Projekt multispoof

System automatycznego wykorzystywania podatności sieci lokalnych pod względem nieupoważnionego dostępu

Opracował:
Paweł Pokrywka

Promotor:
dr Tomasz Surmacz

Prowadzący seminarium dyplomowe:
prof. Wojciech Zamojski

Plan prezentacji

- Autentykacja w sieciach lokalnych
- multispoof
  - Wprowadzenie
  - Budowa systemu
  - Wyniki
- Detekcja
- Zagłuszanie
- Prewencja
- Kierunki dalszego rozwoju

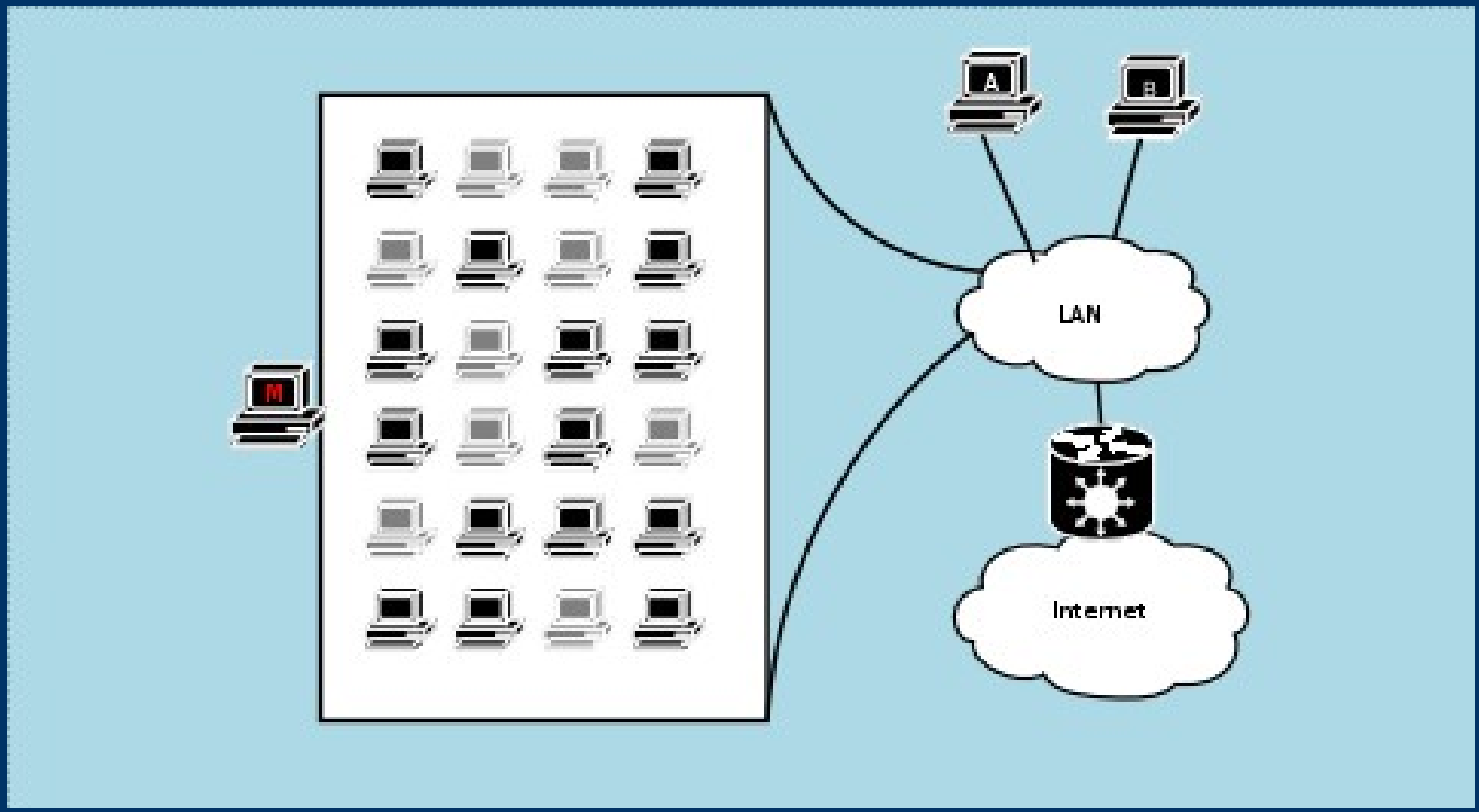
Autentykacja w sieciach lokalnych

- Obszar zainteresowań: sieć lokalna z dostępem do Internetu
- Sieć składa się z połączonych ze sobą komputerów
- Za dostęp do sieci płacą ludzie
- Ludzie korzystają z sieci za pomocą komputerów
- Jak powiązać transmisje sieciowe komputera z człowiekiem?

