

Packetyzer dla MS Windows

Paweł Wawrzyniak

p.wawrzyniak@it-faq.pl

16 maja 2005

Ciekawa alternatywa dla sniffera Ethereal

Packetyzer dla MS Windows

Wśród darmowych rozwiązań ułatwiających sniffing w sieciach lokalnych wyróżnia się Ethereal, który dostępny jest w wersjach dla systemów uniksowych oraz MS Windows. Program ten jest rozwijany na zasadach Open Source i rozpowszechniany na licencji GNU GPL. Charakteryzuje go bogactwo dostępnych funkcji oraz wygodny graficzny interfejs użytkownika, który

Wśród darmowych rozwiązań ułatwiających sniffing w sieciach lokalnych wyróżnia się Ethereal, który dostępny jest w wersjach dla systemów uniksowych oraz MS Windows. Charakteryzuje go bogactwo dostępnych funkcji oraz wygodny graficzny interfejs użytkownika, który wykorzystuje wieloplatformową bibliotekę GTK+. Jeśli jednak nie odpowiada nam GUI oparte na GTK+, a naszym systemem jest MS Windows, możemy skorzystać z alternatywnego rozwiązania jakim jest Packetyzer opracowany przez firmę Network Chemistry.

wykorzystuje wieloplatformową bibliotekę GTK+. Jeśli jednak nie odpowiada nam GUI oparte na GTK+, a naszym systemem jest MS Windows, możemy skorzystać z alternatywnego rozwiązania jakim jest Packetyzer opracowany przez firmę Network Chemistry. Ponadto, program ten oferuje kilka dodatkowych funkcji.

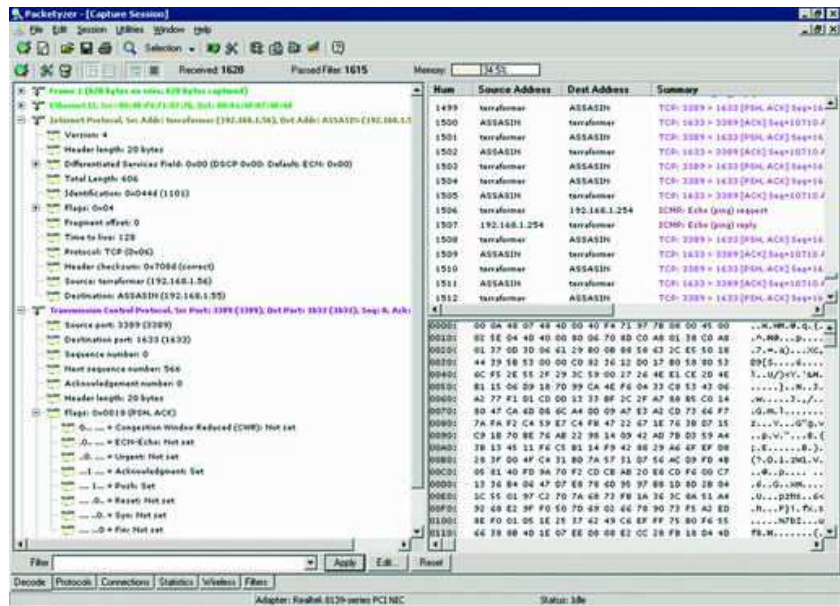
Czym jest Packetyzer?

Packetyzer to nakładka graficzna (ang. frontend) na bibliotekę ethereal.dll (będącą także podstawą sniffera Ethereal dla MS Windows - libethereal.dll), służącą do przechwytywania i analizy pakietów sieciowych. Interfejs programu wykorzystuje standardowe elementy graficzne MS Windows (nakładkę napisano za pomocą Borland C++ Buildera), stąd nie jest konieczna instalacja GTK+. Dodatkowo GUI Packetyзера zostało zreorganizowane i wydaje się być bardziej przejrzyste - z czym oczywiście nie muszą zgadzać się dotychczasowi użytkownicy Ethereala. Packetyzer oferuje bardzo zbliżoną funkcjonalność do sniffera Ethereal. Warto jednak zauważyć, że jego rozwój zwykle znajduje się krok wstecz w stosunku do Ethereala. W chwili pisania tego artykułu najnowsza edycja sniffera Ethereal nosiła numer 0.10.4, a opisywana wersja Packetyзера 2.0.0 została stworzona w oparciu o bibliotekę ethereal.dll 0.10.3. W większości przypadków nie powinno to jednak oznaczać jakichkolwiek problemów. Oprócz biblioteki ethereal.dll Packetyzer wymaga instalacji popularnej w tego typu programach biblioteki WinPcap. Wersja 2.0.0 programu jest dostarczana wraz z WinPcap w wersji 3.01a. Nie oznacza to jednak, że nie można wykorzystać innego wydania WinPcap, np. 3.1b3, choć znane są przypadki nieprawidłowego działania programu w niektórych systemach (użytkownicy Standardy i protokoły Obsługiwane protokoły i standardy Wśród 483 obsługiwanych przez Packetyзера protokołów można wyróżnić m.in.: Address Resolution Protocol (ARP), ATM, Data Link Switching, DCE RPC, Domain Name Service (DNS), Ethernet over IP (EoIP), Ethernet, File Transfer Protocol (FTP), Gnutella Protocol, Interbase, ICMPv4/ICMPv6, Internet Printing Protocol (IPP), Internet Protocol (IPv4/IPv6), Internet Relay Chat (IRC), Kerberos, Microsoft Directory Replication Service, Microsoft Distributed File System, Microsoft Exchange MAPI, Microsoft Local Security Architecture, Microsoft Messenger Service, Microsoft Network Logon, Microsoft Registry, Microsoft Security Account Manager, Microsoft Server Service, Microsoft Service Control, Microsoft Spool Subsystem, Microsoft Task Scheduler Service, Microsoft Telephony API Service, Microsoft Windows Browser Protocol, Microsoft Windows Lanman Remote API Protocol, Microsoft Windows Logon Protocol, Microsoft Workstation Service, NetBIOS, MySQL Protocol, Post Office Protocol 3 (POP3), Point to Point Protocol (PPP), Radius Protocol, Rlogin Protocol, Secure Socket Layer (SSL), SMB, Transmission Control Protocol (TCP), Trivial File Transfer Protocol, TFTP. Jeżeli chodzi o współpracę z innymi narzędziami, to za pomocą Packetyзера można analizować pakiety przechwycone i zapisane w plikach przez m.in.: tcpdump, Ethereal, Novell LANalyzer, Network Associates Sniffer (skompresowane i nieskompresowane), Microsoft Network Monitor, Sniffer Pro, wyjściowe pliki do debuggowania z routerów Lucent/Ascend, wyjście (zrzut pakietów) z routerów ISDN firmy Toshiba, Etherpeek i Airoppeek. Packetyzer 2.0.0 pozwala także wykorzystywać wtyczki dostępne dla wersji Ethereala, na której został oparty. Pełna ich lista znajduje się w katalogu \Packetyzer\plugins\0.10.3. modemów powinni np. skorzystać z biblioteki WinPcap w wersji 2.3, dzięki czemu będą mieć możliwość sniffowania, ponieważ wersje 3.x biblioteki nie obsługują połączeń dialup). Packetyzer może być zainstalowany w systemach Windows 9x/Me/NT/2000/XP/ Server 2003. Wszystkie niezbędne biblioteki (WinPcap, ethereal.dll) wchodzi w skład pakietu instalacyjnego Packetyзера. Podobnie jak pierwowzór - Ethereal - Packetyzer rozprowadzany jest na licencji GNU GPL. Adresy, pod którymi można odnaleźć obydwa programy podano w ramce Narzędzia. Packetyzer ma możliwość rozpoznawania i dekodowania pakietów przesyłanych za pomocą 483 protokołów (wybrane z nich przedstawiono w ramce Obsługiwane protokoły i standardy).

Interfejs obsługi

Packetyzer posiada bardzo wygodny i przejrzysty interfejs obsługi. Główne okno składa się z kilku części - poniżej menu programu i paska narzędzi, który zawiera skróty do najczęściej wykorzystywanych opcji, mamy trzy pola. W lewym (największym) prezentowane są zdekodowane informacje pochodzące z przechwyconego i wskazanego w prawym, górnym polu pakietu. Prawe, dolne pole pokazuje surową (ang. raw) zawartość przechwyconej ramki. Poniżej znajdują się opcje dotyczące filtrowania pakietów oraz sześć zakładek, pozwalających przełączać się do innych widoków (patrz Rys. 1):

- **Decode** - główny widok, pozwalający podglądać zdekodowaną zawartość ramek,
- **Protocols** - widok przedstawiający statystyczne zestawienie wykorzystywanych przez przechwycone ramki protokołów,



Rys. 1: Główny widok Packetyзера po zakończonej sesji przechwytywania. Widać najważniejsze części interfejsu

- **Connections** - widok ukazujący statystyczne zestawienie wykorzystywanych protokołów w poszczególnych, monitorowanych połączeniach pomiędzy maszynami,
- **Statistics** - statystyki dotyczące aktywnej sesji przechwytywania (General - ogólne, 802.11 - związane z przechwytywaniem pakietów w sieciach WLAN),
- **Wireless** - widok związany z przechwytywaniem pakietów w sieciach WLAN,
- **Filters** - podgląd dostępnych dla programu filtrów (zdefiniowanych przez producenta jak i dodanych przez użytkownika).

W każdym z pól możliwe jest wykorzystanie prawego przycisku myszy. Dzięki temu, jeżeli można wykonywać na wskazanym polu dodatkowe operacje, wyświetlane jest menu kontekstowe zawierające skróty do odpowiednich funkcji. Jeśli np. po zakończeniu sesji przechwytywania ramek chcemy wskazać wybrany pakiet i odfiltrować wyłącznie pakiety, które mu odpowiadają (o identycznej budowie), wystarczy kliknąć prawym przyciskiem myszy na wybranym pakiecie i wybrać z menu kontekstowego opcję Create Filter from Packet.... Wówczas zostanie otworzone okno Filter Designera, w którym znajdować się będzie wygenerowane wyrażenie filtrujące. Po dokonaniu wymaganych zmian i zapisaniu filtra będzie można go w dowolnej chwili wykorzystać. Na podobnej zasadzie funkcjonuje dostęp do pozostałych opcji, np. edytora pakietów - wystarczy wskazać ramkę i wybrać z menu kontekstowego pozycję Packet Editor. Zostaniemy przełączeni do okna, w którym możemy zmieniać zawartość przechwyconego pakietu i - ewentualnie - odesłać (wstrzyknąć) go do sieci.

Konfiguracja programu

Zanim jednak będziemy mogli rozpocząć sesję przechwytywania ramek według ustalonych reguł, należy przygotować konfigurację programu. Do najważniejszych opcji dotyczących pracy Packetyзера mamy dostęp poprzez pasek narzędzi (ikona Modify Global Options) lub za pomocą menu: Edit->Global Options. Opcje zgrupowane są w następujących zakładkach:

- **Global** - tutaj ustawiamy opcje, które będą obowiązywać w przypadku wszystkich sesji przechwytywania:
 - **Name Resolution** - grupa opcji pozwalających na włączenie lub wyłączenie rozwiązywania nazw/adresów. Dostępne opcje to: Resolve MAC Addresses, Resolve network addresses i Resolve transport names,
 - **Ask before closing session** - pytanie o potwierdzenie przed zakończeniem sesji,
 - **Analyze packets when loading a file** - włączenie opcji sprawia, że podczas wczytywania pliku zawierającego wcześniej przechwycone pakiety będą one na bieżąco poddawane analizie.
- **Default Capture** - opcje domyślne dla bieżącej sesji przechwytywania:
 - **Adapter** - pozwala wskazać interfejs sieciowy, za pomocą którego będziemy przechwytywać pakiety; jeżeli w systemie jest kilka kart sieciowych, można wskazać odpowiednią z listy rozwijanej,
 - **Capture name** - pozwala określić nazwę dla pliku, w którym zachowywane będą przechwytywane pakiety,
 - **Limit each packet to** - umożliwia określenie limitu danych przechwyconych w każdym pakiecie. W większości przypadków nie ma potrzeby przechwytywania całych pakietów, gdyż podczas diagnozowania problemów z siecią wystarczą nam jedynie nagłówki ramek. Dane użytkownika nie mają wówczas żadnego znaczenia, a przechwytywanie mniejszej ilości danych trwa krócej i jest bardziej efektywne. Kwestia wygląda zupełnie inaczej, jeżeli mamy zamiar podglądać komunikację między użytkownikami (np. hasła używane do uwierzytelniania itp.),
 - **Capture packets in promiscuous mode** - oznacza przechwytywanie pakietów przez interfejs programowo przełączony w tryb pracy bezładnej (ang. promiscuous), który pozwala odbierać wszystkie pakiety docierające do wybranego interfejsu sieciowego, nawet jeśli nie są zaadresowane bezpośrednio do maszyny podsłuchującej. Jeżeli chcemy przechwytywać tylko ruch dotyczący lokalnego komputera, możemy wyłączyć tę opcję,

- **Automatic scrolling during capture** - jeśli opcja jest włączona, prawe górne okno na zakładce Decode będzie przesuwane się automatycznie w miarę, jak łapane będą kolejne pakiety,
- **Limit total capture to** - określanie maksymalnej wielkości pliku bufora dla przechwyconych pakietów,
- **Reuse capture buffer when it is full** - ta opcja pozwala ponownie wykorzystać zapełniony bufor. Jeżeli jest zaznaczona, to w momencie, kiedy podczas sesji przechwytywania bufor zostanie zapełniony, a pojawią się nowe pakiety, bufor będzie zapisywany od początku (pierwszy nowy pakiet na miejscu pierwszego w buforze, drugi nowy pakiet na miejscu drugiego w buforze itd.).
- **Protocol Options** - w liście rozwijanej mamy dostęp do wszystkich obsługiwanych przez Packetyzer protokołów. Po wskazaniu dowolnego z nich, wyświetlone zostają dodatkowe opcje konfiguracyjne, charakterystyczne tylko dla niego, np. w przypadku protokołu IPv4 możemy ustalić, czy pole TOS (ang. Type of Service) nagłówka ma być traktowane w sposób tradycyjny, czy jako pole DS (ang. Differentiated Services). W oparciu o te ustawienia interpretowane będą dane z przechwyconych pakietów.
- **WLAN Options** - tutaj można ustawiać opcje i parametry związane z pracą Packetyзера w sieciach WLAN.

Jeśli zamierzamy wprowadzić zmiany w ustawieniach dotyczących przechwytywania dla konkretnej sesji, należy skorzystać z ikony Change Capture Options na pasku narzędzi (lub wybrać menu Session->Capture Options). Dostępne opcje odpowiadają tym, które grupuje zakładka Default Capture w ustawieniach globalnych, jednak wprowadzone zmiany obowiązywać będą tylko wskazaną sesję.

Łapanie pakietów

Po uruchomieniu programu, wskazaniu interfejsu, który ma posłużyć do pracy i określeniu opcji przechwytywania możemy rozpocząć nową sesję. W tym celu wystarczy kliknąć ikonę Start the current capture na pasku skrótów. Rozpocznie się przechwytywanie, podczas którego stopniowo będą uzupełniane informacje we wszystkich trzech polach okna głównego. Podczas pracy stosowane będą reguły filtrowania, więc jeśli nie zostały one do tej pory zdefiniowane przez użytkownika, program będzie starał się przechwycić wszystkie pakiety. Jeśli jednak obowiązują jakieś filtry, to przechwytywane będą tylko te pakiety, które spełniają zawarte w nich kryteria. Podczas procesu przechwytywania aktualizowane będą także następujące informacje:

- **Received** - oznacza ilość przechwyconych pakietów,
- **Passed Filter** - oznacza ilość pakietów, które zostały przechwycone, gdyż spełniały kryteria zdefiniowane w filtrach,
- **Memory** - wskaźnik zajętości ustalonego bufora.

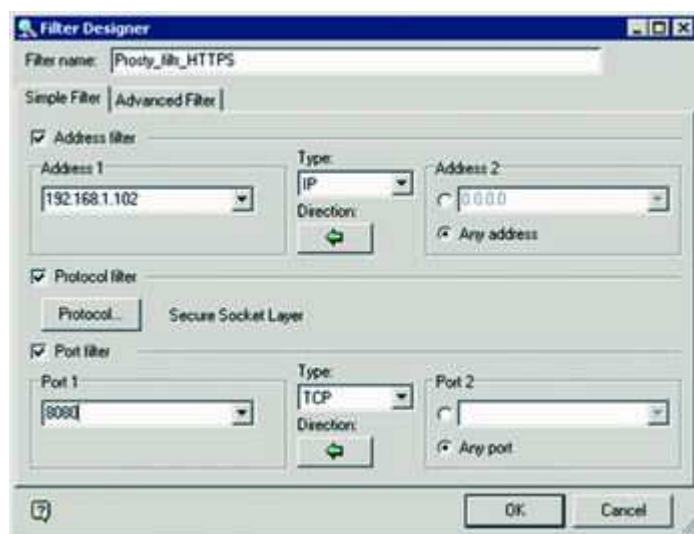
W zależności od tego, jak ściśle są reguły filtrowania, pakietów może być bardzo dużo lub mogą one pojawiać się bardzo rzadko. Oznacza to, że umiejętny dobór warunków filtrowania jest istotny, gdyż nadmiar informacji może utrudnić pracę. Zagadnienie to omówimy jeszcze dokładniej w dalszej części tekstu.

Teraz możemy zatrzymać pierwszą sesję i dostosować warunki pracy, w tym zdefiniować odpowiednie filtry. Wystarczy wcisnąć ikonę Stop the current capture na pasku skrótów (efekt zakończenia sesji będzie zbliżony do pokazanego na Rys. 1).

Filtrowanie pakietów

Podobnie jak Ethereal, Packetyzer oferuje wielkie możliwości związane z filtrowaniem przechwyconych pakietów. Użytkownik może dowolnie definiować reguły filtrowania z wykorzystaniem określonych adresów IP lub MAC, protokołów, numerów portów i operatorów logicznych lub wyrażeń (np. equal to - równe z, not equal to - różne od). W zależności od poziomu opanowania programu, można definiować filtry poprzez wybieranie gotowych reguł lub pisać własne, złożone wyrażenia.

Filtry służące do przechwytywania pakietów pozwalają odrzucić te z nich, które nie spełniają określonych kryteriów. Jeśli jednak zakończyliśmy sesję i chcemy ograniczyć ilość danych, możemy wskazać (w pasku filtrowania na dole okna) określony filtr



Rys. 2: Okno Filter Designer podczas edycji własnego filtra

związany z wyświetlaniem przechwyconych pakietów. Oba typy filtrów używają identycznej składni. Ponadto, jest ona całkowicie zgodna ze składnią znaną z Ethereala (co zresztą nie może dziwić), więc dotychczasowi użytkownicy tego programu mogą bez problemu używać własnych filtrów.

Jak stworzyć filtr pozwalający odrzucić zbędne pakiety podczas przechwytywania? Pierwsza możliwość, o której już wspominaliśmy, to utworzenie filtra na podstawie struktury przechwyconego pakietu. Wystarczy wskazać prawym przyciskiem myszy interesujący nas typ pakietów i z menu kontekstowego wybrać pozycję Create Filter from Packet..., a następnie zmodyfikować według własnych potrzeb wygenerowane na podstawie pakietu wyrażenie filtrujące. To prosty sposób tworzenia całkiem użytecznych filtrów, ale możliwości w tym zakresie są znacznie większe. Zajmiemy się teraz opracowaniem własnego filtra. Na początek należy przejść na zakładkę Filters (na dole głównego okna). Teraz wybieramy przycisk Create a new filter, aby otworzyć Filter Designera (patrz Rys. 2). Okno projektanta filtrów zawiera dwie zakładki:

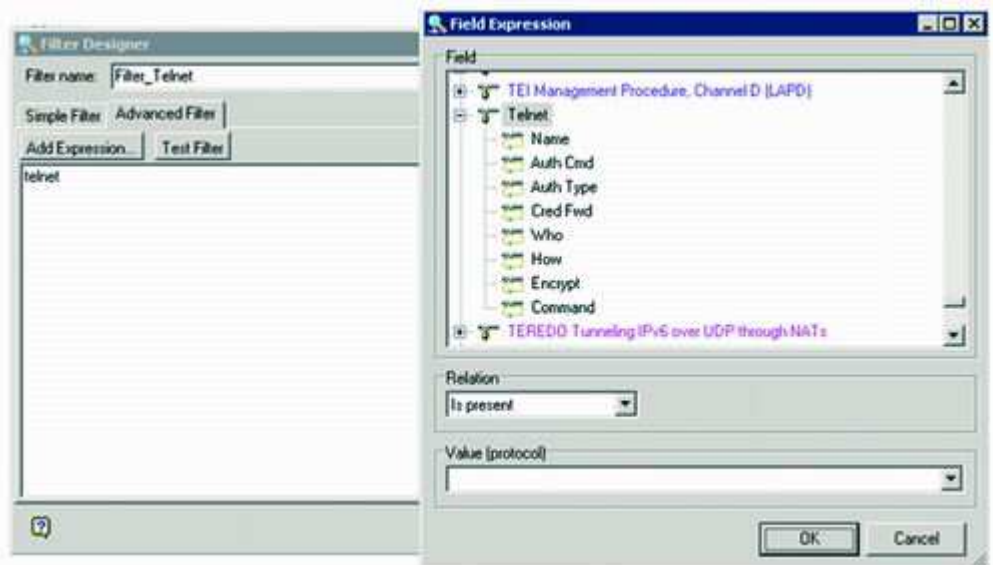
Simple Filter oraz Advanced Filter. Za pomocą ustawień na pierwszej z nich można bardzo szybko

wygenerować nawet dość złożone wyrażenie filtrujące. Druga pozwala wpisywać wyrażenia bezpośrednio oraz testować ich poprawność. Zajmiemy się teraz zakładką Simple Filter – mamy tutaj następujące możliwości:

- **Address filter** (filtrowanie po adresach) - po wskazaniu tego pola wyboru określamy typ adresów (Type - IP lub MAC) oraz wpisujemy odpowiednie adresy w polach Address 1 i Address 2. W polu Address 2 można wskazać dowolny adres docelowy (Any address) lub wskazać konkretną maszynę. Następnie za pomocą przycisku Direction ustalamy kierunek przepływu pakietów, które zamierzamy przechwytywać (lub odfiltrować z już zakończonej sesji). Do wyboru mamy: Either direction (komunikacja obustronna), Address 1 to 2 i Address 2 to (dla wybranej strony komunikacji).
- **Protocol filter** (filtrowanie po protokołach) - po zaznaczeniu tego pola wyboru wciskamy przycisk Protocol. Otwarte zostanie okno Select Protocol zawierające listę wszystkich obsługiwanych protokołów. Wybieramy ten, który nas interesuje (np. telnet lub Post Office Protocol). Wybór potwierdzamy przyciskiem Select.
- **Port filter** (filtrowanie po numerze portu) - zaznaczamy pole wyboru filtra. Z listy rozwijanej wybieramy nazwę protokołu (jest ona powiązana z określonym portem) lub podajemy własny numer (np. 80 dla HTTP, 110 dla POP3 itd.). Następnie wskazujemy typ protokołu (czy jest on osadzony na protokole TCP czy UDP) w liście rozwijanej Type. Na końcu podajemy port docelowy w polu Port 2 - może to być konkretny lub dowolny port (Any port - opcja domyślna). Możemy także ustalić interesujący nas kierunek przechwytywanej komunikacji za pomocą przycisku Direction - analogicznie jak w przypadku filtrowania po adresach.

Jak widać użytkownik jest w stanie zbudować bardzo zaawansowany filtr wprowadzając odpowiednie kombinacje powyższych opcji. Aby mieć całkowitą pewność, że w wybranych przez nas kryteriach filtrowania nie wystąpił żaden błąd, warto przełączyć się na zakładkę Advanced Filter. Powinno być tutaj widoczne automatycznie wygenerowane wyrażenie, które można sprawdzić za pomocą opcji Test Filter. Jeśli występuje w nim jakiś błąd (np. logiczny) zostaniemy o tym poinformowani i będziemy mogli wprowadzić korektę. Na zakładce Advanced Filter możemy także wpisywać własne wyrażenia z ominięciem opcji dostępnych pod zakładką Simple Filter.

Zaawansowanym użytkownikom (np. Ethereala) daje znacznie większe możliwości. Łatwo też nauczyć się zasad pisania własnych wyrażeń filtrujących, ponieważ w edytorze mamy możliwość skorzystania z prostego kreatora dostępnego pod przyciskiem Add Expression... (patrz Rys. 3). Po jego wskazaniu pojawia się okno Field Expression, w którym kolejno określamy:



- **Zawartość pola (Field)** - z listy możemy

Rys. 3: Okno "Add Expression" kreatora wyrażeń filtrujących pozwala tworzyć je w sposób intuicyjny

wskazać dowolny obsługiwany protokół i po rozwinięciu gałęzi przy jego nazwie, dodatkowe pola, po których mają być filtrowane pakiety,

- **Relację (Relation)** - pozwala skojarzyć wyżej określone pole dla danego protokołu z oczekiwaną zawartością na zasadzie relacji logicznej lub porównania (np. "is present" - jest obecny, "==" - równa się, "!=" - nie równa się, "<=" - mniejszy lub równy itd.). Operatory dostępne w liście są zależne od wyboru dokonanego w sekcji Field.
- **Wartość pola (Value)** - tutaj podajemy wartość, która będzie służyła do wykonania operacji filtrowania. W zależności od ustawień w sekcji Field i wybranego operatora będziemy mieli do wyboru określone wartości, np. jeśli wskazaliśmy protokół telnet, wybraliśmy pole Command i określiliśmy relację na is present to w polu Value, do wyboru będą wyłącznie wartości liczbowe (1 byte unsigned - typu byte, bez znaku) od 0 do 6, odpowiadające następującym komendom sterującym: 0 - Auth, 1 -Reject, 2 - Accept, 3 - Response, 4 - Forward, 5 - Forward Accept, 6 - Forward Reject. Oczywiście jeśli wśród zdefiniowanych domyślnych wartości nie znajdują się te, których oczekujemy, można podawać własne.

Przykładowy filtr

Przykładowy filtr

Aby zdefiniować własny filtr przechwytyjący komunikację z użyciem protokołu telnet pomiędzy dwoma komputerami wykonamy następujące czynności:

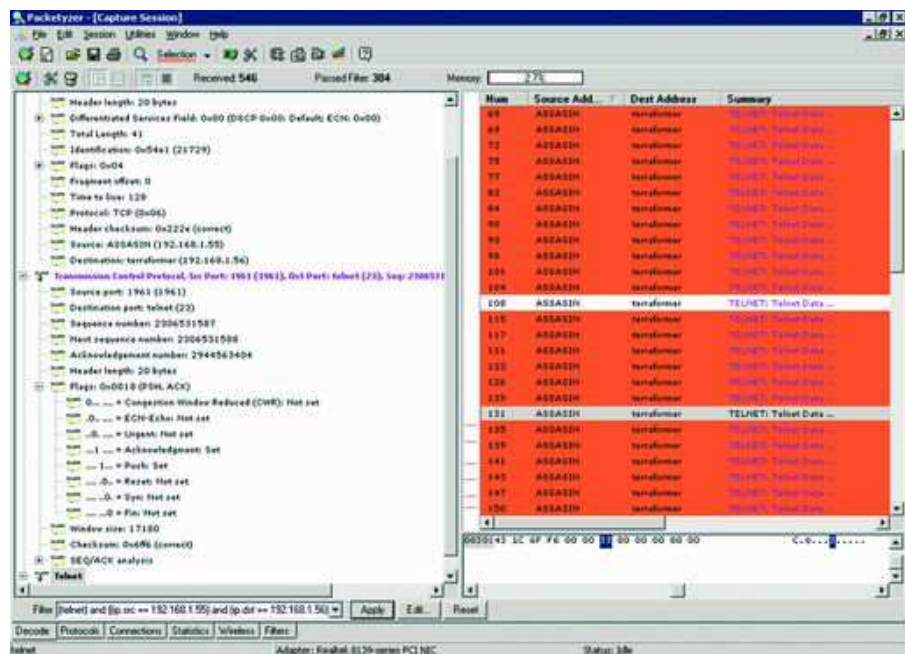
- Kliknij zakładkę Filters,
- kliknij przycisk Create a new filter,
- w oknie Filter Designera podaj nazwę swojego filtra, np.: telnet,
- klikamy pole wyboru Address Filter,
- w polu Address 1 podajemy adres IP: 192.168.1.55,
- w polu Address 2 podajemy adres IP: 192.168.1.56,
- przyciskiem Direction ustalamy kierunek komunikacji Address 1 to 2,
- kliknij pole wyboru Protocol, a następnie przycisk Protocol,
- wybierz protokół telnet z listy wyboru w oknie Select Protocol,
- przełącz się na zakładkę Advanced Filter i sprawdź poprawność wyrażenia (Test Filter),
- zapisz filtr - przycisk OK.

Nasze wyrażenie powinno wyglądać następująco:

(telnet) and ((ip.src == 192.168.1.55) and (ip.dst == 192.168.1.56))

Taki filtr spowoduje, że Packetyzer będzie przechwytywał wyłącznie pakiety kierowane z komputera 192.168.1.55 - klient telnet do komputera 192.168.1.56 - serwer telnet z wykorzystaniem protokołu telnet (lub ukryje wszystkie inne pakiety znajdujące się w buforze po zakończeniu sesji). Efekt działania filtra pokazano na Rys. 4.

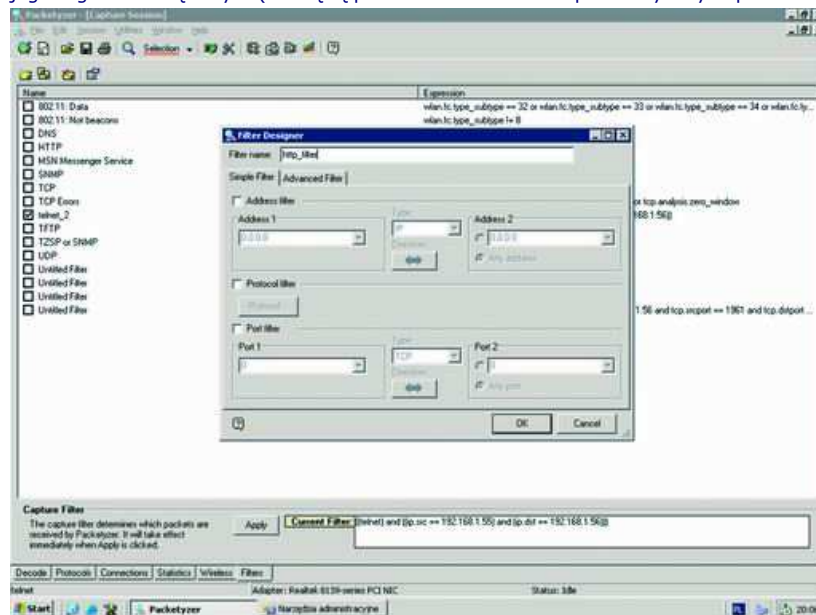
Po zdefiniowaniu filtra, należy jeszcze określić jego nazwę w polu Filter name - dzięki temu będzie można łatwo go zlokalizować. Przed zapisaniem gotowego filtra wykonujemy weryfikację poprawności wyrażenia za pomocą opcji Test filter. Kiedy zapiszemy własny filtr będzie on dostępny na liście wszystkich filtrów. Jeżeli chcemy skorzystać z dowolnego z nich należy przełączyć się na zakładkę Filters. Następnie w polach wyboru przy dostępnych filtrach oznaczamy te, które będą nam potrzebne i potwierdzamy wybór przyciskiem Apply. Jeśli chcemy, aby filtrowanie dotyczyło procesu przechwytywania pakietów, musimy rozpocząć nową sesję (przycisk Start Capture). Jeżeli już zakończyliśmy sesję przechwytywania i teraz chcemy ograniczyć liczbę



Rys. 4: Wynik sesji przechwytywania. Wykorzystano filtr dla połączeń telnet. Na pomarańczowo (opcja Selection) zaznaczono pakiety danych zawierające informacje użyte do uwierzytelniania (login i hasło)

wyświetlanych informacji, filtry zostaną użyte zaraz po ich zatwierdzeniu. Warto zauważyć, że podczas przechwytywania pakietów, jeśli wykorzystane zostało filtrowanie, wszystkie te, które nie spełniły kryteriów będą odrzucone. Natomiast, jeśli zakończyliśmy sesję i w buforze znajduje się jej zapis, to po zaaplikowaniu dowolnego filtra, te pakiety, które nie spełniają jego reguł zostaną ukryte (nie będą prezentowane na liście przechwyconych pakietów, znajdującej się w prawym górnym panelu głównego okna) - Paketyzator nie będzie ich usuwał z bufora.

Teraz, aby zastosować filtr wystarczy zaznaczyć go na liście. Jeżeli będziemy musieli zmodyfikować reguły filtrowania wskazujemy filtr i wciskamy przycisk View and modify the properties of the selected filter. Pojawi się okno Filter Designer, gdzie można wprowadzać zmiany. Oprócz dodawania i modyfikowania filtrów, można wykonywać na nich także takie operacje jak: usuwanie i duplikowanie. Wszystkie dostępne są pod zakładką Filters (patrz Rys. 5).



Dekodowanie pakietów

Dekodowanie pakietów odbywa się całkowicie automatycznie i nie wymaga żadnej interwencji ze strony użytkownika. Warto jednak mieć świadomość, że

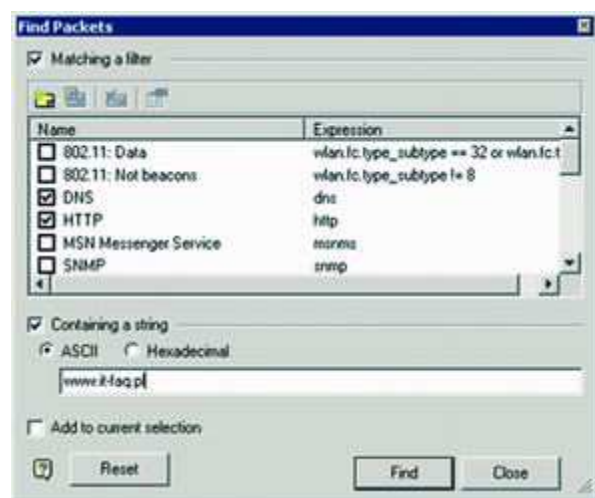
Rys. 5: Zakładka "Filters". Tutaj możemy wykonywać operacje na filtrach i dodawać te z nich, które mają być stosowane podczas sesji przechwytywania

proces ten zależy w pewnym sensie od ustawień dotyczących protokołów, które poczyniliśmy podczas konfigurowania opcji globalnych (Global Options). W zależności od nich interpretacja wyników może mieć nieco inny efekt. Zdekodowane pakiety są wyświetlane pod zakładką Decode. W podstawowym widoku prezentowane są kolejno: informacja pochodząca ze zdekodowanego pakietu (w postaci drzewa w lewym panelu), który został wskazany na liście wszystkich przechwyconych i przefiltrowanych pakietów (lista w prawym górnym panelu) oraz podgląd zawartości (heksadecymalny i ASCII - w prawym dolnym panelu). Po drzewie poruszamy się w standardowy sposób, rozwijając i zwiżając jego węzły. Pod prawym przyciskiem tego obszaru mamy dostęp do opcji menu kontekstowego (np. Expand all - rozwiń wszystkie węzły, Collapse all - zwiń wszystkie węzły). Kiedy klikamy na pozycje w drzewie, automatycznie w podglądzie HEX/ ASCII zaznaczany jest fragment pakietu, który odnosi się do wskazanych informacji. Przydatna jest także opcja zaznaczania pakietów kolorami - Selection, co pozwala je łatwo lokalizować podczas analizy. W widoku Decode możemy wykonywać wszelkie operacje edycyjne - kopiowanie, usuwanie pakietów itp. Jeżeli chcemy poddać pakiet modyfikacji, wystarczy wskazać pakiet w panelu zawierającym listę i wcisnąć przycisk Show the packet editor window. Wówczas zostaniemy przełączeni do edytora pakietów, który składa się z dwóch paneli. Górny zawiera drzewko prezentujące zdekodowane informacje - tutaj możemy lokalizować interesujące nas pola pakietu. Jeśli zamierzamy zmienić ich zawartość wykorzystujemy dolny panel, w którym przedstawiona jest zawartość pakietu (HEX/ASCII). Po wprowadzeniu dowolnych modyfikacji możemy spróbować odesłać pakiet do sieci (można np. zmienić adres docelowy odbiorcy) za pomocą przycisku Send One.

Wyszukiwanie pakietów

Podczas pracy z dużą ilością pakietów, pomimo możliwości łatwego ich lokalizowania, automatycznego dekodowania i zaawansowanych filtrów, wyszukiwanie specyficznych informacji może okazać się bardzo trudne. Paketyzator pozwala wyszukiwać pakiety zawierające określone przez użytkownika łańcuchy danych. Mechanizm wyszukiwawczy nie filtruje listy pakietów i nie zmienia sposobu ich wyświetlania. Pozwala on jedynie podświetlić te pakiety, które zawierają szukaną informację. Aby przeszukać pakiety według ustalonych kryteriów, należy kliknąć przycisk Search for packets matching a set of criteria (CTRL+F - patrz Rys. 6). Następnie pojawi się okno Find Packets. Teraz możemy:

- wyszukiwać pakiety, które spełniają reguły filtrowania (pole wyboru Matching a filters) - wskazujemy z listy dostępne filtry i wybieramy Find. Program przeszuka wszystkie pakiety i wyświetli listę tych, które zostały przefiltrowane,
- wyszukiwać pakiety, które zawierają wskazany ciąg (pole wyboru Containing a string box) -



Rys. 6: Okno "Find Packets" pozwalające na filtrowanie i wyszukiwanie pakietów

wyberamy czy ma to być ciąg ASCII czy heksadecymalny, a następnie wprowadzamy odpowiedni łańcuch znaków. Wybieramy opcję Find - program wyszuka pakiety zawierające podany ciąg.

Oczywiście istnieje możliwość łączenia obu sposobów wyszukiwania (filtry i ciągi znaków), a także zawężanie lub rozszerzanie kryteriów. Za każdym razem kiedy przeszukamy pakiety, program zwróci określoną ich liczbę (jeśli zostaną spełnione właściwe kryteria). Przy dużej liczbie pakietów, wciąż może być ich za wiele, więc jeśli chcemy dalej przeszukiwać zaznaczony zbiór wydajemy polecenie Add to current selection i ponawiamy wyszukiwanie. Jeśli chcemy skasować kryteria wyszukiwania wiskamy Reset.

Przykładowe wyszukiwanie

Przykładowe wyszukiwanie

Najpierw należy uruchomić nową sesję przechwytywania. Wówczas z komputera 192.168.1.100 łączymy się z komputerem 192.168.1.56 za pomocą telnetu, a następnie kończymy sesję. Teraz postaramy się wyszukać wszystkie pakiety, które przesłał komputer 192.168.1.100 do 192.168.1.56 podczas sesji telnet i zaznaczymy je. Wykonujemy więc poniższe czynności:

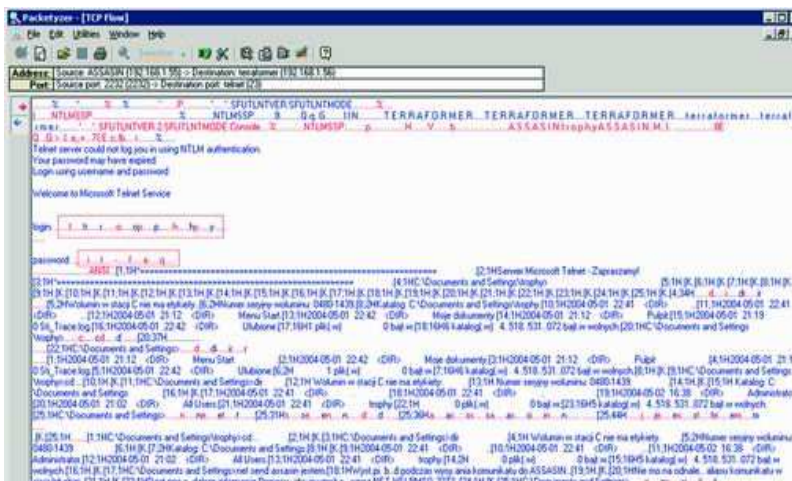
- wiskamy przycisk Search for packets marching a set of criteria (CTRL+F),
- zaznaczamy pole obok naszego filtra telnet,
- wybieramy opcję Find.

Na liście pakietów (prawy, górny panel) zostaną podświetlone tylko te, które spełniły kryterium wyszukiwania. Zamykamy okno - Close. Możemy teraz rozpocząć wyszukiwanie pakietu zawierającego informacje z banneru serwera telnet (np. ciąg "login"). Po takim pakiecie powinny nastąpić kolejne, zawierające znaki (pole data) składające się na login i hasło użyte do uwierzytelnienia.

Śledzenie ruchu TCP

Packetyzer pozwala śledzić ruch pakietów TCP generowanych w sieci. Opcja ta dostępna jest w wielu miejscach programu, w zależności od kontekstu. Najprościej wywołać ją z listy pakietów (prawy, górny panel na zakładce Decode), z menu kontekstowego - pozycja Follow TCP Flow.

Kiedy uruchomimy śledzenie ruchu TCP pojawi się okno, pokazujące przebieg połączenia między dwoma komputerami w sposób graficzny. Najbardziej obrazowym przykładem będzie śledzenie połączenia telnet. Podczas przechwytywania pakietów (lub po zakończeniu sesji), należy wskazać prawym przyciskiem myszy pakiet TCP, który odpowiada połączeniu telnet między dwoma maszynami i wybrać opcję Follow TCP Flow lub przejść na zakładkę Connections, wybrać interesujące nas połączenie, rozwinąć jego węzły, aż otrzymamy informację o pakietach, a następnie z menu kontekstowego pod prawym przyciskiem myszy wskazać opcję Analyze TCP Flow. Wówczas ukaże się nowe okno - na dole znajdują się dwie zakładki: Decode i Trace. Pierwsza z nich przedstawia zawartość wszystkich pakietów



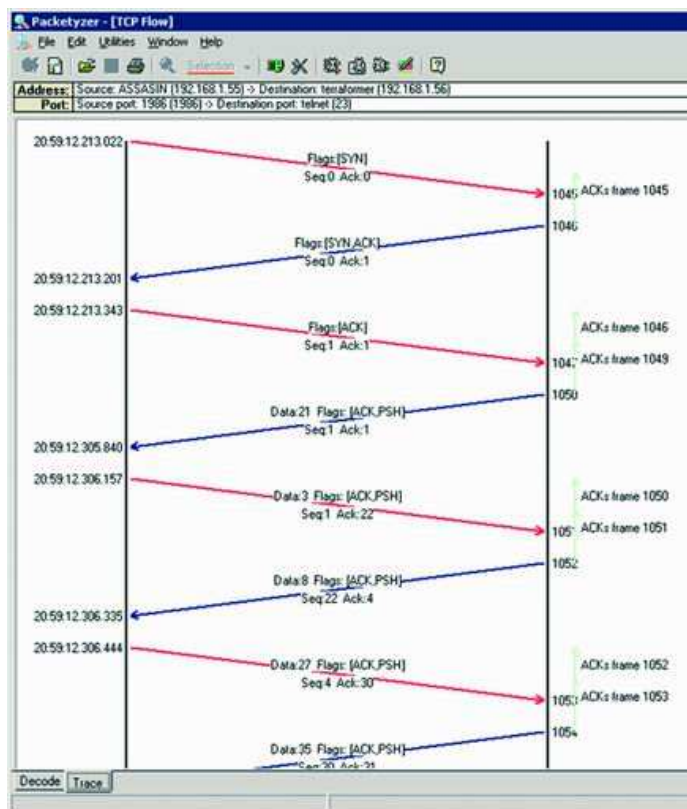
Rys. 7: Zakładka "Debug" pokazuje zawartość wszystkich przechwyconych pakietów biorących udział w komunikacji pomiędzy maszynami. Na czerwono zaznaczono login i hasło użytkownika komputera 192.168.1.55 logującego się na komputerze 192.168.1.56 w czasie sesji telnet

przechwyconych w trakcie konwersacji między hostami - te, które zostały wysłane zaznaczone są na czerwono, pakiety odebrane mają kolor niebieski (do przełączania podglądu służą przyciski strzałek w lewym górnym rogu okna - patrz Rys. 7).

Druga zakładka przedstawia graficzny przepływ pakietów pomiędzy punktami końcowymi komunikacji (patrz Rys. 8). Na górze okna znajdują się także informacje o adresach połączonych maszyn i wykorzystywanych przez nie portach. Diagram znajdujący się pod zakładką Trace jest przydatny podczas analizy połączeń i diagnozowania ewentualnych problemów. Śledząc przebieg konwersacji pomiędzy maszynami możemy uzyskać informacje konieczne do orzeczenia, czy pakiety są właściwie zsynchronizowane i zatwierdzone oraz czy połączenia są poprawnie inicjowane i zakończone. Zakładka Decode może być przydatna podczas analizy danych przesyłanych w trakcie połączenia. Za jej pomocą można bardzo łatwo odnaleźć informacje potrzebne do uwierzytelniania na zdalnych maszynach (login i hasło przesyłane czystym tekstem - patrz przykład z protokołem telnet).

Sieci używające przełączników

Packetyzer z powodzeniem może być wykorzystywany w sieciach LAN używających klasycznych koncentratorów, gdzie każdy pakiet rozsyłany jest na wszystkie porty. Jeśli jednak mamy do czynienia z siecią korzystającą z przełączników, używanie sniffera będzie znacznie utrudnione. Niektóre przełączniki posiadają specjalny port, który przeznaczony jest do prowadzenia nasłuchu. Wówczas wystarczy podpiąć do niego maszynę, na której będziemy uruchamiać Packetyzer. Typowe przełączniki nie oferują jednak takiej możliwości. Problem można rozwiązać na kilka sposobów. Najprostszy, ale nie zawsze możliwy, polega na wpięciu przed przełącznik koncentratora, połączeniu



Rys. 8: Zakładka "Trace" pokazuje przepływ pakietów pomiędzy punktami końcowymi komunikacji

obu urządzeń i podpięciu do koncentratora maszyny, na której ma być prowadzony sniffing. Inne metody związane są z prowadzeniem tzw. aktywnego sniffingu, który pozwala zmusić przełącznik do rozsyłania pakietów na wszystkie (lub niewłaściwe) porty. Trzeba tutaj wykorzystać jedną z opisanych w poprzednim numerze metod ataku: CAM Table Flooding, ARP Cache Poisoning czy Switch Port Stealing. Oczywiście do tego celu można wykorzystać odpowiednie narzędzia, które pozwalają prowadzić atak automatycznie według wybranej metody (patrz ramka - Narzędzia). Należy jednak pamiętać, że tego typu działania mają skutki uboczne i nie gwarantują wysokiego komfortu pracy (więcej na ten temat patrz: Artur Ogłóża, Paweł Wawrzyniak, "Sniffing na różne sposoby", IT FAQ, 05/2004). Sam Packetyzer nie oferuje żadnych funkcji umożliwiających prowadzenie skutecznego sniffingu w sieciach z przełącznikami. To z pewnością jego duża wada. Jeśli nie interesuje nas wykorzystanie dodatkowych narzędzi, możemy skorzystać z innego sniffera, np. Ettercapa (również darmowego), który potrafi automatycznie wykryć fakt sniffowania w sieci z przełącznikami i ułatwia to zadanie. Jeżeli chodzi o pakiet dsniff dla systemu MS Windows, to warto zauważyć, że jest to jedynie częściowo przeniesione narzędzie. Jego składnikiem - w przeciwieństwie do wersji dla GNU/Linux czy *BSD - nie jest np. użyteczny program MACOF, który pozwala modyfikować tablice CAM przełącznika.

Podsumowanie

Packetyzer 2.0.0 z pewnością jest potężnym narzędziem, które doskonale wykorzystuje bibliotekę ethereal.dll. Czy stanowi zagrożenie dla samego Ethereala? Trudno powiedzieć, bo duże znaczenie będzie miała tutaj siła przyzwyczajenia. Nie można

Nazwa produktu	Packetyzer 2.0.0
Przeznaczenie	Przechwytywanie i analiza pakietów w sieciach LAN
Typ programu	Nakładka graficzna wykorzystująca standardowe elementy GUI MS Windows, oparta na bibliotece ethereal.dll
Licencja	GNU GPL
Producent	Network Chemistry http://www.networkchemistry.com/

Tabela 1: Informacje o produkcie

jednak odmówić Packetyzerowi wysokiej jakości i faktu, że oferuje wiele użytecznych funkcji, a jednocześnie posiada łatwy do opanowania interfejs obsługi. Zaletą jest także bardzo dobra angielska dokumentacja dostępna w postaci pliku PDF (znajduje się w katalogu, w którym zainstalowano program). Funkcjonalność programu można też rozszerzać za pomocą wtyczek dla Ethereala, ponadto wraz z Packetyzerem otrzymujemy kilka dodatkowych narzędzi konsolowych (również znanych z Ethereala).

A są to: text2pcap - program pozwalający generować pliki zawierające pakiety zapisane w formacie obsługiwanym przez sniffer na podstawie plików ASCII, mergcap - program łączący dwa pliki zawierające zapis sesji w jeden oraz editcap - konwerter formatów plików z zapisanymi sesjami przechwytywania. Jeżeli chodzi o wady rozwiązania, to z pewnością jest to fakt braku funkcji ułatwiających prowadzenie sniffingu w sieciach z przełącznikami. Pewną nadzieją może być tutaj wykorzystanie możliwości przechwytywania pakietów na zdalnej maszynie za pomocą biblioteki WinPcap - niestety do dziś nie umożliwia tego ani Packetyzer, ani Ethereal. Ta funkcja WinPcap została wprowadzona w wersji 3.0 (demon rpcap). Jeżeli będzie wspierana przez Packetyzer to znacznie zwiększą się możliwości przechwytywania pakietów np. w sieciach, które są chronione zaporą ogniową uniemożliwiającą nawiązywanie połączeń z zewnątrz (zapewni to aktywny tryb pracy rpcap, kiedy to demon przechwytyjący pakiety inicjuje połączenie ze snifferem znajdującym się w sieci zewnętrznej). Pozwoli to także na zmyślne obchodzenie problemu przełączników w niektórych przypadkach (pakiety będzie można zrzucić na zdalnej maszynie, np. routerze i przesyłać do analizy na dowolny komputer, na którym działa Packetyzer). Na razie trzeba jednak radzić sobie w inny sposób.

Warto także zauważyć, że program stanowi część komercyjnego rozwiązania Neutrino Sensor, które oferowane jest przez firmę Network Chemistry. Dzięki temu połączeniu możliwy jest wygodny podsłuch komunikacji w sieciach standardu 802.11.

Narzędzia

Narzędzia:

- Network Chemistry Packetyzer 2.0.0:
<http://www.networkchemistry.com/products/packetyzer/>
<http://www.packetyzer.com/>
- Ethereal 0.10.4:
<http://www.ethereal.com/>
- Cain&Abel - zaawansowany sniffer i łamacz haseł:
<http://www.oxid.it/cain.html>
- Ettercap dla Windows:
<http://ettercap.sourceforge.net/>
- Biblioteka WinPcap:
<http://winpcap.polito.it/>
- EtherFlood dla Windows 2000/XP/2003 (MAC Flooding):
<http://ntsecurity.nu/toolbox/etherflood/>
- ARP0C/WCI (ARP spoofing):
<http://www.phenoelit.de/arpoc/index.html>
- ARPWorks 1.0 dla Windows 9x/Me (ARP spoofing):
<http://www.oxid.it/arpworks.html>