BLUE TEAM
I CYBERBEZPIECZEŃSTWO
ZESTAW NARZĘDZI DLA SPECJALISTÓW OD ZABEZPIECZEŃ W SIECI

NADEAN H. TANNER

WILEY

Helion

Tytuł oryginału: Cybersecurity Blue Team Toolkit

Tłumaczenie: Aleksander Łapuć

ISBN: 978-83-283-7368-6

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/cybbez
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Rozdział

2

Rozwiązywanie problemów w systemie Microsoft Windows

W tym rozdziale omówimy:

- narzędzie Monitor niezawodności,
- narzędzie Rejestrator kroków,
- program PathPing,
- program MTR,
- pakiet Sysinternals,
- narzędzie Windows Master Control Panel.

W 2012 roku opuściłam wspaniałą Luizjanę i przeniosłam się do Kolorado, by prowadzić szkolenia dla żołnierzy z zakresu ochrony informacji w strukturach Dowództwa Telekomunikacji Elektronicznej Armii Stanów Zjednoczonych (ang. *Communications-Electronics Command* — CECOM) w Fort Carson. Wymagania Departamentu Obrony, zapisane w dyrektywie numer 8570, jasno określają, że wszyscy członkowie stałej lub czasowej służby wojskowej z dostępem do informacji poufnych oraz kontraktorzy z takim dostępem powinni uzyskać szereg certyfikatów komputerowych. Prowadziłam zajęcia przygotowujące do egzaminów certyfikacyjnych, pomagając żołnierzom osiągnąć poziom kompetencji w bezpieczeństwie informacji wymagany na ich stanowiskach.

Mój dowódca, Ryan Hendricks, był sieciowym guru i wolał prowadzić zajęcia przygotowujące do egzaminów certyfikacyjnych Cisco. Wobec tego ktoś musiał zająć się przygotowaniem do egzaminów A+, Network+, Security+, Server+, CASP i CISSP oraz szkoleniami dotyczącymi Microsoft

Active Directory, SCCM i SharePointa. Oboje uważaliśmy, że nauczyciel przygotowujący do egzaminu powinien wcześniej uzyskać nauczany certyfikat — inne podejście byłoby nieuczciwe wobec słuchaczy. Dlatego on pozostał przy ścieżce certyfikacyjnej Cisco, a ja zajęłam się ścieżką Microsoft CompTIA.

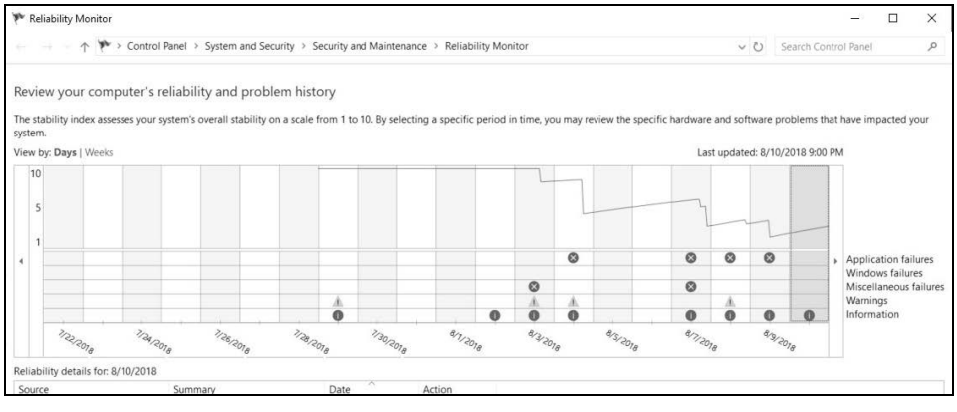
W czasie przygotowywania się do egzaminów certyfikacyjnych nieraz doznawałam olśnienia, odkrywając narzędzie lub metodę niesamowicie ułatwiające rozwiązywanie problemów w systemie Windows. Większość takich odkryć stosuję na co dzień. Później, gdy prowadziłam szkolenia dla firmy Rapid7, zwykłam pokazywać niektóre z nich, gdy czekaliśmy, aż wszyscy uczestnicy wrócą po przerwie obiadowej. Traktowałam to jako mały prezent dla punktualnych osób.

Gdy pokazywałam te narzędzia nawet całkiem doświadczonym osobom, zdarzało mi się usłyszeć w ich głosie żal, że nie znali i nie używali ich wcześniej, czasem wyrażony w dosyć niewybrednych słowach. Wiele z tych narzędzi może ułatwić Ci wykonywanie zadań, nad którymi do tej pory musiałeś mozolnie się trudzić. Zwłaszcza ułatwią Ci życie, jeżeli administrujesz siecią złożoną przeważnie z komputerów pracujących pod kontrolą systemu Windows.

Monitor niezawodności

Czasem nazywam to narzędzie **NI**, bo zwykle tylko tyle trzeba wpisać w polu wyszukania na pasku zadań, aby system Windows odnalazł pozycję *Wyświetl historię niezawodności* (*Reliability History*), W menu *Start* narzędzie istnieje pod taką właśnie nazwą. Ale po uruchomieniu programu okno nazywa się *Monitor niezawodności* (*Reliability Monitor*). (Dzięki za ułatwienie życia, zespole Microsoftu). Narzędzie wywodzi się z Windows Vista i pozwala przyjrzeć się stabilności pracy komputera na osi czasu. W angielskiej wersji systemu narzędzie nazywa się Reliability Monitor (a można je odnaleźć, wpisując **RELI** w pole wyszukiwania na pasku zadań).

Monitor niezawodności przedstawia ważne zdarzenia systemowe, wystąpienia błędów aplikacji i systemu, aktualizacje oraz inne, potencjalnie przydatne, informacje w postaci wykresu na osi czasu. Na rysunku 2.1 umieściłam przykładowy wykres obejmujący kilka wystąpień usterek aplikacji i systemu operacyjnego oraz innych problemów. Jak korzystać z Monitora niezawodności, dowiesz się w ćwiczeniu 2.1.



