekcja dostępu do plików przez aktywne procesy

19. Użyj programu handle, by uzyskać listę otwartych plików w systemie. Zaobserwuj różnicę w działaniu programu uruchomionego z normalnymi uprawnieniami i z pełnym tokenem administracyjnym.
20. Wykorzystaj program handle, by znaleźć procesy, które aktualnie korzystają z pliku kernel32.dll. Zapisz polecenie:

21. Sporządź listę plików otwartych przez Notatnik poleceniem:

22. Sporządź listę plików z katalogu Program Files otwartych przez program explorer poleceniem:

1.4 Inspekcja dostępu do plików w systemowym dzienniku zdarzeń

23. Dla pliku Test.txt włącz rejestrowanie modyfikacji jego zawartości w dzienniku zdarzeń.
24. Prześledź zdarzenia zarejestrowane przez system w związku z pojedynczym dostępem do tego pliku. Sprawdź do jakiej kategorii zdarzeń system Windows je zalicza? Jak dokładnie zdarzenia zostały zarejestrowane? Ile ich jest?
25. Sprawdź jak w aplikacji Podgląd zdarzeń uzyskać listę tylko wybranych zdarzeń.