

Sieci komputerowe - laboratorium

Temat ćwiczenia: Analizator sieciowy Ethereal

Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z programem Ethereal służącym do analizy ruchu sieciowego oraz poznanie i analiza wybranych protokołów sieciowych.

Wprowadzenie

Redakcja amerykańskiego tygodnika InfoWorld przeprowadziła odpowiednie badania i sporządziła listę zawierającą 10 produktów i narzędzi, które cieszą się wśród administratorów największym wzięciem. Wśród tych 10 produktów znalazł się Ethereal - narzędzie pozwalające przechwytywać pakiety, analizować wydajność sieci, testować ją, budować raporty oraz wykonywać szereg innych, niezwykle przydatnych dla administratora, zadań. Narzędzie jest dostępne w wersji Windows i dla większości platform uniksowych, i jest udostępniane bezpłatnie [Networld 6/2004].

Analizatory sieciowe umożliwiają dokładną analizę przesyłanych danych w podsieci, do której jest podłączony komputer z odpowiednim programem. Można dzięki temu uzyskać informacje o rodzaju usług i protokołach wykorzystywanych w sieci, adresach komputerów z którymi się łączą użytkownicy danej podsieci, treści przesyłanych danych, itd. Umożliwia to lepsze zrozumienie działania sieci, ułatwia ewentualną lokalizację błędów lub intruzów, daje informacje służące do poprawy działania sieci lub jej modernizacji.

Literatura oraz wymagane informacje

Instrukcja obsługi programu Ethereal (www.ethereal.com)

Model ISO/OSI .

Wybrane protokoły sieciowe (IP, ICMP, TCP, UDP , HTTP, DNS, ARP, FTP- dokumenty

RFC (np. www.ietf.org), książki, artykuły, strony WWW).

Podstawy technologii Ethernet (książki, artykuły, strony WWW).

Zadania do wykonania

Dla wybranego zadania (podanych poniżej) zapoznać się z opisem odpowiednich protokołów sieciowych z wykorzystaniem: dokumentów RFC (Request For Comments), materiałów o sieciach komputerowych (książki, artykuły z czasopism, strony WWW, itp.)

Zapoznać się z instrukcją programu Ethereal oraz jego działaniem.

Z pomocą programu Ethereal wykonać dwa spośród następujących zadań:

1. Uruchomić program ping dla stacji z tej samej podsieci oraz dla stacji z innej podsieci podając adres domenowy. Przeanalizować w pliku przechwyconych danych protokoły ARP, ICMP, DNS .
2. Uruchomić program tracert dla różnych stacji podając adres domenowy. Przeanalizować w pliku przechwyconych danych protokoły ARP, ICMP, DNS .
3. Uruchomić przeglądarkę WWW dla wybranych adresów sieciowych i przeanalizować w pliku przechwyconych danych protokoły HTTP, DNS .
4. Uruchomić program FTP, zalogować się na dowolny adres, przesłać plik i przeanalizować w pliku przechwyconych danych protokoły FTP, DNS .
5. Uruchomić wybrany przez siebie program sieciowy (np. komunikator, poczta) i przeanalizować w pliku przechwyconych danych odpowiednie protokoły związane z tym programem.

W formie pisemnego sprawozdania przygotować dokładną analizę wykonanych zadań.

Sprawozdanie należy zrealizować według następującego planu:

1. Wprowadzenie, cel ćwiczenia.
2. Opis najważniejszych cech wybranych protokołów sieciowych (wymiana informacji, format pakietów, itp.).
3. Analiza otrzymanych logów z programu Ethereal (dla danego protokołu, po wcześniejszym przefiltrowaniu).
4. Wnioski.

Przykład analizy otrzymanego logu dla protokołu ARP

No.	Time	Source	Destination	Protocol	Info
15	6.481702	156.17.43.50	Broadcast	ARP	Who has 156.17.43.62? Tell 156.17.43.50
16	6.481937	156.17.43.62	156.17.43.50	ARP	156.17.43.62 is at 00:02:bb:55:45:56

Frame 15 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:00:39:45:55:a0, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

Frame 16 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:02:bb:55:45:56, Dst: 00:00:39:45:55:a0
Address Resolution Protocol (reply)

Opis

Protokół ARP (Address Resolution Protocol) służy do uzyskania przez stację A adresu MAC (czyli adresu Ethernet) stacji, która jest bramą dla stacji A.

No. 15. Stacja o adresie IP 156.17.43.50 potrzebuje adresu MAC stacji o adresie 156.17.43.62, która jest bramą (gateway) dla stacji 156.17.43.50. Dlatego wysyła ramkę rozgłoszeniową (broadcast) o adresie docelowym MAC w postaci ff:ff:ff:ff:ff:ff.

No. 16. Z definicji bramy wynika, że musi się znajdować w tej samej podsieci co stacja, dla której jest bramą. Dlatego otrzyma ramkę rozgłoszeniową i odpowie na nią przesyłając swój adres MAC. W tym momencie stacja o adresie IP 156.17.43.50 zna adres MAC swojej bramy, więc może zacząć wysyłać pakiety IP do stacji znajdujących się w innych podsieciach.

Ocena

Na ocenę z tego ćwiczenia będzie wpływać: przygotowanie teoretyczne do ćwiczenia z zakresu wybranych protokołów, praca w czasie realizacji zadań w laboratorium oraz sprawozdanie oddane na następnych (po wykonaniu zadania) zajęciach.