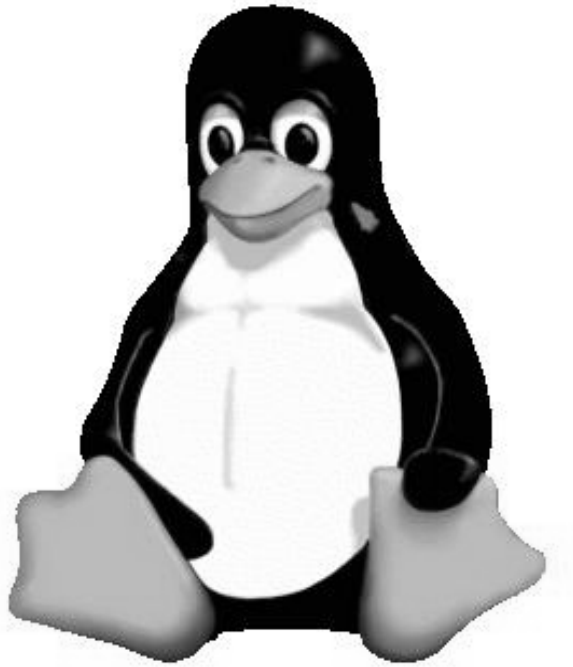
Bezpieczny serwer sieciowy Linux



Jacek Lach

2002

Plan wykładów

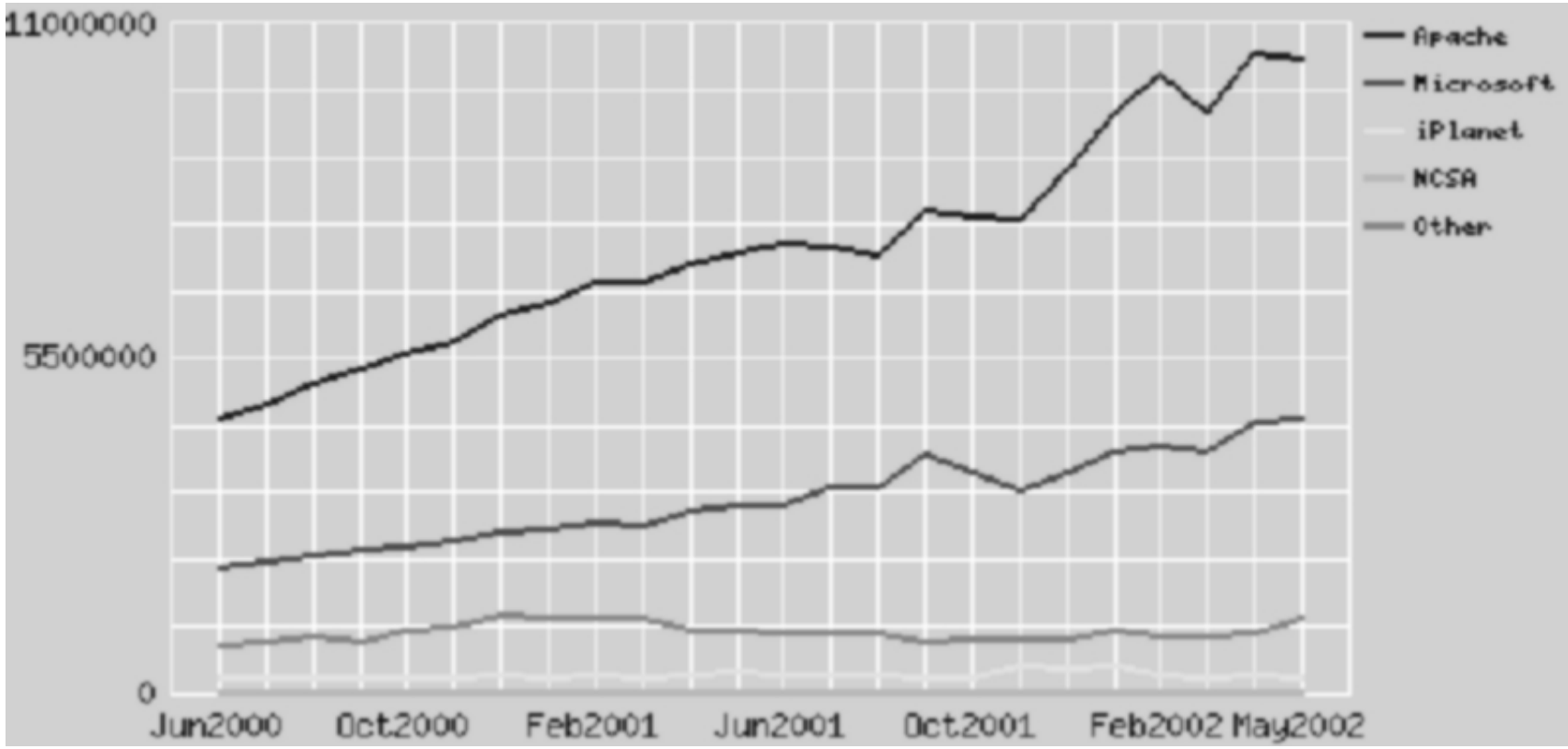
- Wykład wprowadzający
- Testy penetracyjne I - wywiad środowiskowy, skanowanie sieci, skanowanie portow
- Testy penetracyjne II - identyfikacja systemu, narzędzia, przykłady zastosowań
- Zabezpieczanie systemu po instalacji, identyfikacja działających usług
- Zdalny dostep: ssh - konfiguracja, tryby połączeń, typy autentykacji, zabezpieczanie
- Systemy ids. hids, nids. Sposoby działania, przykłady: tripwire, snort
- Firewall'e, wprowadzenie do tematyki, ogólne zasady projektowania firewalli
- Netfilter

