Metody ataków sieciowych

Podstawowy podział ataków sieciowych

- Ataki pasywne
- Ataki aktywne

Ataki pasywne (passive attacks)

- Polegają na śledzeniu oraz podsłuchiwaniu w celu pozyskiwania informacji lub dokonania analizy ruchu sieciowego.
- Z reguły ataki pasywne są pierwszym krokiem do przeprowadzenia ataku aktywnego i maja za zadanie zebranie jak najwięcej informacji o celu ataku.
- Z tego względu, iż ataki pasywne nie dokonują zmian danych, są właściwie nie do wykrycia. W postepowaniu z tymi atakami należy raczej skupić się na zapobieganiu, a nie wykrywaniu.

Ataki aktywne (active attacks)

- Polegają na modyfikacji strumienia danych lub tworzeniu danych o zmienionej strukturze.

Przyjmuje się, że atak składa się z takich faz jak:

- przygotowanie ataku,

- przeprowadzenie ataku,

- zacieranie śladów i/lub pozostawienie otwartej drogi do ponownego włamania.

Przykłady ataków pasywnych

- Social engineering - (socjotechniki) jest to sposób na pozyskanie informacji istotnych z punktu widzenia bezpieczeństwa, takich jak hasła, loginy, procedury bezpieczeństwa. Polega na manipulowaniu ludzką lekkomyślnością w celu osiągniecia korzyści.

Fałszywe e-maile, w których pod pretekstem awarii systemu i powstałych w ten sposób błędów nadawca prosi o ponowne podanie loginu i hasła.

Przykłady ataków pasywnych

- Podglądanie wpisywanych z klawiatury loginów i haseł ;
- Telefony od osób, które pod pretekstem awarii proszą o wpisanie kilku poleceń w konsoli tekstowej;
- Przeglądanie wyrzuconej dokumentacji.

Przykłady ataków pasywnych

- **Ataki na hasła**

- Metoda sitowa (brute force)-sprawdzane są wszystkie możliwe kombinacje znaków. Metoda ta daje pewność znalezienia hasła, ale problemem jest długi czas potrzebny do złamania hasta.
- Metoda słownikowa (dictionary attack) - wykorzystuje się zbiór potencjalnych haseł, które sprawdzane są po kolei.

Programy do łamania haseł mogą w ciągu sekundy testować po kilkaset tysięcy haseł.

Jedna z metod zwiększenia odporności systemu na ataki siłowe i słownikowe jest blokowanie na określone czas możliwości wprowadzenia kolejnego hasła.

Przykłady ataków pasywnych

- **Skanowanie sieci** - celem skanowania jest zebranie jak największej ilości informacji na temat usług działających w sieci, wersji systemu operacyjnego i struktury sieci.

Skanowanie może również dotyczyć pojedynczego komputera lub serwera, aby uzyskać informacje na temat otwartych portów, wersji oprogramowania.

Metody skanowania

- **TCP connect scanning** - polega na nawiązywaniu połączenia z wybranymi portami - jeżeli połączenie zostanie nawiązane, oznacza to, że port jest otwarty. Wadą metody jest łatwy sposób jej wykrycia, ponieważ pozostawia ślady w logach.
- **TCP SYN scanning** - w metodzie tej zawiązywanie połączenia jest przerywane przed jego zakończeniem, nie dochodzi do pełnego połączenia, brak jest wpisów w logach serwera i trudniej jest wykryć próbę skanowania.
- **ICMP echo** - pozwala ustalić za pomocą polecenia ping adresy IP, pod którymi pracują hosty.

Przykłady ataków pasywnych

- **Nasłuchiwanie** (sniffing) - polega na przechwytywaniu pakietów przesyłanych w sieci. W sieci lokalnej każda maszyna ma swój unikatowy adres MAC i odbiera tylko ramki kierowane na ten adres i adres rozgłoszeniowy. Ustawienie karty sieciowej w specjalnym trybie (promiscuous mode) pozwala odbierać wszystkie ramki przesyłane w danym segmencie sieci.

Aplikacje wykorzystywane do tego typu zadań nazywane są snifferami. Zabezpieczeniem sieci jest szyfrowanie danych.

Przykłady programów wireshark, nmap.

Ataki aktywne

- **Spoofing** - podszywanie się pod inne komputery upoważnione do nawiązywania połączeń.
- **DNS-spoofing** - polega na wykonywaniu ataku na serwer DNS, który posiada bazę danych na temat adresów IP dla poszczególnych hostów. Modyfikacja wpisów w systemie DNS może spowodować, że klient zamiast do hosta docelowego będzie przekierowany do innego komputera.
- **IP-spoofing** - opiera się na fałszowaniu źródłowego adresu IP w wysianym przez komputer pakiecie sieciowym, dzięki czemu napastnik może podszyć się pod legalnego użytkownika sieci i wykorzystać uprawnienia posiadane przez atakowany adres.

Ataki aktywne

- **Przechwycenie sesji** (hijacking) —polega na przechwyceniu sesji w protokole TCP. Atakujący zrywa połączenie między serwerem i klientem, aby jako autoryzowany użytkownik móc kontynuować komunikację bez konieczności logowania.
- **Koń trojański** - to program, który podszywając się pod aplikacje użytkownika, dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje np. wysyłanie do serwera napastnika informacji o kontach i hasłach, umożliwienie zalogowania się z prawami administratora lub uruchomienie innych programów.

Ataki aktywne

- **Ataki typu DOS** - uniemożliwiają użytkownikom dostęp do wybranych lub wszystkich usług.
- **SYN Flood** - duża liczba połączeń TCP z komputerem aby wyczerpać jego zasoby
- **Ping od Death** - wysyłanie dużej liczby pakietów testowych za pomocą komendy ping z ustawionym rozmiarem pakietu testowego przekraczającego dopuszczalny zakres.
- **Atak smerfów** - generowanie dużej ilości pingów kierowanych na adresy rozgłoszeniowe adresami źródłowymi zamienionymi na adres ofiary.

Ataki aktywne

- **E-mail bombing** - wysyłanie dużej liczby wiadomości z nieistotnymi treściami na skrzynkę ofiary. Skrzynka może ulec zablokowaniu przez jej przepełnienie.
- **E-mail spamming** - polega na wysyłaniu listów do wszystkich osób korzystających z określonego serwera
- **Ataki przepełnienia bufora** (Buffer overflow) wykorzystują błąd programistyczny polegający na zapisaniu do wyznaczonego obszaru pamięci (bufora) większej ilości danych niż zarezerwował na ten cel programista. Powoduje to nadpisanie danych znajdujących się w pamięci bezpośrednio za buforem, a w rezultacie błędne działanie programu.

Ataki aktywne

- **Disable accounts** – systemy blokują funkcjonowanie konta po określonej liczbie niewłaściwych logowań bądź narzucają przerwy między kolejnymi próbami.
- **Metoda tylnych drzwi** (backdoor) - polega na uzyskaniu dostępu do systemu operacyjnego bez procedury autoryzacji. Wcześniej może zostać zainstalowany do tego celu koń trojański.

Ataki na serwery

- DoS Denial of Service
- DDoS Distributed Denial of Service
- Mail Bombing
- Smurfing
- Flooding

Włamania do systemów

- Sniffing
- Port Scanning
- Social Engineering
- Brute Force
- Dictionary attack
- Spoofing
- Back Door
- Trojan Horse

Destabilizacja systemów

- Blue Bomb – nuking
- Wirus komputerowy
- Logic Bomb

Rozwiąż problemy:

1. Opracuj zasady bezpieczeństwa organizacji (określenie polityki bezpieczeństwa) wykonaj analizę bezpieczeństwa, a także zalecenia dotyczące zapewniania bezpieczeństwa sieciowego systemu operacyjnego.
2. Utwórz hasło dla swojego konta w organizacji spełniające wymagania bezpieczeństwa.

Trochę literatury do poczytania

Windows 7 mają dwa tygodnie na przesiadkę: https://tiny.pl/7mdkc

Jedna czwarta komputerów nadal działa pod Windowsem: https://tiny.pl/7mdkb

Hakerzy już wykorzystują luki bezpieczeństwa w Windows 7

https://tiny.pl/7md2r

Przypadkiem odkryłem ten serwer w naszej sieci…

https://tiny.pl/7md2j

Jeden z serwerów NordVPN zhackowany:

https://tiny.pl/7md8k

Trochę literatury do poczytania

Jak wygląda zaawansowane włamanie krok po kroku – raport z incydentu - https://tiny.pl/7mdsz

Ktoś włamał się na moją stronę www: co robić?

https://tiny.pl/7md67

Zabezpieczenia przed włamaniem

https://tiny.pl/7md6p

Przejęcie domeny Active Directory za pomocą delegacji Kerberos

https://tiny.pl/7mdvq

Dziękuję za uwagę