# Bezpieczeństwo w sieciach

## Prezentacja na systemy operacyjne

Katarzyna Macioszek

styczeń 2007

# Definicja robaka

**Robak** - program komputerowy zdolny do samoreplikacji przez sieć bez interakcji użytkownika

# Scenariusz ataku robaka

- robak infekuje komputer i przejmuje kontrolę nad funkcjami odpowiedzialnymi za przesyłanie informacji
- robak rozmnaża się, to znaczy wysyła swoje kopie do innych komputerów

# Ważne cechy robaka

- **jak zaraża?** (błąd w oprogramowaniu, nieprawidłowa konfiguracja, głupi użytkownik, ...)
- **jak przeżywa?** (modyfikacja plików systemowych, ukrywanie się przed programami skanującymi, ...)
- **jak się rozmnaża?** (e-mail, IRC, P2P, TCP, ...)
- **jak szkodzi?** (...)

# Robak == wirus?

- **Wirus** – kawałek kodu komputerowego, który dołącza się do jakiegoś pliku i zostaje uruchomiony razem z nim
- Wirus NIE jest samodzielnym programem, zainfekowany plik musi być otworzony przez użytkownika.
- Żeby przenieść się na inne komputery, wirus potrzebuje nosiciela (zarażonego pliku)

# Morris Worm

- **jak zaraża?** przepełnienie bufora, zła konfiguracja programu, słabe hasła
- **jak przeżywa?** wcale
- **jak się rozmnaża?** internet
- **jak szkodzi?** pojedyńczy robak – wcale; wszystkie razem – duży ruch w sieci i wykorzystywanie zasobów komputera

# Blaster

- **jak zaraża?** przepełnienie bufora
- **jak przeżywa?** zmienia pliki systemowe, tak, żeby być uruchamianym przy starcie systemu
- **jak się rozmnaża?** DCOM
- **jak szkodzi?** DoS -> windowsupdate.com, niestabilne działanie systemu, backdoor

# Slammer

- **jak zaraża?** przepełnienie bufora
- **jak przeżywa?** nijak :) nie kopiuje się nawet na dysk
- **jak się rozmnaża?** UDP
- **jak szkodzi?** komputerowi – wcale; całej sieci – bardzo...

# Niebezpieczeństwa czyhające w sieci

**Problem:** jakie mamy narzędzia do zapewnienia sieci bezpieczeństwa?

# Co to jest IDS?

**IDS (Intrusion Detection System)** – system wykrywania włamań. Analizuje pakiety i pliki w sieci próbując wykryć nieprawidłowości poprzez:

- szukanie sygnatur znanych ataków
- wykrywanie anomalii ruchu sieciowego

**HIDS (Host-based IDS)** – działa na każdym komputerze w sieci

**NIDS (Network IDS)** – działa na jednym komputerze, monitoruje ruch w całej sieci

# Jak działa IDS?

Różnie :)
Może na przykład:

- kontrolować pakiety
- kontrolować spójność niektórych danych
- kontrolować aktywność użytkowników
- analizować pliki dzienników

Poza tym:

- zapisuje kopie podejrzanych (lub wszystkich) pakietów
- zapisuje logi do plików
- alarmuje administratora o zagrożeniu

# Wady IDS

IDS kontroluje sieć w sposób pasywny, nie może ingerować w zawartość pakietów. W szczególności nie jest w stanie przerwać próby ataku.
Potrzebny jest system, który monitoruje ruch sieciowy tak samo jak IDS, ale w razie zagrożenia może samodzielnie je zwalczać.

# Co to jest IPS?

**IPS (Intrusion Prevention System)** – system przeciwdziałania włamaniom. Analizuje ruch sieciowy in-line (IDS dostawał tylko kopie pakietów) i reaguje odpowiednio na zagrożenia. Może na przykład odpowiednio przekonfigurować firewalla lub przerwać połączenie.

# Jak działa IPS?

IPS analizuje ruch sieciowy, podobnie jak IDS, i w przypadku wykrycia nieprawidłowości reaguje w odpowiedni sposób. Na przykład

- konfiguruje działanie firewalla
- przerywa połączenie
- podmienia pakiety

# Wady IPS

- IPS ma mniej czasu na sprawdzanie pakietów, więc robi to mniej dokładnie
- IPS może podejmować niewłaściwe akcje