Plan wykładów - cd.

== KONFIGURACJA USŁUG ==

- Apache
- Sendmail
- FTP - proftpd
- DNS
- Bazy danych

Liczba serwerów WWW w sieci



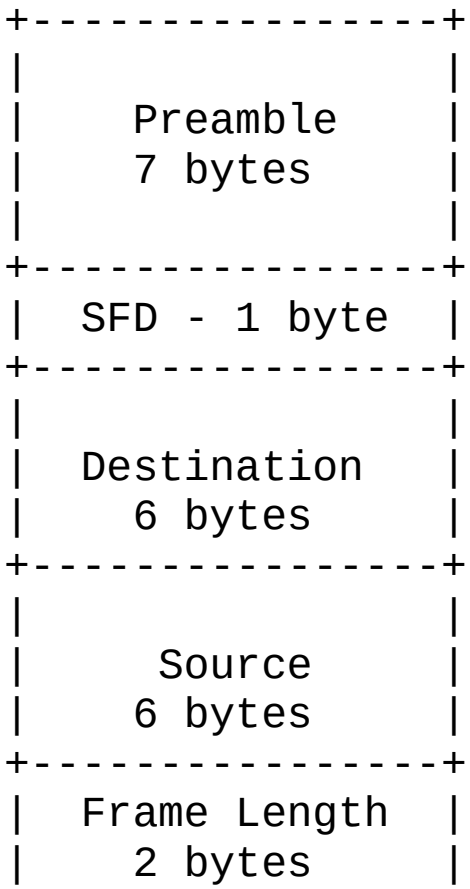
Rodzaje zagrożeń

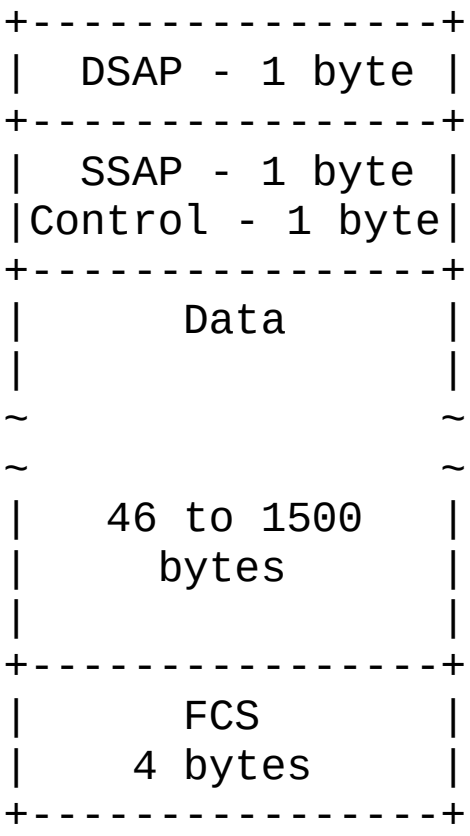
- Penetracja - nieautoryzowane testowanie zastosowanych zabezpieczeń
- Włamanie - bezprawne uzyskanie dostępu do konta/uprawnień użytkownika
- Odmowa usługi - zablokowanie lub obniżenie wydajności udostępnianych usług
- Nieprawidłowe użytkowanie
  - Podszywanie - udawanie innego użytkownika
  - Podsłuchiwanie - uzyskiwanie informacji przeznaczonych dla innego użytkownika
  - Przekłamywanie - naruszanie poprawności dostępnych danych

Zagrożenia - Top 20 (SANS/FBI)

- Remote Procedure Calls (RPC)
- Apache Web Server
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- R-Services -- Trust Relationships
- Line Printer Daemon (LPD)
- Sendmail
- BIND/DNS
- General Unix Authentication -- Accounts with No Passwords or Weak Passwords

