BEZPIECZEŃSTWO TELEINFORMATYCZNE

Wojewódzki Ośrodek Informatyki
Terenowy Bank Danych
w Szczecinie

Andrzej Nowicki
anowicki@szczecin.uw.gov.pl

Kategoryzacja informacji przetwarzanych w systemach teleinformatycznych

- Ochrona informacji niejawnych
- Ochrona danych osobowych
- Ochrona „pozostałych” systemów IT

Ochrona informacji niejawnych

- Szczególne wymagania bezpieczeństwa systemu
- Procedury bezpiecznej eksploatacji

Ochrona danych osobowych

- ***Polityka bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony***
- ***Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych***

Bezpieczeństwo systemów IT

- **Rozporządzenie rady ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych**
- § 3. 1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
- 2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniając postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

Rodzaje zagrożeń, na które są narażone systemy IT

- Zagrożenia zewnętrzne
- Zagrożenia wewnętrzne
- Ochrona antywirusowa
- Ochrona antyspamowa
- Czynnik ludzki

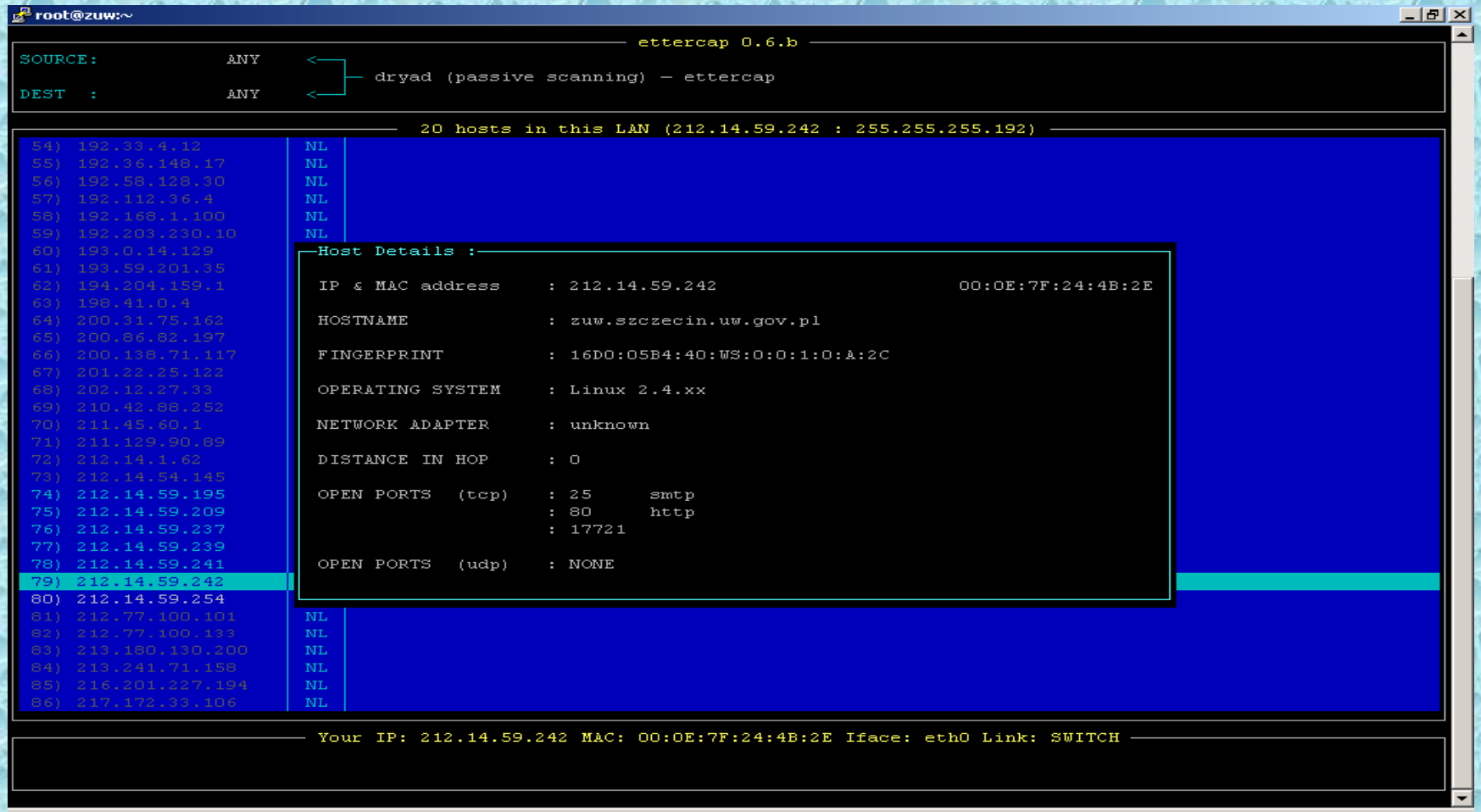
Zagrożenia zewnętrzne # 1

- Sniffing/scanning:
- *network sniffing* (ettercap)
- *network scanning* (nmap)

