23.4 Odszyfrowanie dysku powershell

Znalezienie wszystkich zaszyfrowanych plików i folderów i odszyfrowanie ich za pomocą PowerShell

Znajdź wszystkie zaszyfrowane pliki EFS na komputerze z systemem Windows i odszyfruj je, aby przygotować komputer do usunięcia z domeny. Ponieważ zaszyfrowane pliki EFS są szyfrowane przy użyciu prywatnego klucza przechowywanego w profilu użytkownika, w przeciwnym razie byłyby nieczytelne podczas korzystania z nowego lokalnego profilu użytkownika po usunięciu komputera z domeny. Wykorzystaj Unprotect-FilesOnLogicalDisk_v3.ps1 dostępny w folderze z materiałami.

System Windows zawiera narzędzie szyfrujące do szyfrowania i odszyfrowywania plików, ale chciałem używać natywnego PowerShell, aby rejestrować wszystkie zaszyfrowane i odszyfrowane pliki w pliku dziennika. Aby odszyfrować plik za pomocą PowerShell, możemy użyć metody deszyfrowania znajdującej się w cmdlecie Get-Item.

Jednak foldery nie są w rzeczywistości zaszyfrowane: foldery mają atrybut zaszyfrowany, który szyfruje wszystkie umieszczane w nich pliki. Nie znalazłem łatwego sposobu na usunięcie tego atrybutu za pomocą PowerShell: inne atrybuty, takie jak archiwum, nie stanowiły problemu, ale usunięcie atrybutu szyfrowania wydaje się nie być możliwe. W rezultacie musiałem użyć pliku wykonywalnego szyfru, aby faktycznie usunąć ten atrybut.

Pamiętaj, że jeśli chcesz uruchomić ten skrypt na komputerze, na którym nadal działa PowerShell v2, będziesz musiał zamiast tego użyć poniższego skryptu. Istnieje tylko jedna niewielka modyfikacja umożliwiająca uruchomienie tego skryptu w wersji 2, a mianowicie, że polecenie cmdlet Get-ChildItem nie zawiera przełączników -file ani -directory , więc trzeba filtrować pliki i foldery za pomocą właściwości PSIsContainer . Wykorzystaj Unprotect-FilesOnLogicalDisk_v2.ps1 dostępny w folderze z materiałami.

Pliki dostępne są również https://github.com/MarcoJanse/Scripts/tree/master/FileSystem