Rysunek 2.1. Wykres prezentowany przez Monitor niezawodności

ĆWICZENIE 2.1. MONITOR NIEZAWODNOŚCI

1. Aby uruchomić to narzędzie, otwórz menu *Start* i zacznij wpisywać słowo **`niezawodności`** (zwykle wystarczą dwie pierwsze litery). W angielskiej wersji systemu zacznij wpisywać **`reliability`**.
2. Naciśnij *Enter*, gdy zobaczysz odnalezioną pozycję *Wyświetl historię niezawodności* (*Reliability History*), opatrzoną ikoną z niebieską chorągiewką. Poczekaj na zbudowanie wykresu.
3. Nad lewym górnym rogiem wykresu możesz zmienić skalę osi czasu — do wyboru są dni lub tygodnie.
4. Obszar pod linią wykresu jest podzielony na wiersze, których opisy znajdują się po prawej stronie.
   - ❖ Pierwsze trzy wiersze, licząc od góry, zawierają informacje o wystąpieniach błędów aplikacji, błędów systemu Windows oraz innych błędów. W tych liniach pojawią się informacje o nagłych zatrzymaniach aplikacji lub niepoprawnym zamknięciu systemu Windows. Widać tu jak na dłoni historię awarii systemu, czyli „niebieskich ekranów śmierci". Wystąpienie takich błędów będzie zaznaczone czerwonym kółkiem z białym znakiem *X* na środku.
   - ❖ Kolejny wiersz zawiera informacje o ostrzeżeniach. Ich wystąpienie jest oznaczane żółtym trójkątem z wykrzyknikiem. Zdarzenia skutkujące ostrzeżeniem to na przykład nieudana aktualizacja oprogramowania lub wystąpienie błędu w działaniu aplikacji, który nie spowodował jej całkowitego wyłączenia.
   - ❖ Najniższy, piąty wiersz zawiera wpisy informacyjne oznaczone niebieskim kółkiem z białą literą *i*. Tutaj będą zaznaczane na przykład udane aktualizacje oprogramowania lub pomyślne instalacje sterowników.
5. W lewym dolnym rogu okna znajduje się opcja *Zapisz historię niezawodności...* (*Save reliability history...*) tworząca plik XML z wyświetlanymi danymi. Zapisany plik można wyeksportować i poddać analizie za pomocą zewnętrznych aplikacji raportujących.
6. Obok polecenia zapisu raportu znajduje się opcja *Wyświetl wszystkie raporty o problemach* (*View all problem reports*). Gdy ją wybierzesz, wykres zostanie zastąpiony przez listę wszystkich problemów, jakie wystąpiły na tym komputerze i o których raport można przesłać bezpośrednio do zespołu Microsoftu. Jeżeli dla jakiegoś problemu jest znane rozwiązanie, to stosowna informacja będzie zawarta na ekranie *Zabezpieczenia i konserwacja* (*Security and Maintenance*) w Panelu sterowania (Control Panel). Aby wyświetlić ten ekran, możesz skorzystać z paska nawigacji, znajdującego się w górnej części okna Monitora niezawodności.

KORZYSTANIE Z MONITORA NIEZAWODNOŚCI

Wyobraź sobie, że pracujesz jako administrator systemu. W większości organizacji administratorzy systemów zajmują się instalowaniem, aktualizowaniem i monitorowaniem oprogramowania oraz sprzętu. Załóżmy, że w serwerowni, którą się opiekujesz, jest jedna maszyna, która co jakiś czas wariuje. Próbujesz zidentyfikować i rozwiązać problem, ale nie udaje Ci się odtworzyć zgłoszonej usterki. Zamiast tego uzyskujesz niesławny niebieski ekran śmierci.

Zwykle pierwszą poradą na zgłaszane problemy z komputerem jest prośba o wyłączenie i ponowne uruchomienie. W przypadku nieszczęśliwego wystąpienia niebieskiego ekranu śmierci jedyną dostępną opcją jest ponowne uruchomienie. Dzięki Monitorowi niezawodności masz szansę ustalić przyczynę awaryjnego zatrzymania.

Z mojego doświadczenia wynika, że najczęstszą przyczyną wystąpienia niebieskiego ekranu śmierci są błędne sterowniki, przegrzanie komputera lub zainstalowanie nowego oprogramowania, niekompatybilnego ze sprzętem lub systemem operacyjnym. Monitor niezawodności prawdę Ci powie.

W końcu nikt nigdy się nie przyzna, że awaria nastąpiła po zainstalowaniu gry *Duke Nukem Forever*.

Rejestrator kroków

Zajmujesz się tworzeniem dokumentacji lub procedur zapewniających ciągłość działania organizacji w razie niespodziewanych wypadków? Prowadzisz szkolenia dla innych członków organizacji z zakresu ich obowiązków? A może zostałeś poproszony o przeszkolenie kogoś do wykonywania własnych obowiązków? Czy musisz czasem zdiagnozować problem związany z konkretnym środowiskiem pracy? Albo nagle przygotować prezentację dotyczącą korzystania z oprogramowania?

Rejestrator kroków (ang. *Problem Steps Recorder* lub *PSR*) jest narzędziem dodanym do systemu Windows w wersjach 7 i Server 2008. Jest to połączenie narzędzi do diagnozowania problemów, wsparcia użytkownika, przechwytywania widoku ekranu oraz opatrywania przypisami. Zadziwiająco niewielu specjalistów IT o nim wie i je stosuje. A może ono pomóc w szybkim dokumentowaniu wykonywanych kroków, tworząc serię zrzutów ekranu opatrzonych komentarzem. Korzystając z niego, możesz zdiagnozować przyczynę usterki napotkanej przez użytkownika, który nie jest tak biegły technicznie jak Ty. Jednak moim ulubionym sposobem wykorzystania Rejestratora jest tworzenie dokumentacji.

Jeżeli chcesz poznać prawdziwe potrzeby kierownika IT, to zapytaj go, co nie daje mu spać nocami. Gdy prowadzę zajęcia, staram się jak najlepiej zrozumieć potrzeby moich uczniów i ich cele. Pytani o główne bolączki w obszarze bezpieczeństwa najczęściej odpowiadają: brak dokumentacji i procedur zapewnienia ciągłości działania. Rejestrator kroków pomoże rozwiązać te problemy.

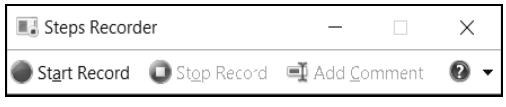
W przeszłości zarządzałam ludźmi bez doświadczenia w IT, którzy zazwyczaj zadawali wciąż i wciąż te same pytania. Chciałam ułatwić im samodzielne poszukiwanie informacji, dlatego zaczęłam tworzyć prezentacje z użyciem Rejestratora kroków, a następnie umieszczałam je na stronie SharePointa. Prezentacje zawierały odpowiedzi na najczęściej powtarzające się pytania, najczęstsze z najczęstszych przykładów wymieniam poniżej.

- Jak dodać statyczny adres IP?
- Jak skonfigurować drukarkę sieciową?
- Jak dodać użytkownika do bazy Active Directory?