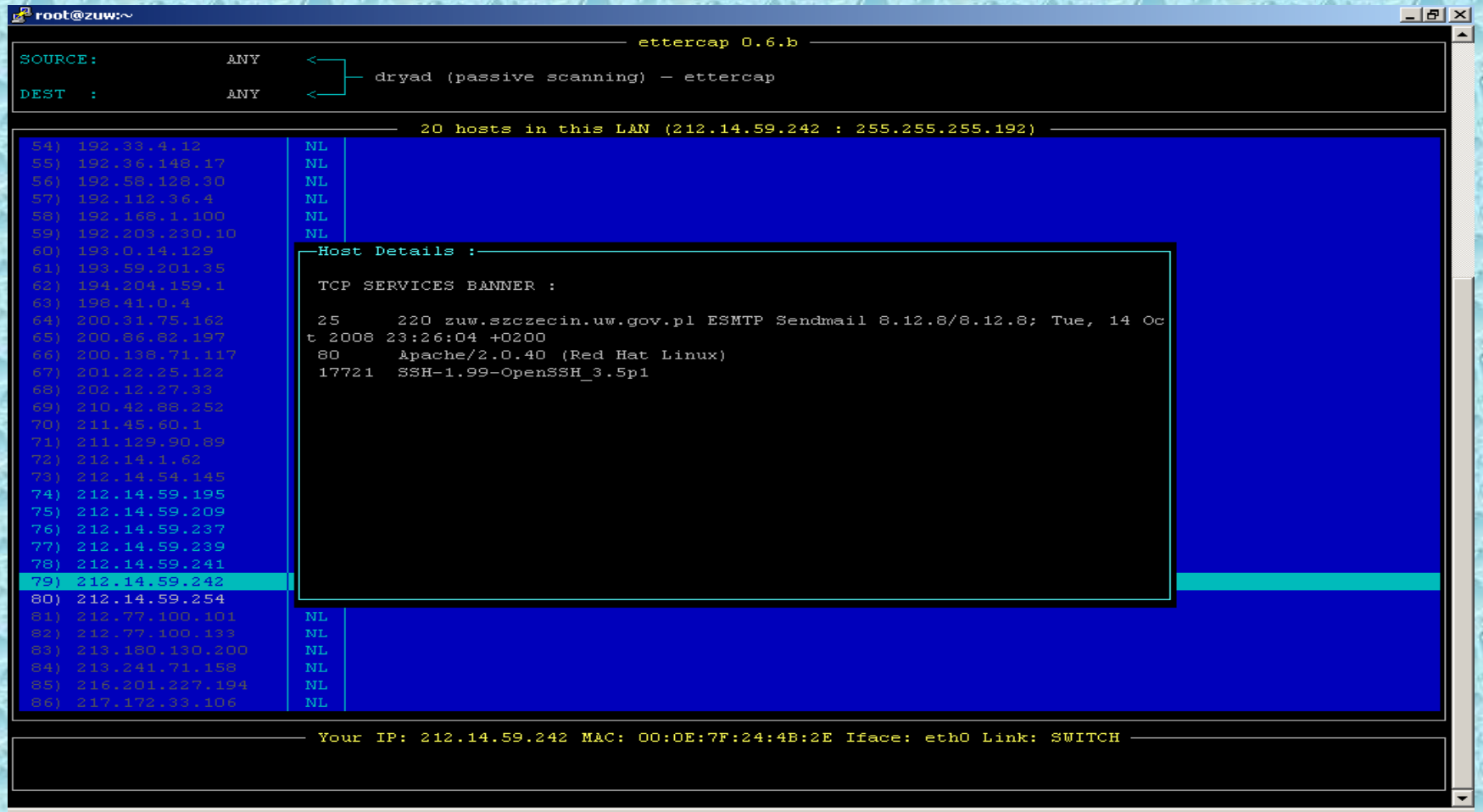
network scanning (nmap)

- Starting nmap 3.48 (http://www.insecure.org/nmap/) at 2008-10-14 23:16 CEST
- Interesting ports on reverse.lightup.net (207.111.54.82):
- (The 1648 ports scanned but not shown below are in state: closed)
- PORT STATE SERVICE
- 80/tcp open http
- 135/tcp open msrpc
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds
- 1025/tcp open NFS-or-IIS
- 1026/tcp open LSA-or-nterm
- 1212/tcp open lupa
- 1433/tcp open ms-sql-s
- 3389/tcp open ms-term-serv

network sniffing (ettercap)



network sniffing (ettercap)