Autentykacja w sieciach lokalnych

- Najpopularniejsze technologie:
  - Ethernet
  - Fast Ethernet
  - WiFi
- Autentykacja ludzi na postawie adresów hostów:
  - Tylko adres IP (!)
  - Para IP-MAC
  - Inne metody w dalszej części prezentacji
- Adres można zmienić (tajemnica!): spoofing

multispoof: Idea



multispoof: Procesy

- Zmiany adresów IP i MAC
- Monitorowanie sieci w celu wykrywania nieaktywnych hostów
- Rozkładanie obciążenia

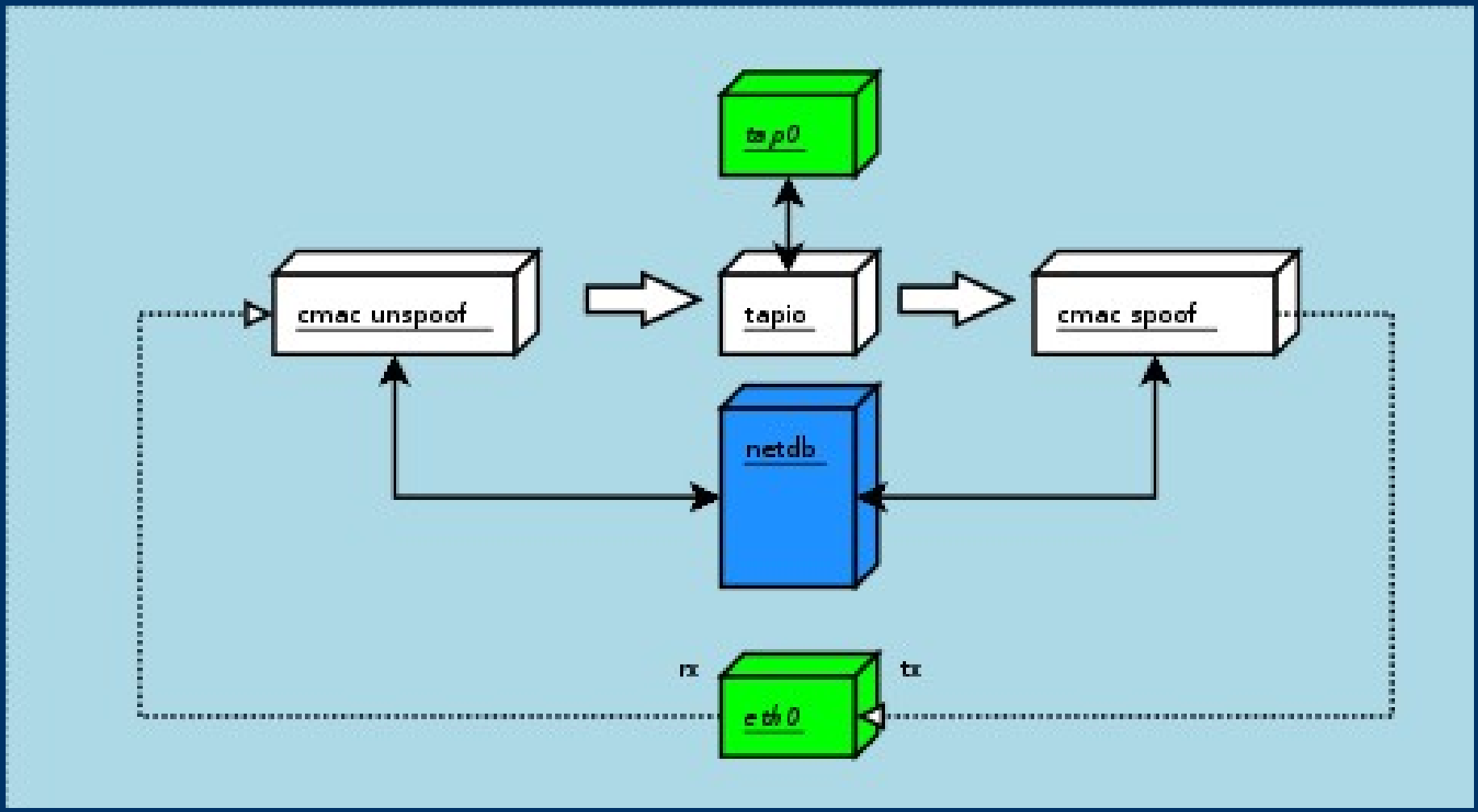
multispoof: Architektura

