Laboratorium 6

1. Narzędzia sieciowe

Narzędzia monitorujące działanie sieci tworzone przez Sysinternals to **AdExplorer**, **AdRestore**, **TCPView**, **Whois (pobierz plik nlan.zip)**.

AdExplorer (Active Direktory Explorer) jest programem którego idea jest podobna do programu ADSIEdit, jest on jednak programem bardziej złożonym, zaawansowanym i posiadającym więcej funkcji. Aplikacja pozwala między innymi zapamiętywać często odwiedzane lokalizacje w bazie Active Direktory, lub wykonywać zaawansowane wyszukiwania. Jedną z ciekawszych funkcji tego narzędzia jest możliwość tworzenia „snapshotów" i ich porównywania, co umożliwia użytkownikowi systemu stwierdzenie, które obiekty i atrybuty zostały zmienione. Rysunek 1 pokazuje pracujące narzędzie AdExplorer.

Rys. 1. Aplikacja Active Directory Explorer

Narzędzie **AdRestore** jest poręczną aplikacją służącą do odzyskiwania obiektów struktury katalogowej. Dopóki nie pojawiło się to narzędzie użytkownicy byli skazani na niewygodny tryb „authoritative restore". AdRestore jest narzędziem tekstowym, które wyświetla utracone obiekty i pozwala je przywrócić.

Jest to proste narzędzie paska poleceń. O następującej składni:

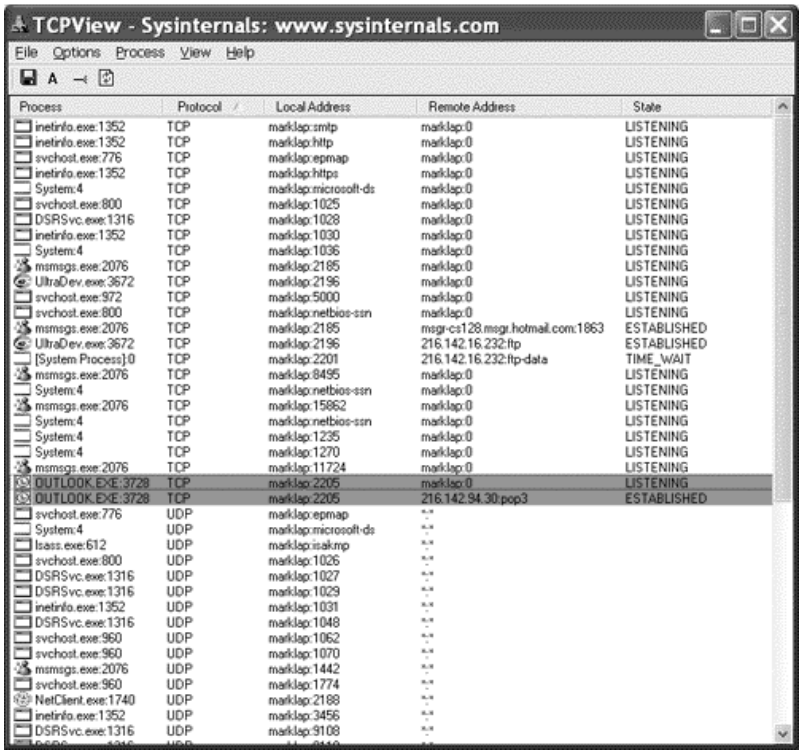
```
adrestore –r filtr_wyszukiwania
```

gdzie:

- `r – opcja wskazująca na odzyskiwanie obiektów znalezionych,`

- `filtr_wyszukiwania – określa ciąg znaków jaki znajdował się w nazwie obiektu.`

TCPView jest prostym ale pomocnym administratorom narzędziem do monitorowania procesów wykorzystujących połączenia za pomocą protokołów TCP lub UDP. TCPView wyświetla listę wszystkich procesów łączących się za pomocą protokołów TCP lub UDP wraz z nazwą aplikacji, rodzajem protokołu, adresem lokalnym (wraz z portem), adresem zdalnym i aktualnym stanem. Program umożliwia zamknięcie połączeń wskazanych procesów lub nawet wyłączenie ich samych. Wyświetlaną listę można w każdej chwili zapisać do pliku tekstowego. W pliku z wersją z wersją instalacyjna programu, załączona jest bliźniacza wersja uruchamiana z wiersza poleceń. Rysunek 2 przedstawia narzędzie TCPView.



Rys. 2. Aplikacja TCPView

Whois jest ostatnim narzędziem z grupy sieciowe proponowanym przez programistów firmy Sysinternals. Tak naprawdę Whois nie jest aplikacją tylko usługą sieciową i z języka angielskiego oznacza „kto jest". Usługa ta pozwala na sprawdzenie kto jest właścicielem domeny.

