Problemy z bezpieczeństwem w sieci lokalnej

- możliwości podsłuchiwania/przechwytywania ruchu sieciowego
- pakiet dsniff
- demonstracja kilku narzędzi z pakietu dsniff
- metody przeciwdziałania

Podsłuchiwanie ruchu sieciowego

Sniffer

program komputerowy, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci. Wspólną cechą wielu takich analizatorów jest przełączenie karty sieciowej w tryb promiscuous, w którym urządzenie odbiera wszystkie ramki z sieci, także te nie adresowane bezpośrednio do niego; sniffery mogą być uruchamiane także na ruterze lub na komputerze będącym jedną ze stron komunikacji sieciowej - i w tych przypadkach tryb promiscuous nie jest konieczny.

źródło: http://pl.wikipedia.org/wiki/Sniffer

UWAGA !

Podsłuchiwanie ruchu sieciowego, którego nie jesteśmy adresatem jest prawnie zabronione!

Jak to działa?

Switche utrzymują tablicę mapowań adres MAC<->port fizyczny.
W celu ustalenia fizycznego adresata używają docelowego adresu MAC zawartego w nagłówku ramki Ethernet.

Arp spoofing

Technika pozwalająca przechwytywać dane przesyłane w obrębie segmentu sieci LAN. Atak polega na rozsyłaniu w sieci LAN odpowiednio spreparowanych pakietów ARP zawierających fałszywe adresy MAC. W efekcie pakiety danych wysyłane przez inne komputery w sieci trafiają do osoby atakującej zamiast do właściwego odbiorcy. Pozwala to na podsłuchiwanie komunikacji.

arpok.png arpzle.png

Narzędzia pakietu dsniff

- dsniff
- arpspoof
- dnsspoof
- mailsnarf
- urlsnarf
- webspy
- msgsnarf
- ggsniff (patch do msgsnarf)
- filesnarf
- sshmitm, webmitm

arpspoof

arpspoof [-t victim] gateway
Przekierowuje pakiety wysyłane przez wszystkich lub wybraną “ofiarę”do wybranego hosta na nasz komputer. W tym celu wysyła “ofierze” spreparowane fałszywe informacje na temat adresu MAC hosta (najczęściej bramy).

dsniff

Nasłuchuje ruch sieciowy na wybranym interfejsie i przechwytuje loginy i hasła np. FTP, SMTP, POP, NFS, CVS, IRC, PostgreSQL, Oracle.

dsniff.png

webspy

webspy host

Otwiera w kolejnych zakładkach domyślnej przeglądarki strony odwiedzane przez podsłuchiwanego. Jest to ulepszona wersja programu urlsnarf, który tylko wypisuje na konsole zapytania HTTP.

mailsnarf

Służy do przechwytywania pobieranej i wysyłanej poczty. Wypisuje e-maila w formacie łatwym do przeglądania w wielu klientach pocztowych, np pine.

mailsnarf.png

msgsnarf (wraz z łatką ggsniff)

Służy do podsłuchiwaniu wielu popularnych komunikatorów internetowych, np. ICQ 2000, IRC, MSN Messenger. Łatka ggsniff umożliwia podsłuchiwanie najpopularniejszego w Polsce Gadu-Gadu.

ggsniff.png

filesnarf

Zapisuje pliki przesyłane przy użyciu protokołu NFS.

dnsspoof

Wysyła fałszywe odpowiedzi na wybrane zapytania DNS. Można podmienić adres IP wybranej domeny na dowolny inny.

Metody przeciwdziałania

- arpwatch
- SSL
- certyfikaty

arpwatch

Arpwatch to bardzo przydatny programik monitorujący sieć w poszukiwaniu nowych adresów MAC kart sieciowych itd. Gdy tylko odnajdzie jakiś wysyła maila do administratora. Przydaje się do wykrywania wszelkiego rodzaju nadużyć, dalszego udostępniania internetu itd.

protokół SSL

SSL = Secure Socket Layer
SSL jest protokołem typu klient-serwer pozwalającym na nawiązanie bezpiecznego połączenia z użyciem certyfikatów. Jest on zorientowany głównie na autentyfikację serwera (np. sklepu internetowego do którego klient wysyła numer karty kredytowej i chce mieć pewność co do odbiorcy), ale przewiduje również możliwość autoryzacji klienta.

Schemat działania SSL

- K -> S ClientHello
  zgłoszenie zawierające m.in. wersję protokołu SSL, Komunikat ten zawiera również liczbę losową używaną potem przy generowaniu kluczy.
- K <- S ServerHello
  komunikat, w którym zwraca klientowi wybrane parametry połączenia: wersję protokołu SSL, rodzaj szyfrowania i kompresji, oraz podobną liczbę losową.

Schemat działania SSL

- K <- S Certificate
  Serwer wysyła swój certyfikat pozwalając klientowi na sprawdzenie swojej tożsamości
- K <- S ServerKeyExchange
  Serwer wysyła informację o swoim kluczu publicznym.
- K <- S ServerHelloDone
  Serwer zawiadamia, że klient może przejść do następnej fazy zestawiania połączenia.

Schemat działania SSL

- K -> S ClientKeyExchange
  Na podstawie ustalonych w poprzednich komunikatach dwóch liczb losowych generuje klucz sesji używany do faktycznej wymiany danych. Następnie wysyła go serwerowi używając jego klucza publicznego.
- K -> S ChangeCipherSpec
  Klient zawiadamia, że serwer może przełączyć się na komunikację szyfrowaną.

Schemat działania SSL

- K -> S Finished
  jest gotowy do odbierania danych zakodowanych.
- K <- S ChangeCipherSpec
  Serwer zawiadamia, że wykonał polecenie - od tej pory wysyłał będzie tylko zaszyfrowane informacje.
- K <- S Finished
  ... i od razu wypróbowuje mechanizm - ten komunikat jest już wysyłany bezpiecznym kanałem!

źródło: http://muflon.photosite.pl/doc/progzesp/ssl.html

Certyfikaty

Certyfikat jest to zbiór danych jednoznacznie identyfikujących pewną jednostkę (na przykład osobę, lub komputer) oraz pozwalający stwierdzić, czy osoba, która się nim legitymuje jest rzeczywiście tym, za kogo się podaje. Jest on potwierdzony przez zaufaną organizację, zwaną w protokole SSL certificate authority (CA).

Certyfikat zawiera:

- Nazwę certyfikowanego obiektu
- Identyfikator obiektu
- Klucz publiczny obiektu
- Czas ważności
- Nazwę wystawcy certyfikatu
- Identyfikator wystawcy
- Podpis wystawcy

Łańcuch certyfikatów

W ogólnym przypadku mamy tak zwany łańcuch certyfikatów. Nie musimy (a nawet nie powinniśmy) bowiem dla każdego obiektu w danym systemie wystawiać certyfikatu potwierdzonego przez CA, gdyż spowodowałoby to przeciążenie tych instytucji i niepotrzebny rozrost bazy danych. Możemy na własne potrzeby ustanowić lokalny urząd certyfikacyjny który będzie poświadczał lokalne certyfikaty, a sam będzie legitymował się certyfikatem poświadczonym przez CA.