Laboratorium 9

Narzędzia zabezpieczające system

Większość narzędzi zabezpieczających system została opisana we wcześniejszych rozdziałach. Wiele narzędzi firmy Sysinternals jest narzędziami uniwersalnymi, które monitorują wiele części naszego systemu. Typowymi narzędziami zabezpieczającymi system są: **Autologon**, **LogonSessions**, **PsLoggedOn**, **RootkitRevealer (pobierz plik bp.zip)**.

Autologon jest narzędziem pozwalającym włączyć/wyłączyć okno logowania w systemie Windows. W programie mamy dwie opcje Enable włączająca okno logowania i Disable wyłączająca okno logowania systemu Windows. Jak wynika z powyższego opisu aplikacja jest dosyć niebezpieczna jeśli logowanie jest wyłączone, ponieważ każde włączenie komputera pozwala każdemu użytkownikowi wejście do naszego systemu.

LogonSessions oraz PsLoggedOn są to dwie aplikacje służące do sprawdzenia kto się logował na naszym komputerze lub kto był na nim zalogowany. Narzędzie LogonSessions listuje kto był ostatnio zalogowany w systemie, a narzędzie PsLoggedOn listuje użytkowników, którzy zalogowali się bezpośrednio do naszego systemu, aplikacja jest częścią pakietu PsTools. Obie aplikacje działają bez instalacji, należy je wkleić do folderu C:\Windows\System32. Działają z linii wiersza poleceń.

Przykład użycia:

logonsessions [-p]

gdzie:

-p wyświetla listy logowania w różnych sesjach,

psloggedon [-] [-l] [-x] [\\computername | username]

gdzie:

- pokazuje pobrane opcje i jednostki pomiarów użyte do wydajności wartości,

-l pokazuje tylko lokalne logowania do systemu,

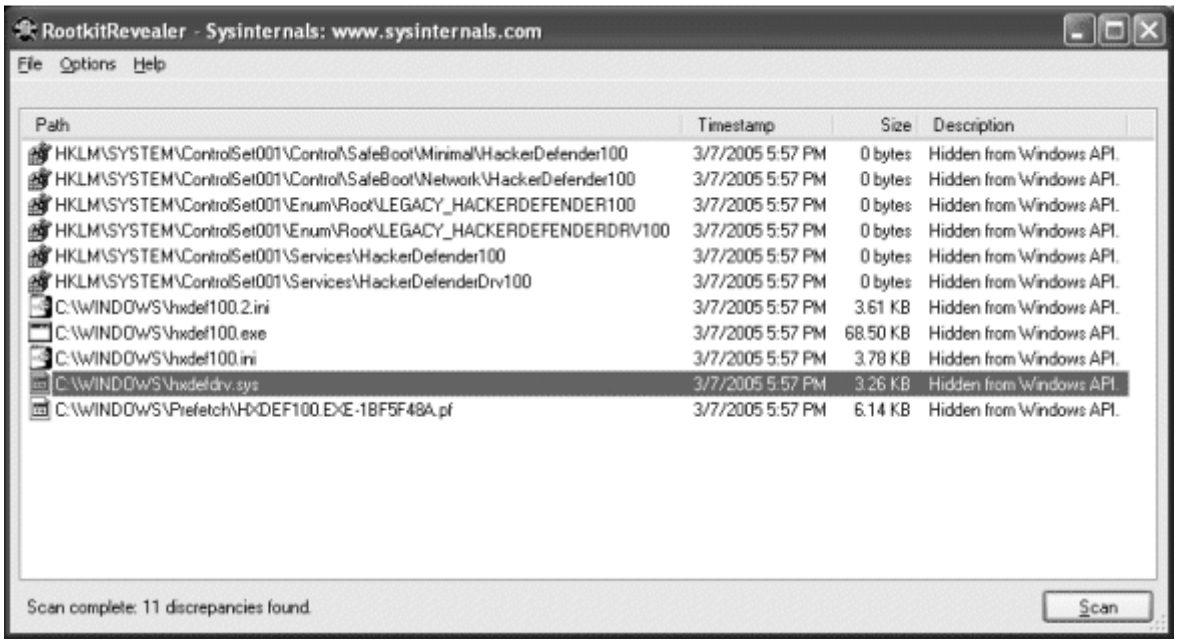
-x nie pokazuje czasu logowania,

\\computername wyświetla nazwę komputera, z którego logowano się do sytemu,

username jeżeli wpiszemy nazwę użytkownika polecenie wyszuka w sieci komputera z którego dany użytkownik logował się do systemu.

RootkitRevealer jest Zaawansowanym narzędziem do wykrywania potencjalnie niebezpiecznego oprogramowania typu rootkit. RootkitRevealer poszukuje w systemie Windows podmienionych API dostępu do rejestru i systemów plików, które najczęściej

wskazują na obecność rootkita działającego w trybie użytkownika lub w trybie jądra. Podejrzane procesy prezentowane są w formie szczegółowej listy zawierającej lokalizację w Rejestrze systemowym lub ścieżkę na dysku, czas, wielkość i opis. RootkitRevealer wykrywa wszystkie rootkity opublikowane na stronie www.rootkit.com, m.in. AFX, Vanquish, HackerDefender. Warto zwrócić uwagę, że nie są wykrywane takie rootkity jak Fu, które nie ukrywają swojej obecności w systemie. Rysunek 1 przedstawia aplikację RootkitRevealer.



Rys. 1. Narzędzie RootkitRevealer