

Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: Procesy w systemie MS Windows

Imię Nazwisko: nr albumu:

data ćwiczenia: godzina:

1. Zabezpieczenia procesów aplikacyjnych

1.1 Tokeny zabezpieczeń (*security tokens/access tokens*)



Aby wykonać poniższe ćwiczenia zaloguj się jako James Bond

1.1.1 Impersonation

1. Uruchom procesor poleceń (cmd) i następnie uruchom jako użytkownik Administrator program Menadżer zadań (%windir%\system32\taskmgr.exe). Zapisz poprawne polecenie:

Zweryfikuj rezultat w Menadżerze zadań.

2. Sprawdź, jak uzyskać ten sam efekt w trybie graficznym.
3. Spróbuj uruchomić nową instancję Exploratora Windows jako użytkownik Administrator.
4. Sprawdź działanie opcji /env polecenia runas, np. porównując:

```
runas /user:Administrator "notepad \"plik 1.txt\""  
runas /env /user:Administrator "notepad \"plik 2.txt\""
```

Wyjaśnij dlaczego opcja /env spowodowała różnice w lokalizacji edytowanego pliku:

5. Sprawdź czy można uruchomić proces w ramach konta użytkownika, który ma puste hasło.

1.2 Poziomy obowiązkowości (*integrity levels*)

6. Posługując się poleceniem psexec, uruchom notepad.exe z niskim poziomem obowiązkowości:

psexec -l %windir%\notepad.exe

7. Sprawdź czy Notatnik może wczytać plik z katalogu systemowego, np. którykolwiek %SystemRoot%\System32*.xml.
8. Spróbuj zmodyfikować wczytany plik i zapisać go w oryginalnej lokalizacji. Jaki jest tego efekt?

9. Spróbuj zapisać plik pod inną nazwą. Z jakim efektem?

10. Gdzie ostatecznie można zapisać ten plik?

11. Uruchom cmd w trybie administracyjnym oraz przeglądarkę Internet Explorer (nie Edge). Zweryfikuj poziomy obowiązkowości tych aplikacji za pomocą narzędzia Process Explorer.

2. Kontrola konta użytkownika – UAC (*User Account Control*)

2.1.1 Wirtualizacja systemu plików i rejestru

12. Zaznacz które z wymienionych procesów mają włączoną wirtualizację UAC:

csrss.exe (Client Server Runtime Subsystem)

dwm.exe (Desktop Window Manager)

explorer.exe (Explorator Windows)

iexplore.exe 64b (Internet Explorer)

iexplore.exe 32b (Internet Explorer)

13. Czy można włączyć wirtualizację UAC dla 64-bitowego Internet Explorera?

TAK / NIE

14. Uruchom cmd (bez podniesionych uprawnień). Korzystając z Menadżera zadań, zmień status wirtualizacji tego procesu na „Włączone”. Następnie w katalogu %windir% zapisz dowolny plik np.:

C:\Windows> echo test 1 > test.txt

15. Sprawdź widoczność tego pliku najpierw za pomocą polecenia `dir`, a później z wykorzystaniem Exploratora Windows. Gdzie znajduje się rzeczywista lokalizacja zwirtualizowanego pliku?

16. Wyłącz wirtualizację dla procesu `cmd`. Czy plik jest nadal widoczny w katalogu `C:\Windows`?

17. Ponownie włącz wirtualizację dla tego procesu. Czy teraz plik powinien być znów widoczny?

18. Sprawdź czy gałąź rejestru `HKLM\Software\Microsoft\Windows` podlega wirtualizacji. Zapisz jakie to niesie konsekwencje: