Programy analizy ruchu w sieci komputerowej (Sniffery)

podrozdział pracy magisterskiej o zaporach ogniowych

Sniffery to programy służące do przechwytywania pakietów sieciowych. Pierwotnym zastosowaniem programów tego typu jest analiza ruchu w sieci i identyfikacja potencjalnych problemów. Przykładowo, w sytuacji kiedy jeden segment sieci działa mało wydajnie – dostarczenie pakietu odbywa się bardzo wolno lub komputery blokują się przy uruchamianiu w sieci. Do dokładnego określenia przyczyny takiego zachowania używamy programu typu Sniffer. Sniffery różnią się znacznie między sobą funkcjonalnością i stopniem programistycznego zaawansowania – niektóre z nich analizują tylko jeden protokół, podczas gdy inne setki. Ogólnie rzecz ujmując, program taki analizuje protokoły:

- Standardowy Ethernet
- TCP/ IP
- IPX
- DECNet

Analizatory protokołów zawsze są kombinacją sprzętu i oprogramowania. Komercyjne programy tego typu są drogie (zazwyczaj sprzedawane są w pakiecie z komputerem zbudowanym z uwzględnieniem funkcji sieciowej, jaką będzie on pełnić), natomiast te, które są dostępne jako oprogramowanie typu freeware, nie oferują żadnej pomocy technicznej.

Analizatory ruchu w sieci komputerowej znacznie różnią się od programów przechwytujących kody naciskanych klawiszy. Programy typu sniffer przechwytują pakiety sieciowe poprzez ustawienie karty sieciowej w tzw. tryb mieszany (promiscuous mode). Lokalne sieci komputerowe są małymi sieciami typu Ethernet (najczęściej). Dane z jednego komputera przesyłane są do drugiego przy pomocy kabla sieciowego.

Istnieją różne rodzaje kabli, różniących się szybkością przesyłania danych, z których najpowszechniej stosowanych jest pięć:

- 10BASE-2 kabel koncentryczny (cienki), którym standardowo można przesyłać dane na odległość 152 metrów.
- 10BASE-5 kabel koncentryczny (gruby), którym standardowo można przesyłać dane na odległość 457 metrów.
- 10BASE-5 kabel światłowodowy
- 10BASE-T skrętka dwuprzewodowa, standardowo przesyłająca dane na odległość 183 metry.
- 100BASE-T kabel przystosowany do przesyłania danych z prędkością 100 megabitów na sekundę, (na odległość do 100 metrów).

Transmisja danych w sieci komputerowej odbywa się małych porcjach – ramkach. Ramki te są podzielone na sekcje, z których każda zawiera z góry określone informacje, na przykład pierwsze 12 bajtów ramki sieci Ethernet niesie informacje o adresie odbiorcy i nadawcy pakietu. Inne sekcje ramki przenoszą właściwe dane użytkownika, nagłówki TCP/IP, nagłówki IPX, itd.

Ramki są przygotowywane do wysłania przez specjalny program, zwany sterownikiem sieciowym. Następnie przesyłane są z komputera wyjściowego do sieci poprzez kartę sieciową, skąd przemieszczają się do miejsca przeznaczenia. Po dotarciu do maszyny docelowej proces jest odwracany, tj. karta sieciowa w komputerze odbiorcy pobiera ramki i, informując system operacyjny o tym fakcie, przekazuje sterowanie odpowiedniemu oprogramowaniu, które zajmuje się dalszą obróbką pakietów.

Analizatory protokołów stanowią zagrożenie dla bezpieczeństwa z powodu sposobu, w jaki ramki są przesyłane i dostarczane do miejsca przeznaczenia. Poniżej przedstawione jest krótkie omówienie tego procesu.

Każda stacja robocza w lokalnej sieci komputerowej ma swój własny adres sprzętowy. Adres ten jest unikalny dla odróżnienia poszczególnych komputerów w sieci (przypomina to system adresowania w sieci Internet). Wysyłając jakiekolwiek dane przez sieć LAN, pakiety z danymi trafiają do wszystkich komputerów w tej sieci.