- Wiele równolegle odbywających się procesów
- Procesy unixowe
  - Modularyzacja i jej zalety
  - Wpływ na wydajność
- IPC
  - Potoki
  - Gniazda lokalne
- Współpraca z jądrem systemu operacyjnego
  - Interfejsy wirtualne tun/tap
  - netfilter

multispoof: oprogramowanie bazowe

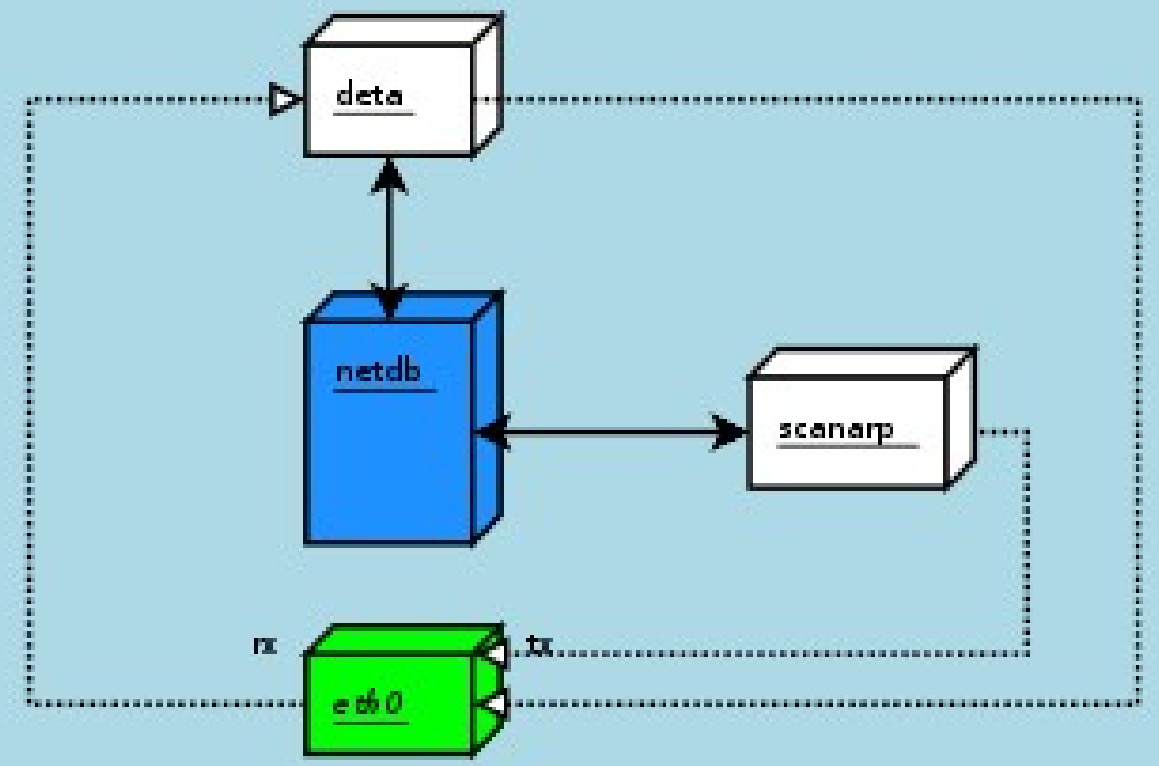
- Linux
  - http://www.kernel.org/
- netfilter + p-o-m
  - http://www.netfilter.org/
- Libnet
  - http://www.packetfactory.net/libnet/
- LIBPCAP (CVS)
  - http://www.tcpdump.org/
- GLib
  - http://www.gtk.org/

