Windows Audit

Wstęp

Narzędzie audytorskie składa się z trzech narzędzi:

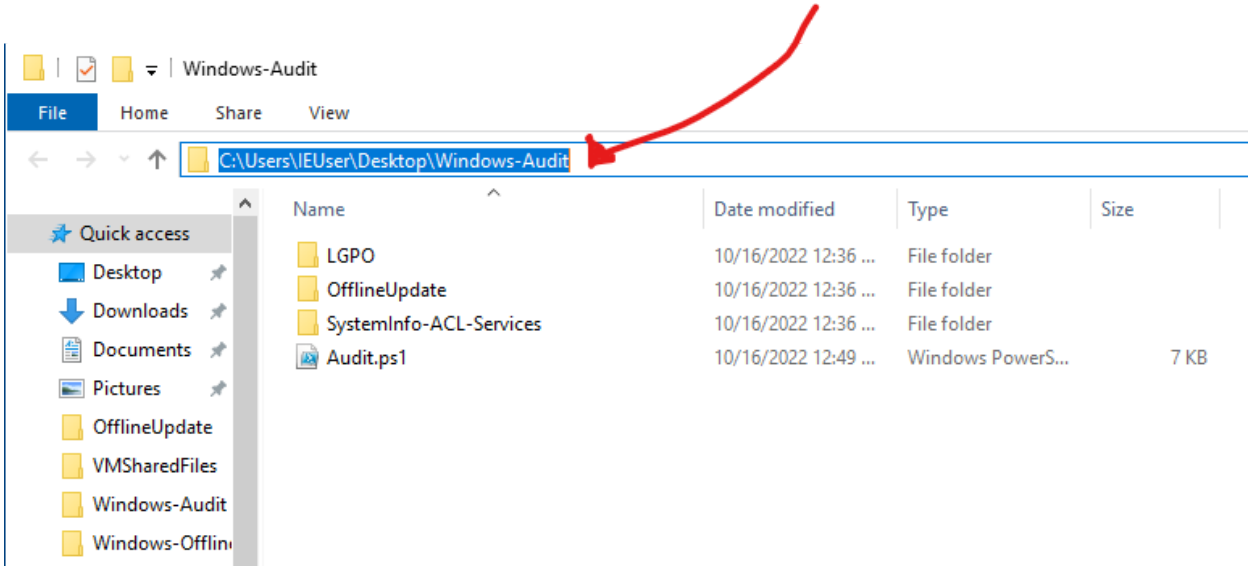
1. Skrypt podstawowy do weryfikacji:
    - Daty instalacji systemu
    - Wersji systemu
    - Dysków – lista dysków, formatowanie, nazwa
    - Stanu aktywacja systemu
    - Konta lokalne w systemie
    - Grupy lokalne w systemie
    - Użytkownicy w poszczególnych grupach
    - Sprawdzenie UAC
    - Sprawdzenie ACL plików *.exe w System32 oraz SysWOW64
    - Sprawdzenie usług
2. Skrypt do sprawdzenia stanu aktualizacji systemu z pomocą bazy **wsusscan2.cab** dostarczanej od Microsoft.
3. Policy Analyzer od Microsoftu

Instrukcja

1. Z nośnika kopiujemy folder z narzędziem np. na pulpit.
2. Uruchamiamy Powershell z **uprawnieniami administratora**.
3. Odblokowujemy możliwość uruchamiania skryptów w systemie przy pomocy komendy:

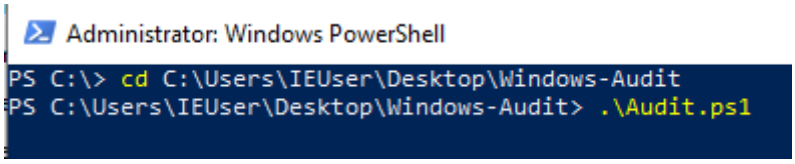
```
Set-ExecutionPolicy Bypass
```

4. Przy pomocy komendy *cd* przechodzimy do folderu gdzie znajduje się skrypt **Audit.ps1** np.:



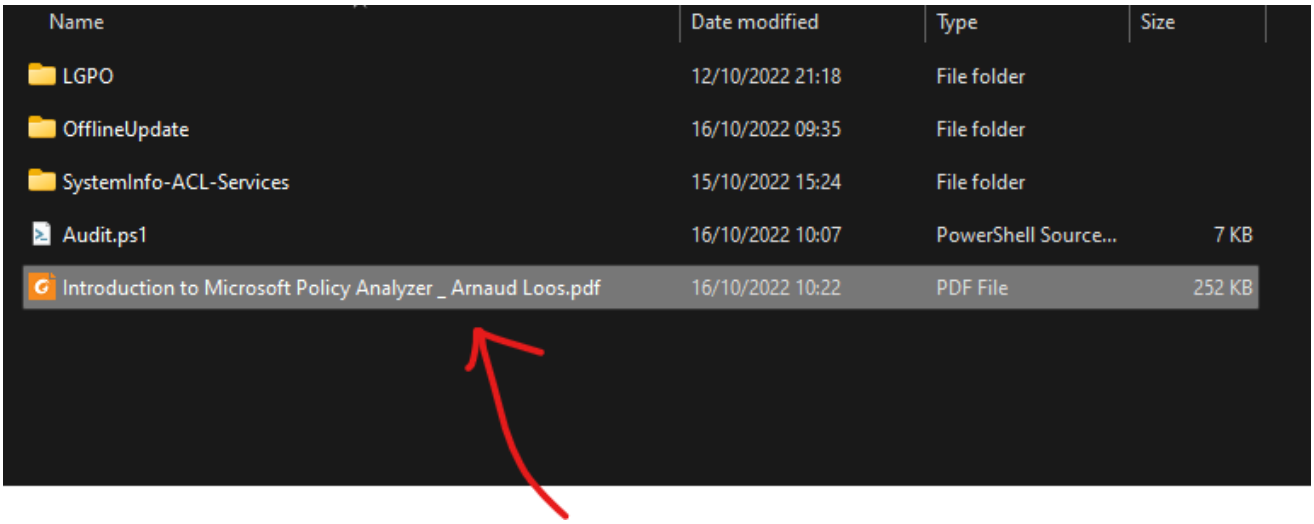

```
cd "C:\Users\IEUser\Desktop\Windows-Audit"
```

5. Uruchamiamy skrypt Audit.ps1 wpisując w Powershell




```
.\Audit.ps1
```

6. Skrypt w prostolinijny sposób prowadzi nas przez kolejne sprawdzenia, aż do momentu zapytania o sprawdzenie LGPO. Jeśli chcemy uruchomić narzędzie PolicyAnalyzer klikamy **YES**. Instrukcję użycia narzędzia można znaleźć w głównym folderze skryptu:



7. Kolejne wyskakujące okienko zapyta nas czy chcemy uruchomić narzędzie do sprawdzania aktualizacji. Jeśli tak, klikamy YES. Wymagane jest posiadanie linku do pliku **wsusscan2.cab** (link do pliku załączony w sekcji Linki niniejszej instrukcji).
- Skrypt poinformuje nas o lokalizacji pliku **.txt** z listą wymaganych aktualizacji.
8. Pamiętamy o wyłączeniu możliwości uruchamiania skryptów:

```
Set-ExecutionPolicy Restricted
```

Linki

Pobieranie Microsoft Security Compliance Toolkit 1.0
Pobieranie najnowszego pliku wsusscan2.cab

Autor i kontakt

Tomasz Pers (2.SLT)
Kontakt internet: t.pers@ron.mil.pl