W normalnych okolicznościach wszystkie komputery w sieci mogą „słyszeć" cały ruch, który się w niej dobywa, ale reagują tylko na te dane, które są zaadresowane specjalnie dla nich (innymi słowy stacja robocza A nie przechwyci danych przeznaczonych dla stacji roboczej B lecz je zignoruje). Jeśli jednak karta sieciowa danej maszyny znajduje się w trybie mieszanym, może przechwytywać wszystkie pakiety i ramki w sieci. Stacja robocza skonfigurowana w ten sposób (i jej oprogramowanie) stanowi analizator ruchu w sieci komputerowej (sniffer).

Programy tego typu sniffer stanowią wysoki poziom ryzyka.

1. Mogą przechwytywać hasła.
2. Mogą przechwytywać poufne lub zastrzeżone informacje.
3. Mogą być użyte do naruszenia bezpieczeństwa sąsiednich sieci lub zdobycia stopniowego dostępu do nich.

Wykrycie przez administratora „obcego" analizatora umieszczonego w jego sieci oznacza w większości przypadków, że zabezpieczenia sieci już zostały pokonane.

Programy tego typu przechwytują wszystkie pakiety danych podróżujące w sieci, lecz w praktyce konieczne jest zawężenie przechwytywanych pakietów do tych, które są dla użytkownika z jakiegoś względu istotne.

Przeprowadzenie ataku przy pomocy sniffera nie jest proste – wymaga dość zaawansowanej wiedzy o sieciach. Zwyczajne zainstalowanie takiego programu i uruchomienie go prowadzi do problemów, gdyż nawet sieć z pięcioma stacjami roboczymi przesyła tysiące pakietów na godzinę. W krótkim czasie plik

wynikowy sniffera może zapełnić cały dysk twardy (jeśli przechwytywany jest każdy pakiet).
Aby obejść ten problem, krakerzy na ogół przechwytują tylko 200-300 początkowych bajtów każdego pakietu, gdzie zawarta jest nazwa użytkownika i jego hasło (a to właściwie wszystko, co kraker chce wiedzieć). Jednakże, jeśli intruz dysponuje maszyną z wystarczającą ilością miejsca na dyskach – może przechwytywać cały ruch w sieci – niekiedy i w dalszej części pakietu można znaleźć interesujące informacje.

Analizator ruchu w sieci może zostać założony w dowolnym miejscu w sieci. Jednak są pewne punkty strategiczne, które pozostają w kręgu szczególnego zainteresowania krakerów (jak na przykład miejsca, gdzie często dokonuje się procedur autoryzacji). Na szczególne niebezpieczeństwo narażone są maszyny będące bramkami pomiędzy sieciami. Ruch generowany w okolicach takiego komputera zawiera stosunkowo najwięcej pakietów pochodzących z procedur autoryzacji. Umiejscowienie sniffera w tym miejscu zwiększa sferę wpływów intruza w sposób wykładniczy.

W ostatnim czasie technologie związane z bezpieczeństwem systemów uległy znacznemu udoskonaleniu. Niektóre systemy operacyjne wykorzystują szyfrowanie na poziomie pakietu i dlatego, nawet jeśli sniffer przechwyci istotne dane, będą one zaszyfrowane. Stanowi to przeszkodę do ominięcia jedynie przez użytkowników posiadających dogłębną wiedzę z dziedzin: bezpieczeństwa systemów, szyfrowania oraz sieci.

Sniffery dostępne są w postaci pakietów komercyjnych (często programowo-sprzętowych) oraz programów typu freeware. Początkującym administratorom zaleca się zapoznanie z ogólną charakterystyką analizatora ruchu na podstawie któregoś z darmowych pakietów. Doświadczeni administratorzy dużych sieci powinni posiadać przynajmniej jeden sniffer komercyjny. Programy te są nieocenione przy diagnozowaniu problemów sieci.

dyplomowe, które mogą służyć za wzór do napisania własnej pracy - gdyby potrzebowali jeszcze Państwo konsultacji to polecamy stronę pisanie prac - fachowa pomoc w pisaniu prac.