W ćwiczeniu 2.2 pokażę Ci, jak korzystać z Rejestratora kroków.

ĆWICZENIE 2.2. REJESTRATOR KROKÓW

1. Aby uruchomić Rejestrator kroków, otwórz menu *Start* i wyszukaj **`Rejestrator problemów`** (tak, to kolejna aplikacja z inną nazwą w spisie i w tytule aktywnego okna — jeszcze raz serdeczne dzięki, zespole Microsoftu!). Naciśnij *Enter*, aby uruchomić program. Przykładowy widok okna zamieściłam na rysunku 2.2.



Rysunek 2.2. Menu Rejestratora kroków

2. Kliknij *Rozpocznij rejestrowanie* (*Start Record*).
3. Uruchom Kalkulator, wpisz z klawiatury **9+9** i naciśnij *Enter*. Uzyskasz wynik 18. W miejscu każdego kliknięcia na ekranie pojawi się na chwilę czerwona kropka — to znak, że został wykonany zrzut ekranu. Trwające nagrywanie jest oznaczone przez migającą czerwoną kropkę na pasku nazwy okna Rejestratora.
4. Teraz kliknij *Zatrzymaj rejestrowanie* (*Stop Record*) i poczekaj, aż będziesz mógł zobaczyć prezentację z nagranymi krokami.

Możesz teraz obejrzeć zarejestrowaną prezentację w wyświetlonym oknie. Jeżeli uznasz, że zarejestrowana treść nie przedstawia dokładnie procesu, który chcesz udokumentować, to możesz ponowić nagranie, klikając opcję *Nowe nagranie* (*New Recording*). Jeżeli uzyskałeś zamierzony efekt, możesz zapisać wynik przyciskiem *Zapisz* (*Save*). Domyślnie wynik jest zapisywany w postaci archiwum *.zip*. Jeżeli Twoi klienci lub pracownicy napotykają problem techniczny, to mogą w ten sposób łatwo przekazać Ci zapis wykonywanych kroków do zbadania. Wewnątrz archiwum *.zip* znajduje się plik MHTML. Możesz otworzyć go do edycji w programie Word, wystarczy, że klikniesz jego nazwę prawym przyciskiem myszy i wybierzesz odpowiednią opcję z menu podręcznego. Możesz w ten sposób poprawić automatycznie generowaną treść, aby mogła służyć jako dokumentacja procesu lub procedury zapewniania ciągłości działania.

Przy każdym kroku zapisane są data i czas wykonania, a na załączonym widoku ekranu okno, które kliknięto, zaznaczone jest zieloną obwódką. Przyjrzyj się zapisanej procedurze z ćwiczenia. Na pierwszym widoku zielona obwódka powinna być wokół menu *Start*, a strzałka kursora powinna być umieszczona w obrębie menu. Powyżej zrzutu ekranu zamieszczony będzie opis wprowadzanych danych. W przypadku rozwiązywania problemów dokładny zapis wprowadzanych informacji może mieć kluczowe znaczenie.

Na dole strony z zarejestrowanymi krokami znajduje się sekcja szczegółów (*Additional details*, także w polskiej wersji językowej). Znajdziesz w niej szczegóły techniczne dotyczące uruchamianych

programów oraz systemu operacyjnego, które są zrozumiałe tylko dla programistów lub zaawansowanych specjalistów IT. Niemniej zawsze należy przejrzeć zawartość tej sekcji, aby upewnić się, że nie zawiera ona informacji, które nie powinny być udostępniane.

Czy kiedykolwiek dostałeś zadanie, żeby poprowadzić prezentację na spotkaniu, które będzie za 15 minut? Uważam, że jestem dobra w swoim fachu, ale nawet dla mnie to ekstremalnie krótki czas. Jeżeli prezentacja ma dotyczyć działań, które możesz pokazać w Rejestratorze kroków, to wystarczy, że odnajdziesz na szczycie strony odnośnik wyświetlania procedury jako prezentacji (*Review the recorded steps as a slide show*, także w polskiej wersji językowej) i klikniesz go.

Pracując z Rejestratorem kroków, warto pamiętać o kilku sprawach. Wynik będzie wyglądać znacznie bardziej profesjonalnie, jeżeli nagrywanie będzie odbywać się tylko na jednym monitorze — narzędzie przechwytuje zawsze wszystkie ekrany naraz. Teksty wprowadzane z klawiatury, na przykład hasła, nie będą rejestrowane — Rejestrator zapisuje jedynie użycie klawiszy funkcyjnych i skrótów klawiaturowych. Narzędzie nie będzie także zapisywać wideo ani gier pracujących w trybie pełnoekranowym. Można jedynie uzyskać statyczną migawkę z ekranu. Domyślnie można zebrać jedynie 25 widoków ekranu. Jeżeli chcesz zarejestrować dłuższą prezentację, to musisz zmienić ustawienia dostępne w menu pomocy (po prawej stronie okna Rejestratora). Zmiana tych ustawień nie będzie zapisana trwale, bowiem przy każdym uruchomieniu programu przywracane są wartości domyślne. Najlepiej od razu wyrób w sobie nawyk ustawiania maksymalnej liczby (999), bo po osiągnięciu limitu narzędzie po prostu nie zarejestruje kolejnych obrazów, ale też nie przerwie rejestrowania ani nie wyświetli ostrzeżenia. Polscy użytkownicy mogą także napotkać dodatkową niespodziankę — Rejestrator przechwytuje działanie skrótu klawiaturowego *Alt+C*, więc gdy program jest uruchomiony, może nie być możliwości wprowadzania litery **ć** z klawiatury…

Kilkukrotnie słyszałam od uczestników moich zajęć, zawodowo pracujących w IT, że poznanie tego jednego narzędzia było warte wszystkich pieniędzy, jakie wyłożyli na czesne za cały kurs.

PathPing

W 2017 roku firma Panasonic opracowała prototyp urządzenia, które nie tylko pierze i suszy ubrania, ale także je składa. Niektóre zadania po prostu powinny być wykonywane razem.

Narzędzie PathPing jest właśnie takim pioráco-susząco-składającym kombajnem dla systemu Windows. Gdybyś wziął narzędzie `ping` i złączył je z `tracert`, to powstanie właśnie PathPing. W wyniku uruchomienia tego polecenia badane jest połączenie do każdego z węzłów pośrednich na trasie do węzła docelowego, tak jakbyś uruchomił dla każdego z nich polecenie `ping`. W rezultacie raportowana jest nie tylko trasa pomiędzy dwoma komputerami, ale także rezultat badania połączenia dla każdego węzła pośredniego. Działanie węzłów jest obserwowane przez dłuższy czas, konkretnie po 25 sekund na każdy węzeł. Uzyskane dane wydajnościowe są znacznie bogatsze niż przy działaniu programu `ping`, który domyślnie wysyła tylko cztery komunikaty, lub programu `tracert`, który pokazuje tylko listę węzłów tworzących trasę.