Podstawy - ETHERNET



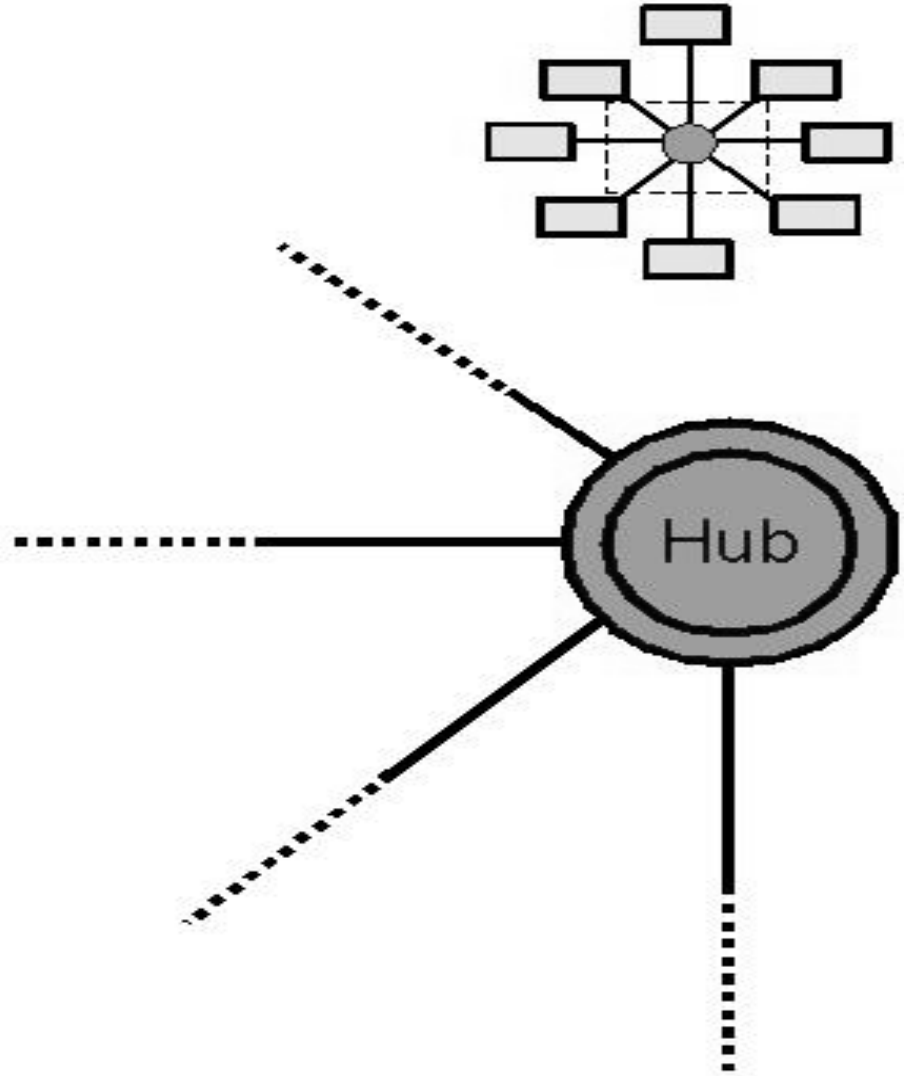