multispoof: Zmiana MAC

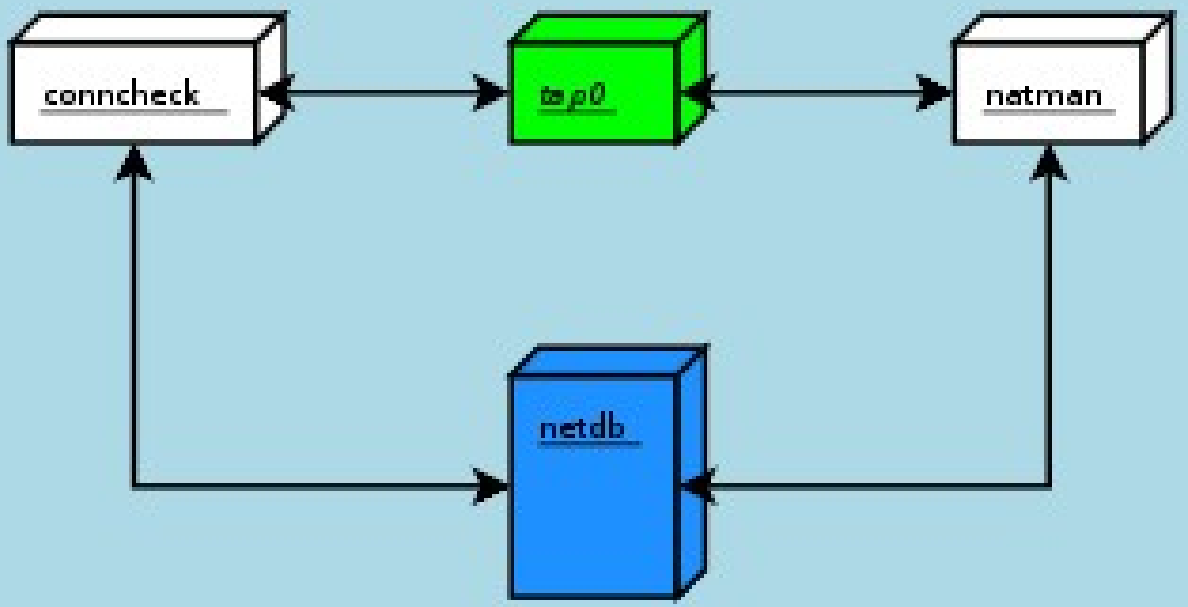


rx | cmac unspoof | tapio | cmac spoof | tx

multispoof: Monitorowanie sieci

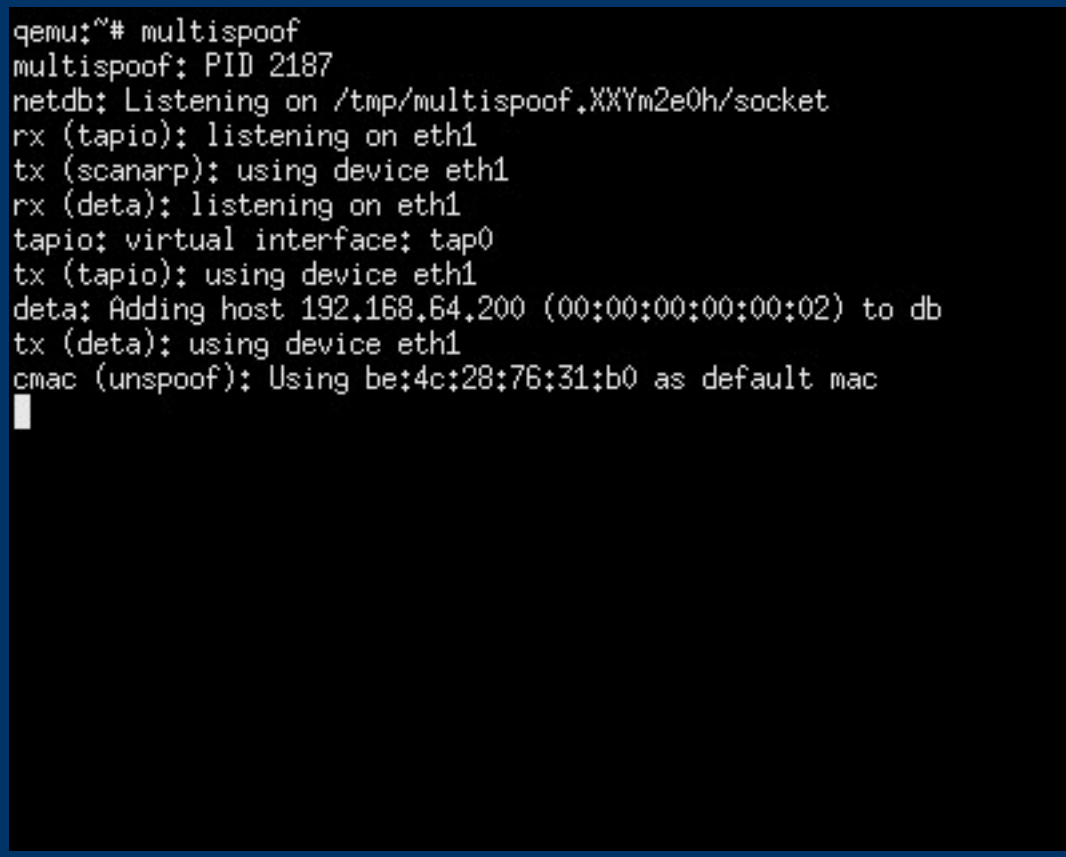


multispoof: Testowanie i LB



Rezultaty

- Działa :)
- Kompilacja i instalacja:
  - make
  - su -c “make install”
- Wyniki:
  - 80-200kbit/s na hosta
  - >2mbit/s - 20 hostów



Detekcja

- Słabości **aktualnej** wersji
- Wykrywanie skanowania ARP
- Fingerprinting, skanowanie portów
- Hosty - pułapki
- Korelacja transmisji sieciowych
- **Moment pojawienia się komputera w sieci**
- Brak standardowych transmisji (DHCP, SMB, ARP)

Zagluszanie

- Utrzymywanie sztucznej aktywności hostów
- Uruchomienie drugiej kopii programu
  - multispoof wyklucza możliwość wielokrotnego uruchamiania w jednej sieci fizycznej
  - MAC? ;-)

Prewencja: Zalozenia

- Użytkownik korzysta z sieci w sesjach
- Na sesję składa się:
  - Logowanie - autentykacja
  - Korzystanie z usługi
  - Wylogowanie – zakończenie sesji
- Sesja musi spełniać następujące warunki:
  - Rozpoczęcie i zakończenie następuje tylko na życzenie osoby, która wykupiła usługę (wylogowanie - DoS)
  - Wszystkie transmisje muszą być uwierzytelnione (niekoniecznie szyfrowane, MAC)
- Powyższe najczęściej wymaga silnej kryptografii

Prewencja: Metody

- Inteligentne przełączniki sieciowe
  - *Port security*
  - 802.1x
- Inna technologia sieci
- Autoryzujące serwery proxy
- Portale, authpf
- VPN (IPSec, PPTP, PPPoE, L2TP, OpenVPN)
- Firewall

Kierunki dalszego rozwoju

- Utrudnianie wykrywania:
  - Randomizacja (kolejność skanowania, interwały)
  - Symulacja normalnej aktywności hosta (DHCP, zapytania ARP, tyle tablic ARP co hostów, honeyd)
  - Problem pojawienia się komputera w sieci:
    - Resetowanie połączeń – tak, czy nie?
    - Przewidywanie przyszłości
- Wybór trybu pracy:
  - wydajność transmisji typu *bulk*
  - wygoda przy normalnym użytkowaniu (priorytety)
  - anonimowość (brak skanowania, tylko jedno IP)
- Statystyki

Download

- Projekt multispoof będzie dostępny w Internecie: http://cryptonix.org/