Po uruchomieniu program PathPing najpierw wykona polecenie `tracert`, by poznać trasę do węzła docelowego. Następnie do każdego węzła pośredniego wyśle po 100 komunikatów ICMP z żądaniem echa. Dzięki temu zostanie sprawdzone opóźnienie wprowadzane przez sieć na trasie od komputera źródłowego do docelowego. Jednak nie można w pełni polegać na informacjach zwracanych przez protokół ICMP, gdy w komunikację zaangażowane są publiczne węzły. Właśnie

dlatego, że są ogólnodostępne, mogą być nadmiernie obciążane przez publiczny ruch w internecie. Badając połączenia poprzez internet, można natrafić na sytuację, gdy odsetek nieudanych żądań odpowiedzi protokołu ICMP wysłanych do pewnego węzła sięga 50 procent, a kolejny węzeł na trasie udziela poprawnej odpowiedzi w 100 procentach przypadków.

Na rysunku 2.3 przedstawiłam wynik śledzenia trasy do publicznego serwera DNS firmy Google o adresie 8.8.8.8. Trasa z mojego komputera do tego serwera składa się z 11 etapów pośrednich. Polecenie `pathping` wylicza całkowity czas transmisji oraz odsetek utraconych pakietów dla każdego z węzłów pośrednich. Jeżeli któryś węzeł ma wysoki odsetek utraconych pakietów, to może oznaczać, że ten router jest przeciążony.

```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Nadean>pathping 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0  DESKTOP-0U8N7VK.HomeRT [192.168.1.18]
  1  router.asus.com [192.168.1.1]
  2  cm-1-acr01.louisville.co.denver.comcast.net [96.120.13.37]
  3  ae-101-rur02.louisville.co.denver.comcast.net [162.151.15.41]
  4  ae-2-rur01.louisville.co.denver.comcast.net [162.151.51.173]
  5  ae-15-ar01.denver.co.denver.comcast.net [162.151.51.201]
  6  be-33652-cr02.1601milehigh.co.ibone.comcast.net [68.86.92.121]
  7  be-12176-pe02.910fifteenth.co.ibone.comcast.net [68.86.83.94]
  8  as1239-pe01.ashburn.va.ibone.comcast.net [75.149.228.174]
  9  108.170.254.81
 10  64.233.175.43
 11  google-public-dns-a.google.com [8.8.8.8]

Computing statistics for 275 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-0U8N7VK.HomeRT [192.168.1.18]
                                 0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  router.asus.com [192.168.1.1]
                                 0/ 100 =  0%   |
  2   11ms     0/ 100 =  0%     0/ 100 =  0%  cm-1-acr01.louisville.co.denver.comcast.net [96.120.13.37]
                                 0/ 100 =  0%   |
  3   15ms     0/ 100 =  0%     0/ 100 =  0%  ae-101-rur02.louisville.co.denver.comcast.net [162.151.15.41]
                                 0/ 100 =  0%   |
  4   13ms     0/ 100 =  0%     0/ 100 =  0%  ae-2-rur01.louisville.co.denver.comcast.net [162.151.51.173]
                                 0/ 100 =  0%   |
  5   14ms     0/ 100 =  0%     0/ 100 =  0%  ae-15-ar01.denver.co.denver.comcast.net [162.151.51.201]
                                 0/ 100 =  0%   |
  6   14ms     0/ 100 =  0%     0/ 100 =  0%  be-33652-cr02.1601milehigh.co.ibone.comcast.net [68.86.92.121]
                                 0/ 100 =  0%   |
  7   12ms     0/ 100 =  0%     0/ 100 =  0%  be-12176-pe02.910fifteenth.co.ibone.comcast.net [68.86.83.94]
                                 0/ 100 =  0%   |
  8   13ms     0/ 100 =  0%     0/ 100 =  0%  as1239-pe01.ashburn.va.ibone.comcast.net [75.149.228.174]
                                 0/ 100 =  0%   |
  9   13ms     0/ 100 =  0%     0/ 100 =  0%  108.170.254.81
                                 0/ 100 =  0%   |
 10  ---     100/ 100 =100%   100/ 100 =100%  64.233.175.43
                                 0/ 100 =  0%   |
 11   13ms     0/ 100 =  0%     0/ 100 =  0%  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

Rysunek 2.3. Polecenie PathPing łączące funkcjonalność śledzenia trasy ze zbieraniem statystyk dla każdego węzła pośredniego

Narzędzie PathPing bardzo ułatwia analizę sytuacji, gdy całkowite opóźnienie transmisji w Twojej sieci jest zbyt duże. Ale nawet jeżeli dostrzegasz anomalie w wynikach dla któregoś węzła pośredniego lub wartości zmierzone dla niego wciąż skaczą w górę i w dół, to niekoniecznie oznacza, że ten konkretny węzeł jest przyczyną problemów. Możliwe, że ten węzeł jest aktualnie bardzo obciążony lub jego procesor ma ważniejsze zadania niż obsługa żądań echa przesyłanych przez Twój program PathPing. Dostawcy usług sieciowych często chronią swoje routery przed nad-

miernym obciążeniem wynikającym z obsługi komunikatów ICMP. W tym celu wykorzystują mechanizmy klasyfikacji i nakładania ograniczeń na ruch (ang. *control-plane policing* — CoPP). Takie zabezpieczenia, jeżeli są aktywne na którymś węźle pośrednim, mogą wpłynąć na uzyskane wyniki z narzędzia PathPing. W ćwiczeniu 2.3 będziesz mógł poznać PathPing w działaniu.

ĆWICZENIE 2.3. PATHPING

1. Otwórz wiersz poleceń, interpreter poleceń PowerShell lub okno terminala.
2. Aby zapoznać się z opcjami dostępnymi w narzędziu PathPing, wpisz polecenie:
   ```
   pathping /?
   ```
3. Wpisz w wierszu poleceń następującą komendę:
   ```
   pathping -q 50 8.8.8.8
   ```

Dzięki wpisaniu opcji `-q 50` ograniczysz o połowę czas oczekiwania, choć wciąż będzie on dosyć długi i wyniesie kilka minut.

MTR

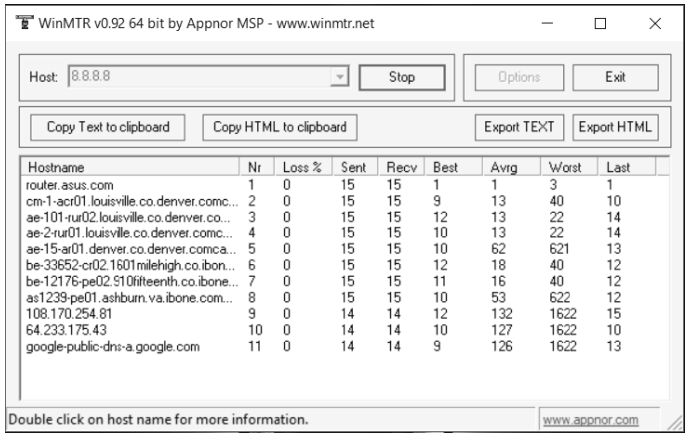
Kolejnym narzędziem jest My TraceRoute (MTR), które także łączy w sobie funkcjonalność kilku innych narzędzi. Zostało ono stworzone przez Matta Kimballa w 1997 roku i początkowo nazywało się Matt's TraceRoute.

Aplikacja WinMTR, pracująca pod kontrolą systemu Windows, łączy działanie poleceń `tracert` i `ping`. Program WinMTR można pobrać pod adresem *https://sourceforge.net/projects/winmtr/*. Narzędzie często znajduje zastosowanie w diagnozowaniu problemów z siecią. Administratorzy otrzymują aktualizowane na bieżąco statystyki dotyczące czasów odpowiedzi i liczby utraconych pakietów dla każdego węzła pośredniego. Dzięki temu mogą zidentyfikować, pomiędzy którymi węzłami pojawiają się problemy najsilniej wpływające na wartość całkowitego opóźnienia transmisji sieciowej. Możliwe jest w ten sposób zidentyfikowanie przeciążonych węzłów. Z narzędziem MTR zapoznasz się w ćwiczeniu 2.4.

ĆWICZENIE 2.4. MTR

1. Pobierz narzędzie WinMTR ze strony *https://sourceforge.net/projects/winmtr/*.
2. Rozpakuj pobrane archiwum *.zip* i zapamiętaj lokalizację rozpakowanych plików.
3. Wybierz odpowiednią wersję oprogramowania dla swojego systemu i otwórz odpowiedni folder (*WinMTR_x32* z wersją 32-bitową lub *WinMTR_x64* z wersją 64-bitową).
4. Uruchom program *WinMTR.exe*. Zostanie wyświetlone okno aplikacji WinMTR — dokumentowanie uzyskanych informacji będzie łatwiejsze dzięki graficznemu interfejsowi.

5. W pole tekstowe *Host* (adres docelowy) wpisz wartość **8.8.8.8** i naciśnij przycisk *Start*. Przykładowy wynik działania przedstawiłam na rysunku 2.4.



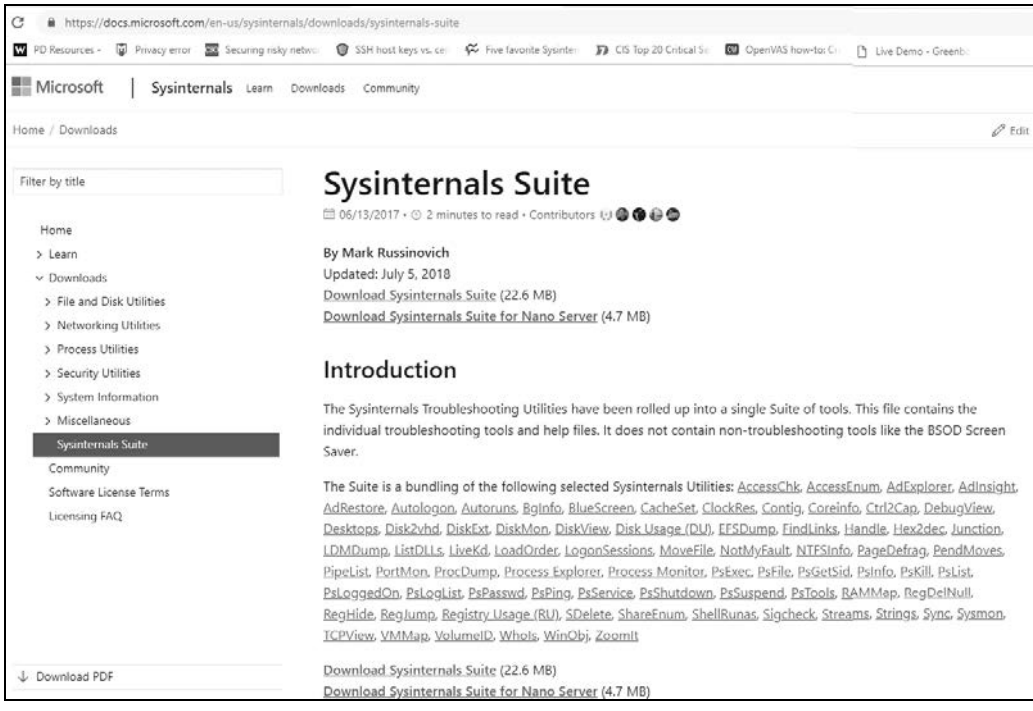
Rysunek 2.4. Narzędzie WinMTR łączące funkcjonalność ping i traceroute

6. Możesz zapisać uzyskane wyniki w pliku tekstowym (przycisk *Export TEXT*) lub HTML (przycisk *Export HTML*). Możesz też skopiować je do schowka (odpowiednio przyciski *Copy Text to clipboard* lub *Copy HTML to clipboard*).
7. Gdy dwukrotnie klikniesz nazwę lub adres węzła pośredniego, zostaną wyświetlone szczegółowe informacje o nim. Przycisk ze strzałką w dół po prawej stronie pola *Host* umożliwia przejrzenie lub wyczyszczenie historii badanych adresów.

Sysinternals

