OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Monitorowanie sieci musi być sprawowane przez administratora na bieżąco, a pojawiające się problemy rozwiązywane.

Administrator powinien mieć przygotowany zestaw narzędzi , gotowych do użycia, z których korzysta na co dzień i w razie awarii.
Pozwala to skrócić czas reakcji na awarię.

Istnieje wiele narzędzi, zarówno bezpłatnych jak i płatnych, pozwalających monitorować oraz pomagać w rozwiązywaniu problemów z siecią.

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Skanery IP

Potrafią sprawdzić, które adresy IP w danej sieci są aktualnie używane.

Jeżeli zdarzy się sytuacja, w której dwa komputery będą miały ten sam adres, to wystąpi konflikt i kłopoty z dostępem do sieci.

Przykładem prostego skanera IP jest **Advanced IP Scanner**– na licencji GPL oraz **Nmap** (**Zenmap-**interfejs graficzny do Nmap)– zaprojektowany do szybkiego skanowania dużych sieci, też na licencji GPL

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Skanery IP

Ćwiczenie 1:

1. Pobierz, zainstaluj i uruchom program **Advanced IP Scanner**

2. Przeskanuj całą sieć o adresie 192.168.11.0/24 i podaj:
   - ile komputerów jest w tej sieci
   - czy są komputery, których adres IP się powtarza

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Skanery IP

Ćwiczenie 2:

1. Pobierz, zainstaluj i uruchom program Nmap

2. Przeskanuj serwer o adresie 192.168.4.11/24 i podaj:
   - ile „ciekawych” portów jest otwartych
   - jaki adres sprzętowy ma karta sieciowa serwera

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Analizatory ruchu w sieci

Służą do zbierania informacji statystycznych dotyczących natężenia ruchu sieciowego w czasie rzeczywistym

Przykładem jest **Ntop** – na licencji GPL. Jego zaletą jest możliwość przeglądania raportów w przeglądarce: dotyczących ruchu w sieci, protokołów itp.

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Analizatory ruchu w sieci

Ćwiczenie 1:

1. Pobierz, zainstaluj i uruchom program Ntop
2. Zinterpretuj otrzymane wyniki dotyczące ruchu w twojej sieci, m. in.:
   - jakiej wielkości pakiety dominują i co to oznacza
   - jaki typ protokołu dominuje i co to może oznaczać
   - Jaki jest udział transmisji broadcast i co to oznacza
   - jaki jest udział transmisji multicast i co to oznacza
   - ile jest błędów związanych z transmisją
   - jaka ostatnio była maksymalna prędkość pobierania danych

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Narzędzia do monitorowania wbudowane w Windows:

netstat – wyświetla statystyki interfejsu

nbtstat – wyświetla statystykę protokołu, tabele nazw oraz pamięć podręczną nazw NetBIOS

NetBIOS wykorzystuje się do zapewnienia aplikacjom komunikacji pomiędzy komputerami znajdującymi się w sieci LAN. Działa w warstwie sesji modelu ISO - dzięki niemu aplikacje nie muszą „posiadać" szczegółowej wiedzy na temat sieci.
Dostarcza on trzy usługi:
– nazewnictwo maszyn w sieci (port 137)
– komunikację połączeniową (port 139)
– komunikację bezpołączeniową (port 138)
NetBIOS to podstawa działania sieci dla systemów Windows.

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Narzędzia do monitorowania wbudowane w Windows:

Ćwiczenie 1:

Sprawdź narzędziami wbudowanymi w Windows:

- Ile bajtów danych zostało wysłanych do sieci
- Ile pakietów innych niż unicast wysłano
- Czy jakaś aplikacja wysyła/odbiera dane za pomocą protokołu UDP
- Jakie aplikacje sieciowe działają na naszym komputerze, z jakich portów korzystają i z jakimi serwerami się łączą
- Jakie numery procesów odpowiadają naszym aplikacjom sieciowym

OPROGRAMOWANIE DO MONITOROWANIA SIECI LAN

Narzędzia do monitorowania wbudowane w Windows:

Ćwiczenie 2:

Sprawdź narzędziami wbudowanymi w Windows:

- Jaka jest zawartość lokalnej bazy NetBIOS
- Jak wyczyścić bazę NetBIOS
- Jak ponownie zarejestrować i odświeżyć nazwy NetBIOS