Bezpieczeństwo

Wyzwania

- Urządzenia mobilne
- Powszechna digitalizacja (dokumenty, elektroniczna tożsamość – np. odcisk palca, rejestry sądowe – np. księgi wieczyste)
- Zarządzanie infrastrukturą (np. światła, kolej)
- Sterowanie procesami przemysłowymi (stuxnet)

Dlaczego jest niebezpiecznie ?

- Projektując systemy/protokoły nie myślano o bezpieczeństwie
- Błędy
- Ignorancja i niedbalstwo
- Brak konsekwencji i staranności

Bezpieczeństwo - definicja

Miara (poziom) uzasadnionego zaufania, że potencjalne straty [wynikające z …] nie zostaną poniesione

Bezpieczeństwo teleinformatyczne

Straty wynikające z:

niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych

Uzasadnione zaufanie

- Analiza ryzyka
  - Zasoby i ich wartość
  - Zagrożenia
  - Podatności
- Audyt
- Mechanizmy zabezpieczeń

Potencjalne straty

- Wartość zasobów
- Koszty niedostępności i przestojów

Klasy zagrożeń

- Siły wyższe (żywioły, katastrofy, zmiany prawa, kryzys finansowy)
- Działania przestępcze
- Błędy użytkowników i operatorów
- Zaniedbania organizacyjne
- Awarie i wady elementów systemu teleinformatycznego

Co grozi informacji ?

- Nieuprawniony odczyt/upublicznienie
- Nieuprawniona modyfikacja, uszkodzenie
- Nieuprawnione usunięcie
- Niedostępność
- Podszywanie pod źródło informacji
- Utrata w wyniku awarii, błędu
- Uszkodzenie
- …

Usługi Sieciowe

- DNS
- DHCP
- WWW (zakupy, rezerwacje, zapisy na zajęcia)
- Poczta
- Zdalne zarządzanie
- …

Co grozi usługom sieciowym ?

- Niedostępność usługi
- Podszywanie pod usługodawcę

Co to znaczy bezpiecznie ?

- Przesyłanie numeru karty kredytowej
- Przesyłanie danych do przelewu
- Przesyłanie informacji o terminie egzaminu
- Sprawdzanie planu zajęć na stronie Uczelni, przesyłanie projektu 2 godz. przed terminem
- Wspólna lodówka w akademiku

Atrybuty bezpieczeństwa/Usługi ochrony

Atrybuty bezpieczeństwa

- **Poufność danych** (*confidentiality*)
  dane są niemożliwe do odczytania przez osobę nieautoryzowaną (nieuprawnioną)

Atrybuty bezpieczeństwa

- **Integralność** (*integrity*)
  dane (przechowywane lub przesyłane) nie mogą być modyfikowane przez nieautoryzowane osoby lub przekłamane (spójność danych)

Atrybuty bezpieczeństwa

- **Dostępność** (*availability*)
  autoryzowane podmioty mają bieżącą i nieprzerwaną możliwość korzystania z zasobów systemów i sieci

Atrybuty bezpieczeństwa

- **Uwierzytelnianie** (*authentication*)
  Tożsamość podmiotów (np. komunikujących się stron) jest potwierdzona.
  Możliwość sprawdzenia, czy użytkownicy (serwery, procesy) komunikujący się ze sobą są rzeczywiście tymi, za których się podają.

Atrybuty bezpieczeństwa

- **Niezaprzeczalność** (*nonrepudiation*)
  dostarczenie dowodów realizacji czynności, np. wysłania konkretnych danych, odebrania danych.

Atrybuty bezpieczeństwa

- **Kontrola dostępu** (*access control*)
  zapewnienie, by dostęp do źródła informacji był kontrolowany, w ten sposób, aby tylko uprawnieni użytkownicy mogli korzystać z tej informacji

Atrybuty bezpieczeństwa

- **Rozliczalność/odpowiedzialność** (*accountability/accounting*)

  Możliwość identyfikacji użytkownika odpowiedzialnego za określone działanie w systemie (np. za modyfikację pliku)

Atrybuty bezpieczeństwa

- **Dystrybucja kluczy** (*key management*)

  zapewnienie poprawnej i bezpiecznej (!) wymiany informacji tajnych i parametrów kryptograficznych (klucze, hasła, uzgadnianie algorytmów)

Inne pojęcia

- **Identyfikacja** (*identification*)

  Operacja zgłaszania się użytkownika w systemie, związana z uwierzytelnianiem.

Inne pojęcia

- **Autoryzacja** (*authorization*)

  Nadawanie uprawnień do korzystania z określonych zasobów

Popularne pakiety

- CIA – jak powinny być traktowane nasze dane / informacja

  Confidentiality, Integrity, Availability
- AAA – czego oczekujemy od systemów kontroli dostępu do zasobów

  Authentication, Authorization, Accounting

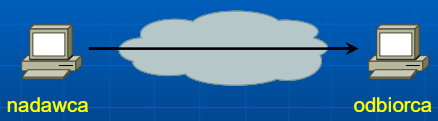
Klasyfikacja zagrożeń bezpieczeństwa

Klasyfikacja zagrożeń w systemach komputerowych

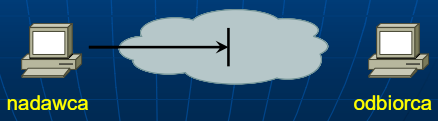
- **Zamierzone** - związane z działaniami wykonywanymi z premedytacją
- **Losowe wewnętrzne** - niezamierzone błędy, zaniedbania użytkowników, defekty sprzętu i oprogramowania
- **Losowe zewnętrzne** - skutki działania temperatury, wilgotności, zanieczyszczenia powietrza, zakłócenia źródła zasilania, wyładowania atmosferyczne, klęski żywiołowe

Zagrożenia bezpieczeństwa w sieciach komputerowych

- Przepływ normalny



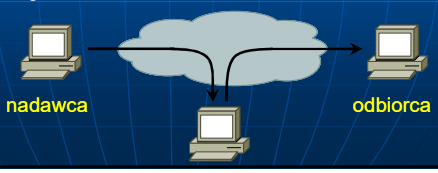
- Przerwanie



Zagrożenia bezpieczeństwa w sieciach komputerowych

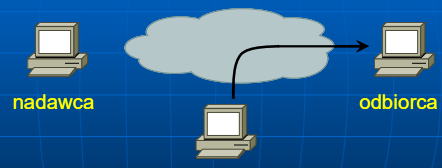
- Przechwycenie

- Modyfikacja

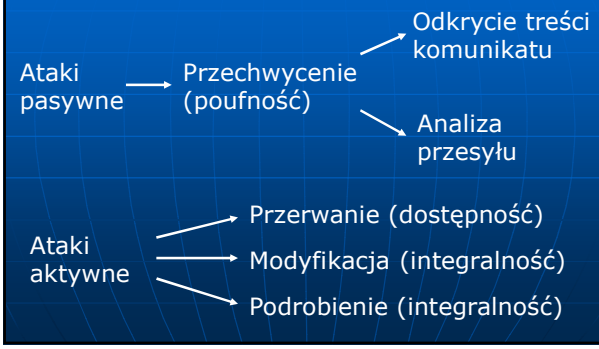


Zagrożenia bezpieczeństwa w sieciach komputerowych

- Podrobienie



Ataki na bezpieczeństwo



Mechanizmy zabezpieczające

Mechanizmy realizacji usług ochrony

Mechanizmy zabezpieczające

- Techniczne
- Fizyczne
- Organizacyjne
- Prawne

Mechanizmy zabezpieczające

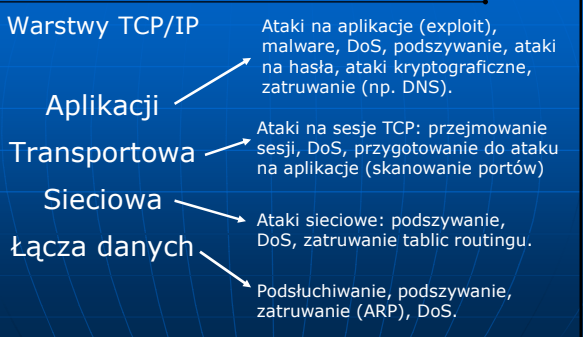
- Kryptografia i steganografia
- Mechanizmy filtrujące i algorytmy rozpoznawania
- Mechanizmy kontroli dostępu
- Mechanizmy podnoszenia niezawodności
- Narzędzia organizacyjne i prawne
- Świadomość i odpowiedzialność użytkowników

Zagrożenia Bezpieczeństwa Sieci Komputerowych

Podstawowe pojęcia

- Zagrożenie (*threat*)
  potencjalne naruszenie zabezpieczeń
- Podatność (*vulnerability*)
  wada lub luka w systemie zabezpieczeń

Bezpieczeństwo w sieci



Etapy ataku

- Rekonesans: adresy IP i domenowe, nazwy kont (socjotechnika)
- Skanowanie sieci i portów
- Wyszukiwanie podatności na otwartych portach
- Exploit, łamanie haseł
- Eskalacja uprawnień, backdoor

Zagrożenia

Warstwa fizyczna

Warstwa fizyczna

- Uzyskanie dostępu do medium
  - Kabel elektryczny
  - Kabel optyczny
  - Kanał bezprzewodowy
- Promieniowanie ujawniające – przypadkowy przeciek informacji

Promieniowanie ujawniające

- Niepożądana emisja akustyczna lub elektromagnetyczna, której sygnał jest skorelowany z informacją użyteczną
- Zagrożenie: infiltracja elektromagnetyczna

TEMPEST

- Badania bezpieczeństwa emisji mają charakter częściowo niejawny
- W USA istnieje niejawny projekt rządowy *Transient ElectroMagnetic Pulse Emanation Standard*, w ramach którego przyznawane są certyfikaty:
  - Kat. 1 – TEMPEST (8 metrów)
  - Kat. 2 – zredukowany TEMPEST (20 m)
  - Kat. 3 – obniżona emisja (100 m)
  - znak CE (w Polsce PN-55022)

Tempest for Eliza

www.erikyyy.de/tempest/

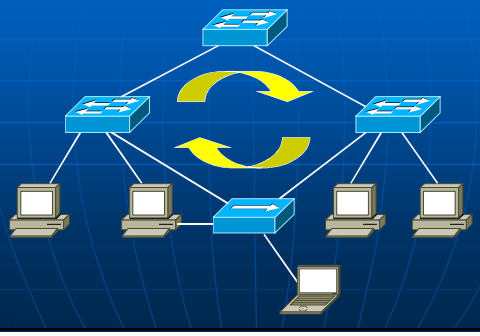
Ograniczanie emisji ujawniającej

- Rozwiązania technologiczne
  wadą są wysokie koszty
- Tłumienie pośrednie
  specjalne konstrukcje ścian, farby, tapety, strefy bezpieczeństwa
- Maskowanie elektromagnetyczne
  wprowadzenie dodatkowych sygnałów szumopodobnych 'zakłócających' niepożądaną emisję

Zagrożenia

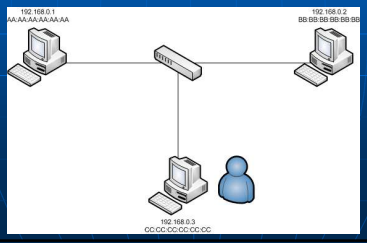
Warstwa łącza danych

Pętle w sieciach Ethernet



Podsłuchiwanie (*sniffing*)

- w domenie kolizyjnej
- w środowisku przełączanym (*ARP Poisoning, ARP Flooding*)



Podszywanie

- Atak na przełącznik:
  - VLAN hoping
  - STP

Zagrożenia

Warstwa sieci

Warstwa sieci

- Podszywanie
  - brama
  - dhcp
  - Router (zatruwanie tablic routingu)
  - Ataki na protokoły routingu
- Routing źródłowy
- Ataki DoS oparte na ICMP

(Distributed) Denial of Service

- Atak polegający na uniemożliwieniu ofierze świadczenia usług (atak na dostępność). Bazuje głównie na błędach w implementacji protokołów:
  - ICMP (Ping of Death, Smurf)
  - TCP (SYN flood, Land.c)
  - UDP (UDP flood)
  - Fragmentacji pakietów (TearDrop)

Atak *Ping of Death*

Polega na wysłaniu zapytania ICMP pakietem o rozmiarze > 65535 B

ping -l 65510 <adres_ip>

65510 + 20 (nagłówek IP) +
8 (zapytanie ICMP - Echo Request)

Atak *Smurf*

- Atakujący wysyła spreparowane pakiety do różnych urządzeń w sieci (*ping request*)
- Jako adres nadawcy podaje adres celu ataku

Zagrożenia

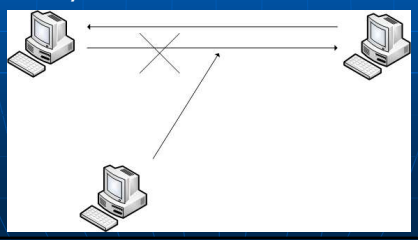
Warstwa transportowa

Warstwa transportowa

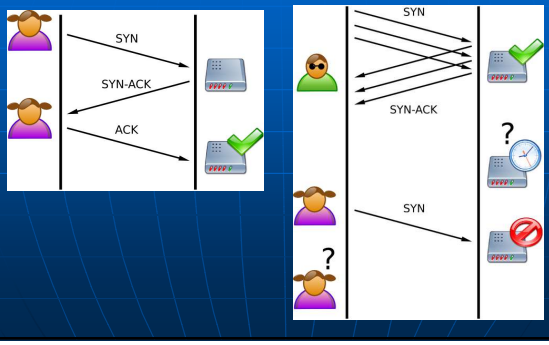
- Przejęcie sesji TCP/IP
- Odmowa usług: DoS i DDoS
- Skanowanie portów

Przejęcie sesji

- Przerwanie połączenia za pomocą RST
- Atak na generatory liczb pseudolos.
- Przewidywanie ISN



Atak *SYN flood* (DoS)

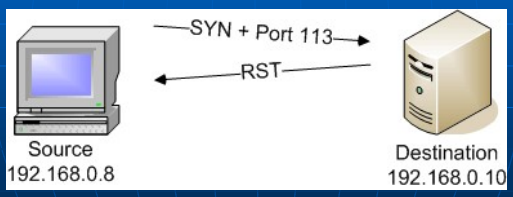


Atak *Land.c* (DoS)

- Atak polega na spreparowaniu pakietu TCP wysyłanego do atakowanego systemu
- Jako adres nadawcy (urządzenia chcącego nawiązać połączenie) podawany jest adres celu ataku
- Zaatakowany nawiązuje połączenie sam ze sobą

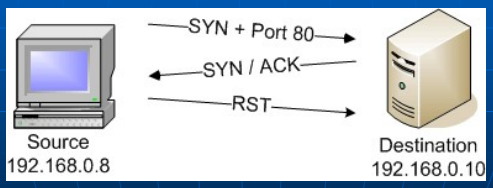
Skanowanie portów

- TCP [SYN] Scan



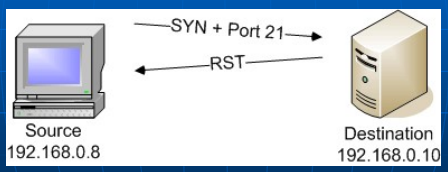
Skanowanie portów

- TCP [SYN] Scan



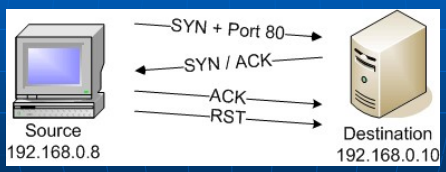
Skanowanie portów

- TCP connect() scan



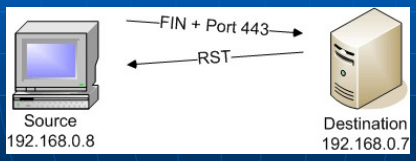
Skanowanie portów

- TCP connect() scan



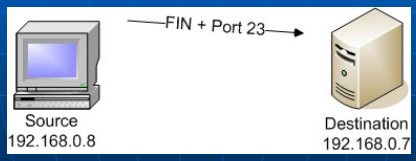
Skanowanie portów

- [FIN] scan



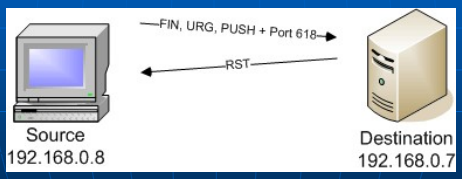
Skanowanie portów

- [FIN] scan



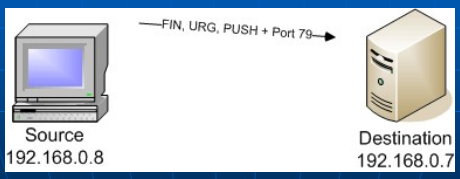
Skanowanie portów

- Xmas tree scan



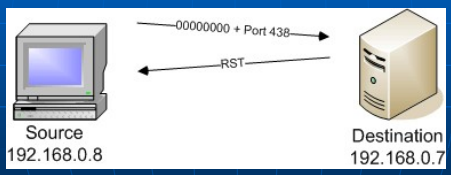
Skanowanie portów

- Xmas tree scan



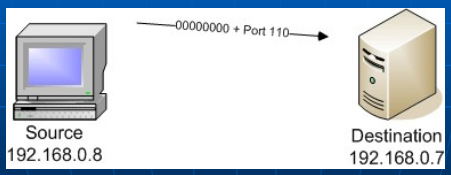
Skanowanie portów

- Null scan



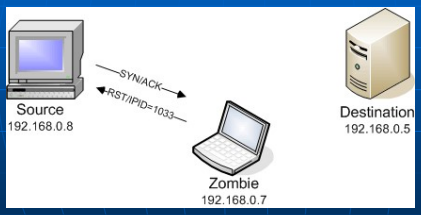
Skanowanie portów

- Null scan



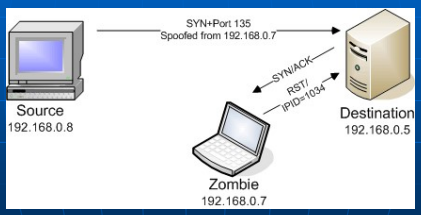
Skanowanie portów

- Idle scan



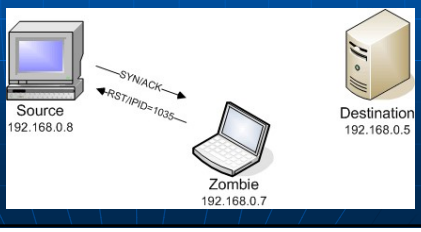
Skanowanie portów

- Idle scan



Skanowanie portów

- Idle scan



Zagrożenia

Warstwy wyższe (aplikacji)

Malicious software

- Wirus, makrowirus
- Robak (*worm*)
- Koń trojański

- Bomba (logiczna, czasowa)
- Dialer
- Exploit

Wirusy

- Wymagają programu-nosiciela
  - Kod wirusa jest doklejany do kodu nosiciela
- Uruchamiają się gdy jest uruchamiany nosiciel
- Rozmnażają się infekując kolejne programy
- Wykonują działania destrukcyjne

Robaki (worm)

- Samodzielny program lub moduł wykonywalny
- Potrafi rozprzestrzeniać się samodzielnie, np. za pomocą poczty
- Może powielać się lawinowo zużywając zasoby (pamięć, moc obliczeniową, przepustowość sieci)

Koń trojański

- Pozornie pożyteczny program, jednak zawierający nieudokumentowany, szkodliwy kod
- Brak zdolności samoreplikacji
- Może być kopiowany za pomocą robaków lub wirusów

- Remote Access Trojan (Backdoor)
- Rootkit (Keylogger)

Malware - Działania

- Backdoor
- Usunięcie/uszkodzenie danych
- Kradzież danych
- Atak odmowy usługi – wyłączenie komputera, zablokowanie zasobów
- Wykorzystanie komputera do celów przestępczych (*zombie*) – na przykład do ataku DDoS

Malware – mechanizmy obronne

- Szyfrowanie - malware szyfruje siebie i na początku umieszcza klucz deszyfrujący. W trakcie propagacji używany jest ten sam klucz deszyfrujący, co umożliwia skanerom antywirusowym wyłapanie malware poprzez poszukiwania klucza

Malware – mechanizmy obronne

- Technika oligomorficzna - malware jest w stanie zmienić (kilka razy) klucz deszyfrujący
- Technika polimorficzna - zmiana klucza deszyfrującego za każdym razem (bardzo trudna detekcja)

Ataki na aplikacje

- Przepełnienie bufora
- Przepełnienia stosowe
- Ciągi formatujące
- Wstrzykiwanie kodu powłoki

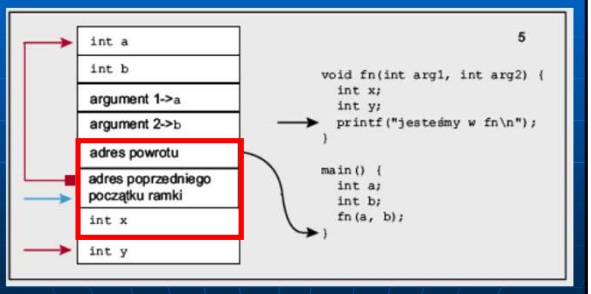
Przepełnienie bufora

```
void fn(char *a) {
  char buf[10];
  strcpy(buf, a);
  printf("koniec funkcji  fn\n");
}

main (int argc, char *argv[]) {
  fn(argv[1]);
  printf("koniec\n");
}
```

C:\> prog Tekst
C:\> prog Bardzo_długi_tekst_przepełniający

Przepełnienie stosu



Wstrzykiwanie kodu

Zamiast przypadkowego łańcucha do bufora wpisujemy ciąg poleceń i adres tego ciągu w pamięci

Wstrzykiwanie kodu

```
char shellcode[] =
„\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\x16\x5b\x31\xc0”
„\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d”
„\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73”
„\x68”;
```

- Shellcode trzeba umieścić w pamięci procesu (najczęściej podać jako argument funkcji),
- Nadpisać (również argumentem funkcji) adres powrotu i zastąpić go adresem `shellcode`

Ciągi formatujące

```
string = „%x”;

printf(„%s”, string);
```

- Umożliwia odczytanie dowolnej komórki pamięci
- Umożliwia zapis (poprzez ciąg formatujący %u) pod dowolny adres w pamięci

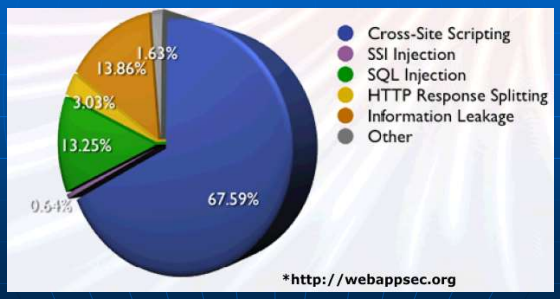
SQL Injection

Wykorzystuje lukę w zabezpieczeniach polegającą na:

- nieodpowiednim filtrowaniu lub niedostatecznym typowaniu
- i późniejszym wykonaniu danych przesyłanych w postaci zapytań SQL do bazy danych

Atak SQL – jak unieszkodliwić radar

Ataki na aplikacje webowe



Phishing