Portal Microsoft Docs jest prawdziwą kopalnią informacji na tematy techniczne związane z produktami firmy Microsoft. Serwis dostępny jest pod adresem *https://docs.microsoft.com/* i można w nim znaleźć wiele darmowych szkoleń, bibliotek, narzędzi, dokumentacji i artykułów oraz porad w rozwiązywaniu problemów. Wcześniej podobne treści firma Microsoft oferowała w ramach portalu TechNet, ale w 2013 roku został on zamknięty. Próba dostępu do adresu starego portalu spowoduje przeniesienie na stronę Microsoft Docs. Szukasz dokumentacji kodów błędów i identyfikatorów zdarzeń wyświetlanych na „niebieskim ekranie śmierci", gdy Twój komputer napotka awarię? Udaj się do portalu Microsoft Docs! Szukasz programów użytkowych usprawniających zarządzanie komputerami pod kontrolą systemu Windows, ich diagnozowanie i usuwanie z nich problemów? Udaj się do Microsoft Docs!

Najszybszym sposobem znalezienia pakietu narzędzi Sysinternals jest odwiedzenie strony Microsoft Docs i wyszukanie go z wykorzystaniem pola wyszukania znajdującego się w prawym górnym rogu. Pakiet Sysinternals łączy wiele małych programów w jedno wielkie, cudowne narzędzie. Na rysunku 2.5 pokazałam widok strony pobierania tego narzędzia. Jedną z największych zalet pakietu Sysinternals jest jego przenośność. Nie trzeba nic instalować — możesz cały pakiet zachować na dysku USB i uruchamiać na dowolnym komputerze.



Rysunek 2.5. Strona pobierania pakietu Microsoft Sysinternals

Pakiet zawiera między innymi narzędzie Process Explorer, które jest bardzo podobne do Menedżera zadań (*Task Manager*), tylko ma całą masę dodatkowych funkcjonalności. W pakiecie znajdziesz też narzędzie Autoruns, które pomaga w zarządzaniu procesem startu systemu operacyjnego. Kolejnym ciekawym narzędziem w pakiecie jest PsExec, które jest prostym zastępnikiem programu `telnet`. Jednym z moich ulubionych narzędzi jest Notmyfault. Serio, narzędzie nazywa się „to nie moja wina". Możesz używać go do analizy nagle zatrzymujących się aplikacji lub wycieków pamięci w jądrze systemu — stanowi nieocenioną pomoc przy diagnozowaniu problemów ze sterownikami urządzeń. Przynajmniej połowa „niebieskich ekranów śmierci", z którymi miałam styczność, wynikała właśnie z takich problemów. W ćwiczeniu 2.5 dowiesz się, jak używać pakietu Sysinternals.

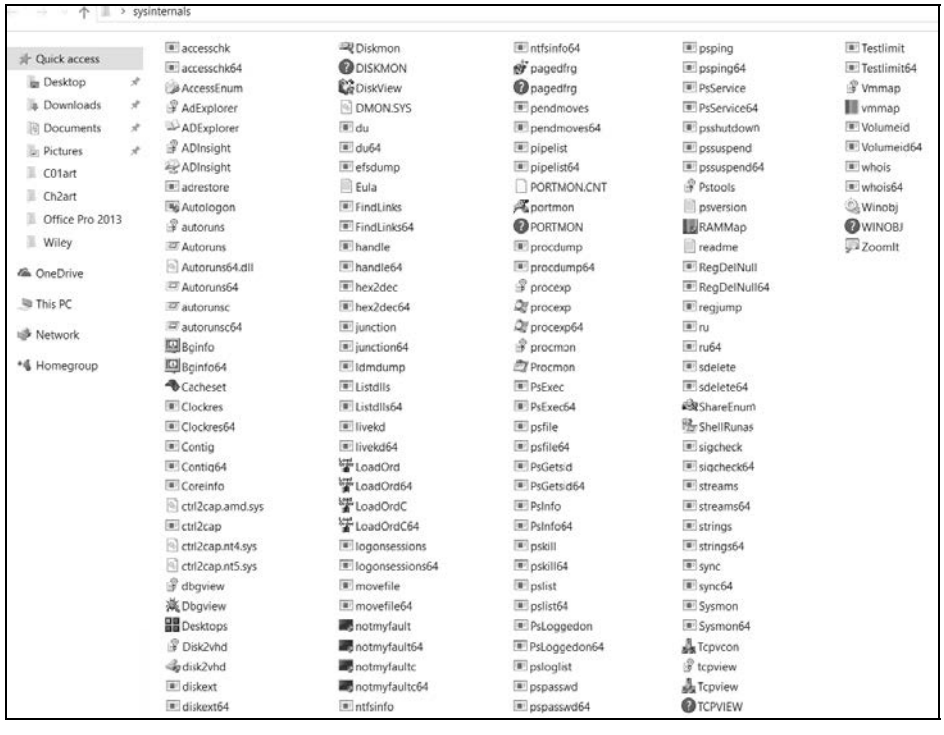
W pakiecie jest tak wiele cudownych narzędzi, że trudno się zdecydować, od którego zacząć. Poniżej zamieszczam listę narzędzi, których sama używam regularnie albo których może nie używam zbyt często, ale były mi bardzo pomocne w pewnych sytuacjach.

- **Process Explorer**. To narzędzie wykorzystuję chyba najczęściej z całego pakietu. To proste narzędzie, ale dostarcza Ci informacji na temat każdego procesu, każdej biblioteki DLL oraz każdej aktywności, które działają na Twoim komputerze. Na rysunku 2.7 pokazałam przykładowy widok listy procesów zawierający statystyki użycia procesora, numery identyfikacyjne procesów (PID) oraz pozostałe informacje. Process Explorer umożliwia Ci weryfikację każdego procesu z listy w serwisie VirusTotal, co jest szczególnie przydatne, gdy podejrzewasz, że do Twojego komputera dokonano włamania i jeden z procesów jest szkodliwym narzędziem.

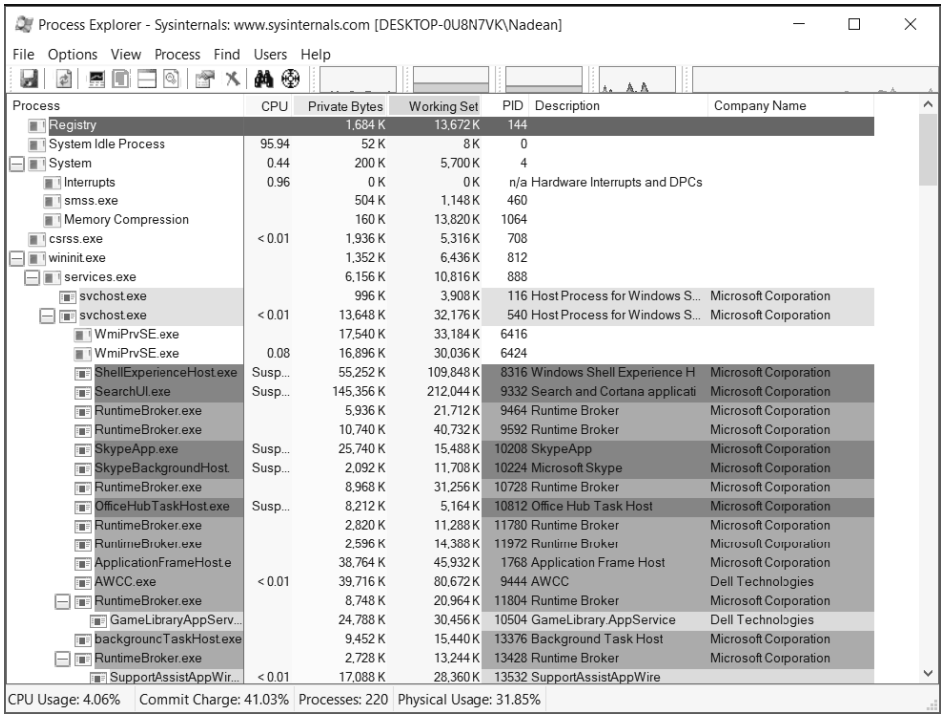
ĆWICZENIE 2.5. SYSINTERNALS

1. Uruchom przeglądarkę i przejdź do strony *https://docs.microsoft.com/*.
2. W polu wyszukania wpisz **`Sysinternals`**. Pierwszym uzyskanym wynikiem powinna być strona pobierania pakietu (*Download Sysinternals Suite*)

   Spakowane archiwum z pakietem zajmuje około 24 MB. Rozpakowany pakiet zajmuje około 60 MB i bez problemu zmieści się na dysku USB.
3. Zapisz plik na dysku i wypakuj całą zawartość. Dobrze zapamiętaj folder, w którym znalazły się pliki pakietu (mówię to tylko dlatego, że sama ciągle mam problem z umiejscowieniem moich narzędzi).
4. Po rozpakowaniu narzędzi przejdź do folderu zawierającego pakiet i zmień widok w Eksploratorze plików (*File Explorer*) na widok listy. Przykładowy widok zamieściłam na rysunku 2.6. Dzięki temu wszystkie narzędzia będą mogły być wyświetlone na jednym ekranie.



Rysunek 2.6. Lista wszystkich składowych pakietu Sysinternals



