Bezpieczeństwo systemów rozproszonych

SPRAWOZDANIE Z ĆWICZENIA: Windows NTFS cz. II

Imię Nazwisko: Dariusz Max Adamski nr albumu: 136674

data ćwiczenia: 15.12.2020 godzina: 15:10

1. System plików NTFS

1.1 Szyfrowanie – EFS

1. Zaloguj się na konto Administratora. Utwórz w katalogu C:\Public plik tekstowy Tajne.txt o dowolnej treści. Wyświetl jego zawartość przy pomocy Eksploratora oraz w konsoli tekstowej (np. poleceniem `type`).
2. Następnie zaszyfruj ten plik i spróbuj ponownie wyświetlić jego zawartość.

   Udało się? TAK

   Czy była wymagana jakaś interwencja użytkownika przy dostępie do zaszyfrowanego pliku (np. podanie hasła, wskazanie klucza itp.)? TAK / NIE
   NIE
3. Wyświetl informacje o zaszyfrowanym pliku poleceniem `cipher /c`.
   Jakim algorytmem zaszyfrowano zawartość pliku?

   AES256

   Kto może deszyfrować ten plik?

   Administrator
4. Odszukaj certyfikat EFS klucza użytkownika.
   Do czego dokładnie jest ten klucz używany (podczas szyfrowania lub deszyfrowania pliku)?

   Do szyfrowania pliku jest uzywany jednorazowy klucz FEK. Ten klucz jest szyfrowany kluczem publicznym z certyfikatu EPS, a nastepnie umieszczony jest w naglowku zaszyfrowanego pliku.

   Jak długo ważny jest certyfikat?

   Prawie 100 lat! (2020-12-01 do 2120-11-07)

   Kto jest wystawcą certyfikatu?

   Administrator

5. Jako użytkownik James Bond spróbuj wyświetlić zawartość tego pliku. Sprawdź, jak umożliwić użytkownikowi James Bond dostęp do tego pliku. Zapisz warunki konieczne jakie musi spełniać konto tego użytkownika:

   Bond musi miec wygenerowany certyfikat. Aby Bond mogl odczytac plik, admin musi we wlasciwosciach pliku -> advanced -> details, kliknac 'Add' w sekcji uzytkownikow, ktorzy maja dostep do pliku, wybrac certyfikat Bonda i zaakceptowac.

   Zweryfikuj rezultat otwierając plik oraz narzędziem cipher.

6. Co należałoby zrobić, aby uzyskać dostęp do zaszyfrowanych plików w innym systemie Windows?

   W managerze certyfikatow (certmgr) nalezy wyeksportowac odpowiedni certyfikat (trzeba zaznaczyc opcje 'export private key'). Na docelowym komputerze aby zaimportowac certyfikat, wystarczy kliknac na niego dwa razy i postepowac zgodnie z instrukcjami w okienku.

7. Przetestuj to z wybranym kontem na sąsiednim komputerze.

1.2 Agent odzyskiwania plików – DRA

8. Zaimportuj wskazane przez prowadzącego klucze DRA (∗.pfx) dla konta James Bond. Następnie wyeksportuj klucz publiczny DRA do certyfikatu umieszczonego w wybranym pliku (∗.cer).
9. Utwórz agenta DRA poprzez Narzędzia administracyjne → Zasady zabezpieczeń lokalnych → Zasady kluczy publicznych → System szyfrowania plików → menu kontekstowe: Dodaj agenta odzyskiwania danych...
   W tym celu musisz wskazać plik ∗.cer z certyfikatem klucza publicznego DRA.
10. Sprawdź narzędziem cipher czy dostęp do wcześniej zaszyfrowanych plików został automatycznie rozszerzony na agenta DRA.

    TAK

11. Z konta James Bond zweryfikuj dostęp do plików zaszyfrowanych przez innych użytkowników.

1.3 Strumienie alternatywne ADS

12. Na potrzeby dalszych ćwiczeń utwórz nowy katalog np. TestADS.
13. Wyszukaj w Internecie i pobierz do tego katalogu md5sums-1.2.zip.
14. Sprawdź, czy wraz z pobranym archiwum został zapisany jakiś strumień ADS.
15. Wypakuj pliki z archiwum. Spróbuj w Eksploratorze Windows uruchomić md5sums.exe. Zaobserwuj monit ostrzegawczy.
16. Sprawdź, czy podobny efekt uzyskasz uruchamiając ten program w konsoli tekstowej.
17. Wyświetl zawartość katalogu poleceniem dir, tak aby ukazały się strumienie ADS:

    dir /r

18. Zmień parametr `ZoneId` dla pliku md5sums.exe, tak aby monit nie był już wyświetlany.
19. Użyj polecenia streams w celu wyświetlenia strumieni ADS w bieżącym katalogu. Spróbuj tym poleceniem usunąć strumień :Zone.Identifier pliku md5sums.exe. Zaobserwuj wpływ tej operacji na przyszły monit.
20. Usuń strumień :Zone.Identifier pliku archiwum i wypakuj jego zawartość ponownie. Sprawdź obecność strumieni alternatywnych.
21. Uzyskaj skrót MD5 zawartości pliku Test.txt. Następnie za pomocą Notatnika utwórz i wyedytuj strumień alternatywny Test.txt:Tajny.txt. Po zapisaniu zmian sprawdź wpływ tej operacji na skrót pliku Test.txt.
22. Sprawdź, czy można utworzyć strumień alternatywny katalogu (np. TestADS).