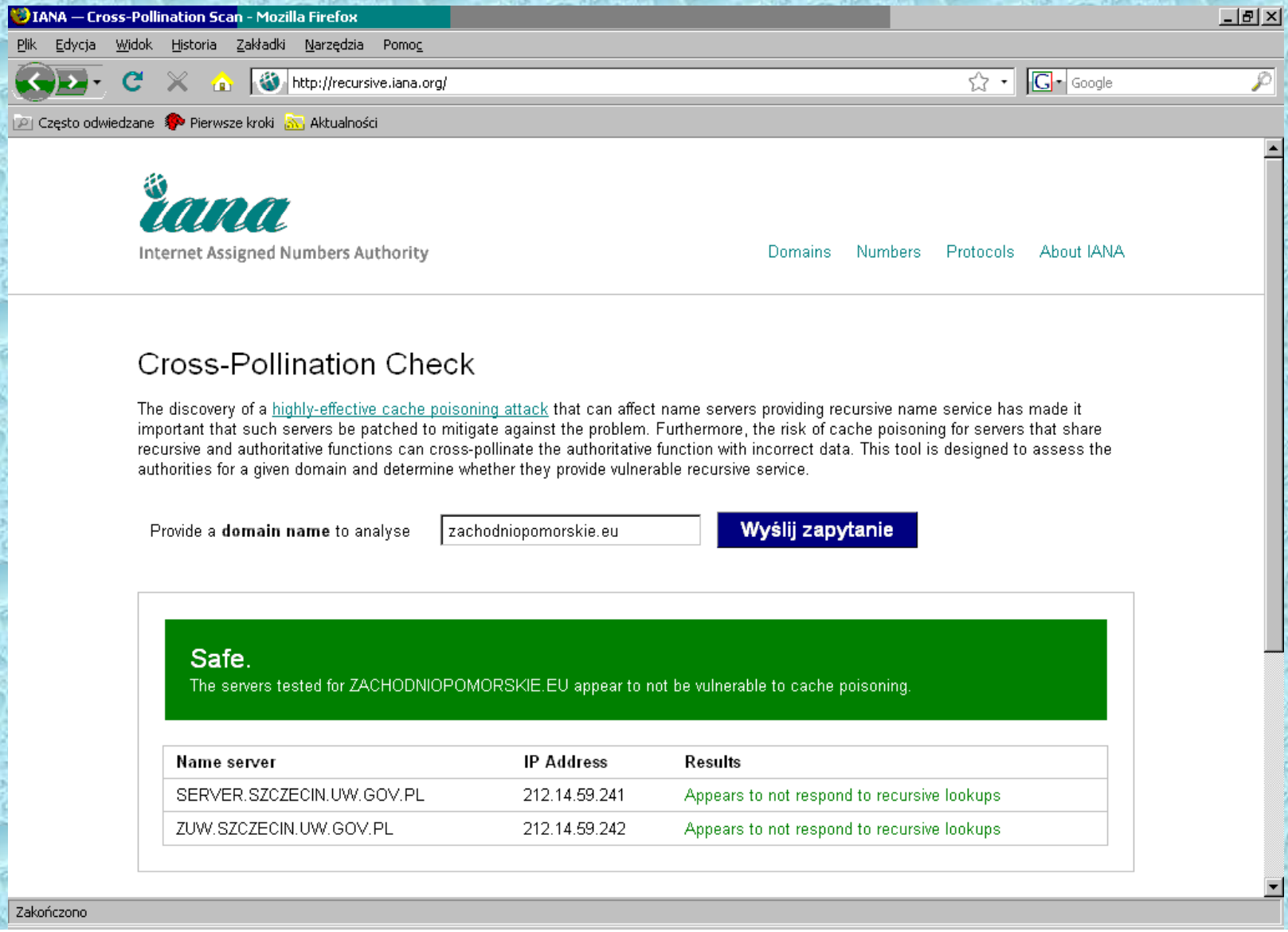
Zagrożenia zewnętrzne # 2

- Spoofing:
  - *session hijacking*
  - *TCP spoofing*
  - *UDP spoofing*

Zagrożenia zewnętrzne # 3

- Poisoning:
- *ARP spoofing/poisoning*
- *DNS cache poisoning* (*pharming*, także znany jako *birthday attack*)
- *ICMP redirect*
- ataki na urządzenia sieciowe przy pomocy protokołu SNMP
- Denial of Service (DoS)

DNS cache poisoning



Przykład ataku

- Użycie sniffer'a – pasywne skanowanie
- Umieszczenie sniffer'a w dowolnym punkcie węzłowym połączenia klient-server
- lub
- *Użycie DNS cache poisoning*
- Na podstawie zdobytych danych zalogowanie do systemu

Dziękuję za uwagę

Andrzej Nowicki
Administrator sieci
Wojewódzkiego Ośrodka Informatyki Terenowego Banku Danych w Szczecinie
anowicki@szczecin.uw.gov.pl
091-4303-444
501-579-907