Rysunek 2.7. Widok narzędzia Process Explorer z pakietu Sysinternals

- **PsList**. Jednym ze sposobów, by zobaczyć listę procesów uruchomionych na komputerze, jest naciśnięcie klawiszy *Ctrl+Alt+Delete* i uruchomienie Menedżera zadań. To wspaniałe narzędzie, ale działa wyłącznie na lokalnej maszynie. Korzystając z PsList, możesz zdalnie sprawdzić listę procesów uruchomionych na innym komputerze.
- **PsKill**. Za pomocą tego programu możesz zakończyć wybrany proces działający na Twoim lokalnym komputerze lub na zdalnej maszynie. Odszukaj identyfikator procesu, korzystając z PsList, a następnie zakończ go przy użyciu PsKill.
- **Autoruns**. Szkodliwe oprogramowanie jest prawdziwą zmorą każdego informatyka. Niektóre takie programy dopisują się do listy aplikacji uruchamianych automatycznie przy starcie systemu. Program Autoruns pomoże Ci zapanować nad automatycznie uruchamianymi aplikacjami, pokazując wszystkie, niezależnie od sposobu dodania do listy samoczynnego startu. Zastosowanie filtrów umożliwia ukrycie wszystkich pożądanych aplikacji i skupienie się na tych, które są potencjalnie niebezpieczne.
- **ZoomIt**. To narzędzie pozwala powiększyć obraz na wybranym fragmencie ekranu. Integruje się z PowerPointem, więc możesz aktywować jego funkcję podczas prezentacji, korzystając z dedykowanych przycisków. Możesz włączyć aktywne powiększanie wybranego obszaru, powiększanie obszaru rysowania lub wpisywania tekstu, a nawet możesz skonfigurować licznik czasu, na przykład by włączyć odliczanie czasu do końca przerwy.
- **PsLoggedOn**. To narzędzie odszukuje użytkowników zalogowanych w systemie. Jego działanie jest oparte na przeszukaniu rejestru systemowego (klucz `HKEY_USERS`) w celu

znalezienia załadowanych profili. Jest to szczególnie przydatne, gdy musisz się dowiedzieć, kto ma uruchomione połączenie z badanym komputerem.

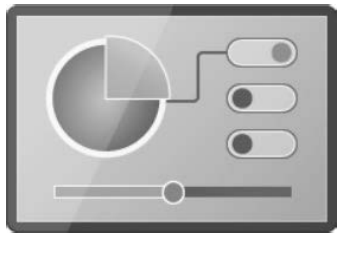
- **SDelete**. Tego narzędzia raczej nie będziesz potrzebować zbyt często, ale bywa bardzo przydatne. Służy do trwałego usuwania plików, aby nawet najlepsze narzędzia do odzyskiwania danych nie mogły przywrócić usuniętych treści. Narzędzie SDelete nadpisuje zerami sektory dysku, na których znajduje się usuwany plik lub folder. Jeżeli kiedykolwiek będziesz chciał trwale usunąć plik lub folder, to wiesz już, czego użyć.
- **PsExec**. Czasem potrzebne jest zdalne uruchomienie programów na innych komputerach. Połączenie `telnet`, realizowane na porcie o numerze 23, przesyła przez sieć nieszyfrowane dane logowania. Znacznie lepszym rozwiązaniem jest program PsExec, który umożliwia wykonanie poleceń na zdalnej maszynie bez konieczności instalowania innego oprogramowania. Możesz w ten sposób uruchomić interaktywny wiersz poleceń lub włączać inne narzędzia na zdalnym komputerze.
- **Notmyfault**. W przypadku gdy wydajność serwera jest znacznie poniżej oczekiwań lub zgłaszane są błędy o braku dostępnych zasobów, to za pomocą narzędzia Notmyfault możesz zdiagnozować bardziej zaawansowane problemy z wydajnością systemu i aplikacji, a także zbadać powody awaryjnych wyłączeń procesów.

Windows Master Control Panel

Moje pierwsze doświadczenie z nieśmiertelnością nastąpiło w 1993 roku, gdy zaczęłam grać w grę *Doom*. Była to strzelanka prowadzona z perspektywy pierwszej osoby, składająca się z dziewięciu poziomów. Gracz wcielał się w postać kosmicznego komandosa, nazywanego DoomGuy, który niespodziewanie znalazł się w Piekle. W grze dostępne były kody ułatwiające rozgrywkę. Po wpisaniu jednego z nich, `IDBEHOLDV`, postać gracza stawała się nieśmiertelna i odporna na strzały przeciwników. Tryb gry z włączoną nieśmiertelnością nazywany jest „God mode".

W 2007 roku, razem z debiutem Windows 7, zostało opublikowane narzędzie nazywane *God mode* („tryb Boga"). Jego oficjalna nazwa to Windows Master Control Panel, ale osobiście uważam, że nazwa *God mode* jest znacznie bardziej imponująca.