Whois pozwala uzyskać następujące dane:

- nazwę właściciele domeny oraz jego dane teleadresowe,
- datę zarejestrowania i wygaśnięcia domeny,

- nazwę i dane firmy opiekującej się domeną od strony technicznej,
- registrara (firmę, w której zarejestrowano domenę),
- nazwy serwerów DNS, które obsługują daną domenę.

Dane wyświetlane przez tą usługę różnią się w przypadku domen polskich i zagranicznych. Jeśli mamy do czynienia z domeną polską dane osób prywatnych nie będą dostępne.

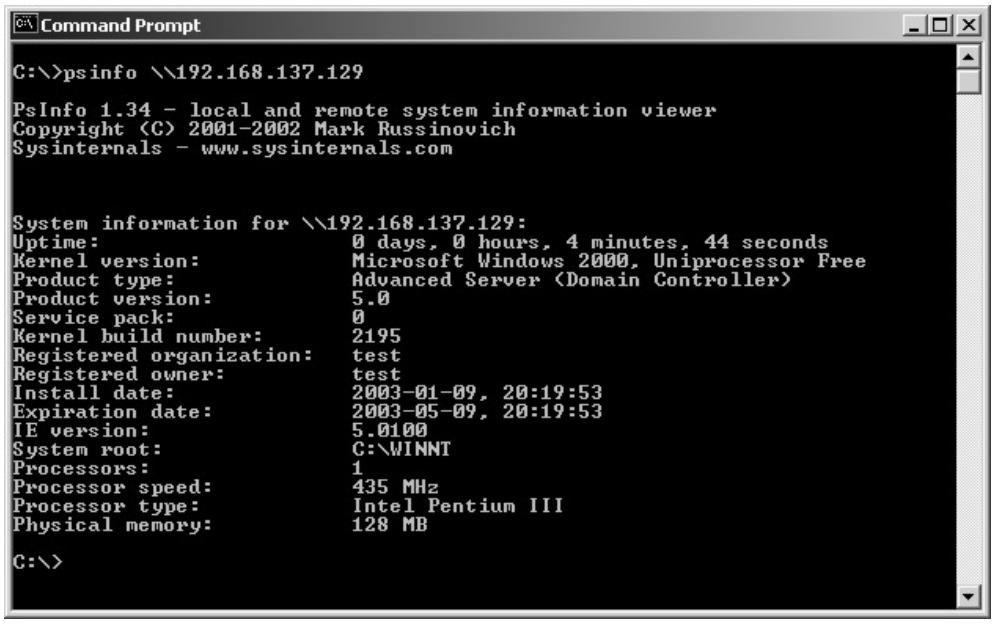
2. Informacje o systemie

W systemie Windows wbudowane jest narzędzie wyświetlające informacje o systemie, natomiast w paczce Sysinternals dostępnych jest kilka odrębnych narzędzi pomagających zebrać użytkownikowi informacje o systemie. Do programów tych należą:

ClockRes mała aplikacja działająca z linii wiersza poleceń, nie posiadająca żadnych argumentów dodatkowych. narzędzie resetuje zegar systemowy. Za pomocą programu można ustawić maksymalny czas działania danego programu.

LoadOrder to programik który wyświetla kolejność uruchamianych usług oraz urządzeń jak również podaje ich tagi.

Jednym z bardziej zaawansowanych narzędzi wyświetlających informacje o systemie proponowanych przez programistów Sysinternals jest wchodząca w skład pakietu PsTools aplikacja **PsInfo**. PsInfo jest bardzo przydatnym narzędziem pozwalającym na szybkie i zdalne kontrolowanie konfiguracji komputerów. jest to program korzystający z linii wiersza poleceń. Program zwraca bardzo ciekawe informacje związane z systemem (zdalnym). Przykładowe informacje wyświetlane przez tą aplikację dla konkretnego adresu IP pokazano na rysunku 3.



Rys. 3. Informacje wyświetlane przez PsInfo

Jak widać na rysunku otrzymaliśmy informacje o wersji jądra systemu, o typie funkcjonalnym produktu (kontroler domeny), wersji 5.0 systemu (Windows 2000), braku zainstalowanych Service Packów, nazwę organizacji i właściciela oraz daty: instalacji i końca okresu testowego (system w wersji ewaluacyjnej). Wersja przeglądarki WWW MS Internet Explorer to 5.01. Są też i inne (mniej istotne) informacje.

Aplikacja posiada tez kilka przydatnych argumentów, które pozwolą wyświetlać dodatkowe informacje o systemie:

- opcja –h pozwala między innymi na kontrolowanie zainstalowanych poprawek systemowych,
- opcja -s pozwala na enumerację zainstalowanych w systemie aplikacji, daje też nieco więcej informacji o zainstalowanych hotfixach (poprawkach systemowych) jak również o Service Packach (dużych zbiorach poprawek).
- opcja -d pozwala uzyskać informację o dyskach, napędach i partycjach istniejących w danym komputerze.