Podstawy - topologie sieci

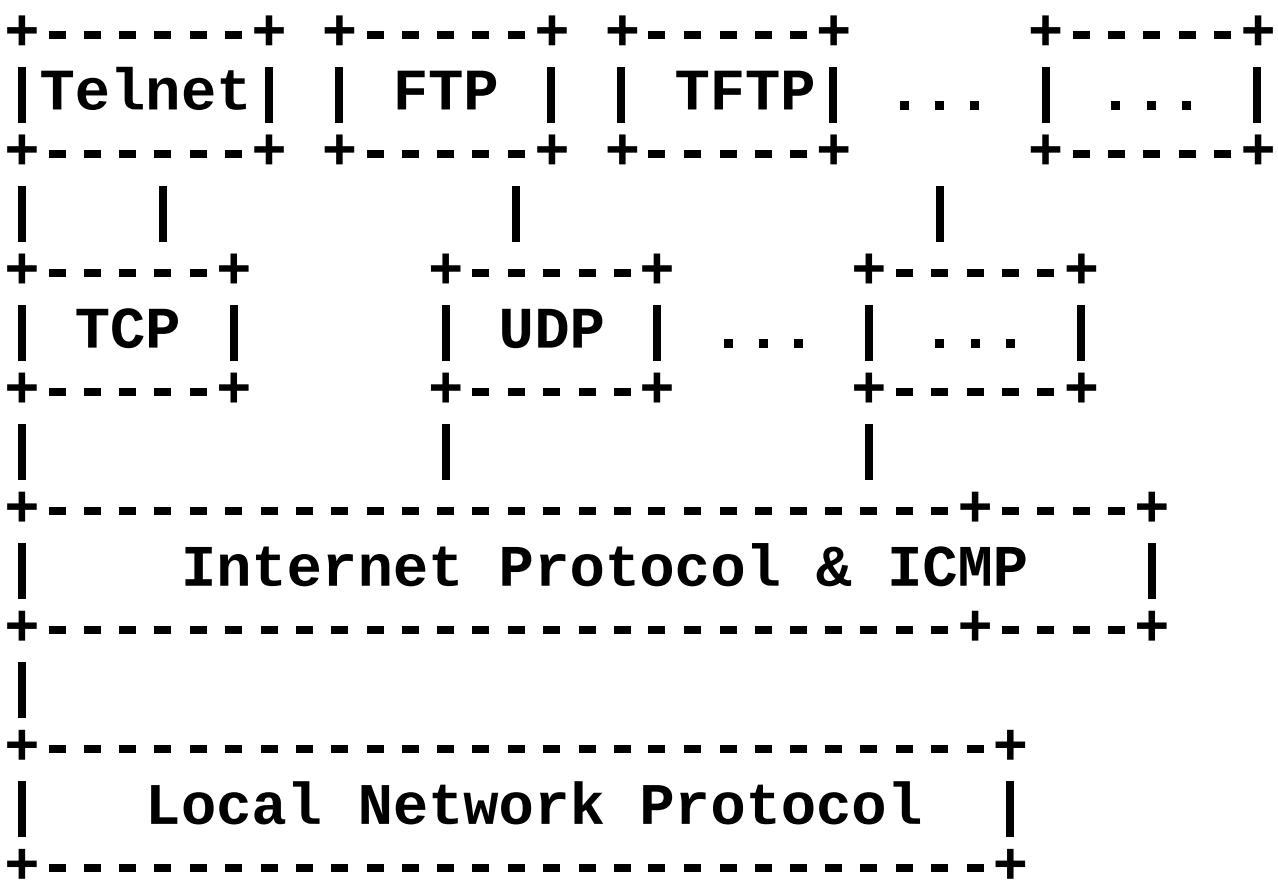
Wybrane topologie:

- magistrala
- pierścień
- gwiazda
- topologia przełączana

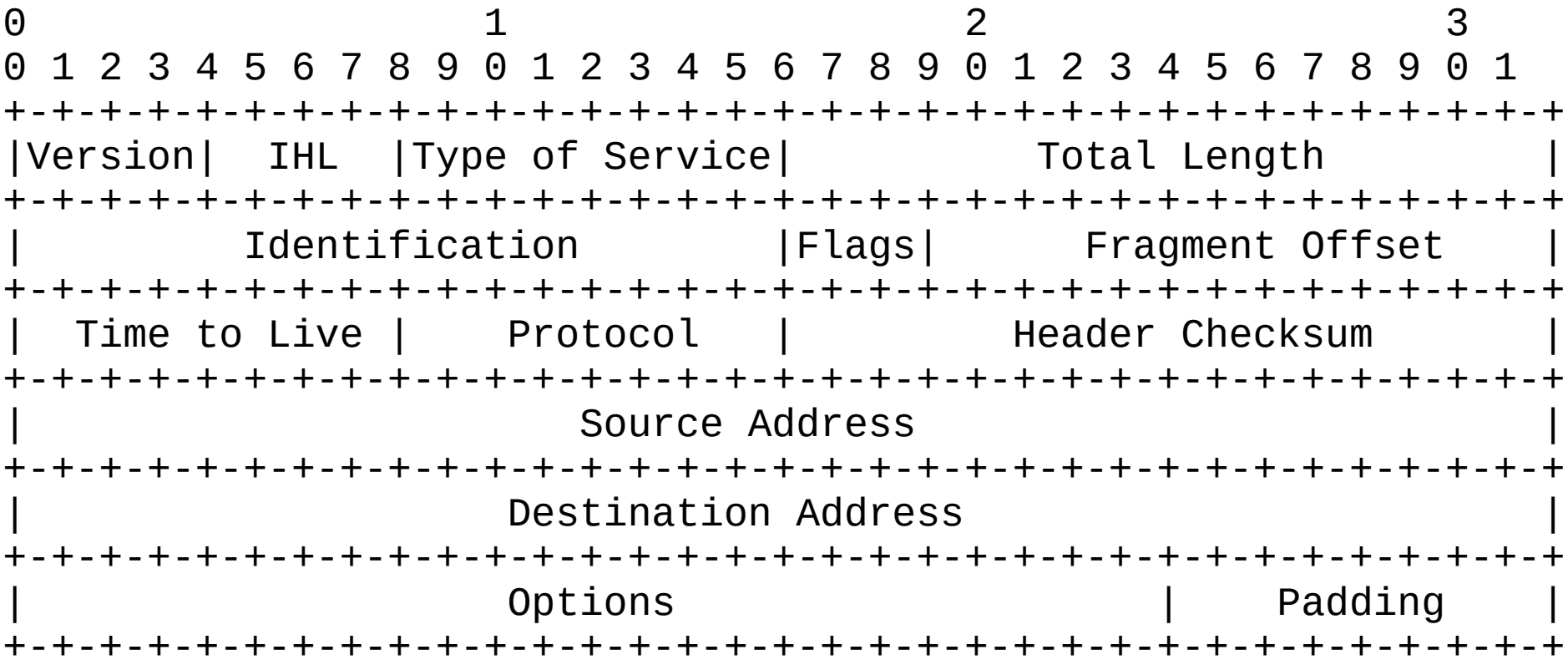
Podstawy - koncentrator vs przełącznik



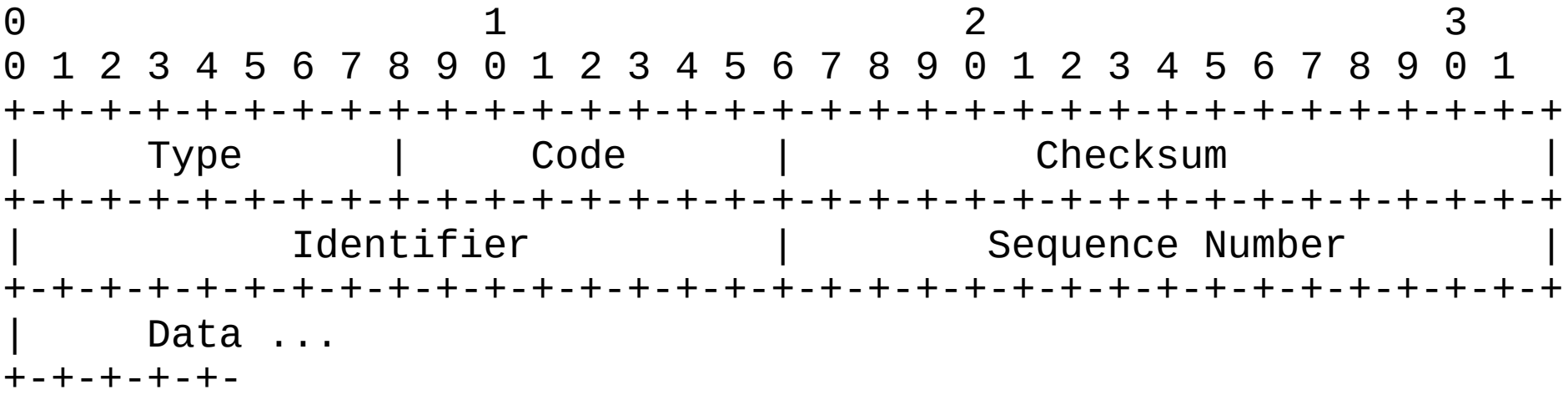
Podstawy - model warstwowy



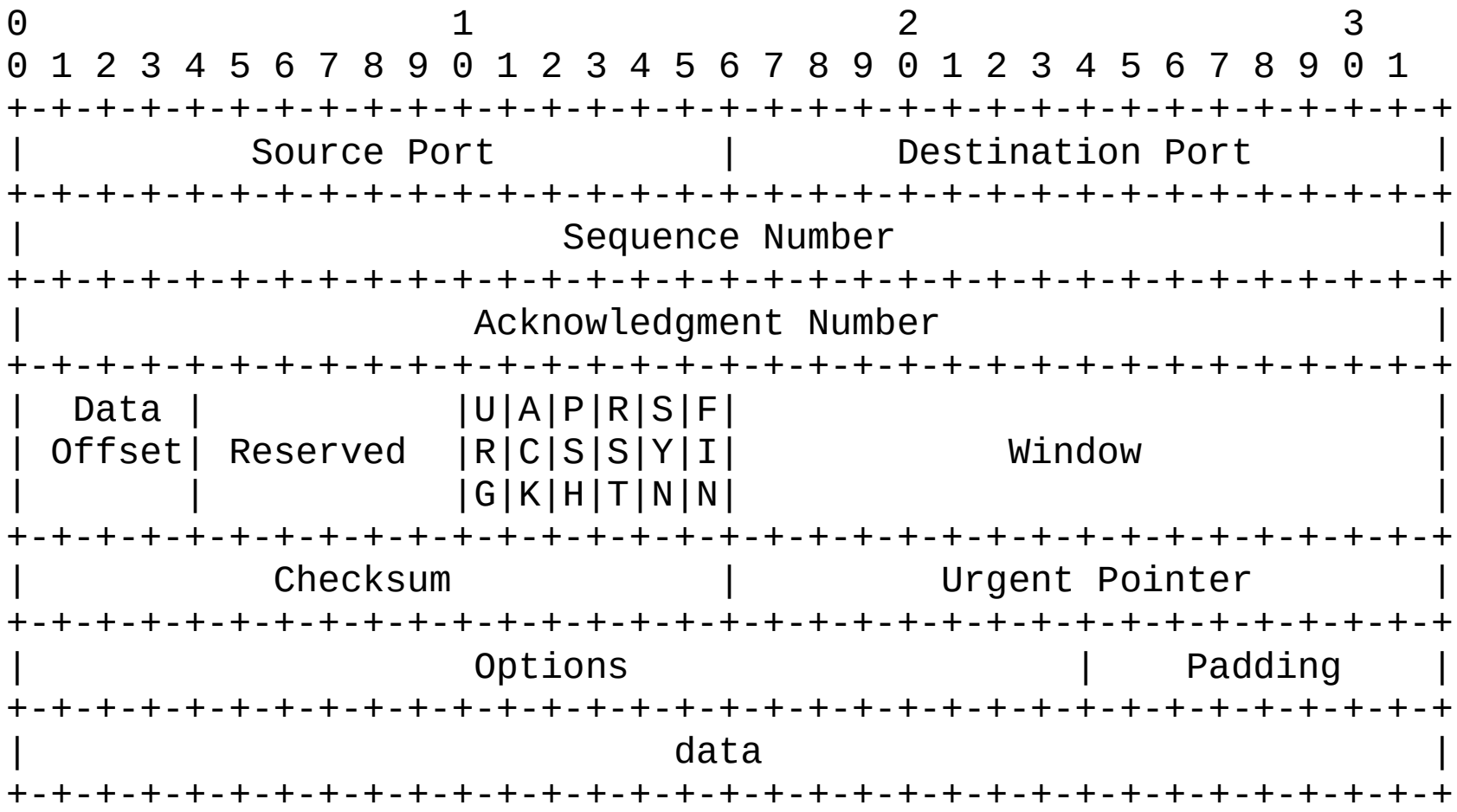
Podstawy - IP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

Podstawy - ICMP



Podstawy - TCP



TCP - nawiązanie połączenia

- Host 1 (ISN1 – SYN) > Host2
- Host2 (ACK - ISN1, SYN - ISN2) > Host1
- Host1 (ACK - ISN2) > Host2
- Zamknięcie połączenia: (FIN)

Test penetracyjny

- Celem testu jest wykazanie odporności na działania podejmowane zwykle przez włamywacza
- Wykonaniem testu zajmuje się inżynier bezpieczeństwa bądź firma wykonująca testy zabezpieczeń (włamanie na zlecenie)
- "Zobacz co Twój system ma do powiedzenia zanim powie to innym"

Etapy testu penetracyjnego

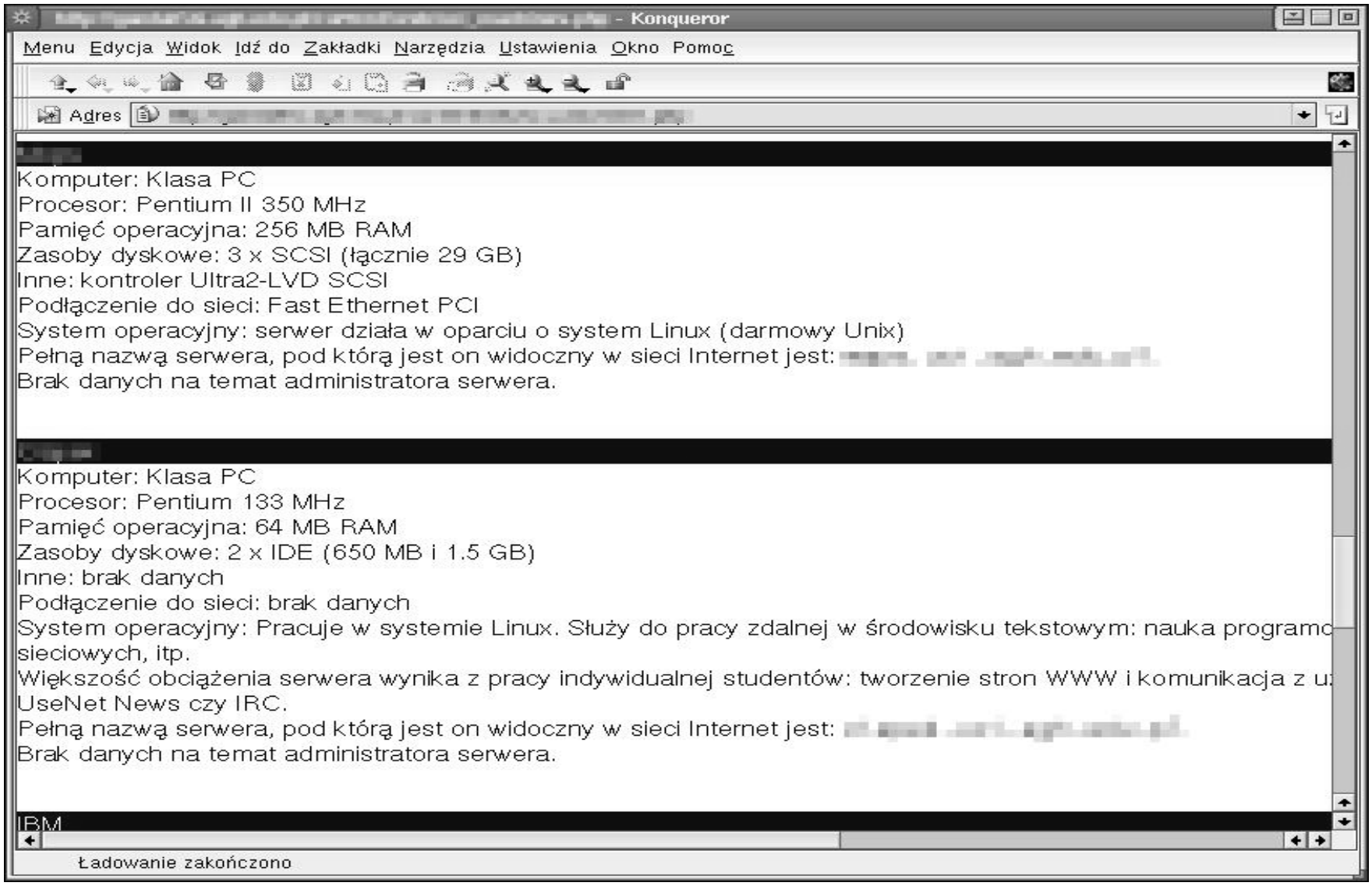
- Wywiad środowskowy
- Rekonesans sieci
- Skanowanie portów
- Identyfikacja systemu operacyjnego

Wywiad środowiskowy

Identyfikacja zagrożeń związanych z informacjami udostępnianymi poprzez:

- Strony WWW instytucji oraz pracowników
- Listy dyskusyjne, w których administratorzy biorą aktywny udział
- Nadmiarowe rekordy DNS (HINFO, WKS, TXT)

WWW - zły przykład



DNS – zły przykład

- HINFO
  host.domain.com IN HINFO VAX-11/780 UNIX
- TXT
  host.domain.com IN TXT (Lokalizacja: p505)
- WKS
  host.domain.com IN x.x.x.x TCP (telnet ftp domain smtp)

Listy dyskusyjne - zły przykład

- **I have apache 1.3.19. How do I remove the os banner [...]**
  XXX YYY
  Security/Network Administrator
  mailto:XYYY@domena.com
- The site www.domena.com is running **Apache/1.3.19 (Unix) (Red-Hat/Linux) mod_ssl/2.8.1 OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4pl1 mod_perl/1.24_01** on **Linux**
- Dodatkowe informacje: DNS, poczta

Za tydzień...

- Skanowanie sieci
- Skanowanie portów
- Identyfikacja systemu operacyjnego