Narzędzie Windows Master Control Panel umożliwia dostęp do wszystkich okien konfiguracyjnych systemu operacyjnego z jednego folderu. Narzędzie to można też aktywować w systemie Windows 8.1 oraz Windows 10. Jest ono bardzo przydatne osobom zarządzającym komputerem lub zaawansowanym ekspertom systemu Windows. Po aktywacji narzędzia zostanie utworzony folder, z którego będziesz mieć dostęp do każdego, bez wyjątków, ustawienia systemu Windows. Na rysunku 2.8 przedstawiłam ikonę tworzonego folderu.



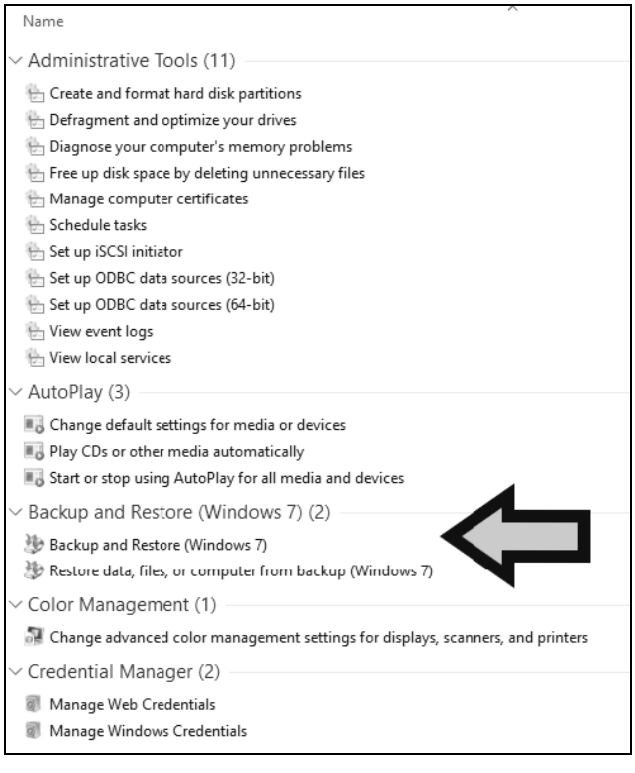
Rysunek 2.8. Ikona folderu Windows Master Control Panel

W ćwiczeniu 2.6 będziesz mógł samodzielnie włączyć narzędzie Windows Master Control Panel.

ĆWICZENIE 2.6. AKTYWACJA NARZĘDZIA WINDOWS MASTER CONTROL PANEL

1. Upewnij się, że jesteś zalogowany z prawami administratora.
2. Kliknij prawym przyciskiem myszy w obszarze pulpitu i wybierz opcję *Nowy/Folder* (*New/Folder*)
3. Nadaj nowo utworzonemu folderowi nazwę **`GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}`**.
4. Naciśnij *Enter* i kliknij dwukrotnie ikonę folderu *Windows Master Control Panel*, aby go otworzyć.

Nie jest to może aż tak ekscytujące jak nieśmiertelność w grze *Doom*, ale zgrupowanie wszystkich narzędzi w jednym miejscu jest całkiem niesamowite. Koniecznie wykonaj kopię zapasową danych z komputera, zanim zaczniesz eksperymentować z dostępnymi narzędziami. Na rysunku 2.9 pokazałam przykładowy spis dostępnych operacji. Jedną z nich jest polecenie *Kopia zapasowa i przywracanie* (*Backup and Restore*).



Rysunek 2.9. Przykład kilku z ponad dwustu narzędzi dostępnych w folderze God mode

Użyj właściwego narzędzia we właściwym czasie — i we właściwy sposób!

Zapewnienie bezpieczeństwa IT spędza sen z powiek nie tylko inżynierom, ale również menedżerom i kierownictwu organizacji. W tym zadaniu mają im pomóc różnorodne narzędzia, jednak ich skuteczne wykorzystanie wymaga nie tylko wyrafinowanej wiedzy technicznej. Konieczne jest nieco szersze spojrzenie na sprawy cyberbezpieczeństwa, aby zastosować właściwe strategie obronne i środki zaradcze. By podejmować trafne decyzje, potrzebna jest wiedza o najlepszych praktykach cyberbezpieczeństwa i o dostępnych narzędziach.

Ta książka to wszechstronny i praktyczny podręcznik dla kierowników i inżynierów. Opisuje różnorodne metody, platformy i technologie pochodzące od wielu dostawców, zawiera też wskazówki, jak je wykorzystać do tworzenia optymalnych rozwiązań. Przedstawiono tu pożyteczne informacje o sieciach komputerowych, podstawowych narzędziach bezpieczeństwa, rozwiązywaniu problemów w systemie Windows, inwentaryzacji sieci, zarządzaniu podatnościami, bezpieczeństwie aplikacji internetowych, zarządzaniu aktualizacjami i konfiguracją oraz wiele innych kwestii. Książka jest równocześnie treściwa i prosta w odbiorze, pozwala zapoznać się z aspektami technicznymi i nietechnicznymi, z teorią i praktyką cyberbezpieczeństwa — z pewnością ułatwi naukę metod oceny zagrożeń oraz sprawdzania i poprawiania stosowanej konfiguracji.

© Brian Lewis

Nadean H. Tanner od ponad 20 lat zajmuje się branżą technologiczną, w tym rozwojem aplikacji, sprzętem, marketingiem i szkoleniami. Doradzała największym firmom z rankingu Fortune 500 i szkoliła pracowników Departamentu Obrony USA z zakresu zaawansowanego cyberbezpieczeństwa. Obecnie jest głównym szkoleniowcem w firmie Rapid7.

W książce znajdziesz:

- teoretyczne i praktyczne aspekty bezpieczeństwa informatycznego
- skuteczne strategie obronne
- rodzaje narzędzi zapewniających cyberbezpieczeństwo
- zastosowanie takich narzędzi jak PuTTY, pathping, sysinternals®, NMAP®, OpenVAS, Metasploit® i WireShark®
- budowanie i korzystanie z wirtualnego laboratorium cyberbezpieczeństwa

ISBN 978-83-283-7368-6

Cena: 69